On the size of determinants in the class number formulae of cyclotomic function fields

Daiki Aoyama\(^1\) and Iwao Kimura\(^2\)

\(^1\) Graduate School of Science and Engineering for Education, University of Toyama, 3190 Gofuku, Toyama city, Toyama 930-8555, Japan
\(^2\) Department of Mathematics, Faculty of Science, University of Toyama, 3190 Gofuku, Toyama city, Toyama 930-8555, Japan

E-mail iwao@sci.u-toyama.ac.jp

Received November 02, 2019, Accepted February 18, 2020

Abstract

We discuss the size of the determinants, which appear in the determinant formulae of the relative class numbers of cyclotomic function fields. These are the determinants of integer symmetric matrices, whose entries are 0 or 1. We show that, for a smaller characteristic, the determinants are significantly large (in the absolute value) compared to the determinants of randomly generated such matrices, while for a larger characteristic, it is not the case. We explain why this happens by comparing some upper bounds.

Keywords cyclotomic function field, class number, determinant formula

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

In this article, we discuss the size of the determinants of specific 0/1 (or ±1) matrices, which appear in the determinant formula of the relative class numbers of cyclotomic function fields. This determinant formula was proved by Jung-Ahn [1, 2].

We show that, for a small characteristic, the determinant formula for cyclotomic function fields produces 0/1 (or ±1) matrices, which have extraordinary huge determinants compared to the random 0/1 (or ±1) matrices. On the contrary, for a larger characteristic, the matrices in the determinant formula are not ones of significant determinant in the random matrices.

We can explain these phenomena by upper bounds of the relative class numbers of cyclotomic function fields, which are a consequence of some algebraic class number formulae and the rationality of the zeta functions proved by A. Weil.

2. Background and notation

For a cyclotomic field \(\mathbb{Q}(\mu_n)\), the determinant formulae of the relative class numbers are well known. One of them is due to Hazama [3]. His formula expresses the relative class numbers of the \(p\)-th cyclotomic fields as the determinants of ±1 matrices. T. Taniguchi (Kanazawa Institute of Technology) found that the determinants of ±1 matrices, which appear in the determinant formula, are extraordinarily huge in the family of random ±1 matrices of the same size.

We first expected that we were able to show that the same holds for the cyclotomic function fields case. But our hope comes true only for function fields of small characteristics, not for those of larger characteristics. We provide the reason why the determinant of the 0/1 matrices, which appear in the determinant formulae, varies.

First, we recall some notion, especially on the arithmetic of cyclotomic function fields. The interested readers are referred to Rosen [4, Chapter 12].

For a prime number \(p\), let \(\mathbb{F}\) be the finite field of \(q\)-elements (\(q\) is a power of \(p\)). We denote \(A = \mathbb{F}[T]\) the ring of polynomials in an indeterminate \(T\) over \(\mathbb{F}\), \(k = \mathbb{F}(T)\) the field of fractions of \(A\). Let \(\rho\) be a Carlitz module, which is an \(\mathbb{F}\)-algebra homomorphism defined by the following:

\[
\rho: A \ni T \mapsto \phi + \mu \in \text{End}_\mathbb{F}(\mathbb{G}_{a,k}),
\]

where the right-hand side is the endomorphism ring of the additive group \(\mathbb{G}_{a,k}\) over \(k\), \(\phi(x) = x^q\) is the Frobenius endomorphism, and \(\mu\) is the multiplication by \(T\) endomorphism. It is well known that for each \(m = m(T) \in A\), \(\rho(m)(x)\) is a separable polynomial with \(A\)-coefficients. We fix, once and for all, a separable closure \(k^s\) of \(k\). Let \(\Lambda_m\) be the \(m\)-th division points of \(\rho\), namely,

\[
\Lambda_m = \{z \in k^s | \rho(m)(z) = 0\}.
\]

We denote by \(K_m = k(\Lambda_m)\) the field generated by \(\Lambda_m\) over \(k\), and call it the \(m\)-th cyclotomic function field.

