Bounding univariate and multivariate reducible polynomials with restricted height

Artūras Dubickas

Abstract
Let $d, H \geq 2, m, u \geq 0$ be some integers satisfying $m + u \leq d$. Consider a set of univariate integer polynomials of degree $d$ whose $m$ coefficients for the highest powers of $x$ and $u$ coefficients for the lowest powers of $x$ are fixed, whereas the remaining $g = d - m - u + 1$ coefficients are all bounded by $H$ in absolute value. We show that among those $(2H + 1)^g$ polynomials at most $c d (2H + 1)^{g-1} (\log(2H))^{\delta}$ are reducible over $\mathbb{Q}$, where the constant $c > 0$ depends only on two extreme coefficients (if they are fixed) and does not depend on $d$ and $H$. Here, $\delta = 2$ if $m = u = 0$; $\delta = 1$ if only one of $m$, $u$ is zero; $\delta = 0$ if none of $m$, $u$ is zero. This estimate is better than the previous one in certain range of $d$ and $H$. We also prove an estimate for the number of integer reducible polynomials in $n \geq 2$ variables of degree $d \geq 1$ in each variable and height at most $H \geq 1$. It is completely explicit in terms of $n, d, H$ and implies that the probability for such a polynomial to be reducible tends to zero as $\max(n, d, H) \to \infty$. The condition $n \geq 2$ is essential in the proof: despite some recent progress the problem in general remains open for $n = 1$.

Keywords Reducible polynomials · Multivariate reducible polynomials · Height

Mathematics Subject Classification 11R09 · 12D05 · 12E05

1 Introduction

Given two positive integers $d, H$, let $\mathcal{P}(d, H)$ be the set of polynomials with integer coefficients of degree $d$ and height at most $H$, that is,

$$\mathcal{P}(d, H) = \{a_d x^d + \cdots + a_0 : a_d \neq 0, a_d, \ldots, a_0 \in \mathbb{Z} \text{ and } |a_j| \leq H \text{ for } j = 0, 1, \ldots, d\}.$$

Recall that a polynomial $f \in \mathbb{Z}[x]$ of degree at least 2 is called reducible over $\mathbb{Q}$ if for some nonconstant polynomials $f_1, f_2 \in \mathbb{Z}[x]$ one has $f(x) = f_1(x) f_2(x)$. In all what follows reducibility is always meant over $\mathbb{Q}$ (and not in the ring $\mathbb{Z}[x]$): for instance, the polynomial

Artūras Dubickas
arturas.dubickas@mif.vu.lt

1 Institute of Mathematics, Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, 03225 Vilnius, Lithuania

Springer
$2x^2 + 4$ is reducible in $\mathbb{Z}[x]$, since it is the product of 2 and $x^2 + 2$, but it is irreducible over $\mathbb{Q}$.

Let $\mathbb{P}(d, H)$ be the probability that a random polynomial in $\mathcal{P}(d, H)$ is reducible, namely,

$$\mathbb{P}(d, H) = \frac{\# \{ f \in \mathcal{P}(d, H) : f \text{-reducible} \}}{\#\mathcal{P}(d, H)} = \frac{\# \{ f \in \mathcal{P}(d, H) : f \text{-reducible} \}}{2H(2H+1)^d}.$$  

Likewise, since the set $\mathcal{P}(d, H)$ contains $(2H+1)^d$ monic polynomials, we can set

$$\mathbb{P}^*(d, H) = \frac{\# \{ f \in \mathcal{P}(d, H) : f \text{-monic and reducible} \}}{(2H+1)^d}$$

for the probability that a random monic polynomial in $\mathcal{P}(d, H)$ is reducible.

The fact that for $d$ fixed and $H \to \infty$ both $\mathbb{P}(d, H)$ and $\mathbb{P}^*(d, H)$ tend to zero is well-known from the paper van der Waerden [25] who obtained the first upper bounds on the number of polynomials whose Galois group is not $S_d$. Later, upper bounds on the quantity $\mathbb{P}(d, H)$ have been obtained by Pólya and Szegö [24, Example 266], Dörge [10] and Kuba [20], where the correct order $\mathbb{P}(d, H) \asymp 1/H$ for $d \geq 3$ was established. See also [23] for the latest estimate in the series of results bounding the number of general and monic polynomials in $\mathcal{P}(d, H)$ whose Galois group is not $S_d$: the upper bound for the number of such monic polynomials now is $H^{d-1}(\log H)^{c(d)}$, where $c(d)$ is a positive constant that grows polynomially in $d$.

As for the functions $\mathbb{P}^*(d, H)$ and $\mathbb{P}(d, H)$, it is known by now that for each fixed $d \geq 3$ and $H \to \infty$ one has

$$\mathbb{P}^*(d, H) \sim \frac{c_d^*}{H}$$  \hspace{1cm} (1.1)  

and

$$\mathbb{P}(d, H) \sim \frac{c_d}{H},$$  \hspace{1cm} (1.2)

where the implied constants $c_d > 0$ and $c_d^* > 0$ depend on $d$ only. The formula (1.1) is due to Chela [8], whereas the formula (1.2) was only recently established by the author [12]. For $d = 2$ and $H \to \infty$ one has $\mathbb{P}^*(2, H) \sim (\log H)/(2H)$ (see [8]) and

$$\mathbb{P}(2, H) \sim \frac{3(3\sqrt{5} + 2\log(1 + \sqrt{5}) - 2\log 2) \log H}{4\pi^2 H}$$

(see [12]).

