

BERTRAND'S AND RODRIGUEZ VILLEGAS' CONJECTURE FOR REAL MULTI-QUADRATIC GALOIS EXTENSIONS OF THE RATIONALS

DOHYEONG KIM AND SEUNGHO SONG

ABSTRACT. The conjecture due to Bertrand and Rodriguez Villegas asserts that the 1-norm of the nonzero element in an exterior power of the units of a number field has a certain lower bound. We prove this conjecture for the exterior square case when the number field is a real multi-quadratic Galois extension of any degree of the rationals.

1. INTRODUCTION

An outstanding conjecture named after Lehmer asserts a lower bound for the Weil height of a unit in a number field. The origin of the conjecture is a problem which Lehmer posed in [?], concerning irreducible polynomials with integer coefficients. It has evolved, as more extensive numerical evidence emerged, into Lehmer's conjecture, which is nowadays often formulated in terms of heights. By the time Zimmert [?] obtained a lower bound for the regulator of a number field, it had become evident that both the Weil height and the regulator could be interpreted as a suitable l^1 -norm. In particular, it became natural to consider not only units but their exterior powers in all degrees, which would recover Lehmer's conjecture in degree one and subsume Zimmert's theorem in the top degree.

For general exterior powers, an analogous problem to find lower bounds for l^2 -norms was proposed by Bertrand [?, p. 210], although the attention was limited to the case of pure wedges, in retrospect. This is so only in retrospect because the formulation therein was in terms of subspaces, and the reason why we phrased it in terms of pure wedges in exterior powers will become clear soon. In any case, the problem posed by Bertrand was confirmed, except for the exterior square case, by Amoroso and David [?].

In 2002, Rodriguez Villegas proposed a sharper version of Bertrand's conjecture, which remained unpublished until it appeared in [?]. It refines Bertrand's in two ways. First, it asserts a lower bound for l^1 -norms, which seems more subtle than the l^2 -counterpart. Second, it is stated for all non-zero vectors in the exterior powers, rather than just pure wedges. We regard this as a common generalization of both

Date: April 13, 2025.

Key words and phrases. Bertrand-Rodriguez Villegas conjecture, units.

Lehmer's conjecture and Zimmert's result. Further background on the history of heights and Lehmer's problem can be found in Bombieri and Gubler [?], as well as in Mckee and Smyth [?].

Our aim in this paper is to provide an evidence for the conjecture. To proceed, we recall some definitions from [?].

Definition 1.1. Let L be a number field and \mathcal{A}_L be the set of its Archimedean places. Then the function $\text{LOG} : \mathcal{O}_L^* \rightarrow \mathbb{R}^{\mathcal{A}_L}$ is defined by

$$(\text{LOG}(\gamma))_v := e_v \log|\gamma|_v \quad \text{where} \quad e_v := \begin{cases} 1 & \text{if } v \text{ is real,} \\ 2 & \text{if } v \text{ is complex} \end{cases}$$

for $\gamma \in \mathcal{O}_L^*$ and $v \in \mathcal{A}_L$. Here, $|\cdot|_v$ is the absolute value associated to v extending the absolute value on \mathbb{Q} .

Definition 1.2. The orthonormal basis $\{\delta^v\}_{v \in \mathcal{A}_L}$ of $\mathbb{R}^{\mathcal{A}_L}$ is given by

$$\delta_w^v := \begin{cases} 1 & \text{if } w = v, \\ 0 & \text{if } w \neq v \end{cases}$$

for $w \in \mathcal{A}_L$. Let $\mathcal{A}_L^{[j]}$ be the set of subsets of \mathcal{A}_L with cardinality j . For each $I \in \mathcal{A}_L^{[j]}$, fix an ordering $\{v_1, v_2, \dots, v_j\}$ of elements of I . Define

$$\delta^I := \delta^{v_1} \wedge \delta^{v_2} \wedge \dots \wedge \delta^{v_j}$$

to get the orthonormal basis $\{\delta^I\}_{I \in \mathcal{A}_L^{[j]}}$ of $\bigwedge^j \mathbb{R}^{\mathcal{A}_L}$. For $w = \sum_{I \in \mathcal{A}_L^{[j]}} c_I \delta^I \in \bigwedge^j \mathbb{R}^{\mathcal{A}_L}$,

define its 1-norm as

$$\|w\|_1 := \sum_{I \in \mathcal{A}_L^{[j]}} |c_I|.$$

Now we state the Bertrand's and Rodriguez Villegas' conjecture from [?].

Conjecture (Bertrand-Rodriguez Villegas). There exist two absolute constants $c_0 > 0$ and $c_1 > 1$ such that for any number field L and any $j \in \mathbb{Z}_{>0}$, the following inequality

$$(1.1) \quad \|w\|_1 \geq c_0 c_1^j$$

holds for any nonzero $w \in \bigwedge^j \text{LOG}(\mathcal{O}_L^*) \subset \bigwedge^j \mathbb{R}^{\mathcal{A}_L}$.

