

# THE DISTRIBUTION OF ROOTS OF A POLYNOMIAL

Andrew Granville  
*Université de Montréal*

## 1. Introduction

How are the roots of a polynomial distributed (in  $\mathbb{C}$ )? The question is too vague for if one chooses one's favourite complex numbers  $z_1, z_2, \dots, z_d$  then the polynomial  $\prod_{j=1}^d (x - z_j)$  has its roots at these points. However if one looks at polynomials that arise frequently then one finds that certain patterns emerge. Take for example  $x^n - 1$ . Here the roots are equidistributed around the unit circle, at the points  $\{e(j/n) : 0 \leq j \leq n-1\}$ , and the larger  $n$ , the more points one has, and the denser they become. (Throughout this article,  $e(t) := e^{2\pi i t}$ .)

In terms of measure, write  $\mu_{\{f\}} = (1/n) \sum_{j=1}^n \delta_{z_j}$  for a polynomial with (not necessarily distinct) roots  $z_1, z_2, \dots, z_d$ , where  $\delta$  is the Dirac delta-measure. Let  $\nu_{\{|z|=1\}}$  be the Haar measure on the unit circle (that is, uniform distribution). Then we have  $\lim_{n \rightarrow \infty} \mu_{\{x^n-1\}} = \nu_{\{|z|=1\}}$  (that is, convergence in the sense of “weak convergence”).

Another interesting example is  $(x-1)^n$ ; in this case all the roots are at the same point on the unit circle, 1; and so  $\lim_{n \rightarrow \infty} \mu_{\{(x-1)^n\}} = \delta_1$ . One more example is  $x^n - 2$ . Here the roots are again equidistributed in angle where, as  $n$  gets larger, the more points one has, and the more uniformly distributed they become. But there is more than that. As  $n \rightarrow \infty$  we have  $2^{1/n} \rightarrow 1$ , so all of the roots get closer and closer to the unit circle as  $n \rightarrow \infty$ . Therefore  $\lim_{n \rightarrow \infty} \mu_{\{x^n-2\}} = \nu_{\{|z|=1\}}$ .

So what distinguishes those sequences of polynomials for which the limiting measure of the roots is the Haar measure on the unit circle? The most obvious difference if one compares polynomials  $x^n - a$  where  $a^{1/n} \rightarrow 1$  as  $n \rightarrow \infty$ , and polynomials like  $(x-1)^n$  is that the latter has coefficients whose size grow exponentially in  $n$ , whereas the former do not. The main point of this section is to prove a result along these lines: “If the coefficients of  $f(x) \in \mathbb{C}[x]$  are not too large then  $\mu_{\{f\}}$  is not far from  $\nu_{\{|z|=1\}}$ ”. Obviously we need to be more precise than this, but we run into a tricky question: What is the best measure of the size of the coefficients of a polynomial? There are several options used in the literature, and it is known that they do not differ in size by much – however the “by much” can be as large as exponential in the degree of  $f$  which is too much for our application.



The first result in this direction, due to Erdős and Turán (Erdős and Turán, 1950) used the re-normalized 1-norm. If  $f(x) = a_d \prod_{j=1}^d (x - \alpha_j) = \sum_{j=0}^d a_j x^j$  where  $a_d a_0 \neq 0$  then

$$L(f) := \frac{1}{(|a_d| |a_0|)^{1/2}} \left( \sum_{j=0}^d |a_j| \right).$$

Progress in arithmetic has suggested that the most natural height is the Mahler measure

$$M(f) := |a_d| \prod_{j=1}^d \max\{1, |\alpha_j|\};$$

this has several advantages, one of which is that if for a given algebraic number  $\alpha$  we take  $f$  to be the minimum polynomial for  $\alpha$  (over  $\mathbb{Q}$ ) and let  $M(\alpha) = M(f)$ , then the renormalized height  $h(\alpha) := (1/d) \log M(\alpha)$  is simple to use in calculations without reference to the smallest field to which  $\alpha$  belongs. Note that if  $f^*(x) = x^d f(1/x)$  then  $L(f^*) = L(f)$  and  $M(f^*) = M(f)$ .

