ACTA ARITHMETICA
164.1 (2014)

Polynomial relations amongst algebraic units of low measure

by

John Garza (Des Moines, IA)

1. Introduction. Amongst the absolute values in a place v of an algebraic number field $\mathbb{K}$, two play a role in this article. If v is archimedean, let $\|\cdot\|_v$ denote the unique absolute value in v that restricts to the usual archimedean absolute value on $\mathbb{Q}$. If v is non-archimedean and $v \mid p$, let $\|\cdot\|_v$ denote the unique absolute value in v that restricts to the usual p-adic absolute value on $\mathbb{Q}$. For each place v of $\mathbb{K}$, let $\mathbb{K}_v$ and $\mathbb{Q}_v$ be the completions of $\mathbb{K}$ and $\mathbb{Q}$ with respect to v and define the local degree of v as $d_v = [\mathbb{K}_v : \mathbb{Q}_v]$. For all places v let $|\cdot|_v = \|\cdot\|_v^{d_v/d}$.

The absolute values $|\cdot|_v$ satisfy the product rule: if $\alpha \in \mathbb{K}^\times$, then $\prod_v |\alpha|_v = 1$. The *absolute* (*logarithmic*) *Weil height* of α is defined as $h(\alpha) = \sum_v \log^+ |\alpha|_v$ where the sum is over all places v of $\mathbb{K}$. Because of the way in which the absolute values $|\cdot|_v$ are normalized, $h(\alpha)$ does not depend on the field $\mathbb{K}$ in which α is contained.

By Kronecker's theorem $h(\alpha) = 0$ if and only if $\alpha = 0$ or $\alpha \in \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$. In 1933, Lehmer [L] asked wether or not there exists a constant $\varrho > 1$ such that

$$\deg(\alpha)h(\alpha) \geq \log \varrho \tag{1.1}$$

in all other cases. Lehmer's question remains unresolved to this day. For algebraic numbers α the *Mahler measure* $M(\alpha)$ of α is defined by $\log M(\alpha) = \deg(\alpha)h(\alpha)$. If $m_{\alpha,\mathbb{Z}} = a_0 \prod_{i=1}^d (x - \alpha_i) \in \mathbb{Z}[x]$ is the minimal polynomial of α in $\mathbb{Z}[x]$, it is known that

$$M(\alpha) = |a_0| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}. \tag{1.2}$$

The smallest non-zero Mahler measure known is that of the roots of $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$, and it is thought by many that

2010 *Mathematics Subject Classification*: Primary 11R09; Secondary 11G50.
Key words and phrases: Mahler measure, Weil height.

DOI: 10.4064/aa164-1-2

if the answer to Lehmer's question is yes then the minimum possible ϱ is the log of the Mahler measure of this polynomial.

If $\alpha \in \overline{\mathbb{Q}}^\times$ is not an algebraic integer, then the $|a_0|$ of equation (1.2) is at least 2. It follows that $M(\alpha) \geq 2$ so that Lehmer's question restricts to algebraic integers. For an algebraic number field $\mathbb{K}$, we let $\mathcal{O}_{\mathbb{K}}$ be the set of algebraic integers in $\mathbb{K}$. Also, if $\alpha \in \overline{\mathbb{Q}}^\times$ is an algebraic integer that is not a unit then

$$\mathrm{Norm}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) \geq 2. \tag{1.3}$$

It follows from (1.2) that (1.3) implies $M(\alpha) \geq 2$ and that Lehmer's problem restricts to consideration of algebraic units. We will let $\mathcal{O}_{\mathbb{K}}^\times$ denote the multiplicative group of algebraic units in $\mathbb{K}$.

It was shown in [G2] that, within a fixed algebraic number field, a large set of units of low measure must satisfy a multiplicative relation with small exponents. This article obtains the results of [G2] as a special case of polynomial relations that must exist amongst a set of algebraic units of low measure. Related results include those obtained by Beukers and Zagier [BZ], Cohen and Zannier [CZ], Garza, Ishak and Pinner [GIP], Samuels [Sa], and Schinzel [Sch].

