A GEL’FOND TYPE CRITERION IN DEGREE TWO

BENOIT ARBOUR AND DAMIEN ROY

1. Introduction

Let $\xi$ be any real number and let $n$ be a positive integer. Defining the height $H(P)$ of a polynomial $P$ as the largest absolute value of its coefficients, an application of Dirichlet box principle shows that, for any real number $X \geq 1$, there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ of degree at most $n$ and height at most $X$ which satisfies

$$|P(\xi)| \leq cX^{-n}$$

for some suitable constant $c > 0$ depending only on $\xi$ and $n$. Conversely, Gel’fond’s criterion implies that there are constants $\tau = \tau(n)$ and $c = c(\xi, n) > 0$ with the property that if, for any real number $X \geq 1$, there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ with

$$\deg(P) \leq n, \quad H(P) \leq X \quad \text{and} \quad |P(\xi)| \leq cX^{-\tau}$$

then $\xi$ is algebraic over $\mathbb{Q}$ of degree at most $n$. For example, Brownawell’s version of Gel’fond’s criterion in [1] implies that the above statement holds with any $\tau > 3n$, and the more specific version proved by Davenport and Schmidt as Theorem 2b of [4] shows that it holds with $\tau = 2n - 1$. On the other hand, the above application of Dirichlet box principle implies $\tau \geq n$. So, if we denote by $\tau_n$ the infimum of all admissible values of $\tau$ for a fixed $n \geq 1$, then we have $\tau_1 = 1$ and, in general

$$n \leq \tau_n \leq 2n - 1.$$

In the case of degree $n = 2$, the study of a specific class of transcendental real numbers in [6] provides the sharper lower bound $\tau_2 \geq \gamma^2$ where $\gamma = (1 + \sqrt{5})/2$ denotes the golden ratio (see Theorem 1.2 of [6]). Our main result below shows that we in fact have $\tau_2 = \gamma^2$ by establishing the reverse inequality $\tau_2 \leq \gamma^2$:

**Theorem.** Let $\xi \in \mathbb{C}$. Assume that for any sufficiently large positive real number $X$ there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ of degree at most 2 and height at most $X$ such that

$$|P(\xi)| \leq \frac{1}{4}X^{-\gamma^2}$$

Then $\xi$ is algebraic over $\mathbb{Q}$ of degree at most 2.

---

1991 Mathematics Subject Classification. Primary 11J13; Secondary 11J82.

Work partially supported by NSERC and CICMA.
Comparing this statement with Theorem 1.2 of [6], we see that it is optimal up to the value of the multiplicative constant $1/4$ in (1). Although we do not know the best possible value for this constant, our argument will show that it can be replaced by any real number $c$ with $0 < c < c_0 = (6 \cdot 2^{1/4})^{-1} \approx 0.253$. As the reader will note, our proof, given in Section 3 below, has the same general structure as the proof of the main result of [3] and the proof of Theorem 1a of [4].

Following the method of Davenport and Schmidt in [4] combined with ideas from [2] and [7], we deduce the following result of simultaneous approximation of a real number by conjugate algebraic numbers:

**Corollary.** Let $\xi$ be a real number which is not algebraic over $\mathbb{Q}$ of degree at most 2. Then, there are arbitrarily large real numbers $Y \geq 1$ for which there exist an irreducible monic polynomial $P \in \mathbb{Z}[T]$ of degree 3 and an irreducible polynomial $Q \in \mathbb{Z}[T]$ of degree 2, both of which have height at most $Y$ and admit at least two distinct real roots whose distance to $\xi$ is at most $cY^{-(3-\gamma)/2}$, with a constant $c$ depending only on $\xi$.

The proof of this corollary is postponed to Section 4 below.

## 2. Preliminaries

We collect here several lemmas which we will need in the proof of the theorem. The first one is a special case of the well-known Gel’fond’s lemma for which we computed the optimal values of the constants.

