Polynomial root separation

by Yann Bugeaud and Maurice Mignotte, Strasbourg

Abstract. *We discuss the following question: How close to each other can be two distinct roots of an integer polynomial? We summarize what is presently known on this and related problems, and we establish several new results on root separation of monic, integer polynomials.*

1. Introduction

It is easy to construct integer polynomials having two distinct roots arbitrarily close to each other. Since an usual measure for the size of an integer polynomial $P(X)$ is given by its height $\mathrm{H}(P)$, defined as the maximal of the absolute values of its coefficients, it is natural to compare the distance between two distinct roots of $P(X)$ with $\mathrm{H}(P)$. The first result in this direction was proved by Mahler [12], who established that

$$|\alpha - \beta| \gg \mathrm{H}(P)^{-d+1}, \tag{1.1}$$

for any distinct roots α and β of the integer polynomial $P(X)$ of degree d. Here, as well as throughout the present text, all the constants implied by $\ll$ and $\gg$ are explicitely computable, and depend at most on the degree d of the polynomials involved. Furthermore, we write $f \asymp g$ when both $f \ll g$ and $f \gg g$ hold.

Since the publication of Mahler's paper, the numerical constant implied in (1.1) was improved by several authors, but the exponent of $\mathrm{H}(P)$ remained unchanged. In 1982, Mignotte [13] exhibited the family of integer polynomials $X^d - 2(aX-1)^2$, for arbitrary integers $d \geq 3$ and $a \geq 2$, which have two roots separated by $\ll a^{-(d+2)/2}$. This shows that the exponent $-d+1$ in (1.1) cannot be replaced by a quantity greater than $-(d+2)/4$. However, this is not sharp enough to give a satisfactory answer to the following question.

Problem. *How close to each other can be two distinct roots of an integer polynomial?*

Three recent papers [5, 9, 17] shed new light on this fascinating problem and it is the purpose of this text, firstly, to summarize what is presently known on this and related questions and, secondly, to establish several new results. By 'related questions', we mean that we may as well restrict our attention to irreducible polynomials or to monic (irreducible) polynomials, as explicitly asked in Problem 52 from [4]. Also, we consider clusters of more than two roots close to each other.

Throughout, by polynomial, we always mean 'integer polynomial'. The present paper is organized as follows. In Section 2, we introduce the various quantities we are studying and treat the easy case of quadratic polynomials. Then, we gather in Sections 3 and 4 the results on polynomials and on monic polynomials, respectively. The main new point concerns root separation of cubic, monic polynomials. Quite surprisingly, this problem is strongly related to the Hall conjecture on small values of $x^3 - y^2$, hence, in particular, to the *abc*-conjecture. In Section 5, we exhibit several explicit families of polynomials that allow us to establish some of our statements. The remaining proofs are postponed to Sections 6 and 7.

2. Preliminaries

Throughout, we denote the minimal distance between two distinct roots of the integer polynomial $P(X)$ of degree d and distinct roots $\alpha_1, \ldots, \alpha_d$ by

$$\mathrm{sep}\,(P) := \min \big\{ |\alpha_i - \alpha_j| : 1 \le i < j \le d \big\},$$

With this notation, (1.1) can be rewritten as

$$\mathrm{sep}\,(P) \gg \mathrm{H}\,(P)^{-d+1}.$$

The discriminant $\Delta(P)$ of $P(X)$ is defined by

$$\Delta(P) = |a_d|^{2d-2} \prod_{1 \le i < j \le d} (\alpha_i - \alpha_j)^2,$$

where a_d is the leading coefficient of $P(X)$. Recall that $\Delta(P)$ is a rational integer and is nonzero if, and only if, $P(X)$ has no multiple roots. In the latter case, we have the sharper estimate

$$\mathrm{sep}\,(P) \gg |\Delta(P)|^{1/2}\, \mathrm{H}\,(P)^{-d+1}, \tag{2.1}$$

established e.g. in [14]. In some cases, this estimate is sharp: Consider the cubic polynomials $P_a(X) = X^3 - (aX-1)^2$, where a is a large positive integer, and observe that $\mathrm{sep}\,(P_a) \ll a^{-5/2}$, while the right-hand side of (2.1) gives $\mathrm{sep}\,(P_a) \gg a^{3/2} \times a^{-2(3-1)} = a^{-5/2}$, since $\Delta(P_a) = 4a^3 - 27$.

Furthermore, (1.1) is a particular case of the lower bound

$$\prod_{1 \le i < j \le k} |\alpha_i - \alpha_j| \gg \mathrm{H}\,(P)^{-d+1}, \tag{2.2}$$

valid for any integer polynomial $P(X)$ of degree d having at least $k \ge 2$ distinct roots $\alpha_1, \ldots, \alpha_k$.

To discuss the sharpness of (1.1) and (2.2), it is convenient to introduce the following quantities.