In order to review the result of [G2], we restate the key definitions presented there. A set $\{\alpha_1, \ldots, \alpha_r\} \subseteq \overline{\mathbb{Q}}^\times$ is said to be *multiplicatively independent* if the only solution to the equation $\alpha_1^{m_1} \cdots \alpha_r^{m_r} = 1$ with $m_1, \ldots, m_r \in \mathbb{Z}$ is $m_1 = \cdots = m_r = 0$. It follows that if $\{\alpha_1, \ldots, \alpha_r\}$ is multiplicatively independent then $\{\alpha_1, \ldots, \alpha_r\} \cap \mathrm{Tor}(\overline{\mathbb{Q}}^\times) = \emptyset$. We will say that $\{\alpha_1, \ldots, \alpha_r\} \subset \overline{\mathbb{Q}}^\times$ is *multiplicatively independent up to exponent* n if the inclusion $\alpha_1^{m_1} \cdots \alpha_r^{m_r} \in \mathrm{Tor}(\overline{\mathbb{Q}}^\times)$ for $0 \leq |m_i| \leq n$ implies that $m_1 = \cdots = m_n = 0$. The paper [G1] established that for algebraic units $\alpha_1, \ldots, \alpha_r$, $d = [\mathbb{Q}(\alpha_1, \ldots, \alpha_r) : \mathbb{Q}]$, $s \in \mathbb{N}$ minimal such that $s > 2^{d/r}$, and $\alpha_1, \ldots, \alpha_r$ multiplicatively independent up to exponent $s-1$,

$$\sum_{i=1}^{r} h(\alpha_i) \geq \frac{\log 2}{2(s-1)}. \tag{1.4}$$

This article will recapture the above inequality as the limiting case of a more general concept.

2. Main result. For $f \in \mathbb{Q}[x_1, \ldots, x_r]$ we define the *length* $\mathcal{L}(f)$ of f as the sum of the absolute values of the coefficients of f. For a monomial $g = x_1^{\beta_1} \cdots x_r^{\beta_r} \in \mathbb{Q}[x_1, \ldots, x_r]$ we define the degree of g as $\max\{\beta_1, \ldots, \beta_r\}$. For $f \in \mathbb{Q}[x_1, \ldots, x_r]$ we define the degree $\partial(f)$ of f as the maximum of the degrees of the monomials of f. For

$$\mathcal{A} = \{(\alpha_1, \ldots, \alpha_r)\} \subset (\mathcal{O}_{\mathbb{K}})^r$$

we define

$$\mathcal{I}(\mathcal{A}) = \{f \in \mathbb{Q}[x_1, \ldots, x_r] \mid f(\alpha_1, \ldots, \alpha_r) = 0\}.$$

That is, $\mathcal{I}(\mathcal{A})$ is the ideal of polynomials in $\mathbb{Q}[x_1, \ldots, x_r]$ that vanish at the point $(\alpha_1, \ldots, \alpha_r)$. For $r, s, m \in \mathbb{Z}^+$ we define

$$\mathcal{P}(r, m, s) = \{f \in \mathbb{Z}[x_1, \ldots, x_r] \mid \mathcal{L}(f) \leq m \text{ and } \partial(f) \leq s\}.$$

The set $\{\alpha_1, \ldots, \alpha_r\}$ is *polynomially independent over* $\mathbb{Z}[x_1, \ldots, x_r]$ *of length* m *and exponent* s if

$$\mathcal{P}(r, m, s) \cap \mathcal{I}(\mathcal{A}) = \{0\}.$$

We now state the main result of this article.

THEOREM 2.1. *Let* $\mathbb{K}$ *be an algebraic number field of degree* d *over* $\mathbb{Q}$ *and let* $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_{\mathbb{K}}$ *be polynomially independent of exponent* s *and length* $2m$. *If*

$$mr \log(s+1) - \log(m!) > d \log(4m) \tag{2.1}$$

then

$$s \sum_{i=1}^{r} h(\alpha_i) > \log 2.$$

3. Preliminary lemmas. In this section we present three lemmas that will be used in the proof of Theorem 2.1. Lemmas 1 and 2 were proven in [G1] and their proofs are not included here.