**Lemma 1.** Let $L, M \in \mathbb{C}[T]$ be polynomials of degree at most 1. Then we have

$$\frac{1}{\gamma} H(L)H(M) \leq H(LM) \leq 2H(L)H(M).$$

The second result is an estimate for the resultant of two polynomials of small degree.

**Lemma 2.** Let $m, n \in \{1, 2\}$, and let $P$ and $Q$ be non-zero polynomials in $\mathbb{Z}[T]$ with $\deg(P) \leq m$ and $\deg(Q) \leq n$. Then, for any complex number $\xi$, we have

$$|\operatorname{Res}(P, Q)| \leq H(P)^nH(Q)^m\left(c(m, n)\frac{|P(\xi)|}{H(P)} + c(n, m)\frac{|Q(\xi)|}{H(Q)}\right)$$

where $c(1, 1) = 1$, $c(1, 2) = 3$, $c(2, 1) = 1$ and $c(2, 2) = 6$.

The proof of the above statement is easily reduced to the case where $\deg(P) = m$ and $\deg(Q) = n$. The conclusion then follows by writing $\operatorname{Res}(P, Q)$ as a Sylvester’s determinant and by arguing as Brownawell in the proof of lemma 1 of [3] to estimate this determinant.

The third lemma may be viewed, for example, as a special case of Lemma 13 of [5].
Lemma 3. Let $P, Q \in \mathbb{Z}[T]$ be non-zero polynomials of degree at most 2 with greatest common divisor $L \in \mathbb{Z}[T]$ of degree 1. Then, for any complex number $\xi$, we have

$$H(L)|L(\xi)| \leq \gamma (H(P)|Q(\xi)| + H(Q)|P(\xi)|).$$

Proof. The quotients $P/L$ and $Q/L$ being relatively prime polynomials of $\mathbb{Z}[T]$, their resultant is a non-zero integer. Applying Lemma 2 with $m = n = 1$ and using Lemma 1, we then deduce, if $L(\xi) \neq 0$,

$$1 \leq |\text{Res}(P/L, Q/L)| \leq H(P/L)|Q(L)| + H(Q/L)|P(L)| \leq \frac{H(P)}{H(L)}|Q(\xi)| + \frac{H(Q)}{H(L)}|P(\xi)|.$$

Lemma 4. Let $\xi \in \mathbb{C}$ and let $P, Q, R \in \mathbb{C}[T]$ be arbitrary polynomials of degree at most 2. Then, writing the coefficients of these polynomials as rows of a $3 \times 3$ matrix, we have

$$|\det(P, Q, R)| \leq 2H(P)H(Q)H(R)\left(\frac{|P(\xi)|}{H(P)} + \frac{|Q(\xi)|}{H(Q)} + \frac{|R(\xi)|}{H(R)}\right).$$

This above statement follows simply by observing, as in the proof ofLemma 4 of [3], that the determinant of the matrix does not change if, in this matrix, we replace the constant coefficients of $P, Q$ and $R$ by the values of these polynomials at $\xi$.

We also construct a sequence of “minimal polynomials” similarly as it is done in §3 of [3]:

Lemma 5. Let $\xi \in \mathbb{C}$ with $[Q(\xi) : \mathbb{Q}] > 2$. Then there exists a strictly increasing sequence of positive integers $(X_i)_{i \geq 1}$ and a sequence of non-zero polynomials $(P_i)_{i \geq 1}$ in $\mathbb{Z}[T]$ of degree at most 2 such that, for each $i \geq 1$, we have:

- $H(P_i) = X_i$,
- $|P_{i+1}(\xi)| < |P_{i}(\xi)|$,
- $|P_{i}(\xi)| \leq |P_{i}(\xi)|$ for all $P \in \mathbb{Z}[T]$ with $\deg(P) \leq 2$ and $0 < H(P) < X_{i+1}$,
- $P_i$ and $P_{i+1}$ are linearly independent over $\mathbb{Q}$.

