JOURNAL OF NUMBER THEORY 52, 85–97 (1995)

# A Demjanenko Matrix for Abelian Fields of Prime Power Conductor

JONATHAN W. SANDS*

*Department of Mathematics and Statistics, University of Vermont, Burlington, Vermont 05405*

AND

WOLFGANG SCHWARZ

*Fachbereich Mathematik, Universität des Saarlandes, 66041 Saarbrücken, Germany*

*Communicated by K. A. Ribet*

Received July 13, 1993; revised August 31, 1993

We introduce a generalized Demjanenko matrix associated with an arbitrary abelian field of odd prime power conductor, and exhibit direct connections between this matrix and both the relative class number and the cyclotomic units of the field. Beyond using the analytic class number formula, all arguments are elementary. Combining the two connections yields a simple proof that the relative class number is odd if and only if all the totally positive cyclotomic units are squares of cyclotomic units, which was known by results of Hasse and Garbanati. An interesting feature of our new class number formula is its expression as the determinant of a matrix with relatively small integer entries. Thus we also easily obtain a reasonable upper bound on the relative class number. 

## I. INTRODUCTION

Fix a power $q = p^r$ of an odd prime $p$, let $G$ denote the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$ and let $M \subset G$ be defined by $M = \{\bar{a} \in G\colon 0 < a \leqslant (q-1)/2\}$. Thus $G$ is the disjoint union $-M \cup M$. The corresponding Demjanenko matrix can be defined using the characteristic function of the set $M$. For $\bar{a} \in G$, let $c_M(\bar{a}) = 1$ if $\bar{a} \in M$ and $c_M(\bar{a}) = 0$ if $\bar{a} \notin M$. The (modified) Demjanenko matrix $D_q$ may then be defined to have its rows and columns

* Research supported by National Security Agency Grant MDA904-89-H-2012 and the Deutsche Forschungsgemeinschaft.



0022-314X/95 $6.00

indexed by the elements of $M$ and its $(\bar{a}, \bar{b})$-entry equal to $c_M(\bar{a}\bar{b})$. We shall use the notation

$$D_q = (c_M(\bar{a}\bar{b}))_{a,b \in M}.$$

The determinant of the Demjanenko matrix $D_q$ provides a formula for the relative class number of the $q$th cyclotomic field $\mathbb{Q}(\zeta_q)$. This was established by Hazama in [7] when $q = p$, and noted for $q = p^r$ in general in [15]. Another basic property shown in [15] is that when $D_q$ is considered modulo 2, its rank determines the number of different configurations of positive and negative conjugates which occur among the real cyclotomic units of this field.

The goal of this work is to completely extend the theory we have just described to allow consideration of a quotient group of $G$ and the corresponding subfield of $\mathbb{Q}(\zeta_q)$. In Section II, we will define the appropriate Demjanenko matrix. Our main result, presented in Section III, is a determinant formula for the relative class number of the subfield. The connection between the Demjanenko matrix and the real cyclotomic units will be developed in Section IV. This leads to a simple proof that the parity of the relative class number equals the parity of the index of the squares of cyclotomic units in the group of totally positive cyclotomic units. Finally, we devote Section V to deriving an upper bound on the relative class number. Aside from the use of the analytic class number formula, all of our proofs are elementary.

We owe much to certain classical results. In 1955, Carlitz and Olson [3] transformed the analytic formula for the relative class number of $\mathbb{Q}(\zeta_p)$ into a simple multiple of the Maillet determinant. The classical literature (see [1, p. 346]) offers an alternate expression for the Bernoulli numbers in the analytic class number formula (see Lemma III.3). Using this alternate expression, for which the character values in the sum do not require any coefficients, one arrives instead at the determinant of a matrix of zeroes and ones, the Demjanenko matrix. This is the essence of Hazama's proof.

Coming more than three decades after the paper by Carlitz and Olson, Hazama's formula still seems a logical extension of their work. Indeed, Carlitz and Olson did show how to manipulate the Maillet matrix to obtain a matrix of zeroes and ones. It is not exactly the Demjanenko matrix, but a computation of Hazama reveals how closely the two are related. It is natural to seek a generalization of Hazama's formula, and that is exactly the subject of Section III of this paper. The entries of our generalized Demjanenko matrix will not necessarily be zeroes and ones, but their absolute values will be bounded by the relative degree of $\mathbb{Q}(\zeta_q)$ over the chosen subfield.

