Proceedings of the Edinburgh Mathematical Society: page 1 of 25
doi:10.1017/S0013091524000464

THE BRUN–HOOLEY SIEVE FOR $\mathbb{F}_2[X]$ AND SQUAREFREE SHIFTS OF INTEGER POLYNOMIALS

PRADIPTO BANERJEE AND AMIT KUNDU

Department of Mathematics, Indian Institute of Technology Hyderabad, Sangareddy, Telangana, India

Corresponding author: Pradipto Banerjee, email: pradipto@math.iith.ac.in

(Received 24 January 2023)

Abstract Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{F}_2[x]$ with deg $f = n$. It is shown that for $n \gg 1$, there is an $g_1(x) \in \mathbb{F}_2[x]$ with deg $g_1 \leqslant \max\{\deg g, 6.7\log n\}$ and $g(x) - g_1(x)$ having $< 6.7\log n$ terms such that $\gcd(f(x), g_1(x)) = 1$. As an application, it is established using a result of Dubickas and Sha that given $f(x) \in \mathbb{F}_2[x]$ of degree $n \geqslant 1$, there is a separable $g(x) \in 2[x]$ with deg g = deg f and satisfying that $f(x) - g(x)$ has $\leqslant 6.7\log n$ terms. As a simple consequence, the latter result holds in $\mathbb{Z}[x]$ after replacing 'number of terms' by the L_1-norm of a polynomial and $6.7\log n$ by $6.8\log n$. This improves the bound $(\log n)^{\log 4+\varepsilon}$ obtained by Filaseta and Moy.

Keywords: Turán's conjecture; squarefree polynomials; function fields; Brun–Hooley sieve

2010 Mathematics subject classification: Primary 11C08
Secondary 11T06; 11N35; 11N36

1. Introduction

For $f(x) \in \mathbb{Z}[x]$ of degree n, let $L_1(f)$ denote the sum of the absolute values of the coefficients of $f(x)$. This is the L_1-norm on the $(n+1)$-dimensional real vector space U_n of real polynomials of degree $\leqslant n$. Let $V_n = U_n \cap \mathbb{Z}[x]$. Further, let $I_n \subset V_n$ be the set of polynomials in V_n that are irreducible over the rationals. It is well-known that asymptotically, a 100% polynomials in V_n are irreducible over the rationals in the sense that

$$\lim_{B\to\infty} \frac{\#\{f(x) \in I_n : L_1(f) \leqslant B\}}{\#\{f(x) \in V_n : L_1(f) \leqslant B\}} = 1$$

Thus, given $f(x) \in \mathbb{Z}[x]$ of degree n, one can naturally expect to be able to find a polynomial $g(x) \in I_n$, such that $L_1(f-g)$ is 'small'. Let $C(n)$ denote the *smallest* positive integer such that for every $f(x) \in \mathbb{Z}[x]$ with deg $f = n$, there is an $g(x) \in I_n$ such that $L_1(f-g) \leqslant C(n)$. It is easy to see that Eisenstein's criterion with $p=2$ implies that $C(n)$ exists and that $C(n) \leqslant n+2$. Pál Turán proposed the problem of showing that $C(n)$ is absolutely bounded. For each odd $n > 1$, the example $f(x) = x^n$ shows that $C(n) \geqslant 2$. Similarly, for every even $n > 2$, the polynomial $x^{n-2}(x^2 - x - 1)$ suggests that $C(n) \geqslant 2$. Filaseta [5] conjectured that $C(n) \leqslant 5$ for all n. In the same paper, he alludes to the possibility that $C(n) \leqslant 2$ cannot be ruled out.

Turán's conjecture remains open for $n > 40$. Bérczes and Hajdu [1, 2] have verified Turán's conjecture with $C(n) \leqslant 4$, for all polynomials $f(x) \in \mathbb{Z}[x]$ with $\deg f \leqslant 24$. Filaseta and Mossinghoff [6] have extended their results to all $f(x) \in \mathbb{Z}[x]$ with $\deg f \leqslant 40$ and with $C(n) \leqslant 5$.

Turán's conjecture is believed to be difficult. For instance, whether it is possible to do better than $C(n) \leqslant n + 2$ is unknown. The present paper is a byproduct of our attempts to improve this bound. Although we fell short in this pursuit, our approach considerably improved the corresponding bound in the *squarefree* analogue of Turán's conjecture. We discuss them next.

We begin with our initial idea to improve the bound on $C(n)$. For $f(x) \in 2[x]$, let $L(f)$ denote the number of terms of $f(x)$. Now, consider Turán's problem in $2[x]$, where the distance between $f(x)$ and $g(x)$ is now taken to be $L(f - g)$. Let $C_2(n)$ denote the counterpart for $C(n)$ in this case. We claim that $C(n) \leqslant C_2(n) + 1$ provided that $\deg g = \deg f = n$. To see this, for an $f(x) \in \mathbb{Z}[x]$ with $\deg f = n$, let $\delta \in \{0, 1\}$ be such that $f_\delta(x) = \delta x^n + f(x)$ has an odd leading coefficient. Let $\overline{f_\delta}(x) \in \mathbb{F}_2[x]$ denote the polynomial obtained by reducing the coefficients of $f_\delta(x)$ modulo 2. Observe that $\deg \overline{f_\delta} = n$. Now, suppose that there is an $g(x) \in \mathbb{F}_2[x]$, irreducible in $\mathbb{F}_2[x]$ with $\deg g = n$