LEMMA 1. *Let* $\mathbb{K}/\mathbb{Q}$ *be a finite Galois extension and let* $p \in \mathbb{N}$ *be a prime with ramification index* e *in* $\mathbb{K}$. *Let* $\mathcal{A}_p = \{v_1, \ldots, v_t\}$ *be the set of places of* $\mathbb{K}$ *extending the* p*-adic place of* $\mathbb{Q}$. *For* $v_i \in \mathcal{A}_p$ *let* $\mathcal{M}_{v_i} = \{\alpha \in \mathbb{K} \mid |\alpha|_{v_i} < 1\}$. *Let* $s \in \mathbb{N}$, $s \leq t$ *and let* $\beta \in \mathbb{K}^\times$. *If* $\beta \in \mathcal{M}_{v_1}^{a_1} \cdots \mathcal{M}_{v_s}^{a_s}$ *for* $a_1, \ldots, a_s \in \mathbb{N} \cup \{0\}$, *then*

$$\sum_{\mathcal{A}_p} \log |\beta|_{v_i} \leq (-\log p) \frac{1}{et} \sum_{j=1}^{s} a_j.$$

LEMMA 2. *Let* $\alpha_1, \ldots, \alpha_n \in \overline{\mathbb{Q}}^\times$, *let* $\mathbb{K}$ *be the Galois closure of the field* $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ *and let* $d = [\mathbb{K} : \mathbb{Q}]$. *For* $1 \leq j \leq n$ *and* $1 \leq k \leq m$ *let* $b_{j,k} \in \mathbb{N} \cup \{0\}$ *be such that* $\sum b_{j,k} \geq 1$ *and let* $c_k \in \mathbb{Z} - \{0\}$. *Define*

$$\delta = \sum_{k=1}^{m} c_k \prod_{j=1}^{n} \alpha_j^{b_{j,k}}, \qquad M_j = \max\{b_{j,k} \mid 1 \leq k \leq m\},$$

$$\mathcal{L} = \sum_{k} |c_k|, \qquad w = \prod_{s \nmid \infty} |\delta|_v.$$

For each place $v \mid \infty$, let $a_v \in \mathbb{R}^+$ *be defined via*

$$\|\delta\|_v = a_v \prod_{j=1}^{n} \max\{1, \|\alpha_j^{M_j}\|_v\}$$

and let

$$A = \prod_{v\mid\infty} (a_v)^{d_v/d}.$$

If $\delta \neq 0$, *then*

$$wA \le 1, \quad A \le \mathcal{L} \quad \textit{and} \quad \sum_{j=1}^{n} M_j h(\alpha_j) \ge \log(1/wA).$$

LEMMA 3. *Let* $\mathbb{K}$ *be an algebraic number field of degree* d *over* $\mathbb{Q}$ *and let* $\mathcal{O}_{\mathbb{K}}$ *be the ring of integers of* $\mathbb{K}$. *For* $m \in \mathbb{Z}^+$,

$$|\mathcal{O}_{\mathbb{K}} : m\mathcal{O}_{\mathbb{K}}| = m^d.$$

Proof. For $m = 1$ there is nothing to prove. Suppose $m \ge 2$. We know that $(\mathcal{O}_{\mathbb{K}}, +)$ is a free abelian group of rank d. Let $\omega_1, \ldots, \omega_d \in \mathcal{O}_{\mathbb{K}}$ be such that $(\mathcal{O}_{\mathbb{K}}, +) = \langle \omega_1, \ldots, \omega_d \rangle$. We have $m\mathcal{O}_{\mathbb{K}} \triangleleft \mathcal{O}_{\mathbb{K}}$. Let $\Psi : \mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{K}}/m\mathcal{O}_{\mathbb{K}}$ be the natural projection homomorphism. Then $\mathcal{O}_{\mathbb{K}}/m\mathcal{O}_{\mathbb{K}} = \langle \Psi(\omega_1), \ldots, \Psi(\omega_d) \rangle$. We must show that there exists no non-trivial linear relation among $\Psi(\omega_1), \ldots, \Psi(\omega_d)$ with coefficients $0 \le c_i \le m-1$. To this end, assume there exist $\{c_1, \ldots, c_d\} \in \{0, \ldots, m-1\}$ not all zero such that $\sum_{i=1}^{d} c_i \Psi(\omega_i) = \overline{0}$. Then $\sum_{i=1}^{d} c_i \omega_i \in \ker \Psi$, so

