Uniform Distribution Theory **7** (2012), no.0, 000–000

uniform distribution theory

# ON THE DISTRIBUTION OF POLYNOMIALS WITH BOUNDED ROOTS II. POLYNOMIALS WITH INTEGER COEFFICIENTS

Shigeki Akiyama and Attila Pethő*

ABSTRACT. In the present paper we give a new type of statistical results on the distribution of integral polynomials of given degree. The main feature of our formula is that we can see a clear distinction with respect to the signature of polynomials. For example, we see that among certain polynomials in question, totally real ones are very rare. Further we show that reducible polynomials are negligible in every formula. We derive asymptotic results on Pisot, Salem and expanding polynomials that often appear as dilation constants of dynamical systems.

*Communicated by*

*Dedicated to the memory of Gérard Rauzy*

## 1. Introduction

For a real polynomial $P(X)$, its degree $d$ is written as $d = r + 2s$ where $r$ and $2s$ denote the numbers of its real and complex zeroes respectively. The pair $(r, s)$ is called the *signature* of $P(X)$. Since $d$ is fixed in the following discussion, we call $s$ the signature of $P(X)$, for simplicity. In the previous paper [4], we investigated the distribution of polynomials with real coefficients, with zeroes inside the unit disk and of given signature. The goal of this paper is to derive several consequences from [4] when we confine ourselves to polynomials with integer coefficients. An additional tool is a theorem of H. Davenport [8], which gives

2010 Mathematics Subject Classification: 11C08, 11K16, 11R09, 11R06.
Keywords: Distribution of integer polynomials, Pisot numbers, Salem numbers, expanding polynomials.
The authors are supported by the Japanese Society for the Promotion of Science (JSPS), Grant in aid 21540010 and Invitation Fellowship Program FY2011, L-11514.

a sharp estimate on the number of lattice points within a given region circumscribed by algebraic surfaces. As we restrict our attention to monic polynomials, the adjective "monic" is omitted throughout this paper.

We show a new type of statistical result on the distribution of integral polynomials of given degree and signature. A remarkable feature of our results is that we can observe explicit dependence on signatures in our asymptotic formulas.

Let us review several known statistical results on polynomials. For a complex polynomial $P(X)$ let $H(P)$ denote its height, i.e., the maximum of absolute values of the coefficients of $P$. Let $B$ denote a - typically large - integer or a real number. Clearly the number of integral polynomials of degree $d$ and height at most $B$ is $(2B)^d + O(B^{d-1})$, where the implied constant depends only on $d$. B.L. van der Waerden [20] confirmed a 'folklore' belief that reducible polynomials are negligible within $\mathbb{Z}[X]$. He proved that among such $(2B)^d + O(B^{d-1})$ polynomials the frequency of reducible polynomials with height at most $B$ and of degree $d = q + r$, which split into factors of degrees $q$ and $r$, tends to $B^{-q}$; if $q < r$, and to $B^{-r} \log B$; if $q = r$.

The investigation of the distribution of integral polynomials having a prescribed Galois group goes back to the beginning of the last century and has a vast literature. It was proved by K. Dörge [9] in 1925 that the natural density of integral polynomials of degree $d$; whose Galois groups are different from the symmetric group tends to zero. Later P.X. Gallagher [12] proved that the number of the above polynomials is $O(B^{d-1/2} \log B)$. We refer to D. Zywina [21] for recent developments. Although the statistical theory of integral polynomials has a rich history, we were not able to find an asymptotic formula for the number of integral polynomials $P(X)$ of degree $d$, signature $s$ and $H(P) \leq B$.

We wish to replace $H(P)$ by a different quantity, which we call 'measure' in this article. First, let us take $|\overline{P}|$, the maximum modulus of zeroes of $P(X)$. This is called *inclusion radius* or *house* of $P$. This measure is widely used in transcendental number theory [5] and in computer algebra [17]. The following trivial inequalities

$$\frac{|\overline{P}|}{d} \leq H(P) \leq (2|\overline{P}|)^d$$

yield some estimates of the number of integral polynomials of degree $d$ and $|\overline{P}| \leq B$, but it does not lead us to an asymptotic formula in terms of $|\overline{P}|$. As a consequence of [4] and the above-mentioned result of H. Davenport [8], an asymptotic formula for the number of such polynomials is proved in Theorem 3.1. Moreover we obtain asymptotic formula for polynomials with a fixed signature.

We also deal with some interesting subsets of $\mathbb{Z}[X]$, choosing different but suitable measures.

A polynomial in $\mathbb{Z}[X]$ is called *Pisot* if it has one real root greater than one, and the others are less than one in modulus. It is called *Salem* if it has one real root greater than one, and others are not greater than one in modulus and at least one root has modulus one. Pisot polynomials are irreducible and their real root greater than one is called *Pisot number*. A Salem polynomial factors into an irreducible Salem polynomial and cyclotomic polynomials. A *Salem number* is the real root greater than one of a Salem polynomial. There is a good overview on these polynomials and their applications in the book of M.J. Bertin et al. [6]. It is well known that Pisot and Salem numbers often appear as dilation constants of self-inducing structures in dynamical systems, and also in numeration systems, see e.g. [1].

