

Quaternionic Minkowski Reduction and its Application in Dual-Polarized MIMO Systems

Sebastian Stern¹, Cong Ling², Cornelia Ott³, Robert F.H. Fischer¹

¹*Institute of Communications Engineering, Ulm University, Germany*

²*Department of Electrical and Electronic Engineering, Imperial College London, United Kingdom*

³*Institute of Communications and Navigation, German Aerospace Center (DLR), Germany*

Email: sebastian.stern@uni-ulm.de, cling@ieee.org, cornelia.ott@dlr.de, robert.fischer@uni-ulm.de

Abstract—The task of finding the shortest vectors of a lattice that form a basis thereof is known as Minkowski reduction. In this work, Minkowski reduction is adapted to discrete subgroups of quaternionic spaces defined over the set of Hurwitz integers which constitutes a Euclidean subring of the (Hamilton) quaternions. Based on a quaternionic variant of Minkowski's greatest-common-divisor condition for suitable lattice vectors, a lattice-basis-reduction algorithm is derived. To that end, a basis-update approach is presented which takes the non-commutativity of quaternionic multiplication into account. The reduction algorithm is finally applied in multi-user multiple-input/multiple-output (MIMO) systems with dual-polarized antennas, where the quaternionic interference is handled by lattice-reduction-aided equalization. It is shown that quaternionic Minkowski reduction achieves significantly better results than state-of-the-art Lenstra–Lenstra–Lovász (LLL) reduction and that the successive minima of quaternionic lattices are approximated quite well.

I. INTRODUCTION

Lattice-reduction-aided (LRA) linear equalization [7], [16], [18] and the related, finite-field-based integer-forcing (IF) linear equalization [7], [19] are popular approaches for multi-user multiple-input/multiple-output (MIMO) communications as they enable low-complexity near-maximum-likelihood transmission. These schemes share the idea of not directly equalizing the MIMO channel by its (Moore–Penrose) inverse, but of transforming the channel into a form for which linear equalization results in significantly lower noise enhancement. This is achieved by interpreting the channel matrix as the generator matrix of a *lattice*—a regular arrangement of points in N -dimensional space—followed by the search for an alternative basis thereof that is “more suited” for equalization.

The most famous approach for *lattice basis reduction* is the polynomial-time Lenstra–Lenstra–Lovász (LLL) algorithm [10], for which only suboptimal bounds on the length of LLL-reduced basis vectors exist. Their norms should be *as small as possible* to achieve optimal equalization performance. In this sense, Minkowski reduction [9], [11], [20] leads to an optimal result by successively selecting the shortest lattice vectors *which can be extended to a basis*, i.e., for which a *unimodular* integer transformation matrix exists that describes the change to an alternative basis spanning the same lattice.

Closely related is the successive minima problem (SMP)—the search for the shortest *independent* lattice vectors. Since they do not necessarily form a basis of the lattice, the related

non-unimodular (full-rank) integer matrix may create a *sublattice*. Even though LRA/IF receivers can generally handle such full-rank matrices [7], [13], [19], some schemes have heavy constraints on the applicable coding that prevent their use [7].

The literature on lattices has initially been strictly real-valued, i.e., lattices over the (real) integers $\mathbb{Z}$ have been treated. Hence, equalization of complex-valued MIMO systems has been performed utilizing the *equivalent real-valued matrix representation* [3] of the channel. Complex LLL (CLLL) reduction [8], in which the complex integers $\mathcal{G}$ (aka *Gaussian integers*) were considered instead, enabled consistent complex-valued MIMO processing. In the sequel, complex variants of Minkowski reduction [5], [13] and algorithms to solve the complex SMP [6], [7], [13] have been proposed.

MIMO systems can be extended to *quaternion-valued* transmission. Such scenarios are, e.g., enabled by *dual-polarized* systems [14], [17], i.e., the use of both polarization planes of electromagnetic waves, or Alamouti space-time coding [12]. To that end, the adaption of lattice algorithms to quaternionic arithmetic is convenient. Unfortunately, the straightforward application of LLL or Minkowski reduction over the *Lipschitz integers* $\mathcal{L}$ —quaternions with *integer components*—is not possible: for these types of reduction the constituent integer ring has to form a *Euclidean ring* [13], [14]—a property which $\mathcal{L}$ does not provide since a division with *small* remainder cannot be guaranteed. Instead, it is enabled by the set of *Hurwitz integers* $\mathcal{H}$ additionally including all quaternions with *half-integer components*. On that basis, quaternionic LLL (QLLL) reduction over $\mathcal{H}$ as well as strategies to solve the two types of quaternionic SMP (over $\mathcal{L}$ and $\mathcal{H}$) have been proposed [14].

Nevertheless, *quaternionic Minkowski reduction* is still an open problem. Existing procedures for *basis update* [5], [15], [20], i.e., the update of the generator matrix once a shortest (suited) vector has been found, require commutative integer rings like $\mathbb{Z}$ or $\mathcal{G}$. However, quaternionic multiplication is non-commutative. Hence, in this work, a novel algorithm for quaternionic Minkowski reduction over $\mathcal{H}$ is proposed. It incorporates a generalized basis update which can handle non-commutative arithmetic. Moreover, the application of this reduction approach is considered in the dual-polarized multi-user MIMO uplink scenario. Numerical results show that excellent performance is achieved in relation to LLL reduction and the solutions obtained from the two types of quaternionic SMP.

The paper is structured as follows: In Sec. II, important definitions and properties of quaternionic sets and related lattices are collected. The quaternionic Minkowski-reduction algorithm is presented in Sec. III. Its utilization in MIMO systems and respective numerical results are studied in Sec. IV. The paper is closed by a summary and an outlook in Sec. V.

II. PRELIMINARIES

This section reviews the most important definitions in the area of quaternions and quaternionic lattices. For a more in-depth insight into the subject the reader is referred to [4], [14].