Carlitz [2] used his determinant formula to obtain an upper bound on the relative class number of $\mathbb{Q}(\zeta_p)$. Once we have our more general determinant formula, it is a simple matter to follow his example and obtain a similar result for any complex subfield of $\mathbb{Q}(\zeta_q)$. The Demjanenko matrix is well-suited for this purpose because there is clearly a good bound on its entries.

It would also be natural to generalize the Maillet matrix just as we have generalized the Demjanenko matrix. This has been done for the field $\mathbb{Q}(\zeta_q)$ by Kühnová in [8], and by Metsänkylä in [11], but seems not to have been done for subfields. In bounding the relative class number, such an approach would be expected to yield weaker results than those we have obtained here. (For instance, our result improves upon that of Carlitz for $\mathbb{Q}(\zeta_p)$, as explained at the end of section V.)

## II. The Generalized Demjanenko Matrix

Consider an arbitrary complex subfield $K$ of $\mathbb{Q}(\zeta_q)$. Of course $G$ is canonically isomorphic to the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, and so by Galois theory, $K$ will correspond to a subgroup $N$ of $G$ in such a way that $G/N$ is canonically isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$. The assumption that $K$ is complex implies that $-\bar{1} \notin N$, and furthermore that the cardinality $|N|$ of $N$ is odd, since $-\bar{1}$ is the only element of order 2 in the cyclic group $G$. Given such a field $K$, we can define an associated generalized Demjanenko matrix. Equivalently, we can associate such a matrix $D = D_{q,N}$ to any subgroup $N$ of $G$ having odd order. It is in fact more natural to pursue the latter approach, emphasizing the role of group theory in our arithmetic results on the relative class number and the real cyclotomic units of $K$.

In order to define the generalized Demjanenko matrix associated with the groups $G$ and $N$, let $M \subset G$ be as in the Introduction, and for each $\bar{a} \in G$, put

$$C(\bar{a}) = C_{q,N}(\bar{a}) = |\bar{a}N \cap M|,$$

$$C'(\bar{a}) = C'_{q,N}(\bar{a}) = |\bar{a}N \cap -M| = |N| - C(\bar{a}).$$

Choose a subset $R \subset M$ which forms a system of representatives for $G/(N \cdot \{\pm\bar{1}\})$, letting $\bar{1} \in R$. We could specify the choice of $R$ uniquely by requiring that its elements have the smallest possible positive residues modules $q$, and we could specify an order on the elements of $R$ by the size of these residues. It will be clear that our results do not depend on these choices. Our generalized Demjanenko matrix $D = D_{q,N}$ has its rows and columns indexed by the elements of $R$. Its $(\bar{a}, \bar{b})$-entry is defined to be $C(\bar{a}\bar{b}) - C'(\bar{b})$. Thus

$$D = D_{q,N} = (C(\bar{a}\bar{b}) - C'(\bar{b}))_{\bar{a}, \bar{b} \in R}.$$

When $N = \{\bar{1}\}$ and $R = M$, note that $C(\bar{a}\bar{b}) - C'(\bar{b}) = C(\bar{a}\bar{b}) = c_M(\bar{a}\bar{b})$, and so we obtain the Demjanenko matrix of the Introduction.

## III. The Relative Class Number and the Determinant of the Demjanenko Matrix

Let $\zeta_q$ be a primitive $q$th root of unity, let $K$ be a complex subfield of $\mathbb{Q}(\zeta_q)$, and let $N$ be the subgroup of $G$ corresponding to $K$ as in section II. Also let $K^+$ be the maximal real subfield of $K$. Thus $K^+$ corresponds to the subgroup $N \cdot \{\pm 1\}$ of $G$. We will be interested in the class numbers $h = h(K)$ and $h^+ = h(K^+)$ of $K$ and $K^+$ respectively, and especially the quotient $h^- = h^-(K) = h(K)/h^+(K)$, which we call the relative class number of $K$; it is known to be an integer [16, Thm. 4.10]. Beginning with the analytic class number formula, we will derive a formula for $h^-$ in terms of the determinant det $D_{q,N}$ of $D_{q,N}$.

