ELEMENTARY AND ANALYTIC THEORY OF NUMBERS
BANACH CENTER PUBLICATIONS, VOLUME 17
PWN-POLISH SCIENTIFIC PUBLISHERS
WARSAW 1985

GREATEST DISTANCE BETWEEN ZEROS OF INTEGRAL POLYNOMIALS

P. E. BLANKSBY

Department of Pure Mathematics, University of Adelaide
Adelaide, 5001, South Australia

1. Introduction

Suppose that f is a polynomial given by

$$f(x) = qx^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \tag{1}$$

where a_j $(1 \leqslant j \leqslant n)$, q are rational integers, $q > 0$. For the purposes of this paper we will assume f to be irreducible over the rationals and primitive. We will denote the zeros of f by $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$, which will therefore be distinct. Of course the $\alpha_1, \alpha_2, \ldots, \alpha_n$ form a conjugate set of algebraic numbers, and in the special case that $q = 1$, a conjugate set of algebraic integers. It will be the case $q = 1$ that will mainly concern us.

The following proposition is a well-known elementary fact about conjugate sets of algebraic numbers.

PROPOSITION. *For given positive integers n, q and a given bounded subset E of the complex plane there are only finitely many (in terms of n, q and E) sets of conjugate algebraic numbers of degree n and leading coefficient q contained in the set E.*

The proof is immediate since if B is such that $|z| \leqslant B$ for all $z \in E$ and $\alpha_j \in E$ $(1 \leqslant j \leqslant n)$, then $|a_j/q|$, being the modulus of the jth elementary symmetric function of $\alpha_1, \alpha_2, \ldots, \alpha_n$, is bounded in terms of n and B. Thus there are only finitely many possibilities for each of the coefficients of the minimal polynomial (1) for such α.

In all but the final part of this paper, we will suppose $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ to be a set of conjugate algebraic integers of degree n, so that $q = 1$. If $r > 0$ we will denote

$$S_r = \{z\colon |z| \leqslant r\}.$$

For a given degree n and for specific small r, we may wish to determine which conjugate sets of algebraic integers of degree n are contained in the disc S_r.

For $0 < r < 1$ the only such conjugate set is $\alpha = 0$. However, S_1 contains additionally all conjugate sets of roots of unity, but no further complete conjugate sets. This is a classical theorem of Kronecker, and is usually stated as follows:

THEOREM 1 (Kronecker [12]). *Let α be an algebraic integer of degree n with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$. If α is non-zero and not a root of unity, then*

$$\max_{1 \leqslant j \leqslant n} |\alpha_j| > 1. \tag{2}$$

The result follows from the proposition after noting a couple of algebraic facts. For a positive integer k, the conjugates of α^k are α_j^k $(1 \leqslant j \leqslant n)$, and the degree of α^k is a factor of n. Thus if all the conjugates of α belong to S_1, so too do all the conjugates of α^k. The proposition then implies the existence of positive integers k and m with $k \neq m$ and such that $\alpha^k = \alpha^m$. It follows that $\alpha = 0$ or α is a root of unity.

Kronecker's theorem suggests the determination, for a given n, of the least $r > 1$ such that S_r first contains a complete conjugate set of algebraic integers of degree n which are not roots of unity and not zero. Applying the proposition to S_2, say, we deduce the existence of a positive function $g(n)$ which strengthens Kronecker's theorem by replacing the inequality (2) with

$$\max_{1 \leqslant j \leqslant n} |\alpha_j| \geqslant 1 + g(n). \tag{3}$$

We define $1 + g(n)$ to be the least value (of the finitely many possibilities) of $\max_{1 \leqslant j \leqslant n} |\alpha_j|$ in the range

$$1 < \max_{1 \leqslant j \leqslant n} |\alpha_j| \leqslant 2.$$

Schinzel and Zassenhaus [25] were the first to propose the evaluation (or estimation) of this function $g(n)$. By considering the zeros of $x^2 - 2$ we have that

$$g(n) \leqslant 2^{1/n} - 1 = O(1/n) \quad \text{as } n \to \infty.$$

Dobrowolski [4] has shown that for every $\varepsilon > 0$ there exists $n_0(\varepsilon)$ such that for $n > n_0(\varepsilon)$

$$g(n) > \frac{2-\varepsilon}{n} \left(\frac{\log \log n}{\log n} \right)^3.$$

This has recently been slightly improved by replacing $2-\varepsilon$ with $4-\varepsilon$ (see Rausch [18], Cantor and Straus [3]).