It seems that neither $H(P)$ nor $|\overline{P}|$ gives us an asymptotic formula for Pisot and Salem polynomials. We employ the *trace*, $T(P) = -p_{d-1}$ of a polynomial $P(X) = X^d + p_{d-1}X^{d-1} + \cdots + p_0$, as our measure. Clearly for Pisot and Salem polynomials we have $|H(P) - |T(P)|| \leq d-1$. In [3] S. Akiyama et al. proved an asymptotic formula for the number of Pisot polynomials[1] of degree $d$ and trace $B$. In Corollary 4.2 we obtain a better error term for Pisot polynomials and Corollary 4.1 gives an asymptotic formula for Salem polynomials of degree $2d$ and trace $B$. These results shows that Salem polynomials are much less frequent than Pisot polynomials.

In the last section we are dealing with *expanding* polynomials, that is, polynomials in $\mathbb{Z}[X]$ whose zeroes lie outside the unit disk. The expanding polynomials also play an important role in numeration systems, see [1]. Similarly to Pisot polynomials, $H(P)$ or $|\overline{P}|$ does not seem to give an asymptotic formula for the number of expanding polynomials. Instead, we choose the norm $N(P) = (-1)^d p_0$ of a polynomial $P(X) = X^d + p_{d-1}X^{d-1} + \cdots + p_0$ as the measure. For expanding $P$, we easily get

$$|N(P)| \leq H(P) \leq 2^d |N(P)|.$$

In [2] S. Akiyama et al. proved an asymptotic formula for the size of the corresponding set. Combining results of [4] with the method of [2] we generalize that formula for the number of integral expanding polynomials of degree $d$ and with norm $B$ and with signature $s$. Finally we prove in a quantitative form that reducible expanding polynomials are in minority.

Our asymptotic formulae have the common shape $c_{d,s}B^{\kappa(d)} + O(B^{\kappa(d)-1})$. Dependency on signature is far from uniform. Indeed, combining Theorem 3.1 with Theorem 6.1 of Part I [4] we see that the frequency of the totally real

[1]The proof in [3] indeed shows that the contribution of Salem polynomials is small and falls into the error term of the formula.

polynomials among all polynomials in consideration is asymptotically $2^{-d^2/2}$, much less than the anticipated uniform frequency $2/d$.

## 2. Preliminary results

Let $d$ be a positive integer. If $P(X) \in \mathbb{R}[X]$ is of degree $d$, then its signature $s$ satisfies the inequality $0 \le s \le \lfloor d/2 \rfloor$. Each set of polynomials can be divided into $\lfloor d/2 \rfloor + 1$ disjoint classes according to their signatures. Our results and proofs will be true not only for these classes but also for their union, i.e., for the original set as well. To simplify the description, we introduce the "signature" $-1$, which means the union of the classes.

Let $B > 0$, which is typically a big integer or a real number. With the above convention on the signatures denote $\mathcal{E}_d^{(s)}(B), s = -1, \dots, \lfloor d/2 \rfloor$ the set of vectors $(p_{d-1}, \dots, p_0) \in \mathbb{R}^d$ such that the corresponding polynomial $P(X) = x^d + p_{d-1}x^{d-1} + \cdots + p_0$ has signature $s$ and satisfies the inequality $|\overline{P}| \le B$. We set[2] $\mathcal{E}_d^{(s)}$ for $\mathcal{E}_d^{(s)}(1)$. The $d$-dimensional Lebesgue measure $\lambda_d(\mathcal{E}_d^{(s)})$ will be denoted by $v_d^{(s)}$. The following theorem was proved by A.T. Fam [10].

**Theorem 2.1.** *Let $d \ge 1$ then*

$$v_d^{(-1)} = \begin{cases} 2^{2m^2} \displaystyle\prod_{j=1}^{m} \frac{(j-1)!^4}{(2j-1)!^2}, & \text{if } d = 2m, \\ 2^{2m^2+2m+1} \displaystyle\prod_{j=1}^{m} \frac{j!^2(j-1)!^2}{(2j-1)!(2j+1)!}, & \text{if } d = 2m+1. \end{cases} \tag{1}$$

For $s \ge 0$ we do not have such explicit formula, but we proved in [4] that $v_d^{(s)}$ can be computed by multiple integrals. In the next theorem $Res_x(P(x), Q(x))$ denotes the resultant of the polynomials $P(x)$ and $Q(x)$.

