Acta Mathematica Sinica, English Series
Mar., 2012, Vol. 28, No. 3, pp. 469–476
Published online: November 15, 2011
DOI: 10.1007/s10114-011-0518-5
Http://www.ActaMath.com

Acta Mathematica Sinica, English Series

On the Number of Polynomials with Small Discriminants in the Euclidean and p-adic Metrics

Jin YUAN
Department of Mathematics, Northwest University, Xi'an 710069, *P. R. China*
E-mail: *yuanj@nwu.edu.cn*

Natalia BUDARINA **Detta DICKINSON**
Department of Mathematics, Logic House, Maynooth, Kildare, Republic of Ireland
E-mail: *nbudarina@maths.nuim.ie* *ddickinson@maths.nuim.ie*

Abstract In this article it is proved that there exist a large number of polynomials which have small discriminant in terms of the Euclidean and p-adic metrics simultaneously. The measure of the set of points which satisfy certain polynomial and derivative conditions is also determined.

Keywords Diophantine approximation, discriminant, polynomial inequalities

MR(2000) Subject Classification 11J83, 11J54, 11J61

1 Introduction and Main Results

In this paper the distribution of the discriminants of integer polynomials is investigated. In particular, a lower bound for the number of polynomials which have small discriminant in both the Euclidean and p-adic metrics is determined. Since, the p-adic norm of these discriminants is small they are clearly divisible by large powers of p. This gives some information regarding the distribution of the roots of polynomials and shows that a large number of integer polynomials have roots which are simultaneously close in the p-adic and Euclidean norms. These and related questions were first introduced and studied by Mahler [1] in 1964. Other results (detailed below) have been separately proved for the real [2] and p-adic [3] fields. More information regarding root separation for integer polynomials may be found in [4–7] and [8].

First some notation is needed. Throughout this paper,

$$P(f) = a_n f^n + \cdots + a_1 f + a_0$$

is an integer polynomial with degree $\deg P = n$ and height $H = H(P) = \max_{0\le j\le n} |a_j|$. Let $\mu_1(A_1)$ be the Lebesgue measure of a measurable set $A_1 \subset \mathbb{R}$, and $\mu_2(A_2)$ the Haar measure of a measurable set $A_2 \subset \mathbb{Q}_p$. Using these definitions, define the product measure μ on $\mathbb{R} \times \mathbb{Q}_p$ by setting $\mu(A) = \mu_1(A_1)\mu_2(A_2)$ for a set $A = A_1 \times A_2$. The cardinality of a set S will be denoted by $\#S$. We will use the Vinogradov symbols $\ll$ (and $\gg$) where $a \ll b$ implies that there exists a constant $C > 0$ such that $a \le Cb$. If $a \ll b \ll a$ then we write $a \asymp b$.

Received September 29, 2010, accepted December 7, 2010
The second author is supported by the Science Foundation Ireland Programme (Grant No. RFP/MTH1512)

Let $\alpha_1, \dots, \alpha_n$ be the complex roots of the polynomial $P \in \mathbb{Z}[x]$. The *discriminant* of P, denoted by $D(P)$ is defined as

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

Alternatively, $D(P)$ can be defined as the determinant of a matrix containing only the coefficients of P. Hence $D(P) \in \mathbb{Z}$ and if P does not have multiple roots then

$$1 \le |D(P)| \ll H(P)^{2n-2}.$$

Consider the set of polynomials

$$\mathbf{P}_n(Q) = \{P \in \mathbb{Z}[x] : \deg P \le n, H(P) \le Q\}$$

and note that the cardinality of this set is comparable to Q^{n+1}. Finally, let $v_1, v_2 \in \mathbb{R}^+ \cup \{0\}$ and define the set of polynomials

$$\mathcal{P}_n(Q, v_1, v_2) = \{P \in \mathbf{P}_n(Q), 1 \le |D(P)| < Q^{2n-2-2v_1}, |D(P)|_p < Q^{-2v_2}\},$$

where $|\cdot|_p$ is the standard p-adic valuation. For this article we will consider $\mathcal{P}_n(Q, v_1, v_1)$ and for simplicity we will write $\mathcal{P}_n(Q, v_1) = \mathcal{P}_n(Q, v_1, v_1)$.