$$\sum_{i=1}^{d} c_i \omega_i = m\beta, \qquad \beta \in \mathcal{O}_{\mathbb{K}}.$$

Since not all c_i are 0, we see that $\beta \neq 0$. Let $b_1, \ldots, b_d \in \mathbb{Z}$ be such that $\sum_{i=1}^{d} b_i \omega_i = \beta$. Since $\beta \neq 0$, there exists $b_j \neq 0$. Now,

$$\begin{aligned} 0 = m\beta - m\beta &= \sum_{i=1}^{d} c_i \omega_i - m\Big(\sum_{i=1}^{d} b_i \omega_i\Big) = \sum_{i=1}^{d} c_i \omega_i - \sum_{i=1}^{d} (m b_i) \omega_i \\ &= \sum_{i=1}^{d} (c_i - m b_i) \omega_i. \end{aligned}$$

The last equation implies that $c_i - m b_i = 0$ for $i = 1, \ldots, d$. In particular, $c_j = m b_j$. Since $b_j \neq 0$, this contradicts the assumption that $0 \le c_j \le m-1$. We have thus shown that there is no non-trivial linear relation amongst $\Psi(\omega_1), \ldots, \Psi(\omega_d)$ with coefficients $0 \le c_i \le m-1$. ∎

4. Proof of the main result. Given $m \in \mathbb{Z}^+$ it follows from Lemma 3 that $|\mathcal{O}_{\mathbb{K}} : 4m\mathcal{O}_{\mathbb{K}}| = (4m)^d$. Let Λ be the set of monic monomials in

$\mathbb{Z}[x_1, \ldots, x_r]$ of degree less than or equal to s. By the Counting Principle, $|\Lambda| = (s+1)^r$. An application of the formula for counting combinations with replacement shows that

$$|\mathcal{P}(r, m, s)| \geq \sum_{j=0}^{m} \binom{|\Lambda| + j - 1}{j}.$$

We now recall the following identity from Pascal's triangle:

$$\sum_{j=0}^{m} \binom{|\Lambda| + j - 1}{j} = \binom{|\Lambda| + m}{m},$$

and recognize the lower bound

$$\binom{|\Lambda| + m}{m} \geq \frac{|\Lambda|^m}{m!}.$$

The inequality (2.1) implies

$$|\mathcal{P}(r, m, s)| > |\mathcal{O}_{\mathbb{K}} : 4m\mathcal{O}_{\mathbb{K}}|.$$

Let $\Psi : \mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{K}}/4m\mathcal{O}_{\mathbb{K}}$ be the natural homomorphism. The last inequality implies the existence of distinct f and g in $\mathcal{P}(r, m, s)$ such that

$$\Psi(f(\alpha_1, \ldots, \alpha_r)) = \Psi(g(\alpha_1, \ldots, \alpha_r)).$$

It follows that $(f - g)(\alpha_1, \ldots, \alpha_r) \in 4m\mathcal{O}_{\mathbb{K}}$. Since $f - g \in \mathcal{P}(r, 2m, s) \setminus \{0\}$ and

$$\mathcal{I}(\mathcal{A}) \cap \mathcal{P}(r, 2m, s) = \{0\},$$

we have $(f - g)(\alpha_1, \ldots, \alpha_r) \neq 0$. An application of Lemmas 1 and 2 with $\delta = (f - g)(\alpha_1, \ldots, \alpha_r) \neq 0$ results in $w \leq 1/4m$ and $A \leq 2m$. Therefore

