International Journal of Applied Mathematics

Volume 32 No. 2 2019, 325-332
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
doi: http://dx.doi.org/10.12732/ijam.v32i2.12

CONSTRUCTION OF EVEN-DIMENSIONAL LATTICES OF FULL DIVERSITY

Antonio A. Andrade[1], J. Carmelo Interlando[2 §]

[1]Department of Mathematics
São Paulo State University
São José do Rio Preto, SP 15054-000, BRAZIL

[2]Department of Mathematics and Statistics
San Diego State University
San Diego, CA 92182-7720, USA

Abstract: In this work even-dimensional ideal lattices of full diversity are obtained via the twisted homomorphism of the ring of integers of a totally real subfield of $\mathbb{Q}(\zeta_p)$, where p is an odd prime.

AMS Subject Classification: 11H06, 11R18, 94B12
Key Words: lattices, cyclotomic fields, modulation schemes

1. Introduction

Ideal lattices with a high modulation diversity have been extensively studied as an alternative approach for transmission over a Rayleigh-fading channel, see [1, 2, 3, 4, 5, 7]. The performance of those modulation schemes, in terms of error probability, essentially depends on their modulation diversity and minimum product distance. Bayer-Fluck-iger et al. [3] constructed rotated $\mathbb{Z}^n$-lattice constellations using cyclic extensions of $\mathbb{Q}$ of prime degree $n > 2$, whereas Elia et al. [4] extended this construction to any odd degree n. Extending the above previous results, the contribution of this work is a procedure for constructing ideal lattices in even dimensions. This will be achieved via cyclic extensions that is, via totally real subfields of even degree of $\mathbb{Q}(\zeta_p)$, where p is an odd prime.

Received: January 29, 2019

§Correspondence author

2. Background on Number Theory and Lattices

The material in this section can be found in [3] and [6]. A number field $\mathbb{L}$ of degree n is an extension of $\mathbb{Q}$ (field of rational numbers) of degree n. An element $\alpha \in \mathbb{L}$ is called an algebraic integer if there is a monic polynomial $f(x)$ with integer coefficients such that $f(\alpha) = 0$. The set $\mathcal{O}_{\mathbb{L}} = \{\gamma \in \mathbb{L} : \gamma \text{ is an algebraic integer}\}$ is a ring, called the ring of integers of $\mathbb{L}$. The ring $\mathcal{O}_{\mathbb{L}}$ can be regarded as a $\mathbb{Z}$-module; a $\mathbb{Z}$-basis $\{\beta_1, \ldots, \beta_n\}$ for the latter is called an integral basis for $\mathbb{L}$. One can always express $\mathbb{L}$ as $\mathbb{Q}(\alpha)$, where α is a suitable algebraic integer. Let $m(x) \in \mathbb{Z}[x]$ be the monic polynomial of smallest degree having α as a root. The n distinct roots $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ of $m(x)$ are the conjugates of α, and the $\mathbb{Q}$-homomorphisms (or embeddings) of $\mathbb{L}$ into $\mathbb{C}$, namely, $\sigma_1, \ldots, \sigma_n$, are given by $\sigma_i(\alpha) = \alpha_i$ for $i = 1, 2, \ldots, n$. An element $\gamma \in \mathbb{L}$ is said to be totally real if $\sigma_i(\gamma) \in \mathbb{R}_{>0}$ for $i = 1, \ldots, n$. If $\sigma_i(\mathbb{L}) \subseteq \mathbb{R}$ for $i = 1, \ldots, n$, then $\mathbb{L}$ is said to be totally real.

The trace of any element $\alpha \in \mathbb{L}$ is defined as the rational number $\mathrm{Tr}_{\mathbb{L}/\mathbb{Q}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$. Let $\zeta_n \in \mathbb{C}$ denote anyone of the nth primitive roots of unity for any integer $n \geq 3$. The number field $\mathbb{F} = \mathbb{Q}(\zeta_n)$ is called the nth cyclotomic field. If $\mathbb{K}$ is a subfield of $\mathbb{F}$ such that $[\mathbb{K} : \mathbb{Q}] = n$, then $\mathbb{K} = \mathbb{Q}(\theta)$, where $\theta = \mathrm{Tr}_{\mathbb{F}/\mathbb{K}}(\zeta_p)$.

