ALGEBRAIC INTEGERS WHOSE CONJUGATES ALL LIE IN AN ELLIPSE

VALÉRIE FLAMMANG AND GEORGES RHIN

Abstract. We find all 15909 algebraic integers $\alpha$ whose conjugates all lie in an ellipse with two of them nonreal, while the others lie in the real interval $[-1, 2]$. This problem has applications to finding certain subgroups of $SL(2, \mathbb{C})$. We use explicit auxiliary functions related to the generalized integer transfinite diameter of compact subsets of $\mathbb{C}$. This gives good bounds for the coefficients of the minimal polynomial of $\alpha$.

1. Introduction

In this paper we solve the following problem of Colin Maclachlan from Aberdeen, submitted to us by C. J. Smyth.

Problem. Find all algebraic integers $\alpha$ of degree $d \geq 2$ with the following property: all the conjugates of $\alpha$ lie inside the ellipse

$$\mathcal{E} = \{ z = x + iy \text{ such that } \left(\frac{x - 1/2}{5/2}\right)^2 + \left(\frac{y}{2}\right)^2 \leq 1\},$$

with two of them conjugate nonreal numbers, while all the others are real in the interval $[-1, 2]$.

Each of these algebraic numbers corresponds to a discrete subgroup of $SL(2, \mathbb{C})$ with two generators: one of order 2 and one of order 3.

We denote by $\mathcal{C}$ the set of the minimal polynomials $P$ of the algebraic integers defined above. It is clear that if $P \in \mathcal{C}$ is of degree $d$, then $(-1)^d P(1 - X)$ is also in $\mathcal{C}$. So we call $\mathcal{C}_1$ the set of polynomials $P \in \mathcal{C}$ such that if $P(z) = 0$ and $z$ is complex, then $\text{Re } z \leq 1/2$. We denote by $\mathcal{E}_1$ the set of the elements $z$ of the ellipse $\mathcal{E}$ with $\text{Re } z \leq 1/2$.

To show that $\mathcal{C}$ is finite, it suffices to show that $\mathcal{C}_1$ is finite. For this we will use the fact that the integer transfinite diameter of the interval $[-1, 2]$ is less than 1. This ensures that there exists a nonzero polynomial $H \in \mathbb{Z}[X]$ such that

$$\sup_{-1 \leq x \leq 2} |H(x)| = \delta_0 < 1.$$

For example, the polynomial $H = X(X - 1)(X + 1)(X - 2)(X^2 - X - 1) + 1$ gives $\delta_0 = 0.703125$. Let $\delta_1 = \sup_{z \in \mathcal{E}_1} |H(z)| = 139.453125$. Suppose that a polynomial
Table 1.

<table>
<thead>
<tr>
<th>degree</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>nber pol in ( C )</td>
<td>22</td>
<td>206</td>
<td>918</td>
<td>2404</td>
<td>4401</td>
<td>4260</td>
<td>2792</td>
<td>600</td>
<td>186</td>
<td>15909</td>
</tr>
</tbody>
</table>

\( P \) of degree \( d \) belongs to \( C_1 \). Then \( P \) does not divide \( H \) and so

\[
1 \leq |\text{Resultant}(P,H)| = \prod_{1 \leq j \leq d} |H(\alpha_j)| \leq \delta_0^{d-2}\delta_1^2,
\]

where \( \alpha_1, \ldots, \alpha_d \) are the roots of \( P \). It is clear that for \( d > d_0 \) (with \( d_0 = 30 \)) the previous inequality is impossible because \( \delta_0^{d-2}\delta_1^2 < 1 \). Then \( \deg P \leq 30 \) and, since the roots of \( P \) are bounded by an absolute constant, the set \( C_1 \) is finite.