Theorem 1.1 *Let $n \ge 3$ and $0 \le v_1 < 1/3$ and let $Q_0(n) \in \mathbb{R}$ be a large constant. Then*

$$\#\mathcal{P}_n(Q, v_1) \gg Q^{n+1-4v_1} \quad \text{for all } Q > Q_0.$$

In [2] it was proved that $\#\mathcal{P}_n(Q, v_1, 0) \gg Q^{n+1-2v_1}$ and in [3] that $\#\mathcal{P}_n(Q, 0, v_2) \gg Q^{n+1-2v_2}$. These results come from metric theorems of Diophantine approximation in the real and p-adic fields respectively. To prove Theorem 1.1 it is necessary to prove a metric theorem in simultaneous Diophantine approximation in $\mathbb{R} \times \mathbb{Q}_p$. For $n = 2$ the discriminant has the form $D(P) = a_1^2 - 4a_0a_2$ and the estimates can be calculated directly as follows. Define v such that $p^{-v} < Q^{-2v_1} \le p^{-v+1}$. Choose a_2, with $0 < a_2 \le Q$ such that $p \nmid a_2$ and fix a_1. Then, there exists $0 \le s < p^v$ such that for $a_0 \equiv s \pmod{p^v}$ the linear congruence $4a_0a_2 \equiv a_1^2 \pmod{p^v}$ is satisfied. For any such triple (a_0, a_1, a_2) we have $|D(P)|_p \le p^{-v} < Q^{-2v_1}$. It remains to count the integers t such that $a_0 = s + tp^v$ and $|a_1^2 - 4a_2a_0| < Q^{2-2v_1}$. From this, t must lie in an interval of length at least $Q^{2-2v_1}/(4a_2p^v)$ which implies that there are at least Q^{1-4v_1} such t and therefore such a_0. Thus $\#\mathcal{P}_2(Q, v_1) \gg Q^{3-4v_1}$.

From now on we assume that $n \ge 3$. Fix a set $I \times K$ where I is an interval contained in $[0, 1) \subset \mathbb{R}$ and K is a cylinder contained in $\mathbb{Z}_p$. Define the set $\mathcal{L}_n = \mathcal{L}_n(v_0, v_1, c_0, \delta_0, Q)$ to be the set of $(x, w) \in I \times K$ such that the inequalities

$$|P(x)| < c_0 Q^{-v_0}, \quad |P(w)|_p < c_0 Q^{-v_0} \tag{1.1}$$

and

$$\delta_0 Q^{1-v_1} < |P'(x)| < c_0 Q^{1-v_1}, \quad \delta_0 Q^{-v_1} < |P'(w)|_p < c_0 Q^{-v_1} \tag{1.2}$$

hold for some $P \in \mathbf{P}_n(Q)$. Theorem 1.1 will follow from Theorem 1.2 below.

Theorem 1.2 *Let $n \ge 3$, $v_0 + v_1 = n/2$ and $0 \le v_1 < 1/3$. For all real numbers κ such that $0 < \kappa < 1$ there exist constants δ_0 and c_0 such that*

$$\mu(\mathcal{L}_n(v_0, v_1, c_0, \delta_0, Q)) > \kappa \mu(I \times K) \quad \text{for } Q \text{ sufficiently large.}$$

It can be readily verified using Dirichlet's box principle that if $c_0 = (n+1)^{3/4}$ then the upper bounds in (1.1) and (1.2) hold for all $(x, w) \in I \times K$. The main difficulty of this paper is to prove the existence of δ_0.

2 Preliminary Results

The following two lemmas show that there is no loss of generality in proving the theorems for the set of irreducible, primitive polynomials P which satisfy

$$H(P) \ll |a_n|, \quad |a_n|_p \gg 1. \tag{2.1}$$

Let $\mathcal{P}_n(Q)$ denote the set of such polynomials with height $H \le Q$ and degree at most n. The first lemma was proved in [9].

Lemma 2.1 *Let $E(x, w)$ be the set of $(x, w) \in \mathbb{R} \times \mathbb{Q}_p$ such that the inequality*

$$|P(x)||P(w)|_p < H(P)^{-w}$$

has infinitely many solutions in reducible polynomials $P \in \mathbb{Z}[x]$ with $\deg P \le n$. Then $\mu(E(x, w)) = 0$ for $w > n - 1$.

The next lemma was proved in [10].

Lemma 2.2 *Let p be a prime number and $P \in \mathbb{Z}[x]$ be primitive and irreducible. Let $C = C(n, p) > 0$ be a constant. There exists a natural number m, $0 \le m \le c(n)$, where $c(n) > 0$ is a constant depending only on n, with the following property. Let $F(x) = P(x + m)$ and $T(x) = x^n F(1/x)$. Then $T(x) = b_n x^n + \cdots + b_1 x + b_0 \in \mathbb{Z}[x]$ satisfies*

$$|b_n| \gg H(T), \quad |b_n|_p \gg 1.$$

The transformations to F and T preserve the discriminant; i.e., $D(P) = D(F) = D(T)$ (see [2] for details).