On the other hand, for $H$ fixed and $d \to \infty$ the problem on whether $\mathbb{P}(d, H)$ and $\mathbb{P}^*(d, H)$ tend to zero is still open. The case of polynomials with 0, 1 coefficients has been studied by Konyagin [18]. According to his result, among $2^{d-1}$ of such degree $d$ polynomials with constant term 1 there are at least $c_0 2^d/\log d$ irreducible polynomials with some absolute constant $c_0 > 0$. This is quite far from the conjecture of Odlyzko and Poonen [22] asserting that all but $o(2^{d-1})$ of such polynomials are irreducible. Very recently, Bary-Soroker and Kozma in [4] gave a substantial progress in this direction. They showed, for instance, that when $H$ is a fixed positive integer divisible by at least 4 distinct primes, say $H = 210 = 2 \cdot 3 \cdot 5 \cdot 7$, then the probability that a random monic polynomial of degree $d$ with positive coefficients in the set $\{1, 2, \ldots, H\}$ is reducible tends to 0 as $d \to \infty$.

However, in general, despite the asymptotic formulas (1.1) and (1.2), no nontrivial upper bounds for $\mathbb{P}(d, H)$ and $\mathbb{P}^*(d, H)$ are known in case $H$ is not very large compared to $d$. The situation remains very similar if the height of a polynomial is replaced by its Mahler measure. (For a polynomial $f$ of degree $d$ they are related by the inequalities $2^{-d} \leq M(f)/H(f) \leq$...
The asymptotic formulas for the cardinality of the set of polynomials with restricted Mahler measure are due to Chern and Vaaler [9]. Unlike $c^*_d$ and $c_d$ in (1.1) and (1.2), the involved constants in their case are rational. Some other asymptotic formulas for some special polynomials (e.g., Perron polynomials or polynomials with given number of real roots), where similar rational constants appear, have been obtained by Akiyama and Pethő [1,2], Calegari and Huang [6]; see also [14].

A generalization of [9] including explicit error terms in the asymptotic formulas was recently given in [15]. Combining the asymptotic formulas of [9] with the results of [13], where similar asymptotic formulas have been established for the number of integer reducible polynomials of degree $d$ with bounded Mahler measure, one can get the analogues of (1.1) and (1.2) with some explicit constants involving the rational constant found in [9] and the values of the Riemann zeta-function at $d − 1$ and $d$. However, since the error terms are very large in $d$, in both contexts (restricted height or restricted Mahler measure), such results for each $d ≥ 3$ imply the upper bounds of the form

$$P(d, H) < \frac{c^d^2}{H} \quad \text{and} \quad P^*(d, H) < \frac{c^*d^2}{H}$$

with some constants $c, c^* > 1$. Note that the formulas (1.3) are nontrivial only in the range

$$\log H \gg d^2.$$ 

In the next theorem we obtain two simple estimates on $P(d, H)$ and $P^*(d, H)$ that are completely explicit and nontrivial in the range $H \gg d(\log d)^2$ (general case) and $H \gg d \log d$ (monic case).

**Theorem 1.1** For any integers $d ≥ 2$ and $H ≥ 2$ we have

$$P(d, H) < \frac{1 + d(\log(2H))^2}{2H + 1}$$

and

$$P^*(d, H) < \frac{1 + d \log(2H)}{2H + 1}.$$  

The proof is based on the argument modulo $M = 2H + 1$, as in the recent paper of Bary-Soroker and Kozma [3], where the same problem for integer polynomials with restricted odd coefficients was investigated.

As we already mentioned above, when the bound on the height is replaced by the bound on the Mahler measure, the asymptotical formulas for the number of integer polynomials and monic integer polynomials of degree $d$ have been given in [9]. In [15], the authors investigated a more general case when several first and several last coefficients of a polynomial are fixed. In our next result (Theorem 1.2) we generalize (1.5) similarly.

To give a corresponding result we suppose that $m ≥ 1$ coefficients of

$$f(x) = a_dx^d + \cdots + a_{d−m+1}x^{d−m+1} + a_{d−m}x^{d−m} + \cdots + a_u x^u + a_{u−1} x^{u−1} + \cdots + a_0$$

for $m$ highest powers of $x$ are fixed, $a_d ≠ 0$, and $u ≥ 0$ coefficients of $f$ for $u$ lowest powers of $x$ are also fixed. That is, the following two vectors

$$\hat{s} = (a_d, \ldots, a_{d−m+1}) ∈ \mathbb{Z}^m \quad \text{and} \quad \hat{r} = (a_{u−1}, \ldots, a_0) ∈ \mathbb{Z}^u$$
are fixed. (In case \( u = 0 \) the vector \( \vec{r} \) is zero dimensional.) Suppose that \( m + u \leq d \) and that \( a_0 \neq 0 \) when \( u \geq 1 \), since otherwise all such polynomials are reducible. The set of polynomials with above restrictions, where the remaining

\[
g = d - m - u + 1
\]

coefficients \( a_{d-m}, \ldots, a_u \) can take any integer values not exceeding \( H \) in absolute value, will be denoted by \( \mathcal{P}(d, H, \vec{s}, \vec{r}) \). Since \( m \geq 1 \), for any fixed \( d, H, \vec{s}, \vec{r} \) one has

\[
\#\mathcal{P}(d, H, \vec{s}, \vec{r}) = (2H + 1)^g.
\]

