Tohoku Math. J.
65 (2013), 253–272

MAHLER MEASURE AND WEBER'S CLASS NUMBER PROBLEM IN THE CYCLOTOMIC $\boldsymbol{Z}_p$-EXTENSION OF $\boldsymbol{Q}$ FOR ODD PRIME NUMBER p

TAKAYUKI MORISAWA AND RYOTARO OKAZAKI

(Received August 29, 2011, revised September 3, 2012)

Abstract. Let p be a prime number and n a non-negative integer. We denote by $h_{p,n}$ the class number of the n-th layer of the cyclotomic $\boldsymbol{Z}_p$-extension of $\boldsymbol{Q}$. Let l be a prime number. In this paper, we assume that p is odd and consider the l-divisibility of $h_{p,n}$. Let f be the inertia degree of l in the p-th cyclotomic field and s the maximal exponent such that p^s divides $l^{p-1} - 1$. Set $r = \min\{n, s\}$. We define a certain explicit constant $G_1(p, r, f)$ in terms of the property of the residue class of l modulo p^r. If l is larger than $G_1(p, r, f)$, then the integer $h_{p,n}/h_{p,n-1}$ is coprime with l. Our proof refines Horie's method.

Introduction. Let p be a prime number and μ_m the group of all m-th roots of unity in $\boldsymbol{C}$ and put $\boldsymbol{Q}(\mu_{p^\infty}) = \bigcup_{n\geq 1} \boldsymbol{Q}(\mu_{p^n})$. We denote by $\boldsymbol{B}_{p,\infty}$ the unique real subfield of $\boldsymbol{Q}(\mu_{p^\infty})$ whose Galois group $\mathrm{Gal}(\boldsymbol{B}_{p,\infty}/\boldsymbol{Q})$ is topologically isomorphic to the p-adic integer ring $\boldsymbol{Z}_p$ as additive groups. Let $\boldsymbol{B}_{p,n}$ be the unique subfield of $\boldsymbol{B}_{p,\infty}$ which is cyclic of degree p^n over $\boldsymbol{Q}$ and $h_{p,n}$ its class number. In the case $p = 2$, Weber [26] showed that 2 does not divide $h_{2,n}$ for any positive integer n and he also showed $h_{2,1} = h_{2,2} = h_{2,3} = 1$. Based on these results, Weber asked whether $h_{2,n} = 1$ for any positive integer n. Then we consider a generalized version of his problem:

WEBER'S CLASS NUMBER PROBLEM. Is the class number $h_{p,n}$ equal to one for any positive integer n?

This problem has been studied by Bauer [1], Cohn [2], Masley [19], who showed $h_{2,4} = 1$. Later, van der Linden [17] showed $h_{2,5} = 1$ or 97. However, Komatsu and Fukuda [4] showed that 97 does not divide $h_{2,n}$ for any positive integer n. Hence we have $h_{2,5} = 1$. In [1] and [17], we know that $h_{p,n} = 1$ for $(p, n) \in \{(3, 1), (3, 2), (3, 3), (5, 1), (7, 1)\}$. Linden also showed that $h_{p,n} = 1$ for $(p, n) \in \{(2, 6), (3, 4), (5, 2), (11, 1), (13, 1)\}$ under the generalized Riemann hypothesis.

However, the direct calculation of $h_{p,n}$ is extremely difficult for large p^n. Therefore, in order to break the wall of the computational complexity, we study the l-divisibility of $h_{p,n}$ for a prime number l and for all positive integer n:

PROBLEM. Does a prime number l divide $h_{p,n}$ for any positive integer n?

2000 *Mathematics Subject Classification.* Primary 11R29; Secondary 11R06, 11R18.
Key words and phrases. Class number, $\boldsymbol{Z}_p$-extension, Mahler measure.
The first author is supported by JSPS Research Fellowships for Young Scientists.

In the case $l = p$, Iwasawa [16] proved that p does not divide $h_{p,n}$ for any positive integer n. Thus we study the non-p-part of $h_{p,n}$. Washington [25] showed that the l-part of $h_{p,n}$ is bounded as n tends to ∞ for each prime number l different from p. In a similar direction, Washington [24] also showed that l does not divide the relative class number $h^-(\boldsymbol{Q}(\mu_{5^n}))$ of $\boldsymbol{Q}(\mu_{5^n})$ for any positive integer n if $l^8 \not\equiv 1 \pmod{100}$.

Horie [8, 9, 10, 11] and Horie and Horie [12, 13, 14, 15] developed a method for proving l-indivisibility of $h_{p,n}$:

THEOREM 0.1 (Horie-Horie [13]). *Let p be a prime number, l a prime number different from p, f the inertia degree of l in $\boldsymbol{Q}(\mu_{2p})/\boldsymbol{Q}$ and p^s the exact power of p dividing $l^f - 1$. Then there exists an explicit positive constant $H(p, s, f)$ such that l does not divide $h_{p,n}$ for any positive integer n if l does not divide $h_{p,s-1}$ and is greater than $H(p, s, f)$.*

From Theorem 0.1 and numerical calculations, K. Horie and M. Horie showed that l does not divide $h_{p,n}$ for any positive integer n if $2 \leq p \leq 23$ and l is a primitive root modulo p^2. In the case $p = 2$, Fukuda and Komatsu [4, 5, 6] showed that l does not divide $h_{2,n}$ for any positive integer n if $l < 5 \times 10^8$ or $l \not\equiv \pm 1 \pmod{32}$. In the case $p = 3$, the first author [20, 21] showed that l does not divide $h_{3,n}$ for any positive integer n if $l < 4 \times 10^5$ or $l \not\equiv \pm 1$ (mod 27). Moreover, in the cases $p = 2$ and $p = 3$, we improved upon Theorem 0.1:

THEOREM 0.2 (The case $p = 2$ [22]). *A prime number l different from 2 is given. Let f be the inertia degree of l in $\boldsymbol{Q}(\mu_4)/\boldsymbol{Q}$ and 2^s the exact power of 2 dividing $l^f - 1$. We put $c = 2^{s-1}$. If l satisfies $l > (c!)^{1/f}$, then l does not divide $h_{2,n}$ for any positive integer n.*

THEOREM 0.3 (The case $p = 3$ [21]). *A prime number l different from 3 is given. Let f be the inertia degree of l in $\boldsymbol{Q}(\mu_3)/\boldsymbol{Q}$ and 3^s the exact power of 3 dividing $l^f - 1$. We put $c = 2 \cdot 3^{s-1}$. If l satisfies $l > (2^{c/2} \cdot c!)^{1/f}$, then l does not divide $h_{3,n}$ for any positive integer n.*

In this paper, we improve the bound for the prime number l in Theorem 0.1 for any odd prime number p.

THEOREM A. *Let p be an odd prime number, l a prime number different from p and n a positive integer. Choose s so that p^s is the exact power of p dividing $l^{p-1} - 1$. We put $r = \min\{n, s\}$ and $c = (p-1) \cdot p^{r-1}$. We denote by f the inertia degree of l in $\boldsymbol{Q}(\mu_p)/\boldsymbol{Q}$. We also put*

$$G_1(p, r, f) = \left(\left(\frac{\sqrt{6}p}{2}\right)^c \cdot c!\right)^{1/f}.$$

If l satisfies $l > G_1(p, r, f)$, then l does not divide $h_{p,n}$.

A more difficult argument gives a further improvement as follows.

THEOREM B. *Let p, l, n, s, r, c and f be the same as in Theorem* A. *We put*

$$G_{\mathrm{cyclo}}(p, r, f) = \left(\sqrt{6}^c \left(\frac{p^{p-2}((p-1)/2)!^2}{(p-1)!}\right)^{c/(p-1)} c!\right)^{1/f}.$$

If l satisfies $l > G_{\mathrm{cyclo}}(p, r, f)$, then l does not divide $h_{p,n}$.

We illustrate the improvement upon previous results by taking $p = 5$ as an example. In [13], K. Horie and M. Horie showed that l does not divide $h_{5,n}$ if $l \equiv a \pmod{25}$ for some $a \in \{2, 3, 4, 8, 9, 12, 13, 14, 17, 19, 22, 23\}$. For $l \equiv 6, 11, 16, 21 \pmod{25}$, that is, $s = 1$ and $f = 1$, we can verify

$$H(5, 1, 1) > 6 \times 10^{12}$$

and

$$G_1(5, 1, 1) = 33750\,, \quad G_{\mathrm{cyclo}}(5, 1, 1) = 18000\,.$$

Acknowledgments. The authors thank Professor Ken Yamamura who gave us useful advices for improving the paper. The authors also thank the referee and editors for reading this paper carefully and giving several valuable comments.