Let $P \in \mathcal{P}_n(Q)$ have complex roots $\alpha_1, \ldots, \alpha_n$ and roots $\gamma_1, \ldots, \gamma_n$ in $\overline{\mathbb{Q}_p}$, where $\overline{\mathbb{Q}_p}$ is the smallest field containing $\mathbb{Q}_p$ and all algebraic numbers. From (2.1), it can be readily verified that

$$|\alpha_i| \ll 1 \quad \text{and} \quad |\gamma_i|_p \ll 1 \tag{2.2}$$

for $i = 1, \ldots, n$; i.e., the roots are bounded (see [11]). Define the sets

$$S_1(\alpha_j) = \Big\{x \in \mathbb{R} : |x - \alpha_j| = \min_{1 \le i \le n} |x - \alpha_i|\Big\}, \quad 1 \le j \le n,$$

$$S_2(\gamma_k) = \Big\{w \in \mathbb{Q}_p : |w - \gamma_k|_p = \min_{1 \le i \le n} |w - \gamma_i|_p\Big\}, \quad 1 \le k \le n.$$

We will consider the sets $S_1(\alpha_j)$ and $S_2(\gamma_k)$ for fixed j and k. Without loss of generality, we will assume that $j = k = 1$. The other roots of P are reordered so that

$$|\alpha_1 - \alpha_2| \le |\alpha_1 - \alpha_3| \le \cdots \le |\alpha_1 - \alpha_n|,$$

$$|\gamma_1 - \gamma_2|_p \le |\gamma_1 - \gamma_3|_p \le \cdots \le |\gamma_1 - \gamma_n|_p.$$

The next lemma is proved in [11].

Lemma 2.3 *Let $x \in S_1(\alpha_1)$ and $w \in S_2(\gamma_1)$ where α_1 and γ_1 are complex and p-adic roots of a polynomial $P \in \mathbb{Z}[x]$ respectively. Then,*

$$|x - \alpha_1| < n|P(x)||P'(x)|^{-1},$$

$$|w-\gamma_1|_p < |P(w)|_p|P'(w)|_p^{-1},$$
$$|x-\alpha_1| < 2^n \min\left(|P(x)||P'(\alpha_1)|^{-1}, (|P(x)||P'(\alpha_1)|^{-1}|\alpha_1-\alpha_2|)^{1/2}\right),$$
$$|w-\gamma_1|_p < \min\left(|P(w)|_p|P'(\gamma_1)|_p^{-1}, (|P(w)|_p|P'(\gamma_1)|_p^{-1}|\gamma_1-\gamma_2|_p)^{1/2}\right)$$

hold.

The following theorem [12] will deal with the case of small derivatives.

Theorem 2.4 ([12, Theorem 1.3]) *For any $(x,w) \in I \times K$, there exist a neighbourhood $W = U \times V \subseteq I \times K$ of (x,w) and a constant $\lambda > 0$ with the following property: for any $\delta > 0$ and ball $B \subset W$, there exists a constant $E > 0$ such that the set*

$$\bigcup_{P \in \mathcal{P}_n(Q)} \{(x,w) \in B : |P(x)| < \delta,\, |P(w)|_p < \delta,\, |P'(x)| < K_\infty,\, |P'(w)|_p < K_p\}$$

has measure at most $E\xi^\lambda \mu(B)$, where $\xi = \max\{\delta, (\delta^2 Q^{n-1} K_\infty K_p)^{\frac{1}{2(n+1)}}\}$.

Using the notation of [12], $f(t) = (t, t^2, \dots, t^n)$, $T_1 = \cdots = T_n = Q$, $\mathcal{R} = \mathbb{Z}$, $g(\mathbb{Z}) = 1$ and $S = \{p, \infty\}$ so that $\#S = 2$.

