

ON A PROBLEM OF FAVARD  
CONCERNING ALGEBRAIC INTEGERS

C. W. LLOYD-SMITH

Let  $\alpha$  be an algebraic integer of degree  $n > 1$  with conjugates  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ . Let  $D(\alpha)$  denote the diameter of  $\{\alpha_1, \dots, \alpha_n\}$  and  $\text{diam}(\alpha) = \max_{i,j} |\alpha_i - \alpha_j|$ . In 1929 Favard showed that

$\text{diam}(\alpha) \geq \sqrt{3/2}$  and that, when  $n = 2$  or  $3$ , the minimal values of  $\text{diam}(\alpha)$  are less than  $2$ . The author shows that  $\text{diam}(\alpha) > \frac{3}{2}$  and  $D(\alpha) > \sqrt{3}$ . He also finds all algebraic integers  $\alpha$  with  $\text{diam}(\alpha) \leq 2$  when  $n \leq 5$ . Similar results are found for  $D(\alpha)$  and, in particular,  $D(\alpha) > 2$  when  $n = 5$ .

1. Introduction

Let  $\alpha$  be an algebraic integer of degree  $n \geq 2$  with conjugates denoted by  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ . The *diameter* of  $\alpha$  is defined by

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

the maximum distance between any two of its conjugates. Favard [1], [2],

---

Received 17 February 1984. I am grateful to one of the examiners of my thesis [5], who suggested the greatly improved technique for finding the inequivalent algebraic integers with diameter less than some prescribed bound. I acknowledge the support of a Commonwealth Postgraduate Research Award while the research at the University of Adelaide was done. I would like to thank my supervisor, Dr. P. E. Blanksby, for his encouragement and advice. I am also grateful to the Australian Bureau of Statistics for permission to use their Cyber 72 computer for the calculations described in this paper.

[3] showed that

$$(1.1) \quad \text{diam}(\alpha) \geq \sqrt{\frac{3}{2}}.$$

On the other hand, there are infinitely many  $n$  for which there are algebraic integers  $\alpha$  of degree  $n$  such that

$$(1.2) \quad \text{diam}(\alpha) \leq 2.$$

This is clear because (1.2) is satisfied if  $\alpha$  is a root of unity. However it is not known whether there are algebraic integers  $\alpha$  satisfying (1.2) for every  $n \geq 2$ . Note that the Euler  $\phi$ -function does not take every positive integer value  $n$ .

In this paper we show that (1.1) can be improved to give

$$(1.3) \quad \text{diam}(\alpha) > \frac{3}{2}.$$

In this paper, algebraic integers  $\alpha, \alpha'$  of degree  $n$  are said to be *equivalent* if the sets of differences  $\{\alpha_i - \alpha_j\}, \{\alpha'_i - \alpha'_j\}$  coincide. If  $\alpha$  and  $\alpha'$  are equivalent, it is clear that some conjugate of  $\alpha'$  is of the form  $\pm \alpha + k$  where  $k$  is a rational integer. It is fairly easy to see that for each  $n$  there are only finitely many inequivalent  $\alpha$  with  $\text{diam}(\alpha)$  not exceeding some prescribed bound. In this paper we also list all inequivalent  $\alpha$  with  $\text{diam}(\alpha) \leq 2$  and degree  $n \leq 5$ .

Favard [2] noted that if  $\alpha$  is totally real, then  $\text{diam}(\alpha) > 2$  and, indeed, Robinson [6] proved that in this case,  $\text{diam}(\alpha) \geq \sqrt{5}$  and even  $\text{diam}(\alpha) > 3$  if  $n \geq 3$ . This result also follows from work of the author [5] on algebraic integers in  $\mathcal{J}$ -fields.

Favard [2] found that the minimal values of  $\text{diam}(\alpha)$  when  $n = 2$  or 3 are less than 2. In [3], he observed that for those  $n$ , the smallest value of  $\text{diam}(\alpha)$  corresponds to an  $\alpha$  which generates a field whose discriminant is of least absolute value for that degree.<sup>1</sup>

---

<sup>1</sup>The author [5] stated incorrectly that Favard found all inequivalent  $\alpha$  with  $\text{diam}(\alpha) \leq 2$  when  $n = 2$  or 3. However, this readily follows from the work of Favard [2].