Jensen's formula gives an analytic interpretation of Mahler's measure:

$$M(f) = \exp \left( \int_0^1 \log |f(e(t))| dt \right);$$

and so  $M(f) \leq \max_i |f(e(t))|$ . Now, note that  $|f(e(t))| \leq \sum_{j=0}^d |a_j| |e(jt)| \leq \sum_{j=0}^d |a_j| = L(f)(|a_d| |a_0|)^{1/2}$  and so  $M(f) \leq L(f)(|a_d| |a_0|)^{1/2}$ , which yields

$$\begin{aligned} \prod_{j=1}^d \max\{|\alpha_j|, 1/|\alpha_j|\} &= \prod_{j=1}^d \max\{1, |\alpha_j|\} \prod_{j=1}^d \max\{1, 1/|\alpha_j|\} \\ &= \frac{M(f)}{|a_d|} \cdot \frac{M(f^*)}{|a_0|} \leq \frac{(L(f)(|a_d| |a_0|)^{1/2})^2}{|a_d| |a_0|} = L(f)^2. \end{aligned}$$

We deduce the following result:

**LEMMA 1.1.** *Suppose that  $f_1, f_2, \dots$  is a sequence of polynomials, where  $f_d$  has (not necessarily distinct) roots  $\alpha_{d,1}, \alpha_{d,2}, \dots, \alpha_{d,d}$ , all non-zero. If  $L(f_d) = e^{o(d)}$  as  $d \rightarrow \infty$  then  $|\alpha_{d,j}| = 1 + o(1)$  for  $\{1 + o(1)\}d$  values  $j$ ,  $1 \leq j \leq d$ .*

This shows that most of the roots come in towards the unit circle. Now we wish to show that they are uniformly distributed around the circle. For a given polynomial  $f$  write the roots as  $\alpha_j = r_j e(\varphi_j)$  with each  $r_j \in \mathbb{R}^+$ . For  $0 \leq \alpha < \beta \leq 1$  define

$$N_f(\alpha, \beta) = \#\{j : 1 \leq j \leq d \text{ such that } \alpha \leq \{\varphi_j\} < \beta\}.$$

PROPOSITION 1.2 (Erdős and Turán, 1950). *For any polynomial  $f$  of degree  $d > 1$ , and any  $0 \leq \alpha < \beta \leq 1$ , we have*

$$|N_f(\alpha, \beta) - (\beta - \alpha)d| \leq 8 \sqrt{d \log L(f)}.$$

Combining these two results we immediately deduce the result we had guessed at earlier:

THEOREM 1.3. *Suppose that  $f_1, f_2, \dots$  is a sequence of polynomials in  $\mathbb{C}[x]$  where  $f_d$  has degree  $d$  and  $f_d(0) \neq 0$ . If  $L(f_d) = e^{o(d)}$  as  $d \rightarrow \infty$  then*

$$\lim_{d \rightarrow \infty} \mu_{\{f_d(x)\}} = \nu_{\{|z|=1\}}.$$

(We stress that this limit is in the sense of “weak convergence” of measures.)

Erdős and Turán’s proof of Proposition 1.2 boils down to the following optimization result.

LEMMA 1.4. *Fix  $\gamma \in [0, 1)$ . Suppose that  $g(x)$  has degree  $d$  with all of its roots on the unit circle, and that  $N_g(0, \gamma) = [\gamma d] + 2\Delta + 1$ . Then  $\max_t |g(e(t))| \geq \exp(\Delta^2/4(d+1))$ .*

*Deduction of Proposition 1.2 from Lemma 1.4.* Given  $f(x) = a_d \prod_{j=1}^d (x - \alpha_j) = \sum_{j=0}^d a_j x^j$  take  $g(x) = \prod_{j=1}^d (x - e(\varphi_j))$  so that  $N_f(0, \gamma) = N_g(0, \gamma)$ . Consider the inequality

$$\begin{aligned} \frac{|re(\varphi) - e(t)|^2}{r} &= r + \frac{1}{r} - 2 \cos(2\pi(\varphi - t)) \\ &\geq 2 - 2 \cos(2\pi(\varphi - t)) = |e(\varphi) - e(t)|^2. \end{aligned}$$

Multiply this over the roots  $r; e(\varphi_j)$  of  $f$ , to obtain

$$|g(e(t))|^2 \leq \frac{|f(e(t))|^2}{a_d^2 \prod_j |r_j|} \leq \frac{L(f)^2 |a_0 a_d|}{|a_0 a_d|} = L(f)^2$$

since  $|f(e(t))| \leq L(f) |a_0 a_d|^{1/2}$  as we established above, and so  $|g(e(t))| \leq L(f)$ . Combining this with Lemma 1.4, we deduce that

$$N_f(0, \gamma) \leq [\gamma d] + 1 + 4 \sqrt{(d+1) \log L(f)} \leq \gamma d + 8 \sqrt{d \log L(f)}$$

since  $L(f) \geq (|a_0| + |a_d|)/|a_0 a_d|^{1/2} \geq 2$ .