Here we will explicitly determine the set \( C_1 \). The complete list of elements of \( C \) can be found on the web site [WE]. The set \( C \) has exactly 15909 elements as given in Table 1. Let us briefly explain the methods that we will use to compute these polynomials. Let \( P = b_0X^d + \cdots + b_d \) be in \( C_1 \) (with \( b_0 = 1 \)). For \( k = 1, \ldots, d \) we define \( s_k = \sum_{1 \leq j \leq d} \alpha_j^k \). We will give, for each \( k \), an upper and a lower bound for \( s_k \). Using Newton’s formula:

\[
s_k b_0 + s_{k-1} b_1 + \cdots + s_1 b_{k-1} + k b_k = 0,
\]

we will obtain by induction some bounds for the coefficients \( b_k \).

The bounds for \( s_k \) will be given by explicit auxiliary functions. This method was extensively used by C. J. Smyth [SM] and the authors [FRS]. As in [FRS] we will closely relate these auxiliary functions with some generalizations of the integer transfinite diameter. We will make use of the algorithm given by Q. Wu [WU] to give good upper bounds for these integer transfinite diameters, and consequently good auxiliary functions. As explained later, we will need some refinements of these methods.

In Section 2, we recall the method of the explicit auxiliary functions. In Section 3, we recall the definition and some properties of the integer transfinite diameter. In Section 4, we recall the relations between the explicit auxiliary functions and the integer transfinite diameter. We give a sketch of Wu’s algorithm and explain how this algorithm gives good auxiliary functions. In Section 5, we give a realistic bound for the degree of the polynomials \( P \), i.e. \( \deg P \leq 12 \), and we describe the technique for computation of the polynomials \( P \) when \( \deg P \leq 7 \). In Section 6, we give improvements of the method to enable us to complete the computations when \( \deg P \geq 8 \).

2. The auxiliary functions

We will explain by an example the use of an explicit auxiliary function. The Schur-Siegel-Smyth problem is the following [B]:

**Problem.** Give a lower bound of \( \text{trace}(\alpha)/\deg(\alpha) \) where \( \alpha \) is a totally positive algebraic integer. It is conjectured that, for all \( \varepsilon > 0 \), this quantity (the absolute trace of \( \alpha \)) is greater than \( 2 - \varepsilon \) if \( \deg(\alpha) \) is large enough.

Let \( P \) be the minimal polynomial of \( \alpha \) of degree \( d \) whose roots (which are all real and positive) are \( \alpha_1, \ldots, \alpha_d \). We consider the auxiliary function \( f \):

\[
f(x) = x - \sum_{1 \leq j \leq d} e_j \log |Q_j(x)|,
\]
where the polynomials \( Q_j \) are nonzero elements of \( \mathbb{Z}[X] \) and the \( e_j \) are real positive numbers. We denote by \( m \) the minimum of the function \( f(x) \) for \( x > 0 \) and \( Q_j(x) \neq 0 \) for \( 1 \leq j \leq J \).

If we suppose that the polynomial \( P \) does not divide any polynomial \( Q_j \) we get

\[
\sum_{1 \leq i \leq d} f(\alpha_i) \geq md
\]

and

\[
\sum_{1 \leq i \leq d} \alpha_i \geq md + \sum_{1 \leq j \leq J} e_j \log \left| \prod_{1 \leq i \leq d} Q_j(\alpha_i) \right|.
\]

But \( \prod_{1 \leq i \leq d} Q_j(\alpha_i) \) is a nonzero rational integer because it is the resultant of \( P \) and \( Q_j \). Therefore \( \sum_{1 \leq i \leq d} \alpha_i \geq md \). Then we have obtained a lower bound of the absolute trace of \( \alpha \). The quality of this bound relies on the choice of the \( Q_j \) and of the \( e_j \). By this method Smyth [SM] proved that if \( \alpha \) is not in a finite set of explicit exceptions, then the absolute trace of \( \alpha \) is greater than 1.771 . . .

