J.Sci.Soc.Thailand, 24(1998) 129-132

A P-ADIC LOWER BOUND FOR POLYNOMIAL EVALUATED AT AN ALGEBRAIC NUMBER

VICHIAN LAOHAKOSOL

Department of Mathematics, Kasetsart University, Bangkok 10900, Thailand.

(Received April 30, 1998)

ABSTRACT

Let F(x) be a polynomial with rational integral coefficients and let α be an algebraic number. A sharp lower bound for the p-adic valuation of nonzero $F(\alpha)$ is derived. The derivation, which makes use of a 1967 technique of R. Güting, gives a quantitative improvement of an old result of K. Mahler

INTRODUCTION

Let F(x) be a polynomial with rational integral coefficients, and let α be an algebraic number. In the theory of transcendence, one often needs to find a good lower bound for the valuation of $F(\alpha)$. Sharp lower bounds have already been obtained in the case of ordinary absolute valuation; see e.g. Shidlovskii [5]. However, in the case of p-adic valuation, the only well-known lower bound for $|F(\alpha)|_p$, where $|\ .\ |_p$ denotes the p-adic valuation ,normalized so that $|p|_p = 1/p$ (see e.g. Koblitz [3]), as distinct from the ordinary absolute valuation $|.|$ is due to Mahler [4, p.46]. The objective of this work is to improve upon this p-adic lower bound of Mahler by using a technique of Güting in 1967. Specifically, we prove the following result.

Theorem. Let α be an algebraic number, and let its minimal polynomial be

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \qquad (n \geq 1),$$

with rational integral coefficients. If

$$F(x) = A_0x^m + A_1x^{m-1} + \ldots + A_m \qquad (m \geq 1)$$

is a polynomial with rational integral coefficients, then either $F(\alpha) = 0$ or

$$|F(\alpha)|_p \geq \{ c_m(f) \max (1, |\alpha|_p^{n-1}) A^n \}^{-1}$$

where $A := \max (|A_0| , |A_1| ,..., |A_m|)$ denotes the height of F, and

$$c_m(f) := |a_0|^m \prod_{i=0}^{n-1}{}', (|\alpha_i|^{m+1} - 1) / (|\alpha_i| - 1) = |a_0|^m \prod_{i=0}^{n-1}{}' \{|\alpha_i|^m + |\alpha_i|^{m-1} + \ldots + 1\}$$

where $\alpha = \alpha_0, \alpha_1,\ldots,\alpha_{n-1}$ are all the conjugates of α, and Π' indicates that if α is a root of unity, then the product is to be replaced by $(m + 1)^n$.

Mahler [4, p.146] proved this theorem with $c_m(f) = (m+n)!a^m$, where $a = \max (|a_0|,|a_1|,\ldots,|a_n|)$ is the height of f . Before proceeding to the proof of the theorem, we first justify that our $c_m(f)$ supersedes the one obtained by Mahler.

Proposition. Let the notation be as above. Then

$$(m+n)!a^m \geq |a_0|^m \prod_{i=0}^{n-1}{}' \{ |\alpha_i|^m + |\alpha_i|^{m-1} + \ldots + 1 \},$$

with equality holds only in the case $m = n = 1$.

Proof of the proposition. For convenience, we call the expressions on the left, and right-hand sides of the assertion LHS and RHS, respectively. We split the proof into two parts.

Part I. Verification of the cases m = 1,2 ; n = 1,2.

Throughout, we implicitly use well-known results on symmetric functions for roots of a polynomial, see e.g. van der Waerden [6, Chapter 5].