For example, \(K_T = k(\Lambda_T)\), where \(\Lambda_T = \{z \in k^s | (\phi + \mu)(z) = 0\}\). Since \((\phi + \mu)(z) = z^q + Tz\), \(K_T = k(\sqrt[q^2]{-T})\).

An analogy between cyclotomic fields and cyclotomic function fields is obvious. The ring \(\mathbb{Z}\) of rational integers is considered as the subring of the endomorphism ring of the multiplicative group \(\mathbb{G}_{m,\mathbb{Q}}\) over the field \(\mathbb{Q}\) of rationals via

\[
\psi: \mathbb{Z} \ni n \to (x \mapsto x^n) \in \text{End}(\mathbb{G}_{m,\mathbb{Q}}),
\]
we find that the group $\mu_n$ of the $n$-th roots of unity is

$$\mu_n = \{ z \in \mathbb{Q}^\times | \psi(n)(z) = z^n = 1 \}.$$ 

Then, the $n$-th cyclotomic field is $\mathbb{Q}(\mu_n)$.

The $m$-th cyclotomic function field $K_m$ satisfies many properties similar to the $n$-th cyclotomic field $Q(\mu_n)$. For example, $K_m/k$ is a finite Abelian extension with the Galois group $\text{Gal}(K_m/k) \cong (\mathbb{Z}/m\mathbb{Z})^\times$. This extension is unramified outside $m$. There is also an analog of the maximal real subfield, namely, the subfield corresponds to the subgroup $(\mathbb{F}_m^\times)^\times$ of $\text{Gal}(K_m/k)$. We denote it by $K_m^+$ and call it the maximal real subfield of $K_m$.

Let $O_m$ and $O_m^+$ be the rings of integers of $K_m$ and $K_m^+$ respectively, which are the integral closures of $A$ in $K_m$ and $K_m^+$. These are Dedekind domains.

We denote the class numbers (the order of the group of divisor classes of degree zero) of $K_m$ and $K_m^+$ by $h_m$ and $h_m^+$. It is well known that $h_m^+ | h_m$. We denote by $h_m^*$ the quotient and call it the relative class number of $K_m$. We also denote the class numbers (the order of the Picard groups) of $O_m$ and $O_m^+$ by $h_m$ and $h_m^*$ respectively. In this case, it is also known that $h_m^* | h_m$. We denote by $h_m^*$ the quotient $h_m/h_m^*$, and call it the relative class number of $O_m$.

3. Determinant formulae for the relative class numbers of cyclotomic function fields

Jung and Ahn [1, 2] showed that the determinant formula of $h_m^+$ and $h_m^*$. We recall their results. Let $p(T) \in A$ be a monic irreducible polynomial of degree $d$. For $n \geq 1$, let $m = p(T)^n$. We set

$$M_m = \{ a \in A | a \neq 0, \deg(a) < \deg(m), (a, m) = 1 \},$$

$$M_m^+ = \{ a \in M_m | a : \text{monic} \},$$

$$M_m^* = M_m \setminus M_m^+.$$ 

For $a \in A$, let $\overline{a} \in M_m$ be the unique element that satisfies $a \equiv \overline{a} \pmod{m}$. Let $\text{sgn}(a)$ be the leading coefficient of $a$, and $\text{sgn}_m(a) := \text{sgn}(\overline{a})$. For $a \in M_m$, set $\overline{a} = a/\text{sgn}_m(a) \in M_m^*$. For $a, b \in M_m$, we set $\langle ab \rangle$ by

$$\langle ab \rangle := \begin{cases} 
1 & (\text{sgn}_m(ab) = 1), \\
0 & (\text{sgn}_m(ab) \neq 1).
\end{cases}$$