3. The integer transfinite diameter

Let \( K \) be a compact subset of \( \mathbb{C} \). If \( P \) is a polynomial in \( \mathbb{C}[X] \) we put \( |P|_{\infty,K} = \sup_{z \in K} |P(z)| \). We define the integer transfinite diameter of \( K \) by

\[
t_\mathbb{Z}(K) = \lim_{n \to \infty} \inf_{n \geq 1} \min_{P \in \mathbb{Z}[X], \deg P = n} |P|_{\infty,K}^{1/n}.
\]

For any \( n \geq 1 \) we say that a polynomial \( P_n \) (not always unique) is a Chebyshev polynomial if \( |P_n|_{\infty,K} = \min_{P \in \mathbb{Z}[X], \deg P = n} |P|_{\infty,K} \). It is known that, if \( K = [a, b] \) is a real interval of length \( b - a \geq 4 \), then \( t_\mathbb{Z}(K) = \frac{b-a}{4} \). However if \( b - a < 4 \), then \( t_\mathbb{Z}(K) < 1 \), but in this case the exact value of \( t_\mathbb{Z}(K) \) is not known. For more details see [BE].

4. Relations between auxiliary functions

and the integer transfinite diameter

If, inside the auxiliary function (2.1), we replace the real numbers \( e_j \) by rational numbers we may write

\[
f(x) = x - \frac{t}{h} \log |H(x)|,
\]

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 \( m \) (on \([0, \infty)\)) is as large as possible. That is to say, we seek a polynomial \( H \in \mathbb{Z}[X] \) such that

\[
\sup_{x > 0} |H(x)|^{t/h} e^{-x} \leq e^{-m}.
\]

Now, if we suppose that \( t \) is fixed, it is clear that we need an upper bound for the quantity

\[
t_\mathbb{Z,\varphi}([0, \infty)) = \lim_{h \to \infty} \inf_{H \in \mathbb{Z}[X], \deg H = h} \sup_{x > 0} |H(x)|^{t/h} \varphi(x),
\]

where we use the weight \( \varphi(x) = e^{-x} \) which allows us to define a weighted integer transfinite diameter of an infinite interval. In general, to get a good value for \( m \), we need a polynomial \( H \) of large degree \( h \) (about \( 10^8 \)), but it is not possible to compute a Chebyshev polynomial \( P_h \) of such a large degree \( h \). So we will proceed as follows.
For a fixed $t$, we can use Wu’s algorithm [WU] to compute a Chebyshev polynomial, or at least a polynomial whose norm is close to the minimal norm, of degree less than 40. We then use the irreducible factors of such a polynomial as polynomials $Q_j$ in the auxiliary function. Thus, in order to deal with the general situation, i.e. for varying $t$, we first take an initial value of $t$ (say $t_0 = 1$) and compute a polynomial $H$ of small degree (if possible less than 5). We define $Q_1$ as an irreducible factor of $H$ and we take the best value of $e_1$ to get the best auxiliary function $f_1$. We deduce from this the value of $t = t_1$ and we compute a new polynomial $H$ to get a new factor $Q_2$, and then we optimize the function $f_2$ with the two factors $Q_1$ and $Q_2$. We continue this process until the degree of $H$ becomes too large. For the optimization of the auxiliary function, we use a refinement of the semi-infinite linear programming method introduced into number theory by Smyth [SM]. This method (with the same auxiliary function) was used in [FGR] to prove that the list of Salem numbers $< 1.3$ and degree $\leq 40$ given by D. Boyd [BO1], [BO2] and M. Mossinghoff [MO] is complete.

5. An upper bound for $\deg P$.

Bounds for the $s_k$

a. We use the following auxiliary function:

\[
(5.1) \quad f(z) = -\log |z| - \sum_{1 \leq j \leq J} e_j \log |Q_j(z)|,
\]

where $Q_j(0) \neq 0$ for $1 \leq j \leq J$. The function $f$ is harmonic outside a union of small disks around the zeros of the polynomials $Q_j$, and so it takes its minimum in $E_1$ on the boundary of $E_1$. Let $m_0$ and $m_1$ be defined by $m_0 = \min_{-1 \leq x \leq 2} f(x)$ and $m_1 = \min_{z \in E_1} f(z)$. If $P$ is in $E_1$, of degree $d$ and roots $\alpha_1, \ldots, \alpha_d$, and does not divide any $Q_j$, then

\[
- \sum_{1 \leq i \leq d} \log |\alpha_i| \geq 2m_1 + (d - 2)m_0
\]

and

\[
|P(0)| \leq \exp(-2m_1 - (d - 2)m_0).
\]