**Theorem 2.2.** *Let $d \ge 1$, $0 \le s \le \lfloor d/2 \rfloor$ and $r = d - 2s$. Then the set $\mathcal{E}_d^{(s)}$ is Jordan measurable. Let $R_k(x) = x^2 - y_j x + z_j, j = 1, \dots, s$ 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*

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

[2]In Part I the sets $\mathcal{E}_d^{(-1)}(B)$ and $\mathcal{E}_d^{(-1)}$ were denoted by $\mathcal{E}_d(B)$ and $\mathcal{E}_d$ respectively. We apologize for this small difference, but we were not able to find a uniform notation.

*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* $dX = dx_1 \dots dx_r dy_1 dz_1 \dots dy_s dz_s$.

The next theorem was proved for $s=-1$ by I. Schur [19], see also A.T. Fam and J.S. Meditsch [11], and for $0 \le s \le \lfloor d/2 \rfloor$ by ourselves [4].

**Theorem 2.3.** *Let $d \ge 1$ and $-1 \le s \le \lfloor d/2 \rfloor$. Then the boundary of $\mathcal{E}_d^{(s)}$ is the union of finitely many algebraic surfaces.*

Now we formulate an easy lemma, which connects $\mathcal{E}_d^{(s)}$ and $\mathcal{E}_d^{(s)}(B)$. It appeared in a slightly different form as Lemma 4.2 in [3], but the present one is more appropriate for our purposes.

**Lemma 2.1.** *Let $d \ge 1$ and $-1 \le s \le \lfloor d/2 \rfloor$. Then we have*

$$\mathcal{E}_d^{(s)}(B) = diag(B,\dots,B^d)\mathcal{E}_d^{(s)}, \tag{2}$$

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

*Moreover*

$$\lambda_d(\mathcal{E}_d^{(s)}(B)) = B^{d(d+1)/2}\lambda_d(\mathcal{E}_d^{(s)}). \tag{3}$$

P r o o f. It is clear that the second assertion is an immediate consequence of the first one. To prove the first assertion, remark that if the absolute value of the roots of $P(X) = X^d + p_{d-1}X^{d-1} + \dots + p_0$ are at most one, then the roots of $P_B(X) = X^d + p_{d-1}BX^{d-1} + \dots + p_0B^d$ are of absolute value at most $B$. Further, it is obvious that the signature of $P$ and $P_B$ is the same. Define the mapping $\psi_B : \mathcal{E}_d^{(s)} \mapsto \mathcal{E}_d^{(s)}$ as $\psi_B(z_1,\dots,z_d) = (z_1B,\dots,z_dB^d)$. Thus $(p_{d-1},\dots,p_0) \in \mathcal{E}_d^{(s)}$ if and only if $\psi_B(p_{d-1},\dots,p_0) \in \mathcal{E}_d^{(s)}(B)$. □

Later we will estimate the number of elements of bounded subsets of $\mathbb{Z}[X]$. We will transform such problems into lattice point counting problems in bounded regions. For our purpose the following result of H. Davenport is appropriate.

**Lemma 2.2** ([8, Theorem]). *Let $\mathcal{R}$ be a closed bounded region in the $n$ dimensional space $\mathbb{R}^n$ and let $\mathrm{N}(\mathcal{R})$ and $\mathrm{V}(\mathcal{R})$ denote the number of points with integral coordinates in $\mathcal{R}$ and the volume of $\mathcal{R}$, respectively. 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 obtained by projecting $\mathcal{R}$ on one of the coordinate spaces defined by equating a selection of $n-m$ of the coordinates to zero; and this condition is satisfied for all $m$ from 1 to $n-1$.*

*Then*

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

*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 2.2 are satisfied, if for example the boundary of $\mathcal{R}$ is the union of finitely many algebraic surfaces. We will apply this lemma in case when $\mathcal{R} = \mathcal{E}_d^{(s)}(B)$ or some transformation of it. By Theorem 2.3 the boundary of $\mathcal{E}_d^{(s)}$ is the finite union of algebraic surfaces, then, by Lemma 2.1 the same holds for $\mathcal{E}_d^{(s)}(B)$. We obtain the volume of $\mathcal{E}_d^{(s)}(B)$ from Theorems 2.1, 2.2 and Lemma 2.1. If we are able to estimate the remaining term precisely enough, then we obtain the desired result. In the next sections we perform this program.

## 3. The main distribution results

In this section we study the distribution of polynomials with integer coefficients and with bounded roots. For $d \ge 1$ and $0 \le s \le \lfloor d/2 \rfloor$ let $N_d^{(s)}(B)$ denote the number of $P(X) \in \mathbb{Z}[X]$, which are monic, of degree $d$, with signature $s$ and with $|\overline{P}| < B$. By our convention $N_d^{(-1)}(B) = \sum_{s=0}^{\lfloor d/2 \rfloor} N_d^{(s)}(B)$. Our aim is to prove

**Theorem 3.1.** *Let $d \ge 1$, $-1 \le s \le \lfloor d/2 \rfloor$ and $B > 0$. Then there exists a constant $c_1$ depending only on $s, d$ such that*

$$|N_d^{(s)}(B) - v_d^{(s)} B^{d(d+1)/2}| \le c_1 B^{d(d+1)/2-1}.$$

P r o o f. In the proof of Lemma 2.1 we introduced the mapping $\psi_B : \mathcal{E}_d^{(s)} \mapsto \mathcal{E}_d^{(s)}(B)$. It is continuous and bijective and transforms algebraic relations into algebraic ones. This implies together with Lemma 2.3 that the boundary of $\mathcal{E}_d^{(s)}(B)$ is the union of finitely many algebraic surfaces.

