On a theorem of Wirsing in Diophantine approximation

Yann Bugeaud

Abstract. *Let n and d be integers with $1 \le d \le n-1$. Let ξ be a real number which is not algebraic of degree at most n. We establish that there exist an effectively computable constant c, depending only on ξ and on n, an integer k with $1 \le k \le d$, and infinitely many integer polynomials $P(X)$ of degree m at most equal to n whose roots $\alpha_1, \ldots, \alpha_m$ can be numbered in such a way that*

$$|(\xi - \alpha_1) \ldots (\xi - \alpha_k)| \le c\, H(P)^{-\frac{d}{d+1}n - \frac{1}{d+1} - 1}.$$

This extends a well-known result of Wirsing who delt with the case $d = 1$.

1. Introduction and result

It follows from the theory of continued fractions that every irrational real number ξ is approximable at order at least two by rational numbers, in the sense that there exist infinitely many rational numbers p/q such that $|\xi - p/q| < 1/q^2$. A natural question then occurs: what can be said on the rate of approximation to ξ by algebraic numbers of bounded degree? This problem has been first considered in a seminal paper of Wirsing [11], who proved Theorem 1.1 below.

Throughout this text, the height $H(P)$ of a complex polynomial $P(X)$ is the maximum of the moduli of its coefficients and the height $H(\alpha)$ of an algebraic number α is the height of its minimal defining polynomial over $\mathbf{Z}$.

Theorem 1.1. *Let n be a positive integer. For any real number ξ which is not algebraic of degree at most n, there exist an effectively computable constant c and infinitely many real algebraic numbers α of degree at most equal to n satisfying*

$$|\xi - \alpha| \le c\, H(\alpha)^{-\frac{n+3}{2}}. \tag{1.1}$$

Theorem 1.1 has been subsequently slightly improved, see Chapter 3 of [1]. Let us just mention that Tishchenko [10] established that its conclusion holds with the exponent $-\frac{n+3}{2}$ in (1.1) replaced by $-\frac{n}{2} - \gamma_n$, where γ_n tends to 3 as n tends to infinity.

2010 *Mathematics Subject Classification :* 11J04.

It is often believed that the statement of Theorem 1.1 remains true with the exponent $-\frac{n+3}{2}$ in (1.1) replaced by $-n-1+\varepsilon$, with ε arbitrarily small, or even by $-n-1$. This is indeed the case when $n=2$, as was proved by Davenport and Schmidt [4] (see also [9]).

Theorem 1.2. *For any real number ξ which is neither rational, nor quadratic, and for any real number c greater than 160/9, there exist infinitely many rational or quadratic real numbers α satisfying*

$$|\xi-\alpha| \le c \max\{1, |\xi|^2\}\, H(\alpha)^{-3}.$$

Theorem 1.2 has been subsequently extended by Davenport and Schmidt [5] (up to the value of the numerical constant) as follows.

Theorem 1.3. *Let $n \ge 2$ be an integer and let ξ be a real number which is not algebraic of degree at most n. Then there exist an effectively computable constant c, depending only on ξ and on n, an integer k with $1 \le k \le n-1$, and infinitely many integer polynomials $P(X)$ of degree n whose roots $\alpha_1, \ldots, \alpha_n$ can be numbered in such a way that*

$$|(\xi-\alpha_1)\ldots(\xi-\alpha_k)| \le c\, H(P)^{-n-1}. \tag{1.2}$$

The goal of this note is to establish the following theorem, which could be viewed as an intermediate result between Theorem 1.1 and Theorem 1.3 (although Theorem 1.3 does not follow from Theorem 1.4).

Theorem 1.4. *Let n and d be integers with $1 \le d \le n-1$. Let ξ be a real number which is not algebraic of degree at most n. Then there exist an effectively computable constant c, depending only on ξ and on n, an integer k with $1 \le k \le d$, and infinitely many integer polynomials $P(X)$ of degree m at most equal to n whose roots $\alpha_1, \ldots, \alpha_m$ can be numbered in such a way that*

$$|(\xi-\alpha_1)\ldots(\xi-\alpha_k)| \le c\, H(P)^{-\frac{d}{d+1}n-\frac{1}{d+1}-1}.$$

By taking $d=1$ in Theorem 1.4 we recover Theorem 1.1. By taking $d=n-1$ in Theorem 1.4 we recover a weaker form of Theorem 1.3, namely with the exponent $-n-1$ in (1.2) replaced by $-n-\frac{1}{n}$. Theorem 1.3 follows from a general result on linear forms with real coefficients, whose proof is rather subtle.

