Information Engineering Express
International Institute of Applied Informatics
2015, Vol. 1, No. 1, 37 – 44

On Product Distance of Lattice Code over a Biquadratic Number Field

Kiyoshi Nagata *

Abstract

Lattice code is a type of error correcting codes composed of the image of embedding map of an integral ideal in a certain algebraic number field with a bilinear form. In a mobile communication, transmitted signals are attenuated by phenomenon called fading, and the Rayleigh fading of multi-path radio wave is one of important and essential type of fading. Some lattice codes are applicable in order to mitigate the influence of the fading and to extract the most feasible source information from the received signal.

The minimum product distance is one of key indicators of lattice code along with the modulation diversity. In this paper, we show some experimental results on the minimum product distance for some lattices of prime ideal in a composition fields of two real quadratic fields using a free formula manipulation system, PARI/GP.

Keywords: Rayleigh Fading, Lattice Code, Minimum Product Distance, PARI/GP.

1 Introduction

Radio wave transmitted from the antenna of a base station follows different routes and is received by mobile receiver. During the transmission, it usually occurs reflections by buildings and Doppler effect, and the receiver catches many radio waves interfered by them. One of typical fading phenomenon in such situation is called the Rayleigh fading, and a simple mathematical model is expressed as follows,

$$\vec{r} = \vec{x}\mathrm{H} + \vec{\varepsilon}, \tag{1}$$

where $\vec{x} = (x_1, \ldots, x_n)$ is an original signal vector, $\vec{r} = (r_1, \ldots, r_n)$ is the received signal vector, $\vec{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n)$ is Gaussian white noise vector, and H is the diagonal matrix with diagonal elements α_i $(i = 1, \ldots, n)$ whose probability follows the normalized Rayleigh distribution $p(\alpha) = 2\alpha e^{-\alpha^2}$. Using the channel component interleaver/deinterleaver, α_i's can be supposed to be independent with each other.

There are some result on relationship between Rayleigh fading and lattice code based on algebraic number theory. In this paper, we refer the previous part of Oggier's thesis [3] studying key indices, "modulation diversity" and "minimum product distance". We give a short program in PARI/GP to calculate the minimum product distance of lattice codes induced from prime ideals in $\mathbb{Q}(\sqrt{m}, \sqrt{n})$ for some numbers m and n. And we notice some

* Faculty of Business Administration, Daito Bunka University, Tokyo, Japa

properties for two part of the index on the analogy of experimental results by executing the program.

2 Lattice Code and Rayleigh Fading

Under some condition such as availability of perfect CSI(Channel State Information), we could assume that every element in the equation (1) is in real numbers. When a lattice generating matrix M in $\mathrm{M}_n(\mathbb{R})$ is given, chose a subset S, called a "signal constellation", of cardinality 2^m in the k-dimensional real lattice $\Lambda = \{x = u\mathrm{M}; u \in \mathbb{Z}^n\}$. Some part of the original message is converted into an element of S using a certain modulation system, and transfered from a single antenna.

The signal is modified by Rayleigh fading and ordinary Gaussian white noise, then received signal vector $\vec{r}$ is expressed in the equation (1). When we adopt the maximum likelihood detection method, our task is to find out an element $\vec{x'} \in \mathrm{S}$ which minimize $m(\vec{x}|\vec{r},\vec{\alpha}) = \sum_{i=1}^{n} |r_i - \alpha_i x_i|^2$.

In order to estimate the error probability for a signal constellation S, fix a Rayleigh fading vector and a Gaussian noise vector, and estimate $P(\vec{x} \to \vec{x'}|\vec{\alpha})$ the probability of receiving $\vec{x'}$ different from the transfered original vector $\vec{x}$.

$$\begin{aligned} P(\vec{x} \to \vec{x'}|\vec{\alpha}) &= P(\sum |r_i - \alpha_i x'_i|^2 \leq \sum |r_i - \alpha_i x_i|^2) \\ &= P(\sum \alpha_i^2 (x_i - x'_i)^2 \leq 2\chi) \\ &= P(\frac{\sigma_\chi^2}{2N_0} \leq \chi) \\ &= Q(\frac{\sigma_\chi}{2N_0}), \end{aligned} \tag{2}$$

where $\chi = \sum \alpha_i (x'_i - x_i)\varepsilon_i$ is also Gaussian zero mean random variable with variance $\sigma_\chi^2 = N_0 \sum \alpha_i^2 (x'_i - x_i)^2$, and $Q(x) = \frac{1}{2\pi} \int_x^\infty e^{-\frac{1}{2}t^2} dt$, the Gaussian tail function.