Let $d, s$ and $B$ be fixed. By Lemma 2.1 the volume of $\mathcal{E}_d^{(s)}(B)$ is $v_d^{(s)} B^{d(d+1)/2}$. It is clear that $P(X) \in \mathbb{Z}[X]$ is monic, of degree $d$, with signature $s$ and with $|\overline{P}| < B$ if and only if the vector of its coefficients belongs to $\mathcal{E}_d^{(s)}(B)$. Thus $N_d^{(s)}(B) = |\mathcal{E}_d^{(s)}(B) \cap \mathbb{Z}^d|$, i.e., the number of lattice points in $\mathcal{E}_d^{(s)}(B)$.

As for this set the assumptions of Lemma 2.2 are satisfied we obtain

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

where $h$ denotes the maximal number of intervals, which cover the intersection of $\mathcal{E}_d^{(s)}(B)$ with any line parallel to one of the $d$ coordinate axis. This number is finite and is independent from $B$.

Further $V_m$ is the sum of the $m$ dimensional volumes of the projections of $\mathcal{E}_d^{(s)}(B)$ on the various coordinate spaces obtained by equating any $d-m$ coordinates to zero, and $V_0 = 1$ by convention. Let $\mathbf{v} \in \mathcal{E}_d^{(s)} \subseteq \mathcal{E}_d^{(-1)}$ and $P_{\mathbf{v}}(X)$ the corresponding polynomial to $\mathbf{v}$. Then, as all roots of $P_{\mathbf{v}}(X)$ belong to the unit disc, we have the trivial bound $|v_m| < 2^d, m = 1, \dots, d$. Thus the above described projections of $\mathcal{E}_d^{(s)}$ are bounded. After applying $\psi_B$ to $\mathcal{E}_d^{(s)}$ we see that the length of the projection of $\mathcal{E}_d^{(s)}(B)$ to any line parallel to the $m$-th coordinate axis is covered by an interval of length at most $O(B^m), m = 1, \dots, d-1$. Thus

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

The theorem is proved. □

The next theorem gives a similar asymptotic formula for the number of irreducible polynomials $P(X) \in \mathbb{Z}[X]$ of degree $d$, signature $s$ and with $|\overline{P}| \le B$. This number is denoted by $I_d^{(s)}(B)$. The theorem is a quantitative version of Corollary of [18] on p. 47.

**Theorem 3.2.** *Let $d \ge 1$, $-1 \le s \le \lfloor d/2 \rfloor$ and $B > 0$. Then there exists a constant $c_2$ depending only on $s, d$ such that*

$$|I_d^{(s)}(B) - v_d^{(s)} B^{d(d+1)/2}| \le c_2 B^{d(d+1)/2-1}.$$

P r o o f. It is clear that we obtain the set of irreducible polynomials with the required properties if we remove from all polynomials the reducible ones. If a

polynomial of degree $d$ is reducible then it has a factor of degree in the interval $[\lceil d/2\rceil, d-1]$. Notice that the signature of the divisors may differ from the dividend, which we have to take into account. Thus

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

Using Theorem 3.1 we obtain

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

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 inequality

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

for the exponents. Thus

$$\begin{aligned} I_d^{(s)}(B) &\geq v_d^{(s)} B^{d(d+1)/2} - dO(B^{d(d+1)/2-1}) + O(B^{d(d+1)/2-1}) \\ &= v_d^{(s)} B^{d(d+1)/2} - O(B^{d(d+1)/2-1}). \end{aligned}$$

The lower bound

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

is an immediate consequence of Theorem 3.1. Thus the assertion is completely proved. □

The following corollary is an immediate consequence of Theorems 3.1 and 3.2.

**Corollary 3.1.** *Let $d \geq 1$, $-1 \leq s \leq \lfloor d/2\rfloor$ and $B > 0$. Then the number of reducible polynomials $P(X) \in \mathbb{Z}[X]$ of degree $d$, signature $s$ and such that $|\overline{P}| \leq B$ is $O(B^{d(d+1)/2-1})$.*

This means that there are much more irreducible polynomials than reducible ones in each signature classes. Theorems 3.1 and 3.2 show that $N_d^{(s)}(B)$ and $I_d^{(s)}(B)$ have for each $s$ the same growth rate in $B$. Hence the frequency of the appearance of a signature $s$ depends on the volume $v_d^{(s)}$. We quantify this by the next corollary.