For some values of j , the conjecture reduces to the case when w is a pure wedge product, i.e. $w = \text{LOG}(\epsilon_1) \wedge \dots \wedge \text{LOG}(\epsilon_j)$ where ϵ_i are multiplicatively independent units of L . This includes the case $j = 1$, where the conjecture is equivalent to Lehmer's conjecture [?], and the case $j = \text{rank}_{\mathbb{Z}}(\mathcal{O}_L^*)$, where the conjecture is equivalent to Zimmert's theorem on regulators [?]. The case $j = \text{rank}_{\mathbb{Z}}(\mathcal{O}_L^*) - 1$ also reduces to the case where w is a pure wedge product. This is because every element of $\bigwedge^j \text{LOG}(\mathcal{O}_L^*)$ can be written in the form $d \cdot \text{LOG}(\epsilon_1) \wedge \dots \wedge \text{LOG}(\epsilon_j)$

where $d \in \mathbb{Z}$ and $\text{LOG}(\epsilon_1), \dots, \text{LOG}(\epsilon_{j+1})$ are the basis of $\text{LOG}(\mathcal{O}_L^*)$ as shown in the Lemma 28 of [?]. In general, showing the inequality (1.1) for nonzero pure wedge products does not guarantee that the inequality holds for all nonzero elements of $\bigwedge^j \text{LOG}(\mathcal{O}_L^*)$. For pure wedge products, recent progress is due to Akhtari and Vaaler [?]. However, little progress has been made in the non-pure case, as noted in [?].

For a totally real number field L , Costa and Friedman [?] showed that for independent elements $\epsilon_1, \dots, \epsilon_j$ of \mathcal{O}_L^* , the inequality

$$(1.2) \quad \|\text{LOG}(\epsilon_1) \wedge \dots \wedge \text{LOG}(\epsilon_j)\|_2 > \frac{1}{(j+2)\sqrt{j}} \left(\frac{[L:\mathbb{Q}]}{j}\right)^{j/2} 1.406^j$$

holds for $1 \leq j < [L:\mathbb{Q}]$. Therefore, with some calculations it follows that

$$\|\text{LOG}(\epsilon_1) \wedge \dots \wedge \text{LOG}(\epsilon_j)\|_1 > \frac{1}{(j+2)\sqrt{j}} \left(\frac{[L:\mathbb{Q}]}{j}\right)^{j/2} 1.406^j \geq 0.001 \cdot 1.4^j$$

also holds, proving the conjecture for pure wedge products of units of totally real fields. This result is a consequence of earlier work by Schinzel [?] and Pohst [?]. The inequality (1.2) is stronger than that of Bertrand-Rodriguez Villegas conjecture, in the sense that the 2-norm is used and that the lower bound diverges as the degree $[L:\mathbb{Q}]$ goes to infinity for a fixed j . This implies that the important part of the conjecture is that the inequality (1.1) holds for all nonzero $w \in \bigwedge^j \text{LOG}(\mathcal{O}_L^*)$, even for w that is not a pure wedge product.

In this paper, we give a lower bound of $\|w\|_1$ for nonzero $w \in \bigwedge^2 \text{LOG}(\mathcal{O}_L^*)$ when L is a real Galois extension of \mathbb{Q} with $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$ for some integer $n \geq 2$. When $n \geq 3$, this case does not necessarily reduce to the case when w is a pure wedge product. Our main theorem is as follows.

Theorem 1.3. *Let $n \geq 2$ be a positive integer, and L be a real Galois extension of \mathbb{Q} with $\text{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$. Then,*

$$\|w\|_1 \geq 2 \log \left(\frac{1 + \sqrt{5}}{2} \right) \log(1 + \sqrt{2}) \approx 0.8483$$

for any nonzero $w \in \bigwedge^2 \text{LOG}(\mathcal{O}_L^*)$.

While our result is limited to the exterior square case where L belongs to a specific family of number fields, we provide a constant lower bound of $\|w\|_1$ independent of the degree $[L:\mathbb{Q}] = 2^n$.

The key idea of the proof of the main theorem is to use the fundamental units of the quadratic subfields of L . The field L has exactly $2^n - 1$ quadratic subfields, and the fundamental unit of these quadratic subfields generate a subgroup E of \mathcal{O}_L^* . Since the Galois module structure of E is known, $\text{LOG}(E)$ is easier to handle than $\text{LOG}(\mathcal{O}_L^*)$. We first give a lower bound of $\|w\|_1$ for nonzero element w of $\bigwedge^2 \text{LOG}(E)$ using elementary linear algebra, and extend this result

to $\bigwedge^2 \text{LOG}(\mathcal{O}_L^*)$. The terms $\frac{1+\sqrt{5}}{2}$ and $1 + \sqrt{2}$ in the lower bound are the fundamental units of the real quadratic fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{2})$, respectively. If we denote by u_m the fundamental unit of a real quadratic field $\mathbb{Q}(\sqrt{m})$ with $u_m > 1$, then $u_5 = \frac{1+\sqrt{5}}{2}$ and $u_2 = 1 + \sqrt{2}$ are the two smallest among them.

