MATHEMATICS OF COMPUTATION
Volume 76, Number 258, April 2007, Pages 1025–1038
S 0025-5718(06)01958-2
Article electronically published on December 29, 2006

ON THE SMALLEST VALUE OF THE MAXIMAL MODULUS OF AN ALGEBRAIC INTEGER

GEORGES RHIN AND QIANG WU

ABSTRACT. The house of an algebraic integer of degree d is the largest modulus of its conjugates. For $d \leq 28$, we compute the smallest house > 1 of degree d, say $\mathrm{m}(d)$. As a consequence we improve Matveev's theorem on the lower bound of $\mathrm{m}(d)$. We show that, in this range, the conjecture of Schinzel-Zassenhaus is satisfied. The minimal polynomial of any algebraic integer $\boldsymbol{\alpha}$ whose house is equal to $\mathrm{m}(d)$ is a factor of a bi-, tri- or quadrinomial. The computations use a family of explicit auxiliary functions. These functions depend on generalizations of the integer transfinite diameter of some compact sets in $\mathbb{C}$. They give better bounds than the classical ones for the coefficients of the minimal polynomial of an algebraic integer $\boldsymbol{\alpha}$ whose house is small.

1. INTRODUCTION

Let $\boldsymbol{\alpha}$ be a nonzero algebraic integer of degree d, whose conjugates are $\boldsymbol{\alpha}_1 = \boldsymbol{\alpha}$, $\boldsymbol{\alpha}_2, \ldots, \boldsymbol{\alpha}_d$, and let

$$P = b_0 X^d + b_1 X^{d-1} + \cdots + b_{d-1} X + b_d,$$

with $b_0 = 1$, be its minimal polynomial. We denote, as usual, by

$$\overline{|\boldsymbol{\alpha}|} = \max_{1 \leq i \leq d} |\boldsymbol{\alpha}_i|$$

the *house* of $\boldsymbol{\alpha}$, and by ν the number of $\boldsymbol{\alpha}_i$ such that $|\boldsymbol{\alpha}_i| > 1$. Then $\overline{|\boldsymbol{\alpha}|} \geq 1$ and Kronecker's theorem asserts that $\overline{|\boldsymbol{\alpha}|} = 1$ if and only if $\boldsymbol{\alpha}$ is a root of unity. We define $\mathrm{m}(d)$ to be the minimum of the houses of the algebraic integers $\boldsymbol{\alpha}$ of degree d which are not a root of unity.

A classical problem, see P. Borwein [PB], is to study the behaviour of $\mathrm{m}(d)$ when d varies. On the one hand, it is clear that $\mathrm{m}(d) \leq 2^{1/d}$ since the polynomial $X^d - 2$ is irreducible of degree d. On the other hand, there is a conjecture of A. Schinzel and H. Zassenhaus [SZ] which asserts that $\mathrm{m}(d) \geq 1 + c_1/d$, where c_1 is a positive constant. Moreover D. Boyd [DB] suggests that c_1 should be equal to $\frac{3}{2}\log(\theta_0)$ where $\theta_0 = 1.3247\ldots$ is the smallest Pisot number which is the real root of $X^3 - X - 1$. This is based on the fact, pointed out by C.J. Smyth, that for $d = 3k$ the number $\boldsymbol{\alpha}$ with minimal polynomial $X^{3k} + X^{2k} - 1$ has $\overline{|\boldsymbol{\alpha}|} = \theta_0^{1/(2k)} = \theta_0^{3/(2d)}$,

Received by the editor December 24, 2005 and, in revised form, December 28, 2005.
2000 *Mathematics Subject Classification.* Primary 11C08, 11R06, 11Y40.
Key words and phrases. Algebraic integer, maximal modulus, Schinzel-Zassenhaus conjecture, Mahler measure, Smyth's theorem, Perron numbers, explicit auxiliary functions, integer transfinite diameter.
Qiang Wu was supported in part by the Natural Science Foundation of Chongqing grant CSTC no. 2005BB8024.

and it is expected that this is equal to $\mathrm{m}(d)$ for this degree. We say that an $\boldsymbol{\alpha}$ which gives $\mathrm{m}(d)$ is *extremal.*

We define the Mahler measure of $\boldsymbol{\alpha}$ (and of P) by

$$\mathrm{M}(\boldsymbol{\alpha}) = |b_0| \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

We say that $\boldsymbol{\alpha}$ is reciprocal if $\boldsymbol{\alpha}^{-1}$ is a conjugate of $\boldsymbol{\alpha}$. Smyth [SM] proved that, if $\alpha \neq 0, 1$ is nonreciprocal, then $\mathrm{M}(\boldsymbol{\alpha}) \geq \theta_0$. Since $\mathrm{M}(\boldsymbol{\alpha}) \leq \overline{|\boldsymbol{\alpha}|}^d$, in this case we have $\overline{|\boldsymbol{\alpha}|} \geq 1 + \log(\theta_0)/d$.

P. Voutier [V] proved that, if $\boldsymbol{\alpha}$ is a nonzero algebraic integer of degree $d \geq 3$ which is not a root of unity, then

$$\mathrm{M}(\alpha) \geq 1 + \frac{1}{4}\Big(\frac{\log\log d}{\log d}\Big)^3.$$

This gives

$$\mathrm{m}(d) \geq \Big(1 + \frac{1}{4}\Big(\frac{\log\log d}{\log d}\Big)^3\Big)^{1/d}. \tag{1.1}$$

A. Dubickas [D] showed that the constant $1/4$ in (1.1) can be replaced by $64/\pi^2 - \varepsilon$ if $d > d_0(\varepsilon)$.