3 Proof of Theorem 1.1

Following (2.1) we need only to prove the theorems for $P \in \mathcal{P}_n(Q)$. Let $(x,w) \in \mathcal{L}_n$. Then, there exists $P \in \mathcal{P}_n(Q)$ such that (1.1) and (1.2) hold. Let $x \in S_1(\alpha_1)$ and $w \in S_2(\gamma_1)$, then from Lemma 2.3, we obtain

$$|x-\alpha_1| < nc_0\delta_0^{-1}Q^{v_1-v_0-1} \quad \text{and} \quad |w-\gamma_1|_p < c_0\delta_0^{-1}Q^{v_1-v_0}. \tag{3.1}$$

Let $v_1 < 1/3$ so that from $v_0 + v_1 = n/2$ we have $v_0 = 2v_1 + \beta$ which implies that

$$v_0 - v_1 = v_1 + \beta \tag{3.2}$$

for some $\beta > 0$. Develop the polynomial P' as a Taylor series in the neighborhood of the roots α_1 and γ_1. This will be demonstrated for the p-adic coordinate. Estimating each term of the Taylor series $P'(w) = \sum_{i=1}^n (i!)^{-1} P^{(i)}(\gamma_1)(w-\gamma_1)^{i-1}$ gives

$$|P''(\gamma_1)|_p|w-\gamma_1|_p \ll Q^{v_1-v_0} < \frac{\delta_0 Q^{-v_1}}{4},$$
$$|P^{(j)}(\gamma_1)|_p|w-\gamma_1|_p^{j-1} \ll Q^{(j-1)(v_1-v_0)} < \frac{\delta_0 Q^{-v_1}}{4(n-2)}$$

for $j = 3, \dots, n$ and Q sufficiently large. The fact that $P \in \mathbb{Z}[x]$ and (2.2) have been used to obtain the trivial bound $|P^{(j)}(\gamma_1)|_p \ll 1$. Thus,

$$\frac{\delta_0 Q^{-v_1}}{2} < \frac{|P'(w)|_p}{2} < |P'(\gamma_1)|_p < 2|P'(w)|_p < 2c_0 Q^{-v_1}. \tag{3.3}$$

Similarly in the real case, using (3.1) and (3.2), for Q sufficiently large, we obtain

$$\frac{\delta_0 Q^{1-v_1}}{2} < \frac{|P'(x)|}{2} < |P'(\alpha_1)| < 2|P'(x)| < 2c_0 Q^{1-v_1}. \tag{3.4}$$

(Again the trivial bound $|P^{(j)}(\alpha_1)| \ll Q$ is used for $j \geq 2$.) Using the facts that $P'(\alpha_1) = a_n \prod_{i=2}^n (\alpha_1 - \alpha_i)$ and $P'(\gamma_1) = a_n \prod_{i=1}^n (\gamma_1 - \gamma_i)$, the formulae for the discriminants can be rewritten to obtain

$$\begin{aligned}|D(P)| &= \left|a_n^{2n-2}\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2\right| = |P'(\alpha_1)|^2\left|a_n^{2n-4}\prod_{2\le i<j\le n}(\alpha_i-\alpha_j)^2\right|,\\ |D(P)|_p &= \left|a_n^{2n-2}\prod_{1\le i<j\le n}(\gamma_i-\gamma_j)^2\right|_p = |P'(\gamma_1)|_p^2\left|a_n^{2n-4}\prod_{2\le i<j\le n}(\gamma_i-\gamma_j)^2\right|_p.\end{aligned} \tag{3.5}$$

As all the roots are bounded, it follows from Lemma 2.2, (3.3), (3.4) and (3.5) that

$$\begin{aligned}|D(P)| &\ll |P'(\alpha_1)|^2Q^{2n-4} \ll Q^{2n-2-2v_1},\\ |D(P)|_p &\ll |a_n^{2n-4}|_p|P'(\gamma_1)|_p^2 \ll Q^{-2v_1}.\end{aligned} \tag{3.6}$$

Thus, for every point $(x,w)\in\mathcal{L}_n$ there exists a polynomial $P\in\mathcal{P}_n(Q)$ which satisfies (3.6). Also, for any such point there exists a polynomial P with roots (α_i,γ_j) satisfying the system of inequalities

$$|x-\alpha_i| < nc_0\delta_0^{-1}Q^{v_1-v_0-1}, \qquad |w-\gamma_j|_p < c_0\delta_0^{-1}Q^{v_1-v_0} \tag{3.7}$$

for $1\le i,j\le n$. For each pair of roots (α_i,γ_j) of P denote the set of solutions of (3.7) by $\mathcal{M}_{ij}(P)$. Let $\mathcal{M}(P)=\bigcup_{1\le i,j\le n}\mathcal{M}_{ij}(P)$. Let s be the number of polynomials $P\in\mathcal{P}_n(Q)$ which satisfy (3.6). By (3.7) and the inequalities

$$\kappa\mu(I\times K) < \mu(\mathcal{L}_n) < s\mu(\mathcal{M}(P)) < 2^3sn^3c_0^2\delta_0^{-2}Q^{-2v_0+2v_1-1} \ll sQ^{-2v_0+2v_1-1},$$

we obtain $s\gg Q^{2v_0-2v_1+1}=Q^{n+1-4v_1}$. Note that by Theorem 1.2 we may choose κ to be close to 1.

