15 June 2023

Multilevel lattice codes from Hurwitz quaternions

Juliana Souza
julianagfs@ime.unicamp.br

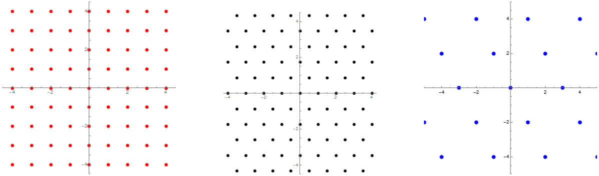
Sueli Costa
IMECC

Cong Ling
Imperial College

Preliminaries

Definition 1 (Lattice)

An N-dimensional **lattice** Λ *can be define as a discrete subgroup of* $\mathbb{R}^N$ *which is closed under reflection and ordinary vector addition, i.e.,* $\forall\lambda \in \Lambda$*, we have* $-\lambda \in \Lambda$*, and* $\forall\lambda_1, \lambda_2 \in \Lambda$ *we have* $\lambda_1 + \lambda_2 \in \Lambda$.



(a) $\mathbb{Z}_2$ (b) A_2 (c) Λ

Figure 1: Lattices in $\mathbb{R}^2$

Preliminaries

Definition 2 (Construction A [1])

Let $q > 1$ be an integer. Let $k, N \in \mathbb{N}$ be integers such that $k \leq N$ and let G be $N \times k$ a generator matrix of a linear code over $\mathbb{Z}_q$. Construction A consists of the following steps:

1. *Consider the linear code $\mathcal{C} = \{x = G \odot y : y \in \mathbb{Z}_q^k\}$, where all operations are over $\mathbb{Z}_q$.*
2. *"Expand" $\mathcal{C}$ to a lattice in $\mathbb{Z}^N$ defined as:*

$$\Lambda_A(\mathcal{C}) = \{x \in \mathbb{Z}^N : x \mod q \in \mathcal{C}\} = \mathcal{C} + q\mathbb{Z}^N.$$

Preliminaries

Theorem 1 (Chinese Remainder Theorem)

Let R be a commutative ring, and $I_1, \ldots, I_k$ be relatively prime ideals in R. Then,

$$R/\cap_{j=1}^{k} I_j \cong (R/I_1) \times \ldots \times (R/I_k).$$

Proposition 1 ([2])

Let $p_1, \ldots, p_k$ be a collection of distinct primes and let $q = \prod_{j=1}^{k} p_j$. There exists a ring isomorphism

$$\phi : \mathbb{Z}_q \to \mathbb{Z}_{p_1} \times \ldots \times \mathbb{Z}_{p_k}.$$

Preliminaries

Definition 3 (Construction π_A [2])

Let $p_1, ..., p_k$ be distinct primes. Let l_j, N be integers such that $l_j \leq N$ and let G_j be a generator matrix of a (N, l_j)-linear code over $\mathbb{Z}_{p_j}$ for $j \in \{1, ..., k\}$. Construction π_A consists of the following steps,

1. *Define the discrete codebooks $\mathcal{C}_j = \{x = G_j \odot u : u \in \mathbb{Z}_{p_j}^{l_j}\}$ for $j \in \{1, ..., k\}$.*
2. *Construct $\mathcal{C} = \phi^{-1}(\mathcal{C}_1, ..., \mathcal{C}_k)$ where $\phi^{-1} : \mathbb{Z}_{p_1}^N \times ... \times \mathbb{Z}_{p_k}^N \to \mathbb{Z}_q^N$ is a ring isomorphism.*
3. *Tile $\mathcal{C}$ to the entire $\mathbb{R}^N$ to form $\Lambda_{\pi_A}(\mathcal{C}) = \mathcal{C} + q\mathbb{Z}^N = \Lambda_A$.*

Preliminaries

Example 1

Let us consider a two-level example where $p_1 = 3$ *and* $p_2 = 2$. *One has* $\mathbb{Z}^2/6\mathbb{Z}^2 \cong \mathbb{Z}_3^2 \times \mathbb{Z}_2^2$ *from the CRT we have that a ring isomorphism can be given by*

$$\phi^{-1}(c_1, c_2) = (4c_1 + 3c_2) \mod 6.$$

where $c_1 \in \mathbb{Z}_3^2$ *e* $c_2 \in \mathbb{Z}_2^2$.
Using the steps of Construction π_A *we have that, we define the codes,*

$$\mathcal{C}_1 = \{x = [2 \;\; 2]^T u; u \in \mathbb{Z}_3\} \; and \; \mathcal{C}_2 = \{x = [1 \;\; 0]^T u; u \in \mathbb{Z}_2\}.$$

