Algorithms and Bounds for Complex and Quaternionic Lattices with Application to MIMO Transmission

Sebastian Stern, *Member, IEEE,* Cong Ling, *Member, IEEE,*
and Robert F.H. Fischer, *Senior Member, IEEE*

Abstract

Lattices are a popular field of study in mathematical research, but also in more practical areas like cryptology or multiple-input/multiple-output (MIMO) transmission. In mathematical theory, most often lattices over real numbers are considered. However, in communications, complex-valued processing is usually of interest. Besides, by the use of dual-polarized transmission as well as the by the combination of two time slots or frequencies, four-dimensional (quaternion-valued) approaches become more and more important. Hence, in this paper, well-known lattice algorithms and related concepts are generalized to the complex and quaternion-valued case. To this end, a brief review of complex arithmetic, including the sets of Gaussian and Eisenstein integers, and an introduction into quaternion-valued numbers, including the sets of Lipschitz and Hurwitz integers, are given. On that basis, generalized variants of two important algorithms are derived: first, of the polynomial-time LLL algorithm, resulting in a reduced basis of a lattice, and second, of an algorithm to calculate the successive minima—the norms of the shortest independent vectors of a lattice—and its related lattice points. Generalized bounds for the quality of the particular results are established and the asymptotic complexities of the algorithms are assessed. These findings are extensively compared to conventional real-valued processing. It is shown that the generalized

S. Stern and R.F.H. Fischer are with the Institute of Communications Engineering, Ulm University, 89081 Ulm, Germany (e-mail: sebastian.stern@uni-ulm.de; robert.fischer@uni-ulm.de).

C. Ling is with the Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, United Kingdom (e-mail: cling@ieee.org).

Parts of this work have been discussed in the conference paper [1] presented at the 25th International Conference on Telecommunications, Saint Malo, France, 2018, and in the author's dissertation [2].

This work has been supported in part by the Deutsche Forschungsgemeinschaft (DFG) under grant Fi 982/13-1 and in part by the Engineering and Physical Sciences Research Council (EPSRC) under grant EP/S021043/1.

approaches outperform their real-valued counterparts in complexity and/or quality aspects. Moreover, the application of the generalized algorithms to MIMO communications is studied, particularly in the field of lattice-reduction-aided and integer-forcing equalization.

Index Terms

Lattices, lattice reduction, LLL algorithm, successive minima, Gaussian integers, Eisenstein integers, quaternions, Lipschitz integers, Hurwitz integers, MIMO, lattice-reduction-aided equalization, integer-forcing equalization.

I. Introduction

The concept of lattices has been studied for almost two centuries. Initial work was, e.g., published by Hermite [3], by Korkine and Zolotareff [4], and by Minkowski [5]. Nevertheless, lattices remained a topic of theoretical mathematical studies for quite a long time.

This situation dramatically changed with the advent of the digital revolution in the late 20th century. Suddenly, enough computational power was available to implement and run particular algorithms for lattice problems. The most prominent one was proposed by Lenstra, Lenstra and Lovász [6]. In particular, the LLL algorithm calculates a *reduced basis* of a lattice, i.e., a more suited mathematical description of the lattice w.r.t. some quality criteria, with only polynomial-time complexity. More powerful strategies for lattice basis reduction were addressed in the sequel, e.g., the concepts of Hermite-Korkine-Zolotareff (HKZ) reduction [7]–[9] or Minkowski reduction [9], [10], that, however, demand an exponentially-growing computational complexity for calculating the reduced basis. All above-mentioned algorithms operate over real numbers, i.e., the lattices are defined over the integer ring $\mathbb{Z}$.

Apart from the application of lattices in cryptological schemes [11], lattices gained popularity in the field of multiple-input/multiple-output (MIMO) communications [12]. In particular, maximum-likelihood (ML) detection was enabled by the sphere decoder [13], however, with the burden of a large computational complexity. An alternative, low-complexity strategy was given with the concept of lattice-reduction-aided (LRA) equalization [2], [14]–[19]. Here, the channel equalization is performed in a *more suited basis* which is obtained by one of the above-mentioned lattice-basis-reduction algorithms—most often, by the polynomial-time LLL algorithm. Since, for block-fading channels, this calculation has only to be done once in the beginning, the computational complexity is dramatically decreased when compared with ML detection. Besides, in comparison to straight-forward linear equalization of the MIMO channel, the noise enhancement can significantly be lowered, even resulting in the optimum diversity behavior as shown in [20].

A few years ago, the concept of integer-forcing (IF) linear (MIMO) equalization has been introduced [21]. The LRA and IF approaches share the philosophy of performing the channel equalization in a more suited representation of the channel matrix such that the noise enhancement inherently caused by equalization is lowered. However, it was found out that the restriction to lattice basis reduction—described by a unimodular integer transformation matrix—is actually not required. Instead, it is sufficient that this integer matrix has full rank—the lattice-basis-reduction problem is weakened to the so-called *successive minima problem*. For a more detailed insight into the topic, see, e.g., [19]. These successive minima are also quite important for the derivation of bounds for lattice-basis-reduction schemes, as they serve as lower bounds for the norms of the basis vectors.

In MIMO transmission, the channel matrix is usually assumed to be complex-valued due to representation in the equivalent complex-baseband domain [22]. Since the algorithms available for lattice-basis-reduction have initially been real-valued, equalization was performed with an equivalent real-valued representation of the complex-valued channel, resulting in a doubled dimension. The concept of LLL reduction could be extended to the complex case in [23], where the lattice was not formed over $\mathbb{Z}$ any more, but over the complex integers—the so-called *Gaussian integers* $\mathcal{G}$ [24], [25]. Moreover, HKZ reduction [26] and Minkowski reduction [27], respectively, were adapted in order to run over Gaussian integers. Efficient algorithms for the determination of the successive minima have recently been proposed in [28]–[30]. The algorithm in [30] only operates over real-valued lattices, whereas the algorithms in [28], [29] have been adapted to operate over complex numbers (and the Gaussian integers as the related ring). Furthermore, it was found out that the use of another complex-valued integer ring may be beneficial [31], [32]—of the so-called Eisenstein integers $\mathcal{E}$ [25], [33], forming the hexagonal lattice over the complex numbers.

Moreover, in recent years, four-dimensional signaling techniques have become more and more popular. In particular, in the field of optical communications, it is already quite common to employ both polarization planes of electromagnetic waves [34], resulting in a *dual-polarized* transmission. In wireless (MIMO) communications, *dual-polarized antennas* have been designed, e.g., in [35]–[37]. Besides, diversity schemes that are suited to combine the transmit symbols of two different time steps or frequencies are known for some time, e.g., the famous Alamouti scheme [38]. Given such a four-dimensional signal space, its representation over the set of *quaternion numbers* [25], [39] is quite obvious [40], [41]. Thereby, it has to be taken into account that quaternion-valued (scalar) multiplication is not commutative any more, i.e., the quaternion numbers do not form a field but only a *skew field*.

Unfortunately, up to now, hardly anything is known about lattice problems and algorithms that are defined over quaternion numbers, particularly over the integer rings of the *Lipschitz integers* $\mathcal{L}$ and the *Hurwitz integers* $\mathcal{H}$ [25], [39]. It has to be clarified to which extent these rings are suited to defined a *quaternion-valued* lattice-basis reduction, particularly based on a generalized variant of the LLL reduction, and if/how the respective successive minima can be calculated. Moreover, such findings still have to be assessed w.r.t. the quality of the results as well as the computational complexity—especially in comparison to lattices over real or complex numbers.

Hence, the aim and contribution of this work is the closing of the gaps in knowledge w.r.t. the extension and/or generalization of schemes for complex and quaternion-valued LLL reduction as well as the determination of the respective successive minima. To this end, generalized variants of the LLL reduction approach and the list-based successive-minima algorithm [29] are proposed which are suited for the combination with all real, complex, and quaternion-valued integer rings mentioned above. Both implementations are provided in such a way that the non-commutative behavior of quaternion-valued multiplication is adequately taken into account.

On the basis of these generalized criteria and their related algorithms, generalized quality bounds are derived. They particularly concern the norms of the basis vectors (and the respective successive minima), as well as the orthogonality defect of a lattice basis. It is shown that the quaternion-valued and/or complex-valued approaches may outperform their real-valued equivalents—especially if lattices over the Eisenstein or the Hurwitz integers are considered. Moreover, the asymptotic computational complexities of the different approaches are established. Concerning the (polynomial-time) LLL lattice-basis-reduction approach, these derivations reveal that the complexity can considerably be decreased if the respective complex- or quaternion-valued variants are employed. By providing additional results from numerical simulations, it is shown that the quality bounds and complexity evaluations reflect the behavior that can be observed when i.i.d. Gaussian stochastic models are applied in practice.

Finally, the application of the derived approaches in MIMO communications, particularly in the case of (multi-user) MIMO uplink transmission [12] based on the concepts of LRA and IF equalization, is extensively studied. This includes a discussion on how the quaternion-valued concept can be employed in dual-polarized transmission, as well as in the Alamouti-based combination of two time steps or frequencies. Respective system models are derived and evaluated by means of numerical simulations for particular transmission scenarios. These results show that the theoretical derivations and bounds also reflect the behavior in practical MIMO schemes.

The paper is structured as follows: In Sec. II, complex integer rings are briefly reviewed and an introduction to quaternions including the sets of Lipschitz and Hurwitz integers is given. In Sec. III, the LLL algorithm as well a list-based algorithm for the determination of the successive minima of a lattice are generalized to complex and quaternion-valued integer rings. Related quality bounds and the assessment of the computational complexities are provided in Sec. IV. In Sec. V, the particular application of the generalized algorithms is regarded in the field of MIMO communications. The paper is closed by a brief summary and an outlook in Sec. VI.

II. Two- and Four-Dimensional Extensions of the Real Numbers and Related Lattices

In this section, the sets of *complex numbers* and *quaternions* that form a two- and four-dimensional extension of the real numbers, respectively, are reviewed. The related algebras are presented and important subsets, particularly integer rings, are discussed. On that basis, generalized *lattices* are defined.

A. Complex Numbers and Quaternions

First, the extension of the real numbers $\mathbb{R}$ to complex numbers and quaternions, respectively, is reviewed. For a deeper insight into the topic, see [25], [39], [42].

1) Complex Numbers: The set of complex numbers

$$\mathbb{C} = \{c = \underbrace{c^{(1)}}_{\mathrm{Re}\{c\}} + \underbrace{c^{(2)}}_{\mathrm{Im}\{c\}}\mathrm{i} \mid c^{(1)}, c^{(2)} \in \mathbb{R}\} \tag{1}$$

forms a *field extension* of the real numbers. It is obtained by extending the first, real component $c^{(1)}$ (*real part* $\mathrm{Re}\{c\}$) by a second component $c^{(2)}$ which is multiplied by the *imaginary unit* $\mathrm{i} = \sqrt{-1}$ (*imaginary part* $\mathrm{Im}\{c\}$).

The complex conjugate of $c \in \mathbb{C}$ reads $c^* = c^{(1)} - c^{(2)}\,\mathrm{i}$ and its absolute value is given as $|c| = \sqrt{(c^{(1)})^2 + (c^{(2)})^2}$. Scalar additions (and subtractions) over complex numbers are performed individually per component. The multiplication of two complex numbers $u, v \in \mathbb{C}$ can be expressed as

$$\begin{aligned} w &= (u^{(1)} + u^{(2)}\,\mathrm{i}) \cdot (v^{(1)} + v^{(2)}\,\mathrm{i}) \\ &= \underbrace{(u^{(1)}v^{(1)} - u^{(2)}v^{(2)})}_{w^{(1)}} + \underbrace{(u^{(1)}v^{(2)} + u^{(2)}v^{(1)})}_{w^{(2)}}\,\mathrm{i}\;. \end{aligned} \tag{2}$$

Hence, four multiplications and two additions/subtractions are required. Following the concept of the Karatsuba algorithm [43], this multiplication can alternatively be realized by three multiplications and five additions/subtractions. The scalar division of u by v is performed by the scalar multiplication $u \cdot v^{-1}$ with the element $v^{-1} = v^*/|v|^2$.

Based on (2), an *equivalent real-valued* representation of complex matrices can be given. An $N \times K$ matrix $\boldsymbol{C} \in \mathbb{C}^{N \times K}$ may be represented via its equivalent $2N \times 2K$ real matrix

$$\boldsymbol{C}_{\mathsf{r}} = \begin{bmatrix} \boldsymbol{C}^{(1)} & -\boldsymbol{C}^{(2)} \\ \boldsymbol{C}^{(2)} & \boldsymbol{C}^{(1)} \end{bmatrix} \in \mathbb{R}^{2N \times 2K}\;, \tag{3}$$

where $\boldsymbol{C}^{(1)}$ and $\boldsymbol{C}^{(2)}$ denote the real and imaginary part of $\boldsymbol{C}$, respectively. If $N \geq K$,

$$\det(\boldsymbol{C}^{\mathsf{H}}\boldsymbol{C}) = \sqrt{\det(\boldsymbol{C}_{\mathsf{r}}^{\mathsf{T}}\boldsymbol{C}_{\mathsf{r}})} \tag{4}$$

is valid [42], where $\boldsymbol{C}^{\mathsf{H}}$ denotes the Hermitian of $\boldsymbol{C}$, i.e., the conjugated transpose. Utilizing (3), the matrix addition (and subtraction) $\boldsymbol{S} = \boldsymbol{U} + \boldsymbol{V}$, where $\boldsymbol{U}$ and $\boldsymbol{V}$ denote complex matrices, as well as the related complex matrix multiplication (and division) $\boldsymbol{W} = \boldsymbol{U} \cdot \boldsymbol{V}$, can isomorphically be represented by the real-valued addition $\boldsymbol{S}_{\mathsf{r}} = \boldsymbol{U}_{\mathsf{r}} + \boldsymbol{V}_{\mathsf{r}}$ and the real-valued multiplication $\boldsymbol{W}_{\mathsf{r}} = \boldsymbol{U}_{\mathsf{r}} \cdot \boldsymbol{V}_{\mathsf{r}}$, respectively.

2) Quaternions: The set of quaternions[1] [25], [39]

$$\begin{aligned} \mathbb{H} &= \{q = \underbrace{q^{\{1\}}}_{q^{(1)}+q^{(2)}\mathrm{i}} + \underbrace{q^{\{2\}}}_{q^{(3)}+q^{(4)}\mathrm{i}}\;\mathrm{j} \mid q^{\{1\}}, q^{\{2\}} \in \mathbb{C}\} \\ &= \{q = q^{(1)} + q^{(2)}\,\mathrm{i} + q^{(3)}\,\mathrm{j} + q^{(4)}\,\mathrm{k} \mid \\ &\qquad q^{(1)}, q^{(2)}, q^{(3)}, q^{(4)} \in \mathbb{R}\} \end{aligned} \tag{5}$$

extends the set of complex numbers by an *additional* complex-valued component which is multiplied by the imaginary unit j. Hence, *four real-valued* components are present, where the real part of a quaternion reads $\mathrm{Re}\{q\} = q^{(1)}$ and its imaginary part is represented by the 3-tuple $\mathrm{Im}\{q\} = (q^{(1)}, q^{(2)}, q^{(3)})$. The related imaginary *quaternion units* are given as i, j, and

[1] In honor of Sir William Rowan Hamilton, the set of quaternions is denoted by $\mathbb{H}$.

TABLE I

Hamilton Equations [39] for the Product $u \cdot v$, where u and v are Quaternion Units, i.e., $u, v \in \{1, \mathrm{i}, \mathrm{j}, \mathrm{k}\}$.

v u	1	i	j	k
1	1	i	j	k
i	i	-1	$+\mathrm{k}$	$-\mathrm{j}$
j	j	$-\mathrm{k}$	-1	$+\mathrm{i}$
k	k	$+\mathrm{j}$	$-\mathrm{i}$	-1

$\mathrm{k} = \mathrm{i}\,\mathrm{j}$. The relations between these units are described by the *Hamilton equations* [39], which are stated in Table I.

From Table I, it becomes apparent that the multiplication of two quaternions is—in general—not commutative. Consequently, the quaternions do not form a field but only a *skew field*, i.e., they fulfill all conditions which are required to form a field—except for the commutativity of the multiplication.

By analogy with complex numbers, the conjugate of a quaternion $q \in \mathbb{H}$ is given as $q^* = q^{(1)} - q^{(2)}\,\mathrm{i} - q^{(3)}\,\mathrm{j} - q^{(4)}\,\mathrm{k}$. Its absolute value is uniquely defined by $|q| = \sqrt{qq^*} = \sqrt{q^*q} = \sqrt{(q^{(1)})^2 + (q^{(2)})^2 + (q^{(3)})^2 + (q^{(4)})^2}$. Moreover, additions (and subtractions) are performed individually per component. The (non-commutative) multiplication of two quaternions $u, v \in \mathbb{H}$ is expressed as [39]

$$\begin{aligned} u \cdot v = &\left(u^{(1)}v^{(1)} - u^{(2)}v^{(2)} - u^{(3)}v^{(3)} - u^{(4)}v^{(4)}\right) \\ &+ \left(u^{(1)}v^{(2)} + u^{(2)}v^{(1)} + u^{(3)}v^{(4)} - u^{(4)}v^{(3)}\right)\mathrm{i} \\ &+ \left(u^{(1)}v^{(3)} - u^{(2)}v^{(4)} + u^{(3)}v^{(1)} + u^{(4)}v^{(2)}\right)\mathrm{j} \\ &+ \left(u^{(1)}v^{(4)} + u^{(2)}v^{(3)} - u^{(3)}v^{(2)} + u^{(4)}v^{(1)}\right)\mathrm{k}\ , \end{aligned} \tag{6}$$

i.e., 16 multiplications and 12 additions/subtractions are required. Alternatively, this multiplication can be realized using eight multiplications and 28 additions/subtractions [44]. The division can be implemented via the multiplication with the inverse element $v^{-1} = v^* \cdot (v^*v)^{-1}$, where this choice ensures that $vv^{-1} = 1$ (right inverse) and $v^{-1}v = 1$ (left inverse).

Similar to the real-valued representation of complex matrices, the quaternion-valued arithmetic defined in (6) can be realized by the *equivalent complex- or real-valued matrix representation.*

In particular, an $N \times K$ matrix $\boldsymbol{M} \in \mathbb{H}^{N \times K}$ can be represented as $2N \times 2K$ complex-valued matrix[3]

$$\begin{aligned} \boldsymbol{M}_{\mathsf{c}} &= \begin{bmatrix} \boldsymbol{M}^{\{1\}} & -\boldsymbol{M}^{\{2\}} \\ (\boldsymbol{M}^{\{2\}})^{*} & (\boldsymbol{M}^{\{1\}})^{*} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{M}^{(1)} + \boldsymbol{M}^{(2)}\mathrm{i} & -\boldsymbol{M}^{(3)} - \boldsymbol{M}^{(4)}\mathrm{i} \\ \boldsymbol{M}^{(3)} - \boldsymbol{M}^{(4)}\mathrm{i} & \boldsymbol{M}^{(1)} - \boldsymbol{M}^{(2)}\mathrm{i} \end{bmatrix} , \end{aligned} \tag{7}$$

where (7) directly corresponds to (3), with the only difference that an additional conjugation has to be performed in the second row. In (3), this step is not required since only real numbers are present. By plugging (7) into (3), i.e., by forming the real-valued representation of the complex matrix $\boldsymbol{M}_{\mathsf{c}}$, one would obtain one particular real-valued $4N \times 4K$ representation of the quaternion-valued matrix $\boldsymbol{M}$. However, for the subsequent system model, it is more convenient to form a real-valued representation according to[2]

$$\boldsymbol{M}_{\mathsf{r}} = \begin{bmatrix} \boldsymbol{M}^{(1)} & -\boldsymbol{M}^{(2)} & -\boldsymbol{M}^{(3)} & -\boldsymbol{M}^{(4)} \\ \boldsymbol{M}^{(2)} & \boldsymbol{M}^{(1)} & -\boldsymbol{M}^{(4)} & \boldsymbol{M}^{(3)} \\ \boldsymbol{M}^{(3)} & \boldsymbol{M}^{(4)} & \boldsymbol{M}^{(1)} & -\boldsymbol{M}^{(2)} \\ \boldsymbol{M}^{(4)} & -\boldsymbol{M}^{(3)} & \boldsymbol{M}^{(2)} & \boldsymbol{M}^{(1)} \end{bmatrix} , \tag{8}$$

in which the four components are directly stacked in the left-most column. Here, if $N \geq K$, we have[3]

$$\det(\boldsymbol{M}^{\mathsf{H}}\boldsymbol{M}) = \sqrt{\det(\boldsymbol{M}_{\mathsf{c}}^{\mathsf{H}}\boldsymbol{M}_{\mathsf{c}})} = \sqrt[4]{\det(\boldsymbol{M}_{\mathsf{r}}^{\mathsf{T}}\boldsymbol{M}_{\mathsf{r}})} , \tag{9}$$

$\boldsymbol{M}^{\mathsf{H}}$ denoting the Hermitian (conjugated transpose) of $\boldsymbol{M}$.

B. Integer Rings

The set of *integers*

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\} \tag{10}$$

[2] In particular, the complex- and real-valued representations (7) and (8), respectively, are not unique. There exist several representations that differ in the positions of the minus signs within the matrices $\boldsymbol{M}_{\mathsf{c}}$ and $\boldsymbol{M}_{\mathsf{r}}$, see, e.g., [25], [45], [46]. However, all these representations isomorphically express the quaternion-valued multiplication (division) according to (6).

[3] Due to the skew-field property, quaternion-valued determinants do not necessarily posses all properties which are known from real or complex ones. However, for Hermitian matrices (here, $\boldsymbol{M}\boldsymbol{M}^{\mathsf{H}}$), they can, to a large extent, be deployed just like real or complex determinants, cf. [45].

forms a subset of the real numbers $\mathbb{R}$ and additionally a *Euclidean ring*. Hence, for $u, \sigma, v, \rho \in \mathbb{Z}$ and $v \neq 0$, a division u/v with *small remainder* according to[4]

$$u = \sigma \cdot v + \rho \;, \tag{11}$$

is possible, where the term small remainder implicates that $|\rho| < |v|$ is valid [47, Def. 2.5]. Consequently, the *Euclidean algorithm* [48] can be used to calculate the *greatest common divisor* (gcd) of two numbers $u, v \in \mathbb{Z}$. The squared minimum distance between the elements of $\mathbb{Z}$ reads $d^2_{\min,\mathbb{Z}} = 1$.

A real number $r \in \mathbb{R}$ is quantized to its nearest integer via

$$\mathrm{Q}_{\mathbb{Z}}\{r\} = \lfloor r \rceil \in \mathbb{Z} \;, \tag{12}$$

i.e., by a simple rounding operation $\lfloor \cdot \rceil$, where ties are resolved towards $+\infty$. The squared maximum quantization error occurs for all half-integer values ($\mathbb{Z} + \frac{1}{2}$) and is given as $\epsilon^2_{\mathbb{Z}} = |\mathrm{Q}_{\mathbb{Z}}\{\frac{1}{2}\} - \frac{1}{2}|^2 = \frac{1}{4}$. The related (non-square) error corresponds with the maximum of the remainder in (11), i.e., we have $|\rho| < \frac{1}{2} < |v|$, since $|v| \geq 1 \; \forall v \in \mathbb{Z} \setminus \{0\}$. Based on the quantization (12), the *modulo function*

$$\mathrm{mod}_{\mathbb{Z}}\{r\} = r - \mathrm{Q}_{\mathbb{Z}}\{r\} \tag{13}$$

yields a congruent point $r + \lambda$, $\lambda \in \mathbb{Z}$ located within $[-\frac{1}{2}, \frac{1}{2})$, forming the Voronoi cell of $\mathbb{Z}$ w.r.t. the origin [22], [25].

1) Complex-Valued Integer Rings: Integers in the complex plane are represented by the *Gaussian integers* [24], [25], [49]

$$\mathcal{G} = \{c = c^{(1)} + c^{(2)}\mathrm{i} \mid c^{(1)}, c^{(2)} \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}\,\mathrm{i} \;. \tag{14}$$

They are illustrated in Figure 1 (left). The squared minimum distance between the elements reads $d^2_{\min,\mathcal{G}} = 1$. The quantization of a complex number $c \in \mathbb{C}$ to $\mathcal{G}$ is performed as

$$\mathrm{Q}_{\mathcal{G}}\{c\} = \lfloor c^{(1)} \rceil + \lfloor c^{(2)} \rceil\,\mathrm{i} \in \mathcal{G} \;, \tag{15}$$

where the squared maximum quantization error sums up to $\epsilon^2_{\mathcal{G}} = |\mathrm{Q}_{\mathcal{G}}\{\frac{1}{2} + \frac{1}{2}\mathrm{i}\} - (\frac{1}{2} + \frac{1}{2}\mathrm{i})|^2 = \frac{1}{2}$. The modulo operation $\mathrm{mod}_{\mathcal{G}}\{c\} = c - \mathrm{Q}_{\mathcal{G}}\{c\}$ reduces a complex number c to the Voronoi cell of $\mathcal{G}$ (w.r.t. the origin), which forms a square in the complex plane where all values are located within the range $[-\frac{1}{2}, \frac{1}{2})$ per component.

[4] We assume that negative remainders may occur, i.e., the modulo operation defined in (13) is assumed to be symmetric w.r.t. the origin.

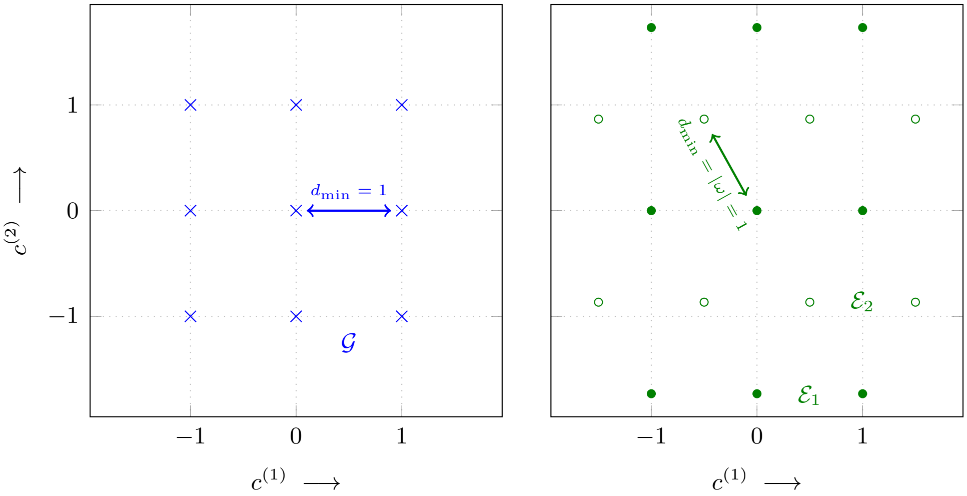


Fig. 1. Illustration of the Gaussian integers $\mathcal{G}$ (left) and the Eisenstein integers $\mathcal{E}$ (right). For the Eisenstein integers, the two subsets $\mathcal{E}_1$ (filled circles) and $\mathcal{E}_2$ (hollow circles) are shown.

The Eisenstein integers [25], [33]

$$\mathcal{E} = \{c = c^{(1)} + c^{(2)}\omega \mid c^{(1)}, c^{(2)} \in \mathbb{Z}\} = \mathbb{Z} + \mathbb{Z}\,\omega\ , \tag{16}$$

with the Eisenstein unit $\omega = \mathrm{e}^{\frac{2\pi}{3}\mathrm{i}}$ (third root of unity), represent the hexagonal numbers ($\boldsymbol{A}_2$ lattice [25]) in the complex plane, cf. Fig. 1 (right). Without a decrease in minimum distance ($d^2_{\min,\mathcal{E}} = 1$), the elements are more densely packed (particularly, the densest packing in two-dimensions is achieved [22], [25]). The quantization is realized as [25], [50]

$$\mathrm{Q}_{\mathcal{E}}\{c\} = \underset{\mathrm{Q}_{\mathcal{E}_1}\{c\},\mathrm{Q}_{\mathcal{E}_2}\{c\}}{\operatorname{argmin}} \{|c - \mathrm{Q}_{\mathcal{E}_1}\{c\}|, |c - \mathrm{Q}_{\mathcal{E}_2}\{c\}|\}\ , \tag{17}$$

$$\mathrm{Q}_{\mathcal{E}_1}\{c\} = \mathrm{Q}_{\mathbb{Z}}\left\{c^{(1)}\right\} + \sqrt{3}\,\mathrm{Q}_{\mathbb{Z}}\left\{\frac{c^{(2)}}{\sqrt{3}}\right\}\mathrm{i}\ , \tag{18}$$

$$\mathrm{Q}_{\mathcal{E}_2}\{c\} = \mathrm{Q}_{\mathbb{Z}}\left\{c^{(1)} - \frac{1}{2}\right\} + \frac{1}{2} + \left(\sqrt{3}\,\mathrm{Q}_{\mathbb{Z}}\left\{\frac{c^{(2)} - \frac{\sqrt{3}}{2}}{\sqrt{3}}\right\} + \frac{\sqrt{3}}{2}\right)\mathrm{i}\ , \tag{19}$$

i.e., by performing a quantization to the subsets $\mathcal{E}_1$ (filled circles in Fig. 1 (right)) and $\mathcal{E}_2$ (hollow circles) and a subsequent decision to the point which is located closer to the original value $c \in \mathbb{C}$. The squared maximum quantization error reads $\epsilon^2_{\mathcal{E}} = \frac{1}{3}$, cf. [2], [22], [25]. The modulo operation $\mathrm{mod}_{\mathcal{E}}\{c\} = c - \mathrm{Q}_{\mathcal{E}}\{c\}$ calculates a point $c + \lambda$, $\lambda \in \mathcal{E}$, located within the *hexagonal* Voronoi cell of $\mathcal{E}$ w.r.t. the origin.

Both Gaussian and Eisenstein integers form Euclidean rings [51]. Due to the maximum quantization errors, for the former, $|\rho| < \frac{1}{\sqrt{2}} < |v|$, with $|v| \geq 1 \; \forall v \in \mathcal{G} \setminus \{0\}$, is valid if the division with remainder according to (11) is performed over $\mathcal{G}$. For the latter, $|\rho| < \frac{1}{\sqrt{3}} < |v|$, with $|v| \geq 1 \; \forall v \in \mathcal{E} \setminus \{0\}$, holds. A division with small remainder can be performed by analogy with (11) and, thus, it is possible to define a Euclidean algorithm over Gaussian and Eisenstein integers.