E. M. Matveev [MAT] proved the following result:

Theorem 1. *Let $\boldsymbol{\alpha}$ be an algebraic integer, not a root of unity, and let $d = \deg(\boldsymbol{\alpha}) \geq 2$. Then*

$$\overline{|\boldsymbol{\alpha}|} \geq \exp(\log(d + 0.5)/d^2). \tag{1.2}$$

Moreover, if $\boldsymbol{\alpha}$ is reciprocal and $d \geq 6$, then

$$\overline{|\boldsymbol{\alpha}|} \geq \exp(3\log(d/2)/d^2). \tag{1.3}$$

The lower bound for $\mathrm{m}(d)$ given in (1.1) is asymptotically better than the bound given in (1.2), but improves it only for $d \geq 1435$. Hence, for d not too large, the inequality (1.2) is better than (1.1).

For $d \geq 29$, we have $\exp(3\log(d/2)/d^2) \leq {\theta_0}^{1/d}$. So by Smyth's theorem, any nonzero algebraic integer $\boldsymbol{\alpha}$ of degree d, not a root of unity, whose house is less than ${\theta_0}^{1/d}$ is reciprocal. Then we may apply the second part of Matveev's theorem. Hence we deduce that, for $d \geq 29$,

$$\mathrm{m}(d) \geq \exp(3\log(d/2)/d^2).$$

In this paper our goal is, on the one hand, to verify the conjecture of Schinzel and Zassenhaus with Boyd's constant up to $d = 28$. On the other hand, we use these results to prove an interesting consequence of Matveev's theorem:

Theorem 2. *Let $\boldsymbol{\alpha}$ be a nonzero algebraic integer, not a root of unity, and $d = \deg(\boldsymbol{\alpha}) \geq 4$.*

Then for $d \leq 12$,

$$\overline{|\boldsymbol{\alpha}|} \geq \exp(3\log(d/3)/d^2) \tag{1.4}$$

and for $d \geq 13$,

$$\overline{|\boldsymbol{\alpha}|} \geq \exp(3\log(d/2)/d^2). \tag{1.5}$$

This result gives a better lower bound than (1.1) for $d \leq 6380$.

As a consequence of our computations we get the following results:

Proposition. *1. The conjecture of Schinzel and Zassenhaus is true, with* $c_1 = \frac{3}{2}\log(\theta_0)$*, for* $1 \leq d \leq 28$.

2. For $1 \leq d \leq 28$, $\mathrm{m}(d)$ *is given by a polynomial which is a factor of a polynomial with at most four monomials.*

3. For $3 \leq d \leq 30$, $\mathrm{m}(d)$ *is stricly less than* $2^{1/d}$.

For degree 31 we have computed the houses of all irreducible polynomials of height 1. They are all $> 2^{1/31}$. So we expect the following.

Conjecture. $m(31) = 2^{1/31}$.

A *Perron number* is a positive algebraic integer $\boldsymbol{\alpha}$ of degree d such that $\boldsymbol{\alpha} > \max_{2 \leq i \leq d} |\boldsymbol{\alpha}_i|$. For the degrees $d = 17$ and $d = 23$ the extremal $\boldsymbol{\alpha}$ is a Perron number. Hence they satisfy the conjecture of Lind–Boyd [DB]:

Conjecture (Lind-Boyd). *The smallest Perron number of degree* $d \geq 2$ *has minimal polynomial*

$$\begin{aligned} X^d - X - 1 &\textit{ if } d \not\equiv 3,5 \mod 6,\\ (X^{d+2} - X^4 - 1)/(X^2 - X + 1) &\textit{ if } d \equiv 3 \mod 6,\\ (X^{d+2} - X^2 - 1)/(X^2 - X + 1) &\textit{ if } d \equiv 5 \mod 6. \end{aligned}$$

Boyd [DB] also made the following conjecture:

Conjecture (Boyd). *1. The extremal* $\boldsymbol{\alpha}$ *is always nonreciprocal.*

2. If $d = 3k$*, then the extremal* $\boldsymbol{\alpha}$ *has minimal polynomial* $X^{3k} + X^{2k} - 1$ *(or* $X^{3k} - X^{2k} + 1$*).*

3. The extremal $\boldsymbol{\alpha}$ *of degree* d *has* $\nu \sim \frac{2}{3}d$ *as* $d \to \infty$.

We give in Table 1 the list of extremal $\boldsymbol{\alpha}$ for $d = 1$ to $d = 28$. We see that the claims 1 and 2 in Boyd's conjecture are satisfied. Boyd noticed that, up to degree 12, $\nu(d)$ is monotone, but this is no longer true for $d > 13$. The minimal polynomial of the extremal $\boldsymbol{\alpha}$ for degree 23 is

$$\begin{aligned} P_{23} = X^{23} &+ X^{22} - X^{20} - X^{19} + X^{17} + X^{16} - X^{14} - X^{13}\\ &+ X^{11} + X^{10} - X^8 - X^7 + X^5 + X^4 - X^2 - X - 1. \end{aligned}$$

Since this is a Perron number which satisfies the conjecture of Lind–Boyd, it can be written as

$$P_{23} = \frac{X^{25} - X^2 - 1}{X^2 - X + 1}.$$

Likewise,

$$P_{19} = X^{19} + X^{18} + X^{15} + X^{14} + X^{11} + X^{10} - X^8 + X^6 - X^4 + X^2 - 1$$

can be written as

$$P_{19} = \frac{X^{22} - X^{11} - X + 1}{X^3 - X^2 + X - 1}.$$

Therefore, for any extremal $\boldsymbol{\alpha}$ of degree d, we write its minimal polynomial P_d as a simple polynomial divided by a product of cyclotomic polynomials.