The problem of finding $g(n)$ is closely connected with the problem of finding the greatest positive function $h(n)$ which strengthens Kronecker's theorem by replacing the inequality (2) with

$$\prod_{j=1}^{n} \max\{1, |\alpha_j|\} \geqslant 1+h(n). \tag{4}$$

It follows that $h(n) = O(1)$ as $n \to \infty$, and D. H. Lehmer [13] has asked whether $h(n)$ is bounded below by a positive constant independent of n. Towards answering this question it has been shown that for every $\varepsilon > 0$ there exists $n_1(\varepsilon)$ such that for $n > n_1(\varepsilon)$

$$h(n) > (2-\varepsilon)\left(\frac{\log\log n}{\log n}\right)^3$$

(see Dobrowolski [4], Rausch [18], Cantor and Straus [3]).

These two problems have attracted considerable attention over the past decade or so. I have discussed them here by way of introduction to the analogous question for discs which are centred at an arbitrary point a on the real axis. Of course if a is a rational integer, we need only consider $\alpha - a$ and we are again in the case of discs centred the origin. Hence the new interest lies in the case when a is not a rational integer. That the answer is not the same is seen immediately by considering the example $a = -1/2$ and α satisfying $\alpha^2+\alpha+1 = 0$ (that is, α is a primitive cube root of unity). Then α and its conjugate lie in the closed disc with centre $-1/2$ and radius $\frac{1}{2}\sqrt{3}$.

In the context of this problem it seems natural to consider the following definition (see Yaglom and Boltyanskiĭ [27]).

Definition. If α is an algebraic integer of degree n with conjugates $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$, the *circumcircle of* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ (or of α) is the circle of least diameter enclosing the points $\alpha_1, \alpha_2, \ldots, \alpha_n$. The *circumdiameter of* α is the diameter of the circumcircle of α and will be denoted by $D(\alpha)$.

That the circumcircle of α exists and is unique is clear. It is easily seen that if $n \geqslant 2$, the circumcircle of α contains at least two conjugates of α. Also if $n \geqslant 3$ and if no two conjugates of α are placed diametrically opposed on the circumcircle, then the circumcircle must contain at least three conjugates of α.

In addition to the circumdiameter we will consider the usual (Euclidean) diameter of the set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$.

Definition. The *diameter of* α is defined and denoted

$$\operatorname{diam}(\alpha) = \max_{i,j} |\alpha_i - \alpha_j|.$$

We have the following classical result of Jung relating the two diameters (see Yaglom and Boltyanskiĭ [27])

$$\tfrac{1}{2}\sqrt{3}\,D(\alpha) \leqslant \operatorname{diam}(\alpha) \leqslant D(\alpha). \tag{5}$$

It is easy to see by example that these inequalities cannot be improved in general.

For the remainder of this paper we will consistently assume that α has degree at least 2, so that $D(\alpha)$ and $\operatorname{diam}(\alpha)$ are both positive. If we know the existence of a positive constant b for which $D(\alpha) > b$ for all such α, then it would follow that any disc with real centre and radius at most $\frac{1}{2}b$ contains no conjugate sets of algebraic integers, except perhaps rational integers.

That such positive b exist follows immediately by considering the discriminant of $\alpha_1, \alpha_2, \ldots, \alpha_n$. If we write d_K for the discriminant of the field K generated by α over the rationals, then

$$|d_K| \leqslant \prod_{i \neq j} |\alpha_i - \alpha_j| \leqslant \{\operatorname{diam}(\alpha)\}^{n(n-1)}.$$

Since $|d_K| > 1$, we deduce (using (5))

$$D(\alpha) \geqslant \operatorname{diam}(\alpha) > 1.$$

We proceed to describe known results of this kind.