Let  $h(x) = \sum_{j=0}^d \overline{a_j} x^j$  so that  $L(h) = L(f)$  and  $N_f(\gamma, 1) = N_h(0, 1 - \gamma)$ . Therefore, by the above,

$$N_f(0, \gamma) = d - N_f(\gamma, 1) = d - N_h(0, 1 - \gamma) \geq \gamma d - 8 \sqrt{d \log L(h)} = \gamma d - 8 \sqrt{d \log L(f)}.$$

Now let  $h(x) = f(e(\alpha)x) = \sum_j b_j x^j$  so that  $b_j = e(j\alpha)a_j$  for each  $j$ , with  $L(h) = L(f)$ , and  $N_h(0, \gamma) = N_f(\alpha, \beta)$  where  $\gamma = \beta - \alpha$ . Thus we may assume, without loss of generality, that  $\alpha = 0$  by replacing  $f$  with  $h$ . The result then follows from the previous two displayed equations.

Their proof of Lemma 1.4 involves several ingenious arguments, blending facts then well-known about polynomials. In the next section we will see a different and complete proof of a related result so here we will just give a

*Sketch of their proof of Lemma 1.4.* The idea is to understand the optimal polynomial; that is,  $g$  satisfying the hypothesis for which  $\max_t |g(e(t))|$  is minimal. So the first thing they do is to show that it takes its maximal value at some point in-between each pair of roots of  $g(x)$  inside the arc in question. Next they apply a result of Turán which says that there cannot be a zero of  $g(x)$  at a distance less than  $\pi/2d$  from one of these maximal points; which implies that at least  $2\Delta$  roots must lie at the endpoints of the interval, and so at least one endpoint has a zero with multiplicity  $\geq \Delta$ . We know from basic complex analysis that a polynomial with a root of high multiplicity must get large, and thus they obtain their lower bound.

## 2. Algebraic Numbers

Theorem 1.3 is a purely analytic result, in that there are no algebraic requirements on  $f$ . It is of more interest in arithmetic to have such requirements; for example if we insist that all of the coefficients of  $f$  are integers then the roots of  $f$  are the union of various complete sets of conjugates of certain algebraic numbers. In this circumstance Bilu proved an arguably stronger result than Theorem 1.3 (in that it involves  $M(f)$  rather than  $L(f)$ ) with a better motivated proof. Also, as we shall see in the next section, it generalizes to higher dimension in a beautiful way.

For a compactly supported measure  $\mu$  on  $\mathbb{C}$  we define the *energy* by

$$E(\mu) := - \int \int \log |z - w| d\mu_z d\mu_w.$$

If  $\mu$  is finitely supported, at  $\{\alpha_1, \dots, \alpha_d\}$ , then define

$$E'(\mu) := - \sum_{i \neq j} \mu(\alpha_i) \mu(\alpha_j) \log |\alpha_i - \alpha_j| \quad \text{and} \quad \|\mu\| = \left( \sum_i \mu(\alpha_i)^2 \right)^{1/2}.$$

Note that  $E'(\mu)$  is not the same as  $E(\mu)$  since we miss out the  $i = j$  terms (and note that  $E(\mu) = \infty$  by including them). We quote a couple of useful results on measures from the literature:

LEMMA A. If  $\{\mu_d\}_{d=1,2,\dots}$  have finite support with  $\|\mu_d\| \rightarrow 0$  as  $d \rightarrow \infty$  and where the  $\mu_d$  weakly converge to  $\mu$ , then

$$E(\mu) \leq \liminf E'(\mu_d).$$

LEMMA B. If  $K \subset \mathbb{C}$  is compact then there exists a unique measure  $\nu = \nu_K$  for which  $E(\nu)$  is minimized over all measures  $\nu$  whose support is a subset of  $K$  (we call  $\nu_K$  the equilibrium measure of  $K$ ). If  $K = \{|z| = 1\}$  is the unit circle then  $E(\nu_K) = 0$ .