A. Quaternions and Related Sets

The (Hamilton) quaternions are defined as [3], [4]

$$\mathbb{H} = \{q^{(1)} + q^{(2)}i + q^{(3)}j + q^{(4)}k \mid q^{(1,2,3,4)} \in \mathbb{R}\}, \quad (1)$$

where $q^{(1)}$ denotes the real part of a quaternion and the tuple $(q^{(2)}, q^{(3)}, q^{(4)})$ the imaginary part. The three imaginary units are denoted by i, j , and $k = ij$. Consequently, the conjugate reads $q^* = q^{(1)} - q^{(2)}i - q^{(3)}j - q^{(4)}k$ and the Euclidean norm is calculated as $\|q\| = \sqrt{qq^*} = \sqrt{q^*q} = \sqrt{(q^{(1)})^2 + (q^{(2)})^2 + (q^{(3)})^2 + (q^{(4)})^2}$. The multiplication of two quaternions α and β is non-commutative and given by [4]

$$\begin{aligned} \alpha \cdot \beta &= (\alpha^{(1)}\beta^{(1)} - \alpha^{(2)}\beta^{(2)} - \alpha^{(3)}\beta^{(3)} - \alpha^{(4)}\beta^{(4)}) \\ &+ (\alpha^{(1)}\beta^{(2)} + \alpha^{(2)}\beta^{(1)} + \alpha^{(3)}\beta^{(4)} - \alpha^{(4)}\beta^{(3)})i \\ &+ (\alpha^{(1)}\beta^{(3)} - \alpha^{(2)}\beta^{(4)} + \alpha^{(3)}\beta^{(1)} + \alpha^{(4)}\beta^{(2)})j \\ &+ (\alpha^{(1)}\beta^{(4)} + \alpha^{(2)}\beta^{(3)} - \alpha^{(3)}\beta^{(2)} + \alpha^{(4)}\beta^{(1)})k. \end{aligned} \quad (2)$$

The inverse of $q \in \mathbb{H}$ is defined by $q^{-1} = q^* \cdot (q^*q)^{-1}$ to assure $q \cdot q^{-1} = 1$ (right inverse) and $q^{-1} \cdot q = 1$ (left inverse).

The Lipschitz integers form a subring of $\mathbb{H}$ defined by

$$\mathcal{L} = \{q^{(1)} + q^{(2)}i + q^{(3)}j + q^{(4)}k \mid q^{(1,2,3,4)} \in \mathbb{Z}\} \quad (3)$$

which is given by all quaternions with integer components. It is isomorphic to a two-dimensional vector of Gaussian integers from $\mathcal{G}^2 = (\mathbb{Z} + \mathbb{Z}i)^2$ or a four-dimensional vector of real integers from $\mathbb{Z}^4$. The quantization $Q_{\mathcal{L}}(q) = \lfloor q^{(1)} \rfloor + \lfloor q^{(2)} \rfloor i + \lfloor q^{(3)} \rfloor j + \lfloor q^{(4)} \rfloor k$ is performed by individual rounding. The Lipschitz integers form a non-Euclidean ring as a (right) division $\alpha \cdot \beta^{-1}$ with *small* remainder ρ , $\|\rho\| < \|\beta\|$, with

$$\alpha = \gamma \cdot \beta + \rho, \quad (4)$$

is not ensured. This stems from the fact that the maximal quantization error is given as $\max_{q \in \mathbb{H}} \|Q_{\mathcal{L}}\{q\} - q\| = 1$, e.g., if $q = \frac{1}{2} + \frac{1}{2}i + \frac{1}{2}j + \frac{1}{2}k$. In such cases, equality $\|\rho\| = \|\beta\|$ may occur since the minimal non-zero norm of β also reads $\min_{\beta \neq 0} \|\beta\| = 1$, implying that the remainder is not *small*.

The set of Hurwitz integers

$$\mathcal{H} = \left\{ q^{(1)} + q^{(2)}i + q^{(3)}j + q^{(4)}k \mid q^{(1,2,3,4)} \in \mathbb{Z} \cup \left(\mathbb{Z} + \frac{1}{2}\right)^4 \right\} \quad (5)$$

includes an additional set of $\mathcal{L}$ with an offset $\frac{1}{2}$ per component. The resulting integer ring is isomorphic to the four-dimensional real-valued checkerboard lattice D_4 [3], [14]. The

Algorithm 1 $[\hat{\alpha}] = \text{HURW_QUANTIZATION}(\alpha)$

```

1:  $\hat{\alpha}_1 = \lfloor \alpha^{(1)} \rfloor + \lfloor \alpha^{(2)} \rfloor i + \lfloor \alpha^{(3)} \rfloor j + \lfloor \alpha^{(4)} \rfloor k$  ▷ rounding to  $\mathcal{L}$ 
2:  $\hat{\alpha}_2 = \lfloor \alpha^{(1)} + \frac{1}{2} \rfloor - \frac{1}{2} + (\lfloor \alpha^{(2)} + \frac{1}{2} \rfloor - \frac{1}{2})i + (\lfloor \alpha^{(3)} + \frac{1}{2} \rfloor - \frac{1}{2})j$ 
    $+ (\lfloor \alpha^{(4)} + \frac{1}{2} \rfloor - \frac{1}{2})k$  ▷ rounding to  $\mathcal{L} + \frac{1+i+j+k}{2}$ 
3: if  $\|\alpha - \hat{\alpha}_1\| < \|\alpha - \hat{\alpha}_2\|$  then
4:    $\hat{\alpha} = \hat{\alpha}_1$  ▷ closest point in  $\mathcal{L}$ 
5: else
6:    $\hat{\alpha} = \hat{\alpha}_2$  ▷ closest point in  $\mathcal{L} + \frac{1+i+j+k}{2}$ 
7: end if
```

Algorithm 2 $[\rho, \gamma] = \text{HURW_RIGHT_DIV_REM}(\alpha, \beta)$

```

1:  $\gamma = \alpha \cdot \beta^{-1}$  ▷ left quotient  $\gamma \in \mathcal{H}$  of  $\alpha, \beta \in \mathcal{H}$ 
2:  $\gamma = \text{HURW\_QUANTIZATION}(\gamma)$ 
3:  $\rho = \alpha - \gamma \cdot \beta$  ▷ remainder  $\rho \in \mathbb{H}$  of right division
```

quantization to $\mathcal{H}$ is defined in Algorithm 1. It is simply performed by quantizing to both $\mathcal{L}$ and $\mathcal{L} + \frac{1+i+j+k}{2}$ followed by the decision for the point closer to the original one, cf. [3], [14]. The Hurwitz integers form a Euclidean ring since the maximal quantization error reads $\max_{q \in \mathbb{H}} \|Q_{\mathcal{H}}(q) - q\| = \frac{1}{\sqrt{2}}$, e.g., if $q = \frac{1}{2} + \frac{1}{2}i$. Hence, a division with *small* remainder according to (4) is guaranteed as $\|\beta\| \geq 1$ for all non-zero elements. The *right* division over $\mathcal{H}$ with small remainder (symmetric w.r.t. the origin) is implemented in Algorithm 2.