2) Quaternion-Valued Integer Rings: With regard to the set of quaternions $\mathbb{H}$, two important subsets, in particular integer rings, can be defined. The first type are the *Lipschitz integers*

$$\begin{aligned} \mathcal{L} = \{q = q^{(1)} + q^{(2)}\mathrm{i} + q^{(3)}\mathrm{j} + q^{(4)}\mathrm{k} \\ \mid q^{(1)}, q^{(2)}, q^{(3)}, q^{(4)} \in \mathbb{Z}\} \\ = \mathbb{Z} + \mathbb{Z}\,\mathrm{i} + \mathbb{Z}\,\mathrm{j} + \mathbb{Z}\,\mathrm{k}\;, \end{aligned} \tag{20}$$

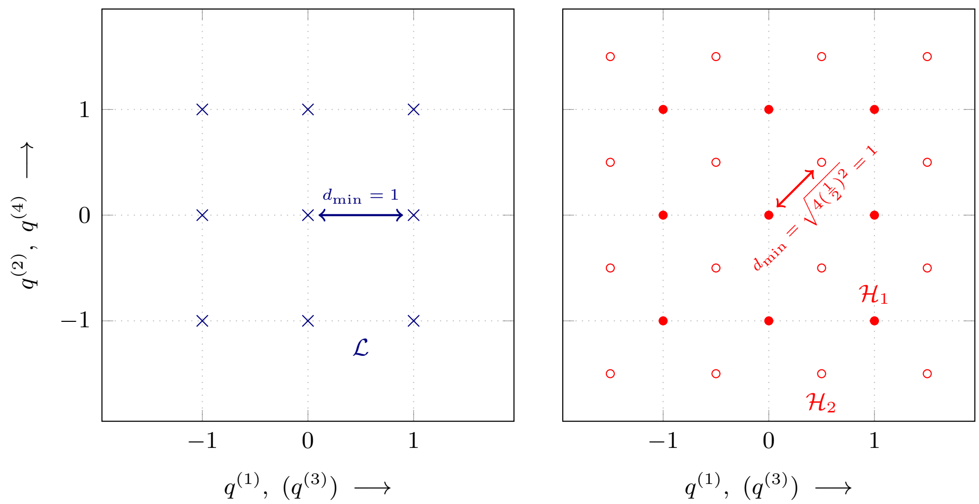
i.e., following the philosophy of the Gaussian integers, integer values are present in each of the four components. A two-dimensional projection of the Lipschitz integers is illustrated in Fig. 2 (left). Again, the squared minimum distance reads $d^2_{\min,\mathcal{L}} = 1$. The quantization of a quaternion $q \in \mathbb{H}$ to the closest Lipschitz integer is realized by

$$\mathrm{Q}_{\mathcal{L}}\{q\} = \lfloor q^{(1)} \rceil + \lfloor q^{(2)} \rceil \,\mathrm{i} + \lfloor q^{(3)} \rceil \,\mathrm{j} + \lfloor q^{(4)} \rceil \,\mathrm{k} \in \mathcal{L}\;. \tag{21}$$

The modulo operation reads $\mathrm{mod}_{\mathcal{L}}\{q\} = q - \mathrm{Q}_{\mathcal{L}}\{q\}$, where the Voronoi region constitutes a *hypercube* with the range $[-\frac{1}{2}, \frac{1}{2})$ per component. The squared maximum quantization error is—in comparison to the Gaussian integers—increased to $\epsilon^2_{\mathcal{L}} = |\frac{1}{2} + \frac{1}{2}\mathrm{i} + \frac{1}{2}\mathrm{j} + \frac{1}{2}\mathrm{k}|^2 = 1$. A direct consequence thereof is that the division with remainder according to (11), with $u, \sigma, v, \rho \in \mathcal{L}$, is not a *Euclidean one* any more [39]: Here, the case $uv^{-1} \in \mathcal{L} + (1 + \mathrm{i} + \mathrm{j} + \mathrm{k})/2$ may occur. Then, for the absolute value of the remainder, $|\rho| = |(1 + \mathrm{i} + \mathrm{j} + \mathrm{k})/2| = 1 \leq |v|$, with $|v| \geq 1 \; \forall v \in \mathcal{L} \setminus \{0\}$, is obtained. Hence, $|\rho| = |v|$ may be present, i.e., the *in*equality required to ensure a *small* remainder is, in general, not achieved. Thus, it is *not* possible to define a Euclidean algorithm in order to calculate the gcd of two Lipschitz integers $u, v \in \mathcal{L}$.

Nevertheless, the non-Euclidean property of the Lipschitz integers can be "cured" by the insertion of additional points at the problematic coordinates—the half-integer values located at $\mathcal{L} + (1 + \mathrm{i} + \mathrm{j} + \mathrm{k})/2$. Then, as depicted in Fig. 2 (right), the so-called Hurwitz integers [25], [39]

$$\begin{aligned} \mathcal{H} = \Big\{ q = q^{(1)} + q^{(2)}\mathrm{i} + q^{(3)}\mathrm{j} + q^{(4)}\mathrm{k} \mid \\ (q^{(1)}, q^{(2)}, q^{(3)}, q^{(4)}) \in \mathbb{Z}^4 \cup \Big(\mathbb{Z} + \frac{1}{2}\Big)^4 \Big\} \end{aligned} \tag{22}$$



1
0
−1
$q^{(2)}, q^{(4)} \longrightarrow$
$d_{\min} = 1$
$\mathcal{L}$
−1
0
1
$q^{(1)}, (q^{(3)}) \longrightarrow$
$d_{\min} = \sqrt{4(\frac{1}{2})^2} = 1$
$\mathcal{H}_1$
$\mathcal{H}_2$
−1
0
1
$q^{(1)}, (q^{(3)}) \longrightarrow$

Fig. 2. Two-dimensional projection of the Lipschitz integers $\mathcal{L}$ (left) and the Hurwitz integers $\mathcal{H}$ (right). The components $q^{(3)}$ and $q^{(4)}$ are projected onto $q^{(1)}$ and $q^{(2)}$, respectively. For the Hurwitz integers, the two subsets $\mathcal{H}_1$ (filled circles) and $\mathcal{H}_2$ (hollow circles) are shown.

are obtained, where *all* components are—at the same time—*either* integers *or* half-integers. In particular, the number of points (in quaternion space) is doubled within the same hypervolume—without a decrease in (squared) minimum distance, which still reads $d^2_{\min,\mathcal{H}} = 1$. They form the densest packing in four-dimensional space [25], as will be discussed in Sec. II-C. The squared maximum quantization error reads $\epsilon^2_{\mathcal{H}} = |\frac{1}{4} + \frac{1}{4}\mathrm{i} + \frac{1}{4}\mathrm{j} + \frac{1}{4}\mathrm{k}|^2 = \frac{1}{2}$, i.e., for the division with remainder according to (11), we have $|\rho| = \frac{1}{\sqrt{2}} \leq |v|$, with $|v| \geq 1 \ \forall v \in \mathcal{H} \setminus \{0\}$. As a consequence, a Euclidean ring is present and a related Euclidean algorithm can be applied. Thereby, similar to the Eisenstein integers in (17), the quantization is performed as [25], [50]

$$\mathrm{Q}_{\mathcal{H}}\{q\} = \underset{\mathrm{Q}_{\mathcal{H}_1}\{q\}, \mathrm{Q}_{\mathcal{H}_2}\{q\}}{\operatorname{argmin}} \{|q - \mathrm{Q}_{\mathcal{H}_1}\{q\}|, |q - \mathrm{Q}_{\mathcal{H}_2}\{q\}|\} \ , \tag{23}$$

$$\mathrm{Q}_{\mathcal{H}_1}\{c\} = \mathrm{Q}_{\mathcal{L}}\{q\} \ , \tag{24}$$

$$\mathrm{Q}_{\mathcal{H}_2}\{c\} = \mathrm{Q}_{\mathcal{L}}\{q - o_{\mathcal{H}}\} + o_{\mathcal{H}} \ , \ o_{\mathcal{H}} = \frac{1 + \mathrm{i} + \mathrm{j} + \mathrm{k}}{2} \ . \tag{25}$$

Hence, both a quantization to all Lipschitz integers (filled circles in Fig. 2 (right)) and a quantization to all Lipschitz integers shifted by $\frac{1}{2}$ per component (hollow circles) is done; subsequently, the closest result is chosen as the quantized value. The modulo reduction is, again, described as $\operatorname{mod}_{\mathcal{H}}\{q\} = q - \mathrm{Q}_{\mathcal{H}}\{q\}$. The points are reduced to the Voronoi cell located around the origin which forms a 24-cell with 24 vertices, 96 edges, and 96 faces [25].

C. Generalized Definition of Lattices

A lattice $\mathbf{\Lambda}$ forms an *infinite* set of points that are distributed over the Euclidean space in such a way that an *Abelian group* w.r.t. addition is present [22], [25], [52]. An N-dimensional lattice of rank K, with $N \geq K$, can be defined by

$$\mathbf{\Lambda}(\boldsymbol{G}) = \left\{ \boldsymbol{G}\boldsymbol{\zeta} = \sum\nolimits_{k=1}^{K} \boldsymbol{g}_k \zeta_k \mid \zeta_k \in \mathbb{I} \right\} \;, \tag{26}$$

where $\boldsymbol{G} = [\boldsymbol{g}_1, \ldots, \boldsymbol{g}_K]$ denotes the $N \times K$ *generator matrix* of the lattice, and $\boldsymbol{\zeta} = [\zeta_1, \ldots, \zeta_K]^{\mathsf{T}}$ an *integer vector* with elements drawn from the constituent integer ring $\mathbb{I}$.

Most often, lattices over the real numbers are considered, i.e., $\mathbb{I} = \mathbb{Z}$ and $\boldsymbol{G} \in \mathbb{R}^{N \times K}$ are assumed. Nevertheless, the generalized definition of lattices in (26) enables the construction of lattices over complex numbers, where $\boldsymbol{G} \in \mathbb{C}^{N \times K}$. Here, both the integers rings $\mathbb{I} = \mathcal{G}$ and $\mathbb{I} = \mathcal{E}$ are suited. Moreover, lattices over the quaternions, with $\boldsymbol{G} = \mathbb{H}^{N \times K}$, can be defined based on the Lipschitz integers ($\mathbb{I} = \mathcal{L}$) or the Hurwitz integers ($\mathbb{I} = \mathcal{H}$) as the constituent integer ring.

The basis of a lattice is not unique. Instead, there exists an infinite number of generator matrices that span the same lattice. The transformation to an alternative generator matrix can be realized by the multiplication with a *unimodular* integer matrix $\boldsymbol{T} \in \mathbb{I}^{K \times K}$ according to

$$\boldsymbol{G}_{\text{red}} = \boldsymbol{G}\boldsymbol{T} \;, \qquad \text{with } \det(\boldsymbol{T}^{\mathsf{H}}\boldsymbol{T}) = 1 \;. \tag{27}$$

The alternative generator matrix is often called *reduced* matrix, since by means of *lattice reduction algorithms*, a matrix is constructed that fulfills some desired quality criteria. Noteworthy, if the unimodularity constraint is relaxed to the full-rank constraint $\operatorname{rank}(\boldsymbol{T}) = K$, *sublattices* of the original lattice with the order $\sqrt{\det(\boldsymbol{T}\boldsymbol{T}^{\mathsf{H}})}$ may be obtained [2], [19].

In order to evaluate the quality of a lattice basis, the length (norm) of the basis vectors $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_K$ is often assessed. The Euclidean norm of a vector $\boldsymbol{v}$ over $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$ is given as

$$\|\boldsymbol{v}\| = \sqrt{\boldsymbol{v}_k^{\mathsf{H}}\boldsymbol{v}} \;. \tag{28}$$

Another quality criterion is the *orthogonality defect* [22], [25]

$$\Omega(\boldsymbol{G}) = \frac{\prod_{k=1}^{K} \|\boldsymbol{g}_k\|}{\operatorname{vol}(\mathbf{\Lambda}(\boldsymbol{G}))} \tag{29}$$

of a lattice basis which is given as the product of the basis vectors over the volume of (a Voronoi cell of) the lattice

$$\operatorname{vol}(\mathbf{\Lambda}(\boldsymbol{G})) = \sqrt{\det(\boldsymbol{G}^{\mathsf{H}}\boldsymbol{G})} \;. \tag{30}$$

Thereby, the volume is the same for all generator matrices that span the same lattice [22], [25].

1) Real Representation of Complex Lattices: The Gaussian integers are isomorphic to the two-dimensional real-valued integer lattice $\mathbb{Z}^2$ (generator matrix[5] $\boldsymbol{G} = \boldsymbol{I}_2$), cf. [25]. Hence, a complex lattice with generator matrix $\boldsymbol{G} \in \mathbb{C}^{N\times K}$ defined over $\mathcal{G}$, can isomorphically be expressed by a real-valued lattice (over $\mathbb{Z}$) with the generator matrix $\boldsymbol{G}_\mathsf{r}$ according to (3).

Moreover, the Eisenstein integers are isomorphic to the two-dimensional real-valued hexagonal lattice $\boldsymbol{A}_2$. A real-valued representation of lattices over $\mathcal{E}$ is obtained via [2]

$$\boldsymbol{G}_{\mathsf{r},\mathcal{E}} = \underbrace{\boldsymbol{G}_\mathsf{r}}_{(3)} \underbrace{\begin{bmatrix} \boldsymbol{I}_K & -\frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \frac{-\sqrt{3}}{2}\boldsymbol{I}_K \end{bmatrix}}_{\boldsymbol{G}_\mathcal{E}} \tag{31}$$

where the right-hand-side matrix in (31) represents the generator matrix of the $\boldsymbol{A}_2$ lattice [25].

2) Real and Complex Representation of Quaternion-Valued Lattices: The Lipschitz integers are isomorphic to the four-dimensional (real-valued) integer lattice $\mathbb{Z}^4$ (generator matrix $\boldsymbol{I}_4$). By analogy with (3), quaternion-valued lattices (over $\mathcal{L}$) can equivalently be expressed by complex-valued lattices (over $\mathcal{G}$) via the construction of a generator matrix $\boldsymbol{G}_\mathsf{c} \in \mathbb{C}^{2N\times 2K}$ according to (7), or by real-valued lattices (over $\mathbb{Z}$) with the corresponding generator matrix $\boldsymbol{G}_\mathsf{r} \in \mathbb{R}^{4N\times 4K}$ from (8).

Regarding the Hurwitz integers, an isomorphism to the four-dimensional *checkerboard lattice* $\boldsymbol{D}_4$ is present [25]. This isomorphism can be exploited in order to define an equivalent real-valued representation (over $\mathbb{Z}$) for lattices over $\mathcal{H}$. Here, the equivalent real-valued generator matrix is obtained as

$$\boldsymbol{G}_{\mathsf{r},\mathcal{H}} = \underbrace{\boldsymbol{G}_\mathsf{r}}_{(8)} \underbrace{\begin{bmatrix} \boldsymbol{I}_K & \boldsymbol{0}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{I}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{0}_K & \boldsymbol{I}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{0}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \end{bmatrix}}_{\boldsymbol{G}_\mathcal{H}} \in \mathbb{R}^{2N\times 2K} \tag{32}$$

by incorporating the generator matrix of the $\boldsymbol{D}_4$ lattice.[6] In the same way, an equivalent complex-

[5] $\boldsymbol{I}_K$ denotes the $K \times K$ identity matrix and $\boldsymbol{0}_K$ the $K \times K$ all-zero matrix (all elements are 0).

[6] In particular, the generator matrix of the lattice *dual* to $\boldsymbol{D}_4$ is employed, that actually corresponds to a version of the orignal $\boldsymbol{D}_4$ lattice that is scaled by a factor of $\frac{1}{2}$. This is possible since $\boldsymbol{D}_4$ and its dual lattice form an isomorphism [25]. Using that strategy, the resulting points directly correspond to the set of Hurwitz integers (with half-integer values).

valued representation (over $\mathcal{G}$) is realized by using the generator matrix

$$\boldsymbol{G}_{\mathsf{c},\mathcal{H}} = \underbrace{\boldsymbol{G}_{\mathsf{c}}}_{(7)} \begin{bmatrix} \boldsymbol{I}_K & (\frac{1}{2}+\frac{1}{2}\,\mathrm{i})\boldsymbol{I}_K \\ \boldsymbol{0}_K & (\frac{1}{2}+\frac{1}{2}\,\mathrm{i})\boldsymbol{I}_K \end{bmatrix} \in \mathbb{C}^{2N\times 2K} \; . \tag{33}$$

III. Algorithms for Generalized Lattice Problems

In this section, algorithms that are suited to (approximately) solve particular lattice problems are reviewed and generalized to all real-, complex-, and quaternion-valued integer rings $\mathbb{I}$ that were considered above.

A. Lattice Basis Reduction and the LLL Algorithm

The task of lattice basis reduction is to find a *more suited basis* $\boldsymbol{G}_{\mathrm{red}} = \left[\boldsymbol{g}_{\mathrm{red},1}, \dots, \boldsymbol{g}_{\mathrm{red},K}\right]$ for the representation of the lattice spanned by the (unreduced) generator matrix $\boldsymbol{G}$. In particular, for generalized lattices, a unimodular integer matrix $\boldsymbol{T} = \left[\boldsymbol{t}_1, \dots, \boldsymbol{t}_K\right] \in \mathbb{I}^{K\times K}$ according to (27) has to be found in such a way that particular quality criteria are fulfilled.

To assess when a lattice basis is reduced, several different criteria can be defined. One is the minimization of the orthogonality defect (29), i.e., the optimality criterion reads

$$\boldsymbol{T} = \underset{\substack{\boldsymbol{T}\in\mathbb{I}^{K\times K} \\ \det(\boldsymbol{T}^{\mathsf{H}}\boldsymbol{T})=1}}{\operatorname{argmin}} \; \Omega(\boldsymbol{G}\boldsymbol{T}) = \underset{\substack{\boldsymbol{T}\in\mathbb{I}^{K\times K} \\ \det(\boldsymbol{T}^{\mathsf{H}}\boldsymbol{T})=1}}{\operatorname{argmin}} \; \frac{\prod_{k=1}^{K} \|\boldsymbol{g}_{\mathrm{red},k}\|}{\mathrm{vol}(\boldsymbol{\Lambda}(\boldsymbol{G}))} \; . \tag{34}$$

Hence, the norms of all basis vectors are incorporated. An alternative approach is to consider the lengths of these vectors individually, e.g., $\|\boldsymbol{g}_{\mathrm{red},1}\|$. The minimization of the *maximum norm* among the basis vectors is particularly known under the name *shortest basis problem* (SBP) and described by

$$\boldsymbol{T} = \underset{\substack{\boldsymbol{T}\in\mathbb{I}^{K\times K} \\ \det(\boldsymbol{T}^{\mathsf{H}}\boldsymbol{T})=1}}{\operatorname{argmin}} \; \max_{k=1,\dots,K} \|\boldsymbol{G}\boldsymbol{t}_k\|^2 \; . \tag{35}$$

The most popular lattice-basis-reduction algorithm was derived by Lenstra, Lenstra, and Lovász in [6]. It was initially proposed for the real-valued case ($\mathbb{I} = \mathbb{Z}$). The algorithm is suboptimal w.r.t. the above-mentioned lattice-basis-reduction criteria, i.e., it only approximates the respective optimization problems. Nevertheless, for LLL reduction, a polynomial asymptotic complexity is ensured (over K), whereas for the solutions to the problems (34) and (35) an exponential complexity is required, cf., e.g., [13], [53]. Moreover, it is possible to derive certain performance guarantees (i.e., bounds) for LLL reduction. More details will be provided in Sec. IV.

In the following, the concept of LLL reduction will be generalized to lattices over real, complex, or quaternion-valued integer rings. To this end, generalized variants of the reduction criteria as well as the reduction algorithm will be given.

1) Gram–Schmidt Orthogonalization: The LLL reduction and its related criteria operate on the Gram–Schmidt orthogonalization (GSO) [54] of the generator matrix[7]

$$\boldsymbol{QR} = \boldsymbol{GP} \ . \tag{36}$$

In particular, $\boldsymbol{Q} = \big[\boldsymbol{q}_1, \dots, \boldsymbol{q}_K\big]$ forms an $N \times K$ matrix with *orthogonal columns*, and $\boldsymbol{R} = \big[r_{k,l}\big]$, $k = 1, \dots, K$, $l = 1, \dots, K$, an upper triangular $K \times K$ matrix with unit main diagonal ($r_{k,k} = 1$, $k = 1, \dots, K$). The $K \times K$ matrix $\boldsymbol{P}$ (*permutation matrix* with a single 1 per column and row and all other elements equal to 0) can be used to sort the Gram-Schmidt vectors in $\boldsymbol{Q}$ according to their length during the orthogonalization process (known as *pivoting*).

The GSO procedure[8] is presented in Algorithm 1. In every step $k = 1, \dots, K$, the pivoting is performed first, i.e., the shortest of the remaining columns $\boldsymbol{q}_k, \dots, \boldsymbol{q}_K$ is inserted at position k (and removed at its original position). Afterwards, the remaining columns are projected onto the orthogonal complement of $\boldsymbol{q}_k$. In contrast to other implementations, e.g., [23], [54], all multiplications are defined in such a way that the non-commutative behavior of quaternion-valued numbers is taken into account. Hence, the procedure can be used for real, complex, or quaternion-valued numbers.

2) Generalized LLL Reduction Criteria: In the initial publication on real-valued LLL (RLLL) reduction, an LLL-reduced basis has been defined w.r.t. two conditions.

Definition 1 (Real-Valued LLL Reduction [6])**.** *A real-valued generator matrix $\boldsymbol{G} \in \mathbb{R}^{N \times K}$ with its related Gram-Schmidt matrices $\boldsymbol{QR} = \boldsymbol{G}$ is called LLL-reduced, if*

1) $\boldsymbol{R}$ *is* size-reduced*, i.e., if*

$$|r_{l,k}| \leq \frac{1}{2} \ , \qquad 1 \leq l < k \leq K \ , \qquad \textit{and if} \tag{37}$$

2) *the Lovász condition*

$$\|\boldsymbol{q}_k\|^2 \geq (\delta - |r_{k-1,k}|^2) \cdot \|\boldsymbol{q}_{k-1}\|^2 \tag{38}$$

[7] The matrices $\boldsymbol{Q}$ and $\boldsymbol{R}$ often describe the *QR decomposition* of a matrix, in which $\boldsymbol{Q}$ is usually assumed to be a unitary matrix ($\boldsymbol{Q}^{\mathsf{H}}\boldsymbol{Q} = \boldsymbol{I}$). Given the GSO (without normalization), the column norms of $\boldsymbol{Q}$ are then absorbed in $\boldsymbol{R}$ (non-unit main diagonal). In this work, we assume that the matrix $\boldsymbol{Q}$ does not have to be unitary but that $\boldsymbol{R}$ is a matrix with unit main diagonal.

[8] To simplify the notation, we denote the selection of the elements with index $k, \dots, l$ of a vector $\boldsymbol{g}$ by $\boldsymbol{g}_{k:l}$. Within a matrix $\boldsymbol{G}$, the selection of the rows $k, \dots, l$ and the columns $m, \dots, n$ is denoted as $\boldsymbol{G}_{k:l,m:n}$.

Algorithm 1 Gram–Schmidt Orthogonalization with Pivoting.

```
$[\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{P}] = \mathrm{GSO}(\boldsymbol{G})$
$\boldsymbol{Q} = \boldsymbol{G}$, $\boldsymbol{R} = \boldsymbol{I}_K$, $\boldsymbol{P} = \boldsymbol{I}_K$
for $k = 1, \ldots, K$ do
    $k_\mathrm{m} = \mathrm{argmin}_{l=k,\ldots,K} \|\boldsymbol{q}_l\|$
    if $k_\mathrm{m} \neq k$ then                                        ▷ pivoting
        $\boldsymbol{Q} = [\boldsymbol{q}_{1:k-1}, \boldsymbol{q}_{k_\mathrm{m}}, \boldsymbol{q}_{k:k_\mathrm{m}-1}, \boldsymbol{q}_{k_\mathrm{m}+1:K}]$
        $\boldsymbol{P} = [\boldsymbol{p}_{1:k-1}, \boldsymbol{p}_{k_\mathrm{m}}, \boldsymbol{p}_{k:k_\mathrm{m}-1}, \boldsymbol{p}_{k_\mathrm{m}+1:K}]$
        In the upper $k-1$ rows of $\boldsymbol{R}$ (index $1 : k-1$):
        $\boldsymbol{R} = [\boldsymbol{r}_{1:k-1}, \boldsymbol{r}_{k_\mathrm{m}}, \boldsymbol{r}_{k:k_\mathrm{m}-1}, \boldsymbol{r}_{k_\mathrm{m}+1:K}]$
    end if
    for $l = k+1, \ldots, K$ do                                          ▷ orthogonalization
        $r_{k,l} = \boldsymbol{q}_k^\mathsf{H} \boldsymbol{q}_l \cdot \|\boldsymbol{q}_k\|^{-2}$
        $\boldsymbol{q}_l = \boldsymbol{q}_l - \boldsymbol{q}_k r_{k,l}$
    end for
end for
```

> *is fulfilled, where δ denotes a* quality parameter *that defines a trade-off between the quality of the reduction and the runtime of the algorithm. The Lovász condition can be checked if $r_{k-1,k}$ is size-reduced and if $0 < (\delta - |r_{k-1,k}|^2) \leq 1$. Hence, as $|r_{k-1,k}|^2 \leq \frac{1}{4}$, a parameter $\delta \in (\frac{1}{4}, 1]$ leads to a valid result* [6], [55]. *Often, the parameter $\delta = \frac{3}{4}$ is chosen (standard parameter).*

The LLL algorithm as proposed in [6] can be interpreted to form some kind of *Euclidean algorithm* for matrices. In particular, the size reduction is performed by a modulo reduction according to (13), i.e., by a (Euclidean) division as defined in (11) with the divisor $v = 1$, where the resulting remainder $r_{l,k} = \rho$ is a *small remainder* since $|r_{l,k}| \leq \frac{1}{2} < |v| = 1$.

In [51], the possibility to extend the concept of LLL reduction to Euclidean rings other than $\mathbb{Z}$, particularly to $\mathcal{G}$, $\mathcal{E}$, and $\mathcal{H}$, was mentioned first. More precisely, since the Lovász condition only incorporates norms of vectors, it is generally valid for Euclidean rings. In contrast, the size-reduction condition has to be adapted to the particular ring. In [51], it was set to $|r_{k-1,k}| \leq \alpha$, with $\alpha = \frac{1}{2}$ for Gaussian, $\alpha = \frac{1}{3}$ for Eisenstein, and $\alpha = \frac{1}{2}$ for Hurwitz integers, by analogy to the "standard parameter" $\delta = \frac{3}{4}$ for RLLL reduction. In [23] it was found out that this condition is actually too unspecific. Here, for complex LLL (CLLL) reduction over $\mathcal{G}$,

$$|\mathrm{Re}\{r_{l,k}\}| \leq \frac{1}{2} \cap |\mathrm{Im}\{r_{l,k}\}| \leq \frac{1}{2} \tag{39}$$

was postulated, i.e., $|r_{l,k}| \leq \frac{1}{\sqrt{2}}$, and, thus, $\delta \in (\frac{1}{2}, 1]$.

Taking advantage of the particular interpretation of the size-reduction operation to form a Euclidean algorithm for matrices, *generalized LLL reduction criteria* can be defined.

Definition 2 (Generalized LLL Reduction)**.** *A generator matrix $\boldsymbol{G}$ with Gram-Schmidt matrices $\boldsymbol{QR} = \boldsymbol{G}$ that spans a lattice over the Euclidean integer ring $\mathbb{I}$ is LLL-reduced over $\mathbb{I}$, if*

1) *$\boldsymbol{R}$ is size-reduced according to*

$$\mathrm{Q}_{\mathbb{I}}\{r_{l,k}\} = 0 \ , \qquad 1 \leq l < k \leq K \ , \qquad \textit{and if} \tag{40}$$

2) *the respective Lovász condition*

$$\|\boldsymbol{q}_k\|^2 \geq (\delta - |r_{k-1,k}|^2) \cdot \|\boldsymbol{q}_{k-1}\|^2 \tag{41}$$

is fulfilled. The quality parameter can be chosen from the range

$$\delta \in (\epsilon_{\mathbb{I}}^2, 1] \ . \tag{42}$$

Remark. *Since, after size reduction, $\mathrm{Q}_{\mathbb{I}}\{r_{l,k}\} = 0$ is valid, $r_{l,k}$ forms the remainder ρ of the division with the divisor $v = 1$ as defined in* (11)*. If $\mathbb{I}$ is a Euclidean ring, $|r_{l,k}| \leq \epsilon_{\mathbb{I}} < |v| = 1$, i.e., a* small remainder *is present. Hence, the Lovász condition becomes operative if $0 < (\delta - \epsilon_{\mathbb{I}}^2) \leq 1$, i.e., if $\delta \in (\epsilon_{\mathbb{I}}^2, 1]$.*

A generalization of the size-reduction operation from [6], [23] is provided in Algorithm 2—given the (reduced) basis $\boldsymbol{G}_{\mathrm{red}}$, its related matrix $\boldsymbol{R}$, the transformation matrix $\boldsymbol{T}$, the indices l and k, and the integer ring $\mathbb{I}$ as input variables. For lattices over $\mathbb{Z}$ and $\mathcal{G}$, the operations are equivalent to the ones defined in the RLLL algorithm [6] and the CLLL algorithm [23], respectively. However, the generalized definition also enables an LLL reduction over $\mathcal{E}$ and $\mathcal{H}$ (and other Euclidean rings).