1. Horie unit. Let p be an odd prime number. We put $\zeta_n = \exp(2\pi\sqrt{-1}/p^n)$, $\boldsymbol{B}_n = \boldsymbol{B}_{p,n}$ and $h_n = h_{p,n}$, for the ease of notation. Given $k \in \boldsymbol{Z}$ which is prime to p, there exists a unique $p-1$-th root of unity $\omega(k) \in \boldsymbol{Z}_p$ such that

$$k \equiv \omega(k) \pmod{p}\,.$$

We call ω the Teichmüller character modulo p. For each $b \in \boldsymbol{Z}_p \setminus p^{n+1}\boldsymbol{Z}_p$, we put

$$\delta(b) = \frac{\zeta_1^b \zeta_{n+1}^b - \zeta_1^{-b} \zeta_{n+1}^{-b}}{\zeta_{n+1}^b - \zeta_{n+1}^{-b}}\,,$$

a cyclotomic unit in $\boldsymbol{Q}(\zeta_{n+1} + \zeta_{n+1}^{-1})$. It can be rewritten as

$$\delta(b) = \frac{\sin(2b(1 + p^n)\pi/p^{n+1})}{\sin(2b\pi/p^{n+1})}.$$

We define the n-th Horie unit

$$\eta_n = \prod_{k=1}^{(p-1)/2} \delta(\omega(k)) \tag{1}$$

as a cyclotomic unit in $\boldsymbol{B}_n$.

REMARK 1.1. The n-th Horie unit is a norm of $\delta(1)$ from $\boldsymbol{Q}(\zeta_{n+1} + \zeta_{n+1}^{-1})$ to $\boldsymbol{B}_n$.

REMARK 1.2. Since $\delta(\omega(p - k)) = \delta(\omega(k))$, we have

$$\eta_n = \prod_{k=(p+1)/2}^{p-1} \delta(\omega(k))\,.$$

Next, let E_n be the unit group of $\boldsymbol{B}_n$, σ the element of the Galois group $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{n+1})/\boldsymbol{Q}(\zeta_1))$ with $\zeta_{n+1}^\sigma = \zeta_{n+1}^{1+p}$ and $\tau = \sigma^{p^{n-1}}$. Then σ and τ generate $\mathrm{Gal}(\boldsymbol{Q}(\zeta_{n+1})/\boldsymbol{Q}(\zeta_1))$ and

$\mathrm{Gal}(\boldsymbol{Q}(\zeta_{n+1})/\boldsymbol{Q}(\zeta_n))$, respectively. An element α in $\boldsymbol{Z}[\zeta_n]$ is uniquely expressed in the form

$$\alpha = \sum_{i=0}^{(p-1)p^{n-1}-1} a_i \zeta_n^i \quad (a_i \in \boldsymbol{Z}) .$$

For each such α, we associate an element α_σ in the group ring $\boldsymbol{Z}[\mathrm{Gal}(\boldsymbol{Q}(\zeta_{n+1})/\boldsymbol{Q}(\zeta_1))]$ by

$$\alpha_\sigma = \sum_{i=0}^{(p-1)p^{n-1}-1} a_i \sigma^i .$$

Since

$$\begin{aligned} \boldsymbol{Z}[\zeta_n] &\cong \boldsymbol{Z}[\mathrm{Gal}(\boldsymbol{Q}(\zeta_{n+1})/\boldsymbol{Q}(\zeta_1))]/(1+\tau+\cdots+\tau^{p-1}) \\ \alpha &\mapsto \alpha_\sigma \bmod (1+\tau+\cdots+\tau^{p-1}) , \end{aligned}$$

the group ring $\boldsymbol{Z}[\zeta_n]$ acts on $(\boldsymbol{B}_{p,n}^\times)^{1-\tau}$. Horie [9] proved the following lemma.

LEMMA 1.3. *Let l be a prime number different from p and F an extension in $\boldsymbol{Q}(\zeta_n)$ of the decomposition field of l for $\boldsymbol{Q}(\zeta_n)/\boldsymbol{Q}$. Then l divides the integer h_n/h_{n-1} if and only if there exists a prime ideal $\mathfrak{L}$ of F dividing l such that $\eta_n^{\alpha_\sigma}$ is an l-th power in E_n for every element α of the integral ideal $l\mathfrak{L}^{-1}$ of F.*

2. Mahler measure and Schinzel's inequality. Let α be an algebraic number. Denote by $\deg\alpha$ its degree over $\boldsymbol{Q}$. Suppose that the minimal polynomial of α in $\boldsymbol{Z}[X]$ factors as

$$a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_{\deg\alpha})$$

over $\boldsymbol{C}$. The Mahler measure $M(\alpha)$ of α is defined by

$$M(\alpha) = |a| \prod_{j=1}^{\deg\alpha} \max\{1, |\alpha_j|\} .$$

It satisfies the following proposition.

PROPOSITION 2.1. *Let α, β be algebraic integers. Then we have the following* (1) through (4).

(1) Let r be a positive integer. If $\deg\alpha^r = \deg\alpha$, then we have $M(\alpha^r) = M(\alpha)^r$.
(2) If $\deg\alpha\beta \le \deg\alpha$ and $\deg\alpha\beta \le \deg\beta$, then we have $M(\alpha\beta) \le M(\alpha)M(\beta)$.
(3) If σ is an automorphism of $\boldsymbol{Q}(\alpha)$, then we have $M(\alpha^\sigma) = M(\alpha)$.
(4) If α is a unit, then we have $M(\alpha^{-1}) = M(\alpha)$.

Let $F(x)$ be the minimal polynomial of a unit in $\boldsymbol{B}_n$. We pay attention to Remark 1.16 in [3] and notice that $F(1)F(-1)$ has an exponential lower bound for the degree of $\boldsymbol{B}_n$. Now we can show the following inequality by tracing the proof of Theorem 1.14 in [3].

THEOREM 2.2. *Let ε be a totally real unit different from ± 1. Let $\mathfrak{M}$ be an ideal of $\boldsymbol{Q}(\varepsilon)$ containing $\varepsilon^2 - 1$. Then we have*

$$M(\varepsilon) \geq \left(\frac{C^{1/d} + \sqrt{C^{2/d} + 4}}{2} \right)^{d/2}$$

where $d = \deg \varepsilon$ and C is the absolute norm of $\mathfrak{M}$. In particular, we have

$$M(\varepsilon) \geq \left(\frac{1 + \sqrt{5}}{2} \right)^{d/2}.$$

PROOF. Let $F(x)$ be the minimal polynomial of ε and $\varepsilon^{(1)}, \dots, \varepsilon^{(d)}$ all conjugates of ε. We put $M = M(\varepsilon)$ and $C_F = |F(1)F(-1)|$. Then we have

$$\begin{aligned}
\log C_F &= \log \left(\prod_{i=1}^{d} |(1 - \varepsilon^{(i)})(1 + \varepsilon^{(i)})| \right) \\
&= \sum_{i=1}^{d} \log \left| \varepsilon^{(i)} - \frac{1}{\varepsilon^{(i)}} \right| \\
&= \sum_{i=1}^{d} \log 2 \sinh |\log |\varepsilon^{(i)}|| \\
&\leq \max \left\{ \sum_{i=1}^{d} \log 2 \sinh t_i \ ; \ t_i \geq 0, \sum_{i=1}^{d} t_i = 2 \log M \right\} \\
&\leq d \log 2 \sinh \frac{2 \log M}{d}.
\end{aligned}$$

This implies the inequality

$$M \geq \frac{C_F^{1/d} + \sqrt{C_F^{2/d} + 4}}{2}.$$

Since $C \leq C_F$, we obtain the assertion. $\square$

3. Upper bound of Mahler measure of Horie unit. In this section, we study an upper bound of Mahler measure of Horie unit.

LEMMA 3.1. *Let ν be a positive integer. Assume sequences $\{a_i\}_{i=1}^{\nu}$ and $\{b_i\}_{i=1}^{\nu}$ satisfy the properties $a_1 \geq a_2 \geq \cdots \geq a_\nu > 0$ and $0 < b_1 \leq b_2 \leq \cdots \leq b_\nu$, respectively. Let λ be the largest number such that $a_\lambda \geq b_\lambda$ if $a_1 \geq b_1$ or 0 otherwise. Let ϕ and ψ be injective maps from $\{1, 2, \dots, \mu\}$ to $\{1, 2, \dots, \nu\}$ for $0 \leq \mu \leq \nu$. Then we have*

$$\prod_{i=1}^{\mu} \frac{a_{\phi(i)}}{b_{\psi(i)}} \leq \prod_{i=1}^{\lambda} \frac{a_i}{b_i},$$

where the left-hand side reads 1 if it is an empty product.