Then Jung-Ahn’s class number formula states that [2, Propositions 2.5, 2.6]:

$$h_m^* = | \det(\langle ab \rangle)_{a, b \in M_m^*} |,$$ 

$$h_m^+ = | \det(\langle ab \rangle)_{a, b \in M_m^+} |.$$ 

We remark that the size of these matrices are given by the following:

$$\# M_m^* = \varphi(m) \left( 1 - \frac{1}{q - 1} \right),$$

where $\varphi(m)$ is Euler’s totient function for polynomials. In this case $m = p(T)^n$, $\varphi(m) = q^{(n-1)d}(q^d - 1)$. The matrix in (1) is a $0/1$ symmetric matrix. It is known, by Yin [5, Lemma 3] that the relation between $h_m$ and $\tilde{h}_m$:

$$h_m = (q - 1)^d \tilde{h}_m^*,$$ 

where $s = q^{(n-1)d}(q^d - 1)/(q - 1) - 1$.

4. Note on 0/1 matrices and $\pm 1$ matrices

As we have just remarked, $\tilde{h}_m$ is given by the determinant of a $0/1$ symmetric matrix. We can rewrite it into a $\pm 1$ matrix by simple transformation: Set $r = \# M_m^* = \varphi(m) | 1 - (q - 1)/d(1 - 1)$, and $H = (h_{a, b})_{a, b \in M_m}$ as follows:

$$h_{a, b} = \begin{cases} 
-1 & (\text{sgn}_m(ab) = 1), \\
1 & (\text{sgn}_m(ab) \neq 1).
\end{cases}$$

Then we have

$$2^r \tilde{h}_m^* = \pm \det \begin{pmatrix} 1 & \cdots & 1 \\
\vdots & & \vdots \\
1 & & 1
\end{pmatrix} H.$$ 

We consider mainly $0/1$ matrices below.

5. Inequality for relative class numbers

It is well-known that the absolute value of the determinant of a complex matrix is bounded by the product of the norms of all the column vectors. For any complex square matrix $M = \langle m_{ij} \rangle$ of size $r$, let $m_j$ be the $j$-th column vector. Let $|m_j|$ be its Euclidean norm. Then we have Hadamard’s inequality:

$$|\det(M)| \leq \prod_{j=1}^r |m_j|.$$ 

If $M$ has bounded elements $|m_{ij}| \leq 1$ $(1 \leq i, j \leq r)$, then we have

$$|\det(M)| \leq r^2.$$ 

Applying this to (4) with $m = p(T)$, we have:

**Proposition 1.**

$$\tilde{h}_m^* \leq \frac{\left( (q-2)(q^d-1) + 1 \right) \left( (q-2)(q^d-1) + 1 \right)}{2 \sqrt{2(q^d-1)}}.$$ 

6. Numerical observation

We conducted some numerical observations to measure how close the determinant expression in (2) to the right-hand side of (6). Unless otherwise stated, we assume that $m$ is an irreducible monic polynomial $(n = 1)$ hereafter.

We observed that
- when $q = 3$, $\tilde{h}_m^*$ is close to Hadamard’s bound (this is a similar phenomenon to the cyclotomic field case). Cf. Table 1,
- when $q > 3$, $\tilde{h}_m^*$ is no longer close to Hadamard’s bound. Cf. Table 2.

We tabulate parts of these numerical observations:

When $q = 3$, $\tilde{h}_m^*$ tend to huge (Table 1).

On the other hand, when $q > 3$, $\tilde{h}_m^*$ is no longer huge (Table 2).
Table 1. Comparison of decimal digits of $\tilde{h} - m$ and the right-hand side of (6) bound ($q = 3$).

| $m$      | digits of $\tilde{h} - m$ | digits of RHS of (6) |
|----------|--------------------------|----------------------|
| $T^4 + T + 2$ | 17                       | 22                   |
| $T^5 + 2T + 1$ | 80                       | 91                   |
| $T^6 + T^3 + 2T + 2$ | 325                      | 359                  |

Table 2. Comparison of decimal digits of $\tilde{h} - m$ and the right-hand side of (6) ($q = 5, 7, 29$).

| $q$ | $m$      | digits of $\tilde{h} - m$ | digits of RHS of (6) |
|-----|----------|--------------------------|----------------------|
| 5   | $T^4 + 2$ | 198                      | 486                  |
| 7   | $T^3 + 3T + 5$ | 198          | 266                  |
| 29  | $T^2 + T + 20$ | 551          | 936                  |

Fig. 1. The size of matrices: 40. The dot is the digits of $\tilde{h} - m$, $q = 3$, $m = T^4 + T^3 + 2T + 1$.