**Corollary 3.2.** *Let $d \geq 1$, $0 \leq s \leq \lfloor d/2 \rfloor$ and $B > 0$. Then*

$$\frac{N_d^{(s)}(B)}{N_d^{(-1)}(B)} = \frac{v_d^{(s)}}{v_d^{(-1)}} + O(B^{-1}).$$

In Part I we studied the quotients $\frac{v_d^{(s)}}{v_d^{(-1)}}$. We proved among others that they are rational numbers, Theorem 5.1. In the case $s = 0$ we were able to show that the size of this quotient is $2^{-d^2/2}$, Theorem 6.1. This means that totally real polynomials are extremely rare. On the other hand for even $d$, in the same theorem, we obtained the conditional bound $\frac{v_d^{(d/2)}}{v_d^{(-1)}} \sim cd^{-3/8}$, i.e. totally complex polynomials has much bigger frequency as the average. It is an interesting problem to describe the asymptotic behavior $\frac{v_d^{(s)}}{v_d^{(-1)}}$ for other indices $s$.

## 4. Distribution of polynomials with a dominating root

Let $d, s$ be as earlier, $a \geq 1$ be fixed and $B \in \mathbb{Z}$. Denote by $\mathcal{B}_{d,a}^{(s)}(B)$ the set of polynomials $P(X) \in \mathbb{Z}[X]$ with trace $B$, signature $s$ and such that the absolute value of all but one of its zeroes is at most $a$. The set containing the irreducible elements of $\mathcal{B}_{d,a}^{(s)}(B)$ will be denoted by $\mathcal{B}_{d,a}^{(s),irr}(B)$. From the correspondence $P(X)$ with $P(-X)$, we easily have $|\mathcal{B}_{d,a}^{(s)}(B)| = |\mathcal{B}_{d,a}^{(s)}(-B)|$, i.e., we may assume $B > 0$ without loss of generality. Taking $a = 1$ and $s = -1$ we obtain the eminent example of this concept, the set of Pisot and Salem polynomials.

In [3], S. Akiyama et al. proved

$$\left| |\mathcal{B}_{d,1}^{(-1)}(B)| - v_{d-1}^{(-1)} B^{d-1} \right| = O(B^{d-1-1/(d-1)}).$$

A new embedding of $\mathcal{B}_{d,a}^{(s)}(B)$ into a $d-1$-dimensional lattice together with Theorem 2.2, especially the case $s = 0$, allow us to estimate the number of Salem polynomials, hence the Pisot polynomials as well. The main result of this section is

**Theorem 4.1.** *Let $d, s, B$ be integers and $a \in R$ such that $d, B \geq 1, a > 0$ and $-1 \leq s \leq \lfloor d/2 \rfloor$. Then*

$$\left| |\mathcal{B}_{d,a}^{(s)}(B)| - v_{d-1}^{(s)} a^{d(d+1)/2} B^{d-1} \right| = O(B^{d-2}),$$

*where the constant in the $O$ depends only on $d, s, a$.*

We obtain similar result for irreducible polynomials.

**Theorem 4.2.** *Let $d, s, a, B$ as in Theorem 4.1. Then*

$$\left| |\mathcal{B}_{d,a}^{(s),irr}(B)| - v_{d-1}^{(s)} a^{d(d+1)/2} B^{d-1} \right| = O(B^{d-2}),$$

*where the constant involved in the $O$ depends only on $d, s, a$.*

Before proving these theorems we formulate their consequences for Pisot and Salem polynomials. You find a good overview on these polynomials and their applications in the book of M.J. Bertin et al. [6]. It is well known that a Salem polynomial has to be reciprocal and its degree is even. Let $d \geq 1, B$ be integers. Denote $S_{2d}(B)$ the number of Salem polynomials $P$ of degree $2d$ and with $T(P) = B$. By the explanation of the beginning of this section we may restrict ourselves to the case $B > 0$. Finally the number of irreducible polynomials among the Salem polynomials will be denoted by $S_{2d}^{irr}(B)$.

**Corollary 4.1.** *With the above notations*

$$\left| S_{2d}(B) - v_{d-1}^{(0)} 2^{d(d+1)/2} B^{d-1} \right| = O(B^{d-2})$$

*and*

$$\left| S_{2d}^{irr}(B) - v_{d-1}^{(0)} 2^{d(d+1)/2} B^{d-1} \right| = O(B^{d-2}),$$

*where the constants in $O$ depend only on the degree $2d$.*

Finally, let $P_d^{(s)}(B)$ denote the number of Pisot polynomials of degree $d$, with signature $s$ and with trace $B$. We may assume $B > 0$ again. As a Pisot polynomial always has a real zero we have to modify the range of signatures as follows: if $d$ is odd, then $-1 \leq s \leq (d-1)/2$ and if $d$ is even then $-1 \leq s \leq d/2-1$. Notice that Pisot polynomials are always irreducible, thus we do not need to introduce extra counting functions for them.