$$s \sum_{i=1}^{r} h(\alpha_i) \geq \log 2.$$

5. Application of the Gröbner basis of $\mathcal{I}(\mathcal{A})$. Fix the lexicographic monomial ordering $x_1 < \cdots < x_r$ on the polynomial ring $\mathbb{Q}[x_1, \ldots, x_r]$. The symbol $G_{\mathcal{A}} = \{g_1, \ldots, g_n\} \subset \mathbb{Q}[x_1, \ldots, x_r]$ will denote the unique reduced Gröbner basis for $\mathcal{I}(\mathcal{A})$. For $g_i \in G_{\mathcal{A}}$ the leading term of g_i will be denoted $\mathrm{LT}(g_i)$ and the monomial ideal generated by the leading terms will be denoted $\mathrm{LT}(\mathcal{I}(\mathcal{A}))$. We recall that $\mathrm{LT}(g_i)$ is a monic monomial and as a result $\mathrm{LT}(g_i) \in \mathbb{Z}[x_1, \ldots, x_r]$. Furthermore, $\mathcal{M}$ will denote the set of monic monomials in $\mathbb{Z}[x_1, \ldots, x_r]$. Define $\Lambda = \mathcal{M} - \mathcal{M} \cap \mathrm{LT}(\mathcal{I}(\mathcal{A}))$. Thus Λ is the set of monic monomials in $\mathbb{Z}[x_1, \ldots, x_r]$ that are not divisible by the leading term of any element of $G_{\mathcal{A}}$. Finally, $\langle \Lambda \rangle \subset \mathbb{Z}[x_1, \ldots, x_r]$ will denote the additive abelian group generated by Λ. It follows from the definitions provided that $\langle \Lambda \rangle \cap \mathcal{I}(\mathcal{A}) = \{0\}$. Applying the formula for counting combinations with replacement we have

$$|\{f \in \langle \Lambda \rangle \mid \mathcal{L}(f) < k\}| \ge \binom{|\Lambda| + k}{k}.$$

Let $m = \min\{\partial(\mathrm{LT}(g_i)) \mid 1 \le i \le r\} - 1$. It follows that $x_1^{\beta_1} \cdots x_r^{\beta_r} \in \Lambda$ for $0 \le \beta_i \le m$, so $|\Lambda| \ge m^r$. This implies that

$$|\{f \in \langle \Lambda \rangle \mid \mathcal{L}(f) < k\}| \ge \binom{m^r + k}{k}.$$

If there exists $k \in \mathbb{Z}^+$ such that $\binom{m^r+k}{k} > (4k)^d$ then an application of the proof of Theorem 2.1 gives $\sum_{i=1}^r h(\alpha_i) \ge (\log 2)/m$.

6. Conclusion. If $\mathcal{I}(\mathcal{A})$ excludes polynomials of bounded length and bounded degree, then this article has shown that either $[\mathbb{Q}(\alpha_1, \ldots, \alpha_r) : \mathbb{Q}]$ or $h(\alpha_1) + \cdots + h(\alpha_r)$ must be large.

References

[BZ] F. Beukers and D. Zagier, *Lower bounds of heights of points on hypersurfaces*, Acta Arith. 79 (1997), 103–111.

[CZ] P. B. Cohen and U. Zannier, *Multiplicative dependence and bounded height, an example*, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), de Gruyter, 2000, 93–101.

[G1] J. Garza, *On the height of algebraic numbers with real conjugates*, Acta Arith. 128 (2007), 385–389.

[G2] J. Garza, *Multiplicative independence and bounded height*, Acta Arith. 151 (2012), 1–6.

[GIP] J. Garza, M. I. M. Ishak and C. Pinner, *On the product of the heights of algebraic numbers summing to real numbers*, Acta Arith. 142 (2010), 51–58.

[L] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.

[Sa] C. L. Samuels, *Lower bounds on the projective heights of algebraic points*, Acta Arith. 125 (2006), 41–50.

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

John Garza
Drake University
2507 University Ave
Des Moines, IA 50311, U.S.A.
E-mail: John.Garza@drake.edu

Received on 31.5.2013
and in revised form on 14.1.2014 (7469)