Definition 1. *Let k and d be integers with $2 \le k \le d$. We denote by $E(d,k)$, respectively $E_{\mathrm{irr}}(d,k)$, the infimum of the real numbers δ for which*

$$\prod_{1 \le i < j \le k} |\alpha_i - \alpha_j| \ge \mathrm{H}(P)^{-\delta}$$

holds for every integer polynomial $P(X)$, respectively irreducible integer polynomial $P(X)$, of degree d and sufficiently large height, with distinct roots $\alpha_1, \ldots, \alpha_d$. [In other words, $E(d,k)$ is the supremum of the exponents δ for which the reverse inequality

$$\prod_{1 \le i < j \le k} |\alpha_i - \alpha_j| \le \mathrm{H}(P)^{-\delta}$$

has infinitely many solutions in integer polynomials $P(X)$ of degree d.] We further use the notation $E^*(d,k)$, respectively $E^*_{\mathrm{irr}}(d,k)$, when we restrict our attention to monic integer polynomials, respectively monic integer irreducible polynomials. To shorten the notation, we set

$$e(d) = E(d,2) \quad \textit{and} \quad e_{\mathrm{irr}}(d) = E_{\mathrm{irr}}(d,2),$$

and

$$e^*(d) = E^*(d,2) \quad \textit{and} \quad e^*_{\mathrm{irr}}(d) = E^*_{\mathrm{irr}}(d,2).$$

In Definition 1 we consider only polynomials with distinct roots. We can remove this restriction (and assume only that $\alpha_1, \ldots, \alpha_k$ are distinct) without changing the values of $e(d), \ldots$ since, in view of Gelfond's Lemma (see Lemma A.3 in [4]), we have $\mathrm{H}(PQ) \asymp \mathrm{H}(P) \cdot \mathrm{H}(Q)$ for every non-zero integer polynomials $P(X)$ and $Q(X)$.

Clearly, it follows from (2.2) that

$$E_{\mathrm{irr}}(d,k) \le E(d,k) \le d-1 \quad \text{and} \quad E^*_{\mathrm{irr}}(d,k) \le E^*(d,k) \le E(d,k),$$

for any d, k with $2 \le k \le d$.

Not surprisingly, to find lower bounds for $E(d,k)$ is much easier than to find lower bounds for $E_{\mathrm{irr}}(d,k)$. The study of $E^*_{\mathrm{irr}}(d,k)$ and of $E^*(d,k)$ seems to be the hardest. In particular, it is not clear whether (2.2) can be improved for monic polynomials: This seems however to be plausible since there remain only d free coefficients.

We begin our study with the case of quadratic polynomials, which is elementary. Let $P(X) = aX^2 + bX + c$ be a squarefree quadratic polynomial, with $a > 0$ and nonzero discriminant $\Delta = b^2 - 4ac$. Then, we know the exact formula $\mathrm{sep}(P) = \sqrt{|\Delta|}/a$.

Choosing $a = k^2 + k + 1$, $b = 2k + 1$ and $c = 1$, we get $\Delta = -3$, the polynomial $P(X)$ is irreducible, has two complex roots, and satisfies

$$\mathrm{sep}(P) = \frac{\sqrt{3}}{a} = \frac{\sqrt{3}}{\mathrm{H}(P)}.$$

Those who are more interested in separating real roots may choose $a = k^2 + k - 1$, $b = 2k+1$ and $c = 1$. Then, we get $\Delta = 5$, the polynomial $P(X)$ is irreducible, has two real roots and, for $k \ge 2$, it satisfies

$$\mathrm{sep}(P) = \frac{\sqrt{5}}{a} = \frac{\sqrt{5}}{\mathrm{H}(P)}.$$

Clearly, all these results are essentially best possible, and they show that estimate (1.1) is optimal for quadratic polynomials. Further explicit examples were given in [3]. With the above notation, we have proved that

$$e_{\mathrm{irr}}(2) = e(2) = 1,$$

and, moreover, these infima are both minima.

The study of monic, quadratic polynomials is almost trivial and gives

$$e^*_{\mathrm{irr}}(2) = e^*(2) = 0.$$

In the sequel we always assume that the degree d is at least equal to three and we shall see that to find the best possible lower bound for $\mathrm{sep}(P)$ is no more an easy problem.

The basic idea for constructing integer polynomials having k distinct roots close to each other is to perturb slightly an integer polynomial having a root of multiplicity k. This is precisely how the polynomials $X^d - 2(aX-1)^2$, mentioned in the Introduction, were found. Indeed, $1/a$ is a root of $2(aX-1)^2$ of multiplicity 2, very close to 0 when a is large, and X^d is then — numerically — a 'small' perturbation.

Unfortunately, at present, there is no general theory for constructing integer polynomials of degree at least four with two roots close to each other. We just exhibit suitable families of polynomials to bound $e(d), e_{\mathrm{irr}}(d), \dots$ from below.

3. Root separation and clusters of roots

We begin with the cubic case. Beside the quadratic case, this is the only case for which the definitive answer is known.

Theorem 1. *For cubic integer polynomials, we have*

$$e_{\mathrm{irr}}(3) = e(3) = 2. \tag{3.1}$$

Theorem 1 was first proved by Evertse [9]. An alternative, and much simpler, proof was found by Schönhage [17] who established that the value of $e_{\mathrm{irr}}(3)$ is actually a minimum. We provide a proof of this assertion in Section 6.

