Bull. Math. Soc. Sci. Math. Roumanie
Tome 60 (108) No. 2, 2017, 141–146

Distribution of Reducible Polynomials with a Given Coefficient Set

by

Shane Chern

Abstract

For a given set of integers $\mathcal{S}$, let $\mathcal{R}_n^*(\mathcal{S})$ denote the set of reducible polynomials $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ over $\mathbb{Z}[X]$ with $a_i \in \mathcal{S}$ and $a_0a_n \neq 0$. In this note, we shall give an explicit bound of $|\mathcal{R}_n^*(\mathcal{S})|$. We also present an application of this bound to reducible bivariate polynomials over $\mathbb{Z}[X,Y]$.

Key Words: Reducible polynomial, bivariate polynomial, counting function, Euler's identity
2010 Mathematics Subject Classification: Primary 11C08
Secondary 11N45

1 Introduction

Here and throughout this note, we say a polynomial is reducible if it is reducible over $\mathbb{Z}[X]$ or $\mathbb{Z}[X,Y]$. Furthermore, the notation $\mathbb{P}(F \text{ reducible})$ denotes the probability of F being reducible under a given coefficient set. In a recent paper [2], L. Bary-Soroker and G. Kozma proved the following

Theorem A. *Let $F = F(X,Y) = \sum_{i,j\leq n} \varepsilon_{i,j} X^iY^j$ be a bivariate polynomial of degree n with random coefficients $\varepsilon_{i,j} \in \{\pm 1\}$. Then*

$$\lim_{n\to\infty} \mathbb{P}(F \text{ reducible}) = 0.$$

This result originates from similar distribution problems of reducible univariate polynomials, which were studied for a long period. Let the *height* of a polynomial $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ with coefficients $a_i \in \mathbb{Z}$ be defined as $H(f) = \max\{|a_i| : i = 0, 1, \ldots, n\}$. For a fixed integer $n \geq 2$ and a real parameter $h \geq 1$, let $\mathcal{R}_n(h)$ denote the set of reducible polynomials $f(X)$ over $\mathbb{Z}$ with degree $n \geq 2$ and height $H(f) \leq h$, and $\mathcal{R}_n^*(h)$ the subset of $\mathcal{R}_n(h)$ with $f(0) \neq 0$. The bound of $|\mathcal{R}_n(h)|$ given by G. Kuba [7] reads

$$h^n \leq |\mathcal{R}_n(h)| \leq C_n h^n \quad \text{for all } n \geq 3 \text{ and } g \geq 1, \tag{1.1}$$

where $C_n > 0$ is a constant depending only on n. In fact, the left hand side comes directly from the reducibility of polynomials with $f(0) = 0$. On the other hand, the upper bound has been studied by many authors; see, e.g., [3, 5, 8, 9]. Furthermore, if we restrict that the coefficients of polynomials should be chosen from a given set $\mathcal{S}$, it is also natural to ask for the bound of number of such reducible polynomials with degree n, or at least the probability $p_{n,\mathcal{S}}$ of such random polynomials as $n \to \infty$; see [6] for the case $\mathcal{S} = \{0, 1\}$ and [10] for the case $\mathcal{S} = \{\pm 1\}$.

However, considering the notorious difficulty of proving

$$\lim_{n\to\infty} p_{n,\mathcal{S}} = 0$$

for some $\mathcal{S}$, as Bary-Soroker and Kozma mentioned, they wanted to seek for a modest generalization, that is, adding one degree of freedom, or more precisely, adding one more variable — just like that given in the above theorem.

2 Revisit of Bary-Soroker and Kozma's proof and our main result

Before presenting our main result, let us go back to Bary-Soroker and Kozma's proof of Theorem A. In my personal opinion, the most crucial part of their proof is the following proposition listed as Eq. (3) of their paper.