2. Earlier results

Favard [5], [6], [7] seems to have been the first to study general lower bounds for the diameters of α. We write

$$M(n) = \min \operatorname{diam}(\alpha),$$

where the minimum is taken over all algebraic integers of degree n. Favard showed that $M(2) = \sqrt{3}$, and if β is the real zero of $x^3 - x - 1$, then

$$M(3) = \left(\frac{3}{\beta^2} + \frac{2}{\beta}\right)^{1/2} = 1.794\ldots$$

He examined the diameters of quadratic and cubic α in some detail, and determined some other α with $\operatorname{diam}(\alpha) \leqslant 2$. In general, he showed that for $n \geqslant 2$

$$M(n) \geqslant \left(\frac{3n}{2(n-1)}\right)^{1/2} > \left(\frac{3}{2}\right)^{1/2}. \tag{6}$$

In the context of this paper we will use the following terminology.

DEFINITION. If α and β are algebraic integers, we say that α *is equivalent* *to* β if $\alpha = \pm\beta'+k$ for some conjugate β' of β, and some rational integer k.

It follows that for equivalent α and β, $\operatorname{diam}(\alpha) = \operatorname{diam}(\beta)$ and $D(\alpha) = D(\beta)$.

In the special case when α is totally real we have $\operatorname{diam}(\alpha) = D(\beta)$. Pólya has earlier shown (see Schur [26]) that for any $\varepsilon > 0$ there exists only a finite number of equivalence classes of totally real algebraic integers with diameter at most $4-\varepsilon$. In fact, it can be shown from his proof that for $n > 2$, $\operatorname{diam}(\alpha) > 4\left(1-\dfrac{\log n}{n}\right)$ (see McAuley [17]).

Somewhat later, R. M. Robinson took up this question of the diameter (span) of totally real algebraic integers. He showed [24] that for such α with $n \geqslant 2$

$$\operatorname{diam}(\alpha) \geqslant \sqrt{5},$$

with equality if and only if α is equivalent to $\frac{1}{2}(1+\sqrt{5})$. If $n \geqslant 3$ then

$$\operatorname{diam}(\alpha) > 3,$$

and he determined [24] all totally real α with diameter at most 3. This work was recently extended by McAuley [17] who determined the 13 equivalence classes of such α for which

$$\operatorname{diam}(\alpha) \leqslant 3.7336$$

(see also Robinson [21]).

In [19], [22] Robinson determined all intervals which can be approximated both by intervals containing infinitely many conjugate sets of totally real algebraic units, and by intervals containing only finitely many such sets.

We will proceed to describe more recent results of Lloyd-Smith, McAuley and the author.

3. Recent results

In 1980 Lloyd-Smith [14], [2] obtained the following improvements of Favard's result (6).

THEOREM 2 (Lloyd-Smith). *Let α be an algebraic integer of degree $n \geqslant 2$.*

(i) $D(\alpha) \geqslant \sqrt{3}$, *with equality if and only if α is equivalent to a primitive cube root of unity.*

(ii) *If* $\sum_{j=1}^{n} \alpha_j \equiv 0 (\operatorname{mod} n)$, *then* $D(\alpha) \geqslant 2$.

Moreover, in this case equality holds if and only if α is equivalent to a primitive m-th root of unity with m not square-free.

Using the inequality (5) we have

Corollary. *Under the hypothesis of the theorem we have*
(i) $\operatorname{diam}(\alpha) > 3/2$.
(ii) *If* $\sum_{j=1}^{n} \alpha_j \equiv 0 (\operatorname{mod} n)$, *then* $\operatorname{diam}(\alpha) > \sqrt{3}$.

Lloyd-Smith's methods were surprisingly simple, and involved estimating the sum $\sum_{j=1}^{n} |\alpha_j - a|^2$, where a is the centre of the circumcircle of α. The lower bound on $\operatorname{diam}(\alpha)$ given by the Corollary (i) is not best possible, and was improved by McAuley [17] to

$$\operatorname{diam}(\alpha) \geqslant 1.659.$$

The following is a rather plausible conjecture.