In order to write the analytic class number formula, let $X$ denote the group of (irreducible complex-valued) characters of $G$ which are trivial on $N$. Then $X$ is naturally identified with the group of characters of $G/N$. A character $\chi$ is called even or odd depending on whether $\chi(-\bar{1})$ equals $+1$ or $-1$, respectively. Fix a choice of odd character $\varepsilon$. If $X^+ \subset X$ denotes the subgroup of even characters, then $X^+$ is naturally identified with the group of characters of $G/(N \cdot \{\subseteq \pm \bar{1}\})$. The collection of odd characters is denoted $X^-$ and coincides with the coset $\varepsilon X^+$. We set $\chi(\bar{a}) = 0$ when $\bar{a} \notin (\mathbb{Z}/q\mathbb{Z})^\times = G$. For a nontrivial $\chi \in X$, the first generalized Bernoulli number (see [16, p. 31]) may be expressed as

$$B_{1,\chi} = \frac{1}{q} \sum_{a=1}^{q} \chi(\bar{a})\, a.$$

Note that, since $q$ is a prime power, and $\chi \neq 1$, it makes no difference whether we view $\chi$ as a character mod $q$ (as we do) or modulo its conductor (as is usual for defining $B_{1,\chi}$).

We also need to fix the notation $E_K$ for the units of the ring of integers of $K$, $E_{K^+}$ for the units of the ring of integers of $K^+$, and $\mu_K$ for the roots of unity in $K$. Finally put $w_K = |\mu_K|$ and $Q_K = |E_K/(E_{K^+} \cdot \mu_K)|$.

Now we can state the analytic class number formula (see [16, Thm. 4.17]).

III.1. THEOREM (Analytic Class Number Formula).

$$h^-(K) = Q_K w_K \prod_{\chi \in X^-} \left(-\tfrac{1}{2} B_{1,\chi}\right).$$

Under our assumption that $K \subset \mathbb{Q}(\zeta_q)$ with $q = p^r$, we also have the following result of Hasse ([6, Satz 23]; see also [16, Cor. 4.13]).

III.2. PROPOSITION (Hasse).

$$Q_K = 1.$$

Like Hazama [7] and Feng [4], we find it advantageous to use an alternate expression for the generalized Bernoulli numbers $B_{1,\chi}$.

III.3. LEMMA. *If $\chi$ is a primitive odd character of $(\mathbb{Z}/f\mathbb{Z})^\times$, then*

$$-(2 - \bar{\chi}(2))\, B_{1,\chi} = \sum_{1 \leqslant a < f/2} \bar{\chi}(\bar{a}).$$

*Proof.* The proof is a straightforward computation. It appears in [1, p. 346] for quadratic characters and in [4] for the general case. ∎

Observe that the sum in the lemma remains the same if the upper limit of summation is changed from $f/2$ to any odd multiple of $f/2$, since $\sum_{a=1}^{f} \chi(\bar{a}) = 0$. Thus we may apply the lemma with $f = q$ for each $\chi \in X^-$.
Combining the previous three results, we then get

$$h^-(K) \prod_{\chi \in X^-} (2 - \chi(\bar{2})) = h^-(K) \prod_{\chi \in X^-} (2 - \bar{\chi}(\bar{2})) = \frac{w_K}{2^d} \prod_{\chi \in X^-} \left( \sum_{a=1}^{(q-1)/2} \chi(\bar{a}) \right),$$

where $d = |X^-| = |X^+| = [K^+ : \mathbb{Q}]$.

Now we evaluate the product on the left, generalizing a computation made by Hazama [7] and by Feng [4]. Note that this product is $2^d$ times the ratio of the Euler factors for the prime 2 in the Dedekind zeta functions of $K$ and $K^+$, evaluated at $s = 1$. Hence we actually have a special case of a standard and even more general computation.

Let $f$ (resp. $f^+$) be the order of the image of $\bar{2}$ in $G/N$ (resp. $G/(N \cdot \{\pm 1\})$), which is the same as the residue degree of each prime ideal above (2) in $K$ (resp. $K^+$).

III.4. LEMMA.

$$\prod_{\chi \in X^-} (2 - \chi(\bar{2})) = (2^{f^-} \pm 1)^{d/f^+}.$$

*the plus sign occurring when $f=2f^+$ is even, and the minus sign occurring when $f=f^+$ is odd.*

*Proof.* Since $X$ is cyclic, $\chi(2)$ runs through the $f$th roots of unity $2d/f$ times as $\chi$ runs through $X$. Letting $T$ be an indeterminate, we have

$$\prod_{\chi \in X} (T-\chi(2)) = (T^f-1)^{2d/f}.$$

Similarly

$$\prod_{\chi \in X^+} (T-\chi(2)) = (T^{f^+}-1)^{d/f^+}.$$

Taking the quotient yields

$$\prod_{\chi \in X^-} (T-\chi(2)) = (T^{f^+} \pm 1)^{d/f^+},$$

and setting $T=2$ yields the result. ∎

Making use of the lemma in the formula which preceded it produces the following proposition.