PROOF. Obviously, we have

$$\prod_{i=1}^{\mu} a_{\phi(i)} \leq \prod_{i=1}^{\mu} a_i\,, \quad \prod_{i=1}^{\mu} b_{\psi(i)} \geq \prod_{i=1}^{\mu} b_i\,.$$

Hence we have

$$\prod_{i=1}^{\mu} \frac{a_{\phi(i)}}{b_{\psi(i)}} \leq \prod_{i=1}^{\mu} \frac{a_i}{b_i}\,.$$

On the other hand, the function

$$\mu \mapsto \prod_{i=1}^{\mu} \frac{a_i}{b_i}$$

takes its maximum at $\mu = \lambda$. □

We put $N = p^n$ and $\Theta = \pi/(2pN)$. Let η_n be the n-th Horie unit in (1). The definition of the Mahler measure implies

$$M(\eta_n) \leq \prod_{j=1}^{(pN-1)/2} \max\{1, |\delta(j)|\}\,.$$

We put $S = \{|\sin(4j\Theta)|\}_{j=1}^{(pN-1)/2}$. Since $\delta(j) = |\sin(4j(1+N)\Theta)|/|\sin(4j\Theta)|$, the numerator and the denominator of $\delta(j)$ are in S. Since $\sin(4j\Theta) = \sin(2(pN-2j)\Theta)$, we have

$$S = \left\{\sin(2j\Theta)\ ;\ j = 1, 2, \ldots, \frac{pN-1}{2}\right\}.$$

Then we have

$$M(\eta_n) \leq \prod_{j=1}^{\lfloor (pN-1)/4 \rfloor} \frac{\sin((pN+1-2j)\Theta)}{\sin(2j\Theta)}$$

from Lemma 3.1. Since

$$\sin((pN+1-2j)\Theta) = \cos((2j-1)\Theta)\,,$$

we have

$$\begin{aligned} M(\eta_n) &\leq \prod_{j=1}^{\lfloor (pN-1)/4 \rfloor} \frac{\cos((2j-1)\Theta)}{\sin((2j-1)\Theta)} \\ &= \prod_{j=1}^{\lfloor (pN-1)/4 \rfloor} \cot((2j-1)\Theta)\,. \end{aligned}$$

We will estimate the logarithm of the right-hand side by using a certain integral. For this purpose, we verify the convexity of the function $\log\cot\theta$ on the interval $0 < \theta < \pi/4$. Indeed, we have

$$\frac{d}{d\theta}\log\cot\theta = -\frac{1}{\sin\theta\cos\theta} < 0$$

and

$$\frac{d^2}{d\theta^2} \log \cot \theta = \frac{\cos 2\theta}{(\sin \theta \cos \theta)^2} > 0 .$$

Therefore, we have

$$\frac{\pi}{pN} \sum_{j=1}^{\lfloor (pN-1)/4 \rfloor} \log \cot((2j-1)\Theta) < \int_0^{\pi/4} \log \cot t \, dt .$$

This implies the inequality

$$M(\eta_n) < \exp\left(\frac{pN}{\pi} \int_0^{\pi/4} \log \cot t \, dt \right) .$$

Here, we put the Lobachevsky function

$$L(\theta) = \int_0^{\theta} \log \cot t \, dt$$

for $0 \le \theta < \pi/2$ (see [7], [18]). Then we get the following lemma.

LEMMA 3.2. *We have*

$$L(\theta) = \sum_{m=0}^{\infty} \frac{1}{(2m+1)^2} \sin(2(2m+1)\theta) .$$

By the above lemma, we have

$$L\left(\frac{\pi}{4}\right) = \sum_{m=0}^{\infty} \frac{(-1)^m}{(2m+1)^2} .$$

The right-hand side is called Catalan's constant. Its value is evaluated as follows

$$L\left(\frac{\pi}{4}\right) = 0.915965594 \cdots .$$

Hence we have

$$\frac{pN}{\pi} L\left(\frac{\pi}{4}\right) < 0.291560904 \cdot pN .$$

Therefore, we have the following lemma.

LEMMA 3.3. *We have*

$$M(\eta_n) < \exp(0.291560904 \cdot pN) .$$

4. Minkowski convex body theorem for Theorem A. Let l be a prime number different from p, n a positive integer and p^s the exact power of p dividing $l^{p-1} - 1$. We put $r = \min\{n, s\}$, $q = p^{r-1}$, $c = (p-1)q$ and $\zeta = \zeta_r$. In this section, we consider the map

$$(2) \qquad \mu : \boldsymbol{Q}(\zeta) \to \boldsymbol{C}^c , \quad \alpha \mapsto \overrightarrow{\alpha} := (\alpha^{\rho})_{\rho \in \mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})} ,$$

and the $\boldsymbol{R}$-vector space

$$(3) \qquad W = \boldsymbol{R}\overrightarrow{1} + \boldsymbol{R}\overrightarrow{\zeta} + \cdots + \boldsymbol{R}\overrightarrow{\zeta^{c-1}} \cong \boldsymbol{R}^c , \quad \sum_{j=0}^{c-1} a_j \overrightarrow{\zeta^j} \mapsto (a_0, a_1, \ldots, a_{c-1}) .$$

We put

$$X_1 = \left\{ \sum_{i=0}^{c-1} a_i \overrightarrow{\zeta_r^i} \in W \ ; \ a_0, \ldots, a_{c-1} \in \boldsymbol{R}, \ |a_0| + |a_1| + \cdots + |a_{c-1}| \leq \frac{2l}{\sqrt{6}p} \right\}$$

and define $|\cdot|_1$ on $\boldsymbol{Z}[\zeta_r]$ by

$$|a_0 + a_1\zeta + \cdots + a_{c-1}\zeta^{c-1}|_1 = |a_0| + |a_1| + \cdots + |a_{c-1}| \,.$$

Now we apply the Minkowski convex body theorem with respect to the volume on W induced by the standard volume on $\boldsymbol{R}^c$ by (3) to see:

LEMMA 4.1. *Let l, n, s, r, c and X_1 be as above and $\mathfrak{L}$ a prime ideal of $\boldsymbol{Q}(\zeta_r)$ dividing l. We denote by f the inertia degree of $\mathfrak{L}$ in $\boldsymbol{Q}(\zeta_r)/\boldsymbol{Q}$. If l satisfies $l^f > (\sqrt{6}p/2)^c \cdot c!$, then there exists a non-zero element $\overrightarrow{\alpha}$ in $X_1 \cap \mu(l\mathfrak{L}^{-1})$. This α lies in $l\mathfrak{L}^{-1}$ and satisfies $|\alpha|_1 \leq 2l/\sqrt{6}p$.*

5. Proof of Theorem A. Let l be a prime number different form p, p^s the exact power of p dividing $l^{p-1} - 1$ and n a positive integer. We put $N = p^n$, $r = \min\{n, s\}$ and $c = (p-1)\cdot p^{r-1}$. We denote by f the inertia degree of l in $\boldsymbol{Q}(\zeta_r)/\boldsymbol{Q}$. Assume that l satisfies $l^f > (\sqrt{6}p/2)^c \cdot c!$. We also assume that l divides h_n/h_{n-1}. By Lemma 1.3 and Lemma 4.1, there exist a prime ideal $\mathfrak{L}$ in $\boldsymbol{Q}(\zeta_r)$ lying above l, an element α in $l\mathfrak{L}^{-1}$ and a unit ε in E_n such that

$$\eta_n^{\alpha_\sigma} = \varepsilon^l \,, \quad |\alpha|_1 < \frac{2l}{\sqrt{6}p} \,. \tag{4}$$

By Theorem 2.2, we have

$$M(\varepsilon) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{N/2} > \exp(0.240605912 \cdot N) \,. \tag{5}$$

Since $\deg \varepsilon^l = \deg \varepsilon$ and $\deg \eta_n^{\alpha_\sigma} \leq \deg \eta_n$, we have

$$M(\varepsilon^l) = M(\varepsilon)^l \tag{6}$$

and

$$M(\eta_n^{\alpha_\sigma}) \leq M(\eta_n)^{|\alpha|_1} \,. \tag{7}$$

By (4), (5), (6), (7) and Lemma 3.3, we have

$$\begin{aligned} \exp(0.240605912 \cdot Nl) \leq M(\varepsilon)^l = M(\varepsilon^l) &= M(\eta_n^{\alpha_\sigma}) \\ &\leq M(\eta_n)^{|\alpha|_1} \\ &< \exp\left(0.291560904 \cdot pN \cdot \frac{2l}{\sqrt{6}p}\right) . \end{aligned}$$

Hence we have

$$0.240605912 < 0.291560904 \cdot \frac{2}{\sqrt{6}} = 0.238058481 \cdots .$$

Contradiction establishes Theorem A.