Theorem 2. *For any even integer $d \geq 4$, we have*

$$e(d) \geq e_{\mathrm{irr}}(d) \geq d/2. \tag{3.2}$$

For any odd integer $d \geq 5$, we have

$$e(d) \geq (d+1)/2 \quad \text{and} \quad e_{\mathrm{irr}}(d) \geq (d+2)/4. \tag{3.3}$$

Theorem 2 is proved in Section 5. The fact that the lower bound for $e_{\mathrm{irr}}(d)$ is much sharper for even values of d than for odd values of d is a consequence of a lack of a suitable irreducibility criterion for the family of odd degree polynomials that we construct.

We now consider clusters of roots.

Theorem 3. *For any integer $d \geq 3$, we have*

$$E_{\mathrm{irr}}(d, d-1) = d - 1. \tag{3.4}$$

For any integer $d \geq 4$ and any integer $k \geq 2$ that divides d, we have

$$E_{\mathrm{irr}}(d, k) \leq \frac{d(k-1)}{k}. \tag{3.5}$$

The first statement of Theorem 3 extends (3.1) and is proved in Section 6. This was obtained in the general case by Evertse [9], with a rather intricate proof involving Roth's theorem, and by Schönhage [17] for $d = 3$ and $d = 4$. We present in Section 6 an alternative proof of (3.4).

4. The case of monic polynomials

Most of the results of the present section are new. The first statement is concerned with the root separation of cubic polynomials.

Recall that a well-known conjecture of Hall [10] asserts that, for any positive real number ε, we have

$$|x^3 - y^2| > x^{1/2-\varepsilon},$$

for any sufficiently large positive integers x and y with $x^3 \neq y^2$. Hall's conjecture is one of the many consequences of the *abc*-conjecture, as proved e.g., in [16], page 206.

Theorem 4. *For cubic, monic polynomials, we have*

$$e^*_{\mathrm{irr}}(3) = e^*(3) \geq 3/2. \tag{4.1}$$

If Hall's conjecture is true, then equality holds in (4.1) and conversely. Furthermore, if α and β are distinct roots of a monic, cubic polynomial $P(X)$, then

$$|\alpha - \beta| \gg \mathrm{H}(P)^{-2} (\log \mathrm{H}(P))^c,$$

for some positive constant c.

For monic polynomials of arbitrary degree, our next result is only slightly weaker than Theorem 2.

Theorem 5. *For any even integer $d \geq 4$, we have*

$$e^*(d) \geq d/2 \quad \text{and} \quad e^*_{\mathrm{irr}}(d) \geq (d-1)/2. \tag{4.2}$$

For any odd integer $d \geq 5$, we have

$$e^*(d) \geq (d-1)/2 \quad \text{and} \quad e^*_{\mathrm{irr}}(d) \geq (d+2)/4. \tag{4.3}$$

Our last statement is devoted to clusters of roots of monic polynomials. It is only slightly weaker than Theorem 3.

Theorem 6. *For any integer $d \geq 3$, we have*

$$E^*_{\mathrm{irr}}(d, d-1) \geq d - 2 + \frac{d-2}{2(d-1)}. \tag{4.4}$$

For any integer $d \geq 4$ and any integer $k \geq 2$ that divides d, we have

$$E^*_{\mathrm{irr}}(d, k) \geq \frac{d(k-1)}{k} - \frac{k-1}{2}. \tag{4.5}$$

We stress that to get all our lower bounds for $E(d, k)$ (and its relatives), we construct infinite families of polynomials $P(X)$ with

$$\prod_{1 \leq i < j \leq k} |\alpha_i - \alpha_j| \leq c\,\mathrm{H}(P)^{-E(d,k)},$$

for some positive constant c.

Our results suggest that it is very hard to make any reasonable conjecture for root separation of (monic) polynomials of degree at least four.

5. Explicit families of polynomials with clusters of roots

The example

$$P(X) = X^d - 2(aX - 1)^2,$$

already mentioned in Section 1, was given by Mignotte [13]. The factor 2 appears just to imply the irreducibility of $P(X)$ by means of the criterion of Eisenstein. For small ε, we have that $P(a^{-1} + \varepsilon) = (a^{-1} + \varepsilon)^d - 2a^2\varepsilon^2$ is very close to $a^{-d} - 2a^2\varepsilon^2$, and it follows that

$$\mathrm{sep}\,(P) \asymp a^{-(d+2)/2}.$$

Thus, for a tending to infinity, since $\mathrm{H}\,(P) = 2a^2$, we get

$$\mathrm{sep}\,(P) \ll \mathrm{H}\,(P)^{-(d+2)/4}.$$

Hence

$$e^*_{\mathrm{irr}}(d) \geq (d+2)/4,$$

and this proves the second statements of (3.3) and (4.3).

For even degrees, better examples were given recently in [5], namely the polynomials

$$P(X) = (X^n - aX + 1)^2 - 2X^{2n-2}(aX - 1)^2. \tag{5.1}$$

It follows from results from [15, 11] that $P(X)$ is irreducible for a large enough. Moreover, it is easy to verify that

$$\mathrm{sep}\,(P) \ll \mathrm{H}\,(P)^{-d/2},$$

where $d = 2n$ is the degree of $P(X)$. This proves (3.2).