Conjecture. *For* $n \geqslant 2$, $\operatorname{diam}(\alpha) \geqslant \sqrt{3}$, *with equality if and only if* α *is equivalent to a primitive cube root of unity.*

Lloyd-Smith has proved a number of results which give support to this conjecture.

Theorem 3 (Lloyd-Smith [14], [2]). *If* α *is equivalent to a reciprocal algebraic integer* β *of degree at least* 2, *then*

$$\operatorname{diam}(\alpha) \geqslant \sqrt{3}.$$

Moreover, for reciprocal α, *equality holds if and only if* α *is a primitive cube or sixth root of unity.*

(An algebraic integer β is said to be *reciprocal* if β^{-1} is a conjugate of β.)

Theorem 4 (Lloyd-Smith [14], [2]). *Let* ζ *be a primitive m-th root of unity (of degree* $\phi(m)$*). If* $m = 3, 6$ *then*

$$D(\zeta) = \operatorname{diam}(\zeta) = \sqrt{3}.$$

If $m \neq 3, 6$ *then*

$$D(\zeta) = 2$$

and

$$\operatorname{diam}(\zeta) = \begin{cases} 2 & \text{if } m \equiv 0 (\operatorname{mod} 4), \\ 2 \sin \dfrac{2\pi}{m} \left[\dfrac{m}{4}\right] & \text{if } m \equiv 2 (\operatorname{mod} 4), \\ 2 \sin \dfrac{\pi}{m} \left[\dfrac{m}{2}\right] & \text{if } m \equiv 1, 3 (\operatorname{mod} 4), \end{cases}$$

(where [ ] *is the integer part function).*

This result and the work of Robinson suggests an investigation of diameters for cyclotomic and totally real fields. More generally,

DEFINITION. A number field is said to be a *CM-field* if it is a totally imaginary quadratic extension of a totally real field.

A number field is called a *J-field* if it is either totally real or is *CM*-field.

See Győry [11], Blanksby and Loxton [1], and the works referred to in these papers for a discussion of these fields.

THEOREM 5 (Lloyd-Smith [14], [15]). *Let α be an algebraic integer of degree at least 2 and belonging to a J-field. Then*

$$D(\alpha) \geqslant 4\cos\frac{\pi}{9} - 1 = 2.758\ldots,$$

except in the following cases:

(i) α *is equivalent to a root of unity* (see Theorem 4);

(ii) α *is equivalent to* $\frac{1}{2}(1+\sqrt{5})$, *when* $D(\alpha) = \sqrt{5}$;

(iii) α *is equivalent to* $\frac{1}{2}(1+\sqrt{-7})$, *when* $D(\alpha) = \sqrt{7}$.

Using the inequality (5), we get the immediate

COROLLARY. *Under the hypothesis of the theorem,*

$$\operatorname{diam}(\alpha) \geqslant \frac{\sqrt{3}}{2}\left(4\cos\frac{\pi}{9} - 1\right) = 2.389\ldots,$$

except in the following cases:

(i) α *is equivalent to a root of unity* (see Theorem 4);

(ii) α *is equivalent to* $\frac{1}{2}(1+\sqrt{5})$, *when* $\operatorname{diam}(\alpha) = \sqrt{5}$.

Extending the work of Favard, Lloyd-Smith determined all algebraic integers α of degrees 2, 3, 4 and 5 for which $\operatorname{diam}(\alpha) \leqslant 2$, and those for which $D(\alpha) \leqslant 2$. These results are tabulated in [14] and [16]. There are respectively 2, 2, 5 and 2 classes for which $\operatorname{diam}(\alpha) \leqslant 2$, and respectively 2, 1, 4 and 0 classes for which $D(\alpha) \leqslant 2$. It follows from his tables that

$$M(2) = \sqrt{3}, \quad M(3) = 1.794\ldots, \quad M(4) = 1.898\ldots, \quad M(5) = 1.991\ldots$$