The proof of the main theorem is given in the following sections. In section 2 we show some properties of subgroups of $(\mathbb{Z}/2\mathbb{Z})^n$ of index 2. We introduce a subgroup E of \mathcal{O}_L^* generated by positive units of quadratic subfields of L , and prove that for any unit $u \in \mathcal{O}_L^*$, $u^{2^{n-1}} \in E$. In section 3, using the values of LOG of the fundamental units, we give a basis of $\bigwedge^2 \text{LOG}(E)$ and the 1-norm of its elements. In section 4 we give a lower bound for the elements of $\bigwedge^2 \text{LOG}(E)$ using elementary linear algebra, and use this result to prove our main theorem.

Acknowledgement. The work of S.S. was supported by College of Natural Sciences Undergraduate Internship Program from Seoul National University.

2. THE STRUCTURE OF UNITS

Fix a positive integer $n \geq 2$ and fix a totally real number field L such that the group $\text{Gal}(L/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$. Let $\lambda : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \text{Gal}(L/\mathbb{Q})$ be a group isomorphism. Identify L with a subfield of \mathbb{C} so that the identity map is an element of $\text{Gal}(L/\mathbb{Q})$. Since L is real, ± 1 are the only roots of unity of L . We can view each element of $\text{Gal}(L/\mathbb{Q})$ as a real place of L and identify \mathcal{A}_L with $\text{Gal}(L/\mathbb{Q})$. Let $A := (\mathbb{Z}/2\mathbb{Z})^n \setminus \{0\}$ and let B be a set consisting of subgroups of $(\mathbb{Z}/2\mathbb{Z})^n$ of index 2. Then each element of B corresponds to a quadratic subfield of L . We first define some notions that will be used throughout this paper.

Definition 2.1. We define $\langle \cdot, \cdot \rangle : (\mathbb{Z}/2\mathbb{Z})^n \times (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/2\mathbb{Z}$ as follows. For two elements $p = (p_1, p_2, \dots, p_n)$ and $q = (q_1, \dots, q_n)$ of $(\mathbb{Z}/2\mathbb{Z})^n$ with $p_i, q_i \in \mathbb{Z}/2\mathbb{Z}$ for $1 \leq i \leq n$, define

$$\langle p, q \rangle := \sum_{i=1}^n p_i q_i,$$

where the multiplication between the elements of $\mathbb{Z}/2\mathbb{Z}$ is defined as in the finite field \mathbb{F}_2 . In other words, for $x, y \in \mathbb{Z}/2\mathbb{Z}$, $xy = 1$ if and only if $x = y = 1$. For $p \in A$, define

$$p^\perp := \{z \in (\mathbb{Z}/2\mathbb{Z})^n \mid \langle p, z \rangle = 0\}.$$

For any $p \in A$, p^\perp is a kernel of a surjective group homomorphism that sends $z \in (\mathbb{Z}/2\mathbb{Z})^n$ to $\langle p, z \rangle$. Thus $p^\perp \in B$. In fact, every element of B are of this form, as stated in the following lemma.

Lemma 2.2. *Let A, B be defined as above. We have:*

- (1) *There is a bijective map ϕ between A and B given by*

$$\phi : A \rightarrow B$$

$$x \mapsto x^\perp$$

and in particular, $|B| = 2^n - 1$.

- (2) For any element x of A , x is in exactly $2^{n-1} - 1$ elements of B .
- (3) For any two distinct elements x and y of A , $|x^\perp \cap y^\perp| = 2^{n-2}$.

Proof. (1) First we show ϕ is surjective. Take any $b \in B$. Then since $(\mathbb{Z}/2\mathbb{Z})^n$ is abelian group, b is a normal subgroup of $(\mathbb{Z}/2\mathbb{Z})^n$, and $(\mathbb{Z}/2\mathbb{Z})^n/b \cong \mathbb{Z}/2\mathbb{Z}$. Thus there exists a surjective homomorphism $h_b : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow \mathbb{Z}/2\mathbb{Z}$ such that its kernel is b . Let e_i be a i -th standard basis of $(\mathbb{Z}/2\mathbb{Z})^n$, i.e. the element with i -th component 1 and other components 0. If we let $a = \sum_{i=1}^n h_b(e_i)e_i$, then $a \in A$ and h_b sends $z \in (\mathbb{Z}/2\mathbb{Z})^n$ to $\langle a, z \rangle$. Thus $\phi(a) = \ker(h_b) = b$, and ϕ is surjective.

We now show ϕ is injective. Let x, y be distinct elements of A . Since $x \neq y$, there exists $1 \leq j \leq n$ such that $\langle x, e_j \rangle \neq \langle y, e_j \rangle$. If $e_j \in x^\perp$, then $e_j \notin y^\perp$ and if $e_j \notin x^\perp$, then $e_j \in y^\perp$. Thus $x^\perp \neq y^\perp$ and ϕ is injective. Therefore ϕ is bijective and $|B| = |A| = 2^n - 1$.

