On the Densest Lattices from Number Fields and Division Algebras

Carina Alves, carina@rc.unesp.br, **UNESP - Rio Claro - SP - Brasil**

Sueli I. R. Costa, Cintya W.O. Benedito, Nelson G.B. Jr.
Imecc-UNICAMP, Campinas - SP - Brasil

XXI Coloquio Latinoamericano de Álgebra - Buenos Aires, Argentina - 2016

I. Introduction

- Signal constellations having a lattice structure have been studied for transmitting data over communications channel.
- In particular, lattices arising from algebraic number fields and division algebras have turned out to be priceless in the code design.
- In order to minimize the probability of error in communication channels with a single antenna there are in the literature many constructions of lattices via number fields.

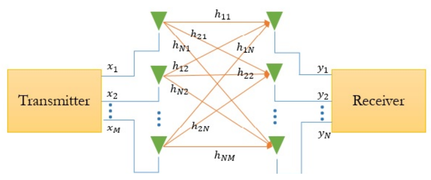
1. M. Craig, A Cyclotomic Construction for $Leech's$ Lattice, *Mathematika*, 25, pages 236–241, 1978.
2. M. Craig, Extreme Forms and Cyclotomy, *Mathematika*, 25, pages 44–56, 1978.
3. E. Bayer Fluckiger, Lattices and Number Fields, *Contemp. Math*, 241, pages 69–84, 1999.

Channels with a Single Antenna: Disadvantages

Transmit data by atmospheric means involving many problems inherent to it, such as:

- meteorological phenomenon;
- blockages caused by buildings;
- others objects in the signal propagation path.

II. Multiple Input Multiple Output (MIMO)



Codes designed for this channel are called space-time codes.

The code $\mathcal{C}$ is $\mathcal{C} = \left\{ X = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \mid x_1, x_2, x_3, x_4 \in \mathbb{C} \right\}$, where x_i are information symbols.

- The pairwise probability of error is bounded by

$$P(X \to \hat{X}) \leq \frac{\text{const}}{|\det(X - \hat{X})|^{2M}},$$

where M is the number of received antennas.

- $\det(X_i - X_j) \neq 0,\ \forall X_i \neq X_j,\ X_i, X_j \in \mathcal{C}$.
- If $\mathcal{C}$ is taken inside an algebra of matrices, the problem simplifies to $\det(X) \neq 0,\ \ 0 \neq X \in \mathcal{C}$.
- Division algebras are rings which every nonzero element has a multiplicative inverse.

III. Goal: Construction of dense lattices in dimension 4n

Codewords are usually constructed over the complex field. However for ultra wideband communication, one needs to design them over the real field.

- B. A. Sethuraman, F. Oggier, Constructions of Orthonormal Lattices and Quaternion Division Algebras for Totally Real Number Fields, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes Lecture Notes in Computer Science*, v. 4851, p. 138–147, 2007.

$$\begin{array}{ccc} \mathcal{A} = (a,b)_{\mathbb{K}} & \rightsquigarrow & \text{quaternion division algebra} \\ \Big| 4 & & \\ \mathbb{K} = \mathbb{Q}(\zeta_s + \zeta_s^{-1}) & \rightsquigarrow & \text{maximal real subfield of} \mathbb{Q}(\zeta_s) \\ \Big| n = \frac{\phi(s)}{2} & & \\ \mathbb{Q} & & \end{array}$$

IV. Lattices

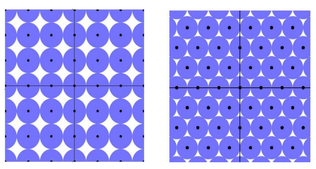
- A lattice Λ is a discrete additive subgroup of $\mathbb{R}^n$ generated by integer combinations of n linearly independents vectors $v_1, \cdots, v_n \in \mathbb{R}^n$.
- A matrix M whose rows are these vectors is said to be a generator matrix for Λ and the matrix

$$G = MM^t = (< v_i, v_j >)_{i,j=1}^m$$

is called a Gram matrix for the lattice Λ. The determinant of Λ is given by $det\Lambda = detG$.

- The packing density of a lattice is the proportion of the space $\mathbb{R}^n$ covered by the non-overlapping spheres of maximum radius centered at the points of Λ. The densest possible lattice packing have only be determined in dimensions 1 to 8 and 24.