Set

\[
\mathbb{P}(d, H, \vec{s}, \vec{r}) = \frac{\#\{ f \in \mathcal{P}(d, H, \vec{s}, \vec{r}) : f \text{-reducible} \}}{\#\mathcal{P}(d, H, \vec{s}, \vec{r})} = \frac{\#\{ f \in \mathcal{P}(d, H, \vec{s}, \vec{r}) : f \text{-reducible} \}}{(2H + 1)^g}
\]

for the probability that a random polynomial in \( \mathcal{P}(d, H, \vec{s}, \vec{r}) \) is reducible. Let also \( \tau(l) \) be the number of positive divisors of \( l \in \mathbb{N} \) (including 1 and \( l \) itself). Then,

**Theorem 1.2** With the above notation and assumptions, for any integers \( d \geq 2 \) and \( H \geq 2 \) we have

\[
\mathbb{P}(d, H, \vec{s}, \vec{r}) < \frac{1 + \tau(|a_d|)d \log(2H)}{2H + 1}
\]

if \( u = 0 \), and

\[
\mathbb{P}(d, H, \vec{s}, \vec{r}) \leq \frac{\tau(|a_d|)\tau(|a_0|)d}{2H + 1}
\]

if \( u \geq 1 \).

Selecting, for instance, \( d = 3, a_3 = a_0 = 1 \), we see that (1.7) implies that among \((2H + 1)^2\) cubic polynomials of the form

\[
x^3 + a_2x^2 + a_1x + 1,
\]

where \( a_1, a_2 \in \{-H, \ldots, H\} \), at most \( \tau(1)^23(2H + 1) = 6H + 3 \) are reducible. The exact number of such reducible polynomials is \( 4H - 1 \). Indeed, each such cubic reducible polynomial must have a root 1 (there are \( 2H - 1 \) of them) or \(-1 \) (there are \( 2H + 1 \) of them, but one, \( x^3 - x^2 - x + 1 \), is counted twice, since both 1 and \(-1 \) are its roots).

In [3], the result of the same type as in (1.4) was applied to show that the probability for a polynomial in two variables with \( \pm 1 \) coefficients and degree \( d \) in each variable to be reducible tends to zero as \( d \to \infty \). In Theorem 1.3 below, we give a similar result for polynomials in several variables with restricted coefficients.

More precisely, for any integers \( n \geq 2 \) and \( d, H \geq 1 \) let \( \mathcal{P}_n(d, H) \) be the set of polynomials in \( \mathbb{Z}[x_1, \ldots, x_n] \) of degree \( d \) in each variable \( x_i \), \( i = 1, \ldots, n \). We call a polynomial \( f \in \mathbb{Z}[x_1, \ldots, x_n] \) reducible if for some nonconstant polynomials \( f_1, f_2 \in \mathbb{Z}[x_1, \ldots, x_n] \) one has \( f = f_1f_2 \). Put

\[
\mathbb{P}_n(d, H) = \frac{\#\{ f \in \mathcal{P}_n(d, H) : f \text{-reducible} \}}{\#\mathcal{P}_n(d, H)}.
\]

**Theorem 1.3** For any integers \( n, d \geq 2 \) and \( H \geq 1 \) we have

\[
\mathbb{P}_n(d, H) < \frac{2^{n+1}(d+1)^2(\log(2H + 1))^2}{(2H + 1)(d+1)^{n-1}}.
\]
Note that Theorem 1.3 implies
\[ \mathbb{P}_n(d, H) \to 0 \quad \text{as} \quad \max(n, d, H) \to \infty. \]

Some other results evaluating various probabilities that a random polynomial in several variables is reducible can be found in [5, 19]. The latest result counting the number of specializations in Hilbert’s irreducibility theorem is due to Castillo and Dietmann [7]. Assuming that \( f(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n] \) is irreducible, they gave an estimate on the number of integer vectors \((y_2, \ldots, y_n)\), where \(|y_j| \leq H\), for which the polynomial \( f(x_1, y_2, \ldots, y_n) \in \mathbb{Z}[x_1]\) is reducible over \(\mathbb{Q}\). Counting problems for one variable polynomials reducible by Eisenstein’s criterion were investigated in [11, 16, 17, 21].

In the next section we will prove Theorems 1.1 and 1.2. The proofs are quite straightforward. Then, in Sect. 3 we will give a proof Theorem 1.3, which is more involved. It uses (1.4) and Lemma 3.2 below, which is a basic tool in the proof. It asserts that certain specialization at some \( n - 1 \) variables of a random polynomial in \( n \geq 2 \) variables of degree \( d \) in each variable is a univariate polynomial of degree \( d \) with uniformly distributed coefficients.

