Now, it is either $\deg B = 1$ or $\deg B = 2$. If $\deg B = 1$, then $B(t)$ has the rational root β such that

$$0 = B(\beta) = B(\alpha) + (\beta - \alpha)B'(\alpha),$$

so

$$|\alpha - \beta| = |B(\alpha)/B'(\alpha)| \ll \|x\|^{-3} \ll \|B\|^{-3} \ll H(\beta)^{-3}.$$

If $\deg B = 2$, then the roots β of $B(t)$ satisfy

$$0 = B(\beta) = B(\alpha) + (\beta - \alpha)B'(\alpha) + \frac{1}{2}(\beta - \alpha)^2 B''(\alpha).$$

By solving this quadratic equation for $\beta - \alpha$, from (13.41), we see that the roots β are real and that one of the roots β satisfies

$$\begin{aligned} |\beta - \alpha| &= |-B'(\alpha) + \sqrt{B'(\alpha)^2 - 2B(\alpha)B''(\alpha)}|/|B''(\alpha)| \\ &= |2B(\alpha)|/|B'(\alpha) + \sqrt{B'(\alpha)^2 - 2B(\alpha)B''(\alpha)}| \\ &\ll |B(\alpha)/B'(\alpha)| \ll \|x\|^{-3} \ll \|B\|^{-3} \ll H(\beta)^{-3}. \end{aligned}$$

□

13.5 Polynomial root separation

Let $P(x) = a_n x^n + \cdots + a_1 x + a_0$ be a polynomial with integer coefficients. We ask how close can two of its distinct roots be. Since the complexity of the polynomial $P(X)$ is usually measured by its height, $H(P) = \max(|a_0|, \ldots, |a_n|)$, it is natural to compare the distance between distinct roots of $P(X)$ with the height $H(P)$. A significant result in this direction was obtained in 1964 by the Australian mathematician of German origins Kurt Mahler (1903 – 1988), by proving that $|\alpha - \beta| \gg H(P)^{-n+1}$, for any two distinct roots α, β of a polynomial $P(X)$ of degree n with integer coefficients. The constant which is implied in $\gg$ is effective, and it only depends on the degree of the given polynomial.

The connection of this problem with the problems and results from Diophantine approximations comes from the fact that the roots α, β of polynomial $P(x)$ are algebraic numbers. We consider one variant of the problem of how well can one algebraic number be approximated by another algebraic number. If, additionally, the polynomial P is monic, then the considered roots α, β are algebraic integers.

Other than the (absolute) height $H(P)$ of a polynomial, there are also other definitions of the height of a polynomial and thus also the height of

an algebraic number. For a polynomial $P(x) = a_n(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n)$, we define the quantity

$$M(P) = |a_n| \prod_{i=1}^{n} \max(|\alpha_i|, 1)$$

which is called the *Mahler measure* of a polynomial P, while the *logarithmic Weil height* is defined by $h(P) = \frac{1}{n} \ln M(P)$. The following inequalities between the absolute height and Mahler measure hold:

$$\binom{n}{\lfloor n/2 \rfloor}^{-1} H(P) \le M(P) \le \sqrt{n+1} H(P) \tag{13.42}$$

(for a proof, see [61, Appendix A]).

We will now prove the mentioned Mahler's result from [285].

Theorem 13.15 (Mahler, 1964)**.** *Let $P(x)$ be a polynomial of degree $n \ge 2$ with integer coefficients and without multiple roots. For any two distinct roots α, β of the polynomial $P(x)$, the inequality*

$$|\alpha - \beta| > \sqrt{3}(n+1)^{-(2n+1)/2} \max(1, |\alpha|, |\beta|) H(P)^{-n+1}$$

holds.

Proof: Let

$$P(x) = a_n x^n + \cdots + a_0 = a_n(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n).$$

We can assume that $|\alpha| \ge |\beta|$ and let us take $\alpha_1 = \alpha$, $\alpha_2 = \beta$. Since the polynomial $P(x)$ does not have multiple roots, its discriminant

$$\mathrm{Disc}(P) = a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

is a non-zero integer (see Chapter 11.2). The discriminant $\mathrm{Disc}(P)$ can also be written using the determinant of the Vandermonde matrix

$$V = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ & & \cdots & & \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