$\mathbb{Z}^2$ $\quad$ A_2



V. Quaternion Algebras

- A quaternion algebra $\mathcal{A} = (a,b)_{\mathbb{K}}$ over a number field $\mathbb{K}$ is an algebra of dimension 4 with basis $\{1, i, j, k\}$ satisfying $i^2 = a,\ j^2 = b$ and $k = ij = -ji$, where $a, b \in \mathbb{K} \setminus \{0\}$.
- If $x \in \mathcal{A}$, let us say

$$x = x_1 + x_2 i + x_3 j + x_4 k,$$

with $x_1, x_2, x_3, x_4 \in \mathbb{K}$, then

$$\overline{x} = x_1 - x_2 i - x_3 j - x_4 k$$

is called conjugated of x.

- For $x \in \mathcal{A}$, the reduced trace and reduced norm of x are defined as

$$Trd(x) = x + \overline{x} \ \text{ and } \ Nrd(x) = x\overline{x},$$

respectively.

- An element of $\mathcal{A} = (a,b)_{\mathbb{K}}$ is such that

$$x = x_0 + x_1 i + x_2 j + x_3 k = \begin{pmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{pmatrix},$$

$x_0, x_1, x_2, x_3 \in \mathbb{K}$.

When a quaternion algebra is a division algebra?

Proposition 1. [1] A quaternion algebra $\mathcal{A} = (a,b)_{\mathbb{K}}$ is a division algebra if only if $b \notin N_{\mathbb{K}(\sqrt{a})/\mathbb{K}}(\mathbb{K}(\sqrt{a}))$.

V.1- Order

- Let R be a ring with field of fractions $\mathbb{K}$, and let $\mathcal{A} = (a,b)_{\mathbb{K}}$ be a quaternion algebra over $\mathbb{K}$. An order $\mathcal{O}$ in $\mathcal{A}$ is a finitely generated R-module such that $\mathcal{A} = \mathbb{K}\mathcal{O}$.

So $\mathcal{O} = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k : \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in R\}$, is an order in $\mathcal{A}$ denoted by $\mathcal{O} = (a,b)_R$.

- Let $\mathcal{O}$ be an R-order in a quaternion algebra $\mathcal{A}$. The reduced discriminant of $\mathcal{O}$, $\mathcal{D}(\mathcal{O})$, is an ideal generated by $\{\{x_1, x_2, x_3\} : x_1, x_2, x_3 \in \mathcal{O}\}$, where

$$\{x_1, x_2, x_3\} = (x_1x_2 - x_2x_1)\overline{x_3} - x_3(\overline{x_1x_2 - x_2x_1}).$$

- A quaternion algebra $\mathcal{A} = (a,b)_{\mathbb{K}}$ is said to be ramified in the ideal $\wp$ of $\mathbb{O}_{\mathbb{K}}$ if and only if $\left(\frac{a,b}{\wp}\right) = -1$, i.e., $z^2 = ax^2 + by^2 (mod \wp)$ has trivial solution in $\mathbb{K}^3$.

- Let $Ram(\mathcal{A})$ be the set of prime ideals $\wp$ where $\mathcal{A}$ is ramified . The discriminant of $\mathcal{A}$ is the ideal defined by

$$\mathcal{D}(\mathcal{A}) = \prod_{\wp \in Ram(\mathcal{A})} \wp$$

V.2- Maximal Order

- An order $\mathcal{M}$ in a quaternion algebra $\mathcal{A}$ is maximal if $\mathcal{M}$ is not properly contained in another order of $\mathcal{A}$.

Proposition 2. [2] An order $\mathcal{M}$ is maximal in the quaternion algebra $\mathcal{A}$ if and only if its discriminant is equal to the discriminant of $\mathcal{M}$, i.e, $\mathcal{D}(\mathcal{M}) = \mathcal{D}(\mathcal{A})$.

VI. From Quaternion Algebra to Ideal Lattices

- Let $\mathbb{K}$ be a totally real number field with degree n and $\mathcal{A}$ be a quaternion algebra over $\mathbb{K}$.
- If $\mathcal{I}$ is an ideal in $\mathcal{A}$ and α is a totally positive element in $\mathbb{K}$, then we have a positive definite symmetric bilinear form $b_\alpha : \mathcal{I} \times \mathcal{I} \to \mathbb{Q}$ given by

$$b_\alpha(x,y) = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(x\overline{y})).$$

In this case, we let $\Lambda = (\mathcal{I}, \alpha)$ denote the ideal lattice associated to b_α.

- Moreover, if $\{w_1, \cdots, w_{4n}\}$ is a $\mathbb{Z}$-basis of the ideal lattice Λ then the Gram matrix of Λ is

$$G = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i\overline{w_j})).$$

Proposition 3. [3] Let $\mathbb{K}$ be a totally real number field and $\mathcal{A}$ be a quaternion algebra over $\mathbb{K}$. If $\mathcal{I} \subseteq \mathcal{M}$ is an ideal of a maximal quaternion order $\mathcal{M}$ of $\mathcal{A}$ and α is a totally positive element in $\mathbb{K}$ so that $\Lambda = (\mathcal{I}, \alpha)$ is a lattice, then

$$det(G) = d_{\mathbb{K}}^4 N(\alpha)^4 N_{\mathbb{K}}(Nrd(\mathcal{I}))^4 (\mathcal{D}(\mathcal{M})^2),$$

where G is the Gram matrix of Λ.