(2) By (1), we only need to count the number of elements of A which are perpendicular to x . Let the j -th component of x be 1. Then for any $z \in (\mathbb{Z}/2\mathbb{Z})^n$, only one of z and $z + e_j$ is perpendicular to x . Thus $\frac{1}{2}|(\mathbb{Z}/2\mathbb{Z})^n| = 2^{n-1}$ elements of $(\mathbb{Z}/2\mathbb{Z})^n$ are perpendicular to x . Excluding 0, exactly $2^{n-1} - 1$ elements of A are perpendicular to x .

(3) Since $x \neq y$, there exists $1 \leq j \leq n$ such that $\langle x, e_j \rangle \neq \langle y, e_j \rangle$. Without loss of generality, let $\langle x, e_j \rangle = 0$ and $\langle y, e_j \rangle = 1$. Then for any $z \in x^\perp$, since $\langle z + e_j, x \rangle = 0$, $z + e_j \in x^\perp$. Since $\langle z, y \rangle \neq \langle z + e_j, y \rangle$, only one of z and $z + e_j$ is also in y^\perp . Thus exactly $\frac{1}{2}|x^\perp| = 2^{n-2}$ elements of x^\perp are in $x^\perp \cap y^\perp$. \square

For each $a \in A$, a^\perp is a subgroup of $(\mathbb{Z}/2\mathbb{Z})^n$ of index 2, so $\lambda(a^\perp)$ is a subgroup of $\text{Gal}(L/\mathbb{Q})$ of index 2. Let $\mathbb{Q}[\sqrt{d_a}]$ be the quadratic subfield of L that corresponds to $\lambda(a^\perp)$, and let $u_a > 1$ be its fundamental unit. Then every unit of $\mathbb{Q}[\sqrt{d_a}]$ is of the form $\pm u_a^m$ where $m \in \mathbb{Z}$. Let $E := \{ \prod_{a \in A} u_a^{m_a} \mid m_a \in \mathbb{Z} \}$. We show the following lemma.

Lemma 2.3. *For any unit u of L , $u^{2^{n-1}}$ is in E .*

Proof. For any $a \in A$, $N_{L/\mathbb{Q}[\sqrt{d_a}]}(u)$ is a product of conjugates of u , so it is a unit of L . Since $N_{L/\mathbb{Q}[\sqrt{d_a}]}(u) \in \mathbb{Q}[\sqrt{d_a}]$, it is also a unit of $\mathbb{Q}[\sqrt{d_a}]$. Hence

$$\prod_{\sigma \in \text{Gal}(L/\mathbb{Q}[\sqrt{d_a}])} \sigma(u) = \pm u_a^{m_a}$$

for some $m_a \in \mathbb{Z}$. By multiplying above equations for every a and taking its absolute value, we get

$$\begin{aligned} \prod_{a \in A} u_a^{m_a} &= \left| \prod_{a \in A} \prod_{\sigma \in \text{Gal}(L/\mathbb{Q}[\sqrt{d_a}])} \sigma(u) \right| \\ &= \left| \prod_{b \in B} \prod_{x \in b} \lambda(x)(u) \right| \end{aligned}$$

where the second equality comes from the bijection between A and B in (1) of Lemma 2.2. In the product $\prod_{b \in B} \prod_{x \in b}$, the element $0 \in (\mathbb{Z}/2\mathbb{Z})^n$ appears $|B| = 2^n - 1$ times, while other elements appear $2^{n-1} - 1$ times by (2) of Lemma 2.2. Thus in the product $\prod_{a \in A} \prod_{\sigma \in \text{Gal}(L/\mathbb{Q}[\sqrt{d_a}])}$, $id \in \text{Gal}(L/\mathbb{Q})$ appears $2^n - 1$ times, while other elements appear $2^{n-1} - 1$ times. Thus we have

$$\begin{aligned} \prod_{a \in A} u_a^{m_a} &= \left| u^{2^n - 1} \cdot \prod_{\sigma \in \text{Gal}(L/\mathbb{Q}) \setminus \{id\}} \sigma(u)^{2^{n-1} - 1} \right| \\ &= \left| u^{2^n - 1} \cdot \prod_{\sigma \in \text{Gal}(L/\mathbb{Q})} \sigma(u)^{2^{n-1} - 1} \right| \\ &= |u^{2^n - 1} \cdot N_{L/\mathbb{Q}}(u)^{2^{n-1} - 1}|. \end{aligned}$$

Since $u \in \mathcal{O}_L^*$, we have $|N_{L/\mathbb{Q}}(u)| = 1$ and therefore $u^{2^n - 1} = \prod_{a \in A} u_a^{m_a} \in E$. \square