6. Volume of a certain convex body. To prove Theorem B, we consider another convex body.

Let p be an odd prime number and r a positive integer. Put $q = p^{r-1}$, $c = (p-1)q$, $\zeta = \zeta_r$ and $\xi = \zeta_1$. We also put

$$\mathcal{B} = \left\{ \sum_{i=0}^{c-1} s_i t_i \overrightarrow{\zeta^i} \ ; \ s_i \in \{+1, -1\}, 0 \le t_i \le 1, (i = 0, 1, \dots, c-1), \sum_{i=0}^{c-1} t_i \le 1 \right\}$$

where $\overrightarrow{\zeta^i}$ is defined in Section 4. In this section, we consider the volume of $\mathcal{B}$.

6.1. The convex hull of standard vectors. We consider more general situations. Let $2 \le \nu \in \boldsymbol{Z}$ and V the linear space

$$V = \boldsymbol{R}^{\nu} .$$

Denote by $\boldsymbol{e}_1, \boldsymbol{e}_2 \dots, \boldsymbol{e}_\nu$ the standard basis for V and set

$$\boldsymbol{d} = \boldsymbol{e}_1 + \boldsymbol{e}_2 + \dots + \boldsymbol{e}_\nu .$$

For any set $\mathcal{M}$ in V, we denote by $\hat{\mathcal{M}}$ the convex hull of $\mathcal{M}$. We also set $\mathcal{N} = \{1, 2, \dots, \nu\}$.

We consider the symmetric convex hull $\mathcal{B}_\nu$ of the set $\mathcal{R} = \{\boldsymbol{d}, -\boldsymbol{d}, +\boldsymbol{e}_i, -\boldsymbol{e}_i \ ; \ i \in \mathcal{N}\}$:

$$\mathcal{B}_\nu = \hat{\mathcal{R}} = \left\{ s_0 t_0 \boldsymbol{d} + \sum_{i=1}^{\nu} s_i t_i \boldsymbol{e}_i \ ; \ s_j \in \{+1, -1\}, 0 \le t_j \le 1, (j = 0, 1, \dots, \nu), \sum_{i=0}^{\nu} t_i \le 1 \right\} .$$

In Subsection 6.3, we will calculate its volume $\mathrm{vol}(\mathcal{B}_\nu)$, where vol denotes the Lebesgue measure on V.

Define the norm $|\cdot|_{\mathrm{cyclo}}$ on V by

$$|\boldsymbol{v}|_{\mathrm{cyclo}} = \inf\{x \in \boldsymbol{R}_{\ge 0} \ ; \ \boldsymbol{v} \in x\mathcal{B}_\nu\} .$$

Then, for $\boldsymbol{v} \in V$, we have

$$|\boldsymbol{v}|_{\mathrm{cyclo}} = \min\{x \in \boldsymbol{R}_{\ge 0} \ ; \ \boldsymbol{v} \in x\mathcal{B}_\nu\} < +\infty .$$

We also denote by $|\cdot|_{\mathrm{cyclo}}$ the norm on V^K defined by

$$|(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_K)|_{\mathrm{cyclo}} = \sum_{i=1}^{K} |\boldsymbol{v}|_{\mathrm{cyclo}} .$$

Let

$$\mathcal{B}_\nu^{(K)} = \{(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_K) \in V^K \ ; \ |(\boldsymbol{v}_1, \boldsymbol{v}_2, \dots, \boldsymbol{v}_K)|_{\mathrm{cyclo}} \le 1\} .$$

In Subsection 6.5, we will calculate its volume $\mathrm{vol}^{(K)}(\mathcal{B}_\nu^{(K)})$, where $\mathrm{vol}^{(K)}$ denotes the Lebesgue measure on V^K.

6.2. A decomposition into simplices. The symmetric convex body $\mathcal{B}_\nu$ contains the convex hull $\mathcal{C}_\nu$ of the set $\mathcal{Q} = \{+\boldsymbol{e}_i, -\boldsymbol{e}_i\ ;\ i \in \mathcal{N}\}$:

$$\mathcal{C}_\nu = \left\{ \sum_{i=1}^{\nu} s_i t_i \boldsymbol{e}_i\ ;\ s_j \in \{+1, -1\}, 0 \leq t_j \leq 1, (j \in \mathcal{N}); \sum_{i=1}^{\nu} t_i \leq 1 \right\}.$$

For an arbitrary subset I of $\{1, 2, \ldots, \nu\}$, we define

$$\mathcal{V}_I = \{+\boldsymbol{e}_i, -\boldsymbol{e}_j; i \in I, j \notin I\}; \quad \mathcal{F}_I = \widehat{\mathcal{V}_I}.$$

Then, $\mathcal{F}_I$ with $I \subset \{1, 2, \ldots, \nu\}$ form the facets of $\mathcal{C}_\nu$. We set

$$\mathcal{S}_I(P) = \widehat{\{P\} \cup \mathcal{F}_I}\,.$$

Obviously, $\mathcal{S}_I(P)$ is a simplex of ν-dimension.

The symmetric convex body $\mathcal{C}_\nu$ has the following decomposition into simplices:

$$\mathcal{C}_\nu = \bigcup_{I \subset \mathcal{N}} \mathcal{S}_I(\boldsymbol{o}),$$

where $\boldsymbol{o} = (0, 0, \ldots, 0)$ is the origin of V.

LEMMA 6.1. *The symmetric convex body $\mathcal{B}_\nu$ is decomposed into a non-overlapping union of ν-dimensional closed simplices as follows:*

$$\mathcal{B}_\nu = \bigcup_{I \subset \mathcal{N}} \mathcal{S}_I(\boldsymbol{o}) \cup \bigcup_{I \subset \mathcal{N};\ 2|I| > \nu} \mathcal{S}_I(+\boldsymbol{d}) \cup \bigcup_{I \subset \mathcal{N};\ 2|I| < \nu} \mathcal{S}_I(-\boldsymbol{d})\,.$$

PROOF. Obviously, $\mathcal{B}_\nu$ contains the right-hand side. It suffice to prove that $\mathcal{B}_\nu$ is contained in the right-hand side.

Let $P \in \mathcal{B}_\nu \setminus \mathcal{C}_\nu$. Then, there exist $x, y, z \in [0, 1]$ and $Q \in \mathcal{C}_\nu$ such that $P = xQ + y(+\boldsymbol{d}) + z(-\boldsymbol{d})$ and $x + y + z = 1$. Let $b = +1$ or -1 according as $y \geq z$ or not. Then, we have $P = |y - z|(b\boldsymbol{d}) + (xQ + (y + z - |y - z|)\boldsymbol{o})$. Thus, P lies on the line segment $\mathcal{L}$ connecting one of $\pm\boldsymbol{d}$ to some point Q' of $\mathcal{C}_\nu$. Since $\mathcal{B}_\nu$ is a symmetric convex body, we may assume that the sign in front of $\boldsymbol{d}$ is positive. The closest point Q'' in $\mathcal{L} \cap \mathcal{C}_\nu$ is uniquely determined since $\mathcal{C}_\nu$ is topologically closed while $Q' \in \mathcal{C}_\nu$, $\boldsymbol{d} \notin \mathcal{C}_\nu$. By the convexity of $\mathcal{C}_\nu$, the line segment connecting Q' to Q'' is contained in $\mathcal{C}_\nu$. Thus, the point P lies on the line segment connecting $\boldsymbol{d}$ to Q''.

Write $Q'' = (x_1, x_2, \ldots, x_\nu)$. Then, we have

$$-1 \leq x_i \leq +1\,, \quad (i \in \mathcal{N})\,; \quad \sum_{i=1}^{\nu} |x_i| = 1\,.$$

By symmetry of the set $\mathcal{B}_\nu$ with respect to permutation of the coordinates, we may assume

$$+1 \geq x_1 \geq x_2 \geq \cdots \geq x_m \geq 0 > x_{m+1} \geq x_{m+2} \geq \cdots \geq x_{m+n} \geq -1,$$

where $m + n = \nu$. An arbitrary point $Y = (y_1, y_2, \ldots, y_\nu)$ on the line segment connecting $\boldsymbol{d}$ to Q'' is written as

$$Y = t\boldsymbol{d} + (1 - t)(x_1, x_2, \ldots, x_\nu)\,, \quad 0 \leq t \leq 1\,.$$

For sufficiently small positive t, we have

$$\begin{aligned} |y_1| + |y_2| + \cdots + |y_\nu| &= \sum_{i=1}^{m} (t + (1-t)\,|x_i|) + \sum_{j=1}^{n} \bigl(-t + (1-t)\,|x_{m+j}|\bigr) \\ &= t\,(m-n) + (1-t) \sum_{k=1}^{\nu} |x_k| \\ &= t(m-n-1) + 1\,. \end{aligned}$$

Here, by the choice of Q'', the left-hand side is larger than 1. Therefore, we have $m > n$.