Preliminaries

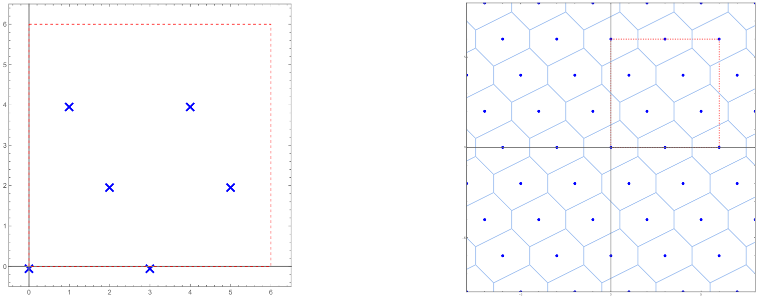


Figure 2: On the left, construction of $\mathcal{C}$ (step 2.) and on the right, tiling of $\mathcal{C}$ to obtain $\Lambda_A(\mathcal{C}) = \mathcal{C} + 6\mathbb{Z}^2$ (step 3.).

Quaternion Algebras

Definition 4 (Quaternion algebra)

Let $\mathbb{F}$ be a field with characteristics different from 2. We call quaternion algebra over $\mathbb{F}$ any (associative) algebra over $\mathbb{F}$ admitting a basis of four elements, denoted $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$, which satisfy the following relations: 1 is the neutral element for multiplication, and

$$\mathbf{i}^2 = a \cdot 1, \quad \mathbf{j}^2 = 1 \cdot b \quad \mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$

for some non-zero elements $a, b \in \mathbb{F}$. We can denote this algebra $\mathbb{F}$ by $\left(\frac{a, b}{\mathbb{F}}\right)$ or in short by $(a, b)_{\mathbb{F}}$. Element 1 is usually omitted in products; in particular, we denote $x \cdot 1 = x$ for all $x \in \mathbb{F}$, which leads to identifying $\mathbb{F}$ with a subfield of $\left(\frac{a, b}{\mathbb{F}}\right)$.

Quaternion Algebras

- The conjugate of a quaternion $x = x_0 + x_1\mathbf{i} + x_2\mathbf{j} + x_3\mathbf{k}$ $\in (a, b)_{\mathbb{F}}$ is the quaternion $\overline{x} = x_0 - x_1\mathbf{i} - x_2\mathbf{j} - x_3\mathbf{k} \in (a, b)_{\mathbb{F}}$.
- We also have that for all $x \in (a, b)_{\mathbb{F}}$, $Tr(x) = x + \overline{x}$ and $N(x) = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$ which we call respectively, **trace** and **norm** of x, are elements of $\mathbb{F}$.
- The typical example of a division algebra over quaternions is due to Hamilton (1843):

$$\mathbb{H} = (-1, -1)_{\mathbb{R}} = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} : (a_0, a_1, a_2, a_3) \in \mathbb{R}\}.$$

Quaternion Algebras

Definition 5 (Order)

An order $O \subseteq B$ is a finitely generated submodule that is also a subring of B.

Proposition 2 ([3], p.245)

Let O and O' be two orders of $B = \mathbb{H}$. If $O \supseteq O'$, then $discrd(O)$ divides $discrd(O')$. Moreover, if $O \supseteq O'$ and $discrd(O) = discrd(O')$, then $O = O'$.

Definition 6 (Maximal Order)

An order $O \subseteq B$ is maximal if it is not properly contained in another order.