III.5. Proposition.

$$h^-(K) = \frac{w_K}{2^d F} \prod_{\chi \in X^-} \left( \sum_{a=1}^{(q-1)/2} \chi(\bar{a}) \right),$$

*where*

$$F = \begin{cases} (2^{f/2}+1)^{2d/f} & \text{if } 2 \mid f \\ (2^f-1)^{d/f} & \text{if } 2 \nmid f. \end{cases}$$

Now let $\pm\bar{a}$ denote the class of $\bar{a}$ in $G/\{\pm\bar{1}\}$ and let

$$\delta(\bar{a}) = \begin{cases} 1, & \bar{a} \in M \\ -1, & \bar{a} \in -M. \end{cases}$$

Then $\varepsilon\delta(\pm\bar{a})$ is well defined, as is $\psi(\pm\bar{a})$ for $\psi \in X^+$, and

$$\begin{aligned} \prod_{\chi \in X^-} \sum_{a=1}^{(q-1)/2} \chi(\bar{a}) &= \prod_{\psi \in X^+} \sum_{a=1}^{(q-1)/2} \psi(\bar{a})\, \varepsilon(\bar{a})\, \delta(\bar{a}) \\ &= \prod_{\psi \in X^+} \sum_{\pm a \in G/\{\pm\bar{1}\}} \psi(\pm\bar{a})\, \varepsilon\delta(\pm\bar{a}) \\ &= \prod_{\psi \in X^+} \sum_{A \in G/(N \cdot \{\pm\bar{1}\})} \psi(A) f(A), \end{aligned}$$

where $f(A) = \sum_{\pm a \in A} \varepsilon\delta(\pm\bar{a})$.

Splitting the sum up this way allows us to apply the Dedekind determinant formula ([9, Thm. 3.6.1]). From this, we obtain the equality

$$\prod_{\chi \in X^+} \sum_{A \in G/(N \cdot \{\pm \bar{1}\})} \psi(A) f(A) = \det_{A, B \in G/(N \cdot \{\pm \bar{1}\})} f(AB^{-1}).$$

Let $R$ denote a system of representatives of $G/(N \cdot \{\pm \bar{1}\})$ as in section II, and write $A = \bar{a}(N \cdot \{\pm \bar{1}\})$ and $B = \bar{b}(N \cdot \{\pm \bar{1}\})$, with $a, b \in R$. Since $-1 \notin N$, we have $(N \cdot \{\pm \bar{1}\})/\{\pm \bar{1}\} \cong N$, and

$$\begin{aligned} f(AB^{-1}) &= \sum_{\pm x \in \bar{a}\bar{b}^{-1}(N \cdot \{\pm \bar{1}\})} \varepsilon\delta(\pm \bar{x}) \\ &= \varepsilon(\bar{a}\bar{b}^{-1}) \sum_{x \in \bar{a}\bar{b}^{-1}N} \delta(\bar{x}) \\ &= \varepsilon(\bar{a}\bar{b}^{-1})(|\bar{a}\bar{b}^{-1}N \cap M| - |\bar{a}\bar{b}^{-1}N \cap -M|) \\ &= \varepsilon(\bar{a}\bar{b}^{-1})(C(\bar{a}\bar{b}^{-1}) - C'(\bar{a}\bar{b}^{-1})) \\ &= \varepsilon(\bar{a}\bar{b}^{-1})(2C(\bar{a}\bar{b}^{-1}) - |N|). \end{aligned}$$

At this point we have shown that

$$h^-(K) = \frac{w_K}{2^d F} \det_{a, b \in R} (\varepsilon(\bar{a}\bar{b}^{-1})(2C(\bar{a}\bar{b}^{-1}) - |N|)).$$

Multiplying the $\bar{a}$-row of the matrix by $\varepsilon(\bar{a})^{-1}$ and the $\bar{b}$-column by $\varepsilon(\bar{b})$ for each $\bar{a}$ and $\bar{b}$ cancels out the factor $\varepsilon(\bar{a}\bar{b}^{-1})$ without changing the determinant. We arrive at the formula

$$h^-(K) = \frac{w_K}{2^d F} \det \tilde{D},$$

with

$$\tilde{D} = (2C(\bar{a}\bar{b}^{-1}) - |N|)_{a, b \in R}.$$

We will use this matrix for bounding $h^-$ in Section V. Note that the entries of $\tilde{D}$ depend only on $\bar{b}N$, and up to sign even only on $\bar{b}(N \cdot \{\pm \bar{1}\})$. Replacing $\bar{b}^{-1}$ by $\bar{b}$ therefore only changes the order and the sign of some of the columns. The $\bar{1}$-row then has entries $2C(\bar{b}) - |N| = C(\bar{b}) - C'(\bar{b}) = |N| - 2C'(\bar{b})$. Adding it to all other rows and dividing them by two yields our matrix

$$D = (C(\bar{a}\bar{b}) - C'(\bar{b}))_{a, b \in R}$$

and the following theorem.