**Corollary 4.2.** *With the above notations*

$$\left| P_d^{(s)}(B) - v_{d-1}^{(s)} B^{d-1} \right| = O(B^{d-2}),$$

*where the constant involved in the $O$ depends only on $d$.*

Now we turn to the proof of the statements.

**Proof of Theorem 4.1.** Let $M$ be a positive integer and $\mathcal{A}_{d,a}^{(s)}(M)$ be the set of vectors $(b_0, b_1, \ldots, b_{d-2}) \in \mathbb{R}^{d-1}$ such that all but one root of $x^d - Mx^{d-1} - b_{d-2}x^{d-2} - \cdots - b_0$ has modulus less than $a$. From the formula

$$(x^{d-1} + r_{d-2}x^{d-2} + \cdots + r_0)(x - M - r_{d-2}) = x^d - Mx^{d-1} - b_{d-2}x^{d-2} - \cdots - b_0.$$

we define the map $(r_0,\dots,r_{d-2}) \mapsto (b_0,\dots,b_{d-2})$. More explicitly, for fixed integers $d, s, M$ and real number $a$ we define $\chi_M : \mathcal{E}^{(s)}_{d-1}(a) \mapsto \mathcal{A}^{(s)}_{d,a}(M)$ by

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

This map is continuous and surjective. By uniqueness of the polynomial factorization, $\chi_M$ is even injective provided $M > da$. This is true because the modulus of the additional root, $M + r_{d-2}$, is larger than $a$. Thus for $M > da$ we have

$$|\mathcal{B}^{(s)}_{d,a}(M)| = |\chi_M(\mathcal{E}^{(s)}_{d-1}(a)) \cap \mathbb{Z}^{d-1}|.$$

As $\chi_M$ is a linear mapping and the boundary of $\mathcal{E}^{(s)}_{d-1}(a)$ is the union of finitely many algebraic surfaces, the same is true for $\chi_M(\mathcal{E}^{(s)}_{d-1}(a))$.

To apply Lemma 2.2 we have to compute the volume of $\chi_M(\mathcal{E}^{(s)}_{d-1}(a))$. Computation of the Jacobian leads to the formula:

$$\lambda_{d-1}(\chi_M(\mathcal{E}^{(s)}_{d-1}(a))) = \int_{\mathcal{E}^{(s)}_{d-1}(a)} |\det(J_1)|\, dr_0 \dots dr_{d-2}$$

with

$$J_1 = \begin{pmatrix} 0 & \dots & & 0 & -1 & M+2r_{d-2} \\ 0 & 0 & \dots & -1 & M+r_{d-2} & r_{d-3} \\ & & \ddots & & \ddots & \\ -1 & M+r_{d-2} & 0 & \dots & 0 & r_1 \\ M+r_{d-2} & 0 & 0 & \dots & 0 & r_0 \end{pmatrix}.$$

Readily $\det(J_1)$ is a monic polynomial in M of degree $d-1$ and its other coefficients are polynomials in $r_0,\dots,r_{d-2}$, i.e. they are bounded in absolute value by some polynomial in $a$. Thus

$$\begin{aligned} \lambda_{d-1}(\chi_M(\mathcal{E}^{(s)}_{d-1}(a))) &= M^{d-1} \int_{\mathcal{E}^{(s)}_{d-1}(a)} dr_0 \dots dr_{d-2} \\ &+ O\left(\sum_{j=0}^{d-2} M^j \int_{\mathcal{E}^{(s)}_{d-1}(a)} p_j(r_0,\dots,r_{d-2})\, dr_0 \dots dr_{d-2}\right) \\ &= \lambda_{d-1}(\mathcal{E}^{(s)}_{d-1}(a)) M^{d-1} + O(M^{d-2}) \\ &= v^{(s)}_{d-1} a^{d(d+1)/2} M^{d-1} + O(M^{d-2}). \end{aligned}$$

For the last step we used Lemma 2.1. From now on we may repeat the proof of Theorem 3.1 because the assumptions of Lemma 2.2 hold for $\chi_B(\mathcal{E}^{(s)}_{d-1}(a))$.

Finally we obtain

$$|\mathcal{B}_{d,a}^{(s)}(B)| = v_{d-1}^{(s)} a^{d(d+1)/2} B^{d-1} + O(B^{d-2}).$$