Now suppose  $f(x) \in \mathbb{Z}[x]$  has distinct roots  $\alpha_1, \dots, \alpha_d$  and lead coefficient  $a_d$ . The discriminant of  $f$  is a non-zero integer,  $\text{Disc}(f) := a_d^{2d-2} \prod_{i \neq j} (\alpha_i - \alpha_j)$ . Therefore

$$\begin{aligned} 0 \leq \frac{1}{d^2} \log(\text{Disc}(f)) &= \frac{2d-2}{d^2} \log |a_d| + \sum_{i \neq j} \frac{1}{d^2} \log |\alpha_i - \alpha_j| \\ &\leq \frac{2}{d} \log M(f) - E'(\mu_{\{f\}}), \end{aligned}$$

and so  $E'(\mu_{\{f\}}) \leq (2/d) \log M(f)$ . We deduce

THEOREM 2.1. Suppose that  $f_1, f_2, \dots$  is a sequence of polynomials in  $\mathbb{Z}[x]$  where  $f_d$  has degree  $d$  and  $f_d(0) \neq 0$ . If  $M(f_d) = e^{o(d)}$  as  $d \rightarrow \infty$  then

$$\lim_{d \rightarrow \infty} \mu_{\{f_d(x)\}} = \nu_{\{|z|=1\}}.$$

*Proof.* As  $f_d(x) \in \mathbb{Z}[x]$  we see  $\prod_j \max\{1, |\alpha_j|\} \leq M(f_d) = e^{o(d)}$  and  $\prod_j \max\{1, 1/|\alpha_j|\} \leq M(f_d^*) = M(f_d) = e^{o(d)}$ , so  $\mu_{\{f_d\}}$  is converging to some measure on the unit circle. Now since this is compact there must be some subsequence of the  $f_d$  such that  $\mu_{\{f_d\}}$  converges weakly to some limit, call it  $\mu$ , supported on  $\{|z| = 1\}$ , on that subsequence. But since  $\|\mu_d\| = 1/\sqrt{d} \rightarrow 0$  as  $d \rightarrow \infty$  we may apply Lemma A to deduce that  $E(\mu) \leq \liminf E'(\mu_d) \leq \liminf (2/d) \log M(f_d) = 0$ . On the other hand  $E(\mu) \geq E(\nu_{\{|z|=1\}}) = 0$  by Lemma B, and so  $E(\mu) = 0$ . However this implies that  $\mu = \nu_{\{|z|=1\}}$  by Lemma B, and this is true for any convergent subsequence. From the above compactness argument it is clear that all  $f_d$  belong to some convergent subsequence, and since they all have this same limiting measure the result follows.

If  $\alpha$  is an algebraic number with minimum polynomial  $f$  we define  $M(\alpha) = M(f)$ ; Theorem 2.1 can easily be reformulated in terms of a sequence of algebraic numbers  $\alpha_d$ .

### 3. In $k$ Dimensions: the Bilu Equidistribution Theorem

Bilu (Bilu, 1997) went on from here to consider whether the conjugates of different algebraic numbers of small height are distributed independently. In other

words if we are given sequences  $\{(\alpha_i, \beta_i) : i = 1, 2, \dots\}$  of algebraic numbers, where both  $\alpha_i$  and  $\beta_i$  have degree  $i$  over the rationals and both have small height (as above) then what is the joint distribution of the conjugates? In other words, let  $H_i$  be the subgroup of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  which gives all distinct pairs of conjugates  $S_i := \{(\alpha_i^\sigma, \beta_i^\sigma) : \sigma \in H_i\}$ , and then consider the measure

$$\mu_{S_i} = \frac{1}{|S_i|} \sum_{\sigma} \delta_{\{\alpha_i^\sigma, \beta_i^\sigma\}}.$$

