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

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 certain new type of statistical results on the distribution of integral polynomial of given degree. The main feature of our formula is that we can see clear distinction with respect to the signature of polynomials. For e.g., we see that among certain polynomials in question, totally real ones are very rare. Further we show that reducible polynomials are negligible in all formula. We derive asymptotic results of Pisot, Salem and expanding polynomials which often appears as dilation constants of dynamical systems.

Communicated by

Dedicated to the memory of Gérard Rauzy

1. Introduction

In the first part of this series of papers we investigated the distribution of polynomials with real coefficients with zeroes inside the unit circle and with given signature. In this second part, we show certain new type of statistical results on the distribution of integral polynomial of given degree and signature, as applications of part I [3].

We shall use several different counting methods in $\mathbb{Z}[X]$. Their common feature is that the number of elements of $\mathbb{Z}[X]$ with given degree, d, and with some parameter B, is finite. By abuse of terminology, we call B the 'measure' from

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.

now on. The task is to estimate the finite number with respect to d, B as precise as possible. We will consider in this paper solely monic polynomials.

Before explaining our results, we wish to review several known statistical results on polynomials. There is a folklore belief that the irreducible polynomials are the majority among $\mathbb{Z}[X]$. Letting B the maximum of absolute values of the coefficients, there are $(2\lfloor B\rfloor+1)^d$ such polynomials. It was proved by B.L. van der Waerden [21], that the proportion of reducible polynomials is small. More precisely he proved that the frequency of reducible polynomials 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 $q=r$. Similar result is expected for all natural defined subsets of $\mathbb{Z}[X]$.

The investigation of the distribution of Galois groups of integer polynomials goes back to the beginning of the last century and has vast literature. It was proved by K. Dörge [10] in 1925 that the natural density of polynomials with a Galois group different from the symmetric group tends to zero. Later P.X. Gallagher [13] proved that the number of the above polynomials is $\ll B^{d-1/2}\log B$. We will not continue the history of this investigations, but refer to a recent paper of D. Zywina [22].

Let $P(X)\in\mathbb{Z}[X]$ be a monic irreducible polynomial. Then the factor ring $\mathbb{Q}[X]/(P(X))$ is an algebraic number field of degree d. This correspondence is of course not bijective, infinitely many polynomials generate an isomorphic number field. A natural measure for a number field is its discriminant. The investigation of the number of number fields with discriminant below a given bound has rich history as well. The first non-trivial results in this direction were proved by H. Davenport and H. Heilbronn [8, 9]. They were able to describe the distribution of cubic number fields with discriminants at most B. Later their result was generalized to higher degree fields with given signature and given Galois group too. We do not go into details, but refer to the recent survey paper of H. Cohen [5].

Similarly, the distribution of irreducible polynomials over finite fields with given degree is well understood, see e.g. [18, 14].

Now we explain the results in the present paper. Firstly, we show asymptotic results on the number of polynomials of given degree and signature with the maximum of absolute value of the zeroes of $P(X)$, denoted by $|\overline{P}|$. This measure is widely used, see again [18] or any other computer algebra book. Secondly we will give similar type of asymptotic results for minimal polynomials of Pisot and Salem numbers, but measured by its 'trace', the coefficient of the second highest degree times -1. Since the other conjugates have modulus not greater than one, the trace gives an alternative natural measure than $|\overline{P}|$ to see its asymptotic

behavior. It is well known that Pisot and Salem number often appears as dilation constants of self-inducing structures in dynamical systems. Thirdly we show an asymptotic result for expanding polynomials measured by their 'norm', the constant term of the polynomial. Note that the norm in this case coincides the Mahler measure, the modulus of the product of the roots outside the unit circle. Thus this choice of measure is again natural. Within the framework of Part I, we can not only considerably generalize [1, 2, 17], but also making more precise our earlier results by improving the error term of the asymptotic formula. Finally we prove in all relevant cases that the number of reducible polynomials in the classes is at most as large as the error term we derived. Thus our results justify the above mentioned folklore expectation.

For a fixed measure the exponent of B in the main terms is the same for the different signature classes. However the constants depend on the signature. Thus the frequency of a signature depends essentially on the quotient of these constants. It follows from Theorem 6.1 of Part I [3] that the frequency of the totally real signature is very small, it is asymptotically $2^{-d^2/2}$. If the polynomials would distribute uniformly among the signature classes, then each would have frequency $2/d$.