□

**Proof of Theorem 4.2.** Like in the proof of Theorem 3.2 we count the number of reducible polynomials in $\mathcal{B}_{d,a}^{(s)}(B)$. We assume that $B > ad$. Let $P(X) \in \mathcal{B}_{d,a}^{(s)}(B)$ be reducible and denote by $\beta$ its dominating root, which exists by the proof of the last theorem. There exist monic polynomials $Q(X), R(X)$ in $\mathbb{Z}[X]$ such that $d-1 \geq \deg Q \geq \deg R \geq 1$ and $P(X) = Q(X)R(X)$. It is clear that $\beta$ can be a zero only one of $Q$ and $R$, the zeroes of the other factor are bounded in absolute value by $a$. Using the estimates of Theorems 3.1 and 4.1 the number of reducible elements in $\mathcal{B}_{d,a}^{(s)}(B)$ is bounded by

$$\begin{aligned} & \sum_{m=\lfloor d/2 \rfloor}^{d-1} v_{m-1}^{(-1)} a^{m(m+1)/2} B^{m-1} v_{d-m}^{(-1)} a^{(d-m)(d-m+1)/2} + O(B^{d-3}) \\ = \quad & O(B^{d-2}), \end{aligned}$$

where the constant in $O$ depends only on $d$ and $a$. Combining this estimate with the result of Theorem 4.1 we complete the proof. □

Now we turn to the proof of the Corollaries.

**Proof of Corollary 4.1** It is well known, see e.g. [6, 14], 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 polynomials, i.e., $P(X) = X^d P(1/X)$. Let $B$ be an integer and assume that $P(X)$ is a Salem polynomial of degree $2d$ and trace $B$. Let $\beta$ denote the dominating root of $P(X)$.

Dividing $P(X)$ by $X^d$ leads to a polynomial $Q(y)$ in $y = X + 1/X$ with integer coefficients and of degree $d$. This polynomial has only real roots and its trace is $B$. If $\gamma$ denotes a zero of $P(X)$ then $\gamma + 1/\gamma$ is a zero of $Q(y)$. Moreover if $\gamma \neq \beta, 1/\beta$ then $|\gamma + 1/\gamma| \leq 2$. Thus

$$S_{2d}(B) = |\mathcal{B}_{d,2}^{(0)}(B)| \quad \text{and} \quad S_{2d}^{irr}(B) = |\mathcal{B}_{d,2}^{(0),irr}(B)|$$

and the statements follow immediately from Theorems 4.1 and 4.2. □

**Proof of Corollary 4.2** Let $B$ be a fixed integer. It is clear that if $P(X) = x^d - Bx^{d-1} + p_{d-2}x^{d-2} + \cdots + p_0 \in \mathbb{Z}[X]$ is such that all but one of its roots lie in the unit disk then it is a Pisot or Salem polynomial. Since the contribution of Salem polynomials is by Corollary 4.1 much smaller, we obtain the result.

## 5. Distribution of expanding polynomials

A polynomial is called expanding, if its zeroes lie outside the unit disk. There are only finitely many expanding polynomials with integer coefficients of degree $d$ and with fixed constant term $B$. By the argument of the beginning of the last section we may assume $B > 0$. Denoting this set by $\mathcal{C}_d(B)$ it was proved by S. Akiyama et al. [2] that

$$\lim_{B\to\infty} \frac{|\mathcal{C}_d(B)|}{B^{d-1}} = v_{d-1}^{(-1)}.$$

Later M. Madritsch and A. Pethő[3] [16] proved a formula with error term:

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

Of course $\mathcal{C}_d(B)$ can also be split in disjoint union of subsets according the signature of the occurring polynomials. In accordance of the earlier definitions these subsets will be denoted by $\mathcal{C}_d^{(s)}(B), -1 \le s \le \lfloor d/2 \rfloor$. Combining the method of [16] with Theorem 3.1 it is easy to prove

**Theorem 5.1.** *With the above notations*

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

As we being not able to improve the error term, we omit the details.

Through this paper we show that the number of irreducible polynomials is at least one magnitude larger than the reducible ones in the investigated sets. This was neither done in [2] nor in [16]. At the end of this paper we fill this gap. Let $\mathcal{C}_d^{(s),irr}(B)$ denote the subset of $\mathcal{C}_d^{(s)}(B)$, which contains its irreducible elements.

**Theorem 5.2.** *With the above notations*

$$|\mathcal{C}_d^{(s),irr}(B)| - v_{d-1}^{(s)} B^{d-1} = O(B^{d-1-1/d}).$$

P r o o f. As in the above proofs we estimate the number of reducible elements in $\mathcal{C}_d^{(s)}(B)$. Assume that $P(X)$ is such an element and $P(X) = Q(X)R(X)$ with $R, Q \in \mathbb{Z}[X], \deg R$ and $\deg Q \ge 1$. Of course both are expansive and one of them is of degree at least $\lfloor d/2 \rfloor$. Moreover, if the constant term of $Q$ is $q$, then $q$ is a divisor of $B$ and the constant term of $R$ is $B/q$. Thus the number of reducible polynomials is at most

$$\sum_{q|B} \sum_{m=\lfloor d/2 \rfloor}^{d-1} |\mathcal{C}_m^{(-1)}(q)||\mathcal{C}_{d-m}^{(-1)}(B/q)|.$$

[3]In both cited papers slightly different notation was used.