## 2 Proofs of Theorems 1.1 and 1.2

**Proof of Theorem 1.1** Assume that
\[ f(x) = a_d x^d + \cdots + a_0 \in \mathbb{Z}[x] \]
of degree \( d \) and height at most \( H \) is reducible. It is clear that there are \( 2H(2H + 1)^{d-1} \) of such polynomials with \( a_0 = 0 \) and all of them are reducible. So, from now on, assume that \( a_0 \neq 0 \). Then, there are positive integers \( \ell \leq t \) satisfying \( \ell + t = d \), a positive integer \( b_\ell \) and three nonzero integers \( c_\ell, b_0, c_0 \) such that a reducible polynomial \( a_d x^d + \cdots + a_0 \in \mathcal{P}(d, H) \) is a product of two polynomials
\[ f_1(x) = b_\ell x^{\ell} + \cdots + b_0 \quad \text{and} \quad f_2(x) = c_\ell x^{\ell} + \cdots + c_0 \]
where \( b_\ell c_\ell = a_d, b_0 c_0 = a_0 \) and where other coefficients of \( f_1 \) and \( f_2 \), namely, \( b_{\ell-1}, \ldots, b_1 \) and \( c_{\ell-1}, \ldots, c_1 \), are all in \(\mathbb{Z}\). Let \( V(b_\ell, c_\ell, b_0, c_0, \ell, t) \) be a subset of \( \mathcal{P}(d, H) \) corresponding to such polynomials \( f_1 \) and \( f_2 \) whose product belongs to \( \mathcal{P}(d, H) \).

We first bound the cardinality of each set \( V(b_\ell, c_\ell, b_0, c_0, \ell, t) \). Consider the image of \( f \), say \( \overline{f}(x) = a_d x^d + \cdots + a_0 \), in the group of primitive residue classes modulo \( M = 2H + 1 \), namely, \( \mathbb{Z}_M = \{\overline{0}, \overline{1}, \ldots, \overline{M - 1}\} \). Observe that the map \( f \to \overline{f} \) is a one to one correspondence between the set \( \mathcal{P}(d, H) \) and the set of degree \( d \) polynomials in \( \mathbb{Z}_M[x] \). Clearly, \( \overline{f} = \overline{f}_1 \cdot \overline{f}_2 \). The number of such pairs \((\overline{f}_1, \overline{f}_2)\) with \( b_\ell, b_0, c_\ell, c_0 \neq 0 \) fixed is at most \( M^{\ell-1} M^{t-1} = M^{\ell+t-2} = M^{d-2} \). Hence,
\[ \#V(b_\ell, c_\ell, b_0, c_0, \ell, t) \leq M^{d-2} \]
for any sextuple \((b_\ell, c_\ell, b_0, c_0, \ell, t)\) as above.

Note that for each fixed positive divisor \( b_\ell = k \) of \( a_d \) there are at most \( 2[H/k] \) possible \( c_\ell \). Similarly, for any positive divisor \( q \) of \( a_0 \neq 0 \) there at most \( 4[H/q] \) pairs \((b_0, c_0) = (\pm q, c_0)\) whose product in modulus does not exceed \( H \). Hence, the number of reducible polynomials in \( \mathcal{P}(d, H) \) is bounded above by
\[ 2H(2H + 1)^{d-1} + M^{d-2} \sum_{\ell=1}^{d/2} \left( \sum_{k,q=1}^H \frac{8H^2}{kq} \right) \leq 2H(2H + 1)^{d-1} + 4H^2(2H + 1)^{d-2} \left( \sum_{k=1}^H \frac{1}{k} \right)^2. \]
Below, we will use the following inequality
\[
1 + \frac{1}{2} + \cdots + \frac{1}{H} < \sqrt{\frac{2H+1}{2H}} \log(2H), \tag{2.2}
\]
which holds for each \(H \geq 2\). (Indeed, by the well-known bound on the harmonic number
\(1 + 1/2 + \cdots + 1/H < \log H + \gamma + 1/(2H)\), the inequality (2.2) holds without the factor
\(\sqrt{(2H+1)/2H}\) for \(H \geq 5\). For \(H = 2, 3, 4\), it can be checked directly.)

By (2.2), the second term in (2.1) is less than \(2H(2H+1)^{d-1} d(\log(2H))^2\). Therefore, dividing (2.1) by \(2H(2H+1)^d\), we deduce that
\[
\mathbb{P}(d, H) < \frac{1}{2H+1} + \frac{d(\log(2H))^2}{2H+1} = \frac{1+d(\log(2H))^2}{2H+1},
\]
as claimed in (1.4).

For the proof of (1.5), we may assume that \(b_\ell = c_t = 1\). Then, as above we obtain
\[
\#V(1, 1, b_0, c_0, \ell, t) \leq M^{d-2}.
\]
Note that \(\mathcal{P}(d, H)\) contains \((2H+1)^{d-1}\) reducible polynomials whose free term is zero. Also, for any positive divisor \(q\) of \(a_0 \neq 0\) there are \(4\lfloor H/q \rfloor\) pairs \((b_0, c_0) = (\pm q, c_0)\) whose product in modulus does not exceed \(H\). Hence, the number of monic reducible polynomials in \(\mathcal{P}(d, H)\) is bounded above by
\[
(2H+1)^{d-1} + M^{d-2} \sum_{\ell=1}^{\lfloor d/2 \rfloor} \sum_{q=1}^H \frac{4H}{q} \leq (2H+1)^{d-1} + 2H(2H+1)^{d-2} \sum_{\ell=1}^H \frac{1}{k}.
\]
By (2.2), the second term is less than \((2H+1)^{d-1} d \log(2H)\). Hence, dividing by \((2H+1)^d\) we obtain
\[
\mathbb{P}^*(d, H) < \frac{1}{2H+1} + \frac{d \log(2H)}{2H+1} = \frac{1 + d \log(2H)}{2H+1},
\]
which proves (1.5).