Quaternion Algebras

Example 2

Let $B = (-1,-1)_{\mathbb{R}} = \mathbb{H}$, *and let*

$$\mathcal{L} = \{a_1 1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k} | a_1, ..., a_4 \in \mathbb{Z}\},$$

where $(1, \mathbf{i}, \mathbf{j}, \mathbf{k})$ *is the standard basis of* B*.We have that it is an order of* B *with* $discrd(\mathcal{L}) = 4$*, but is not a maximal order. This is called the* **Lipschitz order**. *We can add to* $\mathcal{L}$ *the element* $\varepsilon = \frac{1}{2}(1 + \mathbf{i} + \mathbf{j} + \mathbf{k})$ *and verify that*

$$\mathcal{H} = \{b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\varepsilon | b_1, ..., b_4 \in \mathbb{Z}\}$$

is an order with reduced discriminant $discrd(\mathcal{H}) = 2$*, and it is a maximal order over* $\mathbb{H}$*. The order* $\mathcal{H}$ *is called the* **Hurwitz order** *first described in [4] (1919).*

Hurwitz Quaternions

Lemma 1 (Hurwitz order is left-norm Euclidean, [3])

For all $\alpha, \beta \in \mathcal{H}$ *with* $\beta \neq 0$, *there exists* $\mu, \rho \in \mathcal{H}$ *such that,*

$$\alpha = \mu\beta + \rho$$

and $N(\rho) < N(\beta)$.

Proposition 3 ([3])

Every left ideal $\mathfrak{a} \subset \mathcal{H}$ *is left-principal, i.e., there exists* $\beta \in \mathfrak{a}$ *such that* $\mathfrak{a} = \beta\mathcal{H}$.

Definition 7 (Left divides)

Let $\alpha, \beta \in \mathcal{H}$. *We say* β *left divides* α *(or* α *is a left multiple of* β*) and write* $\beta|_L\alpha$ *if there exists* $\gamma \in \mathcal{H}$ *such that* $\alpha = \gamma\beta$.

Hurwitz quaternions

Proposition 4 (Bézout's theorem, [3])

For all $\alpha, \beta \in \mathcal{H}$ not both zero, there exists $\mu, \gamma \in \mathcal{H}$ such that $\mu\alpha + \gamma\beta = \delta$ where δ is a left greatest common divisor of α, β.

Proposition 5 ([3])

Let $p \in \mathbb{Z}$ be prime. Then there exists $\pi \in \mathcal{H}$ such that $N(\pi) = p$.

Definition 8 (Prime ideal)

A two-sided ideal $\mathfrak{P} \subseteq O$ is said to be a prime ideal if $\mathfrak{P} \neq O$ and, for ideals $\mathfrak{U}, \mathfrak{B} \subseteq O$, we have, $\mathfrak{U} \cdot \mathfrak{B} \subseteq \mathfrak{P} \Rightarrow \mathfrak{U} \subseteq \mathfrak{P}$ or $\mathfrak{B} \subseteq \mathfrak{P}$.

Chinese Remainder Theorem

Theorem 2 ([5])

Let O be a maximal order, and let $\mathfrak{P}_1, ..., \mathfrak{P}_n \subseteq O$ be distinct prime (two-sided) ideals. Let $\mathfrak{P} = \prod_{i=1}^{n} \mathfrak{P}_i^{a_i}$, $a_i \in \mathbb{Z}, i = 1, ..., n$. If $a_i \geq 0$ for all $i = 1, ..., n$ then there is a ring isomorphism

$$O/\mathfrak{P} \cong (O/\mathfrak{P}_1^{a_1}) \times ... \times (O/\mathfrak{P}_n^{a_n}).$$

Theorem 3

Let O be a maximal order and $\mathfrak{P}$ be a two-sided prime ideal then exist an isomorphism,

$$O/\mathfrak{P} \cong O/\mathfrak{a} \times O/\mathfrak{b},$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are completely prime left-ideals in O.

Multilevel Lattice Code

Definition 9 (Construction π_A over Hurwitz quaternions)

Let O be a maximal order, let $p_1, ..., p_k$ be distinct primes, such that $\mathfrak{P}_j = \langle p_j \rangle$, for $j = 1, ..., k$, and $\mathfrak{P}_1, ..., \mathfrak{P}_k$ be distinct prime ideals of Λ. Let l_j, N be integers such that $l_j \leq N$ and let G_j be a generator matrix of a (N, l_j)-linear code for $j \in \{1, ..., k\}$. Construction π_A over Hurwitz orders consists of the following steps,

1. *Define the discrete codebooks $\mathcal{C}_j^{(1)} = \{G_j \odot u : u \in O/\mathfrak{a}_j\}$ and $\mathcal{C}_j^{(2)} = \{G_j \odot u : u \in O/\mathfrak{b}_j\}$ for $j \in \{1, ..., k\}$.*
2. *Construct $\mathcal{C} = \Psi^{-1}(\mathcal{C}_1^{(1)}, \mathcal{C}_1^{(2)}, ..., \mathcal{C}_k^{(1)}, \mathcal{C}_k^{(2)})$ where Ψ is a ring isomorphism.*
3. *Tile $\mathcal{C}$ to the entire space to form $\Lambda(\mathcal{C}) = \mathcal{C} + \mathfrak{P}^N$.*