B. Quaternionic Lattices and Related Problems

Lattices have initially been defined over the (real) integers $\mathbb{Z}$, forming discrete subgroups of the N -dimensional Euclidean space $\mathbb{R}^N$. This definition can be generalized to lattices over complex numbers or quaternions defined by [14]

$$\Lambda(\mathcal{G}) = \left\{ G\zeta = \sum_{k=1}^K g_k \zeta_k \mid \zeta_k \in \mathcal{I} \right\}, \quad (6)$$

where $\mathcal{I}$ denotes an integer ring, e.g., the Gaussian, Lipschitz, or Hurwitz integers ($\mathcal{G}$, $\mathcal{L}$, or $\mathcal{H}$). As a consequence, discrete subgroups of $\mathbb{C}^N$ and $\mathbb{H}^N$, respectively, are given. The linearly independent columns of the *generator matrix* given as $G = [g_1, \dots, g_K] \in \mathbb{H}^{N \times K}$ in the quaternionic case form a particular *basis* of the lattice $\Lambda(\mathcal{G})$ where K denotes its *rank*.

The task of lattice reduction is to find an alternative generator matrix $G_{\text{red}} = [g_{\text{red},1}, \dots, g_{\text{red},K}]$, i.e., a *reduced* basis, that spans the same lattice by applying a *unimodular* transformation matrix $T \in \mathcal{I}^{K \times K}$ according to¹

$$G_{\text{red}} = GT, \quad \text{where } \det(T^H T) = 1. \quad (7)$$

The definition of “reduced” depends on the reduction algorithm. In LLL reduction [8], [10], [14], the column norms of the orthogonal matrix Q derived from QR decomposition of G have to fulfill a certain quality condition which is suboptimal when the norms of G_{red} are relevant. The task of finding a basis that minimizes its maximum norm $\max_k \|g_{\text{red},k}\|$ is known as *shortest basis problem* (SBP), cf. [7], [13].

¹The Hermitian matrix (conjugate transpose) of H is denoted as H^H . Given Hermitian matrices (here: the Gram matrix $T^H T$), quaternionic determinants can (almost) be treated like real or complex ones. In general, this is not the case due to the non-commutativity of quaternionic multiplication [2].

A similar task is given by the *successive minima problem* (SMP). The successive minima are the norms of the shortest vectors of a lattice, denoted by $\mu_1, \dots, \mu_K$, which are linearly independent [6], [7], [13], [14]. Analogous to lattice reduction, a related generator matrix $G_{\text{SMP}} = [\mu_1, \dots, \mu_K] = GT$ can be specified. However, the transformation matrix $T \in \mathcal{I}^{K \times K}$ is not necessarily unimodular but only has to have full rank, i.e., $\text{rank}(T) = K$. If T is non-unimodular, only a sublattice $\Lambda(G_{\text{SMP}}) \subsetneq \Lambda(G)$ of the original one is spanned.

The task of finding K independent lattice vectors that (only) minimize $\max_k \|\mu_k\|$ is known as *shortest independent vector problem* (SIVP) [6], [7], [13], [14]. Since a solution to the SMP also solves the (weaker) SIVP, a lower bound on the maximum norm according to the SBP is established.

C. Equivalent Representations of Quaternionic Lattices

Quaternionic lattices defined over $\mathcal{L}$ can be represented by complex or real generator matrices due to the isomorphism of $\mathcal{L}$ to $\mathcal{G}^2$ and $\mathbb{Z}^4$, respectively. A quaternionic generator matrix G is equivalently expressed via the complex matrix

$$G_c = \begin{bmatrix} G^{(1)} + G^{(2)}i & -G^{(3)} - G^{(4)}i \\ G^{(3)} - G^{(4)}i & G^{(1)} - G^{(2)}i \end{bmatrix} \quad (8)$$

of doubled dimensions $2N \times 2K$ or the real-valued matrix

$$G_r = \begin{bmatrix} G^{(1)} & -G^{(2)} & -G^{(3)} & -G^{(4)} \\ G^{(2)} & G^{(1)} & -G^{(4)} & G^{(3)} \\ G^{(3)} & G^{(4)} & G^{(1)} & -G^{(2)} \\ G^{(4)} & -G^{(3)} & G^{(2)} & G^{(1)} \end{bmatrix} \quad (9)$$

with dimensions $4N \times 4K$, cf. [14]. In this way, real or complex lattice algorithms can be applied as a substitution.

In a similar manner, a real-valued representation of lattices over $\mathcal{H}$ can be derived by multiplication with the generator matrix of the isomorphic D_4 lattice [3] according to [14]

$$G_{r,\mathcal{H}} = \underbrace{G_r}_{G_{D_4}} \begin{bmatrix} I_K & 0_K & 0_K & \frac{1}{2}I_K \\ 0_K & I_K & 0_K & \frac{1}{2}I_K \\ 0_K & 0_K & I_K & \frac{1}{2}I_K \\ 0_K & 0_K & 0_K & \frac{1}{2}I_K \end{bmatrix}, \quad (10)$$

I_K denoting the identity matrix of dimension K .

Instead of solving the quaternionic SMP over $\mathcal{L}$, the equivalent complex or real SMPs can be considered. If so, each quaternionic successive minimum occurs twice and four times, respectively [6], [13], [14]. After solving the complex or real SMP, the quaternionic matrix representation can be restored, cf. [14, Algorithm 7]. In contrast, both CLLL and (real) LLL algorithm as well as complex and real Minkowski reduction may destroy the “structures” in (8) and (9). Hence, a quaternionic representation may not be possible any more [13].

III. QUATERNIONIC MINKOWSKI REDUCTION

In this section, the idea of Minkowski reduction is adapted to quaternionic lattices. After discussing the general definitions, a basis-update approach is proposed which can handle the non-commutative algebra at hand. These preliminary considerations are combined into a reduction algorithm in pseudo code.