The conclusion of Theorem 1.4 is not a surprise. It is not unexpected to improve the value $\frac{n+3}{2}$ obtained in (1.1) by taking into account more algebraic numbers. Indeed, a comparable phenomenon occurs for the closely related question of root separation of integer, irreducible polynomials, which we briefly survey below.

Throughout, the numerical constants implied by the signs $\ll$ and $\gg$ depend at most on the degree of the polynomial involved. In 1964, Mahler [8] established that

$$|\alpha_1-\alpha_2| \gg H(P)^{-n+1}, \tag{1.3}$$

for any distinct roots α_1 and α_2 of the integer polynomial $P(X)$ of degree n. This is sharp for $n=2$ and for $n=3$. For $n \ge 4$, it has been shown in [2] that the exponent $-n+1$ in

(1.3) cannot be replaced by something greater than $-\frac{n}{2} - \frac{n-2}{4(n-1)}$, when $P(X)$ is irreducible (a stronger result has been established in [3] for reducible polynomials).

Actually, (1.3) is a special case of the lower bound

$$\prod_{1 \le i < j \le d} |\alpha_i - \alpha_j| \gg H(P)^{-n+1}, \tag{1.4}$$

valid for any integer polynomial $P(X)$ of degree n having at least $d \ge 2$ distinct roots $\alpha_1, \ldots, \alpha_d$. It has been shown in [2] that the exponent $-n+1$ in (1.4) cannot be replaced by $-\nu_d n$, for a real number ν_d less than $(d-1)/d$, when $P(X)$ is irreducible (a stronger result has been established in [3] for reducible polynomials).

Roughly speaking, in the problem of Wirsing and in the question of root separation of integer, irreducible polynomials, the truth lies somewhere between $n/2$ and n. And this interval can be reduced by taking several roots into consideration.

The proof of Theorem 1.4 is a slight extension of Wirsing's proof of Theorem 1.1. The idea is as follows. We construct an infinite family of pairs $(P_k(X), Q_k(X))_{k \ge 1}$ of coprime integer polynomials of degree at most n and taking small values at ξ. Then, considering the resultant of $P_k(X)$ and $Q_k(X)$, Wirsing showed that $P_k(X)$ or $Q_k(X)$ has a root quite close to ξ. By studying every possible distribution of the roots of $P_k(X)$ and $Q_k(X)$ in the ball of radius 1 centered at ξ, we get Theorem 1.4.

2. Proof of Theorem 1.4

We begin by reproducing Lemma A.3 of [1], often referred to as Gelfond's lemma (see Lemma II on page 135 of [7]).

Lemma 2.1. *Let $P_1(X), \ldots, P_r(X)$ be non-zero complex polynomials of degree $n_1, \ldots, n_r$, respectively, and set $n = n_1 + \ldots + n_r$. We then have*

$$2^{-n}\, H(P_1) \ldots H(P_r) \le H(P_1 \ldots P_r) \le 2^n\, H(P_1) \ldots H(P_r).$$

If the conclusion of Theorem 1.4 holds for a real number ξ, then it also holds for any real number of the form $\xi + \frac{p}{q}$, where p, q are integers with $q \ge 1$. Consequently, we may assume that $0 < \xi < 1/10$.

We infer from Minkowski's first theorem and Lemma 2.1 that there exist infinitely many irreducible, primitive, integer polynomials $P(X)$ of degree at most n satisfying

$$0 < |P(\xi)| \ll H(P)^{-n}.$$

Let $P(X)$ be such a polynomial. If $R(X)$ is an integer polynomial of degree at most n which is a multiple of $P(X)$, then, again by Lemma 2.1, there exists a positive constant c, depending only on n and less than 1, such that $H(R) \ge 2c\, H(P)$. By Minkowski's first theorem, the system of inequalities

$$\begin{gathered} |b_n \xi^n + \ldots + b_0| \le c^{-n}\, H(P)^{-n} \\ |b_1|, \ldots, |b_n| \le c\, H(P). \end{gathered}$$

has a non-zero integer solution $(b_0, \ldots, b_n)$. Set $Q(X) = b_n X^n + \ldots + b_1 X + b_0$. If $H(P) \geq 2c^{-1}$, it follows from the assumption $0 < \xi < 1/10$ that $H(Q)$ is at most equal to $cH(P)$. Consequently, by our choice of c, the polynomials $P(X)$ and $Q(X)$ have no common factor.