2. Preliminary results

Let d be a positive integer. If $P(X) \in \mathbb{R}[X]$ is of degree d, then it has r real and s pair of non-real zeros, hence $d = r + 2s$. The pair (r, s) is called the signature of P. We have obviously $0 \le s \le \lfloor d/2 \rfloor$. As d and s uniquely determine r we will omit this parameter and call simply s the signature of P. 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 $P(X) = x^d + p_{d-1}x^{d-1} + \cdots + p_0$ satisfy the inequality $|\overline{P}| \le B$. For $B = 1$ we set[1] $\mathcal{E}_d^{(s)}$. The d-dimensional Lebesgue measure $\lambda_d(\mathcal{E}_d^{(s)})$ will be denoted by $v_d^{(s)}$. Although

[1] 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.

it is a'priori not clear, but these numbers exist. The first theorem was proved by A.T. Fam [11].

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

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

For $s \geq 0$ we do not have such an explicit form, but we proved in [3] that they can be computed by multiple integrals:

Theorem 2.2. *Let $d \geq 1$, $0 \leq s \leq \lfloor d/2 \rfloor$ and $r = d - 2s$. Then the set $\mathcal{E}_d^{(s)}$ 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

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

where

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

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

The next theorem was proved for $s = -1$ by I. Schur [20], see also A.T. Fam and J.S. Meditsch [12], and for $0 \leq s \leq \lfloor d/2 \rfloor$ by ourself [3].

Theorem 2.3. *Let $d \geq 1$ and $-1 \leq s \leq \lfloor d/2 \rfloor$. 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 [2], but the present one is more appropriate for our purposes.

Lemma 2.1. *Let $d \geq 1$ and $-1 \leq s \leq \lfloor d/2 \rfloor$. 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 $P(X) = X^d + p_{d-1}X^{d-1} + \cdots + p_0$ are at most one, then the roots of $P_B(X) = X^d + \frac{p_{d-1}}{B}X^{d-1} + \cdots + \frac{p_0}{B^d}$ are of absolute value at most B. Further, it is obvious that the signature of P and P_B is the same. Thus $(p_{d-1}, \dots, p_0) \in \mathcal{E}_d^{(s)}$ if and only if $(\frac{p_{d-1}}{B}, \dots, \frac{p_0}{B^d}) \in \mathcal{E}_d^{(s)}(B)$. □

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 was appropriate.

Lemma 2.2 ([7, 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

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

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 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 precise 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 $d \geq 1$ and $0 \leq s \leq \lfloor d/2 \rfloor$ 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 $d \geq 1$, $-1 \leq s \leq \lfloor d/2 \rfloor$ and $B > 0$. Then there exists a constant c_1 depending only on s, d such that*

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

Proof. In the proof of Lemma 2.1 we introduced already the mapping $\psi_B : \mathcal{E}_d^{(s)} \mapsto \mathcal{E}_d^{(s)}(B)$ defined as $\psi(z_1, \ldots, z_d) = (z_1 B, \ldots, z_d B^d)$. This is a continuous and bijective mapping, which transforms algebraic relations into similar 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

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

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 the $P_{\mathbf{v}}(X)$ belong to the unit circle, we have the trivial bound $|v_m| < 2^d, m = 1, \ldots, d$. Thus the above

described projections of $\mathcal{E}_d^{(s)}$ are bounded. After applying ψ_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 [19] 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

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

Using the result of Theorem 3.1 we obtain

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

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 estimation

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

for the exponents. Thus

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

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 as 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 s'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.

A *Pisot number* is a real algebraic number greater than one whose all other conjugates have modulus less than one. A *Salem number* is a real number greater than one whose other conjugates have modulus not greater than one and at least one conjugate has modulus exactly one. A Pisot (resp. Salem) polynomial is the minimal polynomial of a Pisot (resp. Salem) number.

In S. Akiyama et al. [2] it was 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 paragraph is

Theorem 4.1. *Let d, s, B be integers, $a \in R$ 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 O depends only on d, s, a.

We obtain similar result for irreducible polynomials.

Theorem 4.2. *Let d, s, aB 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 in 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. [4]. 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 $Tr(P) = B$. 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 we have*

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

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 denote $P_d^{(s)}(B)$ the number of Pisot polynomials of degree d, with signature s and with trace B. We may assume $B > 0$ again. As Pisot polynomials always have real zeroes we had to modify the range of signature as follows: if d is odd, then $-1 \le s \le (d-1)/2$ and if d is even then $-1 \le s \le d/2 - 1$. Notice finally 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 we have*

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

where the O constant 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 $(b_0, b_1, \dots, b_{d-2}) \in \mathbb{R}^{d-1}$ such that all but one roots of $x^d - Mx^{d-1} - b_{d-2}x^{d-2} - \dots - b_0$ have modulus not greater than a. From the formula

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

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

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

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

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

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

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

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

with

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

Obviously $\det(J_1)$ is a monic polynomial in M of degree $d-1$ and such that 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

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

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

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

□

Proof of Theorem 4.2. Like in the proof of Theorem 3.2 we count the number of reducible polynomials in $\mathcal{B}^{(s)}_{d,a}(B)$. We assume that $B > ad$. Let $P(X) \in \mathcal{B}^{(s)}_{d,a}(B)$ be reducible and denote β its dominating root, which exists by the proof of the last theorem. There exist $Q(X), R(X) \in \mathbb{Z}[X]$ such that $d-1 \geq \deg Q \geq \deg R \geq 1$ and $P(X) = Q(X)R(X)$. It is clear that β 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 $\mathcal{B}^{(s)}_{d,a}(B)$ is bounded by

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

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. [4, 15], 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 with trace B. Let β denote the dominating root of $P(X)$.