Applying the inequality $Q(x) \leq \frac{1}{2} e^{-\frac{x^2}{2}}$, we have

$$P(\vec{x} \to \vec{x'}|\vec{\alpha}) \leq \frac{1}{2} e^{-\frac{1}{8N_0} \sum \alpha_i^2 (x'_i - x_i)^2}. \tag{3}$$

Next integrate the probability over all α_i with independent probabilities $p(\alpha_i) = 2\alpha_i e^{-\alpha_i^2}$.

$$\begin{aligned} P(\vec{x} \to \vec{x'}) &= \int P(\vec{x} \to \vec{x'}|\vec{\alpha}) p(\vec{\alpha}) d\vec{\alpha} \\ &\leq \frac{1}{2} \prod_{i=1}^{n} \int_0^{\infty} e^{-\frac{1}{8N_0} \Sigma (x'_i - x_i)^2 \alpha_i^2} p(\alpha_i) d\alpha_i \\ &= \frac{1}{2} \prod_{i=1}^{n} \int_0^{\infty} 2\alpha_i e^{-(1+\frac{1}{8N_0}(x'_i - x_i)^2)\alpha_i^2} d\alpha_i \\ &= \frac{1}{2} \prod_{i=1}^{n} \frac{1}{1 + \frac{1}{8N_0}(x'_i - x_i)^2} \\ &\leq \frac{1}{2} \prod_{x_i \neq x'_i} \frac{8N_0}{(x'_i - x_i)^2} \\ &= \frac{1}{2} \frac{(8N_0)^l}{d_p^{(l)}(\vec{x}, \vec{x'})^2}, \end{aligned} \tag{4}$$

where $d_p^{(l)}(\vec{x}, \vec{x'}) = \prod_{x_i \neq x'_i} |x'_i - x_i|$ and $l = \sharp\{i; x_i \neq x'_i\}$.

Then the error probability of a given constellation S is estimated as follows,

$$\begin{aligned} P_e(S) &\leq P_e(\Lambda) \\ &\leq \sum_{l=L}^{n} \frac{(8N_0)^l}{2} \sum_{d(\vec{x}, \vec{x'})=l} \frac{1}{d_p^{(l)}(\vec{x}, \vec{x'})^2}, \end{aligned} \tag{5}$$

where $L = \min\{l\} = \min_{\vec{x} \neq \vec{x'}} \{d_H(\vec{x}, \vec{x'})\}$ is called the "modulation diversity" of Λ denoted by $div(\Lambda)$.

The dominant term of the estimation formula is

$$d_{p,min} = \min_{d_H(\vec{x}, \vec{x'})=L} \{d_p^{(L)}(\vec{x}, \vec{x'})\},$$

which is called the "minimum produce distance". Therefore, a preferred lattice has large modulation diversity and also large minimum produce distance.

3 Ideal Lattice

As a candidate for real lattice with bigger terms, here we see how to construct a lattice from an ideal in a algebraic number field K of degree n with a $\mathbb{Q}$-linear involution $\bar{\sigma}$.

Definition 1. *Let $\mathfrak{a}$ be ideal of $\mathscr{O}_K$ and $\alpha \in F = K^{\bar{\sigma}}$ satisfying $\alpha \mathfrak{a} \bar{\mathfrak{a}} \subseteq \mathfrak{D}^{-1} = \{x \in K; Tr_{K/\mathbb{Q}}(x\mathscr{O}_K) \subseteq \mathbb{Z}\}$ where $\bar{\mathfrak{a}} = \mathfrak{a}^{\bar{\sigma}}$. Then an ideal lattice is the pair $(\mathfrak{a}, b_\alpha)$ with a symmetric $\mathbb{Z}$-bilinear form*

$$b_\alpha : \mathfrak{a} \times \mathfrak{a} \to \mathbb{Z}$$

defined by $b_\alpha(x, y) = Tr_{K/\mathbb{Q}}(\alpha x \bar{y})$.

Let $Aut_{\mathbb{Q}}K = \{\sigma_1, \ldots, \sigma_{r_1}, \sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_2}, \bar{\sigma}_{r_2}\}$ be the set of r_1 number of real and $2r_2$ number of imaginary automorphisms. We call (r_1, r_2) the "signature" of K.