Given the generalized size-reduction condition from Definition 2, the particular ranges for the choice of δ can be defined. For the Eisenstein integers, $\delta \in (\frac{1}{3}, 1]$ is valid since $\epsilon_{\mathcal{E}}^2 = \frac{1}{3}$, cf. [2]. For the Hurwitz integers, $\delta \in (\frac{1}{2}, 1]$, as $\epsilon_{\mathcal{H}}^2 = \frac{1}{2}$. Since the Lipschitz integers do not form a Euclidean ring, an LLL reduction over $\mathcal{L}$ can—in general—not be defined. This can be seen if

Algorithm 2 Generalized Size Reduction.

```
$[\boldsymbol{G}_{\text{red}}, \boldsymbol{R}, \boldsymbol{T}] = \textsc{SizeRed}(\boldsymbol{G}_{\text{red}}, \boldsymbol{R}, \boldsymbol{T}, l, k, \mathbb{I})$
$r_{\text{q}} = \text{Q}_{\mathbb{I}}\{r_{l,k}\}$
**if** $r_{\text{q}} \neq 0$ **then**
    $\boldsymbol{g}_{\text{red},k} = \boldsymbol{g}_{\text{red},k} - \boldsymbol{g}_{\text{red},l}\, r_{\text{q}}$
    $\boldsymbol{t}_k = \boldsymbol{t}_k - \boldsymbol{t}_l\, r_{\text{q}}$
    In the upper $l$ rows of $\boldsymbol{R}$ (index $1 : l$):
    $\boldsymbol{r}_k = \boldsymbol{r}_k - \boldsymbol{r}_l\, r_{\text{q}}$
**end if**
```

the squared maximum quantization error $\epsilon_{\mathcal{L}}^2$ is inserted into the Lovász condition: even when $\delta = 1$, $\delta - |r_{k-1,k}|^2 = 0$ if $|r_{k-1,k}| = 1$, i.e., the reduction may become inoperative.

Given complex and quaternion-valued matrices, the reduction can alternatively be performed w.r.t. their equivalent real- and real-/complex-valued matrix representations, as defined in (3), (8), and (7). Then, the reduction has to be done with real-valued and/or complex-valued algorithms. However, during the GSO, the particular structure of these matrices (and the isomorphism) is destroyed, i.e., the resulting reduced basis and the related integer matrix cannot be reconverted into equivalent complex/quaternion-valued representations, see also [2]. Consequently, the quality of the reduction will not necessarily be the same in the different representations. More details will be given in Sec. IV.

3) Generalized LLL Reduction Algorithm: In Algorithm 3, a generalized variant of the LLL algorithm is provided. In contrast to other implementations, e.g., in [23], all multiplications are performed in the right order to account for non-commutative behavior. In particular, in the first line, a GSO with pivoting is calculated. The pivoting is not necessarily required, but it is well-known that sorted Gram-Schmidt vectors may speed up the following reduction process [56]. In the loop, the size reduction for the element $r_{k-1,k}$ (over the particular ring $\mathbb{I}$) is done first. Then, the respective Lovász condition can be checked. If it is not fulfilled, the columns $k-1$ and k are *swapped* in $\boldsymbol{G}_{\text{red}}$ and the (unimodular) transformation matrix $\boldsymbol{T}$. As a consequence, the matrices $\boldsymbol{Q}$ and $\boldsymbol{R}$ have to be updated. This can either be done by a complete recalculation of the GSO, or by the procedure in Algorithm 4 that restricts the recalculation to all elements which have to be updated. It is an adapted variant of the procedure in [23], additionally taking the right order of all multiplications into account. If the check of the Lovász condition is successful, the

Algorithm 3 Generalized LLL Reduction.

```
$[\boldsymbol{G}_{\text{red}}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{T}] = \text{LLL}(\boldsymbol{G}_{\text{red}}, \delta, \mathbb{I})$
$[\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{T}] = \text{GSO}(\boldsymbol{G})$    ▷ initial GSO with pivoting
$k = 2$
while $k \leq K$ do
    $[\boldsymbol{G}_{\text{red}}, \boldsymbol{R}, \boldsymbol{T}] = \textsc{SizeRed}(\boldsymbol{G}_{\text{red}}, \boldsymbol{R}, \boldsymbol{T}, k-1, k, \mathbb{I})$
    if $\|\boldsymbol{q}_k\|^2 < (\delta - |r_{k-1,k}|^2) \cdot \|\boldsymbol{q}_{k-1}\|^2$ then    ▷ swap
        $\boldsymbol{G}_{\text{red}} = [\boldsymbol{g}_{\text{red},1:k-2}, \boldsymbol{g}_{\text{red},k}, \boldsymbol{g}_{\text{red},k-1}, \boldsymbol{g}_{\text{red},k+1:K}]$
        $\boldsymbol{T} = [\boldsymbol{t}_{1:k-2}, \boldsymbol{t}_k, \boldsymbol{t}_{k-1}, \boldsymbol{t}_{k+1:K}]$
        $[\boldsymbol{Q}, \boldsymbol{R}] = \textsc{UpdateQR}(\boldsymbol{Q}, \boldsymbol{R}, k)$
        $k = \max(2, k-1)$
    else    ▷ Lovász condition fulfilled
        for $l = k-2, k-3, \ldots, 1$ do
            $[\boldsymbol{G}_{\text{red}}, \boldsymbol{R}, \boldsymbol{T}] = \textsc{SizeRed}(\boldsymbol{G}_{\text{red}}, \boldsymbol{R}, \boldsymbol{T}, l, k, \mathbb{I})$
        end for
        $k = k + 1$
    end if
end while
```

elements $r_{l,k}$, $l = k-2, k-3, \ldots, 1$, are finally reduced and the algorithm continues with the next reduction step until $k = K$.

4) Pseudo-QLLL Reduction: Even though an LLL reduction over the Lipschitz integers can—due to the non-existent Euclidean property—not be defined in general, a *pseudo-QLLL reduction* can be defined instead. In particular, the reduction only becomes inoperative if $|r_{k-1,k}| = 1$. Hence, choosing $\delta = 1$, the LLL algorithm can be applied if the probability that $|r_{k-1,k}| = 1$ tends to zero.

Such a case is, e.g., present if the elements of the generator matrix are drawn i.i.d.ly from a continuous distribution (e.g., an i.i.d. Gaussian one). Then, if the quantization in the size-reduction steps is performed w.r.t. $\mathbb{I} = \mathcal{L}$ and if additionally the parameter $\delta = 1$ is chosen, a pseudo-QLLL-reduced basis obtained. Obviously, no general performance guarantees or bounds can be derived in that case—however, it is at least ensured that the Lovász condition is still operative and that, thus, some kind of "optimized" basis is produced.

Algorithm 4 GSO update if columns k and $k-1$ are swapped.

```
[Q, R] = UPDATEQR(Q, R, k)
$\tilde{\boldsymbol{q}}_{k-1} = \boldsymbol{q}_{k-1}$, $\tilde{\boldsymbol{q}}_k = \boldsymbol{q}_k$, $\tilde{\boldsymbol{R}} = \boldsymbol{R}$        ▷ temporal variables
$\boldsymbol{q}_{k-1} = \boldsymbol{q}_k + \boldsymbol{q}_{k-1} r_{k-1,k}$
$\boldsymbol{r}_{k-1,k} = r^*_{k-1,k} \cdot \|\tilde{\boldsymbol{q}}_{k-1}\|^2 \cdot \|\boldsymbol{q}_k\|^{-2}$
$\boldsymbol{q}_k = \tilde{\boldsymbol{q}}_{k-1} - \boldsymbol{q}_{k-1} r_{k-1,k}$
for $l = k+1, \dots, K$ do
    $r_{k-1,l} = r_{k-1,k} r_{k-1,l} + r_{k,l} \cdot \|\tilde{\boldsymbol{q}}_k\|^2 \cdot \|\boldsymbol{q}_{k-1}\|^{-2}$
    $r_{k,l} = \tilde{r}_{k-1,l} - \tilde{r}_{k-1,k} r_{k,l}$
end for
for $l = 1, \dots, k-2$ do
    $r_{l,k-1} = r_{l,k}$
    $r_{l,k} = \tilde{r}_{l,k-1}$
end for
```

B. Shortest Independent Vectors in Lattices

Another important lattice problem is the determination of the shortest linearly independent vectors in lattices. They are related to the so-called *successive minima*. In particular, the k^{th} successive minimum of a lattice with $N \times K$ generator matrix $\boldsymbol{G}$, $k = 1, \dots, K$, is defined as [5], [57]

$$\mu_k = \inf\{\mu \mid \dim\{\text{span}\{\boldsymbol{\Lambda}(\boldsymbol{G}) \cap \mathrm{B}_N(\mu)\}\} = k\} \ , \tag{43}$$

where $\mathrm{B}_N(\mu)$ denotes the N-dimensional ball with hyperradius μ centered at the origin. In words, μ_k denotes the smallest radius in which K linearly independent vectors can be found within the hyperball. The related lattice points with

$$\mu_k = \|\boldsymbol{\lambda}_{\mathrm{m},k}\| \ , \qquad k = 1, \dots, K \ , \tag{44}$$

form the K linearly independent vectors with the shortest (Euclidean) norms.

Closely related to the *successive minima problem* (SMP)—the determination of the shortest vectors in a lattice—is the *shortest independent vector problem* (SIVP). Here, only the maximum of the norms has to be short as possible, cf. the SBP in (35). Hence, the (generalized) SIVP is a weakened variant of the successive minima problem and defined as

$$\boldsymbol{T} = \underset{\substack{\boldsymbol{T} \in \mathbb{I}^{K \times K} \\ \text{rank}(\boldsymbol{T}) = K}}{\text{argmin}} \ \max_{k=1,\dots,K} \|\boldsymbol{G}\boldsymbol{t}_k\|^2 \ . \tag{45}$$

Obviously, every optimal solution for the successive minima problem is also optimal w.r.t. the SIVP [28], [58].

As becomes apparent from (45), the K independent lattice vectors do not necessarily form a basis of the lattice spanned by $\boldsymbol{G}$. In particular, if the K integer vectors $\boldsymbol{t}_k$ are combined into the integer transformation matrix $\boldsymbol{T} = \left[\boldsymbol{t}_1, \ldots, \boldsymbol{t}_K\right]$, the transformed generator matrix $\boldsymbol{G}_{\text{tra}} = \boldsymbol{GT}$ may only define a *sublattice* of the original one: the integer vectors $\boldsymbol{t}_k$ are only required to be linearly independent, but they do not have form a unimodular transformation matrix in combination. Hence, $\boldsymbol{T}$ may only have full rank, resulting in a "thinned" lattice when multiplied by $\boldsymbol{G}$, depending on the particular determinant $\det(\boldsymbol{T})$. Further details can be, e.g., be found in [2], [19]. Consequently, the successive minima can be used as lower bounds for the norms of the basis vectors of any (alternative) basis for a lattice spanned by a particular generator matrix $\boldsymbol{G}$.

1) Generalized Successive Minima: Even though the successive minima have initially been considered for real-valued lattices over $\mathbb{Z}$, e.g., in [5], [57], it is quite obvious that they can also be determined if other integer rings $\mathbb{I}$ are present. The only condition is that the shortest K linearly independent lattice vectors are found—no additional constraints as, e.g., a Euclidean property of the particular ring are imposed. Hence, the successive minima can be given for all real-, complex-, or quaternion-valued rings that were considered in Sec. II.

In contrast to LLL reduction, the isomorphism of a complex matrix $\boldsymbol{G}$ (over $\mathcal{G}$) and its $2N \times 2K$ real-valued representation $\boldsymbol{G}_{\mathsf{r}}$ according to (3) holds for the successive minima, cf. [28]. The same is valid for quaternion-valued matrices (over $\mathcal{L}$) and their equivalent representations $\boldsymbol{G}_{\mathsf{c}}$ and $\boldsymbol{G}_{\mathsf{r}}$, respectively.

Theorem 1 (Successive Minima of Complex and Quaternionic Lattices over $\mathcal{G}$ and $\mathcal{L}$)**.** *Given a generator matrix $\boldsymbol{G} \in \mathbb{C}^{N \times K}$ for which the successive minima over $\mathbb{I} = \mathcal{G}$ are given as*

$$\boldsymbol{\mu}_{\mathcal{G}} = \left[\mu_1, \mu_2, \ldots, \mu_K\right] \in \mathbb{R}^K \ , \tag{46}$$

the $2K$ successive minima of $\boldsymbol{G}_{\mathsf{r}}$ (over $\mathbb{I} = \mathbb{Z}$) read

$$\boldsymbol{\mu}_{\mathsf{r},\mathbb{Z}} = \left[\mu_1, \mu_1, \mu_2, \mu_2, \ldots, \mu_K, \mu_K\right] \ . \tag{47}$$

Given a generator matrix $\boldsymbol{G} \in \mathbb{H}^{N \times K}$ for which the successive minima over $\mathbb{I} = \mathcal{L}$ are given as

$$\boldsymbol{\mu}_{\mathcal{L}} = \left[\mu_1, \mu_2, \ldots, \mu_K\right] \ , \tag{48}$$

the $2K$ successive minima of $\boldsymbol{G}_{\mathsf{c}}$ (over $\mathbb{I} = \mathcal{G}$) are given as

$$\boldsymbol{\mu}_{\mathsf{c},\mathcal{G}} = \big[\mu_1, \mu_1, \mu_2, \mu_2, \ldots, \mu_K, \mu_K\big] \tag{49}$$

and the $4K$ successive minima of $\boldsymbol{G}_{\mathsf{r}}$ (over $\mathbb{I} = \mathbb{Z}$) read

$$\boldsymbol{\mu}_{\mathsf{r},\mathbb{Z}} = \big[\mu_1, \mu_1, \mu_1, \mu_1, \ldots, \mu_K, \mu_K, \mu_K, \mu_K\big] \ . \tag{50}$$

Proof. Given the equivalent real-valued representation of complex matrices $\boldsymbol{G}_{\mathsf{r}}$ according to (3), pairs of orthogonal (and, thus, linearly independent) column vectors occur at the indices l and $l + K$, which additionally posses the same norm $\|\boldsymbol{g}_{\mathrm{r},k}\| = \|\boldsymbol{g}_{\mathrm{r},k+K}\| = \|\boldsymbol{g}_k\|$, $k = 1, \ldots, K$. Hence, each lattice vector in $\boldsymbol{\Lambda}(\boldsymbol{G}_{\mathsf{r}})$ has an orthogonal counterpart with the same length; both of them isomorphically represent one lattice vector of $\boldsymbol{\Lambda}(\boldsymbol{G})$ over $\mathcal{G}$ (with the same norm). As a consequence, for $\boldsymbol{G}_{\mathsf{r}}$, pairs of linearly independent lattice vectors $\boldsymbol{\lambda}_{\mathrm{m},k}$ and $\boldsymbol{\lambda}_{\mathrm{m},k+1}$ are obtained that yield successive minima with the same value, i.e., $\mu_k = \mu_{k+1}$, $k = 1, 3, \ldots, 2K - 1$.

For quaternion-valued matrices (over $\mathcal{L}$) similar relations hold: In the equivalent complex-valued representation (7), pairs of orthogonal column vectors are present, for which $\|\boldsymbol{g}_{\mathrm{c},k}\| = \|\boldsymbol{g}_{\mathrm{c},k+K}\| = \|\boldsymbol{g}_k\|$, $k = 1 \ldots, K$, is valid. In the equivalent real-valued representation (8), we have orthogonal vectors with $\|\boldsymbol{g}_{\mathrm{r},k}\| = \|\boldsymbol{g}_{\mathrm{r},k+K}\| = \|\boldsymbol{g}_{\mathrm{r},k+2K}\| = \|\boldsymbol{g}_{\mathrm{r},k+3K}\| = \|\boldsymbol{g}_k\|$. Hence, for the former, we obtain $\mu_k = \mu_{k+1}$, $k = 1, 3, \ldots, 2K-1$, and for the latter, $\mu_k = \mu_{k+1} = \mu_{k+2} = \mu_{k+3}$, $k = 1, 5, \ldots, 4K - 3$, is valid. □

For complex and quaternion-valued lattices over $\mathcal{G}$ and $\mathcal{L}$, respectively, the successive minima and the related lattice points and integer vectors are isomorphically obtained by solving the problem via their real-valued and/or complex-valued representations. Hence, a permutation of the real or complex integer vectors can be found such that an integer transformation matrix $\boldsymbol{T}_{\mathsf{r}}$ or $\boldsymbol{T}_{\mathsf{c}}$ is formed that possesses the particular structure defined in (3), (7), or (8). Then, this matrix can be reconverted to a complex or quaternion-valued representation, see also [2, Example 4.3]. Both the "direct" determination of the successive minima over $\mathbb{C}$ or $\mathbb{H}$, and their "indirect" determination over $\mathbb{R}$ or $\mathbb{C}$, finally lead to the same result.

For complex-valued lattices defined over the Eisenstein integers ($\mathbb{I} = \mathcal{E}$), an equivalent real-valued representation can be formed according to (31). The successive minima problem can then be solved over $\mathbb{Z}$—given these results, a reconversion can be conducted in order to solve the problem over $\mathcal{E}$. The same holds for quaternion-valued lattices over $\mathbb{I} = \mathcal{H}$, where the successive minima problem can equivalently be solved over $\mathbb{Z}$ via the representation (32). The reconversion process will be described below (and, additionally, in Appendix A).

C. Generalized Determination of the Successive Minima

For the determination of the successive minima, a special K-dimensional variant of the shortest vector problem has to be solved. It is well-known that already the classical shortest vector problem is NP-hard, i.e., that the computational complexity grows exponentially with the dimension K. Nevertheless, at least for small dimensions, algorithms have been proposed which can efficiently solve the shortest vector problem. The most prominent one is the so-called *sphere decoder* [13].

To solve the successive minima problem, several algorithms have been proposed within the last few years [28]–[30]. One possible strategy applied in [28] is to solve the shortest vector problem K times. Another strategy employed in [29], [30] is to solve an adapted variant thereof once in the beginning, afterwards only operating on the initial result.

In this work, we address the list-based approach initially proposed in [29] which has been shown to perform well w.r.t. runtime behavior if moderate dimensions are present ($K < 20$ in the real-valued case), see also the comparison in [30]. In particular, in that approach, the sphere decoder [13] is initially applied to generate a list that contains all lattice points within a hyperball of a predefined search radius. Then, among those candidates, the shortest linearly independent ones are selected. In the following, this concept is generalized to the real-, complex-, or quaternion-valued integer rings from Sec. II.

The generalized concept is provided in Algorithm 5. As mentioned above, a list-based variant of the sphere decoder is initially applied. As the sphere decoder [13] in combination with Schnorr–Euchner enumeration [8] only operates over real-valued numbers, the generator matrix $\boldsymbol{G}$ has to be converted to its equivalent real-valued representation (given the integer ring $\mathbb{I}$). This is done with the procedure RINGTOZ which is listed in Algorithm 6 in Appendix A. For the list sphere decoder, an initial search radius has to be provided. The naive approach would be to use the maximum (squared) column norm of $\boldsymbol{G}_\mathsf{r}$ as the (squared) radius, since the (squared) solution to the successive minima problem can never be worse than that value. However, the search radius (and the related complexity) can significantly be decreased by applying a reduced basis via the LLL algorithm (Line 2) instead, using the quality parameter $\delta = 1$. Since this call has a low complexity [55], it is negligible in comparison to the call of the list sphere decoder,

Algorithm 5 List-Based Determination of Successive Minima.

```
$[\boldsymbol{G}_{\mathrm{tra}}, \boldsymbol{T}] = \mathrm{SMP}(\boldsymbol{G}, \mathbb{I})$
1: $\boldsymbol{G}_{\mathsf{r}} = \textsc{RingToZ}(\boldsymbol{G}, \mathbb{I})$    ▷ real-valued representation
2: $\left[\boldsymbol{G}_{\mathrm{red}}, \boldsymbol{T}_{\mathrm{LLL}}\right] = \mathrm{LLL}(\boldsymbol{G}_{\mathsf{r}}, 1, \mathbb{Z})$    ▷ reduced basis
3: $\boldsymbol{C}_{\mathrm{t}} = \textsc{ListSphereDecoder}(\boldsymbol{G}_{\mathrm{red}}, \max_k \|\boldsymbol{g}_{\mathrm{red},k}\|^2)$
4: $\boldsymbol{C} = \boldsymbol{T}_{\mathrm{LLL}} \boldsymbol{C}_{\mathrm{t}}$    ▷ convert to original basis
5: $\boldsymbol{C}_{\mathrm{u}} = \textsc{ZToRing}(\boldsymbol{C}, \mathbb{I})$    ▷ go back to ring $\mathbb{I}$
6: $\boldsymbol{C}_{\mathrm{s}} = \textsc{Sort}(\boldsymbol{C}_{\mathrm{u}}, \boldsymbol{G}\boldsymbol{C}_{\mathrm{u}})$    ▷ sort w.r.t. norm
7: $\boldsymbol{i} = \textsc{RowEchelon}(\boldsymbol{C}_{\mathrm{s}})$    ▷ indices of row-echelon form
8: $\boldsymbol{T} = \left[\boldsymbol{c}_{i_1}, \ldots, \boldsymbol{c}_{i_K}\right]$    ▷ shortest independent vectors
9: $\boldsymbol{G}_{\mathrm{tra}} = \boldsymbol{G}\boldsymbol{T}$    ▷ transformed generator matrix
```

which is subsequently applied [13, Algorithm AllClosestPoints]. It results in a matrix of integer candidate vectors $\boldsymbol{C} \in \mathbb{Z}^{K \times N_{\mathrm{c}}}$, where N_{c} denotes the list size. A list of respective candidate vectors w.r.t. the unreduced basis $\boldsymbol{G}_{\mathsf{r}}$ is subsequently calculated by multiplication with $\boldsymbol{T}_{\mathrm{LLL}}$ (Line 4). The integer candidate vectors over the original ring $\mathbb{I}$ are finally obtained by the procedure ZToRing which is listed in Algorithm 6 in Appendix A. In particular, in that procedure, the original complex or quaternion-valued representations are reconstructed from the real-valued ones. In Line 6 of Algorithm 5, the candidate vectors are then sorted in ascending order w.r.t. their norms. This can be done by a standard sorting algorithm [54]. In the procedure RowEchelon, which is listed in Appendix A (Algorithm 7), the matrix of sorted candidate vectors is transformed to row-echelon form. At the particular indices $\boldsymbol{i} = \left[i_1, \ldots, i_K\right]$ where a new dimension is established ("steps" in the row-echelon form), the vector resulting in the k^{th} successive minimum is found as it leads to the shortest vector that is independent from the previous $k-1$ ones. The related transformation matrix $\boldsymbol{T}$ is formed in Line 8, and the respective transformed generator matrix $\boldsymbol{G}_{\mathrm{tra}}$ finally in Line 9.

The reconversion to the original ring $\mathbb{I}$ (as performed in Line 5 in Algorithm 5) can alternatively be performed *after* the calculation of the matrices $\boldsymbol{T}$ and $\boldsymbol{G}_{\mathrm{tra}}$ (defined over $\mathbb{Z}$ and $\mathbb{R}$) takes place. However, then, for complex and quaternion-valued lattices, the calculation of the row-echelon form has to be performed over real numbers with the equivalent $2K \times 2N_{\mathrm{c}}$ and $4K \times 4N_{\mathrm{c}}$ representation of $\boldsymbol{C}$, respectively.

IV. Generalized Quality Bounds and Asymptotic Computational Complexity

Based on the generalized criteria and algorithms discussed previously, quality bounds are derived and compared to each other in this section. In addition, the asymptotic complexity of both above-mentioned (generalized) algorithms is evaluated.

A. Bounds on the Norms

The norms of the basis vectors are suited quantities to assess the quality of a lattice basis. Since the respective successive minima are given as the norms of the shortest independent vectors in the particular lattice, they serve as lower bounds on the norms resulting from any lattice-basis-reduction scheme.

To solve the SIVP (45) and the SBP (35), respectively, it is required that the *maximum* of the K norms has to be as small as possible. However, as stated in [59, p. 35], it is generally not possible to derive bounds for the K^{th} successive minimum and any other of them except from the first. In particular, $\mu_2, \ldots, \mu_K$ can become arbitrarily large in comparison to the lattice volume. It is quite obvious that the same holds for the norms of the basis vectors $\boldsymbol{g}_2, \ldots, \boldsymbol{g}_K$. Nevertheless, for the first successive minimum μ_1 and the related basis vector $\boldsymbol{g}_1$, bounds can in general be given.

1) First Successive Minimum: Given a real-valued lattice ($\mathbb{I} = \mathbb{Z}$) with generator matrix $\boldsymbol{G} \in \mathbb{R}^{N \times K}$, the squared first successive minimum is bounded according to *Minkowski's first theorem* [3], [9], [59]

$$\mu_{1,\mathbb{Z}}^2 \leq \eta_K \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \ , \tag{51}$$

where the factor η_K, which depends on the particular dimension, is called Hermite's constant. It is only known for dimensions up to $K = 8$ as well as $K = 24$, cf. [59, Table on p. 33]. However, it has been shown that Hermite's constant can be upper-bounded by the term [60]

$$\eta_K \leq \frac{2}{\pi} \Gamma\left(2 + \frac{K}{2}\right)^{\frac{2}{K}} \ , \tag{52}$$

where $\Gamma(x) = (x-1)!$ denotes the Gamma function.

For complex and quaternion-valued lattices over $\mathcal{G}$ and $\mathcal{L}$, respectively, (51) can straightforwardly be generalized.

Theorem 2 (Generalized Bounds on the First Successive Minimum for Lattices over $\mathcal{G}$ and $\mathcal{L}$)**.** *For complex-valued lattices over $\mathbb{I} = \mathcal{G}$ with generator matrix $\boldsymbol{G} \in \mathbb{C}^{N \times K}$, the first successive minimum is bounded by*

$$\mu_{1,\mathcal{G}}^2 \leq \eta_{2K} \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \; . \tag{53}$$

For quaternion-valued lattices over $\mathbb{I} = \mathcal{L}$ with generator matrix $\boldsymbol{G} \in \mathbb{H}^{N \times K}$, it is bounded by

$$\mu_{1,\mathcal{L}}^2 \leq \eta_{4K} \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \; . \tag{54}$$

Proof. If $\boldsymbol{G} \in \mathbb{C}^{N \times K}$, we have $\mu_{1,\mathcal{G}}^2 = \mu_{1,\text{r},\mathbb{Z}}^2$, where $\mu_{1,\text{r},\mathbb{Z}}^2$ denotes the first successive minimum of the equivalent $2N \times 2K$ real-valued representation $\boldsymbol{G}_\text{r}$ according to (3), cf. Theorem 1. Moreover, according to (4) and (30), $\operatorname{vol}^{\frac{2}{2K}}(\boldsymbol{\Lambda}(\boldsymbol{G}_\text{r})) = \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G}))$.

If $\boldsymbol{G} \in \mathbb{H}^{N \times K}$, $\mu_{1,\mathcal{L}}^2 = \mu_{1,\text{r},\mathbb{Z}}^2$, where $\mu_{1,\text{r},\mathbb{Z}}^2$ denotes the first successive minimum of the equivalent $4N \times 4K$ real-valued representation $\boldsymbol{G}_\text{r}$ according to (8). Moreover, according to (9), $\operatorname{vol}^{\frac{2}{4K}}(\boldsymbol{\Lambda}(\boldsymbol{G}_\text{r})) = \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G}))$. □

For lattices over the Eisenstein integers $\mathcal{E}$ and the Hurwitz integers $\mathcal{H}$, even better bounds can be derived.

Theorem 3 (Generalized Bounds on the First Successive Minimum for Lattices over $\mathcal{E}$ and $\mathcal{H}$)**.** *For complex lattices defined over the Eisenstein integers $\mathcal{E}$ with generator matrix $\boldsymbol{G} \in \mathbb{C}^{N \times K}$, the first successive minimum is bounded as*

$$\mu_{1,\mathcal{E}}^2 \leq \frac{\sqrt{3}}{2} \eta_{2K} \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \; . \tag{55}$$

For quaternion-valued lattices defined over the Hurwitz integers $\mathcal{H}$ with generator matrix $\boldsymbol{G} \in \mathbb{H}^{N \times K}$, it is bounded by

$$\mu_{1,\mathcal{H}}^2 \leq \frac{1}{\sqrt{2}} \eta_{4K} \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \; . \tag{56}$$

Proof. We can take advantage of the property that for the determinant of the matrix $\boldsymbol{G}_\mathcal{E}$ in (31),

$$\det(\boldsymbol{G}_\mathcal{E}) = \left(-\frac{\sqrt{3}}{2}\right)^K \tag{57}$$

is valid. Hence, we obtain

$$\begin{aligned}
\mu_{1,\mathcal{E}}^2 &\leq \eta_{2K} \operatorname{vol}^{\frac{2}{2K}}(\boldsymbol{\Lambda}(\boldsymbol{G}_{\mathsf{r},\mathcal{E}})) \\
&= \eta_{2K} \det^{\frac{1}{2K}}(\boldsymbol{G}_{\mathsf{r},\mathcal{E}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r},\mathcal{E}}) \\
&= \eta_{2K} \det^{\frac{1}{2K}}(\boldsymbol{G}_{\mathcal{E}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r}} \boldsymbol{G}_{\mathcal{E}}) \\
&= |\det(\boldsymbol{G}_{\mathcal{E}})|^{\frac{1}{K}} \eta_{2K} \det^{\frac{1}{2K}}(\boldsymbol{G}_{\mathsf{r}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r}}) \\
&\overset{(57)}{=} \frac{\sqrt{3}}{2} \eta_{2K} \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \ .
\end{aligned} \tag{58}$$

For lattices over the Hurwitz integers, we have

$$\det(\boldsymbol{G}_{\mathcal{H}}) = \left(\frac{1}{2}\right)^K \ , \tag{59}$$

cf. (32). Consequently, the bound reads

$$\begin{aligned}
\mu_{1,\mathcal{H}}^2 &\leq \eta_{4K} \operatorname{vol}^{\frac{2}{4K}}(\boldsymbol{\Lambda}(\boldsymbol{G}_{\mathsf{r},\mathcal{H}})) \\
&= \eta_{4K} \det^{\frac{1}{4K}}(\boldsymbol{G}_{\mathsf{r},\mathcal{H}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r},\mathcal{H}}) \\
&= \eta_{4K} \det^{\frac{1}{4K}}(\boldsymbol{G}_{\mathcal{H}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r}} \boldsymbol{G}_{\mathcal{H}}) \\
&= |\det(\boldsymbol{G}_{\mathcal{H}})|^{\frac{1}{2K}} \eta_{4K} \det^{\frac{1}{4K}}(\boldsymbol{G}_{\mathsf{r}}^{\mathsf{T}} \boldsymbol{G}_{\mathsf{r}}) \\
&\overset{(59)}{=} \frac{1}{\sqrt{2}} \eta_{4K} \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \ .
\end{aligned} \tag{60}$$

□

For lattices over $\mathcal{E}$, the bound (55) is lower than the one for lattices over $\mathcal{G}$ in (53) since $\frac{\sqrt{3}}{2} \approx 0.866$. Hence, in general, the first successive minimum is expected to be smaller. Noteworthy, (55) is a special variant of the bound for lattices over imaginary quadratic fields [61]. Given quaternion-valued lattices, the bound for $\mathcal{H}$ is lowered by a factor of $\frac{1}{\sqrt{2}} \approx 0.707$ in comparison to the bound for $\mathcal{L}$.