The author [5] found all inequivalent  $\alpha$  such that  $\text{diam}(\alpha) \leq 2$  when  $n = 4$  or  $5$ . The arguments are very complicated and yielded a total of 104,472 polynomials which had to be tested on the Cyber 173 computer at the University of Adelaide. In this paper we present a simpler technique, which serves to handle all the above cases uniformly, and yields all inequivalent  $\alpha$  with  $\text{diam}(\alpha) \leq 2$ . The results are shown in Table 1.

We also define the *circumdiameter* of  $\alpha$  to be the diameter of the smallest circle enclosing all the conjugates of  $\alpha$ , including  $\alpha$  itself. It is denoted by  $D(\alpha)$ . The circle just alluded to will be called the *circumcircle* of  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  and its centre is the *circumcentre* of  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ . Favard [3] found all inequivalent  $\alpha$  of degrees 2 and 3 satisfying  $D(\alpha) \leq 2$ . The author [5] extended this work to degrees 4 and 5. The results are shown in Table 2. It turns out that all algebraic integers of degree 5 have circumdiameter greater than 2.

The diameter and circumdiameter of  $\alpha$  are connected by the following inequality of Jung [7], p. 17,

$$(1.4) \quad \text{diam}(\alpha) \leq D(\alpha) \leq \frac{2}{\sqrt{3}} \text{diam}(\alpha).$$

In general, neither inequality in (1.4) can be improved. To see this, it suffices to take  $\alpha = i$  and  $\alpha = \sqrt[3]{2}$  in turn.

The main result of this paper is the following

**THEOREM.** *Let  $\alpha$  be an algebraic integer of degree  $n \geq 2$  with diameter  $d$  and circumdiameter  $D$ . Then we have:*

1.  $D \geq \sqrt{3}$  with equality if and only if  $\alpha$  is equivalent to a primitive cube root of unity.
2. If  $\alpha_1 + \dots + \alpha_n \equiv 0 \pmod{n}$  then  $D \geq 2$ . Moreover,  $D = 2$  if and only if  $\alpha$  is equivalent to a primitive  $m^{\text{th}}$  root of unity with  $m$  not squarefree.

The foregoing Theorem yields the following

**COROLLARY.** *In the notation of the Theorem we have*

1.  $d > \frac{3}{2}$ .
2. If  $\alpha_1 + \dots + \alpha_n \equiv 0 \pmod{n}$ , then  $d > \sqrt{3}$ .

2. The proofs

Proof of the Theorem. Let  $f(x) = x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$  be the minimal polynomial of  $\alpha$ . Then

$$(2.1) \quad -a_1 = \sum_{j=1}^n \alpha_j,$$

and, by replacing  $\alpha$  with an equivalent algebraic integer if necessary, we lose no generality in supposing that  $0 \leq a_1 \leq [n/2]$ . As usual,  $[x]$  denotes the greatest integer not exceeding  $x$ . Let  $\beta$  be the circumcentre of  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ . Then we have for  $j = 1, 2, \dots, n$ ,

$$(2.2) \quad |\beta - \alpha_j|^2 \leq \frac{D^2}{4}.$$

By symmetry  $\beta$  is necessarily real.

By the arithmetic-geometric mean inequality we have

$$(2.3) \quad \frac{1}{n} \sum_{j=1}^n |\alpha_j|^2 \geq \frac{n}{\prod_{j=1}^n |\alpha_j|^{2/n}} = |\alpha_n|^{2/n} \geq 1.$$

with equality if and only if  $|\alpha_1| = |\alpha_2| = \dots = |\alpha_n| = 1$ . From (2.1), (2.2) and (2.3) we get

$$(2.4) \quad \left\{ \begin{aligned} \frac{D^2}{4} &\geq \frac{1}{n} \sum_{j=1}^n |\beta - \alpha_j|^2 \geq \frac{1}{n} \sum_{j=1}^n |\alpha_j|^2 + \beta^2 + \frac{2\beta a_1}{n} \\ &\geq \frac{1}{n} \sum_{j=1}^n |\alpha_j|^2 + \beta^2 - |\beta| \\ &\geq 1 + (|\beta| - \frac{1}{2})^2 - \frac{1}{4} \\ &\geq \frac{3}{4}. \end{aligned} \right.$$

Hence  $D \geq \sqrt{3}$  as asserted.