The family of polynomials (5.1) can be slightly pertubated, and it is easily seen that the study of the irreducible polynomials

$$P(X) = (X^n - aX + 1)^k - 2X^{nk-k}(aX - 1)^k$$

and

$$P(X) = (X^n - aX + 1)^k - 2X^{nk-2k}(aX - 1)^k$$

implies (3.5), the second statement of (4.2) and (4.5).

For completeness, we add that the study of the family of polynomials

$$P(X) = (aX - 1)(X^n - aX + 1)$$

shows that $e(d) \geq d/2$ for $d \geq 3$. But these polynomials are reducible. Likewise, taking the monic polynomial

$$P(X) = (X^n + X^2 - aX + 1)(X^2 - aX + 1), \quad n \geq 3,$$

an elementary study leads to $\mathrm{sep}\,(P) \asymp a^{-(n+1)} \asymp \mathrm{H}\,(P)^{-(d-1)/2}$, where $d = n + 2$ is the degree of $P(X)$. We have proved the first statement of (4.3).

To prove (4.4), it is sufficient to consider the monic, irreducible polynomial

$$X^d - 2(aX - 1)^{d-1},$$

that has a cluster of $d - 1$ roots very close to each other.

It remains for us to establish the first inequalities of (3.3) and (4.2). The first assertion of Theorem A below can be established following the method of Wirsing [20]. A different proof is due to Bombieri and Mueller [2], see also Chapter 2 of the monograph [4], where the second assertion of Theorem A is established.

Theorem A. *Let $n \geq 2$ be an integer and α be a fixed real algebraic integer of degree n. There exist a constant $c_1(\alpha)$, depending only on α, and infinitely many real algebraic numbers β of degree $n - 1$ for which*

$$|\alpha - \beta| < c_1(\alpha)\,\mathrm{H}\,(\beta)^{-n}.$$

There exist a constant $c_2(\alpha)$, depending only on α, and infinitely many real algebraic integers γ of degree n for which

$$|\alpha - \gamma| < c_2(\alpha)\,\mathrm{H}\,(\gamma)^{-n}.$$

Theorem A can be applied as follows to our problem. Denote respectively by $Q(X)$, $R(X)$ and $S(X)$ the minimal polynomials of α, β and γ. Putting $P(X) = Q(X)R(X)$, we get

$$\mathrm{sep}\,(P) \ll \mathrm{H}\,(R)^{-n} \ll \mathrm{H}\,(P)^{-n},$$

and $\deg P = 2n - 1$. This proves the first assertion in (3.3).

Putting $P(X) = Q(X)S(X)$, we get

$$\mathrm{sep}\,(P) \ll \mathrm{H}\,(P)^{-n},$$

and $\deg P = 2n$. This proves the first assertion in (4.2), since $Q(X)$ and $S(X)$ are monic.

6. Proof that $E_{\mathrm{irr}}(d, d-1) = d - 1$

We now turn our attention to (3.4), which was established by Evertse [9]. We give below an alternative proof, using the ideas of Schönhage, that has the advantage to show that $d - 1$ is actually a minimum, a result not contained in [9].

For $d \geq 3$, consider the polynomial $P(X) = X^d + 3X^{d-1} + (-1)^d$. It is easy to prove that $P(X)$ has a real root less than -2. An application of Rouché's theorem on the unit circle $\{z : |z| = 1\}$ shows that $P(X)$ has $d - 1$ roots of modulus at most 1. It is also easy to see that $P(X)$ has no root on the unit circle. This implies that the monic polynomial $P(X)$ is irreducible. It follows that the polynomial $P_1(X) = P(X - 1)$ is irreducible, has a real root $\alpha_{1,1}$ less than -1 and that its other roots, say $\alpha_{i,1}$ for $2 \leq i \leq d$, have a positive real part. Now, following Schönhage [17], we transform the polynomial by the change of variable $X = q_1 + 1/Y$, where $q_1 = \lceil \alpha_{1,1} \rceil$. Here, $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. The resulting polynomial, denoted by $P_2(X)$, is also irreducible and the formulæ

$$\alpha_{i,1} = q_1 + 1/\alpha_{i,2}, \quad i = 1, 2, \ldots, d$$

(with obvious notation) imply that it has a negative root $\alpha_{1,2}$ less than -1 and that all its other roots are of modulus less than 1 with a positive real part. And we continue this process, obtaining $P_3(X)$, $P_4(X)$, ...

Now consider the square root D of the absolute value of the discriminant of $P(X)$. A short calculation shows that

$$D^2 = 2^d(d-1)^{d-1} + (-1)^{d-1}\, d^d. \tag{6.1}$$

First, notice that this is also the square root of the absolute value of the discriminant of any of the $P_k(X)$'s. For $k \geq 1$, let a_k be the (positive) leading coefficient of $P_k(X)$. Then

$$D = a_k^{d-1} \cdot \prod_{i=2}^{d} |\alpha_{1,k} - \alpha_{i,k}| \times \prod_{2 \leq i < j \leq d} |\alpha_{i,k} - \alpha_{j,k}| = \Pi_1 \times \Pi_2 \quad \text{(say)}.$$