III.6. THEOREM.

$$h^{-}(K)=\frac{w_K}{2^dF}\det\tilde{D}=\pm\frac{w_K}{2F}\det D$$

*where*

$$F=\begin{cases}(2^{f/2}+1)^{2d/f} & \text{if } 2\mid f\\ (2^f-1)^{d/f} & \text{if } 2\nmid f\end{cases}$$

## IV. THE SIGNS OF CYCLOTOMIC UNITS AND THE 2-RANK OF THE DEMJANENKO MATRIX

In our case where $q$ is odd, the group $C$ of cyclotomic units of $K^+$ is the group generated by the numbers

$$\xi_a=N_{\mathbb{Q}(\zeta)/K}\left(-\frac{\zeta_q^a-\zeta_q^{-a}}{\zeta_q^1-\zeta_q^{-1}}\right)=\prod_{x\in N}-\frac{\zeta_q^{ax}-\zeta_q^{-ax}}{\zeta_q^x-\zeta_q^{-x}}.$$

Note that these are real because the numerator and denominator are both purely imaginary. Furthermore, $\xi_{\bar{1}}=-1$, since $|N|$ is odd. As $\{\pm\xi_a\}$ depends only on the class $\bar{a}(N\cdot\{\pm\bar{1}\})$, we may choose $\bar{a}\in R$; recall that we have asumed $\bar{1}\in R$.

We now consider $K\subset\mathbb{Q}(\zeta_q)$ as subfields of $\mathbb{C}$, setting $\zeta=\exp(2\pi i/q)$. Let $C_{\text{pos}}\subseteq C$ be the group of totally positive cyclotomic units of $K$; similarly, $E$ and $E_{\text{pos}}$ will denote the group of units and totally positive units, respectively.

IV.1 THEOREM. *Let $r$ denote the rank of $D$ over $\mathbb{F}_2$. Then $(C:C_{\text{pos}})=2^r$ and $(C_{\text{pos}}:C^2)=2^{d-r}$.*

*Proof.* Let $\sigma_{\bar{b}}\colon\mathbb{Q}(\zeta_q)\to\mathbb{Q}(\zeta_q)$ be the automorphism defined by $\sigma_{\bar{b}}(\zeta_q)=\zeta_q^b$. The automorphisms of $K^+$ are given by the restrictions of $\sigma_{\bar{b}}$ with $\bar{b}\in R$, since $R$ represents $G/(N\cdot\{\pm\bar{1}\})\cong\mathrm{Gal}(K^+/\mathbb{Q})$.

Let sgn: $\mathbb{R}^\times\to\mathbb{F}_2$ be the signum homomorphism, defined by $\mathrm{sgn}(z)=0$ if $z>0$, $\mathrm{sgn}(z)=1$ if $z<0$. Define the homomorphism Sgn: $C\to\mathbb{F}_2^d$ by

$$\mathrm{Sgn}(\xi)=(\mathrm{sgn}(\sigma_{\bar{b}}(\xi)))_{\bar{b}\in R}.$$

The kernel of Sgn is $\ker(\mathrm{Sgn})=C_{\text{pos}}$. Thus we obtain an induced isomorphism between $C/C_{\text{pos}}$ and the image Sgn$(C)$ of Sgn, which is generated by $\{\mathrm{Sgn}(\xi_a)\colon\bar{a}\in R\}$. We now compute $\mathrm{Sgn}(\xi_a)$. First

$$\mathrm{sgn}(\sigma_{\bar{b}}(\xi_a))=\mathrm{sgn}\left(\prod_{x\in N}-\frac{\zeta_q^{abx}-\zeta_q^{-abx}}{\zeta_q^{bx}-\zeta_q^{-bx}}\right).$$

Note that

$$\frac{\zeta_q^v - \zeta_q^{-v}}{i} = 2\sin(2\pi i v/q) > 0 \Leftrightarrow v \bmod q \in \left\{\bar{1}, ..., \overline{\frac{q-1}{2}}\right\}.$$