**Proof of Theorem 1.2** In order to prove (1.6) we suppose that \(m \geq 1\) leading coefficients of a reducible polynomial \(f(x) = a_d x^d + \cdots + a_0\), namely, \(a_d, \ldots, a_{d-m+1}\), are some fixed integers, \(a_d \neq 0\). Assume also that \(a_0 \neq 0\). (We will add \((2H+1)^{8-1}\) reducible polynomials with \(a_0 = 0\) at the end.) Then, there exist positive integers \(\ell \leq t\) satisfying \(\ell + t = d\) such that \(f = f_1f_2\), where
\[
f_1(x) = b_\ell x^\ell + \cdots + b_0, \quad b_\ell \geq 1, \quad \text{and} \quad f_2(x) = c_t x^t + \cdots + c_0
\]
are some integer polynomials. From \(b_\ell c_t = a_d\), it is clear that \(b_\ell\) belongs to a finite set of positive divisors of \(a_d\) and \(c_t = a_d/b_\ell\). As above we shall use the factorizations \(f = f_1f_2\) and \(\overline{f} = f_1 \cdot f_2\).

Suppose first that \(m \leq \ell\). From \(a_{d-\ell} = b_\ell c_{t-\ell} + b_{\ell-1}c_t\) we see that for each pair \((b_\ell, c_t)\) the integer \(c_{t-\ell}\) is uniquely determined by \(b_{\ell-1}\). Arguing in a similar fashion, we get that, with \((b_\ell, b_{\ell-1}, c_t, c_{t-1})\) fixed, \(c_{t-2}\) is uniquely determined by \(b_{\ell-2}\), etc., and, finally, \(c_{t-m+1}\) is uniquely determined by \(b_{\ell-m+1}\). Hence, the number of possible vectors \((b_\ell, \ldots, b_{\ell-m+1})\) modulo \(M = 2H+1\) is \(\tau(|a_d|) M^{m-1}\). The vector \((c_t, \ldots, c_{t-m+1})\) is uniquely determined by the vector \((b_\ell, \ldots, b_{\ell-m+1})\). There are also \(M^{\ell-m+t-m} = M^{d-2m}\) possibilities for the vector \((b_{\ell-m}, \ldots, b_1, c_{t-m}, \ldots, c_1)\) modulo \(M\), which gives at most
\[
\tau(|a_d|) M^{d-m-1}\]
possibilities for \((b_\ell, \ldots, b_1, c_\ell, \ldots, c_1)\). Finally, for each fixed positive integer \(q\) of \(a_0 \neq 0\) there at most \(4|H/q|\) pairs \((b_0, c_0) = (\pm q, c_0)\) whose product in modulus does not exceed \(H\). Consequently, by (2.2) and \(g = d - m + 1\), the number of such reducible polynomials is bounded above by

\[
\tau(|a_d|)M^{d-m-1} \sum_{\ell=m}^{[d/2]} \sum_{q=1}^{H} \frac{4H}{q} < 2\tau(|a_d|)(2H + 1)^{g-1}([d/2] - m + 1) \log(2H). \quad (2.3)
\]

Now, consider the case when the reverse inequality \(m \geq \ell + 1\) holds. Then, arguing as above, we see that the vector \((c_\ell, \ldots, c_{\ell-\ell})\) is uniquely determined by the vector \((b_\ell, \ldots, b_0)\). The coefficients \(c_{\ell-\ell+1}, \ldots, c_{\ell-m+1}\) are also uniquely determined, and we have \(M^{t-m}m\) possibilities for \((c_{\ell-m}, \ldots, c_1)\) modulo \(M\). In total, since there are \(\tau(|a_d|)\) choices for \(b_\ell\) and \(M^{\ell-1}\) choices for \((b_{\ell-1}, \ldots, b_1)\) modulo \(M\), we get

\[
\tau(|a_d|)M^{\ell-1}M^{t-m} = \tau(|a_d|)M^{d-m-1}
\]

possibilities for the vector \((b_\ell, \ldots, b_1, c_\ell, \ldots, c_1)\) modulo \(M\). As above, this gives

\[
\tau(|a_d|)M^{d-m-1} \sum_{\ell=1}^{m-1} \sum_{q=1}^{H} \frac{4H}{q} < 2\tau(|a_d|)(2H + 1)^{g-1}(m - 1) \log(2H).
\]

Adding this with (2.3) and also adding \((2H + 1)^{g-1}\) reducible polynomials (with \(a_0 = 0\)) we get less than

\[
(2H + 1)^{g-1} + (2H + 1)^{g-1}\tau(|a_d|)d \log(2H)
\]

reducible polynomials. Dividing by \((2H + 1)^g\), we obtain

\[
\mathbb{P}(d, H, s, \bar{r}) < \frac{1 + \tau(|a_d|)d \log(2H)}{2H + 1},
\]

as claimed in (1.6).