(i) For m = 1, n = 1, we have

$$\text{LHS} = 2a\,, \quad \text{RHS} = |a_0|\,(\,|\alpha| + 1) = |a_0| + |a_1| \le 2a.$$

(ii) For m = 2, n = 1, we have

$$\text{LHS} = 6a^2\,, \quad \text{RHS} = |a_0|^2(|\alpha|^2 + |\alpha| + 1) = |a_0|^2 + |a_0a_1| + |a_1|^2 \le 3a^2\,.$$

(iii) For m = 1, n = 2, we have

$$\text{LHS} = 6a\,, \quad \text{RHS} = |a_0|(|\alpha| + 1)(|\alpha_1| + 1) = |a_0| + |a_2| + |a_0|(|\alpha| + |\alpha_1|).$$

Now for i = 0, 1, by the quadratic formula, we note that

$$|\alpha_i| \le \frac{|a_1| + \sqrt{|a_1^2 - 4a_0a_2|}}{2|a_0|} \le \frac{a + \sqrt{5a}}{2|a_0|}$$

Thus $|\alpha_0|\,(|\alpha| + |\alpha_1|) \le (1+\sqrt{5})a < 3.3a.$

Hence, RHS < 5.3a .

(iv) For m = 2, n = 2, making use of the estimate in (iii), we see that

$$\text{LHS} = 24a^2\,, \text{ while}$$

$$\begin{aligned}\text{RHS} &= |a_0|^2\,(|\alpha|^2 + |\alpha| + 1)(|\alpha_1|^2 + |\alpha_1| + 1)\\ &= |a_0|^2 + |a_2|^2 + |a_0^2\alpha\alpha_1|(|\alpha| + |\alpha_1|)\\ &\quad + |a_0|^2\{(|\alpha| + |\alpha_1|)^2 - |\alpha\alpha_1|\} + |a_0|^2(|\alpha| + |\alpha_1|)\\ &< a^2 + a^2 + 3.3a^2 + 10.9a^2 + 3.3a^2 < 20a^2.\end{aligned}$$

Part II. Verification of the cases m = 1,2 ; n ≥ 3 and m ≥ 3 ; n any positive integer.

Since $\text{RHS} \le |a_0|^m \prod_{i=0}^{n-1} (m+1) \max(1, |\alpha_i|^m) = (m+1)^n \{\,|a_0| \prod_{i=0}^{n-1} \max(1, |\alpha_i|\,)\,\}^m$,

then by a result of Duncan [1, Theorem 1, p. 58], we have

$$\text{RHS} \le (m+1)^n\,(n+1)^{m/2}\,a^m\,.$$

It remains to show that for m = 1,2 ; n ≥ 3 or m ≥ 3 ; all n , we must have

$$(m+n)!^2 > (m+1)^{2n}\,(n+1)^m\,. \qquad (*)$$

(v) The cases m = 1,2 ; n ≥ 3 can be directly checked by induction on n.

(vi) Finally, we consider the case m ≥ 3 and any positive integer n.

Fix m ≥ 3. We subdivide the consideration into two subcases.

Subcase 1. $1 \le n \le m-1$.

Since $(m+1)^n \le (m+n)!\,/\,m!$, then

$$\frac{(m+n)!^2}{(n+1)^m(m+1)^{2n}} \ge \frac{(m+n)!^2}{(n+1)^m}\,\frac{m!^2}{(m+n)!^2} = \frac{m!^2}{(n+1)^m} \ge \frac{m!^2}{m^m} > 1 \quad \text{for all } m \ge 3,$$

and so (*) is proved for this subcase.

Subcase 2. $n \ge m \ge 3$.

We proceed by induction on n.

(a) When n = m, we have

$$\frac{(m+n)!^2}{(m+1)^{2n}(n+1)^m} = \frac{(2m)!^2}{(m+1)^{3n}} > 1 \quad \text{for all } m \geq 3,$$

and so (*) is true.

(b) Assume (*) holds for n. Then

$$\begin{aligned}
(m+n+1)!^2 &= (m+n+1)^2 (m+n)!^2 \\
&> (m+n+1)^2(m+1)^{2n}(n+1)^m \quad \text{(by induction hypothesis)} \\
&\geq (2m+1)^2\frac{(m+1)^{2n+2}(n+1)^m}{(m+1)^2(n+2)^m}(n+2)^m \quad \text{(using } n \geq m\text{)} \\
&= \frac{(2m+1)^2}{(m+1)^2}(m+1)^{2n+2}(n+2)^m\left[1+\frac{1}{n+1}\right]^{-m} \\
&\geq (m+1)^{2n+2}(n+2)^m\left[2-\frac{1}{m+1}\right]^2\left[1+\frac{1}{n+1}\right]^{-(n+1)} \quad \text{(using } n \geq m\text{)} \\
&\geq (m+1)^{2n+2}(n+2)^m(2-1/4)^2\, e^{-1},
\end{aligned}$$

because $m \geq 3$ and $e > \{1 + 1/(n+1)\}^{n+1}$ for all $n \geq 1$. Since $(1.75)^2e^{-1} > 1$, then the result follows by induction.