Proposition 1. *Let*

$$\Omega(n, h) = \left\{ f = \sum_{i=0}^{n} a_i X^i : a_i \textit{ odd and } H(f) \le 2h - 1 \right\}.$$

Then there exists an absolute constant $C > 0$ such that for any $n > 1$ and $h > 2$ the probability that a random uniform polynomial $f \in \Omega(n, h)$ is reducible satisfies

$$\mathbb{P}_{\Omega(n,h)}(f \text{ reducible}) \le C \cdot \frac{n(\log h)^2}{h} \left(1 + \frac{1}{2h}\right)^n.$$

In view of their proof of this proposition, whose idea is due to I. Rivin [9], I note that we can even step further. Again, let $\mathcal{S} = \{s_1, s_2, \ldots, s_k\}$ be a given set of integers, and $\mathcal{S}^* = \mathcal{S}\backslash\{0\}$. We denote by $\mathcal{R}_n^*(\mathcal{S})$ the set of reducible polynomials $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ with $a_i \in \mathcal{S}$ and $a_0 a_n \neq 0$. At last, let $d(n) = \sum_{d|n} 1$ be the divisor function whose summation runs over all positive divisors of n. Our result is

Theorem 1. *Let M be a positive integer such that*

$$s_i \not\equiv s_j \bmod M \textit{ for all } i \neq j \quad (i, j = 1, 2, \ldots, k).$$

Then

$$|\mathcal{R}_n^*(\mathcal{S})| \le 4(n-1)M^{n-2} \left(\sum_{a \in \mathcal{S}^*} d(a) \right)^2. \tag{2.1}$$

Remark 1. *One readily notes that a possible value of M is $\max \mathcal{S} - \min \mathcal{S} + 1$. However, for some $\mathcal{S}$, we could even find smaller M. For example, in the case of Bary-Soroker and Kozma's Proposition 1, that is, $\mathcal{S}$ being the set of odd integers in the interval $[-2h+1, 2h-1]$, they chose $M = 2h + 1$.*

Proof: We only need to slightly modify Bary-Soroker and Kozma's proof of Proposition 1. Let $\Omega_n(\mathcal{S})$ be the set of polynomials with $a_i \in \mathcal{S}$ and $a_0 a_n \neq 0$. We also fix $s, t > 0$ with $s + t = n$ and $b_0, c_0, b_s, c_t \in \mathbb{Z}$ with $a_0 = b_0 c_0$ and $a_n = b_s c_t$ where $a_0, a_n \in \mathcal{S}^*$. Now we need to count the set $V = V(s, t, b_0, b_s, c_0, c_t)$ containing all polynomials $f \in \Omega_n(\mathcal{S})$ such that $f = pq$ with $\deg p = s$, $\deg q = s$, $p(0) = b_0$, $q(0) = c_0$, and leading coefficients of p and q being b_s and c_t, respectively. This implies

$$|\mathcal{R}_n^*(\mathcal{S})| \leq \sum_{a_0, a_n} \sum_{b_0 | a_0, b_s | a_n} \sum_{s+t=n} |V(s, t, b_0, b_s, a_0/b_0, a_n/b_s)|.$$

Next we bound $|V(s, t, b_0, b_s, c_0, c_t)|$. The method is essentially the same as that of Bary-Soroker and Kozma. We consider the map $\phi : \Omega_n(\mathcal{S}) \to \mathbb{Z}/M\mathbb{Z}[X]$ with

$$\phi(f) \equiv f \bmod M$$

for $f \in \Omega_n(\mathcal{S})$. Since $s_i \not\equiv s_j \bmod M$ for all $i \neq j$ $(i, j = 1, 2, \ldots, k)$, it follows that ϕ is injective. For any $\bar{p}$ (resp. $\bar{q}$) in $\mathbb{Z}/M\mathbb{Z}[X]$ with $\deg \bar{p} = s$ (resp. $\deg \bar{p} = t$), $\bar{p}(0) \equiv b_0 \bmod M$ (resp. $\bar{q}(0) \equiv c_0 \bmod M$), and leading coefficient $\bar{b}_s \equiv b_s \bmod M$ (resp. $\bar{c}_t \equiv c_t \bmod M$), we claim that the pair $(\bar{p}, \bar{q})$ will identify at most one $f \in V(s, t, b_0, b_s, c_0, c_t)$ through the relation