Algorithm 3 $[\beta] = \text{HURW_RIGHT_GCD}(\alpha, \beta)$

```

1: while  $\beta \neq 0$  do ▷ iterative Euclidean algorithm for  $\alpha, \beta \in \mathcal{H}$ 
2:    $\delta = \beta$ 
3:    $[\beta, \sim] = \text{HURW\_RIGHT\_DIV\_REM}(\alpha, \delta)$ 
▷ remainder  $\beta$  from right division  $\alpha\delta^{-1}$  in Algorithm 2
4:    $\alpha = \delta$ 
5: end while

```

Algorithm 4 $[\eta] = \text{HURW_REP_RIGHT_GCD}(\zeta)$

```

1:  $\eta = \zeta_1$ 
2: for  $i = 2, \dots, L$  do ▷ repeated right GCD for  $\zeta \in \mathcal{H}^L$ 
3:    $\eta = \text{HURW\_RIGHT\_GCD}(\eta, \zeta_i)$ 
4: end for

```

A. Definition of Quaternionic Minkowski Reduction

Minkowski reduction is a successive strategy in which the generator matrix of a lattice is updated K times. In each step $k = 1, \dots, K$, the shortest lattice vector $\lambda^{\{k\}}$ which—together with $\lambda^{\{1\}}, \dots, \lambda^{\{k-1\}}$ —can be extended to a basis of the lattice is selected as the k^{th} basis vector. Hence, after the k^{th} reduction step, the generator matrix has the form

$$G_{\text{red}}^{\{k\}} = [\lambda^{\{1\}}, \dots, \lambda^{\{k-1\}}, \lambda^{\{k\}}, g_{k+1}^{\{k\}}, \dots, g_K^{\{k\}}], \quad (11)$$

i.e., it consists of the k shortest vectors that were suited to form a basis, and $K - k$ remaining ones. In step k , the shortest (suited) vector has to be found w.r.t. $G_{\text{red}}^{\{k-1\}}$, starting with $G_{\text{red}}^{\{0\}} = G$. After that, the basis vectors $g_k^{\{k-1\}}, \dots, g_K^{\{k-1\}}$ have to be updated in such a way that $g_k^{\{k\}} = \lambda^{\{k\}}$ and that $g_{k+1}^{\{k\}}, \dots, g_K^{\{k\}}$ —together with $\lambda^{\{1\}}, \dots, \lambda^{\{k\}}$ —span the same lattice as before. This procedure is called *basis update*.

In [11], Minkowski has given a condition for suited basis vectors in step k —restricting to real lattices $\Lambda(G) \in \mathbb{Z}^{N \times K}$. Generalizing Minkowski’s condition to the integer ring $\mathcal{I}$, a lattice vector $\lambda = G_{\text{red}}^{\{k-1\}} \zeta^{\{k\}}$, where $\zeta = [\zeta_1, \dots, \zeta_K]^T \in \mathcal{I}^K$ denotes the corresponding integer vector (coordinates) in (6), is suited for extension in step k if it is *primitive*, i.e.,

$$\|\text{GCD}_{\mathcal{I}}(\zeta_k, \dots, \zeta_K)\| = 1, \quad (12)$$

$\text{GCD}_{\mathcal{I}}$ denoting the *greatest common divisor* over $\mathcal{I}$. Thus, Minkowski reduction can be applied for lattices over Euclidean integer rings like $\mathbb{Z}$, $\mathcal{G}$, and $\mathcal{H}$, but not over $\mathcal{L}$, cf. Sec. II.

In Algorithm 3, the GCD of two Hurwitz integers $\alpha, \beta \in \mathcal{H}$ is calculated. The iterative variant of the Euclidean algorithm is applied, performing a (right) division with remainder according to Algorithm 2 in each step. Minkowski’s (generalized) condition (12) is then simply checked by the repeated calculation of the GCD for the relevant elements of $\zeta^{\{k\}}$ in Algorithm 4. A strategy to find the shortest vector $\lambda^{\{k\}}$ of $\Lambda(G_{\text{red}}^{\{k-1\}})$ also fulfilling (12) will be discussed in Sec. III-C.

B. Quaternionic Basis Update

For real and complex Minkowski reduction as discussed in [20] and [5], respectively, the basis update is enabled by repeated multiplication of the basis vectors with the matrix $U = \begin{bmatrix} \zeta_i/\eta & -\gamma_2 \\ \zeta_j/\eta & \gamma_1 \end{bmatrix}$, where $\zeta_i, \zeta_j \in \mathcal{I}$ denote two adjacent integers

Algorithm 5 $[\hat{\zeta}, P] = \text{PIVOTING}(\zeta)$

- 1: Find a permutation $\tilde{\zeta} = [\tilde{\zeta}_1, \dots, \tilde{\zeta}_L]^T \in \mathcal{I}^L$ of the integer vector $\zeta = [\zeta_1, \dots, \zeta_L]^T$ such that $\tilde{\zeta}_1 \neq 0$, $\tilde{\zeta}_2 \neq 0$, and $\|\tilde{\zeta}_1\| \leq \|\tilde{\zeta}_2\|$.
- 2: Represent the permutation via the permutation matrix P

of the vector ζ related to the shortest primitive vector in step k . Besides, γ_1 , γ_2 , and η have to be calculated with the extended Euclidean algorithm according to $\text{GCD}_{\mathcal{T}}(\zeta_i, \zeta_j) = \gamma_1 \cdot \zeta_i + \gamma_2 \cdot \zeta_j = \eta$. The authors then utilize the fact that $\det(U) = \zeta_i \eta^{-1} \gamma_1 + \zeta_j \eta^{-1} \gamma_2 = 1$ as long as the algebra is commutative—resulting in a unimodular update matrix for lattices over $\mathbb{Z}$ or $\mathcal{G}$. However, for lattices over $\mathcal{H}$ and its non-commutative algebra, an alternative approach has to be found.

