On the distribution of polynomials with integer coefficients

Attila Pethő
(University of Debrecen, Hungary)

based on a joint work with Shigeki Akiyama

Numeration and Substitution, Kyoto, May 5, 2012.

Definitions

• If $P \in \mathbb{R}[x]$, then $|\overline{P}|$: maximum of absolute values of the roots of P.

• For $v = (v_{d-1}, \dots, v_0) \in \mathbb{R}^d$ the polynomial $P_v = x^d + v_{d-1}x^{d-1} + \dots + v_0$ is called associated to v.

• $\mathcal{E}_d(B) \subset \mathbb{R}^d$ such that if $v \in \mathcal{E}_d(B)$ and P_v denotes the to v associated polynomial then $|\overline{P_v}| \leq B$.

• $\mathcal{E}_d^{(r,s)}(B) \subseteq \mathcal{E}_d(B)$. If $v \in \mathcal{E}_d^{(r,s)}(B)$ then P_v has r real and $2s$ non-real coefficients, $r + 2s = d$.

• $v_d = \lambda_d(\mathcal{E}_d(1))$, $v_d^{(r,s)} = \lambda_d(\mathcal{E}_d^{(r,s)}(1))$.

Preliminary results

Theorem 1 *Let $d \geq 1$ and r, s non-negative integers such that $r + 2s = d$. Then the boundary of the set $\mathcal{E}_d^{(r,s)}(1)$ is the union of finitely many algebraic surfaces.*

Idea of the proof: The polynomials on the boundary either have roots ± 1 or a complex number with absolute value one or have multiple real roots. The "inner boundary" is the surface $Disc(P) = 0$, which is a polynomial in the coefficients of P.

Theorem 2 *The set* $\mathcal{E}_d^{(r,s)}(1)$ *is Riemann measurable. Let* $R_k(x) = x^2 - y_j x + z_j, j = 1, \ldots, s$ *and put*

$$D_{r,s} = [-1,1]^r \times [0,1] \times [-2\sqrt{z_1}, 2\sqrt{z_1}] \times \cdots \times [0,1] \times [-2\sqrt{z_s}, 2\sqrt{z_s}].$$

Then we have

$$v_d^{(r,s)} = \lambda_d(\mathcal{E}_d^{(r,s)}) = \frac{1}{r!s!} \int_{D_{r,s}} |\Delta_r| \Delta_s \Delta_{r,s} \, dX,$$

where

$$\begin{aligned} \Delta_r &= \prod_{1 \le j,k \le r} (x_j - x_k), \\ \Delta_s &= \prod_{1 \le j,k \le r} Res_x(R_j(x), R_k(x)), \\ \Delta_{r,s} &= \prod_{j=1}^{r} \prod_{k=1}^{s} R_k(x_j) \end{aligned}$$

and $dX = dx_1 \ldots dx_r dy_1 dz_1 \ldots dy_s dz_s$.

The next lemma was proved by Akiyama, Brunotte, Pethő and Thuswaldner, 2008.

Lemma 3 *We have*

$$\mathcal{E}_d^{(r,s)}(B) = \mathit{diag}(B^d, \ldots, B)\mathcal{E}_d^{(r,s)}(1), \tag{1}$$

where diag$(v_1, \ldots, v_d)$ *denotes the* d*-dimensional diagonal matrix, whose entries are* $v_1, \ldots, v_d$.

Moreover

$$\lambda_d(\mathcal{E}_d^{(r,s)}(B)) = B^{d(d+1)/2}\lambda_d(\mathcal{E}_d^{(r,s)}(1)). \tag{2}$$

The next result is due to H. Davenport, 1964.

Lemma 4 *Let $\mathcal{R}$ be a closed bounded region in $\mathbb{R}^n$ and let* $\mathsf{N}(\mathcal{R}) = \#(\mathcal{R} \cap \mathbb{Z}^n)$ *and* $\mathsf{V}(\mathcal{R})$ *the volume of $\mathcal{R}$. Suppose that:*

• *Any line parallel to one of the n coordinate axes intersects $\mathcal{R}$ in a set of points which, if not empty, consists of at most h intervals.*

• *The same is true (with m in place of n) for any of the m dimensional regions, $1 \leq m \leq n-1$, obtained by projecting $\mathcal{R}$ on one of the coordinate spaces defined by equating a selection of $n-m$ of the coordinates to zero.*

Then

$$\mathsf{N}(\mathcal{R}) - \mathsf{V}(\mathcal{R}) \leq \sum_{m=0}^{n-1} h^{n-m} V_m,$$

where V_m is the sum of the m dimensional volumes of the projections of $\mathcal{R}$ on the various coordinate spaces obtained by equating any $n-m$ coordinates to zero, and $V_0 = 1$ by convention.

The assumptions of Lemma 4 satisfy, if the boundary of $\mathcal{R}$ is the union of finitely many algebraic surfaces.

Distribution of irreducible polynomials

Notations: in this section $P(X) \in \mathbb{Z}[X]$ is monic, of degree d and with $|\overline{P}| < B$.

- $N_d(B)$: the number of polynomials P.
- $N_d^{(r,s)}(B)$: number of $P(X)$, with signature (r, s).