Definition 2. *For a totally real and totally positive number $\alpha \in \mathrm{K}$, the twisted embedding $e_\alpha : \mathrm{K} \to \mathbb{R}^n$ is defined by*

$$\begin{aligned} e_\alpha(x) = (&\sqrt{\alpha_1} x^{\sigma_1}, \ldots, \sqrt{\alpha_{r_1}} x^{\sigma_{r_1}}, \\ &\sqrt{2\alpha_{r_1+1}} Re(x^{\sigma_{r_1+1}}), \sqrt{2\alpha_{r_1+1}} Im(x^{\sigma_{r_1+1}}), \ldots, \\ &\sqrt{2\alpha_{r_1+r_2}} Re(x^{\sigma_{r_1+r_2}}), \sqrt{2\alpha_{r_1+r_2}} Im(x^{\sigma_{r_1+r_2}})), \end{aligned}$$

where $\alpha_i = \alpha^{\sigma_i}$ for $i = 1, \ldots, r_1 + r_2$.

The embedded image of an ideal lattice $(\mathfrak{a}, b_\alpha)$ by e_α, denoted by $\Lambda(\mathfrak{a}, b_\alpha)$, is considered as our candidate and its modulation diversity and minimum product distance are given by the following theorems.

For an ideal lattice $(\mathfrak{a}, b_\alpha)$ in an algebraic number field K of degree $n = r_1 + 2r_2$,

Theorem 3 (Modulation diversity)**.**

$$div(\Lambda(\mathfrak{a}, b_\alpha)) = r_1 + r_2. \tag{6}$$

Theorem 4 (Minimum product distance)**.**

$$d_{p,min}(\Lambda(\mathfrak{a}, b_\alpha)) = \sqrt{\left| \frac{det(b_\alpha)}{d_K} \right|} \min_{0 \neq x \in \mathfrak{a}} \frac{N(x)}{N(\mathfrak{a})}, \tag{7}$$

where $det(b_\alpha) = det(b_\alpha(\omega_i, \omega_j))$ with a $\mathbb{Z}$-basis of $\mathfrak{a} = {}_{\mathbb{Z}} < \omega_1, \ldots, \omega_n >$.

There are Propositions for b_α and for $\Lambda(\mathfrak{a}, b_\alpha)$ to be positive(or negative) definite bilinear form ([1]).

Property 5. *A necessary and sufficient condition for the existence of a definite ideal lattice $(\mathfrak{a}, b_\alpha)$ is that* F *is a totally real and* $\mathrm{K} = \mathrm{F}$ *or CM-field of* F.

Property 6. *If* K *is a totally real or CM-field, then $\Lambda(\mathfrak{a}, b_\alpha)$ is a positive definite ideal lattice.*

4 PARI/GP

PARI/GP is a free formula manipulation system which has been designed to perform the calculations especially in number theory in the high speed not only in matrix, polynomial, power series. PARI/GP was originally developed by Henri Cohen and his co-workers at University of Bordeaux, and licensed currently in GPL being maintained by Karim Belabas while receiving the help of many volunteers contributors [4]. Current stable version is 2.7.2.

An algebraic number field is defined as the quotient field of $\mathbb{Q}[X]$ by a characteristic polynomial, and its elements are expressed as polynomial of X of lower degree than the degree of characteristic polynomial.

Here we pick up some functions and expressions used in calculation of the minimum product distance of lattice code in a algebraic number field.

- K=bnfinit(T): The initialization of the algebraic number field by adjoining a root of irreducible polynomial T in $\mathbb{Q}$, and named as "K" for example.

- K.disc, K.no, K.zk: Output the discriminant, the class number and integral basis of the field K, respectively.
- P=idealprimedec(K,p): The array of the prime ideal decomposition of a prime number p. $pri = P[i]$ represents the i-th prime factor. Two elements corresponding to $pri[1]$ and the vector $pri[2]$ are two generators of pri over $\mathscr{O}_K$. Moreover $pri[3]$ and $pri[4]$ are its ramification index and degree respectively.
- Isp=bnfisprincipal(K,$pr1$): When

$$pr1 = \gamma \prod_{i=1} g_i^{c_i} \tag{8}$$

  in the ideal class group with generator ideals g_i, Isp's first component is the vector of c_i, and the second component is the vector expression of γ corresponding to the integral basis given by K.zk. So the first component is [0] means that $pr1$ is principal.
- idealhnf(K,$pr1$): Output the Hermite normal form of ideal $pr1$ as the expression of square matrix whose column is corresponding to each element of the basis over $\mathbb{Z}$.
- idealnorm(K,$pr1$): Output the norm of $pr1$. Even if the second argument is a element, this function works well, that is output the norm of element.
- nfeltmul(K, a, b): The multiplication of two elements in the field K.
- idealmul(K, $\mathfrak{a}$, $\mathfrak{b}$): The multiplication of two ideals.
- idealpow(K, $\mathfrak{a}$, k): The k-th power of an ideal.
- idealnorm(K, $\mathfrak{a}$): The norm of an ideal.
- polcoeff(T, k): The k-th degree's coefficient of a polynomial of one variable.
- matdet(D): The determinant of a square matrix D.

