ON THE DISTANCE BETWEEN ROOTS OF
INTEGER POLYNOMIALS

YANN BUGEAUD AND MAURICE MIGNOTTE

Université Louis Pasteur, UFR de Mathématiques,
7, rue René Descartes, 67084 Strasbourg Cedex, France
(bugeaud@math.u-strasbg.fr; mignotte@math.u-strasbg.fr)

Abstract   We study families of integer polynomials having roots very close to each other.

1. Introduction

In this paper we denote by $H(P)$ the naive height of an integer polynomial $P(X)$, that is, the maximum of the absolute values of its coefficients. In transcendental number theory, lower estimates for the distance between two algebraic numbers are often needed. A classical result is the so-called *Liouville inequality* (see, for example, [3], a slightly weaker estimate being proved in [5]).

Theorem A. *Let $P(X)$ and $Q(X)$ be non-constant integer polynomials of degree n and m, respectively. Denote by α a zero of $P(X)$ and by β a zero of $Q(X)$. Assuming that $P(\beta) \neq 0$, we have*

$$|\alpha - \beta| \geqslant 2^{1-n}(n+1)^{(1/2)-m}(m+1)^{-n/2}H(P)^{-m}H(Q)^{-n}. \qquad (1.1)$$

Sharp lower bounds for the distance between two roots of a given integer polynomial turn out to be very useful. The first inequality of Theorem B is due to Mahler [7], while the second one is folklore (see, for example, [9]).

Theorem B. *Let $P(X)$ be a separable polynomial with integer coefficients of degree $n \geqslant 2$. For any two distinct zeros α and β of $P(X)$ we have*

$$|\alpha - \beta| \geqslant \sqrt{3}(n+1)^{-(2n+1)/2}H(P)^{-n+1}. \qquad (1.2)$$

Furthermore, if $\alpha_1, \ldots, \alpha_k$ are distinct zeros of $P(X)$, then there exists a positive, effective constant $c_1(n)$ such that

$$\prod_{1 \leqslant i < j \leqslant k} |\alpha_i - \alpha_j| \geqslant c_1(n)H(P)^{-n+1}. \qquad (1.3)$$

553

It is natural to ask whether the lower bounds in Theorems A and B are best possible. Up to now, it is known that the factor $H(P)^{-n+1}$ in (1.2) cannot be replaced by a term larger than $H(P)^{-n/4}$. To show this, it is sufficient to observe that, for any integers a and n with $n \geqslant 3$ and $a \geqslant 10$, the polynomial $X^n - 2(aX - 1)^2$ has two roots approximately $a^{-n/2}$ apart, that is, approximately $H(P)^{-n/4}$ apart (see, for example, [8]).

In the present paper, we prove that Theorem A is optimal and that (1.3) is nearly best possible. Furthermore, we show that the term $H(P)^{-n+1}$ in (1.2) cannot be replaced by a factor larger than $H(P)^{-n/2}$.

2. Results

The purpose of the present note is to establish the following statement.

Theorem. *Inequality (1.1) is best possible in terms of the heights of the polynomials $P(X)$ and $Q(X)$. In inequality (1.2), the exponent of $H(P)$ cannot be replaced by a real number strictly greater than $-n/2$. In inequality (1.3), the exponent of $H(P)$ cannot be replaced by a real number strictly greater than $-n(k-1)/k$.*

To prove the last two assertions of our Theorem, we consider the family of polynomials

$$P_{a,n,k}(X) := (X^n - aX + 1)^k - 2X^{nk-k}(aX - 1)^k,$$

where a, n and k are positive integers with $a \geqslant 10$, $n \geqslant 3$ and $k \geqslant 2$. Using methods of Laurent and Poulakis [6] or Theorem 4.4 of Müller [10], it is possible to prove that these polynomials are irreducible if a is large in terms of n and k. Indeed, performing the change of variables $\alpha = 1/a$, $Y = aX$ in the absolutely irreducible curve

$$F_{n,k}(a, X) = X^n - aX + 1 - \sqrt[k]{2}X^{n-1}(aX - 1) = 0,$$

defined over the field $\boldsymbol{Q}(\sqrt[k]{2})$, we get the curve with equation

$$G_{n,k}(\alpha, Y) = \alpha^n Y^n - Y + 1 - \sqrt[k]{2}\alpha^{n-1}Y^{n-1}(Y - 1) = 0.$$

Since $G_{n,k}(0, 1) = 0$ and $(G_{n,k})'_Y(0, 1) \neq 0$, we apply the analogue over $\boldsymbol{Q}(\sqrt[k]{2})$ of Theorem 4 of [6] (proved only for the number field $\boldsymbol{Q}$) to deduce that the polynomial $G_{n,k}(\alpha, Y)$ is irreducible in $\boldsymbol{Q}(\sqrt[k]{2})[Y]$ for any sufficiently large value of a. This implies that the polynomial $P_{a,n,k}(X)$ is irreducible over $\boldsymbol{Q}[X]$ if a is large enough in terms of n and k.

The family of polynomials $P_{a,n,k}(X)$ can be used in the context of [2], to which we refer for the following notation (the reader can consult Chapter III of [3] as well). For any positive integer n, Mahler and, later, Koksma introduced the functions w_n and w_n^*, defined on the set of real numbers, in order to measure the quality of approximation by algebraic numbers of degree at most n. Although they are very close, these functions do not coincide for any complex number, as first proved by Baker [1]. It is quite easy to establish that the inequalities (see, for example, [12])

$$w_n^*(\xi) \leqslant w_n(\xi) \leqslant w_n^*(\xi) + n - 1$$

hold for any transcendental real number ξ. Baker [1] showed that the range of values of the function $w_n - w_n^*$ includes the interval $[0, (n-1)/n]$. This has been substantially improved by Bugeaud [2]: the function $w_n - w_n^*$ can take any value in $[0, n/4]$. Using the family of polynomials $P_{a,n,2}(X)$ in the construction of [2] instead of the polynomials $X^n - 2(aX - 1)^2$ quoted in §1, it is then quite easy to prove that, for n even, the range of values of the function $w_n - w_n^*$ includes the interval $[0, n/2]$.