We make the following conjecture:

Conjecture. *Any extremal $\boldsymbol{\alpha}$ has minimal polynomial which is a factor of a polynomial which has at most* 4 *monomials.*

Proof of Theorem 2: We have only to verify that, for $4 \leq d \leq 28$, m(d) is greater than the right-hand side in (1.4) or (1.5).

Boyd [DB] has computed the smallest houses for $d \leq 12$. The main tool in his computations is to give bounds for s_k, which is the sum of the k-th powers of the roots of P, for $1 \leq k \leq 3d$. If $\lceil\overline{\boldsymbol{\alpha}}\rceil \leq B$, then $|s_k| \leq dB^k$. He uses these bounds together with Newton's formula:

$$s_k + s_{k-1}b_1 + \ldots + s_1 b_{k-1} + kb_k = 0,$$

which gives by induction bounds for the coefficients b_k, for $1 \leq k \leq d$, in order to get a large set $\mathcal{F}_d$ of polynomials. He computes s_k with Newton's formula for $d+1 \leq k \leq 3d$ (with $b_k = 0$) and, for every k, he eliminates the polynomial when s_k is not within its bounds. So he gets a smaller set $\mathcal{F}_{3d}$.

We use this principle, but the computing time grows exponentially with the degree d. Therefore, to obtain better bounds for the numbers s_k we construct a large family of explicit auxiliary functions. These functions are related to suitable generalizations of the integer transfinite diameter of some compact subsets of the complex plane. This method has been used in [FRSE] to compute all algebraic integers with small Mahler measure up to degree 40.

Here we prove that we may restrict our search to algebraic integers which are units. This property is used to reduce the numbers of polynomials to examine. A priori we cannot assume that this is true for the smallest Perron numbers; therefore the study of smallest Perron numbers will be devoted to a forthcoming paper [WU2].

This paper is organized as follows. In Section 2 we prove that, up to degree 30, for any degree d there exists an algebraic integer such that $1 < \lceil\overline{\boldsymbol{\alpha}}\rceil < 2^{1/d}$. This proves that $|b_d| = 1$. In Section 3 we show how to use explicit auxiliary functions to give bounds for s_k. We also explain how to construct such auxiliary functions. In Section 4 we give some refinements of the previous method. We give relations between s_k and s_{2k}. Moreover, for $d = 26$ and $d = 28$ we show that the triples (b_{d-2}, b_{d-1}, b_d) belong to a rather "small" set. Section 5 is devoted to the final computations. The search for the degree 28 took 6800 hours on a 2.8Ghz PC.

The first author is gratefully indebted to the South West University of China in Chongqing where a great part of this work was done.

2. The norm of $\boldsymbol{\alpha}$ with smallest house for $d \leq 30$

To prove the previous assertion for $3 \leq d \leq 30$, it suffices to prove it for $d = 4$ and when d is an odd prime ≤ 29 because, if $\deg(\boldsymbol{\alpha}) = d$ and $\lceil\overline{\boldsymbol{\alpha}}\rceil < 2^{1/d}$, then $\lceil\overline{\boldsymbol{\alpha}^{1/k}}\rceil < 2^{1/dk}$. For $4 \leq d \leq 23$ the results can be found in Table 1. When P_d is a primitive polynomial, it is written, for $d > 3$, as a quotient with numerator a tri- or a quadrinomial. The denominator is a product of at most two cyclotomic polynomials: $\Phi_1 = X - 1$, $\Phi_4 = X^2 + 1$ and $\Phi_6 = X^2 - X + 1$. When P_d is not primitive, it is written as $P_e(X^k)$ with $d = ek$. For $d = 29$ the minimal polynomial of the number $\boldsymbol{\alpha}$ which gives the smallest house $(= 1.02338300\ldots)$ that we have

TABLE 1. List of extremal $\boldsymbol{\alpha}$ of degree d and minimal polynomial $P_d(X)$. In the last column ν is the number of roots of P_d outside the unit disc.

d	polynomial $P_d(X)$	m(d)	ν
1	$X-2$	2	1
2	X^2-2	$2^{1/2}=1.41421356\dots$	2
3	X^3+X^2-1	$\theta_0^{1/2}=1.15096392\dots$	2
4	$(X^5-X^3+X-1)/\Phi_1$	$1.18375181\dots$	2
5	$(X^7-X^4+X+1)/\Phi_4$	$1.12164517\dots$	4
6	$P_3(X^2)$	$\theta_0^{1/4}=1.07282986\dots$	4
7	$(X^{10}-X^5-X^3+1)/(\Phi_1\Phi_4)$	$1.09284559\dots$	4
8	$(X^{11}-X^6+X-1)/(\Phi_1\Phi_4)$	$1.07562047\dots$	6
9	$P_3(X^3)$	$\theta_0^{1/6}=1.04798219\dots$	6
10	$P_5(X^2)$	$1.05907751\dots$	8
11	$(X^{14}-X^7-X+1)/(\Phi_1\Phi_4)$	$1.05712485\dots$	8
12	$P_3(X^4)$	$\theta_0^{1/8}=1.03577500\dots$	8
13	$(X^{15}-X^8+X+1)/\Phi_4$	$1.05372001\dots$	10
14	$P_7(X^2)$	$1.04539255\dots$	8
15	$P_3(X^5)$	$\theta_0^{1/10}=1.02851905\dots$	10
16	$P_8(X^2)$	$1.03712124\dots$	12
17	$(X^{19}-X^2-1)/\Phi_6$	$1.03930211\dots$	11
18	$P_3(X^6)$	$\theta_0^{1/12}=1.02371001\dots$	12
19	$(X^{22}-X^{11}-X+1)/(\Phi_1\Phi_4)$	$1.03641032\dots$	14
20	$P_5(X^4)$	$1.02911491\dots$	16
21	$P_3(X^7)$	$\theta_0^{1/14}=1.02028875\dots$	14
22	$P_{11}(X^2)$	$1.02816577\dots$	16
23	$(X^{25}-X^2-1)/\Phi_6$	$1.02932014\dots$	15
24	$P_3(X^8)$	$\theta_0^{1/16}=1.01773032\dots$	16
25	$P_5(X^5)$	$1.02322489\dots$	20
26	$P_{13}(X^2)$	$1.02650865\dots$	20
27	$P_3(X^9)$	$\theta_0^{1/18}=1.01574486\dots$	18
28	$P_7(X^4)$	$1.02244440\dots$	16