In equation (5.1) and following the coefficients $e_j$ are chosen for each fixed $d$ to maximize $2m_1 + (d - 2)m_0$. Then we get the bounds given in Table 2 and, for $d \geq 13$, $|P(0)| < 1$, which is impossible. For $2 \leq d \leq 5$ we have used the trivial bounds of the modulus of the roots of $P$.

b. To get a lower bound for $s_k$ we take the auxiliary function:

\[
(5.2) \quad f(z) = \text{Re}(z^k) - \sum_{1 \leq j \leq J} e_j \log |Q_j(z)|
\]

and we obtain a lower bound for $s_k$ for $1 \leq k \leq d - 1$. For $b_d = P(0)$ we use Table 2. For the degree $d \leq 5$ we use the trivial function $f(z) = \text{Re}(z^k)$, and to obtain

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
\text{deg } P & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\
\hline
|P(0)| \leq & 4 & 7 & 12 & 15 & 19 & 22 & 22 & 17 & 9 & 4 & 1 \\
\hline
\end{array}
\]
upper bounds for \( s_k \) we replace \( \text{Re}(z^k) \) in (5.2) by \(-\text{Re}(z^k)\). If we suppose that \( b_1 = -s_1, \ldots, b_{k-1} \) are given, then Newton’s formula gives bounds for \( b_k \). We give in Table 3 the bounds for \( s_k \) in the case \( \deg P = 7 \), for \( 1 \leq k \leq 6 \).

The auxiliary functions of the type (5.2) use the polynomials \( P_1, \ldots, P_5 \) of Table 5 and the polynomials \( X + 2, X - 3, 2X - 1, 2X - 3, X^2 - 3X + 1, 2X^2 - 4X + 1 \) and \( X^3 - 4X^2 + 3X + 1 \).

c. When \( b_1, \ldots, b_k \) are known, we check whether the polynomial \( Q_k = P^{(d-k)} \) has the following properties:

- By the theorem of Gauss-Lucas all the roots of \( Q_k \) are inside the disk \(|z|^2 \leq \frac{17}{4}
- which contains the convex hull of \( E_1 \cup [-1, 2] \) where \( P \) has all its roots. We will use the Schur-Cohn algorithm \[MA\] for this.

- \( Q_k \) has at least \( k - 2 \) real roots in the real interval \([-1, 2]\). For this we use the Sturm algorithm \[MA\].

d. When we get a polynomial \( P \) (with \( \deg P > 2 \)), we check that \( P(2) > 0 \), \((-1)^dP(-1) > 0 \), \( P(0)P(1) \neq 0 \), and that \( P \) is not divisible by any of the polynomials \( X^2 + 1, X^2 + X + 1, X^2 - X + 1 \) or \( X^2 - X - 1 \), eliminating those \( P \) that fail any of these checks. Then we compute the roots of \( P \). We eliminate \( P \) when it has a root outside \( E_1 \cup [-1, 2] \). All these steps are done in Pascal. After that we use Pari \[GP\] to eliminate the reducible polynomials and we add the polynomials \((-1)^dP(1 - X)\) if they are not equal to \( P \).

For \( d > 7 \) we need further improvements of the method, because the computing times increase very quickly with \( d \).

6. IMPROVEMENTS OF THE METHOD WHEN \( \deg P \geq 8 \)

a. The cases \( \deg P = 8, 9 \).

In Section 5 we saw that, for \( \deg P \geq 8 \), \(|P(0)|\) is bounded by a decreasing function of \( d \). It is easy to see that this happens also for the upper bounds of \(|P(1)|\), \(|P(-1)|\) and \(|P(2)|\). We need to replace in (5.1) \(-\log |z| \) by \(-\log |z - 1|\), \(-\log |z + 1|\) and \(-\log |z - 2|\) respectively.