At this point it is convenient to introduce another usual measure for the size of polynomials, namely the Mahler measure. For a complex polynomial $F(X)$ of degree d written as

$$F(X) = c_d X^d + c_{d-1} X^{d-1} + \cdots + c_0 = c_d (X - \beta_1) \cdots (X - \beta_d),$$

its Mahler measure is

$$\mathrm{M}\,(F) = |c_d| \prod_{j=1}^{d} \max\{1, |\beta_j|\}.$$

It is well-known (see Lemma A.2 in [4]) that

$$2^{-d}\,\mathrm{H}(F) \leq \mathrm{M}(F) \leq \sqrt{d+1}\,\mathrm{H}(F).$$

Let k be a positive integer. For $i = 2, \ldots, d$ we have $|\alpha_{1,k} - \alpha_{i,k}| \geq \Re e(-\alpha_{1,k})$ since $\Re e(\alpha_{1,k}) < 0$ and $\Re e(\alpha_{1,k}) \geq 0$. This implies that

$$\Pi_1 > |a_k \alpha_{1,k}|^{d-1} = \mathrm{M}(P_k)^{d-1},$$

as $\alpha_{1,k}$ is the only root of $P_k(X)$ outside the unit disc. Therefore, we have proved that

$$\prod_{2\leq i<j\leq d} |\alpha_{i,k} - \alpha_{j,k}| < D \cdot \mathrm{M}(P_k)^{-d+1}.$$

Combined with (6.1), this gives

$$\prod_{2\leq i<j\leq d} |\alpha_{i,k} - \alpha_{j,k}| < (2d)^{d/2} \cdot \mathrm{M}(P_k)^{-d+1}.$$

Since the polynomial $P(X)$ is irreducible of degree at least three, the numbers $\alpha_{1,k}$ are irrational and the Mahler measures of the $P_k(X)$'s are not bounded from above, thus this construction implies that

$$E_{\mathrm{irr}}(d, d-1) = d-1,$$

as asserted.

7. The monic cubic case

We follow a suggestion of Umberto Zannier: To translate the polynomial so that the coefficient of X^2 vanishes in order to get a much simpler formula for the discriminant in terms of the coefficients. Formally, with $P(X) = X^3 + aX^2 + bX + c$ we associate the polynomial $P^0(X)$ defined by

$$P^0(X) = \begin{cases} P(X - a/3), & \text{if } 3 \mid a, \\ 27\,P(X/3 - a/3), & \text{otherwise.} \end{cases}$$

Write $P^0(X) = X^3 + pX + q$ and observe that

$$\Delta(P^0) = -4p^3 - 27q^2 = \begin{cases} \Delta(P), & \text{if } 3 \mid a, \\ 3^6\,\Delta(P), & \text{otherwise.} \end{cases}$$

It follows from (2.1) that polynomials $P(X)$ with small discriminants are good candidates for having two roots close to each other. Consequently, we are looking for pairs (p, q) of integers such that $4p^3 + 27q^2$ is small compared with $\max\{|p|, |q|\}$.

The study of this problem was initiated by Hall [10]. In 1982, Danilov [6] found explicit infinite sequences of positive rational integers $(x_m)_{m\geq 1}$ and $(y_m)_{m\geq 1}$ such that

$$|x_m^3 - y_m^2| \asymp \sqrt{x_m}, \quad (m \geq 1).$$

Put $p_m = -3x_m$ and $q_m = \pm 2y_m$. This leads to a family of polynomials $P_m(X) = X^3 + p_m X + q_m$ with integer coefficients and positive discriminant for which

$$\Delta(P_m) \asymp \sqrt{|p_m|}.$$

Denote by β_m, α_m, and α'_m the roots of $P_m(X)$ labelled in such a way that $\operatorname{sep}(P_m) = |\alpha_m - \alpha'_m|$. Note that, since the sum of the roots is zero, α_m and α'_m are both close to $-\beta_m/2$. Then, it is easy to see that

$$\Delta(P_m) \asymp (\operatorname{sep}(P_m))^2\, |\beta_m|^4.$$

Note that a similar estimate is true for any monic cubic polynomial with a coefficient of X^2 equal to zero. Hence, using the estimate $|p_m| \asymp |\beta_m|^2$, we get

$$\operatorname{sep}(P_m) \asymp |\beta_m|^{-3/2}.$$

Now, make an integer translation on the variable X to replace $P_m(X)$ by, say, $\tilde{P}_m(X)$ which has two roots of modulus $< 1/2$. Then, we get $H_m := \mathrm{H}(\tilde{P}_m) \asymp |\beta_m|$ and

$$\operatorname{sep}(\tilde{P}_m) \asymp H_m^{-3/2}.$$

This establishes (4.1).

Along the way, we have proved the following result. If

$$\lambda = \liminf_{x,y\to+\infty} \frac{\log|x^3 - y^2|}{\log x},$$

where the limit is taken over positive rational integers for which $x^3 - y^2 \neq 0$, then

$$e^*_{\mathrm{irr}}(3) = e^*(3) = 2 - \lambda.$$

Consequently, the Hall conjecture is equivalent to

$$e^*_{\mathrm{irr}}(3) = e^*(3) = 3/2.$$

The last assertion of Theorem 4 follows from explicit lower bounds for the quantity $|x^3 - y^2|$ obtained by means of estimates for linear forms in the logarithms of algebraic numbers, see e.g., Theorem 1.1 of Chapter VI from [18].

