ACTA ARITHMETICA
111.1 (2004)

A Gel'fond type criterion in degree two

by

Benoit Arbour (Montréal) and Damien Roy (Ottawa)

1. Introduction. Let ξ 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 the Dirichlet box principle shows that, for any real number $X \ge 1$, there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ of degree at most n and height at most X which satisfies

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

for some suitable constant $c > 0$ depending only on ξ 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 $X \ge 1$, there exists a non-zero polynomial $P \in \mathbb{Z}[T]$ with

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

then ξ 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 the Dirichlet box principle implies $\tau \ge n$. So, if we denote by τ_n the infimum of all admissible values of τ for a fixed $n \ge 1$, then we have $\tau_1 = 1$ and, in general,

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

In the case of degree $n = 2$, the study of a specific class of transcendental real numbers in [6] provides the sharper lower bound $\tau_2 \ge \gamma^2$ 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 $\tau_2 \le \gamma^2$:

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

2000 *Mathematics Subject Classification*: Primary 11J13; Secondary 11J82.
Work partially supported by NSERC and CICMA.

and height at most X *such that*

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

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

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 $0 < c < c_0 = (6 \cdot 2^{1/\gamma})^{-1/\gamma} \cong 0.253$. 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 on simultaneous approximation of a real number by conjugate algebraic numbers:

Corollary. *Let* ξ *be a real number which is not algebraic over* $\mathbb{Q}$ *of degree at most* 2. *Then there are arbitrarily large real numbers* $Y \ge 1$ *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* ξ *is at most* $cY^{-(3-\gamma)/2}$, *with a constant* c *depending only on* ξ.

The proof of this corollary is postponed to Section 4.

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*

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

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* $\deg(P) \le m$ *and* $\deg(Q) \le n$. *Then, for any complex number* ξ,

$$|\mathrm{Res}(P,Q)| \le H(P)^n H(Q)^m \Big(c(m,n)\,\frac{|P(\xi)|}{H(P)} + c(n,m)\,\frac{|Q(\xi)|}{H(Q)} \Big)$$

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

$\mathrm{Res}(P,Q)$ as a Sylvester determinant and by arguing as Brownawell in the proof of Lemma 1 of [1] 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 ξ, we have*

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

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 $L(\xi) \neq 0$,

$$\begin{aligned} 1 \le |\mathrm{Res}(P/L, Q/L)| &\le H(P/L)|(Q/L)(\xi)| + H(Q/L)|(P/L)(\xi)| \\ &\le \gamma\,\frac{H(P)}{H(L)}\,\frac{|Q(\xi)|}{|L(\xi)|} + \gamma\,\frac{H(Q)}{H(L)}\,\frac{|P(\xi)|}{|L(\xi)|}. \ \blacksquare \end{aligned}$$

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 3×3 matrix, we have*

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

The above statement follows simply by observing, as in the proof of Lemma 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 ξ.

We also construct a sequence of "minimal polynomials" similarly to §3 of [3]:

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

- $H(P_i) = X_i$,
- $|P_{i+1}(\xi)| < |P_i(\xi)|$,
- $|P_i(\xi)| \le |P(\xi)|$ *for all* $P \in \mathbb{Z}[T]$ *with* $\deg(P) \le 2$ *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 ≤ 2 and height $\le X$. This defines a non-decreasing sequence $p_1 \ge p_2 \ge \ldots$ of positive real numbers converging to 0. Consider the sequence $X_1 < X_2 < \ldots$ of indices $X \ge 2$ for which $p_{X-1} > p_X$. For each $i \ge 1$, there exists a polynomial $P_i \in$

$\mathbb{Z}[T]$ of degree ≤ 2 and height X_i with $|P_i(\xi)| = p_{X_i}$. The sequences $(X_i)_{i\ge1}$ and $(P_i)_{i\ge1}$ clearly satisfy the first three conditions. The last condition follows from the fact that the polynomials P_i are primitive of distinct height. ∎

Lemma 6. *Assume, in the notation of Lemma* 5, *that*

$$\lim_{i\to\infty} X_{i+1}|P_i(\xi)| = 0.$$

Then there exist infinitely many indices $i \ge 2$ 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 $i \ge i_0$. Then the subspace V of $\mathbb{Q}[T]$ generated by P_{i-1} and P_i is independent of i for $i \ge i_0$. Let $\{P, Q\}$ be a basis of $V \cap \mathbb{Z}^3$. Then, for each $i \ge i_0$, 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

$$1 \le \left\| \begin{matrix} a_i & b_i \\ a_{i+1} & b_{i+1} \end{matrix} \right\| = \frac{|a_i P_{i+1}(\xi) - a_{i+1} P_i(\xi)|}{|Q(\xi)|} \le \frac{2c}{|Q(\xi)|} X_{i+1}|P_i(\xi)|$$

in contradiction with the hypothesis as we let i tend to infinity. ∎

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

Let c_1 be an arbitrary real number with $c_1 > c$. By our hypotheses, the sequences $(X_i)_{i\ge1}$ and $(P_i)_{i\ge1}$ given by Lemma 5 satisfy

$$|P_i(\xi)| \le cX_{i+1}^{-\gamma^2}$$

for any sufficiently large i. Then, by Lemma 6, there exist 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

$$\begin{aligned} 1 \le |\det(P_{i-1}, P_i, P_{i+1})| &\le 2X_{i-1}X_iX_{i+1}\left(\frac{|P_{i-1}(\xi)|}{X_{i-1}} + \frac{|P_i(\xi)|}{X_i} + \frac{|P_{i+1}(\xi)|}{X_{i+1}}\right) \\ &\le 2cX_i^{-\gamma}X_{i+1} + 4cX_{i+1}^{1-\gamma}. \end{aligned}$$