5 Experimental Result with PARI/GP

In this paper, we consider the composition field of two real quadratic fields, $K = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ for some positive numbers m and n, and set $\alpha = 1$ in Theorem 3.4. From Proposition 3.6 and Theorem 3.3, any ideal lattice $\Lambda(\mathfrak{a}, b_\alpha)$ is a positive definite with modulation diversity 4.

5.1 Program

In order to initialize the number field, we set T as the simple defining polynomial of $X = \sqrt{m} + \sqrt{n}$. Our program outputs two values in the minimum product distance for a given pair of two distinct prime integers (m,n) and for one of prime ideals, $\mathfrak{p}$, dividing rational prime numbers from 2 to 991 for example.

The first value $\sqrt{\left| \frac{det(Tr_{K/\mathbb{Q}}(\omega_i \omega_j))}{d_K} \right|}$ with $\mathfrak{p} = {}_{\mathbb{Z}} < \omega_1, \ldots, \omega_n >$ can be calculated using the fact that

$Tr_{K/\mathbb{Q}}((\sqrt{m}+\sqrt{n})^3) = Tr_{K/\mathbb{Q}}(\sqrt{m}+\sqrt{n}) = 0,$

$Tr_{K/\mathbb{Q}}((\sqrt{m}+\sqrt{n})^2) = 4(m+n)$, and $Tr_{K/\mathbb{Q}}(1) = 4$. For the second value $\min_{0\neq x\in\mathfrak{p}} \frac{N(x)}{N(\mathfrak{p})}$, we could only give a upper bound using γ in the equation (8). Fig.1 is the program in PARI/GP which output the first value and $\frac{N(\mathfrak{p})}{N(\gamma)}$ for one of factors of all the prime p less than 991. We should notice that the second value is the inverse of original value, but the $\gamma \in K$ is not an integer and it seems that only the denominator remains in $\frac{N(\gamma)}{N(\mathfrak{p})}$.

```
1  {forprime(m=2,100,
2   forprime(n=m+2,100,
3       T=X^4-2*(m+n)*X^2+(m-n)^2;
4       K=bnfinit(T);
5       write("log.txt","m=",m,"¥t n=",n,"¥t ClassNo=",K.no);
6       write("log.txt","p¥t SQRT(det(b1)/Dk)¥t
                                  N(pr1)/N(x)¥t Principal?");
7       base=K.zk;
8   forprime(p=2,991,
9       P=idealprimedec(K,p);
10      pr1=P[1];
11      isp=bnfisprincipal(K,pr1);
12      gen0=base*isp[2];
13      B=idealhnf(K,pr1);
14      A=vector(4);
15      for(i=1,4,A[i]=base*B[,i]);
16      C=matrix(4,4);D=matrix(4,4);
17      for(i=1,4,for(j=1,4,C[i,j]=base*nfeltmul(K,A[i],A[j])));
18      for(i=1,4,for(j=1,4,
            D[i,j]=4*((m+n)*polcoeff(C[i,j],2)+polcoeff(C[i,j],0))));
19      if(K.no==1,write("log.txt","p=",p,"¥t",
            factor(floor(sqrt(abs(matdet(D)/K.disc))))),
            write("log.txt","p=",p,"¥t",
            factor(floor(sqrt(abs(matdet(D)/K.disc)))),"¥t",
            idealnorm(K,pr1)/idealnorm(K,gen0),"¥t",isp[1]));
20  ));)
21  }
```

Figure 1: Program for Key Indices in PARI/GP

The initialization process by setting m and n, and defining K is from the line1 to line7. In the line5, the class number of K along with values of m and n is output in a file named "log.txt". From the line8 to the line20, precesses are in the "for loop" by changing the prime number p from 2 to 991. "gen0" in the line12 is γ. $C[i,j]$ in the line17 and and $D[i,j]$ in the line18 are corresponding to $\omega_i * \omega_j$ and its trace respectively. In the line19, if the class number is 1, then it outputs only first value, and if not it outputs both first and second values.