Set $I = \{1, 2, \ldots, m\}$. Then, $(x_1, x_2, \ldots, x_\nu) \in \mathcal{F}_I$ with $2|I| > \nu$. We now see $P \in \mathcal{S}_I(+\boldsymbol{d})$.

Ambiguity in the choice of I such that $(x_1, x_2, \ldots, x_\nu) \in \mathcal{F}_I$ only occurs if $x_k = 0$ for some k. In this case P belongs to the convex hull of the set $\{\boldsymbol{d}, +\boldsymbol{e}_i, \boldsymbol{e}_j\ ;\ x_i > 0; x_j < 0\}$ consisting less than $\nu + 1$ points. This convex hull has smaller dimension than ν. We now see that our union of the lemma is non-overlapping.

6.3. The volume of each simplex. By decomposing into simplices and evaluating the volume of each simplex, we show the following proposition.

PROPOSITION 6.2. *We have*

$$\operatorname{vol}(\mathcal{B}_\nu) = \begin{cases} \dfrac{2}{(m!)^2} & \textit{if } \nu = 2m+1\,, \\ \dfrac{2m+1}{(m!)^2} & \textit{if } \nu = 2m\,. \end{cases} \tag{8}$$

We can modify (8) *into the following formula*, *which is a bit simpler*

$$\operatorname{vol}(\mathcal{B}_\nu) = \frac{2^\nu}{\nu!} B_m = \operatorname{vol}(\widehat{\mathcal{M}}) B_m\,,$$

where we put,

$$B_m = \frac{(2m+1)!}{2^{2m} m!^2}\,, \quad m = \left\lfloor \frac{\nu}{2} \right\rfloor \tag{9}$$

$$\operatorname{vol}(\widehat{\mathcal{M}_\nu}) = \frac{2^\nu}{\nu!}\,, \quad \mathcal{M}_\nu = \{\boldsymbol{e}_i, -\boldsymbol{e}_i\ ;\ 1 \le i \le \nu\}\,.$$

We begin with the following proposition.

PROPOSITION 6.3. *Put* $M_n = \sum_{k=0}^{2k<n} \binom{n}{k} (n - 2k - 1) + 2^{n-1}$. *Then we have*

$$\operatorname{vol}(\mathcal{B}_\nu) = \frac{2}{\nu!} M_\nu\,.$$

In the following lemma, we evaluate this combinatorial sum.

LEMMA 6.4. *We have*

$$M_{2n} = \frac{2n+1}{2} \binom{2n}{n}\,, \quad M_{2n+1} = (2n+1) \binom{2n}{n}\,.$$

Then Proposition 6.2 follows immediately from Proposition 6.3 and Lemma 6.4.

PROOF OF PROPOSITION 6.3. Let column vectors $\boldsymbol{e}'_1, \boldsymbol{e}'_2, \dots, \boldsymbol{e}'_{\nu+1}$ be the standard basis of $\boldsymbol{R}^{\nu+1}$. Let $\boldsymbol{v} \in V \to \tilde{\boldsymbol{v}} \in \boldsymbol{R}^{\nu+1}$ be the map

$$(z_1, z_2, \dots, z_\nu) \mapsto {}^t(z_1, z_2, \dots, z_\nu, 1)\,.$$

Then, we have

$$\operatorname{vol}(\mathcal{S}_I(\boldsymbol{v})) = \frac{1}{\nu!}\,|\det(\widetilde{s_1\boldsymbol{e}_1}, \widetilde{s_2\boldsymbol{e}_2}, \dots, \widetilde{s_\nu\boldsymbol{e}_\nu}, \tilde{\boldsymbol{v}})|\,,$$

where $s_i = +1$ or -1 according as $i \in I$ or not. In particular,

$$\operatorname{vol}(\mathcal{S}_I(\boldsymbol{d})) = \frac{1}{\nu!}\left|\det\left(\widetilde{s_1\boldsymbol{e}_1}, \widetilde{s_2\boldsymbol{e}_2}, \dots, \widetilde{s_\nu\boldsymbol{e}_\nu}, \widetilde{\boldsymbol{d}}\right)\right|\,,$$

We perform the column operation of subtracting $s_i\widetilde{s_i\boldsymbol{e}_i}$ $(i \in \mathcal{N})$ from the last column on the matrix. Then, we get

$$\operatorname{vol}(\mathcal{S}_I(\boldsymbol{d})) = \frac{1}{\nu!}\,|\det(\widetilde{s_1\boldsymbol{e}_1}, \widetilde{s_2\boldsymbol{e}_2}, \dots, \widetilde{s_\nu\boldsymbol{e}_\nu}, (\nu+1-2|I|)\widetilde{\boldsymbol{o}})| = \frac{2|I|-\nu-1}{\nu!},$$

provided $2|I| > \nu$. By symmetry, we also get

$$\operatorname{vol}(\mathcal{S}_I(-\boldsymbol{d})) = \frac{2(\nu-|I|)-\nu-1}{\nu!} = \frac{\nu-2|I|-1}{\nu!}$$

provided $2|I| < \nu$. We now see

$$\operatorname{vol}(\mathcal{B}_\nu) = \frac{2}{\nu!}\left(\sum_{k=0}^{2k<\nu}\binom{\nu}{k}(\nu-2k-1)+2^{\nu-1}\right) = \frac{2}{\nu!}M_\nu\,.$$

□

Hacene Belbachir kindly gave us permission to include his proof of Lemma 6.4.

PROOF OF LEMMA 6.4. We put $S_n = \sum_{k=0}^{2k<n}\binom{n}{k}$ and $T_n = \sum_{k=0}^{2k<n} k\binom{n}{k}$. Using the fact that

$$k\binom{n}{k} = n\binom{n-1}{k-1},$$

we have

$$T_n = n\sum_{k=0}^{2k<n-2}\binom{n-1}{k}.$$

Now using the symmetry of binomial coefficient, we have

$$S_{2n} = 2^{2n-1} - \frac{1}{2}\binom{2n}{n}, \quad S_{2n+1} = 2^{2n}$$

and

$$T_{2n} = n2^{2n-1} - n\binom{2n}{n}, \quad T_{2n+1} = (2n+1)2^{2n-1} - \frac{2n+1}{2}\binom{2n}{n}.$$

Since $M_n = (n-1)S_n - 2T_n + 2^{n-1}$, we have

$$M_{2n} = \frac{2n+1}{2}\binom{2n}{n}, \quad M_{2n+1} = (2n+1)\binom{2n}{n}.$$

□

6.4. Magnitude of the combinatorial sum M_n. We are interested in the magnitude of the coefficient B_m.

By the Wallis Formula

$$\lim_{m\to+\infty}\left(\frac{(2m)!}{m!^2}\cdot\frac{\sqrt{\pi}\sqrt{m}}{2^{2m}}\right)=1\,,$$

we see that the ratio of B_m and $2\sqrt{m}/\sqrt{\pi}$ tends to 1 as m tends to infinity.

Since B_m and $2\sqrt{m}/\sqrt{\pi}$ have good multiplicative structure, we investigate the ratio B_m/B_{m-1} and its counter part as follows:

$$\left(\frac{B_m}{B_{m-1}}\right)^2=\left(\frac{(2m+1)(2m)}{4m^2}\right)^2=1+\frac{1}{m}+\frac{1}{4m^2}\,,$$

$$\left(\frac{2^{2m+1}\sqrt{m}/\sqrt{\pi}}{2^{2m-1}\sqrt{m-1}/\sqrt{\pi}}\right)^2=\frac{m}{m-1}=1+\frac{1}{m}+\frac{1}{m^2}+\cdots\,.$$

Therefore, $2\sqrt{m}/\sqrt{\pi}$ grows slightly faster than B_m. As their ratio converge to 1, this implies the inequality

$$B_m>\frac{2\sqrt{m}}{\sqrt{\pi}}\,. \tag{10}$$

We consider

$$A_m=4m+3+\frac{1}{8m+7}\quad\text{and}\quad A'_m=4m+3+\frac{1}{8m+6}\,.$$

Since

$$\frac{A_m}{A_{m-1}}-\frac{B_m^2}{B_{m-1}^2}=\frac{6m-7}{4m^2(8m+7)(16m^2-6m+1)}\,,$$

we get $A_m/A_{m-1}>B_m^2/B_{m-1}^2$. Noting that A_m/B_m^2 tends to π, we see the same line of the proof for (10) gives

$$B_m>\frac{\sqrt{4m+3+1/(8m+7)}}{\sqrt{\pi}}\,.$$

Similarly, we have

$$\frac{A'_m}{A'_{m-1}}-\frac{B_m^2}{B_{m-1}^2}=-\frac{9}{4m^2(4m+3)(32m^2-16m+3)}\,.$$