4 Proof of Theorem 1.2

Again, from the arguments in Section 2 we need only to prove the theorem for polynomials which satisfy (2.1). Suppose that for $\delta_0>0$ one or both of the lower bounds in (1.2) does not hold. This defines two sets:

$$\begin{aligned}\mathcal{L}_n' &= \{(x,w) \text{ satisfying (1.1)} : |P'(x)| < c_0Q^{1-v_1}, |P'(w)|_p < \delta_0Q^{-v_1}\},\\ \mathcal{L}_n'' &= \{(x,w) \text{ satisfying (1.1)} : |P'(x)| < \delta_0Q^{1-v_1}, |P'(w)|_p < c_0Q^{-v_1}\}.\end{aligned}$$

Then, $\mathcal{L}_n=(I\times K)\setminus(\mathcal{L}_n'\cup\mathcal{L}_n'')$. It will be demonstrated that $\mu(\mathcal{L}_n')<\frac{1-\kappa}{2}\mu(I\times K)$. Similar results can be obtained in exactly the same way for $\mathcal{L}_n''$. This will obviously imply that $\mu(\mathcal{L}_n)>\kappa\mu(I\times K)$.

First we deal the case of small first derivatives. Note that since $v_1<1/3$ there exists $\varepsilon>0$ such that $v_1=1/3-\varepsilon$. Choose a real number $\gamma>0$ such that $\gamma<3\varepsilon/2$ and let $\mathcal{B}_n$ denote the set of $(x,w)\in\mathcal{L}_n'$ satisfying

$$Q^{1-v_1-\gamma} < |P'(x)| < c_0Q^{1-v_1}, \quad Q^{-v_1-\gamma} < |P'(w)|_p < \delta_0Q^{-v_1}. \tag{4.1}$$

Let $\mathcal{B}_n'$ be defined by $\mathcal{L}_n'=\mathcal{B}_n\cup\mathcal{B}_n'$. From Theorem 2.4, the measure of $\mathcal{B}_n'$ tends to zero as $Q\to\infty$. Hence, for Q sufficiently large, $\mu(\mathcal{B}_n')<\frac{1-\kappa}{4}\mu(I\times K)$. It remains to be shown that $\mu(\mathcal{B}_n)\le\frac{1-\kappa}{4}\mu(I\times K)$ for sufficiently small δ_0.

Assume without loss of generality, that the closest roots of P to x and w are α_1 and γ_1 respectively. Estimates for $|P'(\alpha_1)|$ and $|P'(\gamma_1)|$ are now obtained. From Lemma 2.3, (1.1) and (4.1), it follows that

$$|x-\alpha_1| < nc_0 Q^{v_1-v_0-1+\gamma}, \quad |w-\gamma_1|_p < c_0 Q^{v_1-v_0+\gamma}.$$

Using Taylor's theorem for $P'(f)$ and (3.2) the inequalities

$$\frac{1}{2}|P'(x)| < |P'(\alpha_1)| < 2|P'(x)|, \quad \frac{1}{2}|P'(w)|_p < |P'(\gamma_1)|_p < 2|P'(w)|_p$$

can be obtained in the same way as (3.3) and (3.4). Thus, from (4.1)

$$\frac{1}{2}Q^{1-v_1-\gamma} < |P'(\alpha_1)| < 2c_0 Q^{1-v_1}, \quad \frac{1}{2}Q^{-v_1-\gamma} < |P'(\gamma_1)|_p < 2\delta_0 Q^{-v_1}. \tag{4.2}$$

Let $\sigma(P)$ denote the set of points for which (1.1) and (4.2) hold. Using Lemma 2.3 this set is defined by the inequalities

$$|x-\alpha_1| < nc_0 Q^{-v_0}|P'(\alpha_1)|^{-1}, \quad |w-\gamma_1|_p < c_0 Q^{-v_0}|P'(\gamma_1)|_p^{-1}.$$

Note that $\mathcal{B}_n \subset \bigcup_{P\in\mathcal{P}_n(Q)} \sigma(P)$. We will show that the measure of this union is small.