$$\phi(\bar{p}\bar{q}) = \phi(f),$$

since ϕ is injective. On the other hand, for any $f \in V(s, t, b_0, b_s, c_0, c_t)$ with $f = pq$, we can always find a pair $(\bar{p}, \bar{q}) = (\phi(p), \phi(q))$ such that

$$\phi(\bar{p}\bar{q}) = \phi(f).$$

We therefore conclude that

$$|V(s, t, b_0, b_s, c_0, c_t)| \leq \sum_{(\bar{p}, \bar{q})} 1 = M^{s-1} M^{t-1} = M^{n-2}.$$

To complete our proof, we have

$$\begin{aligned}
|\mathcal{R}_n^*(\mathcal{S})| &\leq \sum_{a_0, a_n} \sum_{b_0 | a_0, b_s | a_n} \sum_{s+t=n} |V(s, t, b_0, b_s, a_0/b_0, a_n/b_s)| \\
&\leq (n-1) M^{n-2} \sum_{a_0, a_n} \sum_{b_0 | a_0, b_s | a_n} 1 \\
&= (n-1) M^{n-2} \left(2 \sum_{a \in \mathcal{S}^*} d(a) \right)^2 .
\end{aligned}$$

∎

It is also noteworthy to mention Kuba's bound (1.1). In fact, he counted the set

$$\mathcal{P}_n^*(h) = \left\{ (p, q) \in (\mathbb{Z}[X] \backslash \mathbb{Z})^2 : \deg p + \deg q = n \text{ and } H(p)H(q) \leq e^n h \right\}.$$

Comparing with our proof, in which we restrict the coefficients of p and q to $\mathbb{Z}/M\mathbb{Z}$, we conclude that Kuba's bound works better for $n = o(\log h)$.

3 An application of Theorem 1

We first step back to the last step of Bary-Soroker and Kozma's proof. As they showed in their Section 3, by substituting $Y = 2$ in $F(X, Y)$, they got

$$F(X,2)=\sum_{i=0}^{n}\left(\sum_{j=0}^{n}\pm 2^{j}\right)X^{i}. \tag{3.1}$$

Now they only need to use the straightfoward argument that if $F(X, Y)$ is reducible, then either of the following holds: 1) $F(X, 2)$ is reducible; 2) $F(2, Y)$ is reducible; 3) $F(X, Y) = f(X)g(Y)$ for some polynomials f and g.

At a glimpse of the inner summation of the right hand of (3.1), the following identity of Euler may immediately come to the reader's mind:

$$\prod_{n=0}^{\infty}\left(x^{-3^{n}}+1+x^{3^{n}}\right)=\sum_{n=-\infty}^{\infty}x^{n}. \tag{3.2}$$

This identity was given in Chapter 16 of Euler's *Introductio in analysin infinitorum* which is entitled "*De Partitio Numerorum*". The reader may refer to J. Blanton's translation [4] of Euler's book. In fact, one may readily prove by induction that

$$\prod_{n=0}^{N-1}\left(x^{-3^{n}}+1+x^{3^{n}}\right)=\sum_{n=-(3^{N}-1)/2}^{(3^{N}-1)/2}x^{n}; \tag{3.3}$$

see [1, Eq. (5.4)], which is also an excellent expository article describing Euler's pioneering work.