Hence we get $A'_m/A'_{m-1}<B_m^2/B_{m-1}^2$. Again, we see

$$B_m<\frac{\sqrt{4m+3+1/(8m+6)}}{\sqrt{\pi}}\,.$$

The error is estimated by the following calculation:

$$\frac{\sqrt{4m+3+1/(8m+6)}/\sqrt{\pi}}{\sqrt{4m+3+1/(8m+7)}/\sqrt{\pi}}=\sqrt{1+\frac{1/(8m+6)-1/(8m+7)}{4m+3+1/(8m+7)}}$$

$$
\begin{aligned}
&= \sqrt{1 + \frac{1}{4(4m+3)(16m^2+26m+11)}} \\
&\le \sqrt{1 + \frac{1}{4 \cdot 7 \cdot 53}} \\
&< 1.0004\,.
\end{aligned}
$$

In particular, we have

$$1 < \frac{\sqrt{4m+3+1/(8m+6)}}{B_m\sqrt{\pi}}, \quad \frac{\sqrt{\pi}\,B_m}{\sqrt{4m+3+1/(8m+7)}} < 1.0004\,. \tag{11}$$

6.5. Calculation of $\mathrm{vol}(\mathcal{B}_\nu^{(K)})$**.** In (8), we have

$$\mathrm{vol}(\mathcal{B}_\nu^{(1)}) = \mathrm{vol}(\mathcal{B}_\nu) = \begin{cases} \dfrac{2}{(m!)^2} & \text{if } \nu = 2m+1\,, \\[2ex] \dfrac{2m+1}{(m!)^2} & \text{if } \nu = 2m\,. \end{cases} \tag{12}$$

Let $K \ge 2$. The set $\mathcal{B}_\nu^K$ is not the direct product (e.g., of $\mathcal{B}_\nu$ and $\mathcal{B}_\nu^{(K-1)}$). However, it is a fiber product:

$$\mathcal{B}_\nu^{(K)} = \bigcup_{\boldsymbol{v} \in \mathcal{B}_\nu} \big(\{\boldsymbol{v}\} \times (1 - |\boldsymbol{v}|_{\mathrm{cyclo}})\mathcal{B}_\nu^{(K-1)}\big)\,.$$

Therefore, we have

$$
\begin{aligned}
\mathrm{vol}(\mathcal{B}_\nu^{(K)}) &= \int_{\boldsymbol{v} \in \mathcal{B}_\nu} \mathrm{vol}^{(K-1)}\big((1 - |\boldsymbol{v}|_{\mathrm{cyclo}})\mathcal{B}_\nu^{(K-1)}\big) d\mathrm{vol}(\boldsymbol{v}) \\
&= \int_0^1 \mathrm{vol}^{(K-1)}\big((1-x)\mathcal{B}_\nu^{(K-1)}\big) d\mathrm{vol}(x\mathcal{B}_\nu),
\end{aligned}
$$

where the right-hand side is the Stieltjes integral. Thus, we can calculate

$$
\begin{aligned}
\mathrm{vol}(\mathcal{B}_\nu^{(K)}) &= \int_0^1 (1-x)^{(K-1)\nu}\, \mathrm{vol}^{(K-1)}\big(\mathcal{B}_\nu^{(K-1)}\big) dx^\nu \mathrm{vol}(\mathcal{B}_\nu) \\
&= \int_0^1 (1-x)^{(K-1)\nu}\, dx^\nu \cdot \mathrm{vol}(\mathcal{B}_\nu) \cdot \mathrm{vol}^{(K-1)}\big(\mathcal{B}_\nu^{(K-1)}\big)\,.
\end{aligned}
$$

Hence we have

$$\mathrm{vol}(\mathcal{B}_\nu^{(K)}) = \nu \int_0^1 (1-x)^{(K-1)\nu}\, x^{\nu-1} dx \cdot \mathrm{vol}(\mathcal{B}_\nu) \cdot \mathrm{vol}^{(K-1)}\big(\mathcal{B}_\nu^{(K-1)}\big)\,. \tag{13}$$

As

$$
\begin{aligned}
\int_0^1 (1-x)^a x^b dx &= \Big[-\frac{1}{a+1}(1-x)^{a+1} x^b \Big]_{x=0}^{x=1} + \int_0^1 \frac{1}{a+1}(1-x)^{a+1} \cdot b x^{b-1} dx \\
&= \frac{b}{a+1} \int_0^1 (1-x)^{a+1} x^{b-1} dx\,,
\end{aligned}
$$

we have

$$\int_0^1 (1-x)^{(K-1)\nu} x^{\nu-1} dx$$

$$= \frac{\nu-1}{(K-1)\nu+1} \cdot \frac{\nu-2}{(K-1)\nu+2} \cdots \frac{\nu-(\nu-1)}{(K-1)\nu+(\nu-1)} \int_0^1 (1-x)^{(K-1)\nu+(\nu-1)} dx$$

$$= \frac{\nu-1}{(K-1)\nu+1} \cdot \frac{\nu-2}{(K-1)\nu+2} \cdots \frac{\nu-(\nu-1)}{(K-1)\nu+(\nu-1)} \cdot \frac{1}{(K-1)\nu+\nu}$$

$$= \frac{(\nu-1)!(K\nu-\nu)!}{(K\nu)!} .$$

Substituting this in (13), we deduce the recursion:

$$\mathrm{vol}(\mathcal{B}_\nu^{(K)}) = \frac{\nu!(K\nu-\nu)!}{(K\nu)!} \cdot \mathrm{vol}(\mathcal{B}_\nu) \cdot \mathrm{vol}^{(K-1)}\big(\mathcal{B}_\nu^{(K-1)}\big) .$$

This implies

$$\mathrm{vol}(\mathcal{B}_\nu^{(K)}) = \frac{\nu!^K}{(K\nu)!} \mathrm{vol}(\mathcal{B}_\nu)^K .$$

By substituting (12) in the right-hand side, we get

$$\mathrm{vol}(\mathcal{B}_\nu^{(K)}) = \frac{\nu!^K}{(K\nu)!} \mathrm{vol}(\mathcal{B}_\nu)^K = \begin{cases} \dfrac{\nu!^K}{(K\nu)!} \dfrac{2^K}{(m!)^{2K}} & \text{if } \nu = 2m+1 , \\ \dfrac{\nu!^K}{(K\nu)!} \dfrac{(2m+1)^K}{(m!)^{2K}} & \text{if } \nu = 2m . \end{cases}$$

Therefore, we have the following lemma.

LEMMA 6.5. *Let $2 \le \nu \in \mathbf{Z}$ and $1 \le K \in \mathbf{Z}$. We have*

$$\mathrm{vol}(\mathcal{B}_\nu^{(K)}) = \begin{cases} \dfrac{\nu!^K}{(K\nu)!} \dfrac{2^K}{(m!)^{2K}} & \textit{if } \nu = 2m+1 , \\ \dfrac{\nu!^K}{(K\nu)!} \dfrac{(2m+1)^K}{(m!)^{2K}} & \textit{if } \nu = 2m . \end{cases}$$

We can modify this into the following formula, which is a bit simpler

$$\mathrm{vol}(\mathcal{B}_\nu^{(K)}) = \frac{2^{K(\nu-2m)}}{(K\nu)!} \frac{(2m+1)!^K}{(m!)^{2K}} = \frac{2^{K\nu}}{(K\nu)!} B_m^K ,$$

where we put $m = \lfloor \nu/2 \rfloor$ and B_m is defined by (9).

By (11), we get

$$\frac{2^{K\nu}}{(K\nu)!} \frac{\sqrt{4m+3+1/(8m+7)}^K}{\sqrt{\pi}^K} < \mathrm{vol}(\mathcal{B}_\nu^{(K)}) < \frac{2^{K\nu}}{(K\nu)!} \frac{\sqrt{4m+3+1/(8m+6)}^K}{\sqrt{\pi}^K} ,$$

where the ratio of smaller and larger approximants is smaller than 1.0004^K.