We obtain, for \( \deg P = 8 \),

\[ |P(0)| \leq 22, \quad |P(1)| \leq 26, \quad |P(-1)| \leq 88, \quad |P(2)| \leq 90. \]

These bounds are obtained from the more powerful relations:

\[
(6.1) \quad |P(0)|, |P(1)|^{0.192}, |P(-1)|^{0.187}, |P(2)|^{0.368} \leq 22.85, \\
(6.2) \quad |P(0)|^{0.137}, |P(1)|, |P(-1)|^{0.350}, |P(2)|^{0.133} \leq 26.062, \\
(6.3) \quad |P(0)|^{0.597}, |P(1)|^{0.883}, |P(-1)|, |P(2)|^{0.724} \leq 88.047, \\
(6.4) \quad |P(0)|^{1.051}, |P(1)|^{0.856}, |P(-1)|^{0.849}, |P(2)| \leq 90.38.
\]
Table 4.

<table>
<thead>
<tr>
<th>i</th>
<th>Polynomials $Q_{ij}$</th>
<th>Exponents $e_{ij}$</th>
<th>Upper bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_{10}$</td>
<td>1.90000, 0.19359, 0.18151, 0.35224, 0.30210, 2.22282</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>$P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_6$, $P_{11}$</td>
<td>0.13696, 1.00000, 0.35047, 0.13405, 0.17713, 26.06187</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>$P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_{12}$</td>
<td>0.49085, 0.83756, 1.00000, 0.64811, 0.29106, 85.18565</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>$P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_{13}$</td>
<td>0.06657, 0.01649, 85.18565</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>$P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_{14}$</td>
<td>1.05123, 0.85617, 0.84926, 1.00000, 0.46536, 52.81816</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>$P_1$, $P_2$, $P_3$, $P_4$, $P_5$, $P_{15}$</td>
<td>1.06128, 1.06128, 1.00000, 1.00000, 0.47634, 111.575</td>
<td></td>
</tr>
</tbody>
</table>

Table 5.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$d$</th>
<th>Coefficients of $P$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P_1$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$P_2$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$P_3$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$P_4$</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$P_5$</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>$P_6$</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$P_7$</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$P_8$</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$P_9$</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>$P_{10}$</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>$P_{11}$</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>$P_{12}$</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>$P_{13}$</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>$P_{14}$</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>$P_{15}$</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>$P_{16}$</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>$P_{17}$</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>$P_{18}$</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>$P_{19}$</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>$P_{20}$</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

But, if we replace in (5.1) the first term by $-\log |z(z-1)|$ and if we look at the coefficients $e_j$ of $\log |z+1|$ and $\log |z-2|$, we get the relation

$$ |P(0)P(1)| |P(-1)|^{0.722} |P(2)|^{0.713} \leq 52.82. $$

Using the same method we get the following inequality:

$$ |P(0)P(1)|^{1.061} |P(-1)P(2)| \leq 111.575. $$

The preceding six inequalities are obtained by the six auxiliary functions $f_i$ given in Table 4. They use the polynomials of Table 5.

Table 4 gives the auxiliary functions $f_i(z) = -\sum_{1 \leq j \leq i} e_{ij} \log |Q_{ij}(z)|$ used to obtain the previous inequalities (6.i) for $1 \leq i \leq 6$. The polynomials $Q_{ij}$ are taken from Table 5 hereafter.
Table 5 shows the polynomials $P$, with $d = \deg P$, used in the auxiliary functions of the type (5.2) and in Table 4.