Therefore, with $c_M$ and $C$ as in Sections I and II,

$$\begin{aligned}\operatorname{sgn}(\sigma_{\bar{b}}(\xi_a)) &= \sum_{x \in N} \left(\operatorname{sgn}\left(\frac{\zeta_q^{abx} - \zeta_q^{-abx}}{i}\right) - \operatorname{sgn}\left(-\frac{\zeta_q^{bx} - \zeta_q^{-bx}}{i}\right)\right) \\ &= \sum_{x \in N} (c_M(\bar{a}\bar{b}\bar{x}) - c_M(\bar{b}\bar{x}) + 1) = C(\bar{a}\bar{b}) - C'(\bar{b}).\end{aligned}$$

Thus $\operatorname{Sgn}(\xi_a)$ is exactly the $\bar{a}$-row of $D$ mod 2. Therefore $\dim_{\mathbb{F}_2} \operatorname{Sgn}(C) = r$, and we have proved that $(C : C_{\text{pos}}) = 2^r$. The second equation of the theorem follows once we show that $(C : C^2) = 2^d$. To compute this index, note that $C$ has the same free rank $d-1$ as $E$, since $(E : C)$ is finite (see [6, Satz 4], for example). The torsion subgroup of $C$ is clearly $\{\pm 1\}$, since $C$ consists of real units. This gives the desired result. ∎

IV.2. Corollary. *The following statements are equivalent*:

(1) *$D$ is singular over $\mathbb{F}_2$*

(2) $2 \mid h^-$

(3) $C_{\text{pos}} \neq C^2$

(4) $2 \mid h^+$ *or* $E_{\text{pos}} \neq E^2$.

*Moreover, with $r$ as in* (4.1), $2^{d-r} \mid h^-$.

*Proof.* (1)$\Leftrightarrow$(2) follows from (III.6) upon noting that $w_K/2$ and $F$ are odd.
(1)$\Leftrightarrow$(3) follows from (IV.1).
(3)$\Leftrightarrow$(4): (compare [6, p. 27, (2)] or [15, Section 3]) We will use the important fact ([6, Satz 4]) that $(E : C) = h^+$. Let $(\varepsilon_a)_{a \in R \setminus \{\bar{1}\}}$ be a system of fundamental units of $K^+$, i.e., a $\mathbb{Z}$-basis of $E/\pm 1$. There is a non-singular matrix $A \in M_{d-1}(\mathbb{Z})$ such that

$$(\xi_a)_{a \in R \setminus \{\bar{1}\}} = A \cdot (\varepsilon_{\bar{a}})_{a \in R \setminus \{\bar{1}\}} \quad \text{in} \quad E/\pm 1,$$

where $\bar{a}$ is to be a row index. Inserting $\xi_{\bar{1}} = -1$ and $\varepsilon_{\bar{1}} := -1$ yields

$$(\xi_a)_{a \in R} = \begin{pmatrix} 1 & 0 \\ * & A \end{pmatrix} \cdot (\varepsilon_a)_{\bar{a} \in R} \quad \text{in} \quad E.$$

($*$ stands for a column of zeroes and ones giving the right signs.) Applying the homomorphism Sgn leads to

$$D \bmod 2 = \begin{pmatrix} 1 & 0 \\ * & A \end{pmatrix} \cdot \operatorname{sgn}(\varepsilon_a)_{a \in R}.$$

The same argument as in the proof of (IV.1) gives us $(E_{\mathrm{pos}} : E^2) = 2^{d-r'}$ where $r'$ is the rank of the matrix $\operatorname{Sgn}(\varepsilon_a)_{a \in R}$. Since $\pm \det A = (E : C) = h^+$, taking determinants yields the desired equivalence.

For the last statement, we use (III.6) and note that $2^{d-r} \mid \det D$. One can see this by taking matrices $A, B \in GL_{d-1}(\mathbb{Z})$ such that $ADB$ has diagonal form. Then $d - r$ is the number of even elements on the diagonal and $\det D$ is the product of the diagonal elements. ∎

## V. An Upper Bound for the Relative Class Number

We start with the class number formula

$$h^-(K) = \frac{w_K}{2^d F} \det \tilde{D},$$

where $\tilde{D} = (2C(\bar{a}\bar{b}^{-1}) - |N|)_{\bar{a}, \bar{b} \in R}$.

The entries of $\tilde{D}$ have absolute value at most $|N|$. Hadamard's inequality says that the determinant is bounded by the product of the lengths of the row vectors. So

$$|\det \tilde{D}| \leqslant (d^{1/2}|N|)^d = d^{d/2}|N|^d = (d|N|)^{d/2}\, |N|^{d/2} = (\phi(q)/2)^{d/2}\, |N|^{d/2}.$$

Combining this inequality with our class number formula yields a class number formula yields a class number bound.