3. THE 1-NORM OF THE WEDGE PRODUCTS

Since E is generated by $\{u_a\}_{a \in A}$, $\text{LOG}(E)$ is generated by $\{\text{LOG}(u_a)\}_{a \in A}$. Identifying $\text{Gal}(L/\mathbb{Q})$ with \mathcal{A}_L , the basis of $\mathbb{R}^{\mathcal{A}_L}$ is $\{\delta^\sigma\}_{\sigma \in \text{Gal}(L/\mathbb{Q})} = \{\delta^{\lambda(x)}\}_{x \in (\mathbb{Z}/2\mathbb{Z})^n}$. We now compute $\text{LOG}(u_a)$ for $a \in A$. If $\lambda(x) \in \text{Gal}(L/\mathbb{Q}[\sqrt{d_a}])$, it fixes u_a and if $\lambda(x) \notin \text{Gal}(L/\mathbb{Q}[\sqrt{d_a}])$, it sends u_a to its conjugate, $\pm \frac{1}{u_a}$. Also, $\lambda(x) \in \text{Gal}(L/\mathbb{Q}[\sqrt{d_a}])$ if and only if $x \in a^\perp$, which is equivalent to $\langle a, x \rangle = 0$. Thus, the coefficient of the basis $\delta^{\lambda(x)}$ of $\text{LOG}(u_a)$ is

$$(\text{LOG}(u_a))_{\lambda(x)} = (-1)^{\langle a, x \rangle} \log(u_a).$$

Here, for $n \in \mathbb{Z}/2\mathbb{Z}$, $(-1)^n = 1$ if $n = 0$ and $(-1)^n = -1$ if $n = 1$. Now give any ordering to $(\mathbb{Z}/2\mathbb{Z})^n$ with 0 being the smallest element, and also give this ordering to A . For $b, c \in A$ and $x, y \in (\mathbb{Z}/2\mathbb{Z})^n$ with $b < c$ and $x < y$, the coefficient of the basis $\delta^{\lambda(x)} \wedge \delta^{\lambda(y)}$ of $\text{LOG}(u_b) \wedge \text{LOG}(u_c)$ is

$$(\text{LOG}(u_b) \wedge \text{LOG}(u_c))_{(\lambda(x), \lambda(y))} = \log(u_b) \log(u_c) \{(-1)^{\langle b, x \rangle + \langle c, y \rangle} - (-1)^{\langle b, y \rangle + \langle c, x \rangle}\}.$$

The abelian group $\bigwedge^2 \text{LOG}(E)$ is generated by $\text{LOG}(u_b) \wedge \text{LOG}(u_c)$'s where $b, c \in A$ and $b < c$. Thus $w \in \bigwedge^2 \text{LOG}(E)$ can be written as

$$(3.1) \quad w = \sum_{\substack{b, c \in A \\ b < c}} n_{b, c} \text{LOG}(u_b) \wedge \text{LOG}(u_c)$$

where all $n_{b, c}$'s are integers. Then its coefficient of the basis $\delta^{\lambda(x)} \wedge \delta^{\lambda(y)} (x < y)$ is

$$(3.2) \quad (w)_{(\lambda(x), \lambda(y))} = \sum_{\substack{b, c \in A \\ b < c}} n_{b, c} \log(u_b) \log(u_c) \{(-1)^{\langle b, x \rangle + \langle c, y \rangle} - (-1)^{\langle b, y \rangle + \langle c, x \rangle}\}.$$

If we let $b + c = d$ and $x + y = z$, then

$$\begin{aligned} (-1)^{\langle b, x \rangle + \langle c, y \rangle} - (-1)^{\langle b, y \rangle + \langle c, x \rangle} &= (-1)^{\langle b, y \rangle + \langle c, x \rangle} \{(-1)^{\langle b+c, x+y \rangle} - 1\} \\ &= (-1)^{\langle b, z-x \rangle + \langle d-b, x \rangle} \{(-1)^{\langle d, z \rangle} - 1\} \\ &= (-1)^{\langle b, z \rangle + \langle d, x \rangle + 2\langle b, x \rangle} \{(-1)^{\langle d, z \rangle} - 1\} \\ &= (-1)^{\langle b, z \rangle + \langle d, x \rangle} \{(-1)^{\langle d, z \rangle} - 1\}. \end{aligned}$$

Then (3.2) and the above equation implies that the 1-norm of w is

$$\begin{aligned} &\sum_{\substack{x, y \in (\mathbb{Z}/2\mathbb{Z})^n \\ x < y}} \left| \sum_{\substack{b, c \in A \\ b < c}} n_{b, c} \log(u_b) \log(u_c) \{(-1)^{\langle b, x \rangle + \langle c, y \rangle} - (-1)^{\langle b, y \rangle + \langle c, x \rangle}\} \right| \\ &= \sum_{z \in A} \sum_{\substack{x \in (\mathbb{Z}/2\mathbb{Z})^n \\ x < z+x}} \left| \sum_{d \in A} \sum_{\substack{b \in A \\ b < b+d}} n_{b, d+b} \log(u_b) \log(u_{d+b}) \cdot (-1)^{\langle b, z \rangle + \langle d, x \rangle} \{(-1)^{\langle d, z \rangle} - 1\} \right| \\ &= \sum_{z \in A} \sum_{\substack{x \in (\mathbb{Z}/2\mathbb{Z})^n \\ x < z+x}} \left| \sum_{\substack{d \in A \\ \langle d, z \rangle = 1}} \sum_{\substack{b \in A \\ b < b+d}} n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle + \langle d, x \rangle} (-2) \right| \\ &= \sum_{z \in A} \sum_{\substack{x \in (\mathbb{Z}/2\mathbb{Z})^n \\ x < z+x}} \left| \sum_{\substack{d \in A \\ \langle d, z \rangle = 1}} \sum_{\substack{b \in A \\ b < b+d}} 2n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle + \langle d, x \rangle} \right|. \end{aligned}$$