Proof. For each positive integer $X$, define $p_X$ to be the smallest value of $|P(\xi)|$ where $P \in \mathbb{Z}[T]$ is a non-zero polynomial of degree $\leq 2$ and height $\leq X$. This defines a non-decreasing sequence $p_1 \geq p_2 \geq p_3 \geq \ldots$ of positive real numbers converging to 0. Consider the sequence $X_1 < X_2 < \ldots$ of indices $X \geq 2$ for which $p_{X-1} > p_X$. For each $i \geq 1$, there exists a polynomial $P_i \in \mathbb{Z}[T]$ of degree $\leq 2$ and height $X_i$ with $|P_i(\xi)| = p_i$. The sequences $(X_i)_{i \geq 1}$ and $(P_i)_{i \geq 1}$ clearly satisfy the first three conditions. The last condition follows from the fact that the polynomials $P_i$ are primitive of distinct height. \qed
**Lemma 6.** Assume, in the notation of Lemma 4, that
\[ \lim_{i \to \infty} X_{i+1} |P_i(\xi)| = 0. \]
Then there exist infinitely many indices \( i \geq 2 \) for which \( P_{i-1}, P_i \) and \( P_{i+1} \) are linearly independent over \( \mathbb{Q} \).

**Proof.** Assume on the contrary that \( P_{i-1}, P_i \) and \( P_{i+1} \) are linearly dependent over \( \mathbb{Q} \) for all \( i \geq i_0 \). Then the subspace \( V \) of \( \mathbb{Q}[T] \) generated by \( P_{i-1} \) and \( P_i \) is independent of \( i \) for \( i \geq i_0 \). Let \( \{P, Q\} \) be a basis of \( V \cap \mathbb{Z}^3 \). Then, for each \( i \geq i_0 \), we can write
\[ P_i = a_i P + b_i Q \]
for some integers \( a_i \) and \( b_i \) of absolute value at most \( cX_i \), with a constant \( c > 0 \) depending only on \( P \) and \( Q \). Since \( P_i \) and \( P_{i+1} \) are linearly independent, we get
\[ 1 \leq \left| \begin{array}{cc} a_i & b_i \\ a_{i+1} & b_{i+1} \end{array} \right| = \frac{|a_i P_{i+1}(\xi) - a_{i+1} P_i(\xi)|}{|Q(\xi)|} \leq \frac{2c}{|Q(\xi)|} X_{i+1} |P_i(\xi)| \]
in contradiction with the hypothesis as we let \( i \) tend to infinity. \( \square \)

3. **Proof of the theorem**

Let \( c \) be a positive real number and let \( \xi \) be a complex number with \( |Q(\xi) : \mathbb{Q}| > 2 \). Assume that, for any sufficiently large real number \( X \), there exists a non-zero polynomial \( P \in \mathbb{Z}[T] \) of degree \( \leq 2 \) and height \( \leq X \) with \( |P(\xi)| \leq cX^{-\gamma}2 \). We will show that these conditions imply \( c \geq c_0 = (6 \cdot 2^{1/\gamma})^{-1/\gamma} > 1/4 \), thereby proving the theorem.

Let \( c_1 \) be an arbitrary real number with \( c_1 > c \). By virtue of our hypotheses, the sequences \( (X_i)_{i \geq 1} \) and \( (P_i)_{i \geq 1} \) given by Lemma 4 satisfy
\[ |P_i(\xi)| \leq cX_{i+1}^{-\gamma}2 \]
for any sufficiently large \( i \). Then, by Lemma 4, there exists infinitely many \( i \) such that \( P_{i-1}, P_i \) and \( P_{i+1} \) are linearly independent. For such an index \( i \), the determinant of these three polynomials is a non-zero integer and, applying Lemma 4, we deduce
\[ 1 \leq |\det(P_{i-1}, P_i, P_{i+1})| \leq 2X_{i-1} X_i X_{i+1} \left( \frac{|P_{i-1}(\xi)|}{X_{i-1}} + \frac{|P_i(\xi)|}{X_i} + \frac{|P_{i+1}(\xi)|}{X_{i+1}} \right) \leq 2cX_i^{-\gamma} X_{i+1} + 4cX_{i+1}^{1-\gamma}. \]
Assuming that \( i \) is sufficiently large, this implies
\[ X_i^\gamma \leq 2c_1 X_{i+1}. \]