Fig. 2. The size of matrices: 40. The dot is the digits of $\tilde{h} - m$, $q = 7$, $m = T^2 + 6T + 3$.

We calculate 100,000 samples of randomly generated symmetric 0/1 matrices of the same size as in the determinant formula (2). This computation had been performed by our program written in C using Pari library [6]. We observed that

- when $q = 3$, $\tilde{h} - m$ is quite huge than the determinants of randomly generated 0/1 symmetric matrices (cf. Fig. 1),
- when $q > 3$, $\tilde{h} - m$ is no longer larger than the determinants of randomly generated 0/1 symmetric matrices or is smaller than them (cf. Figs. 2 and 3).

7. Investigation of numerical observation

Rosen [7, Theorem 3] showed the following bound of the relative class number $\tilde{h} - m$ of $K_m$:

$$
\tilde{h} - m \leq \left( \frac{q^d - 1}{q - 1} \right) \frac{(q - 2)(q^d - 1)}{2(q - 1)^{d + 1}}.
$$

This bound is derived from the explicit forms of the zeta functions of $K_m$, more precisely, it is derived from the rationality of the zeta functions and the fact that the numerators of zeta functions are polynomials of degree $2g_m$, where $g_m$ is the genus of $K_m$.

We have, by (3):

**Proposition 2.**

$$
\tilde{h} - m \leq \left( \frac{q^d - 1}{q - 1} \right) \frac{(q - 2)(q^d - 1)}{2(q - 1)^{d + 1}}.
$$

The relationship between these two upper bounds (6) and (7) is given as follows by elementary calculation:

**Theorem.**

$$
\tilde{h} - m \leq \left( \frac{q^d - 1}{q - 1} \right) \frac{(q - 2)(q^d - 1)}{2(q - 1)^{d + 1}}.
$$

We remark that, for $q = 3$ in (8), (9), and putting $t = \frac{q^d - 1}{q - 1}$, we see that

$$
\tilde{h} - m \leq 2t \frac{t^2}{2t} \leq \left( t + 1 \right) \frac{t^2}{2t},
$$

which shows that these two upper bounds are close in this case, and explains Table 1 and Fig. 1.

On the other hand, for $q > 3$, the expressions in (8) and (9) are very different. This explains that $\tilde{h} - m$ is far less than the upper bound (9), which is given by Hadamard’s bound.
Acknowledgments

We are indebted to Professor Tetsuya Taniguchi (Kanazawa Institute of Technology), who initiated these questions about the size of determinants of ±1 matrices, which appear in the determinant formula of class numbers. We also thank Professor Shoichi Nakajima (Gakushuin) for his kind advice to authors. We thank the anonymous referee for careful reading of the manuscript, which improved the presentation of the publication.

References

[1] H. Jung, J. Ahn, Demjanenko matrix and recursion formula for relative class number over function fields, J. Number Theory, 98 (2003), 55–66.
[2] H. Jung, J. Ahn, On the relative class number of cyclotomic function fields, Acta Arith., 107 (2003), 91–101.
[3] F. Hazama, Demjanenko matrix, class number, and Hodge group, J. Number Theory, 34 (1990), 174–177.
[4] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.
[5] L. Yin, Stickelberger ideals and relative class numbers in function fields, J. Number Theory, 81 (2000), 162–169.
[6] PARI Group, Bordeaux, PARI/GP, Version 2.9.4, 2017, available from http://pari.math.u-bordeaux.fr/.
[7] M. Rosen, A note on the relative class number in function fields, Proc. Amer. Math. Soc., 125 (1997), 1299–1303.