2) First Basis Vector of an LLL Basis: In the initial publication on LLL reduction over $\mathbb{I} = \mathbb{Z}$ [6], it has been shown that the squared norm of the first basis vector can be bounded by

$$\mu_{1,\mathbb{Z}}^2 \leq \|\boldsymbol{g}_{1,\mathbb{Z}}\|^2 \leq \operatorname{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \cdot \left(\frac{1}{\delta - \underbrace{1/4}_{\epsilon_{\mathbb{Z}}^2}}\right)^{\frac{K-1}{2}} \ . \tag{61}$$

It is quite clear that the (squared) first successive minimum serves as a lower bound on the (squared) length of the vector. In the upper bound, the Lovász condition (38) is incorporated, in particular the part within the braces. Thereby, the squared maximum quantization error $\epsilon_{\mathbb{Z}}^2 = \frac{1}{4}$ serves as an upper bound for the particular value of $r_{l,k}$ (cf. Sec. II and Sec. III).

Theorem 4 (Generalized Bound on the First Basis Vector of an LLL Basis)**.** *Given a lattice with $N \times K$ generator matrix $\boldsymbol{G}$ which is LLL-reduced over the particular Euclidean integer ring $\mathbb{I}$, the first basis vector is bounded as*

$$\mu_{1,\mathbb{I}}^2 \leq \|\boldsymbol{g}_{1,\mathbb{I}}\|^2 \leq \mathrm{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \cdot \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{\frac{K-1}{2}} \quad . \tag{62}$$

Proof. The lower bound is quite obvious, since $\mu_{1,\mathbb{I}}$ is the norm of the shortest (non-zero) vector in the lattice. The upper bound is, by analogy with the derivation of the original bound (61) in [6], derived as follows: Due to the Lovász condition (41),

$$\|\boldsymbol{q}_k\|^2 \leq \frac{1}{\delta - \epsilon_{\mathbb{I}}^2} \|\boldsymbol{q}_{k+1}\|^2 \, . \tag{63}$$

Hence, since in the (unsorted) GSO, $\boldsymbol{q}_1 = \boldsymbol{g}_1$,

$$\begin{aligned} \|\boldsymbol{g}_{1,\mathbb{I}}\|^2 &\leq \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{l-1} \|\boldsymbol{q}_l\|^2 \\ &\leq \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{K-1} \|\boldsymbol{q}_l\|^2 \, , \qquad l = 2 \ldots, K \, . \end{aligned} \tag{64}$$

In addition, as $\|\boldsymbol{g}_{1,\mathbb{I}}\| = \|\boldsymbol{q}_1\| \leq \|\boldsymbol{q}_l\|$,

$$\|\boldsymbol{g}_{1,\mathbb{I}}\|^K \leq \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{\frac{K(K-1)}{2}} \prod_{k=1}^{K} \|\boldsymbol{q}_k\|^2 \tag{65}$$

and, since, as stated, e.g., in [6], $\prod_{k=1}^{K} \|\boldsymbol{q}_k\|^2 = \mathrm{vol}^2(\boldsymbol{\Lambda}(\boldsymbol{G}))$,

$$\|\boldsymbol{g}_{1,\mathbb{I}}\| \leq \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{\frac{K-1}{2}} \mathrm{vol}^{\frac{2}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \, . \tag{66}$$

□

3) Comparison of the Bounds: The above upper bounds on the first successive minimum and the first basis vector of an LLL basis are—normalized to the volume of the lattice—illustrated in Fig. 3. In particular, in the upper plot, the complex case is considered. In the bottom plot, quaternion-valued matrices are regarded. To this end, the exact value for Hermite's constant has been chosen for all dimensions where it is exactly known; otherwise, the approximation (52) has been used. For LLL reduction, the (optimal) parameter $\delta = 1$ is assumed.

Considering the first successive minimum, the superiority of lattices over $\mathcal{E}$ and $\mathcal{H}$, in comparison to lattices over $\mathcal{G}$ and $\mathcal{L}$, or their isomorphic real- and complex-valued representations over $\mathbb{Z}$ and $\mathcal{G}$, respectively, is clearly visible. For $N \times 2$ matrices, in both the complex and quaternion-valued case, the LLL-reduced first basis vectors are identical to the respective first successive minima. This is not a surprise since an LLL reduction with $\delta = 1$ is equivalent to a Gaussian reduction, cf. [14], [23]. It is quite obvious that this relation does not hold any more if the LLL reduction is applied to the equivalent $2N \times 4$ or $4N \times 8$ isomorphic representations. When increasing the dimensions, the loss of the LLL approach in comparison to the successive minima becomes more and more apparent. Among all variants of LLL reduction, given $\delta = 1$, the QLLL one ($\mathbb{I} = \mathcal{H}$) performs the best, followed by the ELLL one ($\mathbb{I} = \mathcal{E}$). The RLLL approach ($\mathbb{I} = \mathbb{Z}$) already shows a significant gap, and the CLLL one ($\mathbb{I}= \mathcal{G}$) performs the worst.

In Fig. 3, the quality parameter $\delta = 1$ is considered. Still the question remains which type of LLL reduction is—depending on δ—the best performing one in an asymptotic manner. Given complex lattices, in [23], it has been shown that independently from the dimension K and the parameter δ, the RLLL approach performs better than the CLLL one—except for the case when $\delta = \frac{3}{4}$; then, both perform the same. For the sake of completeness, the derivation is provided in Appendix B and subsequently generalized to the other variants of the LLL algorithm. In particular, given complex matrices and comparing the bound in (62) for the ELLL approach and the CLLL one, it becomes apparent that—independently from K, the ELLL approach performs better as $\delta - \frac{1}{3} > \delta - \frac{1}{2}$. It is shown in Appendix B that if $3/4 - 1/\sqrt{6} < \delta \leq 1$, where $3/4 - 1/\sqrt{6} \approx \frac{1}{3}$, the ELLL algorithm also leads to a lowered bound when compared with the RLLL one (independently from K). Hence, in contrast to the CLLL algorithm, the ELLL approach generally performs better, except from a small range where the quality parameter asymptotically approaches its lower bound $\delta = \frac{1}{3}$.

Given quaternion-valued lattices and comparing the upper bound in (62) with the one for the CLLL algorithm using the equivalent $2N \times 2K$ complex-valued representation (7), it can be stated that the QLLL approach performs better as $(\delta - 1/2)^{-\frac{K-1}{2}} < (\delta - 1/2)^{-\frac{2K-1}{2}}$ for $K \in \mathbb{N}$. In Appendix B, the comparison is also given with respect to ELLL reduction. Then, the QLLL strategy generally performs better except from a small range where $\delta \approx \frac{1}{2}$. The QLLL approach even surpasses the performance of the RLLL one using the equivalent real-valued representation—here, the superiority holds again for all quality parameters except from $\delta \approx \frac{1}{2}$.

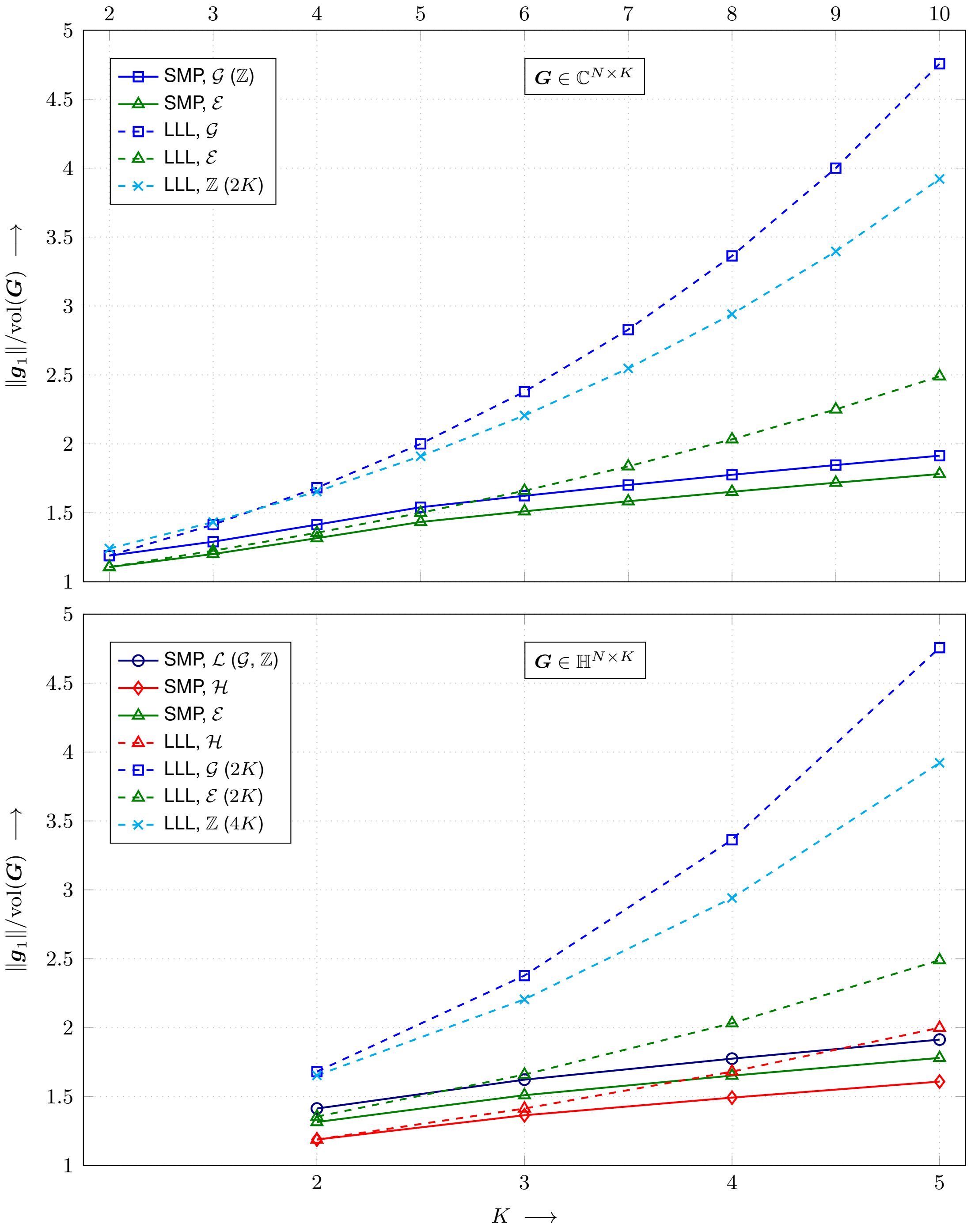


Fig. 3. Upper bounds on the normalized first successive minimum (solid lines) and the normalized first basis vector of an LLL-reduced basis with parameter $\delta = 1$ (dashed lines) over the dimension K. Top: complex-valued lattices. Bottom: quaternion-valued lattices.

B. Bounds on the Product of the Norms

Even though the bounds listed above are restricted to the first vectors, it is possible to gain some indirect knowledge on the norms of the other vectors. In particular, the *product* of the norms can be bounded.

1) Product of the Successive Minima: According to *Minkowski's second theorem* [59], [62], for any $L = 1, \ldots, K$, the product of the first L (squared) successive minima can be bounded by

$$\prod\nolimits_{l=1}^{L} \mu_{l,\mathbb{Z}}^2 \leq \eta_K^L \operatorname{vol}^{\frac{2L}{K}}(\mathbf{\Lambda}(\boldsymbol{G})) \ . \tag{67}$$

Since, for $L = K$,

$$\prod\nolimits_{k=1}^{K} \mu_{k,\mathbb{Z}}^2 \leq \eta_K^K \operatorname{vol}^2(\mathbf{\Lambda}(\boldsymbol{G})) \ , \tag{68}$$

a bound for the orthogonality defect (29) of the transformed matrix $\boldsymbol{G}_{\text{tra},\mathbb{Z}} = \boldsymbol{G}\boldsymbol{T}_{\mathbb{Z}}$ containing the shortest independent lattice vectors (cf. Sec. III) is readily obtained.

Theorem 5 (Bound on the Orthogonality Defect of the Shortest Independent Vectors in a Real-Valued Lattice)**.** *The orthogonality defect of the transformed matrix* $\boldsymbol{G}_{\text{tra}}$ *is upper bounded by*

$$\Omega(\boldsymbol{G}_{\text{tra},\mathbb{Z}}) \leq \eta_K^{\frac{K}{2}} \ . \tag{69}$$

Proof. If $\boldsymbol{T}_{\mathbb{Z}}$ is unimodular, (69) directly follows from (68) since $\mathbf{\Lambda}(\boldsymbol{G}_{\text{tra},\mathbb{Z}}) = \mathbf{\Lambda}(\boldsymbol{G})$ is valid. If $\boldsymbol{T}_{\mathbb{Z}}$ is non-unimodular, $\mathbf{\Lambda}(\boldsymbol{G}_{\text{tra},\mathbb{Z}}) \neq \mathbf{\Lambda}(\boldsymbol{G})$. However, since, then, $\sqrt{\det(\boldsymbol{T}_{\mathbb{Z}}^{\mathsf{H}}\boldsymbol{T}_{\mathbb{Z}})} > 1$, we have $\operatorname{vol}(\mathbf{\Lambda}(\boldsymbol{G}_{\text{tra},\mathbb{Z}})) > \operatorname{vol}(\mathbf{\Lambda}(\boldsymbol{G}))$. Consequently,

$$\Omega^2(\boldsymbol{G}_{\text{tra},\mathbb{Z}}) = \frac{\prod_{l=1}^{L} \mu_{l,\mathbb{Z}}^2}{\operatorname{vol}^2(\mathbf{\Lambda}(\boldsymbol{G}_{\text{tra},\mathbb{Z}}))} < \frac{\prod_{l=1}^{L} \mu_{l,\mathbb{Z}}^2}{\operatorname{vol}^2(\mathbf{\Lambda}(\boldsymbol{G}))} \ , \tag{70}$$

i.e., (69) still follows from (68). □

The above bounds can straightforwardly be generalized to complex and quaternionic lattices over $\mathcal{G}$ and $\mathcal{L}$, respectively.

Theorem 6 (Generalized Bounds on the Product of the Successive Minima and the Related Orthogonality Defect for Lattices over $\mathcal{G}$ and $\mathcal{L}$)**.** *The generalized bound on the product of the successive minima for complex lattices over* $\mathcal{G}$ *reads*

$$\prod\nolimits_{l=1}^{L} \mu_{l,\mathcal{G}}^2 \leq \eta_{2K}^L \operatorname{vol}^{\frac{2L}{K}}(\mathbf{\Lambda}(\boldsymbol{G})) \tag{71}$$

and the related orthogonality defect is bounded by

$$\Omega(\boldsymbol{G}_{\mathrm{tra},\mathcal{G}}) \leq \eta_{2K}^{\frac{K}{2}} \ . \tag{72}$$

Generalizing Minkowski's second theorem to quaternion-valued lattices over $\mathcal{L}$, the bound

$$\prod\nolimits_{l=1}^{L} \mu_{l,\mathcal{L}}^2 \leq \eta_{4K}^{L} \operatorname{vol}^{\frac{2L}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \tag{73}$$

is obtained and the bound on the orthogonality defect reads

$$\Omega(\boldsymbol{G}_{\mathrm{tra},\mathcal{L}}) \leq \eta_{4K}^{\frac{K}{2}} \ . \tag{74}$$

Proof. The argumentation can be done equivalently to the ones which are given in the proofs for Theorem 2 and Theorem 5. □

For lattices over $\mathcal{E}$ and $\mathcal{H}$, respective bounds are readily obtained by the incorporation of the particular properties of the matrices defined in (31) and (32), respectively.

Theorem 7 (Generalized Bounds on the Product of the Successive Minima and the Related Orthogonality Defect for Lattices over $\mathcal{E}$ and $\mathcal{H}$)**.** *For complex-valued lattices defined over the Eisenstein integers, the product of the successive minima is bounded by*

$$\prod\nolimits_{l=1}^{L} \mu_{l,\mathcal{E}}^2 \leq \left(\frac{\sqrt{3}}{2}\right)^{L} \eta_{2K}^{L} \operatorname{vol}^{\frac{2L}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \tag{75}$$

and the orthogonality defect by

$$\Omega(\boldsymbol{G}_{\mathrm{tra},\mathcal{E}}) \leq \left(\frac{3}{4}\right)^{\frac{K}{4}} \eta_{2K}^{\frac{K}{2}} \ . \tag{76}$$

For quaternion-valued lattices which are defined over the Hurwitz integers,

$$\prod\nolimits_{l=1}^{L} \mu_{l,\mathcal{H}}^2 \leq \left(\frac{1}{\sqrt{2}}\right)^{L} \eta_{4K}^{L} \operatorname{vol}^{\frac{2L}{K}}(\boldsymbol{\Lambda}(\boldsymbol{G})) \tag{77}$$

is obtained. Here, the orthogonality defect is bounded by

$$\Omega(\boldsymbol{G}_{\mathrm{tra},\mathcal{H}}) = \left(\frac{1}{4}\right)^{\frac{K}{4}} \eta_{4K}^{\frac{K}{2}} \ . \tag{78}$$

Proof. Again, the argumentation is performed in an equivalent way to the ones which are given in the proofs for Theorem 3 and Theorem 5. □

When employing complex lattices over $\mathcal{E}$, the upper bound on the orthogonality defect shrinks by a factor of $(3/4)^{\frac{K}{4}}$ in comparison to lattices over $\mathcal{G}$. Thereby, in contrast to the bound on the first vector in (55), the expected gain grows with the dimension K. For quaternion-valued lattices over $\mathbb{I} = \mathcal{H}$, the gap to the bound over $\mathbb{I} = \mathcal{L}$ grows by a factor of $(1/4)^{\frac{K}{4}}$ over the dimension K.

2) Product of the Basis Vectors of an LLL Basis: Bounds for the product of the norms of an LLL-reduced basis can be derived in a similar way. In particular, it is known that at least the product over *all* basis vectors is bounded as [6], [59]

$$\prod_{k=1}^{K} \mu_{k,\mathbb{Z}}^2 \leq \prod_{k=1}^{K} \|\boldsymbol{g}_{k,\mathbb{Z}}\|^2 \leq \text{vol}^2(\boldsymbol{\Lambda}(\boldsymbol{G})) \cdot \underbrace{\left(\frac{1}{\delta - 1/4}\right)^{\frac{K(K-1)}{2}}}_{\geq \Omega^2(\boldsymbol{G}_{\text{red},\mathbb{Z}})} . \tag{79}$$

where the rightmost term represents the squared orthogonality defect of the reduced basis $\boldsymbol{G}_{\text{red},\mathbb{Z}} = \boldsymbol{G}\boldsymbol{T}_{\mathbb{Z}}$.

By analogy with the generalized bounds for the first basis vector from Sec. IV-A2, generalized bounds on the product of the norms and the related orthogonality defect can be derived.

Theorem 8 (Generalized Bounds on the Product of the Norms of an LLL-Reduced Basis and its Related Orthogonality Defect)**.** *Given a lattice $\boldsymbol{\Lambda}(\boldsymbol{G})$ spanned by the $N \times K$ generator matrix $\boldsymbol{G}$, the product of the norms of the basis vectors of an equivalent LLL-reduced matrix $\boldsymbol{G}_{\text{red},\mathbb{I}}$ obtained over the integer ring $\mathbb{I}$ w.r.t. the quality parameter δ is bounded as*

$$\prod_{k=1}^{K} \mu_{k,\mathbb{I}}^2 \leq \prod_{k=1}^{K} \|\boldsymbol{g}_{k,\mathbb{I}}\|^2 \leq \text{vol}^2(\boldsymbol{\Lambda}(\boldsymbol{G})) \cdot \underbrace{\left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{\frac{K(K-1)}{2}}}_{\geq \Omega^2(\boldsymbol{G}_{\text{red},\mathbb{I}})} . \tag{80}$$

Thereby, the rightmost term defines an upper bound on the squared orthogonality defect of $\boldsymbol{G}_{\text{red},\mathbb{I}}$.

Proof. The lower bound is readily obtained since $\mu_{k,\mathbb{I}}$ represent the norms of the shortest (non-zero) vectors in the particular lattice. The upper bound is, similar to the proof for the original bound (79) in [6], given as follows: After LLL reduction, the k^{th} basis vector can be written as

$$\begin{aligned} \|\boldsymbol{g}_{k,\mathbb{I}}\|^2 &= \|\boldsymbol{q}_k\|^2 + \sum_{l=1}^{k-1} |r_{k,l}|^2 \|\boldsymbol{q}_l\|^2 \\ &\leq \|\boldsymbol{q}_k\|^2 + \sum_{l=1}^{k-1} \epsilon_{\mathbb{I}}^2 \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{k-l} \|\boldsymbol{q}_k\|^2 \\ &= \left(1 + \epsilon_{\mathbb{I}}^2 \sum_{l=1}^{k-1} \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{k-l}\right) \cdot \|\boldsymbol{q}_k\|^2 \\ &\leq \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{k-1} \cdot \|\boldsymbol{q}_k\|^2 . \end{aligned} \tag{81}$$

Forming the product over all basis vectors, we obtain

$$\prod_{k=1}^{K} \|\boldsymbol{g}_{k,\mathbb{I}}\|^2 \leq \left(\frac{1}{\delta - \epsilon_{\mathbb{I}}^2}\right)^{\frac{K(K-1)}{2}} \underbrace{\prod_{k=1}^{K} \|\boldsymbol{q}_k\|^2}_{\mathrm{vol}^2(\boldsymbol{\Lambda}(\boldsymbol{G}))} . \tag{82}$$

□

3) Comparison of the Bounds: In Fig. 4, the different bounds on the orthogonality defect are depicted (Top: complex lattices, Bottom: quaternionic lattices). Again, Hermite's constant has been chosen exactly if it is known for the particular dimension; otherwise, it has been approximated by (52). The quality parameter $\delta = 1$ is assumed for LLL reduction.

Considering the orthogonality defect of the transformed matrix $\boldsymbol{G}_{\mathrm{tra},\mathbb{I}}$ formed by the shortest vectors in the lattice, the superiority of lattices over $\mathcal{E}$ (Fig. 4 Top) and $\mathcal{H}$ (Fig. 4 Bottom) in comparison to lattices defined over $\mathcal{L}$ and $\mathcal{G}$, respectively, is clearly visible. In the quaternion-valued case, the QLLL reduction approaches the orthogonality defect of $\boldsymbol{G}_{\mathrm{tra},\mathcal{H}}$ quite well. In general, the QLLL reduction shows the best reduction quality, followed by the ELLL one. Interestingly, the CLLL approach ($\mathbb{I} = \mathcal{G}$) performs better than the RLLL one ($\mathbb{I} = \mathbb{Z}$) with doubled dimensions. This is contrary to the behavior for the bounds on the first vector depicted in Fig. 3, for which the RLLL reduction performed better.

Given a particular quality parameter δ, the asymptotic behavior of the different types of LLL reduction still has to be analyzed. This is done with the help of Appendix C, where the respective (long) derivations are provided. In particular, in the complex-valued case, the bound for CLLL reduction is compared to the bound for RLLL reduction employing the equivalent $2N \times 2K$ representation $\boldsymbol{G}_{\mathsf{r}}$. It becomes apparent that, independently from K, the CLLL approach performs better than the RLLL one; the CLLL one only performs worse if δ asymptotically approaches its lower limit, i.e., if $\delta \approx \frac{1}{2}$. Please note that this behavior is contrary to the one for the norm of the first vector as stated above, where the RLLL performed better except from $\delta = \frac{3}{4}$. Hence, the CLLL algorithm achieves a lowered bound on the orthogonality defect, which has not been stated in the original CLLL paper [23]. It is also quite obvious that the ELLL approach performs better than the RLLL one for most δ except from $\delta \approx \frac{1}{3}$. Besides, the ELLL approach generally performs better than the QLLL one since in (80), $\delta - \frac{1}{3} > \delta - \frac{1}{2}$.

Given quaternion-valued lattices, the QLLL reduction is more powerful than the CLLL one applied to the $2N \times 2K$ complex representation $\boldsymbol{G}_{\mathsf{c}}$ since $(\delta - 1/2)^{-\frac{K^2-K}{2}} < (\delta - 1/2)^{-\frac{2(2K^2-K)}{2}}$.

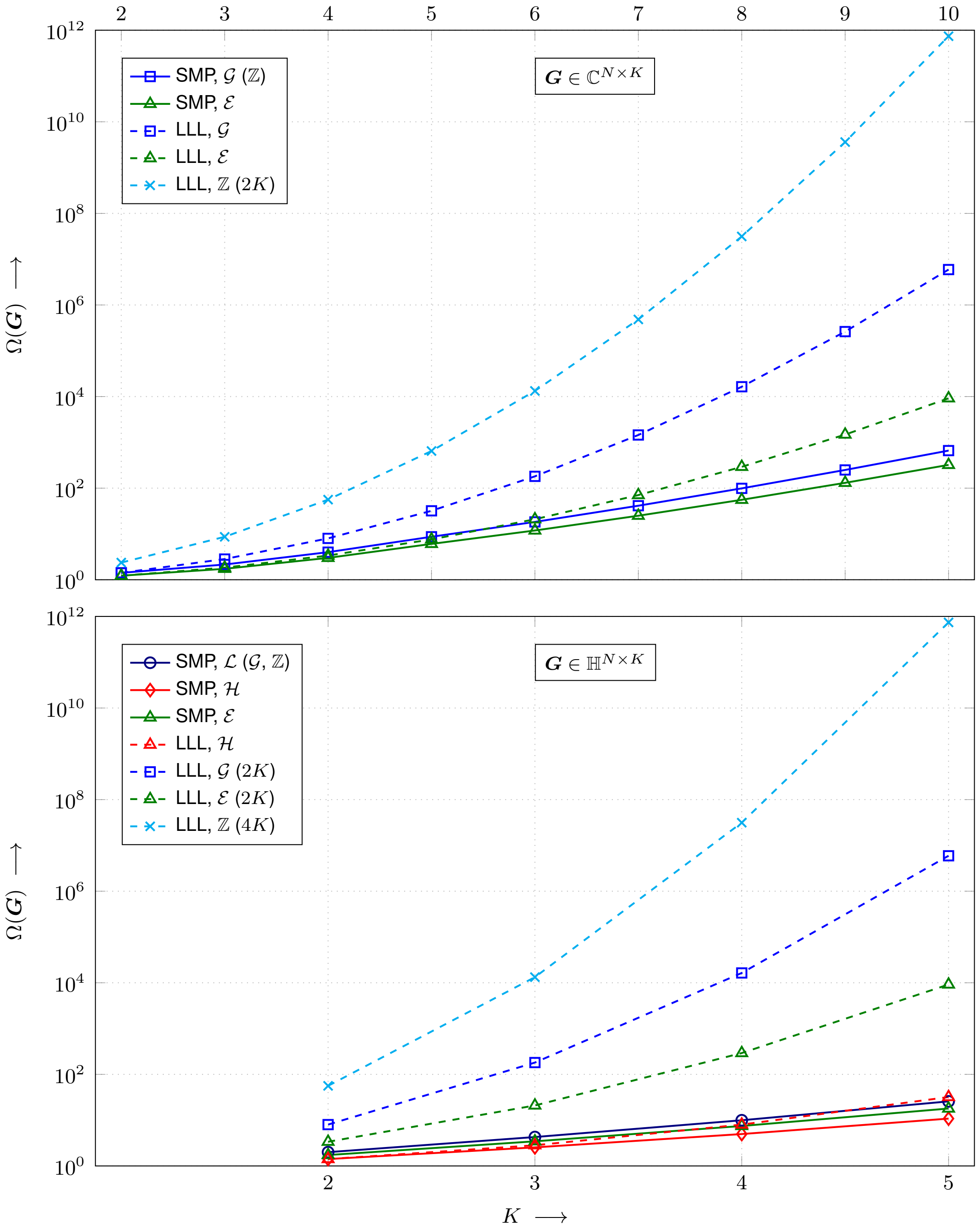


Fig. 4. Upper bounds on the orthogonality defect of the transformed matrix $\boldsymbol{G}_{\text{tra},\mathbb{I}}$ formed by the shortest independent vectors of the lattice (solid lines) and on the orthogonality defect of the LLL-reduced basis $\boldsymbol{G}_{\text{red},\mathbb{I}}$ with parameter $\delta = 1$ (dashed lines) over the dimension K. Top: complex-valued lattices. Bottom: quaternion-valued lattices.

Moreover, as shown in Appendix C, independently from K it performs better than the ELLL reduction on $\boldsymbol{G}_{\mathsf{c}}$ and also better than the RLLL reduction applied to the equivalent $4N \times 4K$ real-valued representation $\boldsymbol{G}_{\mathsf{r}}$, except from a small range where $\delta \approx \frac{1}{2}$.

C. Asymptotic Computational Complexity

The asymptotic computational complexity is studied next. This includes a general discussion on the complexity as well a comparison of the different variants, i.e., of the complexity if different types of integer rings are applied.

1) Complexity of List-Based Determination of the Successive Minima: In Algorithm 5, three main steps can be identified: i) the call of the (real-valued) LLL algorithm to find short initial basis vectors, ii) the call of the list sphere decoder that provides all points within a hypersphere where the maximum norm of the basis defines the radius, and iii) the calculation of the row-echelon form.

Even if $\delta = 1$, the LLL algorithm has a polynomial complexity given a particular dimension [55]; hence, it can efficiently be performed, see also the discussion below. Moreover, the transformation to row-echelon form (Algorithm 7) that applies a simple Gaussian elimination has a polynomial complexity over K as well as the list size N_{c}. In particular, its asymptotic complexity reads $\mathcal{O}(K^2 N_{\mathrm{c}})$, since (less than) K rows of $\boldsymbol{C}$ have to be updated K times, particularly each time when an independent vector was found.

Hence, the crucial point in the algorithm algorithm is the call of the sphere decoder [13], which is known to have an exponential complexity (over K). In [29], it has been stated that the number of candidates, i.e., the number of points within a *real-valued* hypersphere, can be approximated by

$$N_{\mathrm{c},\mathbb{Z}} \approx \frac{(\pi\psi^2)^{K/2}}{\frac{K}{2}!\,\mathrm{vol}(\boldsymbol{\Lambda}(\boldsymbol{G}))}\ , \tag{83}$$

for the real-valued generator matrix $\boldsymbol{G} \in \mathbb{R}^{N\times K}$, see also [25], where ψ^2 denotes the squared search radius which is defined as $\psi^2 = \max_k \|\boldsymbol{g}_{\mathrm{LLL},k}\|^2$. Since the maximum norm of an LLL-reduced basis (as well as the Kth successive minimum) cannot be bounded, the list size cannot be bounded, too.