(2)

Suppose first that \( P_i \) and \( P_{i+1} \) are not relatively prime. Then, their greatest common divisor is an irreducible polynomial \( L \in \mathbb{Z}[T] \) of degree 1, and Lemma 4 gives
\[ H(L)|L(\xi)| \leq \gamma \left( X_i |P_{i+1}(\xi)| + X_{i+1} |P_i(\xi)| \right) \leq 2\gamma cX_{i+1}^{-\gamma}. \]

(3)
Since \( P_{i-1}, P_i \) and \( P_{i+1} \) are linearly independent, the polynomial \( L \) does not divide \( P_{i-1} \) and so the resultant of \( P_{i-1} \) and \( L \) is a non-zero integer. Applying Lemma 2 then gives

\[
1 \leq |\text{Res}(P_{i-1}, L)| \leq H(P_{i-1})H(L)^2 \left( \frac{|P_{i-1}(\xi)|}{H(P_{i-1})} + 3\frac{|L(\xi)|}{H(L)} \right)
\]

\[
\leq cX_i^{-\gamma^2}H(L)^2 + 3X_{i-1}H(L)|L(\xi)|.
\]

Combining this with (3) and with the estimate \( H(L) \leq \gamma H(P_i) \leq \gamma X_i \) coming from Lemma 4 we conclude that, in this case, the index \( \gamma \) of polynomials of degree at most 2 in \( \mathbb{R} \) and therefore their resultant is a non-zero integer. Using Lemma 2 we then find

\[
1 \leq |\text{Res}(P_i, P_{i+1})| \leq 6X_iX_{i+1} \left( cX_iX_{i+2}^{-\gamma^2} + cX_{i+1}^{-\gamma} \right) \leq 6c_1X_iX_{i+1}^{1-\gamma}
\]

since from (2), we have \( cX_i \leq (c_1 - c)X_{i+1} \) for large \( i \). Using (2) again, this implies

\[
1 \leq 6c_1(2c_1)^{1/\gamma}
\]

and thus, \( c_1 \geq c_0 = (6 \cdot 2^{1/\gamma})^{-1/\gamma} \). The choice of \( c_1 > c \) being arbitrary, this shows that \( c \geq c_0 \) as announced.

4. Proof of the corollary

Let \( \xi \) be as in the statement of the corollary and let \( V \) denote the real vector space of polynomials of degree at most 2 in \( \mathbb{R}[T] \). It follows from the theorem that there exist arbitrarily large real numbers \( X \) for which the convex body \( C(X) \) of \( V \) defined by

\[
C(X) = \{ P \in V ; |P(\xi)| \leq (1/4)X^{-\gamma^2}, |P'(\xi)| \leq c_1X \text{ and } |P''(\xi)| \leq c_1X \}
\]

with \( c_1 = (1 + |\xi|^2)^{-2} \) contains no non-zero integral polynomial. By Proposition 3.5 of [1] (a version of Mahler’s theorem on polar reciprocal bodies), this implies that there exists a constant \( c_2 > 1 \) such that, for the same values of \( X \), the convex body

\[
C^*(X) = \{ P \in V ; |P(\xi)| \leq c_2X^{-1}, |P'(\xi)| \leq c_2X^{-1} \text{ and } |P''(\xi)| \leq c_2X^{\gamma^2} \}
\]

contains a basis of the lattice of integral polynomials in \( V \).