6.6. The volume of $\mathcal{B}$. In the case $\nu = p-1$ and $K = q$, we have $\mathcal{B}^{(q)}_{p-1} = \mathcal{B}$. From Lemma 6.5, we get the following:

LEMMA 6.6. *We have*

$$\mathrm{vol}(\mathcal{B}) = \frac{(p-1)!^q}{(q(p-1))!}\,\frac{p^q}{((p-1)/2)!^{2q}}\,.$$

7. Minkowski convex body theorem for Theorem B. Let l be a prime number different from p, n a positive integer and p^s the exact power of p dividing $l^{p-1}-1$. We put $r = \min\{n, s\}$, $q = p^{r-1}$, $c = (p-1)q$, $\zeta = \zeta_r$ and $\xi = \zeta_1$. Let μ be the map in Section 4 (2), i.e.,

$$\mu : \boldsymbol{Q}(\zeta) \to \boldsymbol{C}^c\,, \quad \alpha \mapsto \overrightarrow{\alpha} := (\alpha^\rho)_{\rho \in \mathrm{Gal}(\boldsymbol{Q}(\zeta)/\boldsymbol{Q})}\,,$$

and W the $\boldsymbol{R}$-vector space $\boldsymbol{R}\overrightarrow{1} + \boldsymbol{R}\overrightarrow{\zeta} + \cdots + \boldsymbol{R}\overrightarrow{\zeta^{c-1}}$. We put

$$W_i = \boldsymbol{R}\overrightarrow{\zeta^i} + \boldsymbol{R}\overrightarrow{\zeta^i\xi} + \cdots + \boldsymbol{R}\overrightarrow{\zeta^i\xi^{p-2}}.$$

Then we have

$$W \cong \boldsymbol{R}^c\,, \quad \sum_{j=0}^{c-1} a_j \overrightarrow{\zeta^j} \mapsto (a_0, a_1, \dots, a_{c-1}), \tag{14}$$

$$W_i \cong \boldsymbol{R}^{p-1}, \quad \sum_{j=0}^{p-2} a_{i+qj}\overrightarrow{\zeta^i\xi^j} \mapsto (a_i, a_{i+q}, \dots, a_{i+q(p-2)})\,,$$

and

$$W = W_0 + W_1 + \cdots + W_{q-1}\,.$$

By the above isomorphism, we identify W with $\boldsymbol{R}^c$ and W_i with $\boldsymbol{R}^{p-1}$. Then $\overrightarrow{\zeta^i\xi^{p-1}}$ is $(-1, \dots, -1)$ in W_i. We define $|\cdot|_{\mathrm{cyclo}}$ on W similarly as in Subsection 6.1 for $\nu = p-1$ and $K = q$. Let

$$\mathcal{B} = \left\{ \sum_{i=0}^{c-1} s_i t_i \overrightarrow{\zeta^i}\ ;\ s_i \in \{+1, -1\}, 0 \le t_i \le 1, (i = 0, 1, \dots, c-1), \sum_{i=0}^{c-1} t_i \le 1 \right\}$$

and

$$X_{\mathrm{cyclo}} = \frac{2l}{\sqrt{6}p}\mathcal{B}\,.$$

From Lemma 6.6 and the Minkowski convex body theorem with respect to the volume on W induced by the standard volume on $\boldsymbol{R}^c$ by (14), we have the following lemma.

LEMMA 7.1. *Let l, n, s, r, q, c and X_{cyclo} be as above and $\mathfrak{L}$ a prime ideal of $\boldsymbol{Q}(\zeta_r)$ dividing l. We denote by f the inertia degree of $\mathfrak{L}$ in $\boldsymbol{Q}(\zeta_r)/\boldsymbol{Q}$. If l satisfies*

$$l^f > \sqrt{6}^c \left(\frac{p^{p-2}((p-1)/2)!^2}{(p-1)!} \right)^q c!,$$

then there exists a non-zero element $\overrightarrow{\alpha}$ in $X_{\mathrm{cyclo}} \cap \mu(l\mathfrak{L}^{-1})$. This α lies in $l\mathfrak{L}^{-1}$ and satisfies $|\mu(\alpha)|_{\mathrm{cyclo}} \le 2l/\sqrt{6}p$.

8. Proof of Theorem B. Let l be a prime number different form p, p^s the exact power of p dividing $l^{p-1}-1$ and n a positive integer. We put $N = p^n$, $r = \min\{n, s\}$, $q = p^{r-1}$, $c = (p-1)q$ and $\xi = \zeta_1$. We denote by f the inertia degree of l in $\boldsymbol{Q}(\zeta_r)/\boldsymbol{Q}$. Assume that l satisfies

$$l^f > \sqrt{6}^c \left(\frac{p^{p-2}((p-1)/2)!^2}{(p-1)!} \right)^q c!\,.$$

We also assume that l divides h_n/h_{n-1}. By Lemma 1.3 and Lemma 7.1, there exist a prime ideal $\mathfrak{L}$ in $\boldsymbol{Q}(\zeta_r)$ lying above l, an element α in $l\mathfrak{L}^{-1}$ and a unit ε in E_n such that

$$\eta_n^{\alpha_\sigma} = \varepsilon^l\,, \quad |\mu(\alpha)|_{\text{cyclo}} < \frac{2l}{\sqrt{6}p}\,. \tag{15}$$

By Theorem 2.2, we have

$$M(\varepsilon) \geq \left(\frac{1+\sqrt{5}}{2} \right)^{N/2} > \exp(0.240605912 \cdot N)\,. \tag{16}$$

Since $\deg \varepsilon^l = \deg \varepsilon$, $\deg \eta_n^{\alpha_\sigma} \leq \deg \eta_n$ and $1 + \xi + \cdots + \xi^{p-1} = 0$, we have

$$M(\varepsilon^l) = M(\varepsilon)^l, \quad M(\eta_n^{\alpha_\sigma}) \leq M(\eta_n)^{|\mu(\alpha)|_{\text{cyclo}}}\,. \tag{17}$$

By (15) through (17) and Lemma 3.3, we have

$$\begin{aligned} \exp(0.240605912 \cdot Nl) &\leq M(\varepsilon)^l = M(\varepsilon^l) = M(\eta_n^{\alpha_\sigma}) \\ &\leq M(\eta_n)^{|\mu(\alpha)|_{\text{cyclo}}} \\ &< \exp\left(0.291560904 \cdot pN \cdot \frac{2l}{\sqrt{6}p} \right). \end{aligned}$$

Hence we have

$$0.240605912 < 0.291560904 \cdot \frac{2}{\sqrt{6}} = 0.238058481 \cdots.$$

This is a contradiction.

9. Appendix. If we fix a prime number p, then we get a better estimate than Theorems A and B.

Let p be an odd prime number. We put $\zeta = \zeta_{n+1}$ and $N = p^n$. Let $\mathfrak{P}$ be a prime ideal in $\boldsymbol{Q}(\zeta)$ dividing p and $\mathrm{ord}_{\mathfrak{P}}(x)$ the normalized additive $\mathfrak{P}$-adic valuation of x. Moreover, we let $\mathfrak{p}$ be a prime ideal in $\boldsymbol{B}_n$ dividing p and $\mathrm{ord}_{\mathfrak{p}}(x)$ the normalized additive $\mathfrak{p}$-adic valuation of x which satisfies $\mathrm{ord}_{\mathfrak{p}}(x) = (p-1) \cdot \mathrm{ord}_{\mathfrak{P}}(x)$ for all x in $\boldsymbol{B}_n$. We denote by τ the generator of $\mathrm{Gal}(\boldsymbol{B}_n/\boldsymbol{B}_{n-1})$ which satisfies $\zeta^\tau = \zeta^{N+1}$.

LEMMA 9.1. *Let ε be a unit in $\boldsymbol{B}_n$. If $Nr_{\boldsymbol{B}_n/\boldsymbol{B}_{n-1}}(\varepsilon) = 1$ and $\varepsilon \neq 1$, then we have*

$$\mathrm{ord}_{\mathfrak{p}}(\varepsilon - 1) \geq \frac{N-1}{p-1}\,.$$

PROOF. There exists an element x in $\boldsymbol{Z}[\zeta]$ such that $\varepsilon = x^{1-\tau}$ by Hilbert's theorem 90. Since $\mathfrak{P}^p = (1-\zeta^p)$ and $(1-\zeta^p)^\tau = 1-\zeta^p$, we may assume $\mathrm{ord}_{\mathfrak{P}}(x) = 0, 1, \dots, p-1$. Note that if α is an element of $\boldsymbol{Z}[\zeta]$ then we have $\mathrm{ord}_{\mathfrak{P}}(\alpha - \alpha^\tau) \geq N$. Hence we have

$$\mathrm{ord}_{\mathfrak{P}}(\varepsilon - 1) = \mathrm{ord}_{\mathfrak{P}}\left(\frac{x - x^\tau}{x^\tau}\right) \geq N - p + 1\,,$$

that is, $(p-1)\mathrm{ord}_{\mathfrak{p}}(\varepsilon - 1) \geq N - p + 1$. Since $\mathrm{ord}_{\mathfrak{p}}(\varepsilon - 1)$ is a rational integer, we have

$$\mathrm{ord}_{\mathfrak{p}}(\varepsilon - 1) \geq \frac{N-1}{p-1}\,.$$

□

Note that the absolute norm of $\mathfrak{p}$ is equal to p. From Theorem 2.2 and Lemma 9.1, we get the following lemma.