Given complex-valued lattices over $\mathcal{G}$ with generator matrix $\boldsymbol{G} \in \mathbb{C}^{N\times K}$, the estimated list size is obtained as

$$N_{\mathrm{c},\mathcal{G}} \approx \frac{(\pi\psi^2)^{K}}{K!\,\mathrm{vol}(\boldsymbol{\Lambda}(\boldsymbol{G}_{\mathsf{r}}))} = \frac{(\pi\psi^2)^{K}}{K!\,\mathrm{vol}^2(\boldsymbol{\Lambda}(\boldsymbol{G}))}\ , \tag{84}$$

since the search is actually performed with the $2N \times 2K$ representation $\boldsymbol{G}_{\mathsf{r}}$ with $\mathrm{vol}(\boldsymbol{G}_{\mathsf{r}}) = \mathrm{vol}^2(\boldsymbol{G})$, cf. Sec.II. However, for lattices over Eisenstein integers, the search is actually performed with $\boldsymbol{G}_{\mathsf{r},\mathcal{E}}$ from (31). In that case, using an equivalent derivation as in (57) and (58), we obtain

$$N_{\mathrm{c},\mathcal{E}} \approx \frac{(\pi\psi^2)^K}{K!\,(\frac{\sqrt{3}}{2})^K \mathrm{vol}^2(\boldsymbol{\Lambda}(\boldsymbol{G}))}\;, \tag{85}$$

i.e., the number of candidates is increased in comparison to a search for lattices over Gaussian integers. This is quite obvious as the Eisenstein integers constitute a denser packing—within the same hypervolume, more points are located. However, please note that the initial RLLL reduction is then performed with $\boldsymbol{G}_{\mathsf{r},\mathcal{E}}$. Thereby, lower search radii may be obtained, counteracting the increase in list size.

If quaternion-valued lattices over $\mathcal{L}$ are present, the approximated list size reads

$$N_{\mathrm{c},\mathcal{L}} \approx \frac{(\pi\psi^2)^{2K}}{(2K)!\,\mathrm{vol}(\boldsymbol{\Lambda}(\boldsymbol{G}_{\mathsf{r}}))} = \frac{(\pi\psi^2)^{2K}}{(2K)!\,\mathrm{vol}^4(\boldsymbol{\Lambda}(\boldsymbol{G}))}\;. \tag{86}$$

For lattices over Hurwitz integers, (59) and the derivation in (60) can be used to form the adapted list size

$$N_{\mathrm{c},\mathcal{H}} \approx \frac{(\pi\psi^2)^{2K}}{(2K)!\,(\frac{1}{2})^K \mathrm{vol}^4(\boldsymbol{\Lambda}(\boldsymbol{G}))}\;. \tag{87}$$

Again, the estimated number of candidates is increased since the Hurwitz integers are more densely packed than the Lipschitz integers (doubled number of points). However, the initial search radius obtained by RLLL reduction of $\boldsymbol{G}_{\mathsf{r},\mathcal{H}}$ reduction may be different (lowered) again.

2) Complexity of LLL Reduction: The computational complexities of the different LLL approaches are finally assessed and compared to each other. The complexity is assessed w.r.t. the number of *real-valued multiplications* since, in hardware implementation, multiplications are usually much more costly than additions. To this end, please note that for the straightforward multiplication of complex numbers according to (2), four real-valued multiplications are required. For the quaternion-valued multiplication as defined in (6), 16 real-valued multiplications are necessary. If not stated otherwise, we restrict to these naive implementations. Hence, for the moment, we denote the number of real-valued multiplications by N_{r}, i.e., we have $N_{\mathsf{r},\mathbb{Z}} = 1$ for real-valued, $N_{\mathsf{r},\mathcal{G}} = 4$ or $N_{\mathsf{r},\mathcal{E}} = 4$ for complex-valued, and $N_{\mathsf{r},\mathcal{H}} = 16$ for quaternion-valued arithmetic.

It has been shown in the literature that an upper bound on the number of iterations in the LLL algorithm, i.e., on the number of runs of the code lines within the while-loop in Algorithm 3, can be given [53], [63]. To this end, the elements of the generator matrix have to be assumed to be drawn from a real-valued unit-variance uniform [53] or Gaussian [63] distribution. Then, the asymptotic number of iterations reads $\mathcal{O}(K \log_{\frac{1}{\delta}}(K))$, where the base of the logarithm is the inverse of the quality parameter δ. It has been derived in [63] that the same behavior holds for the complex case if a circular-symmetric unit-variance Gaussian distribution is present. Adapting the derivation in [63] to the quaternion-valued case, it can straightforwardly been shown that a circular-symmetric unit-variance quaternion-valued Gaussian distribution leads to the same result.

It is well-known that the complexity inside the while loop of the LLL algorithm—assuming an efficient implementation of the Gram-Schmidt update—is dominated by the for-loop for size reduction (Line 11–13 in Algorithm 3), which has an asymptotic complexity of $\mathcal{O}(NK)$, cf., e.g., [23]. Hence, in total,[9] this leads to the famous result that the LLL reduction as implemented in Algorithm 3 has the asymptotic complexity

$$\mathcal{O}(K^3 N \log_{\frac{1}{\delta}}(K)) \ . \tag{88}$$

Noteworthy, this complexity analysis holds for all types of LLL reduction described in this work—under the assumption that the operations are performed in the particular real-, complex-, or quaternion-valued arithmetic.

Given complex or quaternionic lattices, a complexity comparison of different LLL reduction strategies w.r.t the number of totally required *real-valued* multiplications, denoted as M_{r}, is of interest. In [23], such a comparison was given for complex matrices and CLLL versus RLLL reduction. This comparison is briefly reviewed and extended to all integer rings considered previously.

The ratio between the number of real-valued multiplications in the CLLL algorithm and the respective number in the RLLL one using the equivalent $2N \times 2K$ representation of the generator matrix can be expressed as

$$\begin{aligned} \frac{M_{\mathrm{r},\mathcal{G}}}{M_{\mathrm{r},\mathbb{Z}}} &= N_{\mathsf{r},\mathcal{G}} \cdot \frac{K^3 N \log_{\frac{1}{\delta}}(K)}{(2K)^3 2N \log_{\frac{1}{\delta}}(2K)} \cdot \xi_{\mathcal{G},\mathbb{Z}} \\ &= 4 \cdot \frac{\log_{\frac{1}{\delta}}(K)}{16 \, \log_{\frac{1}{\delta}}(2K)} \cdot 2 \approx \frac{1}{2} \ . \end{aligned} \tag{89}$$

[9] The initial GSO (with pivoting) according to Algorithm 1 is not relevant in the analysis of the asymptotic behavior of the LLL algorithm as it only has a complexity of $\mathcal{O}(NK)$ required once in the beginning. Besides, even if a naive update of the GSO is performed within the while-loop, the total asymptotic complexity of one iteration still reads $\mathcal{O}(NK)$.

The middle part represents the particular asymptotic complexity according to (88). In addition, it has to be taken into account that the size reduction only has to be performed if $\mathrm{Q}_{\mathbb{I}}\{r_{l,k}\} \neq 0$, cf. Algorithm 2. To describe the ratio between the probabilities that the reduction is required, the variable

$$\xi_{\mathcal{G},\mathbb{Z}} = \frac{\Pr\{\mathrm{Q}_{\mathcal{G}}\{r_{l,k}\} \neq 0\}}{\Pr\{\mathrm{Q}_{\mathbb{Z}}\{r_{l,k}\} \neq 0\}} \tag{90}$$

is used. In the real-valued case, the size reduction is necessary if $|r_{l,k}| > \frac{1}{2}$. Thereby, in the equivalent real-valued $2N \times 2K$ representation, the particular value $r_{k,l}$ describes either a real part or an imaginary part of the complex-valued matrix. In the original $N \times K$ complex-valued representation, size reduction for $r_{k,l} = r_{k,l}^{(1)} + r_{k,l}^{(2)}$ is required if $|r_{l,k}^{(1)}| > \frac{1}{2} \cup |r_{l,k}^{(2)}| > \frac{1}{2}$, i.e., if it is located within a square over the complex plane. Both components are statistically independent due to the above-mentioned radial-symmetrical stochastic model. Since, as stated in [64], the real value $|r_{l,k}|$ and the complex-valued components $|r_{l,k}^{(1)}|$ and $|r_{l,k}^{(2)}|$ have quite similar statistics, $\Pr\{\mathrm{Q}_{\mathcal{G}}\{r_{l,k}\} \neq 0\} \approx 2\Pr\{\mathrm{Q}_{\mathbb{Z}}\{r_{l,k}\} \neq 0\}$. Since

$$\lim_{K\to\infty} \frac{\log_{\frac{1}{\delta}}(K)}{\log_{\frac{1}{\delta}}(2K)} = 1 \ , \tag{91}$$

the approximation in (89) reveals that the number of required real-valued multiplications is halved when the CLLL instead of the RLLL is used.

Considering ELLL reduction for complex-valued matrices, one significant difference to CLLL reduction can be observed: in the size-reduction step, the quantization is not performed w.r.t. a square Voronoi cell but a hexagonal one is present instead. A Voronoi cell of the hexagonal lattice covers less space ($\mathrm{vol}(\mathcal{E}) = \mathrm{vol}(\boldsymbol{A}_2) = \frac{\sqrt{3}}{2}$, cf. (57)) than the one of the two-dimensional integer lattice ($\mathrm{vol}(\mathcal{G}) = \mathrm{vol}(\mathbb{Z}^2) = 1$). However, the hexagonal cell is more similar to a two-dimensional hypersphere, i.e., a circle, than the square one. Hence, it covers a circular-symmetric (Gaussian) distribution more precisely. It can be expected that both effects roughly compensate each other. Thus, $\xi_{\mathcal{E},\mathcal{G}} \approx 1$ can be assumed, and we obtain the asymptotic complexity estimations $\frac{M_{\mathrm{r},\mathcal{E}}}{M_{\mathrm{r},\mathcal{G}}} \approx 1$, and $\frac{M_{\mathrm{r},\mathcal{E}}}{M_{\mathrm{r},\mathbb{Z}}} \approx \frac{1}{2}$.

When comparing the computational complexity of the QLLL algorithm to the particular complexities of the CLLL and the RLLL algorithm for quaternion-valued lattices, we can use the same strategy as in (89). In particular, four statistically independent components $r_{l,k}^{(1)}$, $r_{l,k}^{(2)}$, $r_{l,k}^{(3)}$, and $r_{l,k}^{(4)}$ can be assumed. However, here it has to be taken into account that the Voronoi cell of $\mathcal{H}$ forms a 24-cell as mentioned in Sec. II, which covers less volume ($\mathrm{vol}(\mathcal{H}) = \frac{1}{2}$, cf. (59)) than a four-dimensional hypercube ($\mathrm{vol}(\mathcal{L}) = \mathrm{vol}(\mathbb{Z}^4) = 1$). Hence, by analogy with the Eisenstein integers, we can assume that $\xi_{\mathcal{H},\mathcal{L}} \approx 1$ and, as a consequence, that $\xi_{\mathcal{H},\mathcal{G}} \approx 2$ and $\xi_{\mathcal{H},\mathbb{Z}} \approx 4$. On that basis, the complexity ratio with respect to RLLL reduction can be estimated as

$$\begin{aligned} \frac{M_{\mathrm{r},\mathcal{H}}}{M_{\mathrm{r},\mathbb{Z}}} &= N_{\mathsf{r}} \cdot \frac{K^3 N \log_{\frac{1}{\delta}}(K)}{(4K)^3 4N \log_{\frac{1}{\delta}}(4K)} \cdot \xi_{\mathcal{H},\mathbb{Z}} \\ &= 16 \cdot \frac{\log_{\frac{1}{\delta}}(K)}{256 \, \log_{\frac{1}{\delta}}(4K)} \cdot 4 \cdot \approx \frac{1}{4} \end{aligned} \tag{92}$$

i.e., using the QLLL reduction, the complexity can be reduced to roughly one fourth. If the complexity of the QLLL algorithm is compared to the one of the CLLL one,

$$\begin{aligned} \frac{M_{\mathrm{r},\mathcal{H}}}{M_{\mathrm{r},\mathcal{G}}} &= \frac{N_{\mathsf{r},\mathcal{H}}}{N_{\mathsf{r},\mathcal{G}}} \cdot \frac{K^3 N \log_{\frac{1}{\delta}}(K)}{(2K)^3 2N \log_{\frac{1}{\delta}}(2K)} \cdot \xi_{\mathcal{H},\mathcal{G}} \\ &= 4 \cdot \frac{\log_{\frac{1}{\delta}}(K)}{16 \, \log_{\frac{1}{\delta}}(2K)} \cdot 2 \cdot \approx \frac{1}{2} \end{aligned} \tag{93}$$

is obtained. Hence, about one half of the multiplications can be saved. For the comparison between QLLL and ELLL, $\xi_{\mathcal{H},\mathcal{E}} \approx 2$ can be assumed. Consequently, $\frac{M_{\mathrm{r},\mathcal{H}}}{M_{\mathrm{r},\mathcal{E}}} \approx \frac{1}{2}$ is obtained accordingly.

Finally, we briefly consider the complexity ratios for the case when "advanced" multiplication schemes are applied. As mentioned in Sec. II, a complex-valued multiplication can be implemented by only $N_{\mathsf{r}} = 3$ real-valued multiplications, and a quaternion-valued multiplication by only $N_{\mathsf{r}} = 8$ ones. Hence, for complex- versus real-valued processing, the ratios $\frac{M_{\mathsf{r},\mathcal{G}}}{M_{\mathsf{r},\mathbb{Z}}} \approx \frac{M_{\mathsf{r},\mathcal{E}}}{M_{\mathsf{r},\mathbb{Z}}} \approx \frac{3}{8}$ are obtained. For quaternion-valued versus complex-valued processing, the complexity ratios are given as $\frac{M_{\mathsf{r},\mathcal{H}}}{M_{\mathsf{r},\mathcal{G}}} \approx \frac{M_{\mathsf{r},\mathcal{H}}}{M_{\mathsf{r},\mathcal{E}}} \approx \frac{1}{3}$, and for quaternion-valued versus real-valued processing, the number of required multiplications is reduced to $\frac{M_{\mathsf{r},\mathcal{H}}}{M_{\mathsf{r},\mathbb{Z}}} \approx \frac{1}{8}$. Please note that these decreased numbers of multiplications are accompanied by increased numbers of required additions. Hence, the best-performing strategy largely depends on the particular hardware architecture.

D. Numerical Evaluation and Comparison

To complement the theoretical derivations provided in this section, numerical simulations have been performed. In particular, for both the complex and the quaternion-valued case, 10^6 i.i.d. unit-variance complex or quaternionic Gaussian random matrices have been considered. Since we are interested in upper bounds on the quality and complexity, the assessment is performed by evaluating the 0.99-quantiles of the particular quantities, i.e., the values which are surpassed by exactly $1\ \%$ of the observed realizations. Again, for LLL reduction, the optimal quality parameter $\delta = 1$ is assumed.

1) Norms of the Vectors: In Fig. 5, the 0.99-quantiles of the normalized norms are illustrated, cf. Fig. 3 (Top: complex matrices, Bottom: quaternionic matrices). In addition to the norms of the first vectors, their maximum values are shown. The maximum among the vector norms, which can only be evaluated numerically (see above), is the relevant quantity for the SBP (35) and the SIVP (45).

Restricting the considerations to the norms of the first vectors in Fig. 5, the conclusions follow the ones that were drawn for the theoretical upper bounds in Fig. 3: Lattices over $\mathcal{E}$ and $\mathcal{H}$ possess lower first successive minima than lattices over $\mathcal{G}$ and $\mathcal{L}$, respectively. The LLL reductions over $\mathcal{E}$ and $\mathcal{H}$ show the best quality; their respective quantiles may even fall below the ones of the successive minima over $\mathcal{G}$ and $\mathcal{L}$ for small dimensions. Among the "genuine" LLL approaches, the reduction over $\mathcal{G}$ performs the worst. In the quaternion-valued case, only the curve for pseudo-QLLL reduction (over $\mathcal{L}$) possesses higher quantiles. However, for statistical models like the i.i.d. Gaussian one at hand, its application still results in a reasonable performance, though alternative approaches may be more appropriate if the first vector is relevant.

For the maximum of the vector norms in Fig. 5, similar conclusions can be drawn—except for two important observations: First, in contrast to the first vector and similar to the theoretical bounds on the orthogonality defect in Fig. 4, the CLLL reduction performs better than the RLLL reduction. Second, in the quaternion-valued case, the pseudo-QLLL reduction even possesses lower quantiles than the CLLL or RLLL reduction. Hence, concerning an approximate solution for the SBP and the SIVP, respectively, the application of the pseudo-QLLL reduction over $\mathcal{L}$ may even be beneficial in practice, if and only if the "genuine" QLLL reduction over $\mathcal{H}$ is not desired.

2) Orthogonality Defect: In Fig. 6, the 0.99-quantile of the orthogonality defect is plotted as the statistical quantity. Again, the complex case is shown at the top; the quaternionic case at the bottom.

The shapes of the curves correspond to the behavior that can be expected when the theoretical bounds from Fig. 4 are regarded. For the complex case, the orthogonality defect of the matrix formed by the shortest independent vectors over $\mathcal{E}$ is the lowest one, whereas the application of the RLLL algorithm results in the worst quality.

For quaternion-valued lattices, the successive minima over $\mathcal{H}$ as well as the related LLL re-

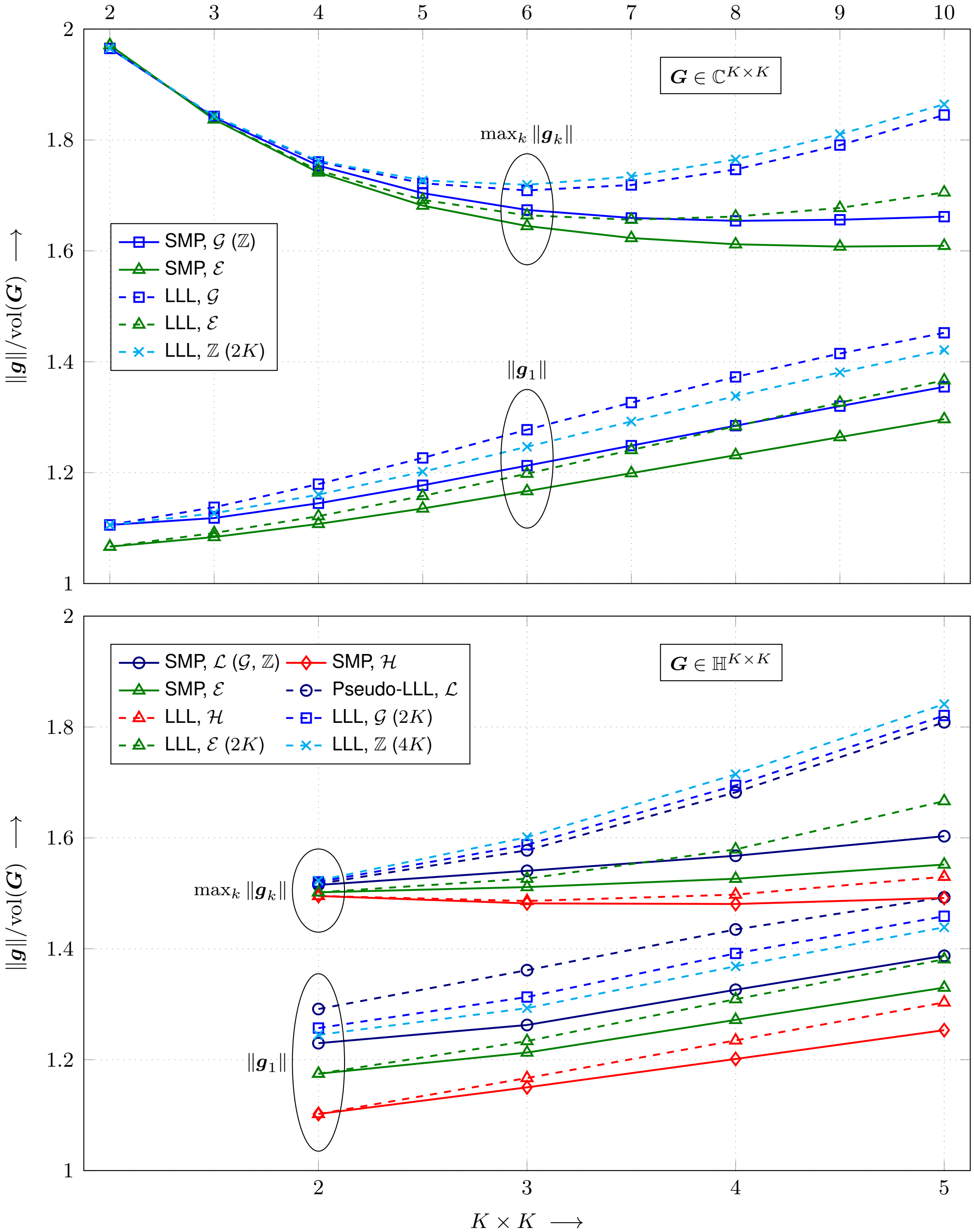


Fig. 5. 0.99-quantiles for the normalized first successive minimum (solid lines) and the normalized first basis vector of an LLL-reduced basis with parameter $\delta = 1$ (dashed lines) as well as the related maximum values among all vectors over the dimensions $K \times K$ obtained from numerical simulations. Top: complex-valued lattices. Bottom: quaternion-valued lattices.

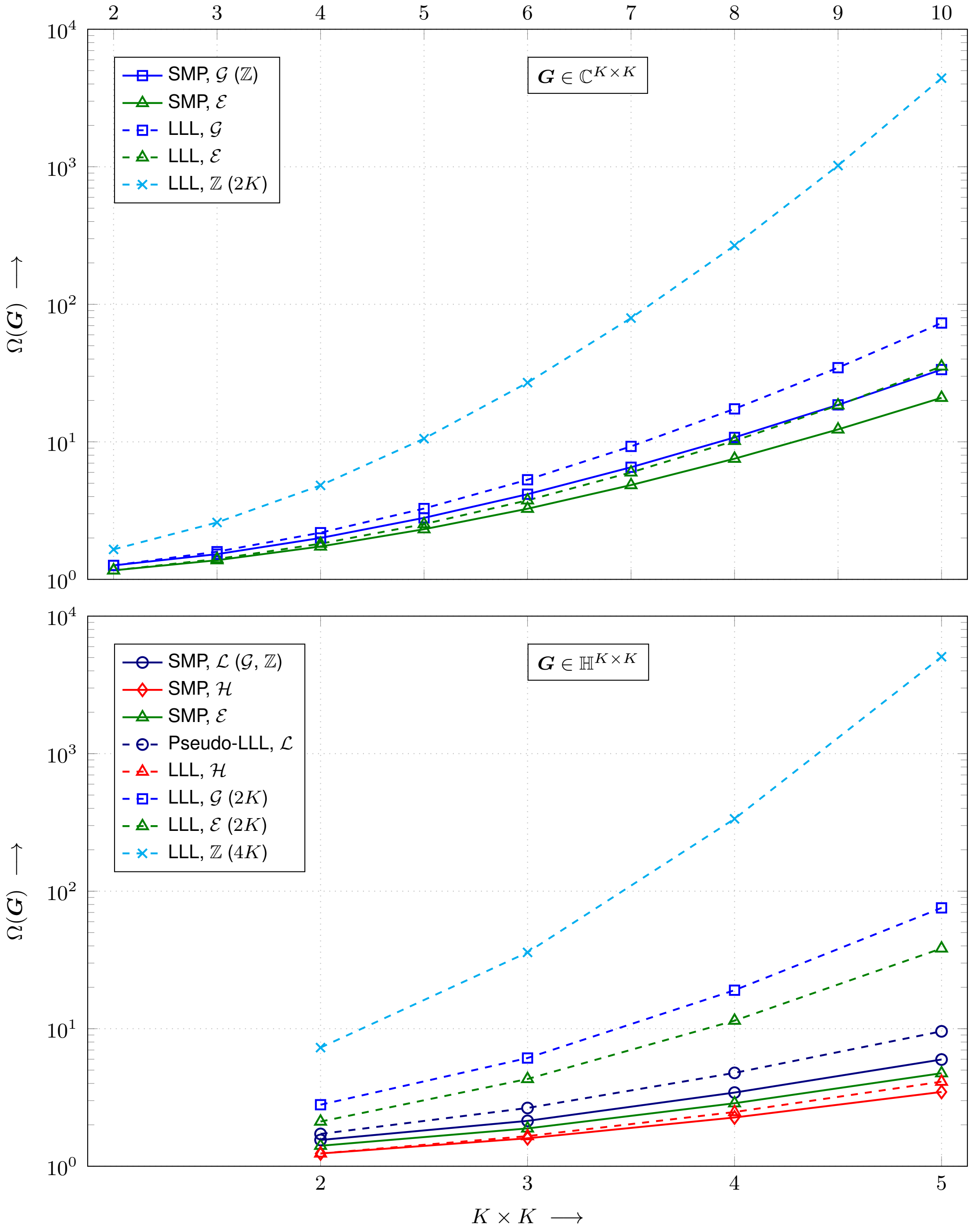


Fig. 6. 0.99-quantiles for the orthogonality defect of the matrix formed by the shortest independent vectors of the lattice (solid lines) as well as the related basis vectors of an LLL-reduced basis with parameter $\delta = 1$ (dashed lines) over the dimensions $K \times K$ obtained from numerical simulations. Top: complex-valued lattices. Bottom: quaternion-valued lattices.

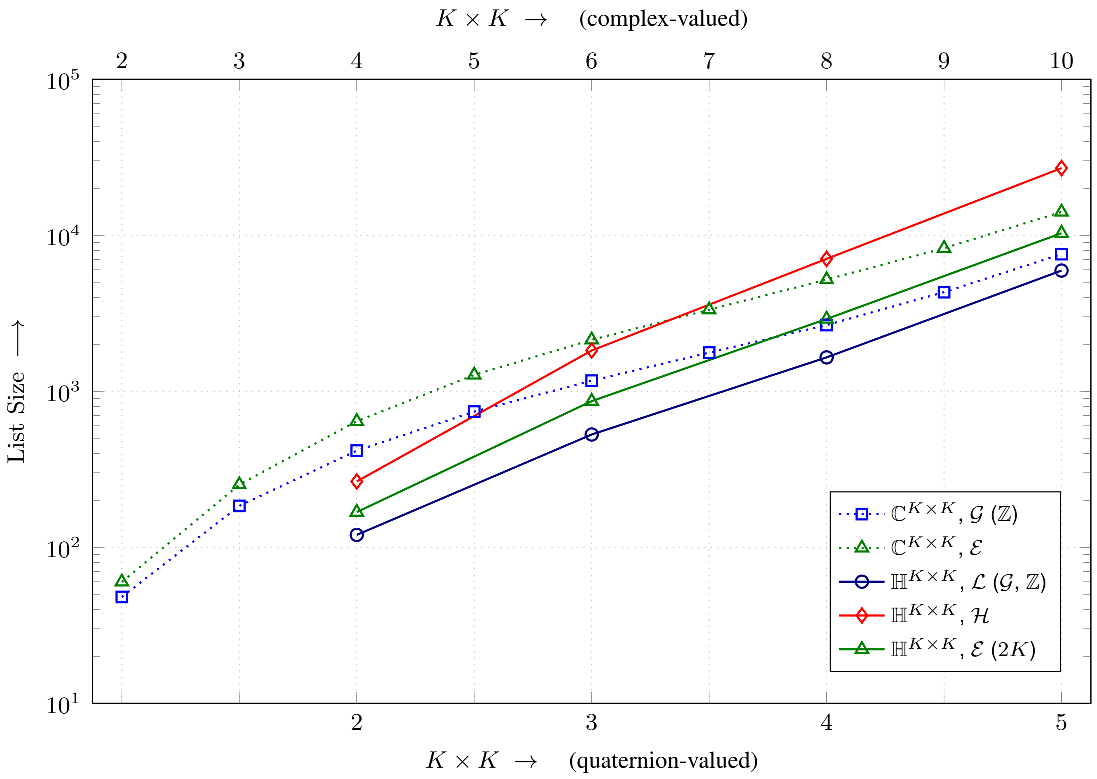


Fig. 7. 0.99-quantiles of the list sizes for the determination of the successive minima according to Algorithm 5 over different integer rings $\mathbb{I}$ obtained by numerical simulations. Dashed curves: complex-valued lattices with generator matrix $\boldsymbol{G} \in \mathbb{C}^{K\times K}$. Solid curves: quaternion-valued lattices with generator matrix $\boldsymbol{G} \in \mathbb{H}^{K\times K}$.

duction are accompanied by the lowest orthogonality defects. Again, the classical LLL reduction over $\mathbb{Z}$ shows the worst quality. Surprisingly, at least w.r.t. the orthogonality defect, the pseudo-QLLL reduction over $\mathcal{L}$ results in quite a good performance. In particular, the orthogonality defect falls significantly below the one of any equivalent complex or real-valued strategy.

3) List Sizes of the Successive-Minima Algorithm: Fig. 7 depicts the 0.99-quantiles of the list sizes for the list-based determination of the successive minima of a lattice as described in Sec. III-B. Both the complex-valued ($\boldsymbol{G} \in \mathbb{C}^{K\times K}$) and the quaternion-valued case ($\boldsymbol{G} \in \mathbb{H}^{K\times K}$) are considered.

With regard to complex lattices, the determination of the successive minima over $\mathcal{E}$ is accompanied by a slightly increased list size in comparison to $\mathcal{G}$. As explained in Sec. IV-C1, this increase in complexity is caused by an increased number of lattice points within a given search radius due to the denser packing. Obviously, even though the initial search radius obtained by *real-valued* LLL reduction may be lowered a little bit for lattices over Eisenstein integers, the denser packing seems to be the more dominating point.

The same holds for the quaternion-valued case: here, lattices over $\mathcal{L}$ result in the lowest quantiles for the list size, whereas lattices over $\mathcal{H}$ are—due to the densest packing in four dimensions—accompanied by the largest quantities. If the successive minima w.r.t. $\mathcal{E}$ are calculated for the equivalent complex-valued representation, the list size is located in between the one of $\mathbb{I} = \mathcal{L}$ and $\mathbb{I} = \mathcal{H}$, as the packing is denser than the one of $\mathcal{G}^2$, but sparser than the one of $\mathcal{H}$.