Multilevel Lattice Code

- Using **Theorem 3** we can obtain an isomorphism that better "decomposes" the levels of the constructed lattice.
- Consider $p_1, \ldots, p_n$ rational primes, put $q = p_1 \cdot \ldots \cdot p_n$.
- We know that for each prime we have $p_i = N(\pi_i), \pi_i \in \mathcal{H}, i = 1, \ldots, n$
- By, **Theorem 2** and **Theorem 3** we can define the following ring isomorphism:

$$\begin{aligned} \mathcal{H}/q\mathcal{H} &\cong \mathcal{H}/\mathfrak{P}_1 \times \ldots \times \mathcal{H}/\mathfrak{P}_n \\ &\cong \mathcal{H}/\mathfrak{a}_1 \times \mathcal{H}/\mathfrak{b}_1 \times \ldots \times \mathcal{H}/\mathfrak{a}_n \times \mathcal{H}/\mathfrak{b}_n. \end{aligned}$$

Multilevel Lattice Code

Example 3

- *Consider* $p_1 = 3, p_2 = 5$ *with* $\mathfrak{P}_1 = \langle 3 \rangle$ *and* $\mathfrak{P}_2 = \langle 5 \rangle$*, as we can write* $3 = (1 + \mathbf{i} + \mathbf{j})(1 - \mathbf{i} - \mathbf{j})$ *and* $5 = (1 + 2\mathbf{i})(1 - 2\mathbf{i})$*, then we have* $q = 3 \times 5 = 15$ *with* $\mathfrak{P} = 15\mathcal{H}$*,* $\pi_1 = 1 + \mathbf{i} + \mathbf{j}$*,* $\overline{\pi}_1 = 1 - \mathbf{i} - \mathbf{j}, \pi_2 = 1 + 2\mathbf{i}$ *and* $\overline{\pi}_2 = 1 - 2\mathbf{i}$
- *we can obtain an isomorphism,*

$$\Psi : \mathcal{H}/\mathfrak{P} \to \mathcal{H}/\mathfrak{a}_1 \times \mathcal{H}/\mathfrak{b}_1 \times \mathcal{H}/\mathfrak{a}_2 \times \mathcal{H}/\mathfrak{b}_2$$
$$\alpha \mapsto (\alpha \mod \pi_1, \alpha \mod \overline{\pi}_1, \alpha \mod \pi_2, \alpha \mod \overline{\pi}_2).$$

Multilevel Lattice Code

- For Construction π_A we need the inverse isomorphism,

$$\Psi^{-1} : \mathcal{H}/\mathfrak{a}_1 \times \mathcal{H}/\mathfrak{b}_1 \times \mathcal{H}/\mathfrak{a}_2 \times \mathcal{H}/\mathfrak{b}_2 \to \mathcal{H}/\mathfrak{P}$$

- For that, as $q = p_1.p_2 = p_2.p_1$ we can define

$$\begin{aligned}
\mu_1 &= \pi_1^{-1} q = \pi_1^{-1}.(p_1.p_2) = p_2.\overline{\pi}_1 = 5 - 5\mathbf{i} - 5\mathbf{j} \\
\mu_2 &= \overline{\pi}_1^{-1} q = \overline{\pi}_1^{-1}.(p_1.p_2) = p_2.\pi_1 = 5 + 5\mathbf{i} + 5\mathbf{j} \\
\mu_3 &= \pi_2^{-1} q = \pi_2^{-1}.(p_2.p_1) = p_1.\overline{\pi}_2 = 3 - 6\mathbf{i} \\
\mu_4 &= \overline{\pi}_2^{-1} q = \overline{\pi}_2^{-1}.(p_2.p_1) = p_1.\pi_2 = 3 + 6\mathbf{i}.
\end{aligned}$$