Hence, one can build two sequences $(P_k)_{k\geq 1}$ and $(Q_k)_{k\geq 1}$ of non-zero integer polynomials of degree at most n, such that the height of $P_k(X)$ tends to infinity with k,

$$|P_k(\xi)| \ll H(P_k)^{-n}, \quad H(Q_k) \ll H(P_k), \quad |Q_k(\xi)| \ll H(P_k)^{-n} \quad (k \geq 1), \tag{2.1}$$

and

$$P_k(X) \text{ and } Q_k(X) \text{ are coprime } (k \geq 1).$$

We need an auxiliary result, which extends a lemma of Wirsing [11]. Notice that in Lemma 2.2 below and in its proof, the constant implied in $\ll$ depends only on t.

Lemma 2.2. *Let $t \geq 2$ be an integer and let $P(X)$ and $Q(X)$ be coprime polynomials with integer coefficients of degrees less than or equal to t. Let d be a positive integer at most equal to t. Let ξ be a real number with $|\xi| \leq 1$ and which is not algebraic of degree less than or equal to t. Assume that there exist a root of $P(X)$ and a root of $Q(X)$ in the open disk centered at ξ of radius 1. Then, we either have*

$$1 \ll \max\{|P(\xi)|^{d+1} \cdot H(P)^{t-d-1} \cdot H(Q)^t, |Q(\xi)|^{d+1} \cdot H(Q)^{t-d-1} \cdot H(P)^t\}, \tag{2.2}$$

or there exist roots $\alpha_1, \ldots, \alpha_u$, with $u \leq d$, of the polynomial $P(X)$ or roots $\beta_1, \ldots, \beta_v$, with $v \leq d$, of the polynomial $Q(X)$ such that one of the following six cases holds:

$$|\xi - \alpha_1| \cdots |\xi - \alpha_u| \ll |P(\xi)| \cdot H(P)^{-1}, \tag{2.3}$$

$$|\xi - \beta_1| \cdots |\xi - \beta_v| \ll |Q(\xi)| \cdot H(Q)^{-1}, \tag{2.4}$$

$$(|\xi - \alpha_1| \cdots |\xi - \alpha_d|)^{d+1} \ll |P(\xi)|^{d+1} \cdot |Q(\xi)| \cdot H(P)^{t-d-1} \cdot H(Q)^{t-1}, \tag{2.5}$$

$$(|\xi - \alpha_1| \cdots |\xi - \alpha_d|)^{d+1} \ll |P(\xi)| \cdot |Q(\xi)|^{d+1} \cdot H(P)^{t-1} \cdot H(Q)^{t-d-1}, \tag{2.6}$$

$$(|\xi - \beta_1| \cdots |\xi - \beta_d|)^{d+1} \ll |P(\xi)| \cdot |Q(\xi)|^{d+1} \cdot H(P)^{t-1} \cdot H(Q)^{t-d-1}, \tag{2.7}$$

$$(|\xi - \beta_1| \cdots |\xi - \beta_d|)^{d+1} \ll |P(\xi)|^{d+1} \cdot |Q(\xi)| \cdot H(P)^{t-d-1} \cdot H(Q)^{t-1}. \tag{2.8}$$

Proof. We denote by $\alpha_1, \ldots, \alpha_m$ the roots of $P(X)$ and by $\beta_1, \ldots, \beta_n$ those of $Q(X)$, numbered in such a way that, if $p_i := |\alpha_i - \xi|$ and $q_j := |\beta_j - \xi|$ for $i = 1, \ldots, m$ and $j = 1, \ldots, n$, we have $p_1 \leq \ldots \leq p_m$ and $q_1 \leq \ldots \leq q_n$. Let δ and δ' be the largest indices such that $p_\delta \leq 1$ and $q_{\delta'} \leq 1$, respectively.

Corollary A.1 of [1] applied with $\rho = 1$ gives

$$|P(\xi)| \ll H(P) \prod_{1 \leq i \leq \delta} p_i \ll |P(\xi)| \tag{2.9}$$

and

$$|Q(\xi)| \ll H(Q) \prod_{1 \leq j \leq \delta'} q_j \ll |Q(\xi)|. \tag{2.10}$$

If $\delta \le d$, then, by (2.9), we get

$$p_1 \dots p_\delta \ll H(P)^{-1}\,|P(\xi)|,$$

and (2.3) holds with $u = \delta$. Likewise, if $\delta' \le d$, then, by (2.10), we get

$$q_1 \dots q_{\delta'} \ll H(Q)^{-1}\,|Q(\xi)|,$$

and (2.4) holds with $v = \delta'$. Thus, we can assume that m, n, δ and δ' are all at least equal to $d+1$.