Evidently  $S_i \subset \overline{\mathbb{Q}}^2$  and, in the limit we know (from the previous section) that these measures are supported on the two dimensional torus  $\mathbb{U}^2$  where  $\mathbb{U} := \{z \in \overline{\mathbb{Q}}^* : |z| = 1\}$ . Then the question is whether they have a limit and, if so, whether that limit is the Haar measure. In other words, writing  $\alpha_i^\sigma = c_i e(\varphi_{i,\sigma})$  and  $\beta_i^\sigma = b_i e(\theta_{i,\sigma})$ , we ask whether for any  $0 \leq u_j < v_j \leq 1$ ,

$$\#\{\sigma \in H_i : u_1 \leq \varphi_{i,\sigma} < v_1 \quad \text{and} \quad u_2 \leq \theta_{i,\sigma} < v_2\} \sim (v_1 - u_1)(v_2 - u_2)|H_i|$$

as  $i \rightarrow \infty$ ? There are some obvious cases in which this cannot be true: for example if  $\alpha_i = \beta_i$  for each  $i$ , or  $\alpha_i \beta_i = 1$  for each  $i$ . So the conjecture becomes that the pairs should be uniformly distributed on  $\mathbb{U}^2$ , unless they belong to some obvious family of exceptions and it is now necessary to try to determine the correct formulation of the exceptional set:

The  $k$ -dimensional algebraic torus  $\mathbb{T}_k$  is isomorphic to  $(\overline{\mathbb{Q}}^*)^k$ , and a *torsion subvariety* of  $\mathbb{T}_k$  is a translate of a subtorus by a torsion point. We will call a sequence of points  $\alpha_1, \alpha_2, \dots \in \mathbb{T}_k$  *strict* if there are only finitely many such points in any proper torsion subvariety. Bilu's result works for strict sequences of small height, though first we need to define height here:

Given  $\gamma \in \overline{\mathbb{Q}}^*$  define  $\deg(\gamma)$  to be the degree of the minimum polynomial of  $\gamma$ , and let  $H(\gamma) = M(\gamma)^{1/\deg(\gamma)}$  (thus the condition in Theorem 2 can be rewritten as  $H(\gamma_d) = 1 + o(1)$  if  $f_d$  is the minimum polynomial of  $\gamma_d$ ). For  $\gamma = (\gamma_1, \gamma_2, \dots, \gamma_k) \in \mathbb{T}_k$ , define  $\deg(\gamma) = \min_i \deg(\gamma_i)$ , and  $H(\gamma) = \prod_i H(\gamma_i)$ .

**THEOREM 3.1** (Bilu, 1997). *Suppose that  $\alpha_1, \alpha_2, \dots \in \mathbb{T}_k$  is a strict sequence with  $\deg(\alpha_d) \geq d$  for each  $d$ , and  $H(\gamma_d) = 1 + o(1)$  as  $d \rightarrow \infty$  (we call this last condition small height). Then*

$$\lim_{d \rightarrow \infty} \mu_{\{\alpha_d\}} = \nu_{\mathbb{U}^k}.$$

*Sketch of Proof.* As we noted above, almost all conjugates of  $\alpha_d$  are getting closer and closer to  $\mathbb{U}^k$  as  $d \rightarrow \infty$  and so, by compactness, there must be some subsequence that tends to a limiting measure (call it  $\nu$ ).

For any non-trivial character  $\chi : \mathbb{T}_k \rightarrow \overline{\mathbb{Q}}$  the sequence  $\chi(\alpha_d)$  is strict and has small height. Thus applying Theorem 2.1 to our subsequence we see that

$\chi_*(\nu) = \nu_{\mathbb{U}}$  (where  $\chi_*$  should be interpreted as the action of  $\chi$  on the support of the measure, and thus the measure). But this is true for any non-trivial character  $\chi$  and so  $\nu$  must be the Haar measure on  $\mathbb{U}_k$ , namely  $\nu_{\mathbb{U}^k}$ . But this is true for any convergent subsequence and so for the whole sequence (by the same argument as in the proof of Theorem 2.1).

This beautiful result has many powerful consequences. Most famous, perhaps, is

**COROLLARY 3.2** ((Zhang, 1995)). *Suppose that  $X \subset \mathbb{T}_k$  is Zariski closed. Let  $W$  be the union of the torsion subvarieties that lie entirely in  $X$ . There exists a constant  $c(X) > 1$  such that if  $\alpha \in X \setminus W$  then  $H(\alpha) > c(X)$ .*

*Proof.* Northcott's theorem tells us that there are only finitely many algebraic numbers of given degree below a certain height. So if Zhang's theorem is false then there is an strict sequence  $\alpha_1, \alpha_2, \dots \in \mathbb{T}_k$  with  $\deg(\alpha_d) \geq d$  for each  $d$ , and  $H(\alpha_d) = 1 + o(1)$  as  $d \rightarrow \infty$ . By Bilu's Theorem (Theorem 3.1) these become equidistributed around  $\mathbb{U}^k$ , and so, as  $X(\mathbb{T}_k)$  is closed (since  $X$  is Zariski closed), thus  $\mathbb{U}^k \subset X(\mathbb{T}_k)$ . However  $\mathbb{U}^k$  is Zariski dense (as may be proved by induction on  $k$ ) and so  $X(\mathbb{T}_k) = \mathbb{T}_k$  in which case  $W = X$  and the result is trivial.