The real-valued basis-update strategy from [15] is suited for adaption to the non-commutative algebra at hand. Its generalized variant utilizes the representation of a lattice vector according to $\lambda = G\zeta = \sum_{l=1}^L g_l \zeta_l$, cf. (6), L now denoting the rank of the lattice. Via the pivoting defined in Algorithm 5, the integer vector $\zeta \in \mathcal{I}^L$ is permuted to $\tilde{\zeta} \in \mathcal{I}^L$ with $\lambda = \tilde{G}\tilde{\zeta} = \sum_{l=1}^L \tilde{g}_l \tilde{\zeta}_l$, where $\tilde{G} = GP$ denotes the generator matrix permuted accordingly and P the related permutation matrix. The pivoting ensures that the first two elements of $\tilde{\zeta}$ are non-zero and that $\|\tilde{\zeta}_1\| \leq \|\tilde{\zeta}_2\|$. Hence, the division with small remainder $\tilde{\zeta}_2 = \gamma \cdot \tilde{\zeta}_1 + \rho$, cf. (4), can be performed. As the remainder is small, $\|\tilde{\zeta}_2 - \gamma \cdot \tilde{\zeta}_1\| \leq \|\tilde{\zeta}_1\|$. Consequently,

$$\lambda = (\tilde{g}_1^{\{0\}} + \tilde{g}_2^{\{0\}} \gamma^{\{0\}}) \cdot \tilde{\zeta}_1^{\{0\}} + \tilde{g}_2^{\{0\}} \cdot (\tilde{\zeta}_2^{\{0\}} - \gamma \tilde{\zeta}_1^{\{0\}}) + \sum_{l=3}^L \tilde{g}_l^{\{0\}} \tilde{\zeta}_l^{\{0\}}, \quad (13)$$

where the index $\{0\}$ indicates the initial step. The basis update is then carried out by iterative update of (13) according to

$$\tilde{\zeta}_2^{\{i+1\}} = \tilde{\zeta}_2^{\{i\}} - \gamma^{\{i\}} \cdot \tilde{\zeta}_1^{\{i\}}, \quad (14)$$

$$\tilde{g}_1^{\{i+1\}} = \tilde{g}_1^{\{i\}} + \tilde{g}_2^{\{i\}} \cdot \gamma^{\{i\}}, \quad (15)$$

followed by Algorithm 5 after each update to obtain the pivoted variants $\tilde{\zeta}^{\{i+1\}}$ and $\tilde{G}^{\{i+1\}} = G^{\{i+1\}} P^{\{i+1\}}$ for which $\lambda = \sum_{l=1}^L \tilde{g}_l^{\{i+1\}} \tilde{\zeta}_l^{\{i+1\}}$ still holds. After a finite number ω of iterations which is guaranteed by the division with small remainder, the lattice vector is represented by only a single term $\lambda = \tilde{g}_1^{\{\omega\}} \tilde{\zeta}_1^{\{\omega\}}$. Then, $\tilde{\zeta}_1^{\{\omega\}}$ is a linear combination of the entries of $\zeta^{\{0\}}$ and $\tilde{g}_1^{\{\omega\}}$ a linear combination of the vectors in G and since $\zeta^{\{0\}}$ is assumed to be primitive, i.e., $\|\text{GCD}_{\mathcal{T}}(\zeta_1^{\{0\}}, \dots, \zeta_L^{\{0\}})\| = 1$, $\|\tilde{\zeta}_1^{\{\omega\}}\| = 1$. Consequently, $[\lambda, \tilde{g}_2^{\{\omega\}}, \dots, \tilde{g}_L^{\{\omega\}}]$ forms a new basis of the lattice $\Lambda(G)$.

The basis update over $\mathcal{H}$ is implemented in Algorithm 6, additionally updating the integer transformation matrix T . After initial pivoting of ζ representing the (shortest) primitive vector, the division with remainder of ζ_2 and ζ_1 is performed (Algorithm 2). The remainder is assigned to ζ_2 and both g_1 and t_1 are updated via the factor γ , implementing the iterative basis update from (14) and (15), respectively. The algorithm terminates when ζ_1 is the only non-zero element in ζ . Then, g_1 and t_1 are updated one more time such that the final vectors are rotated by the correct unit element of $\mathcal{H}$ represented by ζ_1 .

Algorithm 6 $[G, T] = \text{HURW_BASIS_UPD}(\zeta, G, T)$

- 1: $[\zeta, P] = \text{PIVOTING}(\zeta)$ $\triangleright$ pivoting of ζ with Algorithm 5
- 2: $G = GP$, $T = TP$ $\triangleright$ sort G and T accordingly
- 3: **while** $\zeta_2 \neq 0$ **do**
- 4: $[\rho, \gamma] = \text{HURW_RIGHT_DIV_REM}(\zeta_2, \zeta_1)$
- 5: $\zeta_2 = \rho$ $\triangleright$ assign the remainder $\rho = \zeta_2 - \gamma \cdot \zeta_1$ to ζ_2
- 6: $g_1 = g_1 + g_2 \cdot \gamma$ $\triangleright$ update g_1 using γ
- 7: $t_1 = t_1 + t_2 \cdot \gamma$ $\triangleright$ update t_1 using γ
- 8: $[\zeta, P] = \text{PIVOTING}(\zeta)$ $\triangleright$ repeat pivoting after update
- 9: $G = GP$, $T = TP$
- 10: **end while**
- 11: $g_1 = g_1 \cdot \zeta_1$ $\triangleright$ final update (rotation) with ζ_1
- 12: $t_1 = t_1 \cdot \zeta_1$

Algorithm 7 $[G, T] = \text{HURW_MINK_REDUCT}(G)$

- 1: $T = I_K$ $\triangleright$ initially set T to identity matrix
- 2: **for** $k = 1, \dots, K$ **do** $\triangleright K$ reduction steps
- 3: $\zeta = \text{SHORTEST_VECTOR_GCD}(G, k)$ $\triangleright$ [1], [14]
- 4: $[G_{:,k:K}, T_{:,k:K}] = \text{HURW_BASIS_UPD}(\zeta_{k:K}, G_{:,k:K}, T_{:,k:K})$ $\triangleright$ Alg. 6
- 5: $G_{:,k} = G_{:,k} + G_{:,1:k-1} \cdot \tilde{u}_{:,1:k-1}$ $\triangleright$ contr. of $g_1, \dots, g_{k-1}$
- 6: $T_{:,k} = U_{:,k} + T_{:,1:k-1} \cdot \tilde{u}_{:,1:k-1}$
- 7: **end for**

C. Quaternionic Reduction Algorithm

Quaternionic Minkowski reduction over $\mathcal{H}$ is implemented in Algorithm 7, in which the integer transformation matrix T is initially set to the identity matrix (Line 1). Then, G and T are successively updated K times as stated in (11).