We have $\det(V) = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)$ (see [184, Chapter 6.6.2]), so $\mathrm{Disc}(P) = \pm a_n^{2n-2} (\det(V))^2$. The value of the determinant V will not change if we

replace the first row with the difference between the first and second row. In the new matrix, the elements of the first row are $\alpha^j - \beta^j$. Let us now apply to that new matrix Hadamard's inequality, which states that the absolute value of a determinant is not greater than the product of lengths of row vectors (or column vectors) of the matrix (see [385, Chapter 8]). Hence, we have

$$\begin{aligned}
|\operatorname{Disc}(P)| &\le |a_n|^{2n-2}\Big(\sum_{j=1}^{n-1}|\alpha^j-\beta^j|^2\Big)\cdot\prod_{i=2}^{n}(1+|\alpha_i|^2+\cdots+|\alpha_i|^{2n-2}) \\
&\le |a_n|^{2n-2}|\alpha-\beta|^2\Big(\sum_{j=1}^{n-1}|\alpha^{j-1}+\alpha^{j-2}\beta+\cdots+\beta^{j-1}|^2\Big) \\
&\qquad \times n^{n-1}\prod_{i=2}^{n}\max(1,|\alpha_i|)^{2n-2} \\
&\le |\alpha-\beta|^2 n^{n-1} M(P)^{2n-2}\max(1,|\alpha|)^{-2}\cdot(1+2^2+3^2+\cdots+(n-1)^2).
\end{aligned}$$

Now, from $1+2^2+\cdots+(n-1)^2 = \frac{n(n-1)(2n-1)}{6} < \frac{n^3}{3}$ (Example 1.1), $|\operatorname{Disc}(P)| \ge 1$ and inequality (13.42), we obtain the statement of the theorem. □

For a polynomial $P(x)$ of degree $n \ge 2$ with integer coefficients and distinct roots $\alpha_1, \ldots, \alpha_n$, we define

$$\operatorname{sep}(P) = \min_{1\le i<j\le n} |\alpha_i - \alpha_j|$$

and the *separation exponent* $e(P)$ by

$$\operatorname{sep}(P) = H(P)^{-e(P)}.$$

Furthermore, for fixed $n \ge 2$, we define

$$e(n) = \limsup_{\deg(P)=n,\ H(P)\to+\infty} e(P),$$

$$e_{\text{irr}}(n) = \limsup_{\substack{\deg(P)=n,\ P \text{ irred.}\\ H(P)\to+\infty}} e(P),$$

where, in the last case, the limit superior is taken over all irreducible integer polynomials $P(x)$ of degree n.

Mahler's theorem shows that $e(n) \le n-1$ for every n. The exact values for $e(n)$ and $e_{\text{irr}}(n)$ are only known for $n = 2$ and $n = 3$. The case $n = 2$

is trivial, while the case $n = 3$ (for the irreducible polynomials) is more involved. We have $e_{\text{irr}}(2) = e(2) = 1$ and $e_{\text{irr}}(3) = e(3) = 2$.

For $n = 2$, we have $P(x) = ax^2 + bx + c$, $\operatorname{Disc}(P) = b^2 - 4ac$, $\operatorname{sep}(P) = \sqrt{|\operatorname{Disc}(P)|}/|a|$. If we take, e.g. $a = k^2 + k - 1$, $b = 2k + 1$, $c = 1$, then $\operatorname{Disc}(P) = 5$, so $\operatorname{sep}(P) \ll H(P)^{-1}$.

In 1982, Mignotte [301] found a family of polynomials $X^n - 2(aX - 1)^2$ for arbitrary integers $n \geq 3$ and $a \geq 2$ with very good separation properties (the coefficient 2 ensures the irreducibility of polynomials according to Eisenstein's criterion – Theorem 11.15). Namely, these polynomials have two roots very close to a^{-1}. Indeed, from $P(a^{-1} + \varepsilon) \approx a^{-n} - 2a^2\varepsilon^2$, we see that $P(x)$ has roots approximately equal to

$$a^{-1} \pm a^{(-n-2)/2}/\sqrt{2}.$$

Since $H(P) = 2a^2$, if we let a go to infinity, we get $\operatorname{sep}(P) \ll H(P)^{-(n+2)/4}$, i.e.

$$e(n) \geq e_{\text{irr}}(n) \geq (n + 2)/4.$$

Since then, there were a few improvements of Mignotte's result, but the question of what is the best possible exponent is still open.