Each term of the inner sum is estimated in Theorem 5.2 by $O(B^{d-2})$, which implies the same estimate for the whole inner sum. Hence the number of reducible polynomials in $\mathcal{C}_d^{(s)}(B)$ is at most

$$d(B)O(B^{d-2}),$$

where $d(B)$ denotes the number of divisors of $B$, which is $o(B)$, see e.g. [15].

□

## 6. Acknowledgments

The first author moved from Niigata University to the current address in August 2012. The paper was written, when the second author was visiting Niigata University as a long term research fellow of JSPS. Both of us wish to express our deep gratitude to all the staffs in Department of Mathematics, Niigata University and the support from JSPS, Grant in aid 21540010 and Invitation Fellowship Program FY2011, L-11514. The second author was partially supported by the OTKA grant K104208 and by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project is implemented through the New Hungary Development Plan, co-financed by the European Social Fund and the European Regional Development Fund.

The authors thank Lajos Rónyai for his valuable hints to the literature. We also thank the anonymous referee for detailed comments, which considerably improved the presentation of this paper.

REFERENCES

[1] S. Akiyama, T. Borbély, H. Brunotte, A. Pethő and J. Thuswaldner, *Generalized radix representations and dynamical systems I*, Acta Math. Hungar., **108 (3)** (2005), 207 - 238.

[2] S. Akiyama, H. Brunotte, A. Pethő and J. M. Thuswaldner, *Generalized radix representations and dynamical systems III*, Osaka J. Math. **45** (2008), 347 – 374.

[3] ———, *Generalized radix representations and dynamical systems. IV*, Indag. Math. (N.S.) **19** (2008), no. 3, 333–348.

[4] S. Akiyama and A. Pethő, *On the distribution of polynomials with bounded roots I. Polynomials with real coefficients*, to appear in J. Math. Soc. Japan.

[5] A. Baker, Transcendental number theory. Second edition. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1990.

[6] M.-J. Bertin, A. Decomps-Guilloux, M. Grandet-Hugot, M. Pathiaux-Delefosse and J.P. Schreiber, Pisot and Salem numbers, Birkhauser Verlag, Basel, 1992.

[7] S.D. Cohen, *The distribution of the Galois groups of integral polynomials*, Illinois J. Math. **23** (1979), 135-152.

[8] H. Davenport, *On a principle of Lipschitz.* J. London Math. Soc. **26**, (1951). 179–183. *Corrigendum* ibid **39** (1964), 580.
[9] K. Dörge, *Über die Seltenheit der reduziblen Polynome und der Normalgleichungen*, Math. Ann. **95** (1925), 247–256.
[10] A. Fam, *The volume of the coefficient space stability domain of monic polynomials*, Circuits and Systems, 1989., IEEE International Symposium on, vol. 3, may 1989, pp. 1780 –1783.
[11] A. T. Fam and J. S. Meditch, *A canonical parameter space for linear systems design*, IEEE Trans. Automat. Control **23** (1978), no. 3, 454–458.
[12] P.X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Sympos. Pure Math., Amer. Math. Soc., vol. **24** (1973), 91–101.
[13] J. von zur Gathen and J. Gerhard, Modern computer algebra. Second edition. Cambridge University Press, Cambridge, 2003.
[14] E. Ghate and E. Hironaka, *The arithmetic and geometry of Salem numbers*, Bull. Amer. Math. Soc. **38** (2001), 293-314.
[15] Hua, Lo-keng, Introduction to number theory; translated from the Chinese by Peter Shiu, Berlin ; New York : Springer-Verlag, 1982.
[16] M.G. Madritsch and A. Pethő, *A note on generalized radix representations and dynamical systems*, Osaka Journal of Mathematics, to appear.
[17] M. Mignotte and D. Ştefanescu, Polynomials. An algorithmic approach. Springer Series in Discrete Mathematics and Theoretical Computer Science. Springer-Verlag Singapore, Singapore; Centre for Discrete Mathematics & Theoretical Computer Science, Auckland, 1999.
[18] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Third Edition, Springer, 1990.
[19] I. Schur, *Über Potenzreihen, die im Inneren des Einheitskreises beschränkt sind II*, J. reine angew. Math., **148** (1918), 122–145.[4]
[20] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. Phys. **43** (1936), 133-147.
[21] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, arXiv:1011.6465v1 [math.NT]

Received 0.0.0000
Accepted 0.0.0000

*Institute of Mathematics*
*University of Tsukuba*
*Tennodai 1-1-1, Tsukuba, Ibakari, JAPAN*
*E-mail*: akiyama@math.tsukuba.ac.jp

*Department of Computer Science*
*University of Debrecen*
*H-4010 Debrecen*
*P.O. Box 12, HUNGARY*
*E-mail*: Petho.Attila@inf.unideb.hu

[4]Reprinted in Schur's collected papers: I. Schur, Gesammelte Abhandlungen. Band I.-III. (German) Herausgegeben von Alfred Brauer und Hans Rohrbach. Springer-Verlag, Berlin-New York, 1973.