According to computations of Collins [4], the 'true' exponent of $H(P)$ in inequality (1.2) should be $-n/2$.

With the same ideas used to construct the polynomials $P_{a,n,k}(X)$, we can also provide examples of integer polynomials having two very close p-adic roots.

3. Proofs

The constants $c_2(n), \ldots, c_7(n)$ occurring below are positive, effective and depend only on n.

Let $n \geqslant 2$ and $a \geqslant 10$ be integers with $a \geqslant n$ and set

$$Q_1(X) = aX - 1, \quad Q_2(X) = X^n - aX + 1 \quad \text{and} \quad Q_3(X) = (a+1)X^n - X^{n-1} - aX + 1.$$

We notice that

$$|\mathrm{Res}(Q_1, Q_2)| = |\mathrm{Res}(Q_2, Q_3)| = 1,$$

where 'Res' denotes the resultant. Furthermore, $Q_2(X)$ and $Q_3(X)$ have roots α and β, respectively, with

$$\alpha = a^{-1} + a^{-n-1} + O(a^{-2n}), \qquad \beta = a^{-1} + a^{-n-1} + O(a^{-2n}).$$

Hence, after some easy calculation, we get $|\alpha - \beta| \leqslant 4a^{-2n}$, while Theorem A gives the lower bound $|\alpha - \beta| \geqslant c_2(n)a^{-2n}$. Consequently, Theorem A is best possible in terms of the heights of the polynomials involved.

Another example is provided by $|1/a - \alpha|$, which is less than $2a^{-n-1}$ and, by Theorem A, greater than $c_3(n)a^{-n-1}$.

We now turn to Theorem B. Let $k \geqslant 2$ be an integer and set

$$P_{a,n,k}(X) := (X^n - aX + 1)^k - 2X^{nk-k}(aX - 1)^k. \tag{3.1}$$

The coefficient -2 occurs in (3.1) to prevent the polynomial from being obviously irreducible. If we replace it with the constant -1, we obtain a reducible polynomial: actually, $P_{a,n,2}(X)$ (with -2 replaced by -1) is then divisible by the polynomial $Q_3(X)$.

We observe that the degree of $P_{a,n,k}(X)$ is kn and that its height is equal to $2a^k - 1$. Furthermore, using Rouché's theorem, it is easy to check that $P_{a,n,k}(X)$ has k roots $\alpha_1, \ldots, \alpha_k$ lying in the disc with centre $a^{-1} + a^{-n-1}$ and of radius $2a^{-2n}$.

Taking $k = 2$, we get

$$|\alpha_1 - \alpha_2| \leqslant 4a^{-2n} \leqslant c_4(n)H(P_{a,n,2})^{-n/2},$$

which should be compared with the lower bound (1.2).

Taking now k arbitrary, we get

$$\prod_{1\leqslant i<j\leqslant k} |\alpha_i - \alpha_j| \leqslant c_5(n)(a^{-2n})^{k(k-1)/2} \leqslant c_6(n)H(P_{a,n,k})^{-n(k-1)}. \qquad (3.2)$$

Since the degree of $P_{a,n,k}(X)$ is nk, inequality (1.3) gives that

$$\prod_{1\leqslant i<j\leqslant k} |\alpha_i - \alpha_j| \geqslant c_7(n)H(P_{a,n,k})^{-nk+1},$$

which, in view of (3.2), is close to being best possible in terms of the height of the polynomial.

The same example allows us to prove that Proposition 10.1 of Roy and Waldschmidt [**11**] is nearly best possible.

References

1. R. C. BAKER, On approximation with algebraic numbers of bounded degree, *Mathematika* **23** (1976), 18–31.
2. Y. BUGEAUD, Mahler's classification of numbers compared with Koksma's, *Acta Arith.* **110** (2003), 89–105.
3. Y. BUGEAUD, *Approximation by algebraic numbers*, Cambridge Tracts in Mathematics (Cambridge University Press, 2004).
4. G. E. COLLINS, Polynomial minimum root separation, *J. Symb. Computat.* **32** (2001), 467–473.
5. R. GÜTING, Polynomials with multiple zeros, *Mathematika* **14** (1967), 181–196.
6. M. LAURENT AND D. POULAKIS, On the global distance between two algebraic points on a curve, *J. Number Theory* **104** (2004), 210–254.
7. K. MAHLER, An inequality for the discriminant of a polynomial, *Michigan Math. J.* **11** (1964), 257–262.
8. M. MIGNOTTE, Some useful bounds, in *Computer algebra* (ed. B. Buchberger, G. E. Collins and R. Loos), pp. 259–263 (Springer, 1982).
9. M. MIGNOTTE, On the distance between the roots of a polynomial, *Applic. Alg. Engng Commun. Comput.* **6** (1995), 327–332.
10. P. MÜLLER, Finiteness results for Hilbert's irreducibility theorem, *Annls Inst. Fourier* **52** (2002), 983–1015.
11. D. ROY AND M. WALDSCHMIDT, Diophantine approximation by conjugate algebraic integers, *Compositio Math.* **140** (2004), 593–612.
12. E. WIRSING, Approximation mit algebraischen Zahlen beschränkten Grades, *J. Reine Angew. Math.* **206** (1961), 67–77.