found for this degree is

$$P = X^{29} + X^{28} - X^{26} - X^{25} + X^{23} + X^{22} - X^{20} - X^{19} + X^{17}$$
$$+X^{16} - X^{14} - X^{13} + X^{11} + X^{10} - X^{8} - X^{7} + X^{5} + X^{4} - X^{2} - X - 1,$$

which may be written as

$$P = \frac{X^{31} - X^2 - 1}{X^2 - X + 1}.$$

In order to prove this assertion and to get good bounds B for our further computations, we seek all houses of irreducible polynomials of height 1 whose house is less than $2^{1/d}$ from degree 13 to degree 31. Then, in the sequel, the bound B will be taken, for any d, equal to the smallest house we have found during this computation. We use this bound to compute the auxiliary functions of Sections 3 and 4.

3. The bounds for s_k

a. We consider an explicit auxiliary function f of the following type:

$$f(z) = -\mathrm{Re}(z) - \sum_{1 \le j \le J} e_j \log |Q_j(z)|, \tag{3.1}$$

where z is a complex number, the e_j are positive real numbers and the integer polynomials Q_j belong to a fixed set S that will be defined later. The numbers e_j are always chosen to get the best auxiliary function. We denote by m the minimum of $f(z)$ for $|z| \le B$. Since the function f is harmonic in this disc outside the union of small discs around the roots of the polynomials Q_j, this minimum is taken over $|z| = B$.

We now assume that the polynomial P does not divide any polynomial $Q_j(\pm X^k)$ for $1 \le k \le 3d$. Then

$$\sum_{1 \le i \le d} f(\boldsymbol{\alpha}_i) \ge md$$

and

$$-s_1 \ge d\, m + \sum_{1 \le j \le J} e_j \log \left| \prod_{1 \le i \le d} Q_j(\boldsymbol{\alpha}_i) \right|.$$

$\prod_{1 \le i \le d} Q_j(\boldsymbol{\alpha}_i)$ is equal to the resultant of P and Q_j. Since P does not divide Q_j, this is a nonzero integer. Therefore

$$s_1 \le -dm. \tag{3.2}$$

By symmetry, the same inequality is valid for $-s_1$. If we replace B by B^k and the numbers $\boldsymbol{\alpha}_i$ by the numbers $\pm{\boldsymbol{\alpha}_i}^k$, we get upper bounds for $\pm s_k$.

Remark. In his proof of Theorem 1, Matveev used an auxiliary function of this type with the four polynomials: X, $X-1$, $X-2$ and $X^2 - X - 1$.

b. Relations between explicit auxiliary functions and the integer transfinite diameter.

If, inside the auxiliary function (3.1), we replace the real numbers e_j by rational numbers we may write

$$f(z) = -\mathrm{Re}(z) - \frac{t}{h} \log |H(z)|,$$

where H is in $\mathbb{Z}[X]$ of degree h and t is a positive real number. We want to get a function f whose minimum m in $|z| \le B$ is as large as possible. That is to say, we seek a polynomial $H \in \mathbb{Z}[X]$ such that

$$\sup_{|z|\le B} |H(z)|^{t/h} e^{\mathrm{Re}(z)} \le e^{-m}.$$

Now, if we suppose that t is fixed, say $t = 1$, it is clear that we need an effective upper bound for the quantity

$$t_{\mathbb{Z},\boldsymbol{\varphi}}(|z| \le B) = \liminf_{\substack{h\ge 1\\ h\to\infty}} \inf_{\substack{H\in\mathbb{Z}[X]\\ \deg H=h}} \sup_{|z|\le B} |H(z)|^{t/h} \boldsymbol{\varphi}(z), \tag{3.3}$$

where we use the weight $\boldsymbol{\varphi}(z) = e^{\mathrm{Re}(z)}$. To get an upper bound for $t_{\mathbb{Z},\boldsymbol{\varphi}}(|z| \le B)$, it suffices to get an explicit polynomial $H \in \mathbb{Z}[X]$ and then to use the sequence of the successive powers of H.

This is a generalization of the integer transfinite diameter. For any $h \ge 1$ we say that a polynomial H (not always unique) is an *Integer Chebyshev Polynomial* if the quantity $\sup_{|z|\le B} |H(z)|^{t/h}\boldsymbol{\varphi}(z)$ is a minimum. With Wu's algorithm [WU1], we compute polynomials H of degree less than 30 or 40 and take their irreducible factors as polynomials Q_j. We start with the polynomial $X - 1$, get the best e_1 and take $t = e_1$. After computing J polynomials, we optimize the numbers e_j as explained in the next subsection. This gives us a new number t, and we continue by induction to get $J + 1$ polynomials. The list of polynomials Q_j of the set S is given in Table 2.

c. Optimization of the numbers e_j.