To summarize, we have given explicitly an infinite family $(Q_n(X))_{n\geq 1}$ of cubic, monic, integer polynomials such that

$$\operatorname{sep}(Q_n) \ll \mathrm{H}(Q_n)^{-3/2},$$

and whose coefficients grow exponentially fast in terms of n.

It is a challenging problem to decide whether there are families $(P_n(X))_{n\geq 1}$ of integer polynomials such that $\mathrm{sep}\,(P_n)$ remains very small compared to $\mathrm{H}\,(P_n)$ and whose coefficients grow polynomially fast in terms of n, like for the families of polynomials given in Section 5.

The best polynomial family we found is given by the polynomials

$$X^3 + (a^5 + 3a^2)X^2 - (2a^4 + 4a)X + (a^3 + 1),$$

for which we have

$$\mathrm{sep}\,(P) \asymp \mathrm{H}\,(P)^{-7/5}.$$

Besides $X^3 - 2(aX - 1)^2$ mentioned in Section 5, other interesting examples are

$$X^3 + (16a^3 + 4a)X^2 - (8a^2 + 1)X + a,$$

$$X^3 + (a^4 + a^3 + 3a^2 + 1)X^2 - (2a^3 + 2a^2 + 4a)X + (a^2 + a + 1),$$

and

$$X^3 + (a^6 + a^5 + 5a^4 + 3a^3 + 6a^2 + 3a + 1)X^2 - (2a^5 + 2a^4 + 8a^3 + 4a^2 + 6a + 2)X + (a^4 + a^3 + 3a^2 + a + 1),$$

for which we have, respectively,

$$\mathrm{sep}\,(P) \asymp \mathrm{H}\,(P)^{-4/3}, \quad \mathrm{H}\,(P)^{-11/8}, \quad \mathrm{H}\,(P)^{-4/3}.$$

This question is very similar to a celebrated problem on small values of $f^3 - g^2$ whose origin is in a paper by Birch *et al.* [1]. Davenport [7] established that if f, g are polynomials with complex coefficients, then either $f^3 = g^2$ or $\deg(f^3 - g^2) \geq 1 + (\deg f)/2$. There are several examples of polynomials f, g of small degree, with rational coefficients, that attain this lower bound; see [19, 8]. At present, no example is known with $\deg f \geq 12$. However, if we remove the assumption that the polynomials should have rational coefficients, then, for every degree, Davenport's inequality cannot be improved. This was established by Zannier [21].

Along our long search, the best example we could find is

$$P(X) = X^3 + 305\,X^2 - 273\,X + 61, \quad \text{for which} \quad \frac{\log \mathrm{sep}\,(P)}{\mathrm{H}\,(P)} = -1.67076\ldots,$$

i.e., $\mathrm{sep}\,(P) < \mathrm{H}\,(P)^{-1.67}$. A deeper analysis of the problem yields the following result.

Proposition 1. *Let $P(X) = X^3 + aX^2 + bX + c$ be a monic separable cubic polynomial with integer coefficients of height H. Then,*

$$\mathrm{sep}\,(P) \gg H^{-5/4} \quad \textit{if} \quad b^2 - 4ac = 0.$$

If the roots of $P(X)$ are α, α' and β with $\operatorname{sep}(P) = |\alpha - \alpha'|$ *and if* $\gamma = (\alpha+\alpha')/2$, *then*

$$\operatorname{sep}(P) \gg H^{-7/5} \quad \textit{if} \quad |\gamma| \leq \tfrac{1}{2} H^{-1/5} \quad \textit{or} \quad |\gamma| \geq H^{3/20},$$

where the constants implied by $\gg$ are effectively computable.

We now prove Proposition 1. Consider a squarefree monic cubic polynomial with integer coefficients,

$$P(X) = X^3 + aX^2 + BX + c = (X-\alpha)(X-\alpha')(X-\beta)$$

of height $\mathrm{H}(P) = H$ for which $\operatorname{sep}(P) = |\alpha - \alpha'|$. Our goal is to study the quantity

$$\rho = \rho(P) = -\frac{\log \operatorname{sep}(P)}{\mathrm{H}(P)},$$

more precisely we want to find examples for which $\rho(P)$ is rather large and we try to prove non trivial upper bounds for $\rho(P)$.

The following inequalities hold (Cauchy, Mahler)

$$\max\{|\alpha|, |\alpha'|, |\beta|\} < H+1, \quad \tfrac{1}{3} H \leq \mathrm{M}(P) := \max\{1,|\alpha|\}\cdot\max\{1,|\alpha'|\}\cdot\max\{1,|\beta|\} < 2H$$

and

$$\max\{1,|\alpha|^{-1}\}\cdot\max\{1,|\alpha'|^{-1}\}\cdot\max\{1,|\beta|^{-1}\} < 2H.$$

Put

$$\gamma = (\alpha+\alpha')/2, \quad \delta = (\alpha'-\alpha)/2, \quad \pi = \alpha\alpha',$$

and also $|\gamma| = H^\theta$; then

$$a = -\beta - 2\gamma, \quad b = 2\beta\gamma + \pi, \quad c = -\beta\pi \quad \text{and} \quad \operatorname{sep}(P) = |2\delta|.$$

The discriminant Δ of $P(X)$ satisfies

$$\Delta = -4ca^3 + b^2a^2 + 18abc - 4b^3 - 27c^2 = 4\delta^2\bigl((\beta-\gamma)^2 - \delta^2\bigr)^2$$

and

$$1 \leq |\Delta| \leq |4\delta^2|(|\beta-\gamma| + |\delta|)^4.$$

Hence

$$\operatorname{sep}(P) > (2H+3)^{-2},$$

which implies the "trivial" upper bound $\rho \leq 2$.