This result was proved by Szpiro, Ullmo and Zhang for points on an abelian variety by rather different means, something that will be discussed by Ullmo (Ullmo, 2006) in a subsequent section.

It is perhaps a little difficult to understand Zhang's theorem, so let's examine a special case, the solutions to  $x + y = 1$  in algebraic numbers. There are four torsion solutions  $1 + 0 = 0 + 1 = 1$  and  $e(1/6) + e(5/6) = e(5/6) + e(1/6) = 1$ , so we now investigate solutions omitting these: So suppose that we have a solution  $\alpha + (1 - \alpha) = 1$  with  $H(\alpha)H(1 - \alpha)$  small. Note that if  $H(\beta)$  is small then most conjugates  $\beta^\sigma$  of  $\beta$  must be close to the unit circle, that is  $|\beta^\sigma| \approx 1$ . Thus for most conjugates  $\alpha^\sigma$  of  $\alpha$  we have  $|\alpha^\sigma|, |1 - \alpha^\sigma| \approx 1$ . The circles of radius 1 centered at 0 and 1 only intersect at  $e(1/6)$  and  $e(5/6)$ , so we must have  $\alpha^\sigma \approx e(\pm 1/6)$  whence  $1 - \alpha^\sigma \approx e(\mp 1/6)$  for almost all  $\sigma$ . In such cases  $(\alpha^\sigma)^2 - \alpha^\sigma + 1 = 1 - \alpha^\sigma(1 - \alpha^\sigma) \approx 0$ , and thus the norm of  $\alpha^2 - \alpha + 1$  over  $\mathbb{Q}$  is very small, whereas it should be a non-zero integer (and thus  $\geq 1$  in absolute value). Formalizing and refining this argument, Zagier (Zagier, 1993) was able to show that in any non-torsion algebraic solution of  $x + y = 1$  we have  $H(x)H(y) \geq ((1 + \sqrt{5}/2)^{1/2})$ . It is amusing to try to develop an analogous argument for other varieties (see for example (Bombieri and Zannier, 1995)).

#### 4. Lower Bounds on Heights

Kronecker established a result on roots of unity on the unit circle which can be re-interpreted as stating that for any integer  $d \geq 1$ , if  $M(\alpha) > 1$  then there exists a constant  $\delta(d) > 0$  such that  $M(\alpha) \geq 1 + \delta(d)$  for all  $\alpha$  of degree  $d$ . In 1933 Lehmer (Lehmer, 1933) made the extraordinary conjecture that  $\delta(d) \geq \delta(10) = .1762808\dots$  obtained from the example where  $\alpha$  is a root of  $x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$ .

In 1979 Dobrowolski (Dobrowolski, 1979) showed that one can take  $\delta(d) = (1 - \epsilon)(\log \log d / \log d)^3$  but this has not been much improved subsequently.

#### 5. Compact Sets with Minimal Energy

Let  $K$  be a compact subset of the complex plane and suppose that  $E(\nu_K) = 0$ . One example is where  $K$  is the unit circle but there are many other interesting examples besides (for example the line segment  $[-2, 2]$ ). Rumely (Rumely, 1999) showed that Bilu's result, our Theorem 2.1, can be extended when appropriately reformulated to any such  $K$  (note though that Rumely prefers to work with the *capacity* of  $K$ , which is given by  $\exp(-E(\nu_K))$ , and is thus 1 in this case).

I cannot resist at least mentioning the first few results of capacity theory as they motivate some of the ideas in this article, which link several obvious notions: First we have that if  $\alpha_1, \dots, \alpha_d \in K$  is the support of measure  $\mu = \mu_\alpha$  where  $\mu_\alpha(\alpha_j) = 1/d$  then

$$E(\nu_K) = \lim_{d \rightarrow \infty} \min_{\alpha_1, \dots, \alpha_d \in K} E'(\mu_\alpha).$$

The right-side here is the logarithm of what Fekete called the *transfinite diameter* of a compact set  $K$ . From this one can deduce that  $\nu_K$  is supported only on the outer boundary of  $K$ .