We give a brief scheme of the semi-infinite linear programming method introduced into number theory by C. J. Smyth. More details can be found in [FRSE].

To optimize the numbers e_j, we first put the coefficient of $\mathrm{Re}(z)$ equal to $e_0 = 1$. We take a set X_1 of "well distributed" points of modulus equal to B. By linear programming, we get the maximum μ of the minimum of a finite set of linear forms whose coefficients are $-\mathrm{Re}(z_i)$ and $-\log|Q_j(z_i)|$ for $1 \le j \le J$ for any z_i in X_1. This gives an auxiliary function f which has a minimum $m > \mu$. We add to X_1 a selection of the points of $|z| = B$ where f has a local minimum. With this new set X_2 we get another value for m and μ. We stop the process when the integer parts of m and μ coincide.

d. A refinement for the bounds of s_k.

When B^k becomes too large (say for $k \sim 2d$) the bounds given by the auxiliary functions are not as good as for small k. We give now better bounds. For this we need the lemma:

Lemma 1. *Let $d \ge 2$ be an integer, $b \ge 1$ a real number and $\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_d$ d positive real numbers satisfying the following properties:*

$\boldsymbol{\alpha}_i \le b$ *for* $1 \le i \le d$ *and* $\prod_{1\le i\le d} \boldsymbol{\alpha}_i = 1$.

Then we have

$$\sum_{1\le i\le d} \boldsymbol{\alpha}_i \le (d-1)b + \frac{1}{b^{d-1}}. \tag{3.4}$$

Proof. We may assume that

$$\frac{1}{b^{d-1}} \le \boldsymbol{\alpha}_1 \le \ldots \le \boldsymbol{\alpha}_d \le b,$$

TABLE 2. List of polynomials Q_j of the set S which are used in the auxiliary functions of Section 3, $d_j = \deg Q_j$, and the coefficients of Q_j are written from degree d_j to 0.

Q_j	d_j	Coefficients of Q_j						
Q_1	1	1	−1					
Q_2	1	1	−2					
Q_3	1	1	−3					
Q_4	1	1	−4					
Q_5	1	1	−5					
Q_6	1	1	−6					
Q_7	1	1	−7					
Q_8	2	1	0	1				
Q_9	2	1	−1	1				
Q_{10}	2	1	−2	2				
Q_{11}	2	1	−3	3				
Q_{12}	2	1	−4	5				
Q_{13}	2	1	−5	7				
Q_{14}	2	2	−4	3				
Q_{15}	3	1	−1	0	1			
Q_{16}	4	1	0	−1	0	1		
Q_{17}	4	1	−1	1	−1	1		
Q_{18}	4	1	−2	3	−3	2		
Q_{19}	4	1	−3	5	−5	3		
Q_{20}	4	1	−4	8	−9	5		
Q_{21}	6	1	0	0	1	0	0	1

whence

$$1 \leq \boldsymbol{\alpha}_d \leq b.$$

If $\boldsymbol{\alpha}_1 = 1$, then $\boldsymbol{\alpha}_1 = \ldots = \boldsymbol{\alpha}_d = 1$ and

$$\sum_{1\leq i\leq d} \boldsymbol{\alpha}_i = d \leq (d-1)b + \frac{1}{b^{d-1}} \tag{3.5}$$

since the right-hand side in (3.5) is an increasing function of b on $[1,\infty)$. If $\boldsymbol{\alpha}_1 = \frac{1}{b^{d-1}}$, then

$$\boldsymbol{\alpha}_2 = \ldots = \boldsymbol{\alpha}_d = b$$

and we get (3.4). If $\frac{1}{b^{d-1}} < \boldsymbol{\alpha}_1 < 1$, then there exists an integer $k \geq 1$ such that

$$\frac{1}{b^{d-1}} < \boldsymbol{\alpha}_1 \leq \ldots \leq \boldsymbol{\alpha}_k < \boldsymbol{\alpha}_{k+1} = \ldots = \boldsymbol{\alpha}_d = b.$$

Let γ be a real number such that $\boldsymbol{\alpha}_1 \gamma \boldsymbol{\alpha}_k = 1$. Then we have $\gamma \boldsymbol{\alpha}_k^2 \geq 1$. Since

$$\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_k = \frac{1}{\gamma \boldsymbol{\alpha}_k} + \boldsymbol{\alpha}_k$$

is an increasing function of $\boldsymbol{\alpha}_k$, we get (3.4) if we increase successively $\boldsymbol{\alpha}_k, \ldots, \boldsymbol{\alpha}_2$ until they reach b.

TABLE 3.

k	1	2	3	4	8	16	28	48	60	76	84
s_k	0	0	0	-4	4	-12	24	36	-44	72	24
max	5	6	7	8	13	23	41	74	102	145	174
MAX	28	29	29	30	33	39	52	81	106	151	180

Since $b_d = \pm 1$, we may apply Lemma 1 to the set $|\boldsymbol{\alpha}_i|$, $1 \leq i \leq d$, of the moduli of the roots of P. Thus we get

$$|s_k| \leq (d-1)B^k + \frac{1}{B^{k(d-1)}}.$$

This is better than the previous bounds that we have computed with the explicit auxiliary functions.

e. A numerical example for degree 28.

We give, in Table 3, the bounds that we obtain for $|s_k|$ (max) for some values of k and the corresponding classical bounds (MAX). We give also the values of s_k for the polynomial P_{28}.