In summary,

$$(3.3) \quad \|w\|_1 = \sum_{z \in A} \sum_{\substack{x \in (\mathbb{Z}/2\mathbb{Z})^n \\ x < z+x}} \left| \sum_{\substack{d \in A \\ \langle d, z \rangle = 1}} \sum_{\substack{b \in A \\ b < b+d}} 2n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle + \langle d, x \rangle} \right|$$

for w given by (3.1).

4. THE LOWER BOUND OF THE 1-NORM

To give a lower bound for (3.3), we turn to the following lemma.

Lemma 4.1. *Let m be a nonnegative integer, and let P be a $2^m \times 2^m$ matrix with each entries 1 or -1 . Assume that the rows of P are perpendicular to each other.*

Then for any vector $X \in \mathbb{R}^{2^m}$, the following inequality

$$\|PX\|_1 \geq 2^m \|X\|_\infty$$

holds. Here, $\|\cdot\|_1$ and $\|\cdot\|_\infty$ are the usual 1-norm and ∞ -norm defined in \mathbb{R}^{2^m} .

Proof. $PP^T = 2^m I$ and in particular, P^T is invertible. Let $X = P^T Y$. Then

$$(4.1) \quad \|PX\|_1 = \|PP^T Y\|_1 = \|2^m Y\|_1 = 2^m \|Y\|_1.$$

For $1 \leq i \leq 2^m$, let the i -th component of X, Y be x_i, y_i respectively. For $1 \leq i, j \leq 2^m$, let $P_{i,j}$ be the i -th row, j -th column entry of P . Then from $X = P^T Y$,

$$x_i = \sum_{j=1}^{2^m} P_{j,i} y_j$$

for any $1 \leq i \leq 2^m$ and thus

$$|x_i| = \left| \sum_{j=1}^{2^m} P_{j,i} y_j \right| \leq \sum_{j=1}^{2^m} |P_{j,i}| |y_j| = \sum_{j=1}^{2^m} |y_j| = \|Y\|_1.$$

It follows that

$$\|X\|_\infty = \max_{1 \leq i \leq 2^m} \{|x_i|\} \leq \|Y\|_1$$

and with (4.1), we are done. \square

Fix $z \in A$. Let $X_z := \{x \in (\mathbb{Z}/2\mathbb{Z})^n \mid x < z + x\}$ and $D_z := \{d \in A \mid \langle d, z \rangle = 1\}$. Then $|X_z| = 2^{n-1}$ and by (2) of Lemma 2.2, we also have $|D_z| = 2^{n-1}$. Let $X_z = \{x_1, x_2, \dots, x_{2^{n-1}}\}$ and $D_z = \{d_1, d_2, \dots, d_{2^{n-1}}\}$. The order of the elements is irrelevant. Let V be a vector in $\mathbb{R}^{2^{n-1}}$, whose i -th element is

$$(4.2) \quad v_i := \sum_{\substack{b \in A \\ b < b+d_i}} 2n_{b, d_i+b} \log(u_b) \log(u_{d_i+b}) (-1)^{\langle b, z \rangle}$$

for $1 \leq i \leq 2^{n-1}$. Let P_z be a $2^{n-1} \times 2^{n-1}$ matrix whose entry of i -th row, j -th column is $(-1)^{\langle x_i, d_j \rangle}$ for $1 \leq i, j \leq 2^{n-1}$. Then each entry of P_z is either 1 or -1 . Now we show that the rows of P_z are perpendicular. Let $1 \leq i < j \leq 2^{n-1}$. Then the inner product in $\mathbb{R}^{2^{n-1}}$ of i -th row and j -th row of P_z is

$$\sum_{k=1}^{2^{n-1}} (-1)^{\langle x_i, d_k \rangle} \cdot (-1)^{\langle x_j, d_k \rangle} = \sum_{k=1}^{2^{n-1}} (-1)^{\langle x_i+x_j, d_k \rangle} = \sum_{d \in D_z} (-1)^{\langle x_i+x_j, d \rangle}.$$

Take any element d' of D_z . Then $D_z = d' + z^\perp$, and thus

$$\sum_{d \in D_z} (-1)^{\langle x_i+x_j, d \rangle} = \sum_{d \in z^\perp} (-1)^{\langle x_i+x_j, d+d' \rangle} = (-1)^{\langle x_i+x_j, d' \rangle} \sum_{d \in z^\perp} (-1)^{\langle x_i+x_j, d \rangle}.$$