Moreover,  $D^2 = 3$  only if  $|\alpha_1| = |\alpha_2| = \dots = |\alpha_n| = 1$  and  $|\beta| = \frac{1}{2}$ . By (2.2), (2.3) and (2.4),  $D^2 = 3$  implies that

$$|\beta - \alpha_j| = \frac{\sqrt{3}}{2} \text{ for } j = 1, 2, \dots, n.$$

Since the circles  $|z - \beta| = \frac{\sqrt{3}}{2}$  and  $|z| = 1$  intersect in only two points,  $\alpha$  is of degree at most 2. Since the conjugates of  $\alpha$  all lie on the unit circle, it is readily seen that  $\alpha$  must be a primitive cube or sixth root of unity. This proves the first part of the Theorem.

For the proof of the second part of the Theorem, we lose no generality in assuming that  $\alpha_1 = 0$ . From (2.2) and (2.3) we get

$$(2.5) \quad \frac{D^2}{4} \geq 1 + \beta^2 \geq 1.$$

Hence  $D \geq 2$ . From (2.2), (2.3), (2.4) and (2.5) it follows that  $D = 2$  if and only if all the conjugates of  $\alpha$  lie on the unit circle. A result of Kronecker [4] implies that  $\alpha$  must be a root of unity.

Let  $m$  be the integer such that  $\alpha$  is a primitive  $m^{\text{th}}$  root of unity. It is well known that  $\alpha$  has trace equal to  $\mu(m)$ . As usual,  $\mu(m)$  denotes the Möbius function. Thus  $\alpha_1 = -\mu(m)$ . From the definition of the Möbius function, it follows that  $m$  is not squarefree since  $\alpha_1 = 0$ . This completes the proof of the Theorem.

Proof of the Corollary. From (1.4) and the first part of the Theorem, it follows that  $d \geq \frac{3}{2}$  and if  $D > \sqrt{3}$  then  $d > \frac{3}{2}$ . If  $D = \sqrt{3}$  then  $\alpha$  is necessarily equivalent to a primitive cube root of unity. So  $d = \sqrt{3}$  in this case. Hence we always have  $d > \frac{3}{2}$ .

For the proof of the second part of the Corollary, we lose no generality in assuming that  $\alpha_1 = 0$ . If  $D > 2$ , the result is immediate. If  $D = 2$ , then  $\alpha$  is a root of unity by the second part of the Theorem. If  $\alpha$  is a primitive  $m^{\text{th}}$  root of unity ( $m \geq 3$ ), it is readily shown that

$$\text{diam}(\alpha) = \begin{cases} 2 \sin \frac{\pi}{m} [m/2] & \text{if } 2 \nmid m \\ 2 \sin \frac{2\pi}{m} [m/4] & \text{if } 2|m, 4 \nmid m \\ 4 & \text{if } 4|m. \end{cases}$$

Since  $\alpha$  has zero trace, we know that  $\alpha$  cannot be a primitive cube or sixth root of unity. Applying the above formulae then shows that  $d > \sqrt{3}$ . Thus the Corollary is completely proved.

3. Determination of inequivalent  $\alpha$  with  $\text{diam}(\alpha) \leq 2$ .

We retain all the notations of the previous section. In particular, we lose no generality in supposing that  $0 \leq a_1 \leq [n/2]$ .

In this section we derive some useful bounds on the coefficients of  $f(x)$  in terms of  $d = \text{diam}(\alpha)$ .

By the arithmetic-geometric mean inequality, we have

$$(3.1) \quad \frac{1}{n} \sum_{j=1}^n |a_j|^2 \geq |a_n|^{2/n}.$$

Let  $\beta$  be the circumcentre of  $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$  as before.

By (1.4) we have

$$(3.2) \quad \left\{ \begin{aligned} \frac{d^2}{3} &\geq \frac{D^2}{4} \geq \frac{1}{n} \sum_{j=1}^n |\beta - \alpha_j|^2 \\ &= \frac{1}{n} \sum_{j=1}^n |a_j|^2 + \beta^2 + \frac{2\beta a_1}{n} \\ &\geq |a_n|^{2/n} + (\beta + \frac{a_1}{n})^2 - \frac{a_1^2}{n^2}. \end{aligned} \right.$$

So

$$d^2 \geq 3 \left( |a_n|^{2/n} - \frac{1}{n^2} [n/2]^2 \right).$$

If we assume that  $d \leq 2$  then it follows that  $|\alpha_n| = 1$  for  $n = 2$  or  $3$  and  $|\alpha_n| = 1$  or  $2$  for  $n = 4$  or  $5$ .