PROOF OF THE THEOREM

The proof employed here is based upon an original idea of Mahler [4], but at one point we use a technique of Güting [2, Lemma C] to compute the absolute upper bound of the resultant involved.

Since f(x) has rational integral coefficients, then we can view $\alpha = \alpha_0$ and all its conjugates $\alpha_1,\ldots,\alpha_{n-1}$ as elements of both the field of complex numbers and that of the completion of the algebraic closure of the field of p-adic numbers. Let R be the resultant of f(x) and F(x), then (see e.g. van der Waerden [6, p. 106]) we have

$$R = a_0^m F(\alpha) F(\alpha_1)\ldots F(\alpha_{n-1}) .$$

For $i = 0,1,\ldots,n-1$, we see that

$$|F(\alpha_i)| = |A_0\alpha_i^m + A_1\alpha_i^{m-1} + \ldots + A_m| \leq AD_i(m) ,$$

where $$D_i(m) = \begin{cases} m+1 & \text{if } |\alpha_i| = 1 . \\ (|\alpha_i|^{m+1}-1)/(|\alpha_i|-1) & \text{if } |\alpha_i| \neq 1 \end{cases}$$

Therefore, $|R| \leq c_m(f) A^n$. Since f(x) is irreducible over the field of rational numbers, then $F(\alpha) = 0$ if and only if f(x) divides F(x) and so $F(\alpha) = 0$ if and only if $R = 0$. We now assume that $R \neq 0$. As R is a nonzero determinant all of whose elements are rational integers, we must have that

$$|R|_p \geq |R|^{-1} \geq (c_m(f) A^n)^{-1} .$$

By the arguments used in van der Waerden [6, p.105], and also in Mahler [4, pp.44-45], we conclude that there exist two polynomials g(x) and G(x) with rational integral coefficients and with deg G = n-1 such that $R = f(x)g(x) + F(x)G(x)$. That $f(\alpha) = 0$, $R \neq 0$, and $F(\alpha) \neq 0$, then imply $F(\alpha) = R /G(a)$. Since G(x) has rational integral coefficients and deg G = n-1, then

$$|G(\alpha)|_p \leq \max (1, |\alpha|_p^{n-1}) .$$

Hence, $$|F(\alpha)|_p \geq \{ c_m(f) \max (1, |\alpha|_p^{n-1}) A^n \}^{-1}$$ as desired.

REFERENCES

1. R. L. Duncan (1966) Some inequalities for polynomials, *Amer. Math. Monthly* **73**,58-59.
2. R. Güting (1967) Polynomials with multiple zeros, *Mathematika* **14**,181-196.
3. N. Koblitz (1977) P-adic Numbers, P-adic Analysis, and Zeta-Functions, Springer-Verlag, New York.
4. K. Mahler (1961) Lectures on Diophantine Approximations, University of Notre Dame Press, Notre Dame.
5. A. B. Shidlovskii (1989) Transcendental Numbers, Walter de Gruyter, Berlin.
6. B. L. van der Waerden (1970) Algebra, Volume I, Frederick Ungar, New York.

บทคัดย่อ

ให้ F(x) เป็นพหุนามที่มีสัมประสิทธิ์เป็นจำนวนเต็มตรรกยะ และให้ α เป็นจำนวนพีชคณิต ในงานนี้เป็นการหาขอบเขตล่างที่ดีขึ้นสำหรับค่าอนุวัตพี-แอดิกของ $F(\alpha)$ ที่ไม่เป็นศูนย์ วิธีการที่ใช้คือเทคนิคเมื่อปี ค.ศ. 1967 ของกุตติง และสิ่งที่ได้รับให้ผลที่ดีขึ้นกว่าผลเดิมของมาห์เลอร์