In order to prove (1.7) we suppose that \(m \geq 1\) leading coefficients and \(u \geq 1\) coefficients for the lowest terms of \(x\) of a reducible polynomial \(f(x) = a_dx^d + \cdots + a_0\), namely, \(a_d, \ldots, a_{d-m+1}, a_{u-1}, \ldots, a_0\) are some fixed integers, where \(a_d, a_0 \neq 0\). Then, for some positive integers \(\ell \leq t\) satisfying \(\ell + t = d\) we have \(f = f_1f_2\), where \(f_1(x) = b_\ell x^\ell + \cdots + b_0\), \(b_\ell \geq 1\), and \(f_2(x) = c_\ell x^\ell + \cdots + c_0\) are some integer polynomials. From \(b_\ell c_\ell = a_d\) and \(b_0c_0 = a_0\) it follows that \(b_\ell\) belongs to a finite set of positive divisors of \(a_d\), and that \(b_0\) a is positive or negative divisor of \(a_0\). Clearly, \(c_\ell = a_d/b_\ell, c_0 = a_0/b_0\). From \(\bar{f} = \bar{f}_1 \cdot \bar{f}_2\) we get at most

\[
2\tau(|a_d|)\tau(|a_0|)M^{t-1}
\]

possibilities for the vector \((b_\ell, \ldots, b_0)\) modulo \(M\). With \(b_\ell, \ldots, b_0\) being fixed, the coefficients \(c_\ell, \ldots, c_{\ell-m+1}\) and and also \(c_{u-1}, \ldots, c_0\) are uniquely determined. In addition, there are \(M^{t-m-u+1}\) possibilities for the vector \((c_{\ell-m}, \ldots, c_0)\) modulo \(M\).

In total, in view of \(g = \ell + t - m - u + 1\) this gives at most

\[
2\tau(|a_d|)\tau(|a_0|)M^{t-1}M^{t-m-u+1} = 2\tau(|a_d|)\tau(|a_0|)(2H + 1)^{g-1} \quad (2.4)
\]

possibilities. Since there are \([d/2]\) pairs of possible \((\ell, t)\), for the number of reducible polynomials in \(\mathcal{P}(d, H, s, \bar{r})\), by (2.4), one gets the upper bound

\[
[d/2]2\tau(|a_d|)\tau(|a_0|)(2H + 1)^{g-1} \leq \tau(|a_d|)\tau(|a_0|)d(2H + 1)^{g-1}.
\]
This yields the upper bound (1.7) for \( P(d, H, \vec{s}, \vec{r}) \).

3 Proof of Theorem 1.3

For the proof of this theorem we introduce the following sequences

\[ y_j = (2H + 1)^{(d+1)^{j-1}}, \quad j \in \mathbb{N}, \]  

and

\[ z_j = \frac{(2H + 1)^{(d+1)^j} - 1}{2}, \quad j \in \mathbb{N} \cup \{0\}. \]  

Then,

\[ y_j = 2z_{j-1} + 1 \]  

for each \( j \in \mathbb{N} \).

Observe that, by (3.1) and (3.3), it follows that

\[ 2z_{j-1}(1 + y_j + \cdots + y_j^{d^j}) = 2z_{j-1} \frac{y_j^{d+1} - 1}{y_j - 1} = y_j^{d+1} - 1 = y_{j+1} - 1 = 2z_j. \]  

Hence, each integer between 0 and \( 2z_j \) can be written uniquely in the form

\[ c_0 + c_1 y_j + \cdots + c_d y_j^d, \]

where the ‘digits’ \( c_0, c_1, \ldots, c_d \) in base \( y_j \) run through the set \( 0, 1, \ldots, 2z_{j-1} \). Consequently,

**Lemma 3.1** For \( j \in \mathbb{N} \) each integer between \( -z_j \) and \( z_j \) can be written uniquely in the form

\[ c_0 + c_1 y_j + \cdots + c_d y_j^d, \]  

where the integers \( c_0, c_1, \ldots, c_d \) run through the set \( \{-z_{j-1}, \ldots, z_{j-1}\} \).

We shall also need the following lemma.

**Lemma 3.2** For each \( k \in \{1, \ldots, n\} \) and each \( f \in \mathcal{P}_n(d, H) \) the polynomial

\[ f(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1}) \in \mathbb{Z}[x_k] \]

has degree \( d \) in \( x_k \) and integer coefficients not exceeding \( z_{n-1} \) in absolute value.

**Proof** Write \( f \in \mathbb{Z}[x_1, \ldots, x_n] \) in the form

\[ f(x_1, \ldots, x_n) = \sum_{j=0}^{d} g_j(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n)x_k^j, \]

where

\[ g_j(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n] \]

for \( j = 0, 1, \ldots, d \). In particular, \( g_d \) is a nonzero integer polynomial in \( n-1 \) variables with coefficients not exceeding \( H \) in absolute value. It remains to prove that \( g_d(y_1, \ldots, y_{n-1}) \neq 0 \) and that the coefficients of all \( g_j(y_1, \ldots, y_{n-1}), j = 0, \ldots, d \), do not exceed \( z_{n-1} \) in absolute value.
We will prove that for any nonzero polynomial

\[ G(x_1, \ldots, x_{n-1}) = \sum_{0 \leq k_1, \ldots, k_{n-1} \leq d} b_{k_1,\ldots,k_{n-1}} x_1^{k_1} \cdots x_{n-1}^{k_{n-1}} \]  

