Journal of Mathematical Inequalities
Volume 6, Number 3 (2012), 447–451
doi:10.7153/jmi-06-41

ON A CONJECTURE OF SCHINZEL AND ZASSENHAUS

YILUN SHANG

(*Communicated by B. Uhrin*)

Abstract. A. Schinzel and H. Zassenhaus had the following conjecture regarding algebraic integers: If $\alpha \neq 0$ is an algebraic integer of degree n which is not a root of unity, then there exists a constant $c > 0$ such that

$$|\bar{\alpha}| \geqslant 1 + \frac{c}{n},$$

where $|\bar{\alpha}| = \max_{1 \leqslant i \leqslant n} |\alpha_i|$, $\alpha_1 = \alpha$ and $\alpha_2, \cdots, \alpha_n$ are the conjugates of α.

We give some partial solutions to this conjecture in this paper via spectral properties.

1. Introduction

In algebra, an algebraic integer of degree n is a complex root α of an irreducible monic polynomial $P(x)$ (a polynomial whose leading coefficient is 1) of degree n with integer coefficients, its minimal polynomial [7]. The other roots of $P(x)$ are called the conjugates of α. A theorem of Kronecker states that if α is an algebraic integer such that α and all of its conjugates in the complex numbers have absolute value 1, then α is a root of unity. Here, a root of unity is a complex number that equals 1 when raised to some integer power n. Furthermore, Schinzel and Zassenhaus [15] posed the following conjecture:

If $\alpha \neq 0$ is an algebraic integer of degree n which is not a root of unity, then there exists a constant $c > 0$ such that

$$|\bar{\alpha}| \geqslant 1 + \frac{c}{n},$$

where $|\bar{\alpha}| = \max_{1 \leqslant i \leqslant n} |\alpha_i|$ is said to be the maximal modulus of α, $\alpha_1 = \alpha$ and $\alpha_2, \cdots, \alpha_n$ are the conjugates of α.

This conjecture and some related issues such as Lehmer's conjecture [10] attracted a series of investigation on the maximal modulus of algebraic integers in the past couples of decades, see e.g. [1, 2, 4, 9, 12, 13, 14, 16]. Some progresses have already been made. Dobrowolski [5] first showed that

$$|\bar{\alpha}| > 1 + \frac{2 - \varepsilon}{n} \left(\frac{\ln \ln n}{\ln n} \right)^3,$$

Mathematics subject classification (2010): 15A42, 11R04.
Keywords and phrases: algebraic integer, eigenvalue, conjugate, root of unity.

Paper JMI-06-41

for $n > n_0(\varepsilon)$. The above constant coefficient $2-\varepsilon$ has been improved successively by Cantor and Straus [3] to $4-\varepsilon$, Louboutin [11] to $\frac{9}{2}-\varepsilon$ and Dubickas [6] to $\frac{64}{\pi^2}-\varepsilon$. Numerous relevant results have been reviewed in the monograph [13].

In this paper, we move a further step in this direction and provide some partial solutions to Schinzel and Zassenhaus's conjecture by virtue of some spectral properties of matrices. The main results are given in the next section.

2. The results

The following lemma of matrix spectrum is useful. The necessity in Lemma 1 is obvious while the sufficiency is not easy to see.

LEMMA 1. ([8]) *Let $A \in M_n(\mathbb{Z})$, the set of $n \times n$ matrices over $\mathbb{Z}$. Suppose A is non-singular. For $i = 1, \cdots, n$, let λ_i be characteristic roots of A (i.e., roots of its characteristic polynomial $\det(\lambda I - A) = 0$). The necessary and sufficient condition for λ_i, $i = 1, \cdots, n$, to be roots of unity is $|\lambda_i| = 1$ for $i = 1, \cdots, n$.*

As is customary, the spectral radius of a square matrix is defined as the supremum among the absolute values of its eigenvalues. The next lemma gives a lower bound for the spectral radius of a complex matrix.