4. Improvements of the method

a. Relations between the bounds for s_k and the bounds for s_{2k}.

The classical inequality relating s_k and s_{2k} is the following [DB]:

$$s_{2k} \geq \frac{2s_k^2}{d} - dB^{2k}.$$

Here we exploit the relations between s_k and s_{2k} that will be given by explicit auxiliary functions of the following type:

$$f(z) = \mathrm{Re}(z^2) - e_0\mathrm{Re}(z) - \sum_{1 \leq j \leq J} e_j \log |Q_j(z)|\,, \tag{4.1}$$

where the numbers e_j and the polynomials Q_j are as in Section 3. We add to the previous set S of 21 polynomials given in Table 2, the 10 polynomials of Table 4. If m is the minimum of $f(z)$ for $|z| \leq B$, by the same argument as in Section 3 we get

$$s_2 - e_0 s_1 \geq md.$$

If we assume that s_1 has the value $\boldsymbol{\sigma}$, then $s_2 \geq dm + e_0\boldsymbol{\sigma}$. We optimize the numbers $e_0, \ldots, e_J$ to get a maximal value for $dm + e_0\boldsymbol{\sigma}$. Therefore we get a lower bound for s_2 depending on the value of $\boldsymbol{\sigma}$. If we take $\boldsymbol{\sigma}$ close to its upper bound, then we get a bound for s_2 better than the one given in Section 3. If in (4.1) we replace $-e_0\mathrm{Re}(z)$ by $e_0\mathrm{Re}(z)$, we get the same lower bound for s_2 when s_1 has the value $-\boldsymbol{\sigma}$. We may also replace $\mathrm{Re}(z^2)$ by $-\mathrm{Re}(z^2)$ and get upper bounds for s_2. Then, replacing B by B^k, we get bounds for s_{2k} when s_k has values close to its bounds. We give a numerical example for $d = 18$. For $k = 6$ we have $-7 \leq s_6 \leq 7$ and

TABLE 4. List of new polynomials which are used in the auxiliary functions of Section 4a. Two different subsets of the polynomials $Q_1, \ldots, Q_{31}$ are used to get the upper bounds for s_{2k}, respectively the lower bounds for s_{2k}.

Q_j	d_j	Coefficients of Q_j						
Q_{22}	1	1	1					
Q_{23}	2	1	1	1				
Q_{24}	2	1	0	−2				
Q_{25}	3	1	−1	−3	4			
Q_{26}	3	1	−1	−4	5			
Q_{27}	3	1	−2	−1	3			
Q_{28}	3	1	−3	1	3			
Q_{29}	4	1	0	0	0	1		
Q_{30}	4	1	1	1	1	1		
Q_{31}	6	1	1	1	1	1	1	1

$-12 \leq s_{12} \leq 12$. Then we decrease the upper bounds of s_{12} as follows:

$$\begin{aligned} &\text{if } |s_6| = 7, \text{ then } s_{12} \leq 3,\\ &\text{if } |s_6| = 6, \text{ then } s_{12} \leq 5,\\ \text{and } &\text{if } |s_6| = 5, \text{ then } s_{12} \leq 10. \end{aligned}$$

For the lower bounds of s_{12} we get

$$\begin{aligned} &\text{if } |s_6| \geq 6, \text{ then } s_{12} \geq -9,\\ &\text{if } |s_6| = 5, \text{ then } s_{12} \geq -10,\\ \text{and } &\text{if } |s_6| = 4, \text{ then } s_{12} \geq -11. \end{aligned}$$

Remark. The polynomial $P_{18} = X^{18} + X^{12} - 1$, which is the minimal polynomial of the extremal $\boldsymbol{\alpha}$, does not satisfy these conditions since, for P_{18}, we have $s_6 = -6$ and $s_{12} = 6$. This is because we have used the polynomial $X^3 - X^2 + 1$ in the auxiliary function and $-\boldsymbol{\alpha}^6$ is a root of this polynomial. If we do not use the polynomial $X^3 - X^2 + 1$ in the auxiliary function, then for $|s_6| = 6$ we have $s_{12} \leq 8$. So, for every d, we add to the set of polynomials obtained by our computations all the irreducible factors of degree d of the polynomials $Q_j(\pm X^k)$.

When d is large the results are more spectacular. For $d = 28$ we have $|s_{42}| \leq 64$ and $|s_{84}| \leq 174$. If $|s_{42}| = 64$, then $105 \leq s_{84} \leq 118$.

b. A study of the triples (b_{d-2}, b_{d-1}, b_d).

Here we want to get good bounds for $|b_{d-2}|$ and $|b_{d-1}|$. Since $|b_d| = 1$, we have $|b_{d-2}| = |\sum_{1\leq i\leq d} 1/\boldsymbol{\alpha}_i^2|$ and $|b_{d-1}| = |\sum_{1\leq i\leq d} 1/\boldsymbol{\alpha}_i|$. But we have $|1/\boldsymbol{\alpha}_i| \leq B^{d-1}$, so this implies, when $d = 28$ and $B = 1.02245$, $|b_{d-1}| \leq dB^{d-1} < 50.992$ and $|b_{d-2}| \leq dB^{2(d-1)} < 92.87$. These bounds are unsatisfactory. Therefore, in order to obtain reasonable bounds for b_{d-2} and b_{d-1}, we study $\boldsymbol{\sigma}_k = \sum_{1\leq i\leq d} \boldsymbol{\alpha}_i^k + 1/\boldsymbol{\alpha}_i^k$ for $k = 1,\ 2$. The advantage is that the numbers $\boldsymbol{\alpha}_i^k + 1/\boldsymbol{\alpha}_i^k$ lie inside an ellipse which is "not too far" from the real axis. Moreover we will see that, in the worst case, all these numbers but one are inside an ellipse which is very close to the interval $[-2, 2]$. Since the auxiliary functions $f(z)$ of the type (3.1) are more efficient when z has a very small imaginary part, we will get good bounds for $\boldsymbol{\sigma}_1$ and $\boldsymbol{\sigma}_2$. For

$d = 28$ we get $|\boldsymbol{\sigma}_1| \leq 8$ and $|\boldsymbol{\sigma}_2| \leq 13$. This gives, for a fixed pair (s_1, s_2), 566 triples.