In each step k , the shortest primitive vector has to be found, cf. (12). This is performed by the procedure in Line 3. It can, e.g., be realized by a variant of the sphere-decoding algorithm [1] in which Algorithm 4 (check for primitive vector) is called every time a potential shortest vector has been found. If the check is successful the search can be terminated; otherwise, it has to be continued. If the classical real-valued sphere-decoding algorithm [1] is applied, the quaternionic generator matrix has to be transformed to its real-valued representation (10) and the vector candidates back to quaternionic form, see also [14, Algorithms 6 and 7].

After finding the shortest primitive vector, the basis has to be updated accordingly. This is performed by the call of Algorithm 6. However, in step k , the (already optimal) basis vectors $g_1 = \lambda^{\{1\}}, \dots, g_{k-1} = \lambda^{\{k-1\}}$ have to be kept constant, cf. (11). Only the vectors $g_k, \dots, g_K$ have to be updated such that $g_k = \lambda^{\{k\}}$ and the same lattice is spanned. Hence, the basis update as implemented by Algorithm 6 has to operate on the submatrices $G_{:,k:K}$ and $T_{:,k:K}$ and the subvector $\zeta_{k:K}$, respectively.² In this way, the k^{th} basis vector first reads $g_k = \sum_{l=k}^K g_l \zeta_l$ and the remaining columns $g_{k+1}, \dots, g_K$ are updated such that the same basis is present. Following this, the contribution of the first $k-1$ basis vectors to $\lambda^{\{k\}}$ still has to be incorporated. This is done in Line 5, resulting in $g_k = \lambda^{\{k\}} = g_k + \sum_{l=1}^{k-1} g_l \zeta_l$ as desired.

²Notation: $G_{:,k:K}$ means that the submatrix of G is selected in which all rows and the columns with index $k, \dots, K$ are contained. Moreover, $\zeta_{k:K}$ denotes the subvector of ζ containing only the elements with index $k, \dots, K$.

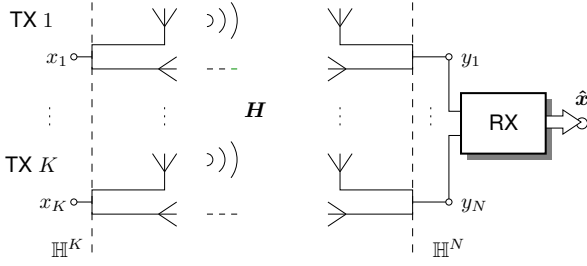


Fig. 1. Dual-polarized (quaternion-valued) MIMO uplink model with K transmitters (TX 1, ..., K) and a joint receiver (RX) with N antennas [14].

IV. APPLICATION IN DUAL-POLARIZED MIMO SYSTEMS

The performance of quaternionic Minkowski reduction is evaluated in this section. To this end, MIMO transmission with *dual-polarized* antennas [14], [17] is considered.

A. Dual-Polarized MIMO Systems

The *MIMO uplink channel* given dual-polarized antennas at transmitter and receiver side is depicted in Fig. 1, see also [14]. At each transmitter, a quaternionic symbol $x_k \in \mathcal{X} \subset \mathbb{H}$, $k = 1, \dots, K$, is radiated per time step, realized by transmission of the first two components by vertically and the last two ones by horizontally polarized waves. In this work, the signal constellation $\mathcal{X} \in \{\pm 1 \pm 1i \pm 1j \pm 1k\} \subset \mathcal{L} \subset \mathcal{H}$, is chosen, i.e., binary phase-shift keying (BPSK) in each component. The (total) variance of these symbols reads $\sigma_x^2 = 4 \cdot 1 = 4$.

The MIMO system equation

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n} \quad (16)$$

models the links between the transmitters and the central receiver. In particular, the vector $\mathbf{x} = [x_1 \dots, x_K]^T \in \mathcal{X}^K$ contains the K transmit symbols, $\mathbf{n} = [n_1 \dots, n_N]^T \in \mathbb{H}^N$ quaternionic noise samples with variance σ_n^2 per sample, and $\mathbf{y} = [y_1 \dots, y_N]^T \in \mathbb{H}^N$ the received values per dual-polarized antenna. The channel matrix $\mathbf{H} \in \mathbb{H}^{N \times K}$ consists of zero-mean unit-variance i.i.d. quaternionic channel coefficients with independent Gaussian distribution per component.

B. Lattice-Reduction-Aided Equalization

In the MIMO uplink scenario, the receiver can jointly process all incoming symbols, cf. Fig. 1. The easiest way to handle the multi-user interference is to equalize the channel matrix $\mathbf{H}$ by its Moore–Penrose inverse³ $\mathbf{H}^+ = (\mathbf{H}^H \mathbf{H})^{-1} \mathbf{H}^H$, usually resulting in large noise enhancement.

More enhanced is the concept of LRA linear equalization, in which the channel matrix is factorized according to [7], [14]

$$\underbrace{\mathbf{F}^H}_{\mathbf{G}_{\text{red}} \in \mathbb{H}^{N \times K}} = \underbrace{\mathbf{H}^{+H}}_{\mathbf{G} \in \mathbb{H}^{N \times K}} \cdot \underbrace{\mathbf{Z}^{-H}}_{\mathbf{T} \in \mathcal{L}^{K \times K}} \quad (17)$$

when applying the zero-forcing criterion.⁴ To that end, the Hermitian inverse of $\mathbf{H}$ is interpreted as the generator matrix

³The Hermitian matrix of the Moore–Penrose inverse is denoted by $\mathbf{H}^{+H} = (\mathbf{H}^+)^H$. If $\mathbf{H}$ is a square matrix, $\mathbf{H}^{+H} = \mathbf{H}^{-H} = (\mathbf{H}^{-1})^H$.

⁴The MMSE criterion can be considered by using *augmented* channel matrices instead, see [7], [14].