V.1. Theorem. $h^-(K) \leqslant (w_K/F)(d^{1/2}|N|/2)^d = (w_K/F)(\phi(q)\, |N|/8)^{d/2}$ ∎

V.2. *Remark.* (1) *If $f$ is even, then $F > (2^{f/2})^{2d/f} = 2^d$. If $f = 1$ (in other words, if $\bar{2} \in N$), then $F = 1$. If $f$ is odd but $f \neq 1$, then $f \geqslant 3$ and consequently $F \geqslant 7^{d/3}$. This inequality clearly holds whenever $f \neq 1$. The following estimate is valid for arbitrary $f$. Put $t = 2^f - 1$ and note that* $\exp(1/t) \geqslant 1 + (1/t) = (t+1)/t$. *Thus*

$$F \geqslant (2^f - 1)^{d/f} = 2^d \left(\frac{t}{t+1}\right)^{d/f}$$
$$\geqslant 2^d \exp\left(-\frac{d}{tf}\right) \geqslant 2^d \exp\left(-\frac{d}{t}\right).$$

*In particular, for* $K=\mathbb{Q}(\zeta_q)$, *the congruence* $2^f \equiv 1 \pmod q$ *implies that* $t \geqslant q > \phi(q) = 2d$, *so* $F \geqslant 2^d \exp(-\frac{1}{2}) \geqslant 2^{d-1}$.

(2) *The entries of the matrix are* $2C(\bar{a}\bar{b}^{-1}) - |N| = |\bar{a}\bar{b}^{-1}N \cap M| - |\bar{a}\bar{b}^{-1}N \cap M|$. *One expects that about half of the class* $\bar{a}\bar{b}^{-1}N$ *should be in* $M$ *and half in* $-M$. *The difference is expected to be of order* $O(|N|^{1/2})$ *by probabilistic arguments, but this seems to be hard to prove.*

Bounds on relative class numbers have appeared prior to this primarily in two cases, the case of $K=\mathbb{Q}(\zeta_q)$ (or $N=\{\bar{1}\}$), and the case of $K \subset \mathbb{Q}(\zeta_p)$ (or $q=p$). Our method has provided a unified approach to both of these case. More importantly, it applies to new ones as well. This approch provides reasonable bounds in a simple manner, but does not improve upon results obtained by analytic methods in special situations. However, even in specail cases, our bound seems to be the best one obtained by means of the determinant method introduced by Carlitz.

We briefly present some explicit comparisons.

When specialized to the case of $K=\mathbb{Q}(\zeta_q)$, our theorem coincides exactly the main result of Feng [4]. He used the method of orthogonality relations for characters introduced by Metsänkylä in [13]. In this case, we have $N=\{\bar{1}\}$, $w_K=2q$, $d=\phi(q)/2$. Our estimate $F \geqslant 2^{d-1}$ then yields

$$h^-(\mathbb{Q}(\zeta_q)) \leqslant 2q \cdot 2^{1-\phi(g)/2}(\phi(q)/8)^{\phi(g)/4} = 4q(\phi(q)/32)^{\phi(q)/4}.$$

Feng's result actually superceded prior analytic results.

For the case of $K \subset \mathbb{Q}(\zeta_p)$, our theorem implies that

$$h^-(K) \leqslant (w_K/F)((p-1)/8)^{d/2} |N|^{d/2}.$$

This is to be compared with the inequalities

$$p^{(1-\varepsilon)d/2} < h^-(K) < p^{(1+\varepsilon)d/2}$$

of Metsänkylä [12, 14], which hold for all but a finite number of $p$ once $\varepsilon > 0$ is fixed.

In the most special case of $K=\mathbb{Q}(\zeta_p)$, our bound is

$$h^-(\mathbb{Q}(\zeta_p)) \leqslant (2p/F)((p-1)/8)^{(p-1)/4} \leqslant 4p((p-1)/32))^{(p-1)/4}.$$

This improves by a factor of $2^{p-3}$ on the original result of Carlitz [2] obtained from determinant formulas. The more precise analytic result of Masley and Montgomery [10] states that

$$h^-(\mathbb{Q}(\zeta_p)) = (p/4\pi^2)^{p/4} p^{3/4+7\theta},$$

for some $-1 \leqslant \theta \leqslant 1$.

Finally, note that there is indeed a well known general method for bounding the relative class number of a complex abelian number field. With a result such as (III.5) in hand, this method follows immediately from a lemma of Polya-Vinogradov. See [16, p. 214] for a short proof.