Choose two real numbers u_1 and u_2 with the following properties:

$$\begin{aligned} &u_1+u_2 = 1-2v_1,\\ &v_0 > u_1 > 2v_1+2\gamma-1 \geq v_1-1,\\ &v_0 > u_2 > 2v_1+2\gamma > v_1. \end{aligned} \tag{4.3}$$

That this is possible can be readily verified using the conditions on v_1, v_0 and γ. Then, define the set $\sigma_1(P)$ as the set of (x,w) for which the inequalities

$$|x-\alpha_1| < c_1 Q^{-u_1}|P'(\alpha_1)|^{-1}, \quad |w-\gamma_1|_p < Q^{-u_2}|P'(\gamma_1)|_p^{-1}$$

hold for c_1 to be chosen later. From (4.3) and Q sufficiently large we have that $\sigma(P) \subset \sigma_1(P)$. The polynomial P is now developed as a Taylor series in $\sigma_1(P)$ and each term is estimated from above. Only the real coordinate will be demonstrated. We have

$$|P'(\alpha_1)||x-\alpha_1| < c_1 Q^{-u_1}, \quad \frac{1}{j!}|P^{(j)}(\alpha_1)||x-\alpha_1|^j \ll Q^{1-j(u_1+1-v_1-\gamma)}$$

for $j=2,\ldots,n$. The fact that $|P^{(j)}(\alpha_1)| \ll Q$ was used. Thus, from (4.3), $|P(x)| \leq 2c_1 Q^{-u_1}$ for Q sufficiently large. It is similarly possible to estimate $P'(x)$ on $\sigma_1(P)$ so that $|P'(x)| \leq 3c_0 Q^{1-v_1}$. In exactly the same way the inequalities

$$|P(w)|_p \leq 2Q^{-u_2}, \quad |P'(w)|_p \leq 3\delta_0 Q^{-v_1}$$

can also be obtained.

Let $\mathbf{b}$ be the vector $(a_n,\ldots,a_2)$ and let $\mathcal{P}_n^{\mathbf{b}}(Q)$ be the set of polynomials in $\mathcal{P}_n(Q)$ which have the same vector $\mathbf{b}$. Note that the number of vectors $\mathbf{b}$ is at most $(2Q+1)^{n-1} \leq (3Q)^{n-1}$. We now use Sprindzuk's method of essential and inessential domains (see [11] for details). A polynomial $P \in \mathcal{P}_n^{\mathbf{b}}(Q)$ is called *essential* if $\mu(\sigma_1(P)\cap\sigma_1(P')) \leq \frac{1}{2}\mu(\sigma_1(P))$ for all polynomials $P' \in \mathcal{P}_n^{\mathbf{b}}(Q)$. It is called *inessential* otherwise. Let $E_n^{\mathbf{b}}(Q)$ be the set of essential P and $I_n^{\mathbf{b}}(Q)$ be the set of inessential P. Thus $\mathcal{P}_n^{\mathbf{b}}(Q) = I_n^{\mathbf{b}}(Q) \cup E_n^{\mathbf{b}}(Q)$ and

$$\bigcup_{P\in\mathcal{P}_n^{\mathbf{b}}(Q)} \sigma(P) = \Bigg(\bigcup_{P\in E_n^{\mathbf{b}}(Q)} \sigma(P)\Bigg) \cup \Bigg(\bigcup_{P\in I_n^{\mathbf{b}}(Q)} \sigma(P)\Bigg).$$

First we consider the essential polynomials. Note that $\mu(\sigma(P)) \le \frac{nc_0^2}{c_1}Q^{-2v_0+u_1+u_2}\mu(\sigma_1(P))$. Clearly $\sum_{P\in\mathcal{P}_n^{\mathbf{b}}(Q)}\mu(\sigma_1(P)) \le 2\mu(I\times K)$. Thus, from (4.3) and the fact that $v_0+v_1 = n/2$, the set of points lying in sets $\sigma(P)$ for $P\in E_n^{\mathbf{b}}(Q)$ satisfies

$$\mu\Big(\bigcup_{\mathbf{b}}\bigcup_{P\in E_n^{\mathbf{b}}(Q)}\sigma(P)\Big) \le \sum_{\mathbf{b}}\sum_{P\in E_n^{\mathbf{b}}(Q)}\mu(\sigma(P)) \le \sum_{\mathbf{b}}\sum_{P\in E_n^{\mathbf{b}}(Q)}\frac{nc_0^2Q^{-2v_0+u_1+u_2}}{c_1}\mu(\sigma_1(P))$$
$$\le \frac{3^{n-1}c_0^2n}{c_1}Q^{n-1}Q^{-2v_0+u_1+u_2}\mu(I\times K) = \frac{3^{n-1}c_0^2n}{c_1}\mu(I\times K).$$

Thus, by choosing $c_1 = \frac{4.3^n c_0^2 n}{1-\kappa}$ the measure of the set of points lying in sets $\sigma(P)$ for $P\in\bigcup_{\mathbf{b}}E_n^{\mathbf{b}}(Q)$ is at most $\frac{1-\kappa}{8}\mu(I\times K)$.

