

HEIGHTS OF ALGEBRAIC NUMBERS AND SZEGÖ'S THEOREM

WAYNE LAWTON¹

ABSTRACT. In the present paper we derive an algorithm which yields approximations to the height of an algebraic number. The techniques are analytical and are motivated by prediction theoretic concepts.

Definition 1. Let $P(z) = a_n z^n + \cdots + a_1 z + a_0$ be a polynomial of degree n with complex coefficients. We define the *height* of P by the formula

$$H(P) = |a_n| \prod_{i=1}^n \sup(1, |x_i|),$$

where x_1, \dots, x_n are the complex roots of P and $|\cdot|$ denotes usual absolute value.

Definition 2. Let x be an algebraic number over the field of rational numbers and let P be the irreducible polynomial with integer coefficients such that $P(x) = 0$. We define the *height* of x to be $H(P)$.

Remark 1. If A is an endomorphism of a Lie group G and P is the characteristic polynomial of a matrix which represents the induced linear map by A on the tangent space to G at the identity, then $\log H(P)$ is the *entropy* of A as defined in [2, Corollary 16].

Remark 2. Our definition of height for an algebraic number is equivalent to the definition given in [7, Chapter 3]. Heights of algebraic numbers are important in diophantine geometry, particularly in the statement and proof of the celebrated Thue-Siegel-Roth theorem [7, Theorem 1, p. 93].

For any polynomial P as in Definition 1, we describe the construction of a decreasing sequence (h_l) of positive real numbers such that $\lim_{l \rightarrow \infty} h_l = (H(P))^2$. Each term of the sequence will be expressed as the quotient of two positive real numbers, each of which are sums of product combinations of the coefficients of the given polynomial. Thus, in order to approximate the

Received by the editors January 30, 1974.

AMS (MOS) subject classifications (1970). Primary 12D10; Secondary 30A08.

Key words and phrases. Height of algebraic number, Hilbert space, Gram determinant, Jensen's theorem, Szegő's theorem.

¹ Research supported by NSF grant GP-18961.

Copyright © 1975, American Mathematical Society

height of a polynomial, we do not utilize specific knowledge about the roots of the polynomial.

Let $P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_1 z + a_0$ be as in Definition 1. For any integer k define $\phi(k)$ by the formula

$$\phi(k) = \begin{cases} a_n \overline{a_{n-k}} + a_{n-1} \overline{a_{n-k-1}} + \cdots + a_{k+1} \overline{a_1} + a_k \overline{a_0} & \text{if } 0 \leq k \leq n, \\ \overline{a_n} a_{n+k} + \overline{a_{n-1}} a_{n+k-1} + \cdots + \overline{a_{-k+1}} a_1 + \overline{a_{-k}} a_0 & \text{if } -n \leq k < 0, \\ 0 & \text{if } k > n \text{ or } k < -n. \end{cases}$$

Now, for any positive integer l , define an $l \times l$ matrix M_l by the formula $M_l = (m_{ij})$ with $m_{ij} = \phi(i-j)$. Finally, let $g_l = \det(M_l)$ and define the sequence (h_l) by the rule $h_l = g_{l+1}/g_l$.

Theorem 1. *The sequence (h_l) is decreasing and converges to $(H(P))^2$.*

Our proof of the above statement will proceed using three lemmas. With notation fixed as above, we introduce the Hilbert space V , of all complex valued functions f on $[0, 2\pi]$ such that $\int_0^{2\pi} |f(\theta)|^2 |P(e^{i\theta})|^2 d\theta < \infty$, equipped with the inner product

$$\langle f, g \rangle = \frac{1}{2\pi} \int_0^{2\pi} f(\theta) \overline{g(\theta)} |P(e^{i\theta})|^2 d\theta.$$

Let $w_m = e^{mi\theta} \in V$, $m \geq 0$, and let V_l be the subspace of V spanned by $\{w_1, \cdots, w_l\}$, $l \geq 1$.

Lemma 1. *For every $l \geq 1$, $h_l = \min_{w \in V_l} \|w_0 + w\|^2$.*

Proof. An elementary calculation yields $\langle w_s, w_t \rangle = \phi(t-s)$, hence g_l is the Gram determinant of $\{w_1, \cdots, w_l\}$ and g_{l+1} is the Gram determinant of $\{w_0, \cdots, w_l\}$. Applying [4, Theorem 8.7.4] finishes the proof. Clearly (h_l) is a decreasing sequence of positive numbers.