4) Multiplications within the LLL Algorithm: Finally, we assess the 0.99-quantiles of the numbers of real-valued multiplications M_r that are required to run the (generalized) LLL reduction as defined in Algorithm 3. To this end, the numbers are shown in Fig. 8 (Top: complex lattices, Bottom: quaternionic lattices). Both the standard multiplication approaches (2) and (6), respectively, with $N_\text{r} = 4$ and $N_\text{r} = 16$ real-valued multiplications (solid lines), and the reduced-complexity variants with $N_\text{r} = 3$ and $N_\text{r} = 8$ multiplications (dashed-dotted lines), are evaluated.

Given the complex case in Fig. 8 (Top), it is clearly visible that the CLLL and the ELLL algorithm roughly possess the same number of multiplications, which are halved in comparison to the RLLL approach if the standard multiplication strategy is applied, cf. Sec. IV-C2. If the advanced complex multiplication with $N_\text{r} = 3$ is used instead, these ratios are reduced to about $\frac{3}{8}$ like predicted by the asymptotic assessment of the complexity.

For the quaternion-valued case in Fig. 8 (Bottom), the following conclusions can be drawn: Pseudo-QLLL reduction over $\mathcal{L}$ and QLLL reduction over $\mathcal{H}$ possess about the same number of real-valued multiplications. The same is valid for the CLLL and the ELLL algorithm, using the equivalent complex-valued representation. Restricting to the standard quaternion-valued multiplication approach, the number of multiplications can roughly be halved in comparison to the CLLL and the ELLL approach, and roughly be reduced to one fourth in comparison to the RLLL approach, if the reduction is performed over $\mathcal{L}$ or $\mathcal{H}$. When using the advanced multiplication scheme for quaternionic numbers, these ratios can further be reduced to one third and one eight, respectively, as already derived in the theoretical analysis in Sec. IV-C2.

V. Application to MIMO Transmission

In this section, it is studied in which ways the the generalized algorithms derived and analyzed in the previous sections can be applied to the field of MIMO communications. To this end, the system model of complex MIMO transmission is reviewed and extended to the quaternion-

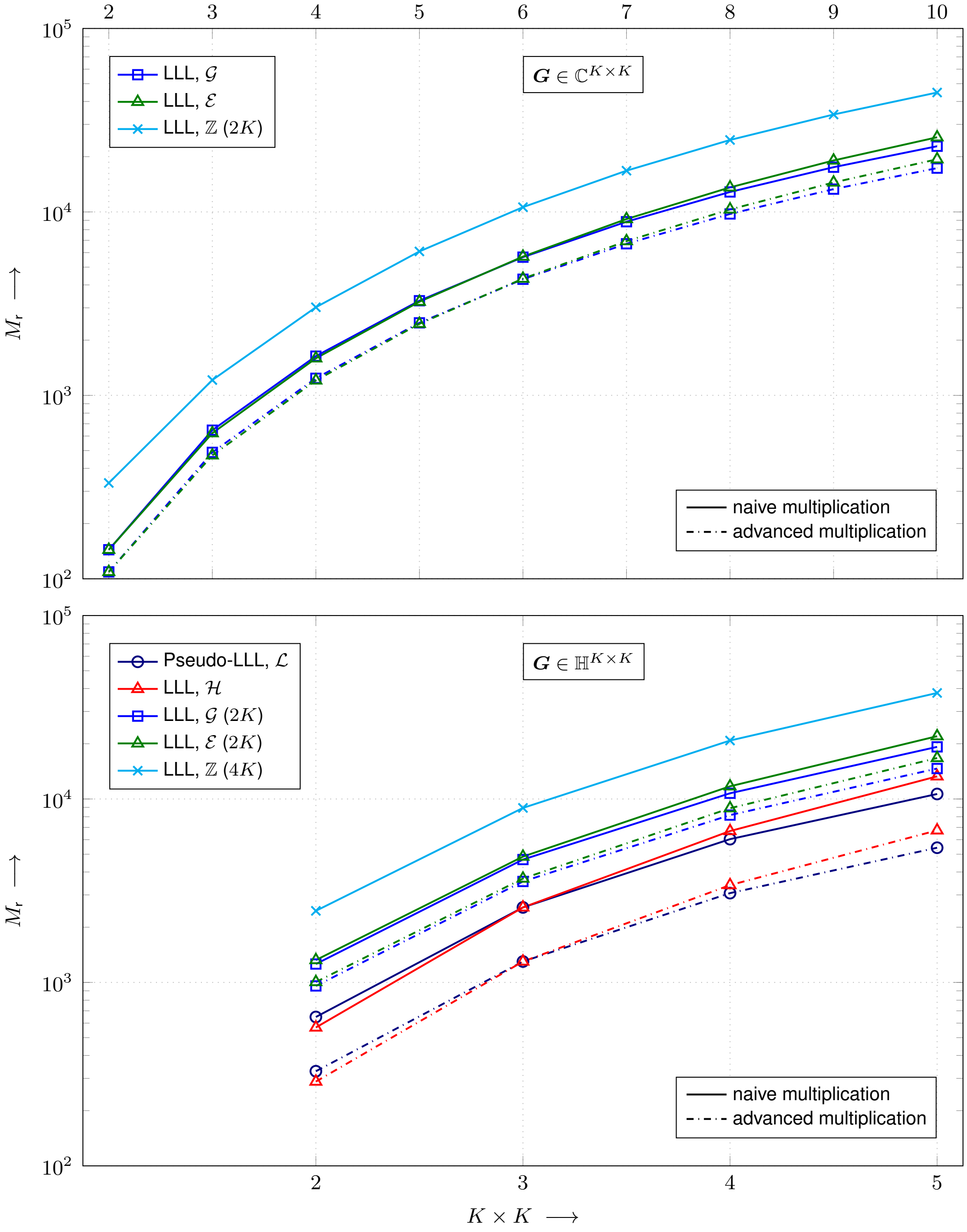


Fig. 8. 0.99-quantiles for the number of real-valued multiplications M_r within the generalized LLL reduction approach as stated in Algorithm 3 obtained by numerical simulations. Over each integer ring, the quality parameter $\delta = 1$ was used. Solid lines indicate the naive implementation of the complex or quaternion-valued multiplication operations, dashed-dotted ones ones the implementation with reduced numbers of real-valued multiplications. Top: complex-valued lattices. Bottom: quaternion-valued lattices.

valued case. Particular scenarios for the use of quaternion-valued arithmetic are identified. In addition, the concepts of lattice-reduction-aided and the closely-related integer-forcing (linear) MIMO equalization are discussed and adapted to the situation at hand.

A. SISO Fading Channel

In wireless transmission, the fading model is quite popular to represent non-line-of-sight connections. In the simplest case, only one transmit and receive antenna is used, i.e., a single-input/single-output (SISO) fading channel is present. It can be modeled by the system equation[10]

$$y = h \cdot x + n \; . \tag{94}$$

Thereby, x is a transmit symbol taken from the finite set of symbols $\mathcal{A}$ (signal constellation), h denotes the fading coefficient (multiplicative distortion), n represents Gaussian noise (additive distortion), and y is the disturbed receive symbol.

1) Complex-Valued Transmission: Most often, (94) is considered to be a complex-valued equation that models radio-frequency transmission in the equivalent complex baseband [22], [65]. Then, a (zero-mean) quadrature-amplitude modulation (QAM) constellation $\mathcal{A} \subset \mathbb{C}$ with the variance $\sigma_{x,\mathsf{c}}^2$ and the cardinality $M_\mathsf{c} = |\mathcal{A}|$ is most commonly applied. These constellations form (shifted) subsets of the Gaussian integers [19], [29]. Alternatively, constellations based on the Eisenstein integers can be employed [2], [19], [31], [33]. In accordance, the fading coefficient is complex (*Rayleigh* fading [66], usually normalized to $\sigma_{h,\mathsf{c}}^2 = 1$), and we have to deal with (radial-symmetric) complex Gaussian noise with some variance $\sigma_{n,\mathsf{c}}^2$.

Taking advantage of (3), the SISO Rayleigh fading channel can equivalently be modeled by a real-valued system with the system equation[11]

$$\begin{bmatrix} y^{(1)} \\ y^{(2)} \end{bmatrix} = \begin{bmatrix} h^{(1)} & -h^{(2)} \\ h^{(2)} & h^{(1)} \end{bmatrix} \begin{bmatrix} x^{(1)} \\ x^{(2)} \end{bmatrix} + \begin{bmatrix} n^{(1)} \\ n^{(2)} \end{bmatrix} \; , \tag{95}$$

where the noise components $n^{(1)}$ and $n^{(2)}$ have the variance $\sigma_{n,\mathsf{r}}^2 = \frac{1}{2}\sigma_{n,\mathsf{c}}^2$ and the variances of the constellation's components read $\sigma_{x,\mathsf{r}}^2 = \frac{1}{2}\sigma_{x,\mathsf{c}}^2$ if the components are independent (e.g., in QAM).

[10] In order to simplify the notation, the time index is omitted in all system equations, i.e., one particular time step (modulation step) is considered.

[11] For x and n, only the left column of the equivalent real-valued representation (3) is employed, as the right column is completely redundant and not required to obtain the final result (left column) of y.

2) Quaternion-Valued Transmission: On the basis of (94), a *quaternion-valued* SISO fading channel model can be defined. Then, the transmit symbols are consistently drawn from a quaternion-valued system constellation $\mathcal{A} \subset \mathbb{H}$ with the (4D) cardinality $M_\mathsf{q} = |\mathcal{A}|$. The signal points can, e.g., be chosen as a subset of the Lipschitz or the Hurwitz integers [1], [67]. The related variance reads $\sigma^2_{x,\mathsf{q}}$. The fading coefficient is given as

$$h = (\underbrace{h^{(1)} + h^{(2)}\,\mathrm{i}}_{h^{\{1\}}}) + (\underbrace{h^{(3)} + h^{(4)}\,\mathrm{i}}_{h^{\{2\}}})\,\mathrm{j}\,, \tag{96}$$

i.e., it consists of *four independent real-valued* or *two independent complex-valued* ones, respectively. Since two independent unit-variance Rayleigh-fading coefficients are present, the variance reads $\sigma^2_{h,\mathsf{q}} = 2\,\sigma^2_{h,\mathsf{c}} = 4\,\sigma^2_{h,\mathsf{r}} = 2$. In the same way, the noise is represented by

$$n = (\underbrace{n^{(1)} + n^{(2)}\,\mathrm{i}}_{n^{\{1\}}}) + (\underbrace{n^{(3)} + n^{(4)}\,\mathrm{i}}_{n^{\{2\}}})\,\mathrm{j}\,, \tag{97}$$

where $\sigma^2_{n,\mathsf{q}} = 2\,\sigma^2_{n,\mathsf{c}} = 4\,\sigma^2_{n,\mathsf{r}}$. A disturbed receive symbol $y \in \mathbb{H}$ is finally obtained.

Benefiting from (7), the quaternion-valued SISO fading channel is equivalently expressed by the complex-valued 2×2 system equation

$$\begin{bmatrix} y^{\{1\}} \\ (y^{\{2\}})^* \end{bmatrix} = \begin{bmatrix} h^{\{1\}} & -h^{\{2\}} \\ (h^{\{2\}})^* & (h^{\{1\}})^* \end{bmatrix} \begin{bmatrix} x^{\{1\}} \\ (x^{\{2\}})^* \end{bmatrix} + \begin{bmatrix} n^{\{1\}} \\ (n^{\{2\}})^* \end{bmatrix} \,. \tag{98}$$

This complex 2×2 system equation and its quaternion-valued (scalar) representation, respectively, are well-suited to model particular transmission scenarios:

1) Transmission with *dual-polarized antennas*: as illustrated in Fig. 9, (98) models the (SISO) transmission with one dual-polarized antenna at both the transmitter and the receiver side. In particular, both horizontal and vertical polarization of the electromagnetic wave are then used for the orthogonal transmission of *two* complex-valued symbols at the same time and on the same frequency band. Thereby, the first complex fading factor $h^{\{1\}}$ describes the *direct gain* within the same polarization plane, whereas $h^{\{2\}}$ represents the *cross-polar gain*, i.e., the crosstalk to the other polarization plane. Moreover, the noise samples $n^{\{1\}}$ and $n^{\{2\}}$ describe the additive noise which is present at the vertically and horizontally polarized receive antenna, respectively. Further details can be found in [1], [40], [41].
2) Transmission with Alamouti (space-time) coding: the system equation (98) directly corresponds to the one of the Alamouti (space-time) coding scheme as a diversity technique [38]. Then, the complex symbols $x^{\{1\}}$ and $x^{\{2\}}$ may actually be radiated at different time

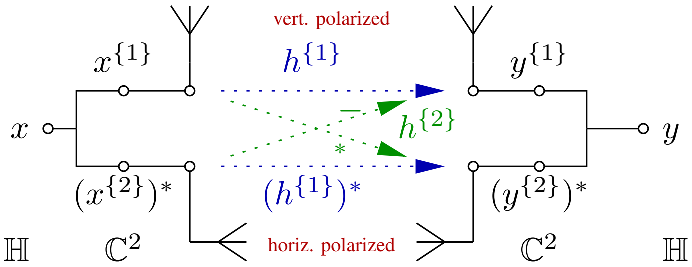


Fig. 9. Transmission with dual-polarized antennas over the SISO fading channel according to (98). At the transmitter and receiver, antenna pairs are present that transmit and receive electromagnetic waves which carry information in both the vertical polarization plane (top) and the horizontal polarization plane (bottom). In the quaternion-valued fading factor $h = h^{\{1\}} + h^{\{2\}}\mathrm{j}$, both the direct gain $h^{\{1\}}$and the cross-polar gain $h^{\{2\}}$ are contained.

steps (or, e.g., frequencies), but are processed jointly. Diversity is obtained if the channel gains $h^{\{1\}}$ and $h^{\{2\}}$ (representing the two time steps, frequencies, ...) differ from each other. The quaternion-valued SISO fading model can be seen as an alternative (scalar) representation of the 2×2 space-time coding scheme. For further details and a deeper comparison of dual-polarized transmission and Alamouti coding, see [68].

B. MIMO Fading Channel (Uplink Transmission)

The complex- or quaternion-valued SISO fading models can be generalized to respective MIMO ones. In this work, *MIMO uplink transmission*—aka *MIMO multiple-access channel*—is treated in an exemplary way.

K uncoordinated single-antenna user devices transmit their data—at the same time and on the same frequency—to *one* central receiver which is equipped with $N \geq K$ antennas. The related system equation is given as

$$\boldsymbol{y} = \boldsymbol{H} \cdot \boldsymbol{x} + \boldsymbol{n}\ . \tag{99}$$

Here, $\boldsymbol{x} = [x_1, \ldots, x_K]^{\mathsf{T}}$ denotes the vector of transmit symbols sent by the users, $\boldsymbol{H}$ the $N \times K$ MIMO channel matrix, $\boldsymbol{n} = [n_1, \ldots, n_N]^{\mathsf{T}}$ a vector with N noise samples, and $y = [y_1, \ldots, y_N]^{\mathsf{T}}$ the vector of N symbols which are received at the central unit.

1) Complex-Valued Transmission: Most often, a complex-valued MIMO channel is considered. A popular model is that the channel matrix

$$\boldsymbol{H} = \big[\, h_{n,k} \,\big]_{\substack{n=1,\ldots,N \\ k=1,\ldots,K}} \in \mathbb{C}^{N \times K} \tag{100}$$

contains i.i.d. complex Gaussian, unit-variance channel gains $h_{n,k} \in \mathbb{C}$ that describe (in equivalent complex baseband representation) the links between the user k and the receive antenna n. At each receive antenna, complex Gaussian noise with the (same) variance $\sigma^2_{n,\mathsf{c}}$ is assumed.

Given the assumption that the transmit symbols $x_1, \dots, x_K$ are drawn from a complex-valued integer ring $\mathbb{I}$, i.e., $x_k \in \mathcal{G}$ or $x_k \in \mathcal{E}$, $k = 1, \dots, K$, and neglecting the noise, the receive symbols are drawn from (a subset of) a complex-valued lattice as defined in (26). Thereby, the generator matrix is given as $\boldsymbol{G} = \boldsymbol{H}$.

The complex-valued system equation is equivalently expressed by the real-valued equation

$$\underbrace{\begin{bmatrix} \boldsymbol{y}^{(1)} \\ \boldsymbol{y}^{(2)} \end{bmatrix}}_{\boldsymbol{y}_\mathsf{r}} = \underbrace{\begin{bmatrix} \boldsymbol{H}^{(1)} & -\boldsymbol{H}^{(2)} \\ \boldsymbol{H}^{(2)} & \boldsymbol{H}^{(1)} \end{bmatrix}}_{\boldsymbol{H}_\mathsf{r}} \underbrace{\begin{bmatrix} \boldsymbol{x}^{(1)} \\ \boldsymbol{x}^{(2)} \end{bmatrix}}_{\boldsymbol{x}_\mathsf{r}} + \underbrace{\begin{bmatrix} \boldsymbol{n}^{(1)} \\ \boldsymbol{n}^{(2)} \end{bmatrix}}_{\boldsymbol{n}_\mathsf{r}} . \tag{101}$$

Consequently, given the case that $\boldsymbol{x} \in \mathcal{G}^K$, an equivalent $2N \times 2K$ real-valued lattice (over $\mathbb{I} = \mathbb{Z}$) with the generator matrix $\boldsymbol{H}_\mathsf{r}$ is spanned, where $\boldsymbol{x}_\mathsf{r} \in \mathbb{Z}^{2K}$. Lattices over $\mathbb{I} = \mathcal{E}$ can be expressed according to (31).

2) Quaternion-Valued Transmission: It is possible to extend the complex-valued MIMO uplink model to the quaternion-valued case. Then, the channel matrix is represented as

$$\boldsymbol{H} = \begin{bmatrix} h_{n,k} \end{bmatrix}_{\substack{n=1,\dots,N \\ k=1,\dots,K}} \in \mathbb{H}^{N \times K} , \tag{102}$$

i.e., it contains i.i.d. quaternion-valued Gaussian channel gains $h_{n,k} \in \mathbb{H}$ (Gaussian distribution in each component) with the total variance $\sigma^2_{h,\mathsf{q}} = 2\,\sigma^2_{h,\mathsf{c}} = 2$, i.e., unit-variance channel gains per complex component as often considered in MIMO communications. Under the assumption that the transmit symbols $x_1, \dots, x_K$ are now chosen from a quaternion-valued integer ring $\mathbb{I}$, i.e., $x_k \in \mathcal{L}$ or $x_k \in \mathcal{H}$, $k = 1, \dots, K$, and neglecting the noise, the receive symbols form a subset of a quaternion-valued lattice according to (26) with $\boldsymbol{G} = \boldsymbol{H}$.

Given the scenario of MIMO uplink transmission via dual-polarized antennas as depicted in Fig. 10, the quaternion-valued channel gains describe the links between the *transmit-antenna pairs* k, $k = 1, \dots, K$, and the *receive-antenna pairs* n, $n = 1, \dots, N$. At each receive-antenna pair, quaternion-valued noise samples with the (total) variance $\sigma^2_{n,\mathsf{q}}$ are assumed that contain the noise of both polarization planes. When using the quaternionic model for the representation of the Alamouti coding scheme, the horizontally polarized antennas can be replaced by "virtual" antennas that represent the transmission at another time step or in another frequency band instead.

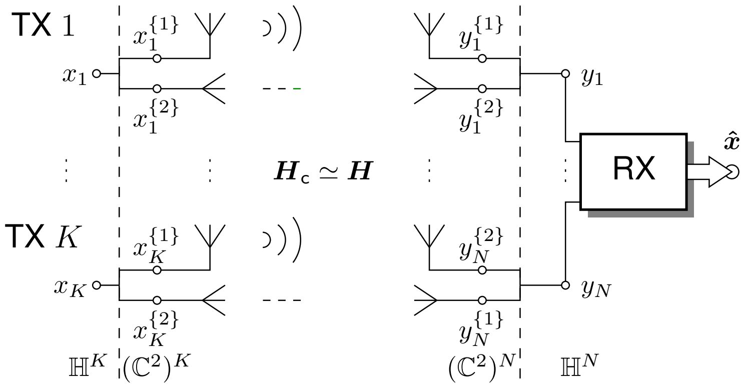


Fig. 10. Quaternion-valued MIMO uplink transmission (MIMO multiple-access channel) with dual-polarized antennas. K uncoordinated pairs of transmit antennas (in each TX, one for vertical and one for horizontal polarization) radiate the users' data symbols to the N pairs of receive antennas. The quaternion-valued receive symbols $y_1, \dots, y_K$ are processed jointly in a central receive unit (RX) in order to obtain estimates of the transmit symbols $x_1, \dots, x_K$.

As becomes apparent from Fig. 10, the quaternion-valued transmission is actually realized by the equivalent $2N \times 2K$ complex-valued system model

$$\underbrace{\begin{bmatrix} \boldsymbol{y}^{\{1\}} \\ (\boldsymbol{y}^{\{2\}})^* \end{bmatrix}}_{\boldsymbol{y}_\mathsf{c}} = \underbrace{\begin{bmatrix} \boldsymbol{H}^{\{1\}} & -\boldsymbol{H}^{\{2\}} \\ (\boldsymbol{H}^{\{2\}})^* & (\boldsymbol{H}^{\{1\}})^* \end{bmatrix}}_{\boldsymbol{H}_\mathsf{c}} \underbrace{\begin{bmatrix} \boldsymbol{x}^{\{1\}} \\ (\boldsymbol{x}^{\{2\}})^* \end{bmatrix}}_{\boldsymbol{x}_\mathsf{c}} + \underbrace{\begin{bmatrix} \boldsymbol{n}^{\{1\}} \\ (\boldsymbol{n}^{\{2\}})^* \end{bmatrix}}_{\boldsymbol{n}_\mathsf{c}} . \tag{103}$$

Hence, if $\boldsymbol{x} \in \mathcal{L}^K$, the quaternion-valued lattice $\boldsymbol{\Lambda}(\boldsymbol{H})$ is isomorphically represented by a complex lattice ($\mathbb{I} = \mathcal{G}$) with the generator matrix $\boldsymbol{G} = \boldsymbol{H}_\mathsf{c}$. In the same way, on the basis of (8), an equivalent real-valued lattice ($\mathbb{I} = \mathbb{Z}$) can be defined. A quaternion-valued transmission with symbols drawn from $\mathbb{I} = \mathcal{H}$ can be represented by equivalent lattices over $\mathbb{I} = \mathbb{Z}$ and $\mathbb{I} = \mathcal{G}$ according to (32) and (33), respectively.

C. Lattice-Reduction-Aided and Integer-Forcing Equalization

In the MIMO (uplink) scenario, handling the (multiuser) interference is a crucial point. It is well-known that (purely) linear channel equalization according to the zero-forcing (ZF) or the minimum mean-square error (MMSE) criterion does not achieve a satisfactory performance since it does not exploit the MIMO channel's (spatial) diversity, see, e.g., [12], [69].

In contrast, the concepts of *lattice-reduction-aided* (LRA) linear equalization [14], [15], [18] and the closely related integer-forcing (IF) linear equalization [21] are suited in order to achieve the receive diversity of the MIMO channel [20], see also the discussion below. In the following,

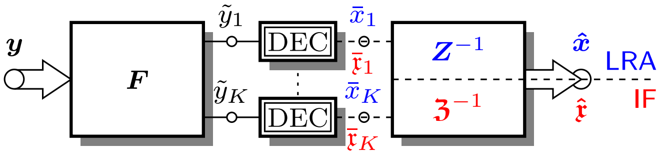


Fig. 11. Receiver structure for LRA and IF linear equalization [19]. In both concepts, the receive symbols y are linearly equalized via the filter matrix $\boldsymbol{F}$ before channel decoding is applied (DEC). Then, in the LRA receiver (blue variables), the decoder reconstructs the original linear combinations $\bar{\boldsymbol{x}} \in \mathbb{I}^K$. They are resolved via $\boldsymbol{Z}^{-1} \in \mathbb{I}^{K \times K}$ and the estimated transmit symbols $\hat{\boldsymbol{x}}$ are obtained. In the IF receiver (red variables), the decoder provides estimated finite-field symbols $\bar{\boldsymbol{\mathfrak{x}}} \in \mathbb{F}_p^K$ which are isomorphic to the signal points of the constellation $\mathcal{A} \simeq \mathbb{F}_p$. The integer interference is resolved using the inverse of the finite-field representation of the matrix $\boldsymbol{Z}$, denoted as $\boldsymbol{\mathfrak{Z}}^{-1}$. The resulting finite-field symbols $\hat{\boldsymbol{\mathfrak{x}}}$ represent the estimated symbols $\hat{\boldsymbol{x}} \in \mathcal{A}^K$.

a universal description of both the LRA and IF receiver concept is provided that enables a lattice-based channel equalization over all above-mentioned integer rings $\mathbb{I}$.

1) Generalized Concept: In both LRA and IF equalization, the transmit symbols $x_1, \ldots, x_K$ are chosen from a subset $\mathcal{A}$ of the integer ring $\mathbb{I}$. Then, as illustrated in Fig. 11, the channel matrix $\boldsymbol{H}$ is *not directly* equalized by its pseudoinverse[12] $\boldsymbol{H}^+$. Instead, a *transformed* channel $\boldsymbol{H}_{\text{tran}}$ is first handled via the $K \times N$ filter matrix $\boldsymbol{F} = \left[\boldsymbol{f}_1^{\mathsf{H}}, \ldots, \boldsymbol{f}_K^{\mathsf{H}}\right]^{\mathsf{H}}$, where the respective rows read $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_K$. Assuming the ZF criterion,[13] the filter matrix is obtained as[14] [19], [20]

$$\boldsymbol{F}^{\mathsf{H}} = \boldsymbol{H}_{\text{tran}}^{+\mathsf{H}} = \boldsymbol{H}^{+\mathsf{H}} \underbrace{\boldsymbol{Z}^{\mathsf{H}}}_{\boldsymbol{T}} , \tag{104}$$

where the transformation is expressed by the *integer matrix* $\boldsymbol{T} \in \mathbb{I}^{K \times K}$. In particular, the matrix $\boldsymbol{F}$ *shapes* the interference in such a way that only *integer interference* is left before decoding—this integer interference is particularly expressed by the integer matrix $\boldsymbol{Z} = \boldsymbol{T}^{\mathsf{H}} \in \mathbb{I}^{K \times K}$ and—in the LRA receiver structure—finally reversed via the matrix

$$\boldsymbol{Z}^{-1} = \boldsymbol{T}^{-\mathsf{H}} , \tag{105}$$

as illustrated in Fig. 11.

[12] The $K \times N$ (left) pseudoinverse of an $N \times K$ matrix $\boldsymbol{G}$ is calculated as $\boldsymbol{G}^+ = (\boldsymbol{G}^{\mathsf{H}}\boldsymbol{G})^{-1}\boldsymbol{G}^{\mathsf{H}}$. If $N = K$, $\boldsymbol{G}^+ = \boldsymbol{G}^{-1}$. The Hermitian of $\boldsymbol{G}^+$ is denoted as $\boldsymbol{G}^{+\mathsf{H}} = (\boldsymbol{G}^+)^{\mathsf{H}}$, and as $\boldsymbol{G}^{-\mathsf{H}}$ if $\boldsymbol{G}$ is a square matrix.

[13] Integer-forcing linear equalization according to the ZF criterion is usually called *exact integer forcing*, cf. [21].

[14] The lattice spanned by $\boldsymbol{G} = \boldsymbol{H}^{+\mathsf{H}}$ is the lattice which is *dual* to the one spanned by $\boldsymbol{G} = \boldsymbol{H}$, cf. [19], [25], [64].

In (104), the transformation matrix $\boldsymbol{T}$ (and, thus, $\boldsymbol{Z}$) should be chosen in a way that the row norms of $\boldsymbol{F}$ are minimized. In the presence of additive white Gaussian noise with the variance σ_n^2, they determine the *noise variances*

$$\sigma_{n,k}^2 = \|\boldsymbol{f}_k\|^2 \cdot \sigma_n^2 \ , \qquad k = 1, \ldots, K \ , \tag{106}$$

and, thus, the individual SNRs and the related mean-square errors (MSEs) before decoding. In order to minimize the MSEs, the ZF criterion applied in (104) is not the optimum strategy. They can be lowered by employing the *MMSE criterion*. To this end, the matrices in (104) can be replaced by their *augmented ones* [17], [70] according to [19], [29]

$$\boldsymbol{\mathcal{F}}^{\mathsf{H}} = \boldsymbol{\mathcal{H}}_{\mathrm{tran}}^{+\mathsf{H}} = \boldsymbol{\mathcal{H}}^{+\mathsf{H}} \underbrace{\boldsymbol{Z}^{\mathsf{H}}}_{\boldsymbol{T}} \ , \tag{107}$$

where

$$\boldsymbol{\mathcal{H}} = \begin{bmatrix} \boldsymbol{H} \\ \frac{\sigma_n}{\sigma_x} \boldsymbol{I}_K \end{bmatrix} \tag{108}$$

denotes the $(N + K) \times K$ augmented channel matrix, in which the (square root of the) *inverse SNR* is incorporated in the lower part.[15] The filter matrix $\boldsymbol{F}$ for MMSE linear equalization is then given as the $K \times N$ *left part* of the $K \times (N + K)$ *augmented filter matrix* $\boldsymbol{\mathcal{F}}$, and the noise variances in (106) are determined by the (complete) rows of $\boldsymbol{\mathcal{F}}$ instead of $\boldsymbol{F}$ [2].