LEMMA 9.2. *Let ε be a unit in $\boldsymbol{B}_n$ with $Nr_{\boldsymbol{B}_n/\boldsymbol{B}_{n-1}}(\varepsilon) = 1$ and put $N = p^n$. Then we have*

$$M(\varepsilon) \geq \left(\frac{p^{(N-1)/(p-1)N} + \sqrt{p^{2(N-1)/(p-1)N} + 4}}{2}\right)^{N/2}.$$

We study the case $p = 5$. From now on, we put $\boldsymbol{B}_n = \boldsymbol{B}_{5,n}$ and $h_n = h_{5,n}$. Let l be a prime number different from 5, n a positive integer and 5^s the exact power of 5 dividing $l^4 - 1$. We put $r = \min\{n, s\}$, $q = 5^{r-1}$ and $c = 4q$. Now we apply the Minkowski convex body theorem and obtain the following lemma.

LEMMA 9.3. *Let $p = 5$, l be a prime number different form 5 and $\mathfrak{L}$ a prime ideal of $\boldsymbol{Q}(\zeta_r)$ dividing l. We denote by f the inertia degree of $\mathfrak{L}$ in $\boldsymbol{Q}(\zeta_r)/\boldsymbol{Q}$. If l satisfies $l^f > (640/3)^q \cdot c!$, then there exists a non-zero element α in $l\mathfrak{L}^{-1}$ such that $|\mu(\alpha)|_{\mathrm{cyclo}} \leq l/2\sqrt{5}$.*

We assume that l divides h_n/h_{n-1}. Since Linden [17] showed that $h_1 = 1$, we may assume $n \geq 2$. By Lemma 9.2, we have

$$M(\varepsilon) \geq \left(\frac{5^{6/25} + \sqrt{5^{12/25} + 4}}{2}\right)^{N/2} > \exp(0.681697987 \cdot N/2)\,. \tag{18}$$

We also assume $l^f > (640/3)^q \cdot c!$. By Lemmas 1.3 and 9.3, there exist a prime ideal $\mathfrak{L}$ in $\boldsymbol{Q}(\zeta_r)$ lying above l, an element α in $l\mathfrak{L}^{-1}$ and a unit ε in E_n such that

$$\eta_n^{\alpha_\sigma} = \varepsilon^l\,, \quad |\mu(\alpha)|_{\mathrm{cyclo}} < \frac{l}{2\sqrt{5}}\,. \tag{19}$$

By (18), (19) and Lemma 3.3, we have

$$\begin{aligned}\exp(0.681697987 \cdot lN/2) &\leq M(\varepsilon)^l = M(\varepsilon^l) = M(\eta_n^{\alpha_\sigma})\\ &\leq M(\eta_n)^{|\mu(\alpha)|_{\mathrm{cyclo}}}\\ &< \exp\left(0.291560904 \cdot 5 \cdot N \cdot \frac{l}{2\sqrt{5}}\right).\end{aligned}$$

Hence we have

$$0.681697987 < 0.291560904 \times \sqrt{5} = 0.651950000\cdots.$$

This is a contradiction. Therefore, we conclude the following theorem.

THEOREM 9.4. *Let $p = 5$, l be a prime number different from 5, n a positive integer and 5^s the exact power of 5 dividing $l^4 - 1$. We put $r = \min\{n, s\}$, $q = p^{r-1}$ and $c = 4q$. We denote by f the inertia degree of l in $\boldsymbol{Q}(\zeta_r)/\boldsymbol{Q}$. If l satisfies $l^f > (640/3)^q \cdot c!$, then l does not divide h_n/h_{n-1}.*

REFERENCES

[1] H. BAUER, Numeriche Bestimmung con Klassenzahlen reeler zyklischer Zahlkörper, J. Number Theory 1 (1969), 161–162.

[2] H. COHN, A numerical study of Weber's real class number calculation I,Numer. Math. 2 (1960), 347–362.

[3] G. EVEREST AND T. WARD, Heights of polynomials and entropy in algebraic dynamics, Universitext, Springer-Verlag London, Ltd., London, 1999.

[4] T. FUKUDA AND K. KOMATSU, Weber's class number problem in the cyclotomic $\boldsymbol{Z}_2$-extension of $\boldsymbol{Q}$, Experiment. Math. 18 (2009), no. 2, 213–222.

[5] T. FUKUDA AND K. KOMATSU, Weber's class number problem in the cyclotomic $\boldsymbol{Z}_2$-extension of $\boldsymbol{Q}$, II, J. The'or. Nombres Bordeaux 22 (2010), no. 2, 359–368.

[6] T. FUKUDA AND K. KOMATSU, Weber's class number problem in the cyclotomic $\boldsymbol{Z}_2$-extension of $\boldsymbol{Q}$, III, Int. J. Number Theory 7 (2011), no. 6, 1627–1635.

[7] I. S. GRADSHTEYN AND I. M. RYZHIK, Table of integrals, series and products, Academic Press, New York-London, 1965.

[8] K. HORIE, Ideal class groups of Iwasawa-theoretical abelian extensions over the rational field, J. London Math. Soc. (2) 66 (2002), 257–275.

[9] K. HORIE, Primary components of the ideal class group of the $\boldsymbol{Z}_p$-extension over $\boldsymbol{Q}$ for typical inert primes, Proc. Japan Acad. Ser. A Math. Sci. 81 (2005), no.3, 40–43.

[10] K. HORIE, The ideal class group of the basic $\boldsymbol{Z}_p$-extension over an imaginary quadratic field, Tohoku Math. J. (2) 57 (2005), 375–394.

[11] K. HORIE, Certain primary components of the ideal class group of the $\boldsymbol{Z}_p$-extension over the rationals, Tohoku Math. J. (2) 59 (2007), 259–291.

[12] K. HORIE AND M. HORIE, The narrow class groups of some $\boldsymbol{Z}_p$-extensions over the rationals, Acta Arith. 135 (2008), no. 2, 159–180.

[13] K. HORIE AND M. HORIE, The ideal class group of the $\boldsymbol{Z}_p$-extension over the rationals, Tohoku Math. J. (2) 61 (2009), 551–570.

[14] K. HORIE AND M. HORIE, The narrow class groups of the $\boldsymbol{Z}_{17}$- and $\boldsymbol{Z}_{19}$-extensions over the rational field, Abh. Math. Semin. Univ. Hambg. 80 (2010), no. 1, 47–57.

[15] K. HORIE AND M. HORIE, The ideal class group of the $\boldsymbol{Z}_{23}$-extension over the rational field, Proc. Japan Acad. Ser. A Math. Sci. 85 (2009), 155–159.

[16] K. IWASAWA, A note on class numbers of algebraic number fields, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.

[17] F. J. VAN DER LINDEN, Class number computations of real abelian number fields, Math. Comp. 39 (1982), 693–707.

[18] N. I. LOBACHEVSKY, Complete works, I, III, V, Gostekhizdat, Moscow and Leningrad (1946–1951).

[19] J. M. MASLEY, Class numbers of real cyclic number fields with small conductor, Compositio math. 37 (1978), 297–319.

[20] T. MORISAWA, A class number problem in the cyclotomic $\boldsymbol{Z}_3$-extension of $\boldsymbol{Q}$, Tokyo J. Math. 32 (2009), 549–558.

[21] T. MORISAWA, Mahler measure of the Horie unit and Weber's class number problem in the cyclotomic $\boldsymbol{Z}_3$-extension of $\boldsymbol{Q}$, Acta Arith. 153 (2012), no. 1, 35–49.

[22] R. OKAZAKI, On a lower bound for relative units, schinzel's lower bound and Weber's class number problem, preprint.

[23] A. SCHINZEL, On the product of the conjugates outside the unit circle of an algebraic number, Acta Arith. 24 (1973), 385–399.

[24] L. C. WASHINGTON, Class numbers and $\boldsymbol{Z}_p$-extensions, Math. Ann. 214 (1975), 177–193.

[25] L. C. WASHINGTON, The non-p-part of the class number in a cyclotomic $\boldsymbol{Z}_p$-extension, Invent. Math. 49 (1978), 87–97.

[26] H. WEBER, Theorie der Abel'schen Zahlkörper, Acta Math. 8 (1886), 193–263.

MAJOR IN PURE AND APPLIED MATHEMATICS
GRADUATE SCHOOL OF FUNDAMENTAL SCIENCE
AND ENGINEERING
WASEDA UNIVERSITY
3–4–1 OKUBO, SHINJUKU
TOKYO 169–8555
JAPAN

E-mail address: da-vinci-0415@moegi.waseda.jp

DEPARTMENT OF MATHEMATICAL SCIENCES
DOSHISHA UNIVERSITY
KYOTANABE, KYOTO, 610–0394
JAPAN

E-mail address: rokazaki@dd.iij4u.or.jp