Moreover, the values of $P(0)$, $P(1)$, $P(-1)$ and $P(2)$ are not independent because we have $P(2) - P(0) \equiv 0 \pmod{2}$ and $P(2) - P(-1) \equiv 0 \pmod{3}$, etc... More generally, for any $d = \deg P \geq 8$, we define the following linear forms:

$$f_d = P(0),$$
$$f_{d-1} = -\frac{1}{3} P(-1) - \frac{1}{2} P(0) + P(1) - \frac{1}{6} P(2),$$
$$f_{d-2} = \frac{1}{2} P(-1) - P(0) + \frac{1}{2} P(1),$$
$$f_{d-3} = -\frac{1}{6} P(-1) + \frac{1}{2} P(0) - \frac{1}{2} P(1) + \frac{1}{6} P(2).$$

These are linear forms in $b_0, \ldots, b_d$ with integer coefficients. For $1 \leq j \leq 3$, $f_{d-j}$ depends only on the coefficient $b_{d-j}$ (with the factor 1) and on the coefficients $b_0, \ldots, b_{d-4}$. If we add to the conditions (6.1), ..., (6.6) the conditions:

$P(0)P(1) \neq 0$, $(-1)^d P(-1) \geq 1$ and $P(2) \geq 1$, then, for $d = 8$, we get only 1000 different values for the vector $(P(-1), P(0), P(1), P(2))$ and also for the vector $(f_{d-3}, f_{d-2}, f_{d-1}, f_d)$. For the degree 9 case we get 332 different values.

Then for $d = 8$ (respectively $d = 9$) we use the algorithm of Section 5 to get possible values for the coefficients $b_0, \ldots, b_{d-4}$, and then we examine all the 1000 (respectively 332) possible values of $(f_{d-3}, f_{d-2}, f_{d-1}, f_d)$. Each of them gives a unique value of $(b_{d-3}, b_{d-2}, b_{d-1}, b_d)$, and we finish off the process as in Section 5.

b. The case $\deg P = 10$.

For degree 10 we get 100 vectors $(P(-1), P(0), P(1), P(2))$, but $b_6$ may take 61 different values and the computing time would be too large. However, we remark that in the auxiliary functions that occur when we compute the upper bounds as in (6.1) and (6.2), the coefficient of $\log|z^2 - z - 1|$ is rather large, i.e., greater than $1/2$. So we get a good upper bound of $|\text{Resultant}(P(X), X^2 - X - 1)|$. If $|P(0)P(1)P(-1)P(2)| \geq 16$, then the bound of the previous resultant is less than 1. Now 80 vectors remain. Of 68 of them the bound for the resultant is 1. For 8 the bound is 3. For the last 4 the bound for the resultant is 11 (so the possible values of the resultant, which are norms in $\mathbb{Z}$ of integers of the real quadratic field $\mathbb{Q}(\sqrt{5})$, are $\pm 1$, $\pm 4$, $\pm 5$, $\pm 9$, $\pm 11$). If we write $P(\sqrt{5}) = a + b \frac{1 + \sqrt{5}}{2}$, where $a$ and $b$ are integers in $\mathbb{Z}$, then Resultant$(P(X), X^2 - X - 1) = a^2 + ab - b^2$. Here $a$ and $b$ are linear forms depending on $b_0, \ldots, b_d$ with integer coefficients. For any vector we replace $b_{d-3}$, $b_{d-2}$, $b_{d-1}$, $b_d$ by their values as functions of $f_{d-3}$, $f_{d-2}$, $f_{d-1}$, $f_d$ and of $b_0, \ldots, b_{d-4}$. For any value of the resultant we get an equation of degree 2 in $b_{d-4}$ depending on the parameters $b_0, \ldots, b_{d-5}$, which are known by induction. If this equation has integral roots, we get a polynomial $P$ and we finish off as in Section 5.

c. The case $\deg P = 11$.

For degree 11 we get 16 vectors $(P(-1), P(0), P(1), P(2))$ and the resultant of $P(X)$ and $X^2 - X - 1$ takes only the values $\pm 1$. Nevertheless, to reduce the computing time, we proceed as follows. The numbers $s_k$ for $1 \leq k \leq d - 1$ are not “independent”. If we replace $\text{Re}(z^k)$ in (5.2) by $\pm (\text{Re}(z^k) + 2\text{Re}(z^{k-1}))$ we
Table 6.