For a compact infinite subset S of the complex plane, Fekete [8], [9], [10] introduced the concept of the *transfinite diameter* d_∞ of S,

$$d_\infty(S) = \lim_{n\to\infty} \Big\{ \max_{z_1, z_2, \ldots, z_n \in S} \prod_{i \neq j} |z_i - z_j| \Big\}^{1/n(n-1)}.$$

If S is a disc, then $d_\infty(S)$ is the radius of the disc. Among other results, Fekete showed that if S is compact and with $d_\infty(S) < 1$, then there are only a finite number of conjugate sets of algebraic integers lying in S (see also Robinson [19], [20], [23]). This result of Fekete can be used to deduce that for every $\varepsilon > 0$, there are only finitely many equivalence classes of algebraic integers for which $D(\alpha) < 2-\varepsilon$.

As pointed out by McAuley [17], [2], this result can be given a quantitative formulation by a simple argument. If, as before, we write d_K for the discriminant of the field K generated by α over the rationals, and a for the centre of the circumcircle of α, then

$$|d_K| \leqslant \prod_{i \neq j} |\alpha_i - \alpha_j| = \prod_{i \neq j} |(\alpha_i - a) - (\alpha_j - a)| = \prod_{i \neq j} \varrho \, |z_i - z_j|,$$

where $\varrho = \varrho(\alpha) = \frac{1}{2} D(\alpha)$ and $z_j = \varrho^{-1}(\alpha_j - a)$ $(1 \leqslant j \leqslant n)$. It follows that the unit circle with centre at the origin is the circumcircle of $z_1, z_2, \ldots, z_n$. By a well-known result (for example, by using Hadamard's inequality on the corresponding Vandermonde determinant),

$$\prod_{i \neq j} |z_i - z_j| \leqslant n^n.$$

Thus

$$D(\alpha) \geqslant 2 \{|d_K|/n^n\}^{1/n(n-1)},$$

and we obtain the straightforward consequence.

Theorem 6 (McAuley [17], [2]). *If α is an algebraic integer of degree $n \geqslant 2$, then*

$$D(\alpha) \geqslant 2\left(1 - \frac{\log n}{n}\right),$$

and

$$\operatorname{diam}(\alpha) \geqslant \sqrt{3}\left(1 - \frac{\log n}{n}\right).$$

The argument above can be refined somewhat, and the following result by Blanksby, Lloyd-Smith and McAuley [2] goes some way towards settling the conjecture mentioned earlier.

Theorem 7. *There exist positive absolute constants c_0 and n_2 such that for all algebraic integers α of degree at least n_2,*

$$\operatorname{diam}(\alpha) > \sqrt{3} + c_0.$$

The method yields explicit values for c_0 and n_2. At the time of writing this account the author is optimistic that the conjecture is within reach, and the details and ideas will form the content of a forthcoming paper.

There are a number of other problems about diameters that can be posed. For example:

(1) Is there an n_3 such that $D(\alpha) \geqslant 2$ for all algebraic integers α of

degree at least n_3? If so, can n_3 be taken to be 5? (See Lloyd-Smith [14].)

(2) Is it true that for every $\varepsilon > 0$ there is an $n_4 = n_4(\varepsilon)$ such that $\operatorname{diam}(\alpha) \geqslant 2-\varepsilon$ for all algebraic integers of degree exceeding n_4?

(3) Favard asked whether $M(n) < 2$ for every $n \geqslant 2$.

4. Diameters of algebraic numbers

In conclusion, we note that if α is an algebraic number whose leading coefficient in the minimal polynomial (1) is q, then $\operatorname{diam}(\alpha)$ may be arbitrarily small when q is sufficiently large. For example, if α is a zero of $qx^2 - -(2q+1)x+q$, then

$$D(\alpha) = \operatorname{diam}(\alpha) = O(1/\sqrt{q}) \quad \text{as } q \to \infty.$$