(3.6)
in \( n-1 \) variable \( x_1, \ldots, x_{n-1} \) and coefficients \( b_{k_1,\ldots,k_{n-1}} \) lying of the set \( \{-H, \ldots, H\} \) one has

\[ 0 < |G(y_1, \ldots, y_{n-1})| \leq z_{n-1}. \]

We proceed by induction on \( n \). For \( n = 2 \) it is clear that \( G(y_1) = G(2H + 1) = 0 \) iff

\[ b_0 + b_1 (2H + 1) + \cdots + b_d (2H + 1)^d = 0, \]  

(3.7)

where

\[ G(x_1) = b_0 + b_1 x_1 + \cdots + b_d x_1^d. \]

As \( b_0, \ldots, b_d \) run through \( \{-H, \ldots, H\} \), by Lemma 3.1 with \( j = 1 \), the expression of the left hand side of (3.7) is zero iff \( b_0 = \cdots = b_d = 0 \). Therefore, \( G \) is zero identically, which is not the case. Hence, \( G(y_1) \neq 0 \). By (3.2), it is also clear that

\[ |G(y_1)| \leq H \left( 1 + y_1 + \cdots + y_1^d \right) = H \frac{y_1^{d+1} - 1}{y_1 - 1} = \frac{(2H + 1)^{d+1} - 1}{2} = z_1. \]

Now, assume that for any nonzero integer polynomial \( G_{n-2} \) in \( n-2 \) variables of degree at most \( d \) in each variable and coefficients at most \( H \) in absolute value one has

\[ 0 < |G_{n-2}(y_1, \ldots, y_{n-1})| \leq z_{n-2}. \]

Consider the nonzero polynomial (3.6) in \( n-1 \) variable and write it in the form

\[ G(x_1, \ldots, x_{n-1}) = \sum_{j=0}^{d} h_j(x_1, \ldots, x_{n-2}) x_{n-1}^j, \]  

(3.8)

where \( h_0, \ldots, h_d \) are polynomials in \( \mathbb{Z}[x_1, \ldots, x_{n-2}] \) of degree at most \( d \) in each variable and height at most \( H \), not all zero. In particular, by the induction hypothesis, they satisfy

\[ |h_j(y_1, \ldots, y_{n-2})| \leq z_{n-2}. \]

Hence, for each \( i = 1, \ldots, n-2 \) inserting \( x_i = y_i \) into (3.8) we find that

\[ G(y_1, \ldots, y_{n-2}, x_{n-1}) = e_0 + e_1 x_{n-1} + \cdots + e_d x_{n-1}^d \]
is an integer polynomial in \( \mathbb{Z}[x_{n-1}] \) of degree at most \( d \) whose coefficients, say, \( e_0, \ldots, e_d \) all lie between \( -z_{n-2} \) and \( z_{n-2} \). Note that, by Lemma 3.1 with \( j = n-1 \),

\[ c_0 + c_1 y_{n-1} + \cdots + c_d y_{n-1}^d \]
takes all values between \( -z_{n-1} \) and \( z_{n-1} \) when \( c_0, \ldots, c_d \) run through the elements of the set \( \{-z_{n-2}, \ldots, z_{n-2}\} \). Therefore, \( G(y_1, \ldots, y_{n-1}) \) is zero iff \( e_0 = e_1 = \cdots = e_d = 0 \), which means that \( G(y_1, \ldots, y_{n-2}, x_{n-1}) \) is zero identically. Thus, by (3.8), \( h_j(y_1, \ldots, y_{n-2}) = 0 \) for \( j = 0, 1, \ldots, n-2 \), and so \( g(x_1, \ldots, x_{n-1}) \) is zero identically, which is not the case. This proves that \( G(y_1, \ldots, y_{n-1}) \neq 0 \).
Since \(|e_j| \leq z_{n-2}\), employing (3.4) we also get
\[
|G(y_1, \ldots, y_{n-1})| = \left| \sum_{j=0}^{d} e_j y_{n-1}^j \right| \leq z_{n-2}(1 + y_{n-1} + \cdots + y_{n-1}^d) = z_{n-1},
\]
and so complete the proof of the induction step.

**Lemma 3.3** The number of reducible \(f \in \mathcal{P}_n(d, H)\) that can be written in the form
\[
f_1(x_{\sigma(1)}, \ldots, x_{\sigma(u)})f_2(x_{\sigma(u+1)}, \ldots, x_{\sigma(n)})
\]
for some integer \(u\) satisfying \(1 \leq u \leq n/2\), some permutation \(\sigma\) of \(\{1, \ldots, n\}\), and some nonconstant polynomials \(f_1, f_2 \in \mathbb{Z}[x_1, \ldots, x_n]\) does not exceed
\[
(2^n - n)(2H + 1)^{(d+1)n-1+d+1}.
\]