Denote by  $S_m$  the power sums

$$S_m = \sum_{j=1}^n \alpha_j^m \quad m = 0, 1, 2, \dots,$$

and note that each  $S_m$  is a rational integer. Newton's formulae yield

$$S_m + a_1 S_{m-1} + \dots + a_{m-1} S_1 + m a_m = 0 \quad \text{for } 1 \leq m \leq n.$$

Without loss of generality, we may suppose that  $|\alpha| = \max_{1 \leq j \leq n} |\alpha_j|$ .

Then

$$\begin{aligned} |n\alpha + a_1| &= \left| \sum_{j=1}^n (\alpha - \alpha_j) \right| \leq \sum_{j=1}^n |\alpha - \alpha_j| \\ &\leq (n-1)d. \end{aligned}$$

Hence

$$n|\alpha| \leq |n\alpha + a_1| + |-a_1| \leq (n-1)d + [n/2].$$

Set  $L_n(d) = \frac{1}{n} (d(n-1) + [n/2])$ . From (2.3) we see that

$$\sum_{j=1}^n |\alpha_j|^2 \leq \frac{nd^2}{3} + \frac{a_1^2}{n} \leq \frac{nd^2}{3} + \frac{1}{n}[n/2]^2.$$

Set  $K_n(d) = \frac{nd^2}{3} + \frac{1}{n}[n/2]^2$ . Then, evidently,

$$(3.3) \quad \left\{ \begin{aligned} |S_k| &\leq \sum_{j=1}^n |\alpha_j|^k \leq |\alpha|^{k-2} \sum_{j=1}^n |\alpha_j|^2 \\ &\leq K_n(d) L_n(d)^{k-2}. \end{aligned} \right.$$

Then Newton's formulae imply that  $a_k$  belongs to an interval of length  $\frac{2|S_k|}{k}$  centred at  $-\frac{1}{k} (a_1 S_{k-1} + \dots + a_{k-1} S_1)$  for given values

of  $a_1, \dots, a_{k-1}$  and hence of  $S_1, \dots, S_{k-1}$ . It is sufficient to test polynomials whose coefficients satisfy the conditions just imposed.

#### 4. Numerical results

In order to determine all inequivalent  $\alpha$  satisfying  $\text{diam}(\alpha) \leq 2$  for given degree  $n$ , it is sufficient to test those polynomials which satisfy the bounds implied by (3.3) when  $d = 2$ . Also, it is easy to see that there exists  $\delta_n > 0$  such that  $\text{diam}(\alpha) \leq 2 + \delta_n$  implies  $\text{diam}(\alpha) \leq 2$ . Moreover we can choose  $\epsilon_n$  so that the set of test polynomials for  $d \leq 2 + \epsilon_n$  is no larger than the set of test polynomials for  $d \leq 2$ . For small values of  $n$ , it is feasible to perform these calculations with the aid of a computer. We exclude all reducible polynomials which turn up in the computations. We shall deal with the cases  $n = 2, 3, 4, 5$  in turn.

(i)  $n = 2$ . This case is trivial since  $a_1 = 0$  or  $1$  and  $|a_2| = 1$ . Also, it is easily seen that if  $d > 2$  then  $d \geq \sqrt{5}$ .

(ii)  $n = 3$ . Here we can take  $\epsilon_3 = 0.1$  and hence  $K_3(d) < 4.75$  and so  $|S_2| \leq 4$  by (3.3). Since  $a_1 = 0$  or  $1$  and  $|a_3| = 1$ , it is enough to test at most  $1 \times 2 \times 5 \times 2 = 20$  polynomials. We find that we can take  $\delta_3 < 0.005\dots$ . Note that if  $\alpha$  is a zero of the polynomial  $x^3 - x - 1$ , then  $\text{diam}(\alpha) = 2.0650\dots$ .

(iii)  $n = 4$ . Here we can take  $\epsilon_4 = 0.02$  and hence  $K_4(d) < 6.45$  and  $L(d) \leq 2.015$ . Hence  $|S_2| \leq 6$  and  $|S_3| \leq 12$  by (3.3). Thus  $a_2$  and  $a_3$  lie in intervals of lengths  $6$  and  $8$  respectively. Since  $0 \leq a_1 \leq 2$  and  $|a_4| = 1$  or  $2$ , it is enough to test at most  $1 \times 3 \times 7 \times 9 \times 4 = 756$  polynomials. We find that we can take  $\delta_4 = 0.02$ .