VII. Construction of Lattices via Quaternion Algebras

A necessary but not sufficient condition for the ideal lattice Λ to be isomorphic to $(\sqrt{c}\Lambda')^n$ a scaled version of a lattice Λ' with scale $c \in \mathbb{Z}$ is that

$$det(\Lambda) = c^n det(\Lambda'),$$

since the Gram matrix of $(\sqrt{c}\Lambda')^n$ is cG, where G is the Gram matrix of Λ'.

VII.1- Construction of E_8

- $\mathcal{A} = (-1,-1)_{\mathbb{K}}$, $\mathbb{K} = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$.
- $\mathcal{M}$ is a maximal quaternion order in $\mathcal{A}$ characterized by the basis

$$B = \left\{1, \frac{1+i}{\sqrt{2}}, \frac{1+j}{\sqrt{2}}, \frac{1+i+j+k}{2}\right\}.$$

In fact,

$$\mathcal{D}(\mathcal{M}) = \langle 1 \rangle = \mathcal{D}(\mathcal{A}).$$

Now, in order to fulfill the condition of the same determinant, for $\Lambda' = E_8$, we need to find $\alpha \in \mathbb{K}$ totally positive and $\mathcal{I} \subseteq \mathcal{M}$ an ideal such that

$$c^8 = d_{\mathbb{K}}^4 N(\alpha)^4 N_{\mathbb{K}}(Nrd(\mathcal{I}))^4 (\mathcal{D}(\mathcal{M})^2),$$

since $det(E_8) = 1$. Thus,

$$c^8 = (2^3)^4 N(\alpha)^4 N(Nrd(\mathcal{I}))^4.$$

If we take $\mathcal{I} = \mathcal{M}$,

$$c^8 = 2^{12} N(\alpha)^4$$

$$c = 2^2 \ \longrightarrow \ N(\alpha) = 2.$$

- $\alpha = 2 - (\zeta_8 + \zeta_8^{-1})$ is a totally positive element in $\mathbb{K}$ such that $N(\alpha) = 2$. Then $\Lambda = (\mathcal{I}, \alpha)$ is an ideal lattice with $\mathbb{Z}-$basis B' given by

$$B' = \left\{1, \sqrt{2}, \frac{1+i}{\sqrt{2}}, 1+i, \frac{1+j}{\sqrt{2}}, 1+j, \frac{1+i+j+k}{2}, \frac{1+i+j+k}{\sqrt{2}}\right\},$$

Moreover, the Gram matrix of $\Lambda = (\mathcal{I}, 2-(\zeta_8+\zeta_8^{-1}))$ is given by

$$G = Tr_{\mathbb{K}/\mathbb{Q}}(\alpha Trd(w_i\overline{w_j})) = \begin{pmatrix} 8 & 8 & 4 & 8 & 4 & 8 & 4 & 4 \\ 8 & 16 & 8 & 8 & 8 & 8 & 4 & 8 \\ 4 & 8 & 8 & 8 & 4 & 4 & 4 & 8 \\ 8 & 8 & 8 & 16 & 4 & 8 & 8 & 8 \\ 4 & 8 & 4 & 4 & 8 & 8 & 4 & 8 \\ 8 & 8 & 4 & 8 & 8 & 16 & 8 & 8 \\ 4 & 4 & 4 & 8 & 4 & 8 & 8 & 8 \\ 4 & 8 & 8 & 8 & 8 & 8 & 8 & 16 \end{pmatrix},$$

where $w_i, w_j \in B'$ and $det(\Lambda) = det(G) = 4^8$.

Applying the LLL algorithm, we obtain a matrix G' that is a Gram matrix of the lattice E_8 (E_8 is the only unimodular lattice of dimension 8 and even). Therefore, $\Lambda = (\mathcal{I}, 2-(\zeta_8+\zeta_8^{-1}))$ is an ideal lattice isomorphic to E_8.

VIII. References

[1] C. Maclachlan and A. W. Reid, **The arithmetic of hyperbolic 3-manifolds**. Springer-Verlag, New York, 2003.

[2] I. Reiner, **Maximal Orders**, Academic Press, London, 1975.

[3] F.-T. Tu and Y. Yang, **Lattice packing from quaternion algebras**, RIMS K$\hat{o}$ky$\hat{u}$roku Bessatsu, 229–237, 2012.