Since x_i and x_j are elements of X_z , we have $x_i < x_i + z$ and $x_j < x_j + z$. Therefore $x_i + x_j \neq z$. Also, $x_i + x_j \neq 0$ since they are distinct. By Lemma 2.2 (3),

$$\begin{aligned} \sum_{d \in z^\perp} (-1)^{\langle x_i + x_j, d \rangle} &= |\{d \in z^\perp \mid \langle x_i + x_j, d \rangle = 0\}| - |\{d \in z^\perp \mid \langle x_i + x_j, d \rangle = 1\}| \\ &= |z^\perp \cap (x_i + x_j)^\perp| - (|z^\perp| - |z^\perp \cap (x_i + x_j)^\perp|) \\ &= 2 |z^\perp \cap (x_i + x_j)^\perp| - |z^\perp| \\ &= 2 \cdot 2^{n-2} - 2^{n-1} \\ &= 0. \end{aligned}$$

Therefore the i -th row and j -th row of P_z are perpendicular. Now by Lemma 4.1,

$$\sum_{i=1}^{2^{n-1}} \left| \sum_{j=1}^{2^{n-1}} v_j (-1)^{\langle x_i, d_j \rangle} \right| = \|P_z V\|_1 \geq 2^{n-1} \|V\|_\infty = 2^{n-1} \max_{1 \leq j \leq n} |v_j|.$$

Rewriting the above inequality without using the indices i and j , and substituting v_j with (4.2), we have

$$\begin{aligned} &\sum_{\substack{x \in (\mathbb{Z}/2\mathbb{Z})^n \\ x < z+x}} \left| \sum_{\substack{d \in A \\ \langle d, z \rangle = 1}} \sum_{\substack{b \in A \\ b < b+d}} 2n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle} (-1)^{\langle d, x \rangle} \right| \\ &\geq 2^{n-1} \max_{\substack{d \in A \\ \langle d, z \rangle = 1}} \left\{ \left| \sum_{\substack{b \in A \\ b < b+d}} 2n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle} \right| \right\}. \end{aligned}$$

Applying the above inequality to each summand of (3.3), we get

$$\|w\|_1 \geq 2^n \sum_{z \in A} \max_{\substack{d \in A \\ \langle d, z \rangle = 1}} \left\{ \left| \sum_{\substack{b \in A \\ b < b+d}} n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle} \right| \right\}.$$

Since every summands are nonnegative, for any $d' \in A$,

$$\begin{aligned} \|w\|_1 &\geq 2^n \sum_{\substack{z \in A \\ \langle d', z \rangle = 1}} \max_{\substack{d \in A \\ \langle d, z \rangle = 1}} \left\{ \left| \sum_{\substack{b \in A \\ b < b+d}} n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle} \right| \right\} \\ &\geq 2^n \sum_{\substack{z \in A \\ \langle d', z \rangle = 1}} \left| \sum_{\substack{b \in A \\ b < b+d'}} n_{b, d'+b} \log(u_b) \log(u_{d'+b}) (-1)^{\langle b, z \rangle} \right| \end{aligned}$$

holds. Therefore we have

$$(4.3) \quad \|w\|_1 \geq 2^n \max_{d \in A} \left\{ \sum_{\substack{z \in A \\ \langle d, z \rangle = 1}} \left| \sum_{\substack{b \in A \\ b < b+d}} n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle} \right| \right\}.$$

This time, fix $d \in A$. The following arguments are similar to above. Let $B_d := \{b \in (\mathbb{Z}/2\mathbb{Z})^n \mid b < d+b\}$ and $Z_d := \{z \in A \mid \langle d, z \rangle = 1\}$. Then $|B_d| = |Z_d| = 2^{n-1}$. Let $B_d = \{b_1, b_2, \dots, b_{2^{n-1}}\}$ with $b_1 = 0$ and let $Z_d = \{z_1, \dots, z_{2^{n-1}}\}$. Let V' be a vector in $\mathbb{R}^{2^{n-1}}$, whose 1st element is $v'_1 = 0$ and i -th element is

$$v'_i := n_{b_i, d+b_i} \log(u_{b_i}) \log(u_{d+b_i})$$

for $1 < i \leq 2^{n-1}$. Let Q_d be a $2^{n-1} \times 2^{n-1}$ matrix whose entry of i -th row, j -th column is $(-1)^{\langle z_i, b_j \rangle}$ for $1 \leq i, j \leq 2^{n-1}$. Then each entry of Q_d is either 1 or -1 . We now show that the rows of Q_d are perpendicular. The previous argument on the rows of P_z shows that in fact the columns of Q_d are perpendicular. Hence $Q_d^T Q_d = 2^{n-1} I = Q_d Q_d^T$, and the rows of Q_d are also perpendicular. Then by Lemma 4.1,

$$(4.4) \quad \|Q_d V'\|_1 \geq 2^{n-1} \|V'\|_\infty.$$

The left hand side of (4.4) is

$$\sum_{i=1}^{2^{n-1}} \left| \sum_{j=1}^{2^{n-1}} v'_j (-1)^{\langle b_j, z_i \rangle} \right| = \sum_{\substack{z \in A \\ \langle d, z \rangle = 1}} \left| \sum_{\substack{b \in A \\ b < b+d}} n_{b, d+b} \log(u_b) \log(u_{d+b}) (-1)^{\langle b, z \rangle} \right|$$

while the right hand side of (4.4) is

$$2^{n-1} \max\{0, |v'_2|, \dots, |v'_{2^{n-1}}|\} = 2^{n-1} \max_{\substack{b \in A \\ b < b+d}} \{|n_{b, d+b} \log(u_b) \log(u_{d+b})|\}.$$