Let p be an odd prime, $\mathbb{K} \subseteq \mathbb{Q}(\zeta_p)$ a totally real number field of degree n, α a totally positive element of $\mathbb{K}$, and $\mathcal{A} \subseteq \mathcal{O}_{\mathbb{K}}$ an ideal. An ideal lattice is a lattice $(\mathcal{A}, q_\alpha)$ where $q_\alpha : \mathcal{A} \times \mathcal{A} \to \mathbb{Z}$, $q_\alpha(x, y) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha x y)$, for all $x, y \in \mathcal{A}$. The Galois group of $\mathbb{L}$ over $\mathbb{Q}$, denoted by $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ is the cyclic group $\langle\sigma\rangle$ for some embedding σ of $\mathbb{L}$ into $\mathbb{C}$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a $\mathbb{Z}$-basis for $\mathcal{A}$. The generator matrix M of the lattice $\Lambda = (\mathcal{A}, q_\alpha)$ is given by $M = (\sqrt{\sigma^i(\alpha)}\sigma^i(\alpha_j))$ for $i = 0, 1, \ldots, n-1$ and $j = 1, 2, \ldots, n$, whereas $G = MM^t = (\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha\alpha_i\alpha_j))_{i,j=1}^{n}$, is the Gram matrix of Λ, where t denotes matrix transposition.

3. Construction of Ideal Lattices

Let n be a positive even integer and let p be an odd prime such that $p \equiv 1 \pmod{n}$. Let $\mathbb{K} \subset \mathbb{Q}(\zeta_p)$ be a number field such that $[\mathbb{K} : \mathbb{Q}] = n$ and $n \mid (p-1)/2$, that is, $[\mathbb{Q}(\zeta_p) : \mathbb{K}] = (p-1)/n$. Let $\sigma = \sigma_r$ be a generator of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, $m = \frac{p-1}{2}$, and $\alpha = \prod_{k=0}^{m-1}(1 - \zeta_p^{r^k})$. Since $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{K}) = \langle\sigma^n\rangle = \{\sigma^n, \sigma^{2n}, \ldots, \sigma^{n\frac{p-1}{n}}\}$, it follows that $\theta = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) = \sum_{a=0}^{\frac{p-1}{n}} \sigma^{an}(\zeta_p)$.

Lemma 1. *[3] If $\lambda \in \mathbb{Z}$ is such that $\lambda(r-1) \equiv 1 \pmod{p}$, then $\sigma(\alpha) = -\zeta_p^{p-1}\alpha$, $\sigma(\zeta_p^\lambda \alpha) = -\zeta_p^\lambda \alpha$ and $(\zeta_p^\lambda \alpha)^2 = (-1)^m p$.*

Next we present another proof of Proposition 4.5 of [1].

Theorem 2. *If $z = \zeta_p^\lambda \alpha(1-\zeta_p)$ and $x = \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{K}}(z)$, then*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = \begin{cases} (-1)^m p^2(\frac{p-1}{n}+1) & \text{if } t=0; \\ (-1)^{m+t}p^2(\frac{p-1}{n}) & \text{if } t=1,\ldots,n-1. \end{cases}$$

Proof. The elements x and $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x))$ are well defined because $z \in \mathbb{Q}(\zeta_p)$ and $x, \sigma^t(x) \in \mathbb{K}$. Since $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \{\sigma^0, \ldots, \sigma^{n-1}\}$, one has

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = \sum_{a=0}^{n-1} \sigma^a(x\sigma^t(x)),$$

$t = 0, 1, \ldots, n-1$. Since

$$x\sigma^t(x) = \sum_{c=1}^{\frac{p-1}{n}} \sigma^{cn}(z) \sum_{j=1}^{\frac{p-1}{n}} \sigma^{t+jn}(z) = \sum_{c=1}^{\frac{p-1}{n}} \sum_{j=1}^{\frac{p-1}{n}} \sigma^{cn}(z)\sigma^{t+jn}(z),$$

one has

$$\begin{aligned} T_t &= \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\sigma^t(x)) = \sum_{a=0}^{n-1}\sum_{c=1}^{\frac{p-1}{n}}\sum_{j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(z)\sigma^{a+t+jn}(z) \\ &= \sum_{a=0}^{n-1}\sum_{c=1}^{\frac{p-1}{n}}\sum_{j=1}^{\frac{p-1}{n}} \sigma^{a+cn}(\zeta_p^\lambda\alpha(1-\zeta_p))\sigma^{a+t+jn}(\zeta_p^\lambda\alpha(1-\zeta_p)) \\ &\overset{(1)}{=} \sum_{a=0}^{n-1}\sum_{c=1}^{\frac{p-1}{n}}\sum_{j=1}^{\frac{p-1}{n}} (-1)^{a+cn}\zeta_p^\lambda\alpha(1-\zeta_p^{r^{a+cn}})(-1)^{a+t+jn}\zeta_p^\lambda\alpha(1-\zeta_p^{r^{a+t+jn}}) \\ &\overset{(2)}{=} \sum_{a=0}^{n-1}\sum_{c=1}^{\frac{p-1}{n}}\sum_{j=1}^{\frac{p-1}{n}} (-1)^t(\zeta_p^\lambda\alpha)^2(1-\zeta_p^{r^{a+cn}})(1-\zeta_p^{r^{a+t+jn}}) \\ &= (-1)^t \sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}} (\zeta_p^\lambda\alpha)^2(1-\zeta_p^{r^{a+cn}})(1-\zeta_p^{r^{a+t+jn}}) \end{aligned}$$