V.3. LEMMA (Polya–Vinogradov). *If $\chi$ is a non-trivial primitive character of $(\mathbb{Z}/f\mathbb{Z})^\times$, and $u$ is any positive integer, then*

$$\left|\sum_{a=1}^{u} \chi(a)\right| < f^{1/2}\log(f).$$

V.4. THEOREM. *Let $K$ be a complex abelian subfield of $\mathbb{Q}(\zeta_q)$ of degree $2d$ over $\mathbb{Q}$. Then*

$$h^-(K) < (w_K/F)(q^{1/2}\log(q)/2)^d$$

*Proof.* Consider the formula of Proposition (III.5):

$$h^-(K) = \frac{w_K}{2^d F} \prod_{\chi \in X^-} \left(\sum_{a=1}^{(q-1)/2} \chi(\bar{a})\right).$$

Each character $\chi$ is primitive modulo a non-trivial divisor $p^{k(\chi)}$ of $q = p^r$. As we have remarked before, the character sum for $\chi$ is the same whether we take the modulus to be $p^{k(\chi)}$ or $q$. Thus we may apply the Polya–Vinogradov lemma and conclude that

$$\left|\sum_{a=1}^{(q-1)/2} \chi(\bar{a})\right| < p^{k(\chi)/2}\log(p^{k(\chi)}) \leqslant q^{1/2}\log(q).$$

Taking the product yields the result. ∎

The comparison between (V.1) and (V.4) is clear; we have simply replaced the term $\phi(q)|N|/8 = q(1-1/p)\,|N|/8$ in (V.1) by $q\log^2(q)/4$. Thus the Polya–Vinogradov bound is preferable for $|N| > 2(p/(p-1))\log^2(q)$ and the Demjanenko matrix bound is preferable for $|N| < 2(p/(p-1))$ $\log^2(q)$. Clearly this method of using the Polya–Vinogradov lemma extends to other complex abelian fields as well.

## ACKNOWLEDGMENTS

We heartily thank T. Metsänkylä, R. Kučera, and L. Skula for useful discussions. We also thank the referee for a careful reading and illuminating comments.

## REFERENCES


1. Z. BOREVICH AND I. SHAFAREVICH, "Number Theory," Academic Press, London/New York, 1966.
2. L. CARLITZ, A generalization of Maillet's determinant and a bound for the first factor of the class number, *Proc. Amer. Math. Soc.* **12** (1961), 256–261.
3. L. CARLITZ AND F. R. OLSON, Maillet's determinant, *Proc. Amer. Math. Soc.* **6** (1955), 265–269.
4. K. FENG, On the first factor of the class number of a cyclotomic field, *Proc. Amer. Math. Soc.* **84** (1982), 479–482.
5. D. GARBANATI, Unit signatures, and even class numbers, and relative class numbers, *J. Reine Angew. Math.* **274/275** (1975), 376–384.
6. H. HASSE, "Über die Klassenzahl Abelscher Zahlkörper," Akademie-Verlag, Berlin, 1952.
7. F. HAZAMA, Demjanenko matrix, class numbers, and Hodge group, *J. Number Theory* **34** (1990), 174–177.
8. J. KÜHNOVÁ, Maillet's determinant $D_{p^n}$, *Arch. Math. 4 Scripta Fac. Sci. Nat. Ujep Brunensis* **15** (1979), 209–212.
9. S. LANG, "Cyclotomic Fields I and II," Springer-Verlag, Berlin/New York, 1990.
10. J. MASLEY AND H. MONTGOMERY, Cyclotomic fields with unique factorization, *J. Reine Angew. Math.* **286/287** (1976), 248–256.
11. T. METSÄNKYLÄ, Bemerkung über den ersten Faktor der Klassenzahl des Kreiskörpers, *Ann. Univ. Turku. Ser. AI* **105** (1967), 1–15.
12. T. METSÄNKYLÄ, Estimations for $L$-functions and the class numbers of certain imaginary cyclic fields, *Ann. Univ. Turku., Ser. AI* **140** (1970), 1–11.
13. T. METSÄNKYLÄ, Class number and $\mu$-invariants of cyclotomic fields, *Proc. Amer. Math. Soc.* **43** (1974), 199–200.
14. T. METSÄNKYLÄ, The index of irregularity of primes, *Exposit. Math.* **5** (1987), 143–156.
15. W. SCHWARZ, Demjanenko matrix and 2-divisibility of class numbers, *Arch. Math.* **60** (1993), 154–156.
16. L. C. WASHINGTON, "Introduction to Cyclotomic Fields," Springer-Verlag, Berlin/New York, 1982.