If q is held fixed, Fekete also proved a result about d_∞ analogous to the one quoted earlier. This suggests a generalization of Theorem 6, and using the method of the theorem it can be shown that if α has degree $n \geqslant 2$ and leading coefficient q then

$$D(\alpha) \geqslant 2\left(1 - \frac{\log(nq^2)}{n-1}\right),$$

and so

$$\operatorname{diam}(\alpha) \geqslant \sqrt{3}\left(1 - \frac{\log(nq^2)}{n-1}\right).$$

Indeed the result of Theorem 7 generalizes in the following way:

THEOREM 8. *There exists a positive absolute constant c_1 and a number $n_5 = n_5(q)$ such that for all algebraic numbers α with leading coefficient q and degree at least n_5,*

$$\operatorname{diam}(\alpha) > \sqrt{3} + c_1.$$

References

[1] P. E. Blanksby and J. H. Loxton, *A note on the characterization of CM-fields*, J. Austral. Math. Soc. (Series A) 26 (1978), 26–30.

[2] P. E. Blanksby, C. W. Lloyd-Smith and M. J. McAuley, *On diameters of algebraic integers* (to appear).

[3] D. G. Cantor and E. G. Straus, *On a conjecture of D. H. Lehmer*, Acta Arith. 42 (1982), 97–100; Correction, ibid. 42 (1983), 327.

[4] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, ibid. 34 (1979), 391–401.

[5] J. Favard, *Sur les nombres algébriques*, C. R. Acad. Sci. Paris 186 (1928), 1181–1182.
[6] –, *Sur les formes décomposables et les nombres algébriques*, Bull. Soc. Math. France 57 (1929), 50–71.
[7] –, *Sur les nombres algébriques*, Mathematica 4 (1930), 109–113.
[8] M. Fekete, *Über die Verteilung der Wurzeln bei gewissen, algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. 17 (1923), 228–249.
[9] –, *Über den transfiniten Durchmesser ebener Punktmengen*, ibid. 32 (1930), 108–114, 215–221.
[10] M. Fekete and G. Szegö, *On algebraic equations with integral coefficients whose roots belong to a given point set*, ibid. 63 (1955), 158–172.
[11] K. Györy, *Sur une classe des corps des nombres algébriques et ses applications*, Publ. Math., Debrecen 22 (1975), 151–175.
[12] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Koefficienten*, J. Reine Angew. Math. 53 (1857), 173–175.
[13] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. Math. (2) 34 (1933), 461–479.
[14] C. W. Lloyd-Smith, *Problems on the distribution of conjugates of algebraic numbers*, Ph. D. Thesis, University of Adelaide, 1980.
[15] –, *On minimal diameters of algebraic integers in J-fields* (to appear).
[16] –, *On a problem of Favard concerning algebraic integers*, Bull. Austral. Math. Soc. 29 (1984), 111–121.
[17] M. J. McAuley, *Topics in J-fields and a diameter problem*, M. Sc. Thesis, University of Adelaide, 1981.
[18] U. Rausch, *On a theorem of Dobrowolski* (to appear).
[19] R. M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*, Studies in Mathematical Analysis and Related Topics: Essays in Honor of George Pólya, Stanford 1962, 305–315.
[20] –, *Conjugate algebraic integers in real point sets*, Math. Z. 84 (1964), 415–427.
[21] –, *Algebraic equations with span less than* 4, Math. Comp. 18 (1964), 547–559.
[22] –, *Intervals containing infinitely many sets of conjugate algebraic units*, Ann. Math. (2) 80 (1964), 411–428.
[23] –, *On the transfinite diameter of some related sets*, Math. Z. 108 (1969), 377–380.
[24] –, *Conjugate algebraic integers on a circle*, ibid. 110 (1969), 41–51.
[25] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Mich. Math. J. 12 (1965), 81–84.
[26] I. Schur, *Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten*, Math. Z. 1 (1918), 377–402.
[27] I. M. Yaglom and V. G. Boltyanskiĭ, *Convex Figures* (translated by Paul J. Kelly and Lewis F. Walton), Holt, Rinehart and Winston, New York 1961.

Presented to the Semester
Elementary and Analytic Theory of Numbers
September 1–November 13, 1982