- $I_d(B)$: the number of irreducible polynomials P.

- $I_d^{(r,s)}(B)$: number of irreducible polynomials P with signature (r, s).

Theorem 5 *Let $d \geq 1$ and r, s be non-negative integers such that $d = r + 2s$. Let $B > 0$. Then there exist constants c_1, c_2 depending only on r, s, d such that*

$$|N_d^{(r,s)}(B) - v_d^{(r,s)} B^{d(d+1)/2}| \leq c_1 B^{d(d+1)/2-1}$$

and

$$|N_d(B) - v_d B^{d(d+1)/2}| \leq c_2 B^{d(d+1)/2-1}.$$

Outline of the proof. It is clear that $P(X) \in \mathbb{Z}[X]$ monic, of degree d, with signature (r, s) and with $|\overline{P}| < B$ if and only if the vector of its coefficients belongs to $\mathcal{E}_d^{(r,s)}(B)$. Thus $N_d^{(r,s)}(B)$ is the number of lattice points in $\mathcal{E}_d^{(r,s)}(B)$.

The volume of $\mathcal{E}_d^{(r,s)}(B)$ is $v_d^{(r,s)} B^{d(d+1)/2}$.

The boundary of $\mathcal{E}_d^{(r,s)}(B)$ is the union of finitely many algebraic surfaces. $\longrightarrow$ Apply the Theorem of Davenport:

$$|N_d^{(r,s)}(B) - v_d^{(r,s)} B^{d(d+1)/2}| \leq \sum_{m=0}^{d-1} h^{d-m} V_m,$$

where h is independent from B.

V_m is the sum of the m dimensional volumes of the projections of $\mathcal{E}_d^{(r,s)}(B)$ on the various coordinate spaces Let $\mathbf{v} \in \mathcal{E}_d^{(r,s)} \subset \mathcal{E}_d$. Then, we have the trivial bound $|v_i| < 2^d, i = 1, \ldots, d$. The projection of $\mathcal{E}_d^{(r,s)}(B)$ to any line parallel to the i-th coordinate axis is covered by an interval of length at most $O(B^i), i = 1, \ldots, d$. Thus

$$V_m \leq O(B^{d(d+1)/2-(1+\ldots+m)}) \leq O(B^{d(d+1)/2-1}).$$

Theorem 6 *Let $d \geq 1$ and r, s be non-negative integers such that $d = r + 2s$. Let $B > 0$. Then there exist constants c_3, c_4 depending only on r, s, d such that*

$$|I_d^{(r,s)}(B) - v_d^{(r,s)} B^{d(d+1)/2}| \leq c_3 B^{d(d+1)/2-1},$$

and

$$|I_d(B) - v_d B^{d(d+1)/2}| \leq c_4 B^{d(d+1)/2-1}.$$

Outline of the proof. {irreducible polynomials} = {polynomials} \ {reducible polynomials}. If a polynomial of degree d is reducible then it has a divisor of degree at least $\lceil d/2 \rceil$. Notice that the signature of the divisors may differ from the dividend. Thus

$$I_d^{(r,s)}(B) \geq N_d^{(r,s)}(B) - \left(\sum_{j=\lceil d/2 \rceil}^{d-1} N_j(B) N_{d-j}(B) \right).$$

Using Theorem 5 we obtain

$$\begin{aligned} I_d^{(r,s)}(B) &\geq v_d^{(r,s)} B^{d(d+1)/2} - \left(\sum_{j=\lceil d/2 \rceil}^{d-1} v_j B^{j(j+1)/2} v_{d-j} B^{(d-j)(d-j+1)/2} \right) \\ &+ O(B^{d(d+1)/2-1}). \end{aligned}$$

Now

$$B^{j(j+1)/2} B^{(d-j)(d-j+1)/2} = B^{j(j+1)/2+(d-j)(d-j+1)/2}$$

and we have the estimation

$$\frac{(d-j)(d-j+1)}{2} + \frac{j(j+1)}{2} = \frac{d(d+1) - 2j(d-j)}{2} \leq \frac{d(d+1)}{2} - 1$$

for the exponents. Thus

$$I_d^{(r,s)}(B) \geq v_d^{(r,s)} B^{d(d+1)/2} - O(B^{d(d+1)/2-1}).$$

The lower bound is an immediate consequence of Theorem 5.

Distribution of Salem polynomials

A polynomial with integral coefficients is *Salem polynomial* if all but one roots lie in and at least one on the unit circle. It is well known that the degree of a Salem polynomial is even, it has two real roots one of which is larger, the other is less then one and all others are non-real complex numbers, lying on the unit circle. Moreover they are reciprocal, i.e., $P(X) = X^d P(1/X)$.

Denote $S_d(B)$ the number of Salem polynomials $P(X) = X^{2d} + p_{d-1}X^{2d-1} + \ldots + p_{d-1}X + 1$ such that $|p_{d-1}| < B$. The number of irreducible polynomials among the Salem polynomials will be denoted by $S_d^{irr}(B)$.