Denote by a_m the leading coefficient of $P(X)$ and by b_n that of $Q(X)$. Denoting by R the resultant of the polynomials $P(X)$ and $Q(X)$, we have

$$1 \le |R| = |a_m|^n |b_n|^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} |\alpha_i - \beta_j| \ll |a_m b_n|^t \prod_{\substack{1\le i\le m\\ 1\le j\le n}} \max\{p_i, q_j\} =: AB, \tag{2.11}$$

where

$$A = \prod_{1\le i\le\delta}\ \prod_{1\le j\le\delta'} \max\{p_i, q_j\} \tag{2.12}$$

and

$$B \le |a_m b_n|^t \prod_{\substack{1\le i\le m\\ 1\le j\le n}} \big(\max\{1, p_i\}\max\{1, q_j\}\big) \ll H(P)^t\, H(Q)^t.$$

We distinguish several cases, which cover all the possible configurations of the roots of $P(X)$ and $Q(X)$. We assume that $p_1 \le q_1$.

• First case: $p_1 \le q_1 < \dots < q_{d+1} < p_{d+1}$.

Observe that

$$\prod_{1\le j\le\delta'} \max\{p_1, q_j\} = \prod_{1\le j\le\delta'} q_j \ll |Q(\xi)| \cdot H(Q)^{-1}, \tag{2.13}$$

by (2.10), and that, for $j = 1, \dots, d+1$,

$$\prod_{2\le i\le\delta} \max\{p_i, q_j\} \le \prod_{d+1\le i\le\delta} p_i.$$

Consequently, it follows from (2.9), (2.12) and (2.13) that

$$\begin{aligned}(p_1 \dots p_d)^{d+1} A &\ll |Q(\xi)| \cdot H(Q)^{-1} \prod_{1\le i\le\delta} p_i^{d+1}\\ &\ll |Q(\xi)| \cdot H(Q)^{-1}\,(|P(\xi)| \cdot H(P)^{-1})^{d+1}.\end{aligned}$$

Thus, by (2.11), we get

$$(p_1 \dots p_d)^{d+1} \ll |P(\xi)|^{d+1}\,|Q(\xi)|\,H(P)^{t-d-1}\,H(Q)^{t-1},$$

giving (2.5).

• Second case: $p_1 < \ldots < p_{d+1} \leq q_1$.
Then, we have by (2.10) that

$$A \ll (q_1 \ldots q_{\delta'})^{d+1} \ll |Q(\xi)|^{d+1} \cdot H(Q)^{-d-1},$$

thus

$$1 \leq AB \ll |Q(\xi)|^{d+1} \cdot H(Q)^{t-d-1}\, H(P)^t,$$

which corresponds to (2.2).

• Third case: $q_1 < p_{d+1}$ and $p_1 \leq q_1 < \ldots < p_{d+1} \leq q_{d+1}$.
Then, observe that, for $i = 2, \ldots, d+1$,

$$\prod_{2 \leq j \leq \delta'} \max\{p_i, q_j\} \leq \prod_{d+1 \leq j \leq \delta'} q_j.$$

Combined with

$$\prod_{2 \leq i \leq \delta} \max\{p_i, q_1\} \leq p_{d+1} \ldots p_\delta$$

and (2.13), this gives

$$\begin{aligned}(p_1 \ldots p_d)(q_1 \ldots q_d)^d A &\ll |Q(\xi)| \cdot H(Q)^{-1} \prod_{1 \leq j \leq \delta'} q_j^d \prod_{1 \leq i \leq \delta} p_i \\ &\ll (|Q(\xi)| \cdot H(Q)^{-1})^{d+1}\, |P(\xi)| \cdot H(P)^{-1}.\end{aligned}$$

If $p_1 \ldots p_d \leq q_1 \ldots q_d$, then we get

$$(p_1 \ldots p_d)^{d+1} \ll |Q(\xi)|^{d+1}\, |P(\xi)|\, H(Q)^{t-d-1}\, H(P)^{t-1},$$

namely (2.6), and, otherwise,

$$(q_1 \ldots q_d)^{d+1} \ll |Q(\xi)|^{d+1}\, |P(\xi)|\, H(Q)^{t-d-1}\, H(P)^{t-1},$$

which corresponds to (2.7).