Dividing $P(X)$ by X^d it is clear that the result is a polynomial in $y = X+1/X$ with integer coefficients of degree d. Denote it by $Q(y)$. This has only real roots, i.e. $s = 0$, and its trace is B. If γ 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 circle then it is a Pisot or Salem polynomial. Since the contribution of Salem polynomial 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 circle. 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 S. Akiyama et al. [1] that

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

Later M. Madritsch and A. Pethő[2] [17] was able to prove a formula with the 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

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

these subsets will be denoted by $\mathcal{C}_d^{(s)}(B)$, $-1 \le s \le \lfloor d/2 \rfloor$. Combining the method of [17] with Theorem 3.1 it is easy to prove

Theorem 5.1. *With the above notations we have*

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

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

Through this paper we showed 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 [1] nor in [17]. 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 we have*

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

P r o o f. As in the earlier proofs we estimate again 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 $R, Q \in \mathbb{Z}[X], \deg R, \deg Q \ge 1$. Of course both have to be expansive and one of them has to be of degree at least $\lfloor d/2 \rfloor$. Moreover, if the constant term of Q is q, then it is a divisor of B and the constant term of R is B/q. Thus the number of reducible polynomials is at most

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

Each term of the inner sum can be estimated by 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. [16]

□

6. Acknowledgments

The paper was written, when the second author was visiting Niigata University as a long term research fellow of JSPS. He thanks the hospitality of the University and the support from JSPS.
His research was partially supported by the OTKA grant K100339 and by the TÁMOP

4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, cofinanced by the European Social Fund and the European Regional Development Fund.

The authors also thank Lajos Rónyai for his valuable comments to an earlier version and for hints to the literature.

REFERENCES

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

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

[3] S. Akiyama and A. Pethő, *On the distribution of polynomials with bounded roots I. Polynomials with integer coefficients*, in preparation.

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

[5] H. Cohen, *Constructing and counting number fields*, in Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002), Higher Ed., Beijing, 2002, 129– 138.

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

[7] H. Davenport, *On a principle of Lipschitz.* J. London Math. Soc. **26**, (1951). 179–183. *Corrigendum* ibid **39** (1964), 580.

[8] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields I,* Bull. London Math. Soc. 1 (1969), 345-348.

[9] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II,* Proc. Royal. Soc. A 322 (1971), 405-420.

[10] K. Dörge, *Über die Seltenheit der reduziblen Polynome und der Normalgleichungen*, Math. Ann. **95** (1925), 247–256.

[11] 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.

[12] 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.

[13] P.X. Gallagher, *The large sieve and probabilistic Galois theory*, Proc. Sympos. Pure Math., Amer. Math. Soc., vol. **24** (1973), 91–101.

[14] J. von zur Gathen and J. Gerhard, Modern computer algebra. Second edition. Cambridge University Press, Cambridge, 2003.

[15] E. Ghate and E. Hironaka, *The arithmetic and geometry of Salem numbers*, Bull. Amer. Math. Soc. **38** (2001), 293-314.

[16] Hua, Lo-keng, Introduction to number theory; translated from the Chinese by Peter Shiu, Berlin ; New York : Springer-Verlag, 1982.

[17] M.G. Madritsch and A. Pethő, *A note on generalized radix representations and dynamical systems*, Osaka Journal of Mathematics, to appear.

[18] M. Mignotte, Mathematics for computer algebra. Translated from the French by Catherine Mignotte. Springer-Verlag, New York, 1992.

[19] W. Narkiewicz, Elementary and analytic theory of algebraic numbers, Third Edition, Springer, 1990.
[20] I. Schur, *Über Potenzreihen, die im Inneren des Einheitskreises beschränkt sind II*, J. reine angew. Math., **148** (1918), 122–145.[3]
[21] B. L. van der Waerden, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. Phys. **43** (1936), 133-147.
[22] D. Zywina, *Hilbert's irreducibility theorem and the larger sieve*, arXiv:1011.6465v1 [math.NT]

Received 0.0.0000
Accepted 0.0.0000

Department of Mathematics
Faculty of Science
Niigata University
Ikarashi 2-8050, Niigata 950-2181, JAPAN
E-mail: akiyama@math.sc.niigata-u.ac.jp

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

[3]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.