Example 13.2. Consider the polynomials $Q_n(x) = (q_nX - p_n)(X^2 - 2)$, where p_n/q_n are convergents in the continued fraction expansion of $\sqrt{2}$. The polynomial $Q_n(x)$ has two close roots: $x_1 = p_n/q_n$ and $x_2 = \sqrt{2}$. Since $|x_1 - x_2| < 1/q_n^2 \ll H(Q_n)^{-2}$, we conclude that $e(3) = 2$.

Example 13.3. Let α be an algebraic number of degree 3 and $Q(x)$ its minimal polynomial over $\mathbb{Z}$. According to the Davenport-Schmidt theorem (Theorem 13.11), there are infinitely many algebraic numbers β of degree ≤ 2 with the property that $|\alpha - \beta| \ll H(\beta)^{-3}$. Let $R(x)$ be the minimal polynomial of β over $\mathbb{Z}$. Let us consider the polynomial $P(x) = Q(x)R(x)$. It has roots α and β, and $H(P) \ll H(R) = H(\beta)$ (since α is fixed). We can assume that the degree of $P(x)$ is equal to 5 (if needed, we multiply it by a linear factor). Thus, we conclude that $e(5) \geq 3$.

Example 13.4 (Bugeaud-Dujella, 2011)**.** For $a \geq 1$, the roots of the polynomial

$$P_{4,a}(x) = (20a^4 - 2)x^4 + (16a^5 + 4a)x^3 + (16a^6 + 4a^2)x^2 + 8a^3x + 1$$

are approximately equal to

$$\begin{aligned}
r_1 &= -1/4a^{-3} - 1/32a^{-7} - 1/256a^{-13} + \dots,\\
r_2 &= -1/4a^{-3} - 1/32a^{-7} + 1/256a^{-13} + \dots,\\
r_3 &= -2/5a + 11/100a^{-3} + 69/4000a^{-7} + 4/5a\,i + \dots,\\
r_4 &= -2/5a + 11/100a^{-3} + 69/4000a^{-7} - 4/5a\,i + \dots.
\end{aligned}$$

We have $H(P_{4,a}) = O(a^6)$, $\operatorname{sep}(P_{4,a}) = |r_1 - r_2| = O(a^{-13})$. Furthermore, by applying Eisenstein's criterion to the reciprocal polynomial $x^4 P_{4,a}(1/x)$, we conclude that the polynomial $P(x)$ is irreducible. So, letting a tend to infinity, we obtain $e(4) \geq e_{\text{irr}}(4) \geq 13/6$. ♢

The families of polynomials from the previous example can be generalized to an arbitrary degree (in the construction of the polynomials $P_{n,a}$ the Catalan numbers $c_k = \frac{1}{k+1}\binom{2k}{k}$ are used). In this manner, the following inequality was proved in [65],

$$e_{\text{irr}}(n) \geq \frac{n}{2} + \frac{n-2}{4(n-1)},$$

which gives the best currently known bound for $e_{\text{irr}}(n)$ when $n \geq 4$.

For reducible polynomials, the best current bounds (and the first ones of the form $e(n) \geq cn$, for $c > 1/2$) are given in the following theorem from [66].

Theorem 13.16 (Bugeaud-Dujella, 2014)**.** *For $n \geq 4$, we have*

$$e(n) \geq \frac{2n-1}{3}.$$

Proof: We want to construct a parametric family of polynomials $p_{n,a}(x)$ of degree n which have one root very close to the rational number

$$x_a = (a+2)/(a^2+3a+1).$$

Then the polynomial

$$P_{n,a}(x) = ((a^2+3a+1)x - (a+2))p_{n-1,a}(x)$$

will have two close roots. The sequence of polynomials $p_{n,a}(x)$ is defined recursively by

$$\begin{aligned}
p_{0,a}(x) &= -1, \quad p_{1,a}(x) = (a+1)x - 1,\\
p_{n,a}(x) &= (1+x)p_{n-1,a}(x) + x^2 p_{n-2,a}(x). \qquad (13.43)
\end{aligned}$$

We claim that

$$p_{n,a}\Big(\frac{a+2}{a^2+3a+1}\Big) = \frac{(-1)^{n-1}}{(a^2+3a+1)^n}. \tag{13.44}$$

Indeed, (13.44) evidently holds for $n = 0$ and $n = 1$. Let us now assume that $n \geq 2$ and that (13.44) holds for $p_{n-1,a}(x)$ and $p_{n-2,a}(x)$. Then, from recurrence (13.43), we obtain

$$\begin{aligned} p_{n,a}\Big(\frac{a+2}{a^2+3a+1}\Big) &= \frac{(-1)^{n-2}}{(a^2+3a+1)^{n-1}} \cdot \frac{a^2+4a+3}{a^2+3a+1} \\ &\quad + \frac{(-1)^{n-3}}{(a^2+3a+1)^{n-2}} \cdot \frac{a^2+4a+4}{(a^2+3a+1)^2} \\ &= \frac{(-1)^{n-1}}{(a^2+3a+1)^n}, \end{aligned}$$

as claimed.