Multilevel Lattice Code

- By Bézout identity, there are $\gamma_1, \gamma_2, \gamma_3, \gamma_4 \in \mathcal{H}$ such that

$$\mu_1\gamma_1 + \mu_2\gamma_2 + \mu_3\gamma_3 + \mu_4\gamma_4 = 1$$

- We can put $\gamma_1 = \mathbf{j} + \mathbf{k}, \gamma_2 = 2\mathbf{j} + \mathbf{k}, \gamma_3 = 3\mathbf{i}$ and $\gamma_4 = -2 + \mathbf{i} - 3\mathbf{j} + \mathbf{k}$, so

$$\Psi^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (\mu_1\gamma_1\alpha_1 + \mu_2\gamma_2\alpha_2 + \mu_3\gamma_3\alpha_3 + \mu_4\gamma_4\alpha_4) \mod 15\mathcal{H}$$

- Therefore,

$$\begin{aligned}\Psi^{-1}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = {} & [(5 - 5\mathbf{i} + 10\mathbf{j})\,\alpha_1 + (-10 + 5\mathbf{i} + 5\mathbf{j} + 15\mathbf{k})\,\alpha_2 + \\ & + (18 + 9\mathbf{i})\,\alpha_3 + (-12 - 9\mathbf{i} - 15\mathbf{j} - 15\mathbf{k})\,\alpha_4] \mod 15\mathcal{H}\end{aligned}$$

Multilevel Decoder

- The received point $y \in \mathbb{R}^N$ at the receiver is given by

$$y = x + n$$

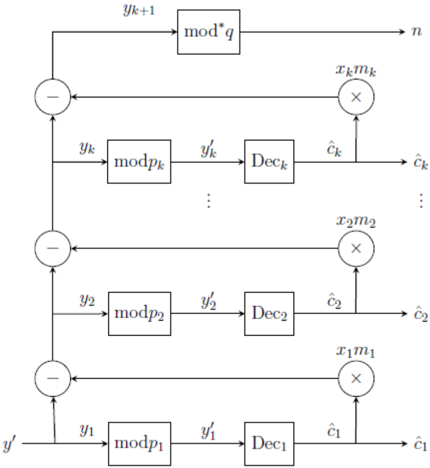
where $x \in \Lambda_{\pi_A}(\mathcal{C})$ and $n \in \mathbb{R}^N$ is the noise.

- As x belongs to Construction π_A lattice, it can be decomposed as

$$x = (x_1 m_1 c_1 + x_2 m_2 c_2 + ... + x_k m_k c_k) \mod q + q\tilde{z}$$

where $c_i = G_i u_i$, for $i = 1, ..., k$ and $q = \prod_{j=1}^{k} p_j$.

Multilevel Decoder

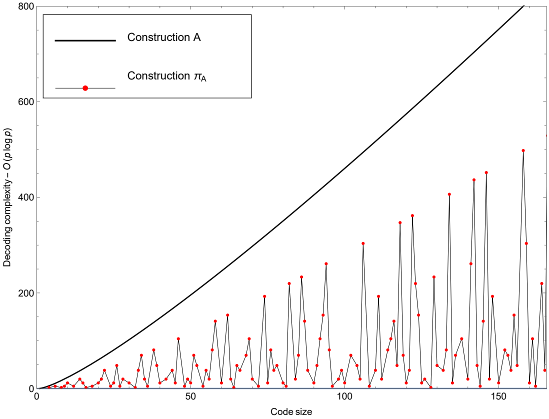


Usefulness of Construction π_A over Hurwitz quaternions

p	Code Size	Time using Construction A decoder	Time using Construction π_A decoder
3	81	0.05159	0.00504
5	625	5.86613	0.00511
7	2401	105.209	0.00516
11	14641	4054.63	0.00548

Table 1: Time comparison using decoding algorithm in Construction A and Construction π_A for codes of the same size, the time was measured in seconds. The Construction A lattice uses a linear code over $\mathbb{Z}_p^4$ while the Construction π_A lattice uses a code over $p\mathcal{H}$.

Usefulness of Construction π_A over Hurwitz quaternions



References

- S. Costa, F. Oggier *et al.*, *Lattices Applied to Coding for Realiable and Secure Communications*. Springer, 2017.
- Y.-C. Huang and K. R. Narayanan, “Construction π_A and π_D lattices: Construction, goodness, and decoding algorithms,” *IEEE Transactions on Information Theory*, vol. 63, no. 9, pp. 5718–5733, 2017.
- J. Voight, *Quaternion algebras*. Springer Nature, 2021.
- A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*. Springer, 1919.
- I. Reiner, *Maximal Orders*. Academic Press London, 1975.

Thank you for your attention!