LEMMA 2. ([8]) *Let A be an $n \times n$ complex matrix with $|\det A| > 1$ and let*

$$|\bar{\lambda}| = \max_{1 \leqslant i \leqslant n} |\lambda_i|,$$

where λ_i are the eigenvalues of A for $i = 1, \cdots, n$, then

$$|\bar{\lambda}| \geqslant 1 + \frac{\ln |\det A|}{n}.$$

THEOREM 1. *Let $\alpha \neq 0$ be an algebraic integer of degree n which is not a root of unity. Let $\alpha_1 = \alpha$, and $\alpha_2, \cdots, \alpha_n$ be the conjugates of α. Denote by $|\bar{\alpha}| = \max_{1 \leqslant i \leqslant n} |\alpha_i|$.*

(i) If the product $\alpha_1 \alpha_2 \cdots \alpha_n$ is not a root of unity, then

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln 2}{n};$$

(ii) If $M(\alpha) := |\alpha_1 \alpha_2 \cdots \alpha_n| > k \in \mathbb{N}$, then

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln(k+1)}{n}.$$

Proof. By definition, we have an irreducible polynomial $P(x)$:

$$P(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n, \tag{1}$$

where $a_i \in \mathbb{Z}$ for $i = 1, \cdots, n$, such that $\alpha_1, \cdots, \alpha_n$ are solutions of the equation $P(x) = 0$.

Define a matrix $A \in M_n(\mathbb{Z})$ by

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -a_n & -a_{n-1} & -a_{n-2} & \cdots & -a_2 & -a_1 \end{pmatrix}.$$

Thus, from (1) it is straightforward to check that $P(x)$ is the characteristic polynomial of matrix A, that is, $P(x) = \det(xI - A)$, where I is the $n \times n$ identity matrix. Therefore, $\alpha_1, \cdots, \alpha_n$ are the eigenvalues of A.

As for (i), since the product $\alpha_1 \alpha_2 \cdots \alpha_n$ is not a root of unity, by Lemma 1, we obtain

$$M(\alpha) = |\alpha_1 \cdots \alpha_n| \neq 1. \tag{2}$$

Since $A \in M_n(\mathbb{Z})$, then $\det A \in \mathbb{Z}$. In view of (2), we have

$$|\det A| = |\alpha_1 \cdots \alpha_n| \geqslant 2.$$

It follows from Lemma 2 that

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln |\det A|}{n}.$$

Consequently, we have

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln 2}{n}$$

as desired.

As for (ii), we similarly have

$$|\det A| = |\alpha_1 \cdots \alpha_n| \geqslant k + 1.$$

By Lemma 2, we analogously derive

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln(k+1)}{n},$$

which concludes the proof of Theorem 1. □

In the next result, we do not exclude the case α being the root of unity.

THEOREM 2. *For $k \in \mathbb{N}$ and $k > 1$, let $\alpha \neq 0$ be an algebraic integer of degree $n \geqslant \frac{1-\varepsilon}{\varepsilon} \ln k$ for some $\varepsilon \in (0,1)$. If $M(\alpha) = |\alpha_1 \alpha_2 \cdots \alpha_n| = k$, then*

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln k}{n},$$

where $|\bar{\alpha}| = \max_{1\leqslant i\leqslant n}|\alpha_i|$, $\alpha_1 = \alpha$ *and* $\alpha_2, \cdots, \alpha_n$ *are the conjugates of* α.

Proof. Since $M(\alpha) = |\alpha_1\alpha_2\cdots\alpha_n| = k$, there must be some i such that $|\alpha_i| \geqslant k$. Without loss of generality, we assume

$$|\alpha_1| = |\bar{\alpha}| = \max_{1\leqslant i\leqslant n}|\alpha_i| \geqslant k. \tag{3}$$

In what follows, we consider two situations separately: (a) $|\alpha_2\cdots\alpha_n| \geqslant 1$, and (b) $|\alpha_2\cdots\alpha_n| < 1$.