If $q_1 < p_1$, then, by distinguishing three cases as above, we get (2.7), (2.2), (2.8) or (2.5). This completes the proof of the lemma. □

Completion of the proof of Theorem 1.4. If there are infinitely many integer polynomials $P(X)$ of degree at most n such that $|P(\xi)| \leq H(P)^{-2n}$, then, by (3.11) of [1], there exist infinitely many algebraic numbers α of degree at most n such that $|\xi - \alpha| \leq H(\alpha)^{-n-1}$ and the theorem clearly holds in that case.

Consequently, we assume that there are only finitely many integer polynomials $P(X)$ of degree at most n such that $|P(\xi)| \leq H(P)^{-2n}$. Since the height of $P_k(X)$ tends to infinity with k, it then follows from the last inequality of (2.1) that the height of $Q_k(X)$ also tends to infinity with k

Let k be sufficiently large such that $|P_k(\xi)| < 1$ and $|Q_k(\xi)| < 1$. Then, the polynomials $P_k(X)$ and $Q_k(X)$ have a root in the open disk centered at ξ of radius 1. Apply Lemma 2.2 to the pairs of polynomials (P_k, Q_k). By (2.1), we get

$$\max\{|P_k(\xi)|^{d+1} \cdot H(P_k)^{n-d-1}\, H(Q_k)^n, |Q_k(\xi)|^{d+1} \cdot H(Q_k)^{n-d-1}\, H(P_k)^n\} \ll H(P_k)^{-1}.$$

Thus, (2.2) cannot hold for k large enough.

Furthermore, we derive from (2.1) that

$$|Q_k(\xi)|^{d+1}\, |P_k(\xi)|\, H(Q_k)^{n-d-1}\, H(P_k)^{n-1} \ll H(P_k)^{-(nd+d+2)} \ll H(Q_k)^{-(nd+d+2)}$$

and

$$|P_k(\xi)|^{d+1}\, |Q_k(\xi)|\, H(P_k)^{n-d-1}\, H(Q_k)^{n-1} \ll H(P_k)^{-(nd+d+2)} \ll H(Q_k)^{-(nd+d+2)}.$$

Combined with (2.5) to (2.10), this shows that there are roots $\alpha_1, \ldots, \alpha_d$ of $P_k(X)$ such that

$$(|\xi - \alpha_1| \cdots |\xi - \alpha_d|)^{d+1} \ll H(P_k)^{-(nd+d+2)}$$

or there are roots $\beta_1, \ldots, \beta_d$ of $Q_k(X)$ such that

$$(|\xi - \beta_1| \cdots |\xi - \beta_d|)^{d+1} \ll H(Q_k)^{-(nd+d+2)}.$$

This completes the proof of the theorem. □

Acknowledgements: The author is very grateful to the referee for valuable suggestions and a careful reading.

References

[1] Y. Bugeaud, Approximation by algebraic numbers, Cambridge Tracts in Mathematics, Cambridge, 2004.

[2] Y. Bugeaud and A. Dujella, *Root separation for irreducible integer polynomials*, Bull. Lond. Math. Soc. 43 (2011), 1239–1244.

[3] Y. Bugeaud and A. Dujella, *Root separation for reducible integer polynomials*, Acta Arith. 162 (2014), 393–403.

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

[5] H. Davenport and W. M. Schmidt, *A theorem on linear forms*, Acta Arith. 14 (1967/1968), 209–223.

[6] H. Davenport and W. M. Schmidt, *Approximation to real numbers by algebraic integers*, Acta Arith. 15 (1969), 393–416.

[7] A. O. Gel'fond, Transcendental and algebraic numbers. Translated from the first Russian edition by Leo F. Boron Dover Publications, Inc., New York, 1960.

[8] K. Mahler, *An inequality for the discriminant of a polynomial*, Michigan Math. J. 11 (1964), 257–262.

[9] W. M. Schmidt, Diophantine Approximation. Lecture Notes in Math. 785, Springer, Berlin, 1980.

[10] K. I. Tishchenko, *On the application of linearly independent polynomials in the Wirsing problem*, Dokl. Nats. Akad. Nauk Belarusi 44 (2000), no. 5, 34–36 (in Russian).

[11] E. Wirsing, *Approximation mit algebraischen Zahlen beschränkten Grades*, J. reine angew. Math. 206 (1961), 67–77.

Yann Bugeaud
Université de Strasbourg
Mathématiques
7, rue René Descartes
67084 STRASBOURG (FRANCE)

bugeaud@math.unistra.fr