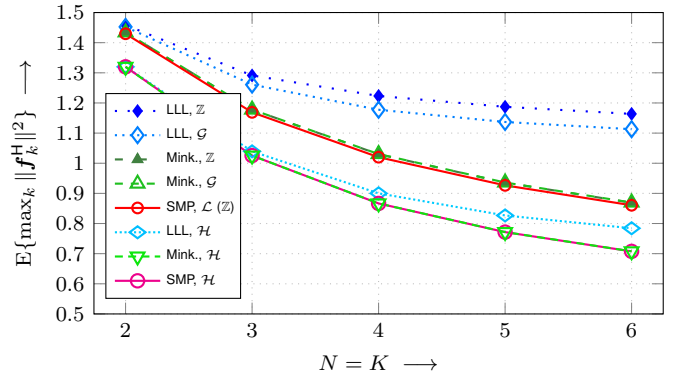


Fig. 2. Expectation of the maximum squared column norm of $\mathbf{F}^H$ obtained by solving the factorization task (17) with different lattice algorithms. The results are given for quaternionic channel matrices over the dimensions $N = K$.

of a lattice. Lattice reduction is then performed to shorten the column norms of the reduced basis $\mathbf{F}^H = [\mathbf{f}_1^H, \dots, \mathbf{f}_K^H]$ which correspond to the row norms of the linear equalization matrix $\mathbf{F}$. They directly determine the K noise enhancements via

$$\tilde{\sigma}_{n,k}^2 = \|\mathbf{f}_k^H\|^2 \cdot \sigma_n^2. \quad (18)$$

In the LRA receiver, the equalized symbols $\bar{\mathbf{y}} = \mathbf{F}\mathbf{y} \in \mathbb{H}^K$ are (individually) quantized to $\bar{\mathbf{x}} = [\mathbf{Q}_I(\bar{y}_1), \dots, \mathbf{Q}_I(\bar{y}_K)]^T \in \mathcal{L}^K$. In coded transmission, the quantization is replaced by decoding [7], [13], [19]. The vector $\bar{\mathbf{x}} = \mathbf{Z}\mathbf{x}$ contains linear combinations of the symbols in $\mathbf{x}$. Hence, the estimated transmit symbols are obtained by resolving the “integer interference” via $\hat{\mathbf{x}} = \mathbf{Z}^{-1}\bar{\mathbf{x}}$ without any further noise enhancement.

The minimum signal-to-noise-ratio (SNR), equivalently represented by $\max_k \|\tilde{\sigma}_{n,k}^2\|$ according to (18), dominates the transmission performance. Restricting to lattice basis reduction, this optimization task corresponds to the SBP given $\mathbf{G} = \mathbf{H}^{+H}$, i.e., it is optimally solved by Minkowski reduction. If the integer matrix $\mathbf{T} = \mathbf{Z}^{-H}$ can be non-unimodular, even better performance may be achieved by solving the SMP (i.e., the SIVP) instead. As mentioned in Sec. I, LRA and IF receivers can generally handle such matrices [7], [13], [19], but restrictions may apply to specific coding schemes [7].

C. Numerical Results

The proposed reduction algorithm is assessed by results obtained from numerical simulation over 10^5 quaternionic channel realizations. Complex and real algorithms employ the representations (8) and (9), respectively. The SMP over $\mathcal{H}$ has been solved based on (10), cf. [14]. All variants of LLL reduction are performed with the quality parameter $\delta = 1$.

1) *Noise Enhancement*: The expectation of $\max_k \|\mathbf{f}_k^H\|^2$, the crucial quality measure according to (18), is illustrated in Fig. 2 over the (quaternionic) dimensions $N = K$.

Starting with lattices over $\mathcal{L}$ and their equivalent representations, the SMP result ($\mathcal{L} \simeq \mathcal{G}^2 \simeq \mathbb{Z}^4$, cf. Sec. II) performs best as expected. The Minkowski reductions over $\mathcal{G}$ and $\mathbb{Z}$ perform almost the same but give a slightly worse result in comparison to the SMP one. The two kinds of LLL reduction over $\mathcal{G}$ and $\mathbb{Z}$ perform the worst, see also the comparisons in [13], [14].

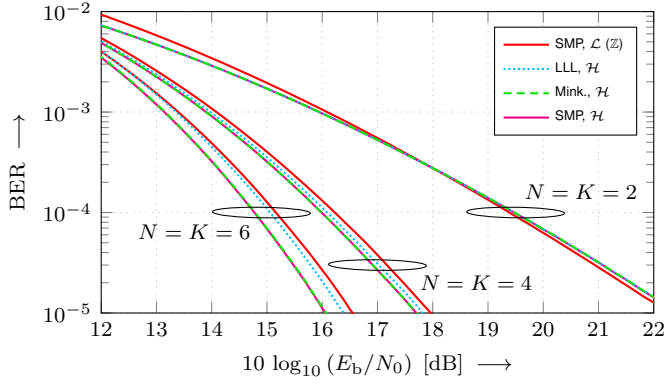


Fig. 3. Average BER over the SNR represented as energy per bit E_b (TX side) over the noise power spectral density N_0 . BPSK per quaternionic component with 10^3 symbols per channel realization. Quaternionic channel matrices with dimensions $N = K = 2, 4, 6$. Channel factorization according to (17).

TABLE I
PERCENTAGE OF QUATERNIONIC CHANNELS IN WHICH MINKOWSKI
REDUCTION IS OPTIMAL (SOLUTION TO SMP IS UNIMODULAR)

K	2	3	4	5	6
$\mathbb{Z}$	96.93 %	90.42 %	63.38 %	78.06 %	74.05 %
$\mathcal{G}$	96.93 %	90.42 %	63.37 %	78.05 %	74.01 %
$\mathcal{H}$	100 %	99.91 %	99.67 %	99.25 %	98.28 %

Lattices over $\mathcal{H}$ enable significantly better performance. For example, the SMP result over $\mathcal{H}$ has much lower average norms than over $\mathcal{L}$. This effect is known as *factorization gain* [13], [14]: Since $\mathcal{H}$ has a denser *sphere packing*, more potential candidate vectors can be used. In this context, quaternionic LLL reduction performs even better than the SMP result over $\mathcal{L}$. However, most important, there exists no relevant difference between Minkowski reduction over $\mathcal{H}$ and the related SMP.