Lemma 2. $\lim_{l \rightarrow \infty} h_l = \exp[(1/2\pi) \int_0^{2\pi} \log |P(e^{i\theta})|^2 d\theta]$.

Proof. Clearly

$$\lim_{l \rightarrow \infty} \left(\min_{w \in V_l} \|w_0 + w\|^2 \right) = \inf_Q \frac{1}{2\pi} \int_0^{2\pi} |Q(\theta)|^2 |P(e^{i\theta})|^2 d\theta$$

where the infimum is taken over all positive trigonometric polynomials with leading coefficient 1 = w_0 . The equality stated in the lemma is a direct consequence of Szegő's theorem [5, pp. 189–192].

Lemma 3. $(1/2\pi) \int_0^{2\pi} \log |P(e^{i\theta})|^2 d\theta = \log(H(P))^2$.

Proof. Define the holomorphic function $\psi(z) = z^n P(1/z)P(z)$ and use Jensen's theorem [6, pp. 256–257] to evaluate $(1/2\pi)\int_0^{2\pi}\log|\psi(e^{i\theta})| d\theta = \log(H(P))^2$. Since $|\psi(e^{i\theta})| = |P(e^{i\theta})|^2$ we are done.

Our proof is concluded by exponentiating both sides of the equation in Lemma 3 and then comparing with the equation in Lemma 2. A direct consequence of an inequality for Gram determinants found in [4, Theorem 8.8.1] is an upper bound for the height of a polynomial given by

$$\text{Corollary 1. } H(P) \leq \sqrt{|a_0|^2 + \cdots + |a_n|^2}.$$

This upper bound strengthens the result in [7, p. 47] which states that $H(P) \leq 2^n \max|a_i|$ when P is monic.

Remark 3. In [9] the question is raised as to whether the set of heights of algebraic numbers which are not roots of unity is bounded away from 1. It is still open.² The smallest value known for a height above 1 is 1.17628, corresponding to the polynomial

$$x^{10} + x^9 - x^7 - x^6 - x^4 - x^3 + x + 1.$$

Certain questions arising in topological dynamics have led the author to conjecture that the set of heights of algebraic numbers which are not roots of unity is bounded away from 1. Using the techniques in [8], it is possible to show this conjecture is equivalent to the conjecture that no infinite dimensional compact topological group admits an ergodic automorphism having finite entropy. The set of heights of those algebraic numbers of absolute value greater than 1 and whose conjugates have absolute value less than 1 is bounded away from 1. Such numbers are the Pisot-Vajayayagharan numbers discussed in [3, Chapter 8]. Since the set of all such numbers is a closed subset in the complex plane [3, p.134], the conjecture is true for these numbers. In [1] it is proved that the height of an algebraic integer of degree h which is not a root of unity is greater than $1 + (52h \log 6h)^{-1}$. It would be interesting, as a heuristic amusement, to calculate heights in specific number fields using Theorem 1 and a computer.

BIBLIOGRAPHY

1. P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. **18** (1971), 355–369.
2. Rufus Bowen, *Entropy for group endomorphisms and homogeneous spaces*, Trans. Amer. Math. Soc. **153** (1971), 401–414. MR **43** #469.

² The history of this problem was brought to the author's attention by the referee's report.

3. J. W. S. Cassels, *An introduction to diophantine approximation*, Cambridge Tracts in Math. and Math. Phys., no. 45, Cambridge Univ. Press, New York, 1957. MR 19, 396.
4. P. J. Davis, *Interpolation and approximation*, Blaisdell, New York, 1963. MR 28 #393.
5. H. Dym and H. P. McKean, *Fourier series and integrals*, Academic Press, New York, 1972.
6. Einar Hille, *Analytic function theory*. Vol. 1, Ginn, Boston, Mass., 1959. MR 21 #6415.
7. Serge Lang, *Diophantine geometry*, Interscience Tracts in Pure and Appl. Math., no. 11, Interscience, New York, 1962. MR 26 #119.
8. Wayne Lawton, *The structure of compact connected groups which admit an expansive automorphism*, Lecture Notes in Math., vol. 318, Springer-Verlag, Berlin and New York, 1973, pp. 182–196.
9. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.

DEPARTMENT OF MATHEMATICS, RICE UNIVERSITY, HOUSTON, TEXAS 77001

Current address: School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540