$$\overset{(3)}{=} \quad (-1)^{t+m}p\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+cn}})(1-\zeta_p^{r^{a+t+jn}}).$$

Equalities (1) and (3) follow from Lemma 1, whereas equality (2) follows from the fact that $(-1)^{a+cn}(-1)^{a+t+jn} = (-1)^t$ because n is even. Since

$$\sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+cn}})(1-\zeta_p^{r^{a+t+jn}}) = \sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+cn}}-\zeta_p^{r^{a+t+jn}}+\zeta_p^{r^{a+cn}}\zeta_p^{r^{a+t+jn}}) =$$

$$\sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+cn}})-\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}+\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}, \quad \text{it follows that}$$

$$T_t = (-1)^{t+m}p\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\left(\sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+cn}})-\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}+\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}\right).$$

Since $1-\zeta_p^{r^{a+cn}}$ does not depend on j, it follows that

$$\sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+cn}}) = \frac{p-1}{n}(1-\zeta_p^{r^{a+cn}}),$$

so

$$\begin{aligned}T_t &= (-1)^{t+m}p\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\left(\frac{p-1}{n}(1-\zeta_p^{r^{a+cn}})-\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}+\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}\right)\\ &= (-1)^{t+m}p\left(\frac{p-1}{n}\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}(1-\zeta_p^{r^{a+cn}})-\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}+\right.\\ &\left.\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}\right).\end{aligned}$$

Since $\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}$ does not depend on c, it follows that

$$\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}} = \frac{p-1}{n}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}.$$

Thus,

$$\begin{aligned} T_t &= (-1)^{t+m}p\left(\frac{p-1}{n}\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}(1-\zeta_p^{r^{a+cn}}) - \frac{p-1}{n}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}\right. \\ &\quad \left. + \sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}\right) \\ &= (-1)^{t+m}p\left(\frac{p-1}{n}\left(\sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}(1-\zeta_p^{r^{a+cn}}) - \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}}\right) + \right. \\ &\quad \left. \sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}\right). \end{aligned}$$

Now, let

$$\begin{aligned} y_1 &= \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+jn}}) - \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}} \\ y_2 &= \sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}. \end{aligned}$$

One then has

$$\begin{aligned} y_1 &= \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}(1-\zeta_p^{r^{a+jn}}) - \sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+t+jn}} \\ &= (p-1) - \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\theta) - \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\sigma^t(\theta)) = (p-1)+2 = p+1. \end{aligned}$$

For y_2, let $l=(p-1)/n$. Since $\overline{r}$ is a generator of the group $\mathbb{Z}_p^*$, it follows that $r^{p-1} \equiv 1 \pmod{p}$, that is, $r^{(p-1)q} = (r^{p-1})^q \equiv 1^q = 1 \pmod{p}$, for all $q \in \mathbb{Z}$. So,

$$r^{a+(lq+c)n} = r^{a+(\frac{p-1}{n}q+c)n} = r^{a+cn}r^{(p-1)q} \equiv r^{a+cn} \pmod{p}$$

and $\zeta_p^{r^{a+cn}} = \zeta_p^{r^{a+(lq+c)n}}$ for all $q \in \mathbb{Z}$. If $s \equiv c \pmod{l}$, then $s = lq+c$ for some $q \in \mathbb{Z}$. Thus, $\zeta_p^{r^{a+sn}} = \zeta_p^{r^{a+cn}}$. Regarding c and j in $\mathbb{Z}_l$, one has

$$y_2 = \sum_{a=0}^{n-1}\sum_{c=1}^{\frac{p-1}{n}}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}} = \sum_{c=1}^{\frac{p-1}{n}}\sum_{a=0}^{n-1}\sum_{j=1}^{\frac{p-1}{n}}\zeta_p^{r^{a+cn}+r^{a+t+jn}}.$$