In both LRA and IF equalization, the crucial performance criterion is usually the *worst-link SNR*, i.e., the lowest SNR among the K data streams *before decoding*. It dominates the error curves in case of uncoded transmission—from which the spatial *diversity order* of the MIMO system becomes apparent [12]—as well as the coded performance expressed in achievable bit rates according to Shannon [21]. Considering the worst-link SNR as the performance criterion and applying the MMSE criterion according to (107), the classical optimization problem for the integer matrix reads

$$\underbrace{\boldsymbol{Z}}_{\boldsymbol{T}^{\mathsf{H}}} = \underset{\substack{\boldsymbol{Z} \in \mathbb{I}^{K \times K} \\ \det(\boldsymbol{Z}\boldsymbol{Z}^{\mathsf{H}})=1}}{\operatorname{argmin}} \ \max_{k=1,\ldots,K} \left\{ \| \underbrace{\boldsymbol{\mathcal{H}}^{+\mathsf{H}}}_{\boldsymbol{G}} \boldsymbol{z}_k^{\mathsf{H}} \|^2 \right\} \ , \tag{109}$$

where the rows of $\boldsymbol{Z}$ correspond to the columns of its Hermitian matrix $\boldsymbol{Z}^{\mathsf{H}} = [\boldsymbol{z}_1^{\mathsf{H}}, \ldots, \boldsymbol{z}_K^{\mathsf{H}}]$. Hence, given the generator matrix $\boldsymbol{G} = \boldsymbol{\mathcal{H}}^{+\mathsf{H}}$, the unimodular integer transformation matrix

[15] Instead of using the augmented matrix $\boldsymbol{\mathcal{H}}$, often the Cholesky square root $\boldsymbol{L}^{\mathsf{H}}$ of $\boldsymbol{L}\boldsymbol{L}^{\mathsf{H}} = (\boldsymbol{H}^{\mathsf{H}}\boldsymbol{H} + \sigma_n^2/\sigma_x^2)$ is applied to calculate the MMSE variant of the channel transformation in (104). Both approaches are equivalent since $\boldsymbol{\mathcal{H}}$ is an alternative square-root of $\boldsymbol{L}\boldsymbol{L}^{\mathsf{H}}$ [2], [19].

$\boldsymbol{T} = \boldsymbol{Z}^{\mathsf{H}}$ in the lattice basis reduction according to (27) has to be solved in such a way that the maximum squared column norm of $\boldsymbol{G}_{\text{red}} = \boldsymbol{\mathcal{F}}^{\mathsf{H}}$ is minimized. This problem corresponds to the SBP as defined in (35).

In the literature on LRA equalization, (109) has been solved by lattice-basis-reduction algorithms, e.g., in [9], [15], [18], [23], most often employing the LLL algorithm due to its polynomial complexity. Consequently, a *more suited basis* for equalization according to (27) has been calculated for the particular generator matrix $\boldsymbol{G} = \boldsymbol{\mathcal{H}}^{+\mathsf{H}}$, where $\boldsymbol{T}$ describes a *unimodular* transformation. In particular, $\boldsymbol{G} = \boldsymbol{\mathcal{F}}^{\mathsf{H}}$ spans the same lattice as $\boldsymbol{G} = \boldsymbol{\mathcal{H}}^{+\mathsf{H}}$, and the lattice-basis reduction is finally inverted by the unimodular integer inverse $\boldsymbol{Z}^{-1} \in \mathbb{I}^{K \times K}$.

However, in the meantime, this unimodularity constraint could be relaxed [19], [21]: if the transformation matrix $\boldsymbol{T}$, and thus $\boldsymbol{Z}$, describes a *full-rank integer linear combination* of the transmit symbols, i.e., if the constraint $\text{rank}(\boldsymbol{T}) = K$ is imposed, $\boldsymbol{G} = \boldsymbol{\mathcal{F}}^{\mathsf{H}}$ may only define a *sublattice* of $\boldsymbol{G} = \boldsymbol{\mathcal{H}}^{+\mathsf{H}}$, cf. Sec. II-C. Hence, after linear equalization via $\boldsymbol{F}$, the vector of linear combinations of the transmit symbols, $\boldsymbol{Zx}$, may be drawn from a *subspace* of $\mathbb{I}^K$. Nevertheless, only valid lattice points are obtained. Using a suited lattice-decoding strategy, the linear combinations can still successfully be reconstructed, and the non-unimodular relaxation does not impair the equalization approach. The optimization problem is then expressed as

$$\underbrace{\boldsymbol{Z}}_{\boldsymbol{T}^{\mathsf{H}}} = \underset{\substack{\boldsymbol{Z} \in \mathbb{I}^{K \times K} \\ \text{rank}(\boldsymbol{Z}) = K}}{\text{argmin}} \; \max_{k=1,\ldots,K} \left\{ \| \underbrace{\boldsymbol{\mathcal{H}}^{+\mathsf{H}}}_{\boldsymbol{G}} \boldsymbol{z}_k^{\mathsf{H}} \|^2 \right\} , \tag{110}$$

i.e., the SIVP (45) has to be solved w.r.t. the generator matrix $\boldsymbol{G} = \boldsymbol{\mathcal{H}}^{+\mathsf{H}}$. As discussed in Sec. III, the SIVP is optimally solved by the calculation of the successive minima of the particular lattice.

2) LRA and IF Equalization: We briefly discuss and compare the (generalized) handling of the integer interference in the LRA and IF receiver concepts, cf. Fig. 11. A profound insight into the topic is provided in [19], see also [19, Fig. 3.1].

In the LRA concept (blue variables in Fig. 11), a *lattice decoder* has to be employed that reconstructs the (original) linear combinations $\boldsymbol{Zx} \in \mathbb{I}^K$. The integer interference is finally resolved over the integer ring $\mathbb{I}$; hence, the estimated transmit symbols $\hat{\boldsymbol{x}} = \boldsymbol{Z}^{-1}\text{DEC}\{\boldsymbol{Zx}\}$ are obtained. If the matrix $\boldsymbol{Z}$ is non-unimodular, its inverse $\boldsymbol{Z}^{-1}$ may contain *non-integer elements*. These elements ensure that the transformation to a subspace of $\mathbb{I}^K$ can be inverted—and that the original signal space $\mathbb{I}^K$ (or its subset $\mathcal{A}^K$) can be reconstructed.

In contrast, in the IF concept (red variables in Fig. 11), the decoder provides symbols drawn from the finite field $\mathbb{F}_p$, p prime, in which the channel coding has been performed in. To this end, a strong relation between the channel code and the signal constellation $\mathcal{A}$ is required; in particular, p-ary *algebraic signal constellations* have to be used that establish an isomorphism $\mathcal{A} \simeq \mathbb{F}_p$ to the particular finite field. The linear combinations are then actually represented via modulo-congruent points drawn from the algebraic constellation $\mathcal{A}$, or, more specifically, via their equivalent elements from $\mathbb{F}_p$. In the IF receiver, the integer interference is represented via the *finite-field integer matrix* $\mathfrak{Z} \in \mathbb{F}_p^{K \times K}$, an isomorphic representation of a modulo-reduced variant of $\boldsymbol{Z}$. Hence, an additional constraint is imposed: the finite-field inverse $\mathfrak{Z}^{-1} \in \mathbb{F}_p^{K \times K}$ only exists if $\mathfrak{Z}$ has *full rank over the finite field* $\mathbb{F}_p$. In an asymptotic manner ($|\mathcal{A}| \to \infty$), this condition is always fulfilled [21], but it may be relevant if a constellation with small cardinality is applied [2].

Algebraic signal constellations over complex numbers, particularly over the Gaussian and the Eisenstein integers, are known for quite some time [2], [24], [31], [33], [71]. For the quaternion-valued case, some initial results on algebraic Hurwitz constellations have already been given in the literature [72], [73].

D. Diversity Orders and Asymptotic Rates

The *diversity order* describes the slope of the symbol or bit error curve of *uncoded* transmission if *the average over all possible channel realizations and users* is considered. Hence, no additional (temporal/space-time) diversity/coding technique is assumed. Given the symbol error ratio (SER) over the SNR represented by σ_x^2/σ_n^2, it is defined as [12]

$$\Delta = - \lim_{\frac{\sigma_x^2}{\sigma_n^2} \to \infty} \frac{\log_{10} \mathrm{SER}(\frac{\sigma_x^2}{\sigma_n^2})}{\log_{10}(\frac{\sigma_x^2}{\sigma_n^2})} \ . \tag{111}$$

In words, in an asymptotic manner, the SER drops by Δ decades per 10 dB increase in SNR.

It has been proven in [20] that LRA equalization is suited to achieve the MIMO channel's receive diversity—which, for the complex fading channel, is simply given by the number of receive antennas N. This receive diversity is even obtained if the SBP is approximately solved by (real-valued) LLL reduction. Briefly spoken, the condition for diversity-achieving reduction is that the product of the norms of the basis vectors can be bounded with respect to the volume according to (79)—for all (generalized) variants of the LLL reduction, this can also be done as stated in Theorem 8. Since the successive minima form lower bounds on the lengths of any basis vectors, it is quite obvious that the respective integer transformation matrix achieves the maximum diversity behavior, too.

In the complex MIMO fading scenario, the (maximum) receive diversity is given as the number of receive antennas $\Delta = N$, as mentioned above. Assuming that only a real-valued channel is present, i.e., that the channel gains in (100) are purely real i.i.d. Gaussian random variables—the number of random variables is halved—hence, the MIMO receive diversity shrinks to $\Delta = N/2$, cf. [74]. If, in turn, the quaternion-valued setting with N antenna-pairs is present, the number of random variables is doubled in comparison to the complex case. Hence, it is quite evident that the diversity order is doubled to $\Delta = 2N$ [68]. This can also be seen from the point of view that the equivalent complex-valued MIMO representation (103) actually forms an Alamouti code over the polarization planes as discussed before—if the complex channel gains are independent in both planes, the diversity in the Alamouti scheme is doubled [38], see also [68]. Summarizing the above considerations, the achievable receive diversity in LRA/IF equalization can universally expressed by

$$\Delta_{\mathrm{LRA/IF}} = \frac{D}{2} N \ , \tag{112}$$

where D denotes the number of (real-valued) Gaussian random variables per channel gain—$D = 1$ for real, $D = 2$ for complex, and $D = 4$ for quaternionic transmission.

In the literature on IF equalization, e.g., [9], the *asymptotic (bit) rate* often serves as a quantity for quality assessment in *coded transmission*. It describes the (same) maximum bit rate *for each user*[16] $k = 1, \ldots, K$ and, in contrast to the diversity order, *one particular channel realization*. It is given as the Shannon capacity for the worst-link SNR, given an infinite-dimensional modulo channel [75]. In the particular setting at hand, the asymptotic bit rate can universally be expressed as

$$R = \frac{D}{2} \max_{k=1,\ldots,K} \log_2 \left(\frac{\sigma_x^2}{\|\boldsymbol{f}_k\|^2 \cdot \sigma_n^2} \right) \ , \tag{113}$$

where D denotes the number of orthogonal components of the data symbols—again, they read $D = 1$, for real $D = 2$ for complex, and $D = 4$ for quaternionic transmission.

E. Numerical Evaluation and Comparison

The performance of the generalized lattice algorithms in the MIMO uplink scenario is finally assessed by means of numerical simulations. To this end, 10^6 i.i.d. complex and quaternionic

[16] In IF equalization, all users are assumed to employ the same channel code and the same signal constellation [21]. Hence, the users also share the same (maximum) rates.

Gaussian *channel matrices* have been generated according to (100) and (102), respectively. Please note that—in contrast to the numerical evaluations in Sec. IV-D—those matrices do not directly form the generator matrices of the lattices to be considered. Instead, since we assume that the MMSE criterion is applied and that the feedforward matrix is calculated as defined in (107), the generator matrices are given by the pseudo-inverses of the respective augmented channel matrices (*MMSE dual-lattice approach*, cf. [19]). Hence, the statistical distributions may differ from the straightforward evaluation of i.i.d. Gaussian matrices. The channel equalization is performed using the LRA/IF receiver as explained in Sec. V-C. For all kinds of LLL reduction, the optimal quality parameter $\delta = 1$ is assumed once again.

1) Symbol Error Ratios in Uncoded Transmission: We start with the assessment of the different SERs which are obtained in case of uncoded transmission. These curves are not only relevant in terms of the quality of the different lattice algorithms, but are also suited the evaluate the different diversity behavior, cf. Sec. V-D. In order to simulate a block-fading environment, bursty transmissions with 10^3 symbols/noise samples per channel matrix have been performed. Due to uncoded transmission, the decoders in Fig. 11 are replaced by quantization operations w.r.t. the particular integer rings. The data symbols are finally estimated by an ML decision based on the signal constellation $\mathcal{A}$.

First, we restrict to the complex-valued case. For lattices defined over the Gaussian integers, the zero-mean 4-ary QAM constellation $\mathcal{A}_{\mathcal{G}} = \{\pm 1 \pm \mathrm{i}\} \subset \mathcal{G}$ with variance $\sigma_x^2 = 2$ has been employed. Since its components are independent, they can individually be processed using the equivalent real-valued representation according to (3), i.e., if algorithms over $\mathbb{Z}$ are considered.[17] Unfortunately, $\mathcal{A}_{\mathcal{G}} \not\subset \mathcal{E}$. Hence, for lattices over $\mathcal{E}$, the alternative zero-mean signal constellation $\mathcal{A}_{\mathcal{E}} = \{1, -1, \sqrt{3}\,\mathrm{i}, -\sqrt{3}\,\mathrm{i}\}$, with $\sigma_x^2 = 2$, has been used. Since both signal constellation possess the same variance, a fair comparison is enabled. However, please note that signal constellations defined over $\mathcal{E}$ are usually beneficial in comparison to constellations over $\mathcal{G}$, since, due their hexagonal shape, they enable a packing and a shaping gain, cf., e.g., [2], [31], [32].

In Fig. 12 (Top), the SER is plotted over the SNR for complex transmission and two scenarios with $N = K = 4$ and $N = K = 8$, respectively. First, the expected diversity orders $\Delta = 4$ and $\Delta = 8$ are clearly visible. If $N = K = 4$, all curves are still quite similar. However, in the high-

[17] Please note that, in this work, one symbol error is always defined w.r.t. the original complex (or quaternion-valued) signal constellation $\mathcal{A}$.

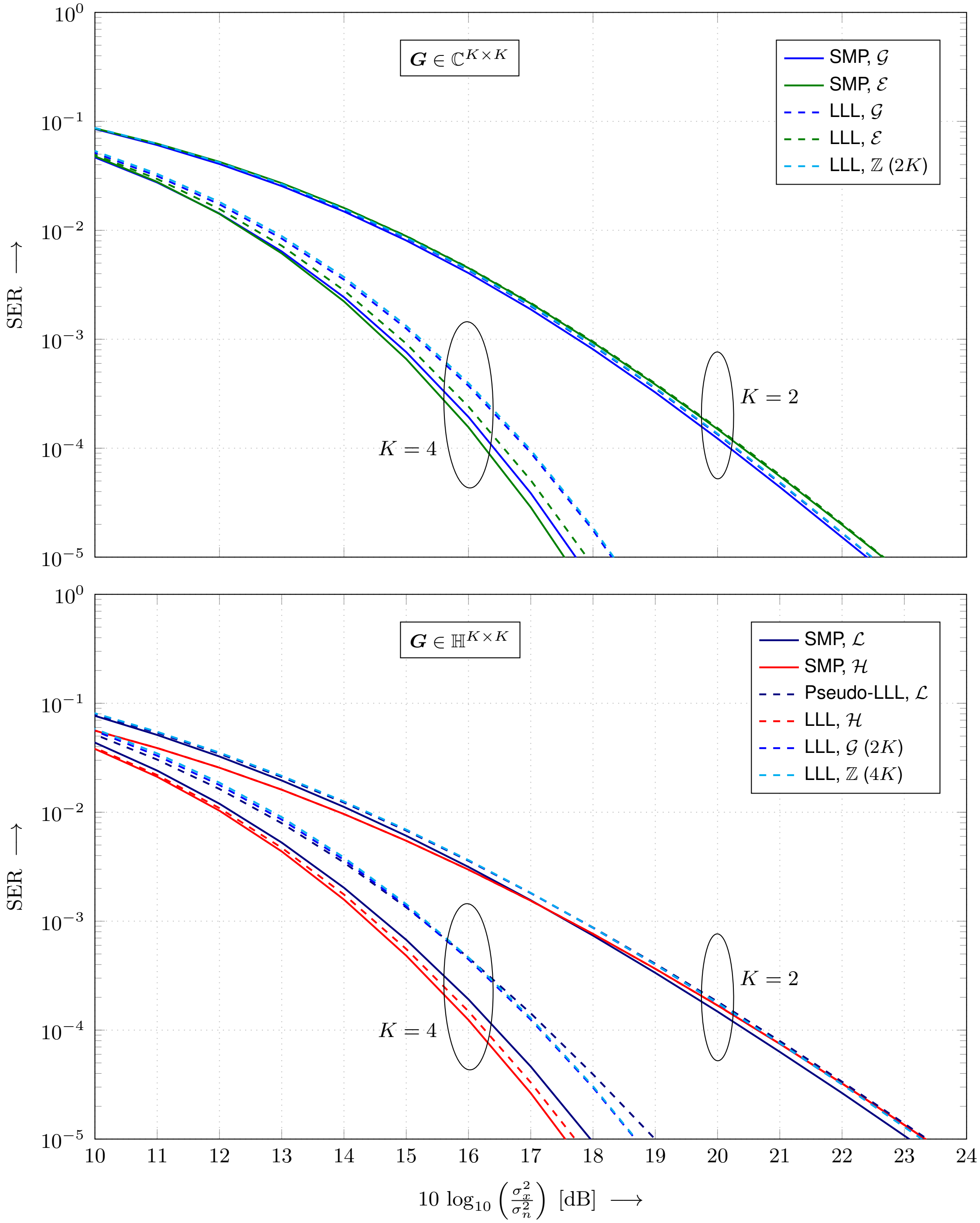


Fig. 12. Symbol error ratio over the SNR in dB for $K \times K$ uncoded MIMO uplink transmission and LRA/IF equalization (MMSE criterion) over different integer rings and algorithms obtained by numerical simulations. For LLL reduction, the optimal parameter $\delta = 1$ is assumed. Top: complex-valued transmission with the signal constellations $\mathcal{A}_{\mathcal{G}} = \{\pm 1 \pm \mathrm{i}\}$ and $\mathcal{A}_{\mathcal{E}} = \{1, -1, \sqrt{3}\,\mathrm{i}, -\sqrt{3}\,\mathrm{i}\}$. Bottom: quaternion-valued transmission with the constellation $\mathcal{A}_{\mathcal{L}} = \{\pm 1 \pm \mathrm{i} \pm \mathrm{j} \pm \mathrm{k}\}$.

SNR regime, the use of the Eisenstein lattice may even be disadvantageous. This is due to the fact that, even if the application of the particular algorithms results in the same (maximum) noise enhancement over $\mathcal{G}$ and $\mathcal{E}$, the "uncoded" decoding over $\mathcal{E}$ (i.e., the quantization, cf. Fig. 11) may result in higher error rates since this lattice is denser packed. In contrast, for $N = K = 8$, the decreased maximum noise enhancement for $\mathcal{E}$ has a positive impact such that a horizontal (SNR) gain is achieved if the ELLL algorithm is applied or if the respective successive-minima vectors are calculated.

Next, we consider the case of quaternion-valued transmission. To this end, the 16-ary constellation $\mathcal{A}_{\mathcal{L}} = \{\pm 1 \pm \mathrm{i} \pm \mathrm{j} \pm \mathrm{k}\}$ (4QAM per complex component) with $\sigma_x^2 = 4$ has been employed for which $\mathcal{A}_{\mathcal{L}} \subset \mathcal{L} \simeq \mathcal{G}^2 \simeq \mathbb{Z}^4$ as well as $\mathcal{A}_{\mathcal{L}} \subset \mathcal{H}$ are valid, since $\mathcal{L} \subset \mathcal{H}$. Hence, this constellation can be used in combination with lattices over $\mathcal{L}$, $\mathcal{H}$, $\mathcal{G}$, and $\mathbb{Z}$. The related SER curves are illustrated in Fig. 12 (Bottom) for two particular scenarios with $N = K = 2$ and $N = K = 4$. First, we see that, in accordance with (112), the diversity orders are the same as in Fig. 12 (Top), even though the dimensions K are halved. For $N = K = 2$, the curves are again quite the same. Moreover, we also have the effect that the quantization to $\mathcal{H}$ may be more erroneous than the one to $\mathcal{L}$ due to the denser packing of the lattice. In contrast, for $N = K = 4$, the Hurwitz lattice achieves a significant gain over $\mathcal{L}$, or its complex and real-valued equivalents, which perform nearly the same if applied in combination with LLL reduction. The pseudo-LLL reduction shows the worst performance. However—even though respective theoretical bounds cannot be derived—it still seems to approach the same diversity behavior in practice.

2) Bit Rates in Coded Transmission: Finally, the performance is assessed w.r.t. coded transmission, for which the rate according to (113)—depending on the particular noise enhancement (maximum squared norm) and the SNR—is the relevant quantity. In Fig. 13, both the expectations and the 0.01-quantiles of the achievable rates are illustrated, assuming $\sigma_x^2/\sigma_n^2 \mathrel{\widehat{=}} 20$ dB (MMSE criterion). In particular, the latter represent the rates for which an outage of $1\ \%$ can be expected.

In the complex-valued case (Fig. 13 (Top)), it is visible that the use of lattices over Eisenstein integers enables a slight gain w.r.t the achievable rate, which increases with the dimension. Just like in the numerical analysis of the maximum norms in Fig. 5 for i.i.d. Gaussian matrices, the RLLL algorithm performs the worst.

In quaternion-valued transmission (Fig. 13 (Bottom)), lattices over Hurwitz integers significantly enhance the achievable rates. The QLLL reduction over $\mathcal{H}$ approximates the solutions the SMP quite well. Moreover, it is quite interesting that—by analogy with the curves in Fig. 5—,

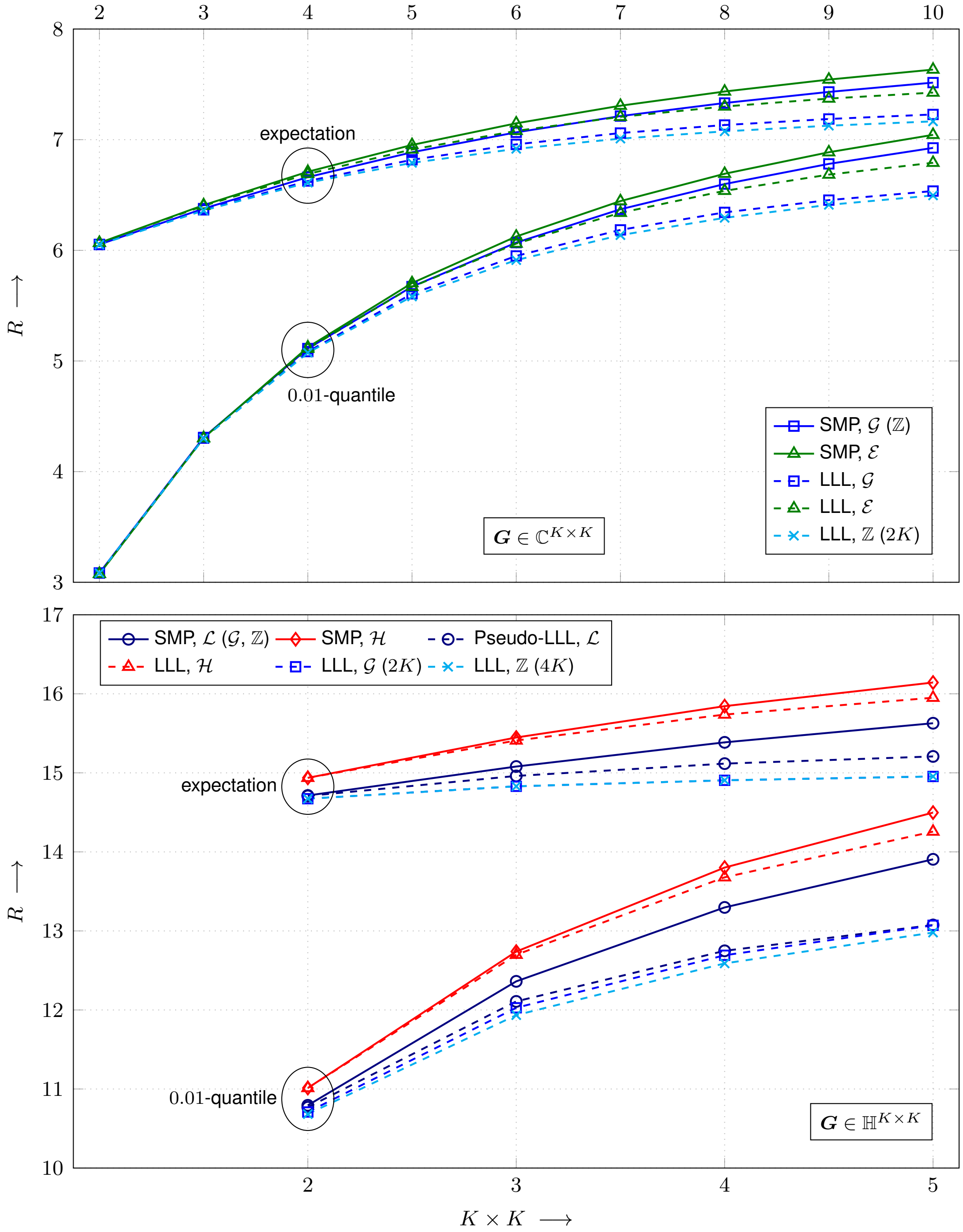


Fig. 13. Achievable rates for IF linear equalization according to (113) in coded transmission ($\sigma_x^2/\sigma_n^2 \mathrel{\widehat{=}} 20$ dB, MMSE criterion) over the $K \times K$ MIMO channel for different integer rings and algorithms obtained by numerical simulations. Both the expectations and the 0.01-quantiles are shown. Top: complex-valued transmission. Bottom: quaternion-valued transmission.

the pseudo-QLLL reduction over $\mathcal{L}$ performs substantially better than its complex or real-valued "genuine" counterparts. Hence, in practice, its usage may be taken into account—even though no theoretical performance guarantees can be given.

VI. Summary and Outlook

In this paper, algorithms and bounds known from the field of *real-valued* lattice problems have been generalized and adapted to operate over complex and quaternion-valued numbers. To this end, a review of the particular arithmetic and the properties of these number sets has been given first. Then, generalized variants of the LLL reduction and a list-based algorithm to determine the successive minima of a lattice have been given. In addition to lattices over the set of (real-valued) integers $\mathbb{Z}$, they can operate over the Gaussian (complex integers) as well as the Eisenstein integers for the complex case, and the Lipschitz as well as the Hurwitz integers for the quaternion-valued case. For all of these integers sets, bounds for the lengths of the first basis vector obtained from LLL reduction as well as for the first successive minimum have been derived. These bounds were complemented by bounds for the particular orthogonality defects, incorporating all basis or successive-minima vectors. The provided results indicate that lattices over the Eisenstein integers (instead of the Gaussian integers) may be beneficial in the complex-valued case, and that lattices over the Hurwitz integers (instead of the Lipschitz integers) may be of advantage in the quaternion-valued case. When running the presented successive-minima algorithm over these rings, the expected complexity is only increased a little bit in comparison to their counterparts. Moreover, when the LLL reduction is applied over these complex or quaternion-valued integer rings, the expected complexity is significantly decreased in comparison to an equivalent real-valued reduction. Finally, particular application scenarios have been identified. These considerations included their use in the field of MIMO communications, in particular in lattice-reduction-aided or integer-forcing equalization for the MIMO uplink channel, where equalization gains can be expected by the use of the Eisenstein integers and the Hurwitz integers, respectively.

Future work could deal with the extension to the multi-dimensional, e.g., the eight-dimensional case, in which several time steps or frequencies could be combined to one symbol. In addition, the adaption of other criteria/algorithms for lattice basis reduction, e.g., HKZ [4] or Minkowski [5] reduction, could be studied and related bounds could be derived for the complex and/or quaternion-valued case. In addition, since algebraic signal constellations are required for the use of the integer-forcing concept, the initial work on four-dimensional algebraic constellations in [72], [73] could be extended to derive algebraic constellations similar to the complex-valued ones in [2], [24], [33].

APPENDIX A
HELPER FUNCTIONS FOR LIST-BASED DETERMINATION OF THE SUCCESSIVE MINIMA

In this appendix, some procedures are listed which are incorporated in Algorithm 5 (determination of the successive minima).

Algorithm 6 Equivalent Real-Valued Representation over $\mathbb{Z}$.

```
$\boldsymbol{G}_\mathsf{r} = \textsc{RingToZ}(\boldsymbol{G})$
switch $\mathbb{I}$ do
    case $\mathbb{Z}$
        $\boldsymbol{G}_\mathsf{r} = \boldsymbol{G}$
    case $\mathcal{G}$                                                        ▷ (3)
        $\boldsymbol{G}_\mathsf{r} = \begin{bmatrix} \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(2)} \\ \boldsymbol{G}^{(2)} & \boldsymbol{G}^{(1)} \end{bmatrix}$
    case $\mathcal{E}$                                                        ▷ (31)
        $\boldsymbol{G}_\mathsf{r} = \begin{bmatrix} \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(2)} \\ \boldsymbol{G}^{(2)} & \boldsymbol{G}^{(1)} \end{bmatrix} \begin{bmatrix} \boldsymbol{I}_K & -\frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \frac{-\sqrt{3}}{2}\boldsymbol{I}_K \end{bmatrix}$
    case $\mathcal{L}$                                                        ▷ (8)
        $\boldsymbol{G}_\mathsf{r} = \begin{bmatrix} \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(2)} & -\boldsymbol{G}^{(3)} & -\boldsymbol{G}^{(4)} \\ \boldsymbol{G}^{(2)} & \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(4)} & \boldsymbol{G}^{(3)} \\ \boldsymbol{G}^{(3)} & \boldsymbol{G}^{(4)} & \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(2)} \\ \boldsymbol{G}^{(4)} & -\boldsymbol{G}^{(3)} & \boldsymbol{G}^{(2)} & \boldsymbol{G}^{(1)} \end{bmatrix}$
    case $\mathcal{H}$                                                        ▷ (32)
        $\boldsymbol{G}_\mathsf{r} = \begin{bmatrix} \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(2)} & -\boldsymbol{G}^{(3)} & -\boldsymbol{G}^{(4)} \\ \boldsymbol{G}^{(2)} & \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(4)} & \boldsymbol{G}^{(3)} \\ \boldsymbol{G}^{(3)} & \boldsymbol{G}^{(4)} & \boldsymbol{G}^{(1)} & -\boldsymbol{G}^{(2)} \\ \boldsymbol{G}^{(4)} & -\boldsymbol{G}^{(3)} & \boldsymbol{G}^{(2)} & \boldsymbol{G}^{(1)} \end{bmatrix} \cdot$
            $\begin{bmatrix} \boldsymbol{I}_K & \boldsymbol{0}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{I}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{0}_K & \boldsymbol{I}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{0}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \end{bmatrix}$
end switch
```

Algorithm 7 Transformation to Row-Echelon Form.

```
$\boldsymbol{i} = \textsc{RowEchelon}(\boldsymbol{C})$
$k = 1$, $l = 1$, $\boldsymbol{i} = [0, \ldots, 0]$
while $k \leq K$ do
    for $m = k + 1, \ldots, K$ do
        if $c_{m,l} \neq 0$ then
            $i_k = l$                                                  ▷ independent vector found
            $\tilde{\boldsymbol{c}} = \boldsymbol{C}_{k,1:N_\mathrm{c}}$                          ▷ interchange rows
            $\boldsymbol{C}_{k,1:N_\mathrm{c}} = \boldsymbol{C}_{m,1:N_\mathrm{c}}$
            $\boldsymbol{C}_{m,1:N_\mathrm{c}} = \tilde{\boldsymbol{c}}$
            $\boldsymbol{C}_{k,1:N_\mathrm{c}} = c_{k,l}^{-1} \cdot \boldsymbol{C}_{k,1:N_\mathrm{c}}$        ▷ normalize $k^{\text{th}}$ row
            for $n = k + 1, \ldots, K$ do                              ▷ eliminate successors
                $\boldsymbol{C}_{n,1:N_\mathrm{c}} = \boldsymbol{C}_{n,1:N_\mathrm{c}} - c_{n,l}\boldsymbol{C}_{k,1:N_\mathrm{c}}$
            end for
            $k = k + 1$
            break
        end if
    end for
    $l = l + 1$
end while
```

Algorithm 6 creates the equivalent real-valued representation of the generator matrix $\boldsymbol{G}$ depending on the integer ring $\mathbb{I}$. These representations have been derived in Sec. II.