Now, let $P\in I_n^{\mathbf{b}}(Q)$. Then there exists $P'\in\mathcal{P}_n^{\mathbf{b}}(Q)$ such that $\mu(\sigma_1(P)\cap\sigma_1(P')) \ge \frac{1}{2}\mu(\sigma_1(P))$. Let $R = P-P'$ so that $R(f) = b_1f+b_0$. Then, R satisfies

$$\begin{aligned}&|b_1x+b_0| \le 4c_1Q^{-u_1}, \quad |R'(x)| = |b_1| \le 6c_0Q^{1-v_1},\\ &|b_1w+b_0|_p \le Q^{-u_2}, \quad |R'(w)|_p = |b_1|_p \le 3\delta_0Q^{-v_1}\end{aligned} \tag{4.4}$$

on $\sigma_1(P)\cap\sigma_1(P')$. From this it follows that $|b_i| \le 6c_0Q^{1-v_1}$. Define s_1 and s_2 such that $p^{s_1}\le Q < p^{s_1+1}$ and $p^{s_2}\le\delta_0 < p^{s_2+1}$. Also note that $1\le 3\le p^2$ for all primes p. Let $[\cdot]$ denote the integer part. Then, as $|b_1|_p \le 3\delta_0Q^{-v_1} \le p^{s_2+3-[s_1v_1]}$ we have $b_1 = p^Lb_1'$ for some integer b_1' with $(b_1',p)=1$ and $L\ge[s_1v_1]-s_2-3$. Since K is a cylinder we can write $K = B(c,p^{-l})$ where $c\in\mathbb{Z}$ and $|c|_p = p^{-T}$ for some T with $T<l$. Thus, if $w\in K$ then $|w|_p = p^{-T}$ and $|b_1w|_p = p^{-T-L}$. There are now two cases to consider. First assume that $p^{-(T+L)} > Q^{-u_2}$. Then, as $|b_1w+b_0|_p \le Q^{-u_2}$ we have $|b_0|_p = |b_1w|_p = p^{-T-L}$ so that $b_0 = p^Lb_0'$ for some $b_0'\in\mathbb{Z}$. Thus $b_1x+b_0 = p^L(b_1'x+b_0')$ and $|b_i'| \le 6c_0p^{-L}Q^{1-v_1}$ for $i=0,1$. From (4.4) and previously it follows that

$$|b_1'x+b_0'| \le 4c_1p^{-L}Q^{-u_1}, \quad |b_1'w+b_0'|_p \le p^LQ^{-u_2}.$$

For an inessential polynomial P these inequalities will hold for some b_1', b_0'. Thus, the problem has now been reduced to considering the measure of the set of points (x,w) for which the above inequalities hold for some suitable b_1', b_0'. The measure of the set of (x,w) satisfying this system for a fixed b_0' and b_1' is

$$\le 8c_1\frac{Q^{-u_1-u_2}}{|b_1'||b_1'|_p} \le \frac{8c_1Q^{-u_1-u_2}}{|b_1'|}$$

as b_1' is an integer and $(b_1',p)=1$. Next, for a fixed b_1', we obtain an upper bound for the number of b_0' such that $b_0'/b_1'\in I$ and $b_0'/b_1'\in K$. From these two inclusions we have that $b_0'\in b_1'I$ and $b_0'/b_1' = c+\sum_{i=0}^{\infty}a_ip^{l+i}$ with $a_i\in\{0,\dots,p-1\}$. Assume that b_0'/b_1' lies in both I and K and assume that t/b_1' also lies in K. Then

$$\frac{t}{b_1'} = \frac{b_0'}{b_1'} + \sum_{i=0}^{\infty}m_ip^{l+i}$$

with $m_i\in\{0,\dots,p-1\}$. Thus $t = b_0'+m_0b_1'p^l+\cdots > b_0'+b_1'p^l$. Hence $t-b_0' > p^l$ and the number of t for which t/b_1' lies in both I and K is at most $\frac{\mu_1(b_1^0 I)}{p^l} = |b_1'|\mu(I\times K)$. Therefore, summing over all b_1' with $|b_1'| \le 6c_0p^{-L}Q^{1-v_1}$ we have that the set of (x,w) satisfying this system has measure at most