Letting $d \equiv c - j \pmod{l}$, it follows that $\zeta_p^{r^{a+cn}} = \zeta_p^{r^{a+(d+j)n}}$. So

$$y_2 = \sum_{d=1}^{\frac{p-1}{n}} \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} \zeta_p^{r^{a+(d+j)n}+r^{a+t+jn}} = \sum_{d=1}^{\frac{p-1}{n}} \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} \zeta_p^{(r^{dn}+r^t)r^{a+jn}}$$
$$= \sum_{d=1}^{\frac{p-1}{n}} \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} \zeta_p^{(r^{dn}+r^t)r^{a+jn}}.$$

For $a \in \{0, 1, \ldots, n-1\}$ and $j \in \{1, \ldots, \frac{p-1}{n}\}$, note that r^{a+jn} assumes values congruent to $s = 1, 2, \ldots, p-1$ modulo p because $\langle \overline{r} \rangle = \mathbb{Z}_p^*$. Hence $\overline{r}^{a+jn} = \overline{s}$ for some $s = 1, 2, \ldots, p-1$, that is, $r^{a+jn} \equiv s \pmod{p}$. So, $\zeta_p^{r^{a+jn}} = \zeta_p^s$, for some s in $\{1, 2, \ldots, p-1\}$. Thus,

$$\sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} \zeta_p^{(r^{dn}+r^t)r^{a+jn}} = \sum_{a=0}^{n-1} \sum_{j=1}^{\frac{p-1}{n}} (\zeta_p^{r^{a+jn}})^{r^{dn}+r^t} = \sum_{s=1}^{p-1} (\zeta_p^s)^{r^{dn}+r^t} = \sum_{s=1}^{p-1} (\zeta_p^{r^{dn}+r^t})^s.$$

For $t = 0, 1, \ldots, n-1$, define $\omega_{d,t} = \zeta_p^{r^{dn}+r^t}$. Then

$$y_2 = \sum_{d=1}^{\frac{p-1}{n}} \sum_{s=1}^{p-1} (\omega_{d,t})^s \text{ where } \sum_{s=1}^{p-1} (\omega_{d,t})^s = \begin{cases} p-1 & \text{if } \omega_{d,t} = 1 \\ -1 & \text{if } \omega_{d,t} \neq 1. \end{cases}$$

In the last equality, the first case is trivial. For $\omega_{d,t} \neq 1$, it is sufficient observe that $\omega_{d,t} = \zeta_p^{r^{dn}+r^t}$ is a root of the polynomial $\frac{x^p-1}{x-1} = x^{p-1} + \cdots + x + 1$. Indeed,

$$\sum_{s=1}^{p-1} (\omega_{d,t})^s = (\omega_{d,t})^{p-1} + \cdots + (\omega_{d,t})^2 + \omega_{d,t} = -1.$$

Now, to calculate y_2, we consider the cases $t = 0$ and $t \neq 0$. For this, consider the following claim, which is proved next:

$$\omega_{d,t} = 1 \iff t = 0 \text{ and } d = \frac{p-1}{2n}. \tag{1}$$

If $t = 0$ and $d = (p-1)/2n$, then $r^{p-1} \equiv 1 \pmod{p}$. Since $p-1$ is even, there exists $m \in \mathbb{Z}$ such that $p - 1 = 2m$. So, $(r^m)^2 = r^{2m} \equiv 1 \pmod{p}$, that is, $p \mid (r^m)^2 - 1 = (r^m + 1)(r^m - 1)$. Thus, $r^m \equiv 1 \pmod{p}$ or $r^m \equiv -1 \pmod{p}$.

The first case is not possible because $p-1$ is the smallest positive integer with this property. So, $r^m \equiv -1 \pmod{p}$, that is, $r^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$. Therefore,

$$\omega_{d,t} = \zeta_p^{r^{dn}+1} = \zeta_p^{r^{(\frac{p-1}{2n})n}+1} = \zeta_p^{r^{\frac{p-1}{2}}+1} = 1.$$