In algorithm 7, the matrix of candidate vectors $\boldsymbol{C}$ is transformed to row-echelon form. To this end, for each candidate with the index l, it is checked if a new dimension is established. This is the case when one of the elements $c_{k,l}, \ldots, c_{K,l}$ is not zero; then, the vector does not depend on the previous ones. Given that case, the particular row with the non-zero element is interchanged with the row k. After normalization[18] to $c_{k,l} = 1$, all other elements $c_{k+1,l}, \ldots, c_{k+1,l}$ are set to zero by subtracting $c_{n,l}$ times the row with index k. All multiplications are performed in such a way that the skew-field property of quaternions is taken into account.

[18] Please note that linearly independent lattice vectors are required, i.e., independent vectors have to be present over $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$. Hence, when calculating the row-echelon form for the integer vectors, non-integer elements may occur. Nevertheless, these non-integer elements are not relevant since only the "steps" within the row-echelon form are of interest. Alternatively, the calculation of the row-echelon form can directly be performed with the related lattice vectors.

Algorithm 8 Reconversion from Representation over $\mathbb{Z}$.

```
$\boldsymbol{C}_{\mathrm{u}} = \textsc{ZToRing}(\boldsymbol{C})$
switch $\mathbb{I}$ do
    case $\mathbb{Z}$
        $\boldsymbol{C}_{\mathrm{u}} = \boldsymbol{C}$
    case $\mathcal{G}$
        $\boldsymbol{C}_{\mathrm{u}}^{(1)} = \boldsymbol{C}_{1:K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(2)} = \boldsymbol{C}_{K+1:2K,1:N_{\mathrm{c}}}$
    case $\mathcal{E}$
        $\tilde{\boldsymbol{C}} = \begin{bmatrix} \boldsymbol{I}_K & -\frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \frac{-\sqrt{3}}{2}\boldsymbol{I}_K \end{bmatrix} \cdot \boldsymbol{C}$
        $\boldsymbol{C}_{\mathrm{u}}^{(1)} = \tilde{\boldsymbol{C}}_{1:K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(2)} = \tilde{\boldsymbol{C}}_{K+1:2K,1:N_{\mathrm{c}}}$
    case $\mathcal{L}$
        $\boldsymbol{C}_{\mathrm{u}}^{(1)} = \boldsymbol{C}_{1:K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(2)} = \boldsymbol{C}_{K+1:2K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(3)} = \boldsymbol{C}_{2K+1:3K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(4)} = \boldsymbol{C}_{3K+1:4K,1:N_{\mathrm{c}}}$
    case $\mathcal{H}$
        $\tilde{\boldsymbol{C}} = \begin{bmatrix} \boldsymbol{I}_K & \boldsymbol{0}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{I}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{0}_K & \boldsymbol{I}_K & \frac{1}{2}\boldsymbol{I}_K \\ \boldsymbol{0}_K & \boldsymbol{0}_K & \boldsymbol{0}_K & \frac{1}{2}\boldsymbol{I}_K \end{bmatrix} \cdot \boldsymbol{C}$
        $\boldsymbol{C}_{\mathrm{u}}^{(1)} = \tilde{\boldsymbol{C}}_{1:K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(2)} = \tilde{\boldsymbol{C}}_{K+1:2K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(3)} = \tilde{\boldsymbol{C}}_{2K+1:3K,1:N_{\mathrm{c}}}$
        $\boldsymbol{C}_{\mathrm{u}}^{(4)} = \tilde{\boldsymbol{C}}_{3K+1:4K,1:N_{\mathrm{c}}}$
end switch
```

In Algorithm 8, the candidate integer vectors are reconverted from the equivalent real-valued representation to the representation in the particular ring $\mathbb{I}$. To this end, for the Gaussian and the Lipschitz integers, the components are simply stacked in the matrix $\boldsymbol{C}$. For the Eisenstein and the Hurwitz integers, the particular generator matrices according to (31) and (32), respectively, have to be incorporated first.

Appendix B
Comparison of the Upper Bounds on the First Basis Vector of Different LLL Variants

In this appendix, the upper bounds on the squared lengths of the first basis vector in case of LLL reduction, as described in Sec. IV-A2, are compared for different cases, i.e., integer rings. Please note that $\mathrm{vol}^{\frac{2}{2K}}(\mathbf{\Lambda}(\boldsymbol{G}_{\mathsf{r}})) = \mathrm{vol}^{\frac{2}{K}}(\mathbf{\Lambda}(\boldsymbol{G}))$ holds for the $2N \times 2K$ equivalent real-valued representation of complex matrices. For quaternion-valued matrices we have $\mathrm{vol}^{\frac{2}{4K}}(\mathbf{\Lambda}(\boldsymbol{G}_{\mathsf{r}})) = \mathrm{vol}^{\frac{2}{2K}}(\mathbf{\Lambda}(\boldsymbol{G}_{\mathsf{c}})) = \mathrm{vol}^{\frac{2}{K}}(\mathbf{\Lambda}(\boldsymbol{G}))$ for the $4N \times 4K$ real-valued and the $2N \times 2K$ complex-valued representations, respectively.

A. CLLL versus RLLL

The first comparison in this Appendix concerns complex matrices. In particular, the bound using the CLLL algorithm is compared to the one using the equivalent real-valued representation. This comparison has already been given in [23] and serves as an example for the other cases.

When comparing the bounds, only the rightmost part is relevant. The CLLL approach performs better if

$$\left(\frac{1}{\delta - 1/2}\right)^{\frac{K-1}{2}} < \left(\frac{1}{\delta - 1/4}\right)^{\frac{2K-1}{2}} \tag{114}$$

which can be rewritten as

$$\tau = \frac{\left(\frac{1}{\delta-1/2}\right)^{\frac{K-1}{2}}}{\left(\frac{1}{\delta-1/4}\right)^{\frac{2K-1}{2}}} < 1\ . \tag{115}$$

Then, τ can be converted to

$$\tau = \frac{\left(\frac{1}{\delta-1/2}\right)^{\frac{K-1}{2}}}{\left(\frac{1}{\delta-1/4}\right)^{\frac{2K-1}{2}}} = \left(\frac{\delta - 1/4}{\sqrt{\delta - 1/2}}\right)^{K} \cdot \underbrace{\left(\frac{\delta - 1/2}{\delta - 1/4}\right)^{\frac{1}{2}}}_{<1}\ . \tag{116}$$

Hence, the CLLL algorithm performs better if

$$\sqrt{\delta - 1/2} > \delta - 1/4\ . \tag{117}$$

This condition is, however, never fulfilled for $\delta \in (1/2, 1]$, but at least equality can be achieved if and only if $\delta = 3/4$.

B. ELLL versus RLLL

If the ELLL reduction is compared to the RLLL one, the term (116) has to be adapted to

$$\tau = \frac{\left(\frac{1}{\delta-1/3}\right)^{\frac{K-1}{2}}}{\left(\frac{1}{\delta-1/4}\right)^{\frac{2K-1}{2}}} = \left(\frac{\delta - 1/4}{\sqrt{\delta - 1/3}}\right)^{K} \cdot \underbrace{\left(\frac{\delta - 1/3}{\delta - 1/4}\right)^{\frac{1}{2}}}_{<1} . \tag{118}$$

Then, the ELLL approach performs better if

$$\sqrt{\delta - 1/3} > \delta - 1/4 . \tag{119}$$

This condition is fulfilled if $3/4 - 1/\sqrt{6} \approx 0.3418 < \delta \leq 1$.

C. QLLL versus ELLL

Next, assuming quaternion-valued matrices, the bound of QLLL reduction is compared to the one of ELLL reduction using the equivalent complex-valued representation. Here, the bounds can be compared via

$$\tau = \frac{\left(\frac{1}{\delta-1/2}\right)^{\frac{K-1}{2}}}{\left(\frac{1}{\delta-1/3}\right)^{\frac{2K-1}{2}}} = \left(\frac{\delta - 1/3}{\sqrt{\delta - 1/2}}\right)^{K} \cdot \underbrace{\left(\frac{\delta - 1/2}{\delta - 1/3}\right)^{\frac{1}{2}}}_{<1} . \tag{120}$$

The related condition reads

$$\sqrt{\delta - 1/2} > \delta - 1/3 . \tag{121}$$

It is fulfilled if $5/6 - 1/(2\sqrt{3}) \approx 0.5447 < \delta \leq 1$.

D. QLLL versus RLLL

Finally, the QLLL reduction is compared with the RLLL one (using the equivalent real-valued representation). Here, the term (116) is changed to

$$\tau = \frac{\left(\frac{1}{\delta-1/2}\right)^{\frac{K-1}{2}}}{\left(\frac{1}{\delta-1/4}\right)^{\frac{4K-1}{2}}} = \left(\frac{(\delta - 1/4)^2}{\sqrt{\delta - 1/2}}\right)^{K} \cdot \underbrace{\left(\frac{\delta - 1/2}{\delta - 1/4}\right)^{\frac{1}{2}}}_{<1} , \tag{122}$$

i.e., the condition

$$\sqrt{\delta - 1/2} > (\delta - 1/4)^2 \tag{123}$$

has to be fulfilled. This is the case when $0.5042 < \delta \leq 1$.

APPENDIX C
COMPARISON OF THE UPPER BOUNDS ON THE PRODUCT OF THE BASIS VECTORS OF DIFFERENT LLL VARIANTS

In this appendix, the upper bounds on the product of the basis vectors obtained from LLL reduction, as described in Sec. IV-B2, are compared for different cases (integer rings).

A. CLLL versus RLLL

Again, we start with the comparison of the CLLL reduction and the RLLL reduction, the latter using the equivalent $2N \times 2K$ representation $\boldsymbol{G}_{\mathsf{r}}$ of the complex-valued generator matrix $\boldsymbol{G}$. The CLLL approach has a lower bound on the product of the norms (and on the related orthogonality defect), if

$$\left(\frac{1}{\delta - 1/2}\right)^{\frac{K^2-K}{2}} < \left(\frac{1}{\delta - 1/4}\right)^{\frac{4K^2-2K}{2}} \quad . \tag{124}$$

This condition can be rewritten as

$$\tau = \frac{\left(\frac{1}{\delta-1/2}\right)^{\frac{K^2-K}{2}}}{\left(\frac{1}{\delta-1/4}\right)^{\frac{4K^2-2K}{2}}} < 1 \; . \tag{125}$$

The ratio τ can further be decomposed into

$$\tau = \frac{\left(\frac{1}{\delta-1/2}\right)^{\frac{K^2-K}{2}}}{\left(\frac{1}{\delta-1/4}\right)^{\frac{4K^2-2K}{2}}} = \left(\frac{(\delta-1/4)^2}{\sqrt{\delta-1/2}}\right)^{K^2} \cdot \underbrace{\left(\frac{\sqrt{\delta-1/2}}{\delta-1/4}\right)^{K}}_{\leq 1} , \tag{126}$$

where the rightmost part is less than or equal to one, cf. (117). Hence, independently from K, $\tau < 1$ if

$$\sqrt{\delta - 1/2} > (\delta - 1/4)^2 \; . \tag{127}$$

This inequality is fulfilled if $0.5042 < \delta \leq 1$, cf. (123).

B. ELLL versus RLLL

If the ELLL algorithm is compared to the RLLL one, the ratio

$$\tau = \frac{\left(\frac{1}{\delta-1/3}\right)^{\frac{K^2-K}{2}}}{\left(\frac{1}{\delta-1/4}\right)^{\frac{4K^2-2K}{2}}} = \left(\frac{(\delta-1/4)^2}{\sqrt{\delta-1/3}}\right)^{K^2} \cdot \left(\frac{\sqrt{\delta-1/3}}{\delta-1/4}\right)^{K} \tag{128}$$

has to be less than one. Then, the ELLL approach performs better if for the left part in (128),

$$\sqrt{\delta - 1/3} > (\delta - 1/4)^2 \tag{129}$$

is valid. Additionally, since the right part is not necessarily less than one,

$$\frac{(\delta - 1/4)^2}{\sqrt{\delta - 1/3}} < \frac{\delta - 1/4}{\sqrt{\delta - 1/3}} \tag{130}$$

has to hold; then, the product of both parts will be less than one if the same holds for the left part. This condition is always fulfilled since $\delta - 1/4 < 1$. Thus, (129) still has to be fulfilled. This is the case when $0.3334 < \delta \leq 1$.

C. QLLL versus ELLL

Next, the bound for QLLL reduction is compared to the one for ELLL reduction using the equivalent $2N \times 2K$ complex-valued representation $\boldsymbol{G}_{\mathsf{c}}$. In particular, the ratio reads

$$\tau = \frac{\left(\frac{1}{\delta - 1/2}\right)^{\frac{K^2-K}{2}}}{\left(\frac{1}{\delta - 1/3}\right)^{\frac{4K^2-2K}{2}}} = \left(\frac{(\delta - 1/3)^2}{\sqrt{\delta - 1/2}}\right)^{K^2} \cdot \left(\frac{\sqrt{\delta - 1/2}}{\delta - 1/3}\right)^{K} . \tag{131}$$

Then, the QLLL reduction performs better if

$$\sqrt{\delta - 1/2} > (\delta - 1/3)^2 \tag{132}$$

and additionally, if

$$(\delta - 1/3)^2 < \delta - 1/3 \, . \tag{133}$$

The latter always holds since $\delta - 1/3 < 1$. The condition (132) is fulfilled if $0.5008 < \delta \leq 1$.

D. QLLL versus RLLL

Finally, the QLLL reduction is compared with the RLLL one, where the latter takes advantage of the $4N \times 4K$ real-valued representation $\boldsymbol{G}_{\mathsf{r}}$. In that case, the ratio is given as

$$\tau = \frac{\left(\frac{1}{\delta - 1/2}\right)^{\frac{K^2-K}{2}}}{\left(\frac{1}{\delta - 1/4}\right)^{\frac{16K^2-4K}{2}}} = \left(\frac{(\delta - 1/4)^8}{\sqrt{\delta - 1/2}}\right)^{K^2} \cdot \left(\frac{\sqrt{\delta - 1/2}}{(\delta - 1/4)^2}\right)^{K} , \tag{134}$$

i.e., we obtain the conditions

$$\sqrt{\delta - 1/2} > (\delta - 1/4)^8 \tag{135}$$

and

$$(\delta - 1/4)^8 < (\delta - 1/4)^2 \, . \tag{136}$$

The latter is always fulfilled since $\delta - 1/4 < 1$. The former is valid if $0.5000 < \delta \leq 1$.

References

[1] S. Stern and R. F. H. Fischer, “Quaternion-valued multi-user MIMO transmission via dual-polarized antennas and QLLL reduction,” in *Proceedings of the 25th International Conference on Telecommunications (ICT)*, Saint Malo, France, Jun. 2018, pp. 63–69.

[2] S. Stern, “Advanced equalization and coded-modulation strategies for multiple-input/multiple-output systems,” Ph.D. dissertation, Ulm University, May 2019.

[3] C. Hermite, “Extraits de lettres de M.Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres,” *Journal für die reine und angewandte Mathematik*, vol. 40, pp. 261–315, 1850.

[4] A. N. Korkine and J. I. Zolotareff, “Sur les formes quadratiques,” *Mathematische Annalen*, vol. 6, pp. 366–389, 1873.

[5] H. Minkowski, “Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen,” *Journal für die reine und angewandte Mathematik*, vol. 107, pp. 278–297, 1891.

[6] A. K. Lenstra, H. W. Lenstra, and L. Lovász, “Factoring polynomials with rational coefficients,” *Mathematische Annalen*, vol. 261, pp. 515–534, Dec. 1982.

[7] R. Kannan, “Improved algorithms for integer programming and related lattice problems,” in *Proceedings of the 15th Annual ACM Symposium on Theory of Computing*, 1983, pp. 193–206.

[8] C. P. Schnorr and M. Euchner, “Lattice basis reduction: Improved practical algorithms and solving subset sum problems,” *Mathematical Programming*, vol. 66, no. 1, pp. 181–199, Aug. 1994.

[9] W. Zhang, S. Qiao, and Y. Wei, “HKZ and Minkowski reduction algorithms for lattice-reduction-aided MIMO detection,” *IEEE Transactions on Signal Processing*, vol. 60, no. 11, pp. 5963–5976, Nov. 2012.

[10] B. Helfrich, “Algorithms to construct Minkowski reduced and Hermite reduced lattice bases,” *Theoretical Computer Science*, vol. 41, pp. 125–139, 1985.

[11] D. Micciancio and O. Regev, *Lattice-based Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 147–191.

[12] D. N. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. New York, NY, USA: Cambridge University Press, 2005.

[13] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, “Closest point search in lattices,” *IEEE Transactions on Information Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.

[14] H. Yao and G. W. Wornell, “Lattice-reduction-aided detectors for MIMO communication systems,” in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM)*, Taipei, Taiwan, Nov. 2002, pp. 424–428.

[15] C. Windpassinger and R. F. H. Fischer, “Low-complexity near-maximum-likelihood detection and precoding for MIMO systems using lattice reduction,” in *Proceedings of the IEEE Information Theory Workshop (ITW)*, Paris, France, Mar. 2003, pp. 345–348.

[16] C. Windpassinger, “Detection and precoding for multiple input multiple output channels,” Ph.D. dissertation, University of Erlangen-Nuremberg, Erlangen, Germany, 2004.

[17] D. Wübben, R. Böhnke, V. Kühn, and K.-D. Kammeyer, “Near-maximum-likelihood detection of MIMO systems using MMSE-based lattice-reduction,” in *Proceedings of the IEEE International Conference on Communications (ICC)*, vol. 2, Paris, France, Jun. 2004, pp. 798–802.

[18] D. Wübben, D. Seethaler, J. Jaldén, and G. Matz, “Lattice reduction,” *IEEE Signal Processing Magazine*, vol. 28, no. 3, pp. 70–91, May 2011.

[19] R. F. H. Fischer, S. Stern, and J. B. Huber, "Lattice-reduction-aided and integer-forcing equalization: Structures, criteria, factorization, and coding," *Foundations and Trends® in Communications and Information Theory*, vol. 16, no. 1-2, pp. 1–155, 2019.

[20] M. Taherzadeh, A. Mobasher, and A. K. Khandani, "LLL reduction achieves the receive diversity in MIMO decoding," *IEEE Transactions on Information Theory*, vol. 53, no. 12, pp. 4801–4805, Dec. 2007.

[21] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, "Integer-forcing linear receivers," *IEEE Transactions on Information Theory*, vol. 60, no. 12, pp. 7661–7685, Dec. 2014.

[22] R. F. H. Fischer, *Precoding and Signal Shaping for Digital Transmission*. New York, NY, USA: John Wiley & Sons, 2002.

[23] Y. H. Gan, C. Ling, and W. H. Mow, "Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection," *IEEE Transactions on Signal Processing*, vol. 57, no. 7, pp. 2701–2710, Jul. 2009.

[24] K. Huber, "Codes over Gaussian integers," *IEEE Transactions on Information Theory*, vol. 40, no. 1, pp. 207–216, Jan. 1994.

[25] J. H. Conway and N. J. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., ser. A Series of Comprehensive Studies in Mathematics. New York, NY, USA: Springer, 1999, vol. 290.

[26] H. Jiang and S. Du, "Complex Korkine-Zolotareff reduction algorithm for full-diversity MIMO detection," *IEEE Communications Letters*, vol. 17, no. 2, pp. 381–384, Feb. 2013.

[27] L. Ding, Y. Wang, and J. Zhang, "Complex Minkowski reduction and a relaxation for near-optimal MIMO linear equalization," *IEEE Wireless Communications Letters*, vol. 6, no. 1, pp. 38–41, Feb. 2017.

[28] L. Ding, K. Kansanen, Y. Wang, and J. Zhang, "Exact SMP algorithms for integer-forcing linear MIMO receivers," *IEEE Transactions on Wireless Communications*, vol. 14, no. 12, pp. 6955–6966, Dec. 2015.

[29] R. F. H. Fischer, M. Cyran, and S. Stern, "Factorization approaches in lattice-reduction-aided and integer-forcing equalization," in *Proceedings of the International Zurich Seminar on Communications*, Zurich, Switzerland, Mar. 2016, pp. 108–112.

[30] J. Wen, L. Li, X. Tang, and W. H. Mow, "An efficient optimal algorithm for the successive minima problem," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1424–1436, Feb. 2019.

[31] N. E. Tunali, Y.-C. Huang, J. J. Boutros, and K. R. Narayanan, "Lattices over Eisenstein integers for compute-and-forward," *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5306–5321, Oct. 2015.

[32] S. Stern and R. F. H. Fischer, "Advanced factorization strategies for lattice-reduction-aided preequalization," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 1471–1475.

[33] K. Huber, "Codes over Eisenstein-Jacobi integers," *Contemporary Mathematics*, vol. 168, pp. 165–165, 1994.

[34] M. Karlsson and E. Agrell, *Multidimensional Optimized Optical Modulation Formats*. John Wiley & Sons, 2016, ch. 2, pp. 13–64.

[35] Y. Cui, R. Li, and H. Fu, "A broadband dual-polarized planar antenna for 2G/3G/LTE base stations," *IEEE Transactions on Antennas and Propagation*, vol. 62, no. 9, pp. 4836–4840, Sep. 2014.

[36] M. Li, Y. Ban, Z. Xu, G. Wu, C. Sim, K. Kang, and Z. Yu, "Eight-port orthogonally dual-polarized antenna array for 5G smartphone applications," *IEEE Transactions on Antennas and Propagation*, vol. 64, no. 9, pp. 3820–3830, Sep. 2016.

[37] F. Ghaedi, J. Jamali, and M. Taghizadeh, "A wideband dual-polarized antenna using magneto-electric dipoles for base station applications," *AEÜ - International Journal of Electronics and Communications*, vol. 126, p. 153395, 2020.

[38] S. M. Alamouti, "A simple transmit diversity technique for wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 8, pp. 1451–1458, Oct. 1998.

[39] J. H. Conway and D. A. Smith, *On Quaternions and Octonions*. Boca Raton, FL, USA: AK Peters/CRC Press, 2003.

[40] O. M. Isaeva and V. A. Sarytchev, "Quaternion presentations polarization state," in 2^{nd} *Topical Symposium on Combined Optical-Microwave Earth and Atmosphere Sensing*, Atlanta, GA, USA, Apr. 1995, pp. 195–196.

[41] B. J. Wysocki, T. A. Wysocki, and J. Seberry, "Modeling dual polarization wireless fading channels using quaternions," in *Joint IST Workshop on Mobile Future and Symposium on Trends in Communications*, Bratislava, Slovakia, Jun. 2006, pp. 68–71.

[42] P. M. Neumann, G. A. Stoy, and E. C. Thompson, *Groups and Geometry*, ser. Oxford Science Publications. Oxford, United Kingdom: Oxford University Press, 1994.

[43] A. A. Karatsuba and Y. P. Ofman, "Multiplication of many-digital numbers by automatic computers," in *Doklady Akademii Nauk*, vol. 145, no. 2. Russian Academy of Sciences, 1962, pp. 293–294.

[44] A. Cariow and G. Cariowa, "An unified approach for developing rationalized algorithms for hypercomplex number multiplication," *Electric Review*, vol. 91, no. 2, pp. 36–39, 2015.

[45] H. Aslaksen, "Quaternionic determinants," *The Mathematical Intelligencer*, vol. 18, no. 3, pp. 57–65, 1996.

[46] R. R. Müller and B. Cakmak, "Channel modelling of MU-MIMO systems by quaternionic free probability," in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, Cambridge, MA, USA, 2012, pp. 2656–2660.

[47] S. Weintraub, *Factorization: Unique and Otherwise*, ser. CMS Treatises in Mathematics. CRC Press, 2008.

[48] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to Algorithms*, ser. Computer Science. Cambridge, MA, USA: MIT Press, 2009.

[49] M. Bossert, *Channel Coding for Telecommunications*. Chichester, United Kingdom: John Wiley & Sons, 1999.

[50] J. Conway and N. Sloane, "Fast quantizing and decoding algorithms for lattice quantizers and codes," *IEEE Transactions on Information Theory*, vol. 28, no. 2, pp. 227–232, Mar. 1982.

[51] H. Napias, "A generalization of the LLL-algorithm over Euclidean rings or orders," *Journal de Théorie des Nombres de Bordeaux*, vol. 8, no. 2, pp. 387–396, 1996.

[52] R. Zamir, B. Nazer, Y. Kochman, and I. Bistritz, *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation and Multiuser Information Theory*. Cambridge, United Kingdom: Cambridge University Press, 2014.

[53] H. Daudé and B. Vallée, "An upper bound on the average number of iterations of the LLL algorithm," *Theoretical Computer Science*, vol. 123, no. 1, pp. 95–115, 1994.

[54] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes: The Art of Scientific Computing*, 3rd ed. Cambridge, United Kingdom: Cambridge University Press, 2007.

[55] A. Akhavi, "The optimal LLL algorithm is still polynomial in fixed dimension," *Theoretical Computer Science*, vol. 297, no. 1, pp. 3–23, 2003.

[56] R. F. H. Fischer, "From Gram–Schmidt orthogonalization via sorting and quantization to lattice reduction," in *Proceedings of the Joint Workshop on Coding and Communications (JWCC)*, Santo Stefano Belbo, Italy, Oct. 2010.

[57] J. C. Lagarias, H. W. Lenstra, and C. P. Schnorr, "Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice," *Combinatorica*, vol. 10, no. 4, pp. 333–348, Dec. 1990.

[58] H. Minkowski, "Diskontinuitätsbereich für arithmetische Äquivalenz," in *Ausgewählte Arbeiten zur Zahlentheorie und zur Geometrie: Mit D. Hilberts Gedächtnisrede auf H. Minkowski, Göttingen 1909*. Vienna, Austria: Springer, 1989, pp. 73–120.

[59] P. Nguyen and B. Vallée, *The LLL Algorithm: Survey and Applications*, ser. Information Security and Cryptography. Berlin, Heidelberg: Springer-Verlag, 2009.

[60] H. F. Blichfeldt, "The minimum value of quadratic forms, and the closest packing of spheres," *Mathematische Annalen*, vol. 101, no. 1, pp. 605–608, 1929.

[61] S. Lyu, C. Porter, and C. Ling, “Lattice reduction over imaginary quadratic fields,” *IEEE Transactions on Signal Processing*, vol. 68, pp. 6380–6393, 2020.

[62] C. Siegel and K. Chandrasekharan, *Lectures on the Geometry of Numbers*. Berlin, Heidelberg: Springer-Verlag, 1989.

[63] C. Ling and N. Howgrave-Graham, “Effective LLL reduction for lattice decoding,” in *Proceedings of the IEEE International Symposium on Information Theory (ISIT)*, 2007, pp. 196–200.

[64] C. Ling, W. H. Mow, and L. Gan, “Dual-lattice ordering and partial lattice reduction for SIC-based MIMO detection,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 3, no. 6, pp. 975–985, Dec. 2009.

[65] H. L. Van Trees, *Detection, estimation, and modulation theory, part I: detection, estimation, and linear modulation theory*. New York, NY, USA: John Wiley & Sons, 2004.

[66] J. G. Proakis and M. Salehi, *Digital Communications*, 5th ed. New York, NY, USA: McGraw-Hill, 2008.

[67] F. Frey, S. Stern, J. K. Fischer, and R. F. H. Fischer, “Two-stage coded modulation for Hurwitz constellations in fiber-optical communications,” *Journal of Lightwave Technology*, vol. 38, no. 12, pp. 3135–3146, Jun. 2020.

[68] S. S. Qureshi, S. Ali, and S. A. Hassan, “Optimal polarization diversity gain in dual-polarized antennas using quaternions,” *IEEE Signal Processing Letters*, vol. 25, no. 4, pp. 467–471, Apr. 2018.

[69] L. Zheng and D. N. Tse, “Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels,” *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073–1096, May 2003.

[70] B. Hassibi, “An efficient square-root algorithm for BLAST,” in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing*, Istanbul, Turkey, Jun. 2000, pp. 737–740.

[71] S. Stern and R. F. H. Fischer, “Lattice-reduction-aided preequalization over algebraic signal constellations,” in *Proceedings of the 9th International Conference on Signal Processing and Communication Systems (ICSPCS)*, Cairns, QLD, Australia, Dec. 2015.

[72] M. Güzeltepe, “Codes over Hurwitz integers,” *Discrete Mathematics*, vol. 313, no. 5, pp. 704–714, 2013.

[73] M. Güzeltepe and O. Heden, “Perfect Mannheim, Lipschitz and Hurwitz weight codes,” *Mathematical Communications*, vol. 19, no. 2, pp. 253–276, 2014.

[74] C. Stierstorfer, “A bit-level-based approach to coded multicarrier transmission,” Ph.D. dissertation, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2009.

[75] G. D. Forney, M. D. Trott, and Sae-Young Chung, “Sphere-bound-achieving coset codes and multilevel coset codes,” *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 820–850, May 2000.