Applying (4.4) to the right hand side of (4.3), we get

$$\|w\|_1 \geq 2^{2n-1} \max_{d \in A} \left\{ \max_{\substack{b \in A \\ b < b+d}} \{|n_{b, d+b} \log(u_b) \log(u_{d+b})|\} \right\}.$$

By Lemma 4.2 below, if $b, c \in A$ and $b < c$, $\log(u_b) \log(u_c) \geq \log\left(\frac{1+\sqrt{5}}{2}\right) \log(1+\sqrt{2})$. If there exists $b, c \in A$ such that $b < c$ and $n_{b,c} \neq 0$, we have

$$(4.5) \quad \|w\|_1 \geq 2^{2n-1} \log\left(\frac{1+\sqrt{5}}{2}\right) \log(1+\sqrt{2}).$$

In summary, the above inequality holds for any nonzero $w \in \bigwedge^2 \text{LOG}(\mathcal{O}_L^*)$.

Lemma 4.2. *For square-free integer m , let $v_m > 1$ be the fundamental unit of $\mathbb{Q}[\sqrt{m}]$. Then, $v_m \geq \frac{1+\sqrt{5}}{2}$ and the equality holds if and only if $m = 5$. Furthermore, if $m \neq 5$, $v_m \geq 1 + \sqrt{2}$ and the equality holds if and only if $m = 2$.*

Proof. First, consider the case $m \equiv 2, 3 \pmod{4}$. The fundamental unit v_m is of the form $a + b\sqrt{m}$ where a, b are the smallest positive integers satisfying $a^2 - mb^2 = \pm 1$. If $m = 2$, $v_2 = 1 + \sqrt{2}$ and if $m \neq 2$, $v_m \geq 1 + \sqrt{m} > 1 + \sqrt{2}$. Now consider the case $m \equiv 1 \pmod{4}$. Then v_m is of the form $\frac{a+b\sqrt{m}}{2}$ where a, b are the smallest positive integers satisfying $a^2 - mb^2 = \pm 4$.

If $m = 5$, $v_5 = \frac{1+\sqrt{5}}{2}$ and if $m = 13$, $v_{13} = \frac{3+\sqrt{13}}{2} > 1 + \sqrt{2}$. Otherwise, if $m \geq 17$, then $v_m \geq \frac{1+\sqrt{m}}{2} \geq \frac{1+\sqrt{17}}{2} > 1 + \sqrt{2}$. \square

We now turn to the proof of the main theorem.

proof of Theorem 1.3. Let u be any element of \mathcal{O}_L^* . By Lemma 2.3, $2^{n-1} \text{LOG}(u) \in \text{LOG}(E)$. Thus if nonzero w is in $\bigwedge^2 \text{LOG}(\mathcal{O}_L^*)$, then $2^{2n-2}w \in \bigwedge^2 \text{LOG}(E)$. Thus by (4.5),

$$(4.6) \quad \|w\|_1 = \frac{1}{2^{2n-2}} \|2^{2n-2}w\|_1 \geq 2 \log \left(\frac{1+\sqrt{5}}{2} \right) \log(1 + \sqrt{2}) \approx 0.8483.$$

\square

Remark 4.3. The lower bound of (4.6) may not be optimal. In other words, there might be a greater lower bound for $\|w\|_1$. However, for the case $L = \mathbb{Q}[\sqrt{2}, \sqrt{5}]$ and $w = \pm \text{LOG}(\frac{1+\sqrt{5}}{2}) \wedge \text{LOG}(1 + \sqrt{2})$, then $\|w\|_1 = 8 \log(\frac{1+\sqrt{5}}{2}) \log(1 + \sqrt{2}) \approx 3.3930$ and thus the optimal lower bound for (4.6) is at most 3.3930.

REFERENCES

- DEPARTMENT OF MATHEMATICAL SCIENCES, SEOUL NATIONAL UNIVERSITY, GWANAK-RO 1,
GWANKAK-GU, SEOUL, SOUTH KOREA 08826
Email address: dohyeongkim@snu.ac.kr
- DEPARTMENT OF MATHEMATICAL SCIENCES, SEOUL NATIONAL UNIVERSITY, GWANAK-RO 1,
GWANKAK-GU, SEOUL, SOUTH KOREA 08826
Email address: shsong0611@snu.ac.kr