<table>
<thead>
<tr>
<th>$k$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s_k$ ≥</td>
<td>0</td>
<td>2</td>
<td>−3</td>
<td>−8</td>
<td>−38</td>
<td>−84</td>
<td>−274</td>
</tr>
<tr>
<td>$s_k$ ≤</td>
<td>8</td>
<td>27</td>
<td>39</td>
<td>83</td>
<td>156</td>
<td>300</td>
<td>544</td>
</tr>
<tr>
<td>$s_k + 2s_{k−1}$ ≥</td>
<td>15</td>
<td>17</td>
<td>61</td>
<td>87</td>
<td>101</td>
<td>30</td>
<td></td>
</tr>
<tr>
<td>$s_k + 2s_{k−1}$ ≤</td>
<td>27</td>
<td>62</td>
<td>118</td>
<td>262</td>
<td>402</td>
<td>747</td>
<td></td>
</tr>
<tr>
<td>$s_k − s_{k−1}$ ≥</td>
<td>1</td>
<td>−18</td>
<td>−18</td>
<td>−18</td>
<td>−67</td>
<td>−100</td>
<td>−276</td>
</tr>
<tr>
<td>$s_k − s_{k−1}$ ≤</td>
<td>20</td>
<td>23</td>
<td>78</td>
<td>108</td>
<td>258</td>
<td>446</td>
<td></td>
</tr>
</tbody>
</table>

get bounds of $s_k + 2s_{k−1}$ for $2 ≤ k ≤ 6$ and $b_7, b_8, b_9, b_{10}, b_{11}$ are computed as for $\deg P = 10$.

d. The case $\deg P = 12$.

For degree 12 we get 4 vectors $(P(−1), P(0), P(1), P(2))$ and the resultant of $P(X)$ and $X^2 − X − 1$ has only the values ±1. But $b_7$ has 116 possible values. As in the previous case we get bounds for $s_k + 2s_{k−1}$ and also for $s_k − s_{k−1}$ for $2 ≤ k ≤ 7$. The results are given in Table 6.

Table 6 shows that, for $2 ≤ k ≤ 7$, $s_k$ and $s_{k−1}$ cannot be simultaneously too close to their upper or lower bounds. Lines 2 and 3 give the lower and upper bounds for $s_k$. Lines 4 and 5 give the lower and upper bounds for $s_k + 2s_{k−1}$ and lines 6 and 7 for $s_k − s_{k−1}$. From lines 2 and 3 we get $−160 ≤ s_6 + 2s_5 ≤ 612$ but lines 4 and 5 give $101 ≤ s_6 + 2s_5 ≤ 402$. From lines 2 and 3 we get $−240 ≤ s_6 − s_5 ≤ 338$ but lines 6 and 7 give $−100 ≤ s_6 − s_5 ≤ 258$.

We also get upper bounds of 8978 for $|P(\frac{1+i\sqrt{7}}{2})|^2 = \text{Resultant}(P(X), X^2 − X + 1)$ and of 51355 for $|P(i)|^2 = \text{Resultant}(P(X), X^2 + 1)$. We write $P(\frac{1+i\sqrt{7}}{2}) = A + B\frac{1+i\sqrt{7}}{2}, P(i) = C + Di$ and we define the following linear forms:

\[ f_d = -\frac{1}{3}A + \frac{1}{10}C + \frac{1}{5}D - \frac{1}{36}P(-1) + \frac{1}{2}P(0) - \frac{1}{4}P(1) + \frac{1}{90}P(2), \]

\[ f_d = -\frac{1}{3}A + \frac{1}{10}C - \frac{1}{5}D + \frac{1}{36}P(-1) - \frac{1}{4}P(1) + \frac{1}{45}P(2), \]

\[ f_d = -\frac{1}{3}A - \frac{1}{18}P(-1) + \frac{1}{2}P(0) - \frac{1}{2}P(1) + \frac{1}{18}P(2). \]

Each $f_{d,j}$ is a linear form in $b_0, \ldots, b_{d−j}$ with integer coefficients. We get the following bounds: $|f_5| ≤ 87, |f_6| ≤ 87$ and $|f_7| ≤ 37$. These give bounds for $b_5, b_6$ and $b_7$ respectively. We add all these conditions into the program and finish off the computation as before.

References


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

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