As for the case (a), we obtain from (3) that

$$|\alpha_1\alpha_2\cdots\alpha_n| \geqslant k > k-1 \in \mathbb{N}.$$

Note that α is not a root of unity by our assumption. Therefore, by Theorem 1 we have

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln k}{n}$$

as desired.

As for the case (b), we denote by

$$|\alpha_2\cdots\alpha_n| = 1-\varepsilon,$$

for $\varepsilon \in (0,1)$. Via (3) and the assumption $M(\alpha) = k$, we obtain

$$|\bar{\alpha}| = \frac{k}{|\alpha_2\cdots\alpha_n|} = \frac{k}{1-\varepsilon}. \tag{4}$$

On the other hand, since $n \geqslant \frac{1-\varepsilon}{\varepsilon}\ln k$, we have

$$\frac{k}{1-\varepsilon} - \frac{k-\varepsilon}{1-\varepsilon} = \frac{\varepsilon}{1-\varepsilon} \geqslant \frac{\ln k}{n},$$

and then

$$\frac{k}{1-\varepsilon} \geqslant 1 + \frac{\ln k}{n}. \tag{5}$$

Combining (4) with (5) yields

$$|\bar{\alpha}| \geqslant 1 + \frac{\ln k}{n},$$

which finishes the proof of Theorem 2. □

We remark that in the above result we do not consider the boundary situation $M(\alpha) = 1$, which has been treated in Theorem 2 in the work [9].

Acknowledgement

The author is grateful to the reviewers whose comments helped improve the paper.

REFERENCES

[1] P. E. BLANKSBY, H. L. MONTGOMERY, *Algebraic integers near the unit circle*, Acta. Arith., 18(1971) 355–369.

[2] D. W. BOYD, *The maximal modulus of an algebraic integer*, Math. Comp., 45(1985) 243–249.

[3] D. C. CANTOR, E. G. STRAUS, *On a conjecture of D. H. Lehmer*, Math. Comp., 42(1982) 97–100.

[4] E. DOBROWOLSKI, *On the maximal modulus of conjugates of an algebraic integer*, Bull. Acad. Polon. Sci. Ser. Sci. Math. Astronom. Phys., 26(1978) 291–292.

[5] E. DOBROWOLSKI, *On a question of Lehmer and the number of irreducible factors of a polynomial*, *Acta. Arith.*, 34(1979) 391–401.

[6] A. DUBICKAS, *On a conjecture of A. Schinzel and H. Zassenhaus*, *Acta. Arith.*, 63(1993) 15–20.

[7] D. S. DUMMIT, R.' M. FOOTE, *Abstract Algebra*, Wiley, New York, 2004.

[8] A. GRYTCZUK, M. SZAŁKOWSKI, *Spectral properties of some matrices*, Acta. Acad. Pead. Agriensis Sectio Math., 20(1991) 43–50.

[9] A. GRYTCZUK, I. KURZYDŁO, *On some application of the spectral properties of the matrices*, Notes Number Theory Discrete Math., 17(2011) 12–17.

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

[11] R. LOUBOUTIN, *Sur la mesure de Mahler d'un nombre algébrique*, C. R. Acad. Sci. Paris, 296(1983) 707–708.

[12] E. M. MATVEEV, *On the cardinality of algebraic integers*, Mat. Zametki, 49(1991) 152–154.

[13] W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers PWN, Warszawa, 1990.

[14] G. RHIN, Q. WU, *On the smallest value of the maximal modulus of an algebraic integer*, *Math. Comp.*, 76(2007) 1025–1038.

[15] A. SCHINZEL, H. ZASSENHAUS, *A refinement of two theorems of Kronecker*, Michigan Math. J., 12(1965) 81–85.

[16] C. L. STEWART, *Algebraic integers whose conjugates lie near the unit circle*, Bull. Soc. Math. France, 196(1978) 169–176.

(Received October 12, 2011)

Yilun Shang
Institute for Cyber Security
University of Texas at San Antonio
San Antonio, Texas 78249
USA
e-mail: shylmath@hotmail.com