Now this identity of Euler along with Theorem 1 immediately give

Theorem 2. *Let $F = F(X, Y) = \sum_{i,j\leq n} \varepsilon_{i,j} X^i Y^j$ be a bivariate polynomial of degree n with random coefficients $\varepsilon_{i,j} \in \{0, \pm 1\}$. Then*

$$\lim_{n\to\infty}\mathbb{P}(F \text{ reducible}) = 0.$$

Proof: We substitute $Y = 3$ in $F(X, Y)$. Then

$$F(X,3)=\sum_{i=0}^{n}\left(\sum_{j=0}^{n}\varepsilon_{i,j}3^{j}\right)X^{i}, \tag{3.4}$$

where $\varepsilon_{i,j} \in \{0, \pm 1\}$. Thanks to Euler's identity, we immediately see that the right hand side of (3.4) consists of all integer coefficient polynomials with degree $\leq n$ and height $\leq (3^{n+1} - 1)/2 = h^*$. Note also that the number of such polynomials with $a_0 a_n = 0$ is less than $2(2h^* + 1)^n$. This implies that we only need to consider the probability $\mathbb{P}(f \text{ reducible})$ where f is a random integer coefficient polynomial with $\deg f = n$, $H(f) \leq h^*$, and $f(0) \neq 0$. Now by Theorem 1, we have

$$|\mathcal{R}_n^*(h^*)| \leq 4(n-1)(2h^*+1)^{n-2}\left(2\sum_{n=1}^{h^*}d(n)\right)^{2},$$

where we put $M = 2h^* + 1$. Hence

$$\mathbb{P}(F(X,3) \text{ reducible}) \ll \frac{|\mathcal{R}_n^*(h^*)|}{(2h^*+1)^{n+1}} \ll \frac{n^3}{3^n} \quad (n \to \infty).$$

Here we use the approximation

$$\sum_{n \le x} d(x) \sim x \log x \quad (x \to \infty).$$

At last, similar to Bary-Soroker and Kozma's argument, we notice that if $F(X,Y)$ is reducible, then either of the following holds: 1) $F(X,3)$ is reducible; 2) $F(3,Y)$ is reducible; 3) $F(X,Y) = f(X)g(Y)$. We also have

$$\mathbb{P}(F(X,Y) = f(X)g(Y)) \le \frac{3^{n+1} \cdot 3^{n+1}}{3^{(n+1)^2}} \ll 3^{-n^2} \quad (n \to \infty),$$

since both f and g have coefficients in $\{0, \pm 1\}$. Hence

$$\mathbb{P}(F(X,Y) \text{ reducible}) \ll \frac{n^3}{3^n} \to 0 \quad (n \to \infty).$$

This ends our proof. $\square$

References

[1] G. E. Andrews, Euler's "De Partitio numerorum", *Bull. Amer. Math. Soc. (N.S.)* **44** (2007), no. 4, 561–573.

[2] L. Bary-Soroker, G. Kozma, Is a bivariate polynomial with ±1 coefficients irreducible? Very likely! *Int. J. Number Theory*, in press.

[3] K. Dörge, Abschätzung der anzahl der reduziblen polynome, *Math. Ann.* **160** (1965) 59–63.

[4] L. Euler, *Introduction to analysis of the infinite. Book I.*, transl. by John D. Blanton, Springer-Verlag, New York, 1988. xvi+327 pp.

[5] P. X. Gallagher, The large sieve and probabilistic Galois theory, *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pp. 91–101. Amer. Math. Soc., Providence, R.I., 1973.

[6] S. V. Konyagin, On the number of irreducible polynomials with 0, 1 coefficients, *Acta Arith.* **88** (1999), no. 4, 333–350.

[7] G. Kuba, On the distribution of reducible polynomials, *Math. Slovaca* **59** (2009), no. 3, 349–356.

[8] G. Pólya, G. Szegö, *Problems and theorems in analysis. II. Theory of functions, zeros, polynomials, determinants, number theory, geometry*, transl. by C. E. Billigheimer. Reprint of the 1976 English translation. *Classics in Mathematics*, Springer-Verlag, Berlin, 1998. xii+392 pp.

[9] I. Rivin, Galois groups of generic polynomials, *Preprint* (2015), arXiv:1511.06446.

[10] Some guy on the street, Irreducible polynomials with constrained coefficients, *MathOverflow*. Available at: `http://mathoverflow.net/q/7969`.

Received: 20.12.2016
Accepted: 23.02.2017

Department of Mathematics,
Pennsylvania State University
E-mail: `shanechern@psu.edu`