We will now show that for a sufficiently large positive integer a, the polynomial $p_{n,a}(x)$ has a root between x_a and

$$z_{n,a} = x_a + \frac{(-1)^n}{a(a^2+3a+1)^n}.$$

Observe that

$$(-1)^{n-1} p_{n,a}(x_a) = \frac{1}{(a^2+3a+1)^n} > 0.$$

According to Lagrange's mean value theorem (see [262, Chapter 3.1], [426, Chapter 5.3.2]), there exists $z'_{n,a}$ between x_a and $z_{n,a}$ such that

$$p_{n,a}(z_{n,a}) = p_{n,a}(x_a) + (z_{n,a} - x_a) p'_{n,a}(z'_{n,a}).$$

It is easily proved by induction that

$$p_{n,a}(x) = -1 + (a-n+2)x + ((n-1)a - (n-1)(n-2)/2)x^2 + \cdots$$

Since $x_a = 1/a + O(1/a^2)$, we have $p'_{n,a}(z'_{n,a}) = a + n + O(1/a)$. Therefore, for sufficiently large a, we obtain $p'_{n,a}(z'_{n,a}) > a$, which implies that

$$(-1)^{n-1} p_{n,a}(z_{n,a}) = \frac{1}{(a^2+3a+1)^n} - \frac{1}{a(a^2+3a+1)^n} p'_{n,a}(z'_{n,a}) < 0.$$

We conclude that the polynomial $P_{n,a}(x) = ((a^2+3a+1)x - (a+2))p_{n-1,a}(x)$ has two close roots: x_a and $y_{n,a}$, which lies between x_a and $z_{n-1,a}$. Hence,

$$\operatorname{sep}(P_{n,a}) \leq |x_a - y_{n,a}| \leq \frac{1}{a(a^2+3a+1)^{n-1}} \leq \frac{1}{a^{2n-1}}, \tag{13.45}$$

for sufficiently large a. Since the height of $P_{n,a}(x)$ is bounded from above by the product of a^3 and a number depending only on n, when we let that $a \to \infty$, we obtain

$$e(n) \geq \frac{2n-1}{3}. \qquad \square$$

Let us mention another variant of the problem of polynomial root separation. That is the question of how close can the absolute values of two real roots of a polynomial with integer coefficients be if those absolute values are distinct. In the paper [68], a complete answer to the question of the best possible separation exponent was obtained. On the one hand, an analogue of Mahler's theorem was proved, showing that

$$||\alpha| - |\beta|| \gg H(P)^{-n+1}.$$

On the other hand, explicit examples which demonstrate that the exponent $-n+1$ cannot be improved were constructed. For example, if $n \geq 4$ is even, then the polynomial

$$q_{n,a}(x) = x^n - (ax^2 - 1)(1 - x^{n-3})$$

has two real roots α, β, such that

$$\alpha \approx -a^{-1/2} - \frac{1}{2}a^{-(n+1)/2} + \frac{1}{2}a^{-n+1},$$
$$\beta \approx a^{-1/2} + \frac{1}{2}a^{-(n+1)/2} + \frac{1}{2}a^{-n+1},$$

so that

$$||\alpha| - |\beta|| = |\alpha + \beta| \approx a^{-n+1} \ll H(P)^{-n+1}.$$

Results on other variants of the problem of polynomial root separation can be found in [38], [59], [67], [69], [107], [108], [151], [178, Chapter 18.1] and [340].

13.6 Exercises

1. Let $g(x)$ be the minimal polynomial of an algebraic number α, let m be a positive integer such that the coefficients of the polynomial $m \cdot g(x)$ are integers and let $\alpha^{(1)} = \alpha, \alpha^{(2)}, \ldots, \alpha^{(d)}$ be the roots of g. Prove that the constant $c(\alpha)$ in Liouville's theorem can be taken to be

$$c(\alpha) = m^{-1} \prod_{j=2}^{d} (1 + |\alpha| + |\alpha^{(j)}|)^{-1}.$$