Conversely, if $\omega_{d,t} = 1$, that is, $\zeta_p^{r^{dn}+r^t} = 1$, then

$$\begin{aligned} &r^{dn} + r^t \equiv 0 \pmod{p} \Leftrightarrow r^{dn} \equiv -r^t \pmod{p} \overset{(i)}{\Leftrightarrow} \\ &r^{dn} \equiv r^{m+t} \pmod{p} \Leftrightarrow m + t \equiv dn \pmod{p-1} \Leftrightarrow \\ &p-1 \mid m + t - dn \Leftrightarrow \exists\ k_1 \in \mathbb{Z};\ t = dn - m + k_1(p-1), \end{aligned}$$

where equivalency (i) follows from the fact that $r^{m+t} \equiv -r^t \pmod{p}$. Now, $n \mid dn$, $n \mid k_1(p-1)$ (because $n \mid p-1$) and $n \mid m$ (because $n(\frac{p-1}{2n}) = m$), and thus, $n \mid t$. Since $t \in \{0, 1, \ldots, n-1\}$, it follows that $t = 0$. Thus, $dn = m - k_1(p-1)$ and therefore

$$d = \frac{p-1}{2n} - k_1(\frac{p-1}{n}) = \frac{p-1}{2n}(1 - 2k_1) = k_2(\frac{p-1}{2n})$$

with $k_2 = 1 - 2k_1$ odd. Since $1 \leq d \leq (p-1)/n$, one has either $k_2 = 1$ or $k_2 = 2$, but since k_2 is odd, it follows that $k_2 = 1$. Therefore, $d = (p-1)/2n$, which proves (1).

Now, to calculate y_2, suppose that $t \neq 0$. From (1), it follows that $\omega_{d,t} \neq 1$ and therefore $\sum_{s=1}^{p-1}(\omega_{d,t})^s = -1$. So,

$$y_2 = \sum_{d=1}^{\frac{p-1}{n}} \sum_{s=1}^{p-1} (\omega_{d,t})^s = \sum_{d=1}^{\frac{p-1}{n}} -1 = -\left(\frac{p-1}{n}\right).$$

Now, suppose that $t = 0$. From (1), if $d = (p-1)/2n$, then $\omega_{d,t} = 1$, and if $d \neq (p-1)/2n$, then $\omega_{d,t} \neq 1$. Thus,

$$y_2 = \sum_{d=1}^{\frac{p-1}{n}} \sum_{s=1}^{p-1} (\omega_{d,t})^s = (p-1) + \sum_{\substack{d=1 \\ d \neq \frac{p-1}{2n}}}^{\frac{p-1}{n}} -1 = (p-1) - \left(\frac{p-1}{n} - 1\right),$$

which proves the theorem. □

The Gram matrix of the ideal lattice is given by $G = (g_{ij})_{i,j=1}^n$, where $g_{ij} = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\sigma^{j-i}(x))$ for $1 \leq i, j \leq n$. For example, if $\mathbb{L} = \mathbb{Q}(\zeta_5)$ and

$\mathbb{K} = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$, then $[\mathbb{K} : \mathbb{Q}] = 2$, $r = 2$, $\alpha = (1-\zeta)(1-\zeta^2)$, $\lambda = 1$, and $z = -2\zeta_5^3 - 4\zeta_5^2 - \zeta_5 - 3$. Thus $x = -5(\zeta_5^3 + \zeta_5^2 + 1)$, $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x^2) = 75$, and $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(x\sigma(x)) = -50$. Hence,

$$G = \begin{pmatrix} 75 & -50 \\ -50 & 75 \end{pmatrix}.$$

Acknowledgments

This work was supported by São Paulo Research Foundation – FAPESP, Brazil, under grant No. 2013/25977-7.

References

[1] A. A. Andrade and E. D. De Carvalho, Constructions of ideal lattices with full diversity, *J. Adv. Res. Appl. Math.*, **3** (2011), 82–92.

[2] A. A. Andrade, C. Alves, T. B. Carlos and A. J. Ferrari, Lattices via cyclotomic fields in dimensions 2 and 4, *Int. J. Appl. Math.*, **20** (2007), 1095–1105.

[3] E. Bayer-Fluckiger, F. Oggier and E. Viterbo, New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel, *IEEE Trans. Inform. Theory*, **50** (2004), 702–714.

[4] P. Elia, B. A. Sethuraman and P. Vijay Kumar, Perfect space-time codes for any number of antennas, *IEEE Trans. Inform. Theory*, **53** (2007), 3853–3868.

[5] J. C. Interlando, J. O. D. Lopes and T. P. da Nóbrega Neto, Four-dimensional lattices from $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, *Int. J. Appl. Math.*, **30** (2017), 401–408, doi: 10.12732/ijam.v30i5.4.

[6] P. Ribenboin, *Classical Theory of Algebraic Numbers*, Springer Verlag, New York (2001).

[7] C. C. Trinca Watanabe, J.-C. Belfiore, E. D. De Carvalho and J. Vieira Filho, E_8-lattice via the cyclotomic field $\mathbb{Q}(\zeta_{24})$, *Int. J. Appl. Math.*, **31** (2018), 63–71, doi: 10.12732/ijam.v31i1.6.