$$48c_0c_1p^{-L}Q^{1-u_1-u_2-v_1}\mu(I\times K)\le 48c_0c_1\delta_0p^{4+v_1}Q^{1-u_1-u_2-2v_1}\mu(I\times K)$$
$$\le 48c_0c_1\delta_0p^{4+v_1}\mu(I\times K)$$

from (4.3) and the definitions of s_1, s_2 and L. Clearly, there exists δ_0 such that the measure of the set of points (x,w) which lie in $\sigma_1(P)$ for at least one $P\in I_n^{\mathsf{b}}(Q)$ is at most $\frac{1-\kappa}{8}\mu(I\times K)$.

Now we consider the second case when $p^{-(T+L)}\le Q^{-u_2}$. In this case we have that $|b_0|_p\le Q^{-u_2}\le p^{[s_1u_2]}$. Hence, for Q sufficiently large, there exists $b_0'\in\mathbb{Z}$ such that $b_0=p^{[s_1u_2]-T}b_0'$. We can also write $b_1=p^Lb_1'=p^{[s_1u_2]-T}p^{L-[s_1u_2]+T}b_1'$. Let $b_1''=p^{L-[s_1u_2]+T}b_1'$ so that $\#b_1'=\#b_1''\le 12c_0p^{-L}Q^{1-v_1}$ and $|b_1''|_p=p^{-(L-[s_1u_2]+T)}$ as $(b_1',p)=1$. Thus

$$|b_1''x+b_0'|\le 4c_1p^{-[s_1u_2]+T}Q^{-u_1},\quad |b_1''w+b_0'|_p\le p^{[s_1u_2]-T}Q^{-u_2}.$$

Again the measure of the set of (x,w) satisfying this system for a fixed b_0' and b_1'' is

$$\le 8c_1\frac{Q^{-u_1-u_2}}{|b_1''||b_1''|_p}\le 8c_1\frac{Q^{-u_1-u_2}p^{L-[s_1u_2]+T}}{|b_1''|}.$$

As before the number of b_0' for a fixed b_1'' is $|b_1''|\mu(I\times K)$. Finally therefore, the measure of the set of (x,w) satisfying the system is at most

$$96c_0c_1p^{-L}Q^{1-v_1}Q^{-u_1-u_2}p^{L-[s_1u_2]+T}\mu(I\times K)=96c_0c_1Q^{1-u_1-u_2-v_1}p^{-[s_1u_2]+T}\mu(I\times K).$$

Using the definition of s_1 this is

$$\le 96c_0c_1p^{u_2+1+T}Q^{1-u_1-2u_2-v_1}\mu(I\times K),$$

which can be made arbitrarily small for Q sufficiently large by (4.3). This completes the proof of the theorem.

References

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

[2] Bernik, V., Götze, F., Kukso, O.: Lower bounds for the number of integral polynomials with given order of discrimants. *Acta Arith.*, 133, 375–390 (2008)

[3] Bernik, V., Götze, F., Kukso, O.: On the divisibility of the discriminant of an integral polynomial by prime powers. *Lith. Math. J.*, 48, 380–396 (2008)

[4] Beresnevich, V., Bernik, V., Götze, F.: The distribution of close conjugate algebraic numbers. *Compos. Math.*, 146, 1165–1179 (2010)

[5] Bugeaud, Y., Dujella, A.: Root separation for irreducible integer polynomials. *Bull. London Math. Soc.*, doi: 10.1112/blms/bdr085 (2011)

[6] Bugeaud, Y., Mignotte, M.: Polynomial root separation. *Intern. J. Number Theory*, 6, 587–602 (2010)

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

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

[9] Zeludevich, F.: Simultane diophantische Approximationen abhangiger Grössen in mehreren Metriken. *Acta Arith.*, 46, 285–296 (1986)

[10] Bernik, V., Budarina, N., Dickinson, D.: Simultaneous Diophantine approximation in the real, complex and p-adic fields. *Math. Proc. Camb. Phil. Soc.*, 149, 193–216 (2010)

[11] Sprindžuk, V.: Mahler's problem in the metric theorem of numbers. Transl. Math. Monographs, Vol. 25, Amer. Math. Soc., Providence, RI, 1969

[12] Mohammadi, A., Salehi Golsefidy, A.: S-arithmetic Khintchine-type theorem. *Geom. Funct. Anal.*, 19, 1147–1170 (2009)