The reason for that becomes apparent from Table I: For the vast majority of channel realizations, Minkowski reduction is already optimal in the sense that no non-unimodular solution performs better. For all other channels, the optimal non-unimodular result is still approximated quite well. This especially concerns lattices over $\mathcal{H}$ —more candidates may lead to a unimodular solution due to the denser packing.

2) *Uncoded Transmission Performance*: Fig. 3 visualizes the uncoded bit-error ratio (BER) over the SNR. For clarity, only quaternionic algorithms and the SMP over $\mathcal{L}$ are shown.

If $N = K = 2$, all algorithms nearly perform the same. The SMP over $\mathcal{L}$ even shows a slightly better curve than the schemes over $\mathcal{H}$. The reason for that is the quantization to $\mathcal{L}$ instead of $\mathcal{H}$ which is more robust against noise, cf. [14]. This property is only relevant in case of uncoded transmission.

For $N = K = 4$, the benefit of lattices over $\mathcal{H}$ becomes apparent. Here, the SMP over $\mathcal{L}$ shows the worst performance; even quaternionic LLL reduction over $\mathcal{H}$ performs better.

If $N = K = 6$, the gain of the SMP over $\mathcal{H}$ instead of $\mathcal{L}$ amounts to more than 0.5 dB in the high SNR regime. Once again, the loss of quaternionic Minkowski reduction is negligible since the optimal unimodular solution is very close or equal to the optimal non-unimodular one.

V. SUMMARY AND OUTLOOK

Minkowski reduction has been adapted to quaternionic lattices defined over Hurwitz integers. The proposed strategy enables a superior performance in comparison to real and complex Minkowski reduction and all kinds of LLL reduction. It even approaches the upper performance limit defined by the SMP.

Future work could concern performance bounds and complexity comparisons—the search for the shortest primitive vector in Minkowski reduction is NP-hard whereas LLL reduction has polynomial complexity. Besides, the adaption of Hermite–Korkine–Zolotareff (HKZ) reduction [20] could be addressed.

REFERENCES

- [1] E. Agrell, T. Eriksson, A. Vardy, and K. Zeger, “Closest point search in lattices,” *IEEE Trans. Inf. Theory*, vol. 48, no. 8, pp. 2201–2214, Aug. 2002.
- [2] H. Aslaksen, “Quaternionic determinants,” *Math. Intell.*, vol. 18, no. 3, pp. 57–65, 1996.
- [3] J. H. Conway and N. J. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY, USA: Springer, 1999.
- [4] J. H. Conway and D. A. Smith, *On Quaternions and Octonions*. Boca Raton, FL, USA: AK Peters/CRC Press, 2003.
- [5] L. Ding, Y. Wang, and J. Zhang, “Complex Minkowski reduction and a relaxation for near-optimal MIMO linear equalization,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 38–41, Feb. 2017.
- [6] L. Ding, K. Kansanen, Y. Wang, and J. Zhang, “Exact SMP algorithms for integer-forcing linear MIMO receivers,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6955–6966, Dec. 2015.
- [7] R. F.H. Fischer, S. Stern, and J. B. Huber, “Lattice-reduction-aided and integer-forcing equalization: Structures, criteria, factorization, and coding,” *Found. Trends Commun. Inf. Theory*, vol. 16, no. 1–2, pp. 1–155, 2019.
- [8] Y. H. Gan, C. Ling, and W. H. Mow, “Complex lattice reduction algorithm for low-complexity full-diversity MIMO detection,” *IEEE Trans. Signal Process.*, vol. 57, no. 7, pp. 2701–2710, Jul. 2009.
- [9] B. Helfrich, “Algorithms to construct Minkowski reduced and Hermite reduced lattice bases,” *Theor. Comput. Sci.*, vol. 41, pp. 125–139, 1985.
- [10] A. K. Lenstra, H. W. Lenstra, and L. Lovász, “Factoring polynomials with rational coefficients,” *Math. Ann.*, vol. 261, pp. 515–534, Dec. 1982.
- [11] H. Minkowski, “Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen,” *J. reine angew. Math.*, vol. 107, pp. 278–297, 1891.
- [12] S. S. Qureshi, S. Ali, and S. A. Hassan, “Optimal polarization diversity gain in dual-polarized antennas using quaternions,” *IEEE Signal Process. Lett.*, vol. 25, no. 4, pp. 467–471, Apr. 2018.
- [13] S. Stern, “Advanced equalization and coded-modulation strategies for multiple-input/multiple-output systems,” Ph.D. dissertation, Ulm University, May 2019.
- [14] S. Stern, C. Ling, and R. F.H. Fischer, “Algorithms and bounds for complex and quaternionic lattices with application to MIMO transmission,” *IEEE Trans. Inf. Theory*, vol. 68, no. 7, pp. 4491–4517, 2022.
- [15] B. L. van der Waerden, “Die Reduktionstheorie der positiven quadratischen Formen,” *Acta Math.*, vol. 96, no. 1, pp. 265–309, 1956.
- [16] C. Windpassinger and R. F.H. Fischer, “Low-complexity near-maximum-likelihood detection and precoding for MIMO systems using lattice reduction,” in *IEEE Inf. Theory Workshop (ITW)*, Paris, France, Mar. 2003, pp. 345–348.
- [17] B. J. Wysocki, T. A. Wysocki, and J. Seberry, “Modeling dual polarization wireless fading channels using quaternions,” in *Joint IST Workshop Mob. Future Symp. Trends Commun. (SympoTIC)*, Bratislava, Slovakia, Jun. 2006, pp. 68–71.
- [18] H. Yao and G. W. Wornell, “Lattice-reduction-aided detectors for MIMO communication systems,” in *IEEE Global Telecommun. Conf. (GLOBECOM)*, Taipei, Taiwan, Nov. 2002, pp. 424–428.
- [19] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, “Integer-forcing linear receivers,” *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7661–7685, Dec. 2014.
- [20] W. Zhang, S. Qiao, and Y. Wei, “HKZ and Minkowski reduction algorithms for lattice-reduction-aided MIMO detection,” *IEEE Trans. Signal Process.*, vol. 60, no. 11, pp. 5963–5976, Nov. 2012.