Fix such an \( X \) with \( X \geq 1 \), and let \( \{ P_1, P_2, P_3 \} \subset C^*(X) \) be a basis of \( V \cap \mathbb{Z}[T] \). We now argue as in the proof of Proposition 9.1 of [7]. We put

\[
B(T) = T^2 - 1, \quad r = X^{-(1+\gamma^2)/2} \quad \text{and} \quad s = 20c_2X^{-1},
\]

and observe that any polynomial \( S \in V \) with \( H(S - B) < 1/3 \) admits at least two real roots in the interval \([-2, 2]\) as such a polynomial takes positive values at \( \pm 2 \) and a negative value at 0. We also note that, since \( P_i \in C^*(X) \), we have

\[
H(P_i(rT + \xi)) \leq c_2X^{-1}, \quad (i = 1, 2, 3).\]

Since \( \{P_1, P_2, P_3\} \) is a basis of \( V \) over \( \mathbb{R} \), we may write
\[
(T - \xi)^3 + sB\left(\frac{T - \xi}{r}\right) = T^3 + \sum_{i=1}^{3} \theta_i P_i(T) \quad \text{and} \quad sB\left(\frac{T - \xi}{r}\right) = \sum_{i=1}^{3} \eta_i P_i(T)
\]
for some real numbers \( \theta_1, \theta_2, \theta_3 \) and \( \eta_1, \eta_2, \eta_3 \). For \( i = 1, 2, 3 \), choose integers \( a_i \) and \( b_i \) with \( |a_i - \theta_i| \leq 2 \) and \( |b_i - \eta_i| \leq 2 \) so that the polynomials
\[
P(T) = T^3 + \sum_{i=1}^{3} a_i P_i(T) \quad \text{and} \quad Q(T) = \sum_{i=1}^{3} b_i P_i(T)
\]
are respectively congruent to \( T^3 + 2 \) and \( T^2 + 2 \) modulo 4. Then, by Eisenstein’s criterion, \( P \) and \( Q \) are irreducible polynomials of \( \mathbb{Z}[T] \). Moreover, we find
\[
H(s^{-1} P(rT + \xi) - B(T)) = s^{-1} H\left((rT)^3 + \sum_{i=1}^{3} (a_i - \theta_i) P_i(rT + \xi)\right)
\]
\[
\leq s^{-1} \ max\{r^3, 6\gamma c_2 X^{-1}\}
\]
\[
< 1/3.
\]
Then, \( P(rT + \xi) \) has at least two distinct real roots in the interval \([-2, 2]\) and so \( P \) has at least two real roots whose distance to \( \xi \) are at most \( 2r \). A similar but simpler computation shows that the same is true of the polynomial \( Q \). Finally, the above estimate implies \( H(P(rT + \xi)) \leq 4s/3 \) and so \( H(P) \leq c_3 X^{\gamma^2} \) for some constant \( c_3 > 0 \), and the same for \( Q \). These polynomials thus satisfy the conclusion of the corollary with \( Y = c_3 X^{\gamma^2} \) and an appropriate choice of \( c \).

References

[1] Brownawell, W. D., Sequences of diophantine approximations, J. Number Theory 6 (1974), 11-21.
[2] Bugeaud, Y., Teulié, O., Approximation d’un nombre réel par des nombres algébriques de degré donné, Acta Arith. 93 (2000), 77-86.
[3] Davenport, H., Schmidt, W. M., Approximation to real numbers by quadratic irrationals, Acta Arith. 13 (1967), 169-176.
[4] Davenport, H., Schmidt, W. M., Approximation to real numbers by algebraic integers, Acta Arith. 15 (1969), 393-416.
[5] Laurent, M., Roy, D., Criteria of algebraic independence with multiplicities and interpolation determinants, Trans. Amer. Math. Soc. 351 (1999), 1845–1870.
[6] Roy, D., Approximation to real numbers by cubic algebraic integers I, Proc. London Math. Soc., (to appear), 22 pages, [arXiv:math.NT/0210181]
[7] Roy, D., Waldschmidt, M., Diophantine approximation by conjugate algebraic integers, Compositio Math., (to appear), 31 pages, [arXiv:math.NT/0207102]