5.2 Result of Executing the Program

Since the number of primes less than 100 is 25 and the number of primes less than 1000 is 167, we get data for 167 primes in 300 distinct totally real number field of degree 4. The list of output of the first values suggests that

$$\sqrt{\left|\frac{det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j))}{d_K}\right|} = p^f = N\mathfrak{p}, \tag{9}$$

where f is the degree of the prime ideal $\mathfrak{p}$. This is trivial from the algebraic number theory when we notice that $N\mathfrak{p} = det(\omega_i^{\sigma_l})^2 = det((\omega_i^{\sigma_l})^t(\omega_j^{\sigma_m})) = det(Tr_{K/\mathbb{Q}}(\omega_i\omega_j))$ for any algebraic number field.

```
m=19     n=43     ClassNo=5↵
p     SQRT(det(b1)/Dk)     N(pr1)/N(x)     Principal?
2       Mat([2, 1])          2          [1]~↵
3       Mat([3, 1])          16         [4]~↵
5       Mat([5, 2])          1          [0]~↵
7       Mat([7, 2])          1          [0]~↵
11      Mat([11, 2])         4          [2]~↵
13      Mat([13, 2])         1          [0]~↵
17      Mat([17, 1])         8          [3]~↵
19      Mat([19, 1])         1          [0]~↵
23      Mat([23, 2])         2          [1]~↵
29      Mat([29, 2])         16         [4]~↵
31      Mat([31, 2])         1          [0]~↵
37      Mat([37, 2])         2          [1]~↵
41      Mat([41, 2])         1          [0]~↵
43      Mat([43, 2])         1          [0]~↵
47      Mat([47, 2])         8          [3]~↵
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~↵
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~↵
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~↵
919     Mat([919, 2])        8          [3]~↵
929     Mat([929, 2])        1          [0]~↵
937     Mat([937, 2])        1          [0]~↵
941     Mat([941, 2])        1          [0]~↵
947     Mat([947, 2])        1          [0]~↵
953     Mat([953, 2])        1          [0]~↵
967     Mat([967, 2])        2          [1]~↵
971     Mat([971, 2])        1          [0]~↵
977     Mat([977, 2])        1          [0]~↵
983     Mat([983, 1])        4          [2]~↵
991     Mat([991, 1])        16         [4]~↵
```

Figure 2: Example of Output

Fig.2 represents an example of outputs in case of $\mathbb{Q}(\sqrt{19},\sqrt{43})$ with the class number 5, where the expression "Mat([a,b])" in the second column means just a^b. In this case, the ideal class is generated by a prime ideal $\mathfrak{p}_2$ dividing 2 of order 5 and of degree 1. When considering $p = 17$ for instance, a prime ideal dividing 17 is expressed as $\mathfrak{p}_{17} = \gamma\mathfrak{p}_2^3$ in the ideal class group, so we have $\mathfrak{p}_{17}\mathfrak{p}_2^2$ is a principal ideal. Thus we have the second value

$$\min_{0\neq x\in\mathfrak{p}_{17}} \frac{N(x)}{N(\mathfrak{p}_{17})} \leq N(\mathfrak{p}_2^2) = 2^2. \tag{10}$$

Although the method used for the inequality(10) can be applicable for any case once we have the structure of the ideal class group, the upper bound may not be optimal since there are many ideals representing a certain class. In the case above, the other possibility for optimal upper bound is only 3 if an ideal dividing 3 represent the same class as $\mathfrak{p}_2^2$. However, from Fig.2, we could see that it can not be possible since one of ideal factors of 3 is in the class of $\mathfrak{p}_2^4$ and we could see that any ideal factors are in the same class or in the class of $\mathfrak{p}_2^{(5-4)} = \mathfrak{p}_2$.

6 Conclusion and Discussion

We study the key values of the minimum product distance of ideal lattice related to the Rayleigh fading, and give a program in PARI/GP to calculate these values for a type of totally real algebraic number field of degree 4. By executing the program, we could have a

list of values which suggests a certain property of the minimum product distance. In order to find or to guess some properties of the second value, we may need to know the structure of the ideal class group. However, it is not difficult to evaluate a upper bound using PARI/GP when a precise values are fixed.

Since our program can be available for other type of algebraic number field, Experimental study will be done to find new type of properties in this research area.

References

[1] E. Bayer-Fluckiger, "Lattices and number fields", Contemporary Mathematics, 241, 1999, pp.69-84.

[2] E. Bayer-Fluckiger, F. Oggier, E. Viterbo, "New algebraic constructions of rotated $\mathbb{Z}^n$-lattice constellations for the Rayleigh fading channel", IEEE Trans. on Information Theory, vol. 50, no 4, 2004, pp. 702-714.

[3] F. Oggier, "Algebraic Methods for Channel Coding", THÈSE N^o 3182, École Polytechnique Fédérale de Lausanne, 2005, 5, Mar. 2014; http://biblion.epfl.ch/EPFL/theses/2005/3182/3182_abs.pdf

[4] PARI/GP Home, 26, Nov. 2014; http://pari.math.u-bordeaux.fr/