Second we have

$$E(\nu_K) = \lim_{d \rightarrow \infty} \min_{\substack{\text{monic } f(z) \in \mathbb{C}[z] \\ \deg f = d}} \frac{1}{d} \sup_{z \in K} \log |f(z)|;$$

the right-side here is the logarithm of the *Chebyshev constant* of  $K$ .

The Mahler measure used above, when  $K$  is the unit disk, can be re-interpreted as a product of parts. The infinite part is the product of terms  $\max\{1, |\alpha|\}$ , the “local parts” the prime powers dividing  $|a_d|$ . In defining an appropriate height function for more general  $K$  we give the same definition for the local parts, but the infinite part is now defined as the exponential of minus the *potential* function for  $K$ . More explicitly

$$M_K(\alpha) := |a_d| \prod_{\sigma} G(\alpha^\sigma, \infty; K),$$



where our Green's function,  $G(z, \infty; K)$ , is defined as  $E(\nu_K) + \int_K \log(|z-w|) d\nu_K(w)$ . (Note that  $G(z, \infty; K) = \max(0, \log(|z|))$  when  $K = D(0, 1)$ .) We interpret  $M_K(f) = M_K(\alpha)$  for any root  $\alpha$  of irreducible  $f$ ; and  $M_K(fg) = M_K(f)M_K(g)$ .

Now, as in the proof of Theorem 2.1, we have, using the above and the well-known fact that  $G(z, \infty; K) \geq 0$  for all  $z$ ,

$$0 = E(\nu_K) \leq \liminf E'(\mu_\alpha) \leq \liminf \frac{2}{d} \log M_K(\alpha) = 0.$$

In this way, Rumely proved:

**THEOREM 5.1.** *Fix a compact set  $K$  with  $E(\nu_K) = 0$ . Suppose that  $f_1, f_2, \dots$  is a sequence of polynomials in  $\mathbb{Z}[x]$  where  $f_d$  has degree  $d$  and  $f_d(0) \neq 0$ . If  $M_K(f_d) = e^{o(d)}$  as  $d \rightarrow \infty$  then*

$$\lim_{d \rightarrow \infty} \mu_{\{f_d(x)\}} = \nu_K.$$

## Acknowledgements

Thanks to Ashkan Nikeghbali for pointing out to me, during the workshop, that a result like Lemma 1.1 is easily deduced from the method in (Hughes and Nikeghbali, 2006). Also to Robert Rumely for his remarks (and corrections) on these notes. Parts of this lecture were derived from notes kindly lent to me by Yuri Bilu.

## References

- Bilu, Y. (1997) Limit distribution of small points on algebraic tori, *Duke Math. J.* **89**, 465–476.
- Bombieri, E. and Zannier, U. (1995) Algebraic points on subvarieties of  $\mathbb{G}_m^n$ , *Internat. Math. Res. Notices* **1995**, 333–347.
- Dobrowolski, E. (1979) On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.* **34**, 391–401.
- Erdős, P. and Turán, P. (1950) On the distribution of roots of polynomials, *Ann. Math.* **51**, 105–119.
- Hughes, C. and Nikeghbali, A. (2006) The zeros of random polynomials cluster uniformly near the unit circle, to appear.
- Lehmer, D. H. (1933) Factorization of certain cyclotomic functions, *Ann. Math.* **34**, 461–479.
- Rumely, R. (1999) On Bilu's equidistribution theorem, *Contemp. Math.* **237**, 159–166.
- Ullmo, E. (2006) Manin–Mumford, André–Oort, the equidistribution point of view, in this book.
- Zagier, D. (1993) Algebraic numbers close to both 0 and 1, *Math. Comp.* **61**, 485–491.
- Zhang, S. (1995) Positive line bundles on arithmetic varieties, *J. Amer. Math. Soc.* **8**, 187–221.



**INDEX**

- Bilu equidistribution theorem, 5
- capacity, 8
- energy, 4
- equilibrium measure, 5
- Lehmer’s conjecture, 8
- Mahler measure, 2
- potential function, 8
- small height, 6
- strict, 6
- torsion subvariety, 6
- Zhang’s theorem, 7