Because of the example $P(X) = X^3 - (tX-1)^2$ with $t \geq 3$ which is irreducible [for any $n \geq 2$ and $\ell \geq 3$ the polynomial $X^d - (\ell X - 1)^{d-1}$ is irreducible "à la Pisot"] we could suppose that $|\delta| \leq H^{-5/4}$, but we prefer to work under the (asymptotically) weaker hypothesis

$$|\delta| \leq \frac{1}{17H}.$$

Then $P(X)$ is irreducible and $\gamma = -(a+\beta)/2$ is irrational. Moreover, a short computer verification shows that this inequality implies $H \geq 50$ and from now on we assume $H \geq 50$. We notice that

$$|\delta| \geq \tfrac{1}{2}\left(|\beta| + |\gamma| + |\delta|\right)^{-2},$$

thus, if $|\beta| \leq |\gamma|$ then

$$\frac{1}{17H} \geq |\delta| \geq \frac{1}{2}\left(2|\gamma| + \frac{1}{17H}\right)^{-2},$$

and using the inequalities $|\gamma|^2 - |\delta|^2 \leq \mathrm{M}(P) < 2H$ we reach a contradiction. Hence our hypothesis on $|\delta|$ implies $|\beta| > |\gamma|$. Thus

$$\frac{1}{17H} \geq |\delta| \geq \tfrac{1}{2}\left(2|\beta| + \frac{1}{17H}\right)^{-2},$$

which implies

$$|\beta| > \sqrt{2H}.$$

Now, since $H \geq |c| \geq |\beta|(|\gamma|^2 - |\delta|^2)$, we see that

$$|\gamma| < H^{1/4} - 1.$$

Applying one more the above inequalities we get the more precise estimates

$$|\beta| > \sqrt{8H}, \quad |\gamma| + \tfrac{1}{2} < \tfrac{1}{2}\, H^{1/4}.$$

Moreover, we see at once that β, γ and δ^2 are real.

Our next step is to prove that we can restrict our study to the case $|\gamma| \leq 1/2$. Changing X into $-X$ if necessary—that does not change $\operatorname{sep}(P)$—we may assume that β is positive. If $|\gamma| > 1/2$ let h be the integer such that $|\gamma - h| < 1/2$ and put

$$P_0(X) = P(X+h) = X^3 + a_0 X^2 + b_0 X + c_0.$$

then clearly $\operatorname{sep}(P_0) = \operatorname{sep}(P)$. We have

$$|h| \leq |\gamma| + \tfrac{1}{2} < \tfrac{1}{2}\, H^{1/4}.$$

Using

$$|a_0| < \beta + 1 \qquad \text{and} \qquad |a| \geq \beta - 0.5\, H^{1/4},$$

we get

$$|a_0| < \frac{\beta + 1}{\beta - 0.5\, H^{1/4}}\, |a| < 1.13\, |a|.$$

In a similar way, we obtain

$$|b_0| < \frac{2\beta+1}{2\beta|\gamma|(1-1.1|\gamma|/\beta)}\,|b| < 1.12\,|b|,$$

and

$$|c_0| < \frac{(\beta+1)(1/4+|\delta|^2)}{(\beta-0.5\,H^{1/4})(|\gamma|^2-|\delta|^2)}\,|c| < 1.13\,|c|,$$

so that

$$\mathrm{H}\,(P_0) < 1.13\,\mathrm{H}\,(P).$$

This short study shows that, if we can prove that

$$\mathrm{sep}\,(P_0) \geq C\,\mathrm{H}\,(P_0)^{-\rho}$$

then

$$\mathrm{sep}\,(P) \geq 0.6\,C\,\mathrm{H}\,(P)^{-\rho},$$

this is the reason why we suppose $|\gamma| < 1/2$ from now on and put $P_0 = P$.

Now consider

$$D = b^2 - 4ac.$$

First, let us estimate D. We have

$$D = (\pi + 2\gamma\beta)^2 - 4(2\gamma+\beta)\pi\beta = -4\pi\beta\gamma + \pi^2 + 4\delta^2\beta^2.$$

It follows that (recall that $|\delta| \leq \frac{1}{10}\,H^{-1}$)

$$|\gamma| \leq \tfrac{1}{4}\,H^{-1/3} \implies D = 0 \implies 4|\pi\beta\gamma| < 1/3 \implies |\gamma| < \tfrac{1}{2}\,H^{-1/3}.$$

- If $D = 0$ then $|b|^3 > 110|c|^3$ (indeed, we have $b^3 = 4abc$, where $a = H$, $b \approx 2H\gamma$ and $|c| \approx H\gamma^2$) and $|b| > 0.98\,|\gamma\beta|$. Using the formula

$$2\Delta = (2a^2 - 9b)D - b^3 - 54c^3$$

we get

$$|\Delta| > \tfrac{1}{4}\,|b|^3 > \tfrac{1}{4.5}\,|\gamma\beta|^3.$$

Hence,

$$|\delta| \geq \tfrac{1}{2.5}\,|\gamma^3/\beta|^{1/2} \geq \tfrac{1}{3}\,H^{-5/4}.$$