We first need a lemma:

Lemma 2. *Let m be a positive real number, let $d \geq 2$ be an integer, and $h(x)$ a real continuous decreasing function defined on the interval $[0,(d-1)m]$. Let $h_1(x)$ and $h_2(x)$ be two linear functions such that:*

For $0 \leq x \leq m,\ h(x) = h_1(x)$ and for $m \leq x \leq (d-1)m,\ h(x) = h_2(x)$.

Let $b_1 \leq \ldots \leq b_d \leq m$ be d real numbers such that

$$\sum_{1\leq i\leq d} b_i = 0.$$

Define

$$\omega = \sum_{1\leq i\leq d} h(|b_i|).$$

Then

$$\omega \geq h((d-1)m) + (d-1)h(m). \tag{4.1}$$

Proof. If all the numbers b_i vanish, then (4.1) is clearly true; otherwise there exist two integers $0 \leq l \leq k < d$ such that

$$-(d-1)m \leq b_1 \leq \ldots \leq b_l \leq -m,$$
$$-m < b_{l+1} \leq \ldots \leq 0,$$

and

$$0 < b_{k+1} \leq \ldots \leq b_d \leq m.$$

Now, if we put $a_i = |b_i|$ for all i, we have $a_1 + \ldots + a_k = a_{k+1} + \ldots + a_d$ and $a_1 + \ldots + a_l \geq lm$.

If $l = 0$, then, since h_2 is linear, we have

$$\omega \geq \sum_{1\leq i\leq d} h_1(m) = \sum_{1\leq i\leq d} h_2(m) = h_2((d-1)m) + (d-1)h_2(m).$$

If $l \geq 1$ we have

$$\omega \geq \sum_{1\leq i\leq l} h_2(a_i) + \sum_{l+1\leq i\leq d} h_1(m). \tag{4.2}$$

Since h_2 is linear and

$$lm \leq \sum_{1\leq i\leq l} a_i \leq (d-k)m,$$

the right-hand side of (4.2) is equal to

$$h_2\left(\sum_{1\leq i\leq l} a_i - (l-1)m\right) + (l-1)h_2(m) + (d-l)h_1(m).$$

Then, since $d-k-l+1 \leq d-1$, we have

$$\omega \geq h_2((d-k-l+1)m) + (d-1)h_2(m) \geq h_2((d-1)m) + (d-1)h_2(m).$$

Let P be a monic integer noncyclotomic polynomial of degree $d \geq 2$ such that $|P(0)| = 1$. Let $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_d$ be its roots in $\mathbb{C}$ and put $b_i = \frac{\log|\boldsymbol{\alpha}_i|}{\log B}$ with $b_1 \leq \ldots \leq b_d \leq 1$. Then there exists an integer $k \leq d-1$ such that $0 < b_{k+1} \leq \ldots \leq b_d \leq 1$.

Put $a_i = |b_i|$ for $1 \le i \le d$. Then $\boldsymbol{\alpha}_i + \frac{1}{\boldsymbol{\alpha}_i}$ is inside the ellipse $\mathcal{E}_{a_i}$ whose axes are $B^{a_i} + B^{-a_i}$ and $B^{a_i} - B^{-a_i}$.

Now let f be an explicit auxiliary function of type (3.1). For $a \ge 0$ we define the function

$$g(a) = \min_{z \in \mathcal{E}_a} f(z). \tag{4.3}$$

Since $\boldsymbol{\alpha}_i + \frac{1}{\boldsymbol{\alpha}_i} \in \mathcal{E}_{a_i}$, we have

$$\boldsymbol{\sigma}_1 \ge \sum_{1 \le i \le d} g(a_i). \tag{4.4}$$

Now we assume that we have a decreasing function h which is continuous on the interval $[0, d-1]$, linear on both intervals $[0,1]$ and $[1, d-1]$ and such that, for all $a \in [0, d-1]$, $h(a) \le g(a)$. Then, By Lemma 2, we get from (4.4) that

$$\boldsymbol{\sigma}_1 \ge (d-1)h(1) + h(d-1).$$

For a fixed ε (say $\varepsilon = 1/10$), we want the function h to satisfy $h \le g$ and to be such that

$$(d-1)h(1) + h(d-1) \ge (d-1)g(1) + g(d-1) - \varepsilon.$$

For $d = 28$ and $B = 1.02245$, we explain how to choose the function h. The polynomials Q_j are the 11 polynomials R_j given in Table 5, and the coefficients e_j are equal to

$$0.16464679,\ 0.49414790,\ 0.61080711,\ 0.04928365,\ 0.03946975,\ 0.21423746,$$
$$0.02691357,\ 0.14143025,\ 0.04972685,\ 0.02489806,\ 0.03963391.$$

We have $m_1 = g(0) = -0.22094287\ldots$, $m_2 = g(1) = -0.22447363\ldots$, $m_3 = g(d-1) = -2.83442434\ldots$ and $(d-1)g(1) + g(d-1) = -8.89521261\ldots$. We put $\varepsilon_1 = \varepsilon_2 = \frac{\varepsilon}{2(d-1)}$ and $\varepsilon_3 = \frac{\varepsilon}{2}$.