Assuming that i is sufficiently large, this implies

$$X_i^{\gamma} \le 2c_1 X_{i+1}. \tag{2}$$

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 3 gives

$$H(L)|L(\xi)| \le \gamma(X_i|P_{i+1}(\xi)| + X_{i+1}|P_i(\xi)|) \le 2\gamma c X_{i+1}^{-\gamma}. \tag{3}$$

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

$$\begin{aligned} 1 \le |\mathrm{Res}(P_{i-1}, L)| &\le H(P_{i-1})H(L)^2\left(\frac{|P_{i-1}(\xi)|}{H(P_{i-1})} + 3\,\frac{|L(\xi)|}{H(L)}\right) \\ &\le cX_i^{-\gamma^2}H(L)^2 + 3X_{i-1}H(L)|L(\xi)|. \end{aligned}$$

Combining this with (3) and with the estimate $H(L) \le \gamma H(P_i) \le \gamma X_i$ coming from Lemma 1, we conclude that, in this case, the index i is bounded.

Thus, assuming that i is sufficiently large, the polynomials P_i and P_{i+1} are relatively prime and therefore their resultant is a non-zero integer. Using Lemma 2 we then find

$$1 \le |\mathrm{Res}(P_i, P_{i+1})| \le 6X_iX_{i+1}(cX_iX_{i+2}^{-\gamma^2} + cX_{i+1}^{-\gamma}) \le 6c_1X_iX_{i+1}^{1-\gamma}$$

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

$$1 \le 6c_1(2c_1)^{1/\gamma},$$

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

4. Proof of the Corollary. Let ξ 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 $\mathcal{C}(X)$ of V defined by

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

with $c_1 = (1 + |\xi|)^{-2}$ contains no non-zero integral polynomial. By Proposition 3.5 of [7] (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

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

contains a basis of the lattice of integral polynomials in V.

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

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

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 ± 2 and a negative value at 0. We also note that, since $P_i \in \mathcal{C}^*(X)$, we have

$$H(P_i(rT + \xi)) \le c_2 X^{-1} \quad (i = 1, 2, 3).$$

Since $\{P_1, P_2, P_3\}$ is a basis of V over $\mathbb{R}$, we may write

$$(T - \xi)^3 + sB\left(\frac{T - \xi}{r}\right) = T^3 + \sum_{i=1}^{3} \theta_i P_i(T), \qquad sB\left(\frac{T - \xi}{r}\right) = \sum_{i=1}^{3} \eta_i P_i(T)$$

for some real numbers $\theta_1, \theta_2, \theta_3$ and η_1, η_2, η_3. For $i = 1, 2, 3$, choose integers a_i and b_i with $|a_i - \theta_i| \le 2$ and $|b_i - \eta_i| \le 2$ 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

$$\begin{aligned} H(s^{-1}P(rT + \xi) - B(T)) &= s^{-1} H\Big((rT)^3 + \sum_{i=1}^{3} (a_i - \theta_i) P_i(rT + \xi)\Big) \\ &\le s^{-1} \max\{r^3, 6c_2 X^{-1}\} < 1/3. \end{aligned}$$

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 ξ is at most $2r$. A similar but simpler computation shows that the same is true of the polynomial Q. Finally, the above estimate implies $H(P(rT + \xi)) \le 4s/3$ and so $H(P) \le c_3 X^{\gamma^2}$ 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] W. D. Brownawell, *Sequences of diophantine approximations*, J. Number Theory 6 (1974), 11–21.

[2] Y. Bugeaud et O. Teulié, *Approximation d'un nombre réel par des nombres algébriques de degré donné*, Acta Arith. 93 (2000), 77–86.

[3] H. Davenport and W. M. Schmidt, *Approximation to real numbers by quadratic irrationals*, ibid. 13 (1967), 169–176.

[4] —, —, *Approximation to real numbers by algebraic integers*, ibid. 15 (1969), 393–416.

[5] M. Laurent and D. Roy, *Criteria of algebraic independence with multiplicities and interpolation determinants*, Trans. Amer. Math. Soc. 351 (1999), 1845–1870.

[6] D. Roy, *Approximation to real numbers by cubic algebraic integers I*, Proc. London Math. Soc., to appear; arXiv:math.NT/0210181.

[7] D. Roy and M. Waldschmidt, *Diophantine approximation by conjugate algebraic integers*, Compositio Math., to appear; arXiv:math.NT/0207102.

Department of Mathematics
McGill University
805 Sherbrooke Ouest
Montréal, Québec H3A 2K6, Canada
E-mail: arbour@math.mcgill.ca

Département de Mathématiques
Université d'Ottawa
585 King Edward
Ottawa, Ontario K1N 6N5, Canada
E-mail: droy@uottawa.ca

Received on 3.1.2003 (4436)