- Now we suppose that $D \neq 0$ and we consider the expression

$$G = bD + 8c^2.$$

One can verify that

$$G = -2\pi^2\gamma\beta + \pi^3 + 4\delta^2(2\gamma\beta^3 - \pi\beta^2).$$

It follows that (recall the notation $|\gamma| = H^\theta$)

$$|\delta| \le \tfrac{1}{4}\, H^{(-3+\theta)/2} \quad \text{and} \quad |\gamma| \le \tfrac{1}{2}\, H^{1/5} \implies G = 0.$$

We notice that $G = 0$ is equivalent to the formula

$$b^3 = 4(ab - 2c)c.$$

Now let p a prime divisor of c and suppose that $p^k \,\|\, c$ and that $p^\ell \,\|\, b$. Then, from the preceding formula we see that

$$3\ell \ge \min\{2k, \ell + k\},$$

which implies $2\ell \ge k$. In other words, c divides b^2, which implies that D is a multiple of c. It follows that when $G = 0$, we have

$$|D| \ge |\pi\beta|,$$

but from the above estimate of D we see that $|D| \le |5\pi\beta\gamma|$ when $|\delta| \le \frac{1}{4}\, H^{(-1+\theta)/2}$. Hence

$$G = 0 \quad \implies \quad |\gamma| \ge \tfrac{1}{5}.$$

If we compare the two above implications we see that we have proved that

$$|\gamma| \le \tfrac{1}{2}\, H^{1/5} \implies |\delta| \ge \tfrac{1}{4}\, H^{(-3+\theta)/2}.$$

Acknowledgements. We are pleased to thank Umberto Zannier for several enlighting observations. We are very grateful to the referee for a detailed report.

References

[1] B. J. Birch, S. Chowla, M. Hall Jr., and A. Schinzel, *On the difference* $x^3 - y^2$, Norske Vid. Selsk. Forh. (Trondheim) 38 (1965), 65–69.

[2] E. Bombieri and J. Mueller, *Remarks on the approximation to an algebraic number by algebraic numbers*, Mich. Math. J. 33 (1986), 83–93.

[3] Y. Bugeaud, *Mahler's classification of numbers compared with Koksma's, III*, Publ. Math. Debrecen 65 (2004), 305–316.

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

[5] Y. Bugeaud and M. Mignotte, *On the distance between roots of integer polynomials*, Proc. Edinburgh Math. Soc. 47 (2004), 553–556.

[6] L. V. Danilov, *The Diophantine equation* $x^3 - y^2 = k$ *and a conjecture of M. Hall*, Mat. Zametki 32 (1982), 273–275, 425 (in Russian); English translation: Math. Notes 32 (1982), 617–618.

[7] H. Davenport, *On $f^3(t) - g^2(t)$*, Norske Vid. Selsk. Forh. (Trondheim) 38 (1965), 86–87.

[8] N. D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction.* In: Algorithmic number theory (Leiden, 2000), 33–63, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.

[9] J.-H. Evertse, *Distances between the conjugates of an algebraic number*, Publ. Math. Debrecen 65 (2004), 323–340.

[10] M. Hall Jr., *The Diophantine equation $x^3 - y^2 = k$.* In: Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), pp. 173–198. Academic Press, London, 1971.

[11] M. Laurent and D. Poulakis, *On the global distance between two algebraic points on a curve*, J. Number Theory 104 (2004), 210–254.

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

[13] M. Mignotte, *Some useful bounds.* In B. Buchberger, G. E. Collins, R. Loos, eds., Computer Algebra, pp. 259–263, Springer–Verlag, 1982.

[14] M. Mignotte et M. Payafar, *Distance entre les racines d'un polynôme*, RAIRO Anal. Numér. 13 (1979), 181–192.

[15] P. Müller, *Finiteness results for Hilbert's irreducibility theorem*, Ann. Inst. Fourier 52 (2002), 983–1015.

[16] W. M. Schmidt, Diophantine Approximations and Diophantine Equations. Lecture Notes in Math. 1467, Springer, Berlin, 1991.

[17] A. Schönhage, *Polynomial root separation examples*, J. Symbolic Comput. 41 (2006), 1080–1090.

[18] V. G. Sprindžuk, Classical Diophantine Equations. Lecture Notes in Math. 1559, Springer-Verlag, Berlin, 1993.

[19] S. Uchiyama and M. Yorinaga, *On the difference $f^3(x) - g^2(x)$*, Tsukuba J. Math. 6 (1982), 215–230.

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

[21] U. Zannier, *On Davenport's bound for the degree of $f^3 - g^2$ and Riemann's existence theorem*, Acta Arith. 71 (1995), 107–137.

Yann Bugeaud, Maurice Mignotte
Université Louis Pasteur
U. F. R. de mathématiques
7, rue René Descartes
67084 STRASBOURG Cedex

e-mail : `bugeaud,mignotte@math.u-strasbg.fr`