**Proof** Firstly, there are
\[
\binom{n}{1} + \cdots + \binom{n}{\lfloor n/2 \rfloor} \leq 2^n - n
\]
possibilities to choose the variables \(x_{\sigma(1)}, \ldots, x_{\sigma(u)}\). Secondly, none of \((d+1)^u\) coefficients of \(f_1\) cannot exceed \(H\) in absolute value. Similarly, none of the \((d+1)^{n-u}\) coefficients of \(f_2\) cannot exceed \(H\) in absolute value. Hence, there are at most
\[
(2H + 1)^{(d+1)^u+(d+1)^{n-u}}
\]
possibilities to choose the coefficients of \(f_1\) and \(f_2\). Since
\[
(d+1)^u + (d+1)^{n-u} \leq (d+1)^{n-1} + d + 1,
\]
this proves the required bound. \(\square\)

Now, we are ready to prove Theorem 1.3. Suppose a reducible polynomial \(f \in \mathcal{P}_n(d, H)\) is not of the form as in Lemma 3.3. Write
\[
f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n)f_2(x_1, \ldots, x_n) \quad \text{(3.9)}
\]
for some nonconstant polynomials \(f_1, f_2 \in \mathbb{Z}[x_1, \ldots, x_n]\). Fix \(k \in \{1, \ldots, n\}\) and put \(d_{k,1} = \deg_{x_k} f_1\) and \(d_{k,2} = \deg_{x_k} f_2\). Then,
\[
d_{k,1} + d_{k,2} = d.
\]
Assume that \(\{d_{k,1}, d_{k,2}\} = \{0, d\}\) for every \(k\). Then, for each \(k \in \{1, \ldots, n\}\) exactly one of the polynomials \(f_1, f_2\) does not depend on \(x_k\). Thus, by (3.9), \(f\) must be of the form as described in Lemma 3.3, a contradiction. Consequently, there exists some \(k \in \{1, \ldots, n\}\) for which \(d_{k,1}, d_{k,2}\) are both positive integers.

Inserting \(y_1, y_2, \ldots, y_{n-1}\) instead of the variables \(x_1, \ldots, x_{k-1}, x_{k+1}, \ldots, x_n\) into (3.9) we see that \(f(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1})\) is equal to the product
\[
f_1(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1})f_2(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1}).
\]
By Lemma 3.2, \(\deg_{x_k} f(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1}) = d\). Setting
\[
d_{k,1}^* = \deg f_1(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1})
\]
and
\[ d_{k,2}^n = \deg f_2(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1}), \]
we clearly have \( d_{k,1}^n \leq d_{k,1} \) and \( d_{k,2}^n \leq d_{k,2} \). However, as
\[ d = d_{k,1}^n + d_{k,2}^n \leq d_{k,1} + d_{k,2} = d, \]
we must have equalities \( d_{k,1}^n = d_{k,1} \) and \( d_{k,2}^n = d_{k,2} \). In particular, \( d_{k,1}^n, d_{k,2}^n \) must be positive integers, so that the polynomial \( f(y_1, \ldots, y_{k-1}, x_k, y_k, \ldots, y_{n-1}) \in \mathbb{Z}[x_k] \) of degree \( d \) is reducible. By Lemma 3.2, its coefficients do not exceed \( z_{n-1} \) in absolute value. Therefore, by (1.4), (3.1), (3.2), there are at most
\[ 2z_{n-1}(2z_{n-1} + 1)^{d-1}(1 + d(\log(2z_{n-1}))^2) \]
of such polynomials and also \( n \) possible choices for \( k \). Combining this with Lemma 3.3 we get at most
\[ (2^n - n)(2H + 1)^{(d+1)n-1} + 2n(2z_{n-1} + 1)^{d-1}(1 + d(\log(2z_{n-1}))^2) \]
reducible polynomials in the set \( P_n(d, H) \).

Now, we will estimate the second term in (3.10). By (3.1) and (3.3), we find that
\[ 2z_{n-1}(2z_{n-1} + 1)^{d-1} < y_n^d = (2H + 1)^{(d+1)n-1}d \]
and
\[ (\log(2z_{n-1}))^2 < (d + 1)^{2n-2}(\log(2H + 1))^2. \]
Consequently, the second term in (3.10) is less than
\[ n(2H + 1)^{(d+1)n-1}d(1 + d(\log(2H + 1))^2. \]
Since the first term in (3.10) does not exceed \( (2^n - n)(2H + 1)^{(d+1)n-1}d \), this implies the following upper bound for (3.10):
\[ 2^n(d + 1)^{2n-1}(2H + 1)^{(d+1)n-1}d(\log(2H + 1))^2. \]  
(3.11)

On the other hand,
\[ \#P_n(d, H) \geq 2H(2H + 1)^{(d+1)n-1} > \frac{(2H + 1)^{(d+1)n}}{2}, \]  
(3.12)
since the polynomials of degree at most \( d \) in each variable whose term for \( x_1^d, \ldots, x_n^d \) is nonzero and height does not exceed \( H \) are all in \( P_n(d, H) \). Dividing (3.11) by (3.12) and using the fact that
\[ (d + 1)^n - (d + 1)^{n-1}d = (d + 1)^{n-1}. \]
we obtain
\[ \mathbb{P}_n(d, H) \leq \frac{2^{n+1}(d + 1)^{2n-1}(\log(2H + 1))^2}{(2H + 1)^{(d+1)n-1}}, \]
as required.

**Acknowledgements** This research was funded by a Grant (No. S-MIP-17-66/LSS-110000-1274) from the Research Council of Lithuania.
References