The function h_1 is the line defined by $h_1(0) = m_1 - \varepsilon_1$ and $h_1(1) = m_2 - \varepsilon_2$. The function h_2 is defined by $h_2(1) = m_2 - \varepsilon_2$ and $h_2(d-1) = m_3 - \varepsilon_3$. We find a staircase function s such that $h \le s \le g$. The sequence of points $0 < a_t < \ldots < a_1 = d-1$ where s is not continuous is defined by induction as follows. We start at $a_1 = d-1$ where $s(a_1) = g(a_1)$. Then $a_2 < a_1$ is defined by $h_2(a_2) = g(a_1)$. Since g and h_2 are decreasing we have, for any $a \in (a_2, a_1)$, $h_2(a) < s(a) = g(a_1) < g(a)$. We continue until we obtain a point a_{r-1} such that $m_2 - \varepsilon_2 < g(a_{r-1}) < m_2$. We take the next point $(a_r, g(a_{r-1}))$ on the line h_1, and we continue the same process as before with h_1 instead of h_2, until $g(a_t) \ge m_1 - \varepsilon_1$. The last stair is $(0, a_t)$ where s has the value $g(a_t)$. In this case $t = 31$ and $(d-1)h(1) + h(d-1) \ge -8.99521261\ldots$ so $\boldsymbol{\sigma}_1 \ge -8$.

5. The final computation

The set $\mathcal{F}_d$ is very large when the degree d increases. For $d = 28$ it contains 1.6×10^{12} polynomials. In this special case (and also for degree 26), for each of the 34 possible values of (s_1, s_2) (restricted to $s_1 \le 0$), we first compute all possible triples (b_{d-2}, b_{d-1}, b_d) and then compute the sets $\mathcal{F}_d$ and $\mathcal{F}_{3d}$ relative to this pair (s_1, s_2). If the set $\mathcal{F}_{3d}$ is not empty, then we use the Schur–Cohn algorithm [MAR] to compute the number of roots of P inside a disc of radius equal to Matveev's bound (1.2). Since we always use a bound B that will be subsequently proved to equal $\mathrm{m}(d) + \varepsilon$, we get few polynomials. For instance, in the case $d = 26$ we

TABLE 5. Polynomials R_j which are used in the auxiliary functions of Section 4b. $d = \deg R_j$ and the coefficients of R_j are written from degree d to 0.

R_j	d	Coefficients of R_j					
R_1	1	1	0				
R_2	1	1	1				
R_3	1	1	2				
R_4	2	1	0	−2			
R_5	2	1	0	−3			
R_6	2	1	1	−1			
R_7	3	1	0	−3	1		
R_8	3	1	1	−2	−1		
R_9	4	1	1	−4	−4	1	
R_{10}	5	1	−4	−3	−3	3	1
R_{11}	5	1	1	−5	−5	4	3

get 11 polynomials. In the case $d = 28$ we get 8 polynomials. For the very last computation we use Pari [PARI] to keep only the irreducible polynomials (which turn out to be always at most 1) and compute the roots of the polynomials P to get ν and $\mathrm{m}(d)$.

In the case $d = 3k$ we get no polynomial at all, because the polynomial $X^3 + X^2 - 1$ is used inside one of the auxiliary functions, as was explained in Section 4a.

References

[DB] D. Boyd, *The Maximal Modulus of an Algebraic Integer*, Math. Comp. **45** (1985), 243–249. MR790657 (87c:11097)

[PB] P. Borwein, *Computational Excursions in Analysis and Number Theory*, CMS Books in Mathematics **10**, Springer-Verlag, New York (2002). MR1912495 (2003m:11045)

[D] A. Dubickas, *On a conjecture of A. Schinzel and H. Zassenhaus*, Acta Arith. **63** (1993), 15–20. MR1201616 (94a:11161)

[FRSE] V. Flammang, G. Rhin and J.M. Sac-Épée, *Integer transfinite diameter and polynomials of small Mahler measure*, Math. Comp. **75** (2006), 1527–1540. MR2219043

[MAR] M. Marden, *Geometry of polynomials*, Amer. Math. Soc. Providence, Rhode Island (1966). MR0225972 (37:1562)

[MAT] E.M. Matveev, *On the cardinality of algebraic integers*, Math. Notes **49** (1991), 437–438. MR1119233 (92g:11070)

[PARI] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *GP-Pari version 2.0.12*, 1998.

[SZ] A. Schinzel and H. Zassenhaus, *A refinement of two theorems of Kronecker*, Michigan Math. J. **12** (1965), 81–85. MR0175882 (31:158)

[SM] C.J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175. MR0289451 (44:6641)

[V] P. Voutier, *An effective lower bound for the height of algebraic numbers*, Acta Arith. **74** (1996), 81–95. MR1367580 (96j:11098)

[WU1] Q. Wu, *On the linear independence measure of logarithms of rational numbers*, Math. Comp. **72** (2002), 901–911. MR1954974 (2003m:11111)

[WU2] Q. Wu, *The smallest Perron numbers (in preparation).*

UMR CNRS 7122, Département UFR MIM, Université de Metz, Ile du Saulcy, 57045 Metz Cedex 01, France
E-mail address: rhin@math.univ-metz.fr

Department of Mathematics, Southwest University of China, 2 Tiansheng Road Beibei, 400715 Chongqing, China
E-mail address: qiangwu@swu.edu.cn