(iv)  $n = 5$ . Here we can take  $\epsilon_5 = 0.003$  and hence  $K_5(d) < 7.487$  and  $L_5(d) < 2.003$ . Thus  $|S_2| \leq 7$ ,  $|S_3| \leq 14$  and  $|S_4| \leq 29$ . Hence  $a_2, a_3$  and  $a_4$  lie in intervals of lengths  $7, \frac{28}{3}$  and  $\frac{29}{2}$



respectively. Since  $0 \leq a_1 \leq 2$  and  $|a_5| = 1$  or  $2$ , it is enough to test at most  $1 \times 3 \times 8 \times 10 \times 15 \times 4 = 14400$  polynomials. We find that we can take  $\delta_5 = 0.003$ .

These computations were carried out on the Cyber 72 computer at the Australian Bureau of Statistics. The zeros of the polynomials selected by the algorithm described above were found using standard numerical procedures (Jenkins-Traub method).

We observe that the eleven inequivalent algebraic integers with  $\text{diam}(\alpha) \leq 2$  are totally imaginary when  $n = 2$  or  $4$  and have only one real conjugate when  $n = 3$  or  $5$ . Also that  $\alpha$  which yields the least value of  $\text{diam}(\alpha)$  for given degree  $n$  also generates a field whose discriminant is the least possible in absolute value for that degree when  $n = 2, 3$  or  $4$  but not when  $n = 5$ .

TABLE 1

INEQUIVALENT ALGEBRAIC INTEGERS WITH  $\text{DIAM}(\alpha) \leq 2.003$ 

<u>Degree</u>	<u>Polynomial</u>	<u>Diameter</u>
2	$x^2+x+1$	1.73205...
	$x^2+1$	2
3	$x^3+x^2-1$	1.79423...
	$x^3+x^2+1$	1.87418...
4	$x^4+2x^3+2x^2+x+1$	1.89882...
	$x^4+x^3+x^2+x+1$	1.90211...
	$x^4-x+1$	1.99391...
	$x^4-x^2+1$	2
	$x^4+1$	2
5	$x^5+2x^4+x^3-x^2-x+1$	1.99179...
	$x^5+x^4-1$	1.99785...

By (1.4) all inequivalent  $\alpha$  with  $D(\alpha) \leq 2$  lie among the  $\alpha$  with  $\text{diam}(\alpha) \leq 2$ . By using the numerical values of the conjugates of  $\alpha$ , we can calculate  $D(\alpha)$ . The procedure is necessarily ad hoc, since it depends on the distribution of the conjugates in the complex plane. The details are given in Favard [3] for  $n = 2$  and  $3$  and in the author's thesis for  $n = 4$  and  $5$ . Moreover, it is easy to see that there exists  $\gamma_n > 0$  such that  $D(\alpha) \leq 2 + \gamma_n$  implies  $D(\alpha) \leq 2$  for algebraic integers of degree  $n$ . We find that we can take  $\gamma_3 = 0.06$ ,  $\gamma_4 = 0.02$  and  $\gamma_5 = 0.003$ .

TABLE 2

INEQUIVALENT ALGEBRAIC INTEGERS WITH  $D(\alpha) \leq 2.003$

<u>Degree</u>	<u>Polynomials</u>	<u>Circumdiameter</u>
2	$x^2+x+1$	1.73205...
	$x^2+1$	2
3	$x^3+x^2-1$	1.97221...
4	$x^4+2x^3+2x^2+x+1$	1.89882...
	$x^4+x^3+x^2+x+1$	2
	$x^4-x^2+1$	2
	$x^4+1$	2

---

References

- [1] J. Favard, "Sur les nombres algébriques", *C.R. Acad. Sc. Paris*, 186 (1928), 1181-1182.
- [2] J. Favard, "Sur les formes décomposables et les nombres algébriques", *Bull. Soc. Math. France* 57 (1929), 50-71.
- [3] J. Favard, "Sur les nombres algébriques", *Mathematica* 4 (1930), 109-113.

- [4] L. Kronecker, "Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten", *J. reine angew. Math.* 53 (1857), 173-175.
- [5] C. W. Lloyd-Smith, "Problems on the distribution of conjugates of algebraic numbers", Ph.D. Thesis, University of Adelaide, 1980.
- [6] R. M. Robinson, "Conjugate algebraic integers on a circle", *Math. Z.* 110 (1969), 41-51.
- [7] I. M. Yaglom and V. G. Bol'yanskii, *Convex Figures* (translated by Paul J. Kelly and Lewis F. Walton, Holt, Rinehart and Winston, New York, 1961).

Australian Bureau of Statistics,  
Post Office Box 10,  
Belconnen,  
A.C.T., 2616,  
Australia.