Theorem 7 *Let $d \geq 1$ and $B > 0$. Then there exist constants c_5, c_6 depending only on d such that*

$$|S_d(B) - v_{d-1}^{(d-1,0)} B^{d-1}| \leq c_5 B^{d-2}$$

and

$$|S_d^{irr}(B) - v_{d-1}^{(d-1,0)} B^{d-1}| \leq c_6 B^{d-2}$$

hold.

Outline of the proof. Set $P(X)/X^d = Q(y)$, where $y = X + 1/X$, and $\deg Q = d$. $Q(y)$ is totally real, i.e. has signature $(d, 0)$ and the coefficient of its $d-1$-degree term is p_{d-1}.

Denote the largest root of $P(X)$ by β. Then $1/\beta$ is an other root of $P(X)$. Hence $|p_{d-1} - (\beta + 1/\beta)| < 2(d-1)$. Apart from

$\beta + 1/\beta$ the zeroes of $Q(y)$ are in modulus at most 2. Thus, if B is large enough, then $\beta + 1/\beta$ is the dominant root of $Q(y)$.

The rest is analogous to the proof of the Pisot polynomial case.

Distribution of Pisot polynomials

A monic $P(X) \in \mathbb{Z}[X]$ is Pisot polynomial if all but one of its roots lie inside the unit circle. They are irreducible. $\mathcal{B}_d(M)$ is the set of coefficient vectors $(b_2, \ldots, b_d)$ of Pisot or Salem polynomials of form $P(X) = X^d - MX^{d-1} - b_2X^{d-2} - \ldots - b_d \in \mathbb{Z}[X]$. Akiyama et al., 2008 proved:

$$\mathcal{B}_d(M) - v_{d-1}M^{d-1} = O(M^{d-1-1/(d-1)}).$$

Now we improve this.

Theorem 8 *Let $d \geq 2$ Then we have*

$$\mathcal{B}_d(M) - v_{d-1}M^{d-1} = O(M^{d-2}).$$

Outline of the proof. Let $\mathcal{E}_{d-1} = \mathcal{E}_{d-1}(1)$. Denote β the largest root of the Pisot polynomial P and let $P = (X - \beta)(X^{d-1} + r_{d-2}X^{d-2} + \ldots + r_0$.
For a fixed integer $M > 0$ let $\psi_M : \mathcal{E}_{d-1} \mapsto \mathcal{B}_d(M)$ be defined as

$\psi_M(r_0, \ldots, r_{d-2}) = (r_{d-2}(M + r_{d-2}) - r_{d-3}, \ldots, r_1(M + r_{d-2}) - r_0, r_0(M + r_{d-2}))$.

This is a continuous mapping, which is injective if M is large enough.
The volume of $\psi_M(\mathcal{E}_{d-1})$ is

$$\lambda_{d-1}(\psi_M(\mathcal{E}_{d-1})) = \int_{\mathcal{E}_{d-1}} \det(J_1)\, d_{r_0} \ldots d_{r_{d-2}},$$

where J_1 denotes the Jacobian of ψ_M. One can show that $\det(J_1)$ is a polynomial in M of degree $d-1$ with leading coefficient one and such that its other coefficients are polynomials in $b_2, \ldots, b_d$.

Thus

$$\begin{aligned}\lambda_{d-1}(\psi_M(\mathcal{E}_{d-1})) &= M^{d-1}\int_{\mathcal{E}_{d-1}} d_{r_0}\dots d_{r_{d-2}} \\ &+ \sum_{j=0}^{d-2} M^j \int_{\mathcal{E}_{d-1}} p_j(r_0,\dots,r_{d-2})\, d_{r_0}\dots d_{r_{d-2}} \\ &= v_{d-1}M^{d-1} + O(M^{d-2}).\end{aligned}$$

As ψ_M is an algebraic mapping and the boundary of $\mathcal{E}_{d-1}$ is the union of finitely many algebraic surfaces, the same is true for $\psi_M(\mathcal{E}_{d-1})$.

Let $M > 2^d$. We show that $(b_2,\dots,b_d) \in \mathbb{Z}^{d-1}$ is a lattice point of $\psi_M(\mathcal{E}_{d-1})$ iff $P(X) = X^d - MX^{d-1} - b_2X^{d-2} - \dots - b_d$ is a Pisot or Salem polynomial. Thus

$$|\mathcal{B}_d(M)| = |\psi_M(\mathcal{E}_{d-1}) \cap \mathbb{Z}^{d-1}|.$$

From here on we may repeat the proof of Theorem 5 because the assumptions of Lemma 4 hold for $\psi_M(\mathcal{E}_{d-1})$. Finally we obtain

$$|\mathcal{B}_d(M)| = v_{d-1}M^{d-1} + O(M^{d-2}).$$

Combining the results of Theorems 8 and 7 with the observation that the exponent of M in the main term in the first one is much bigger than in the second one we immediately obtain

Corollary 9 *Let $d \geq 2$ and $M > 0$ be integers. Denote $P_d(M)$ the number of Pisot polynomials of degree d and such that the coefficient of the term of degree $d-1$ is $-M$. Then*

$$P_d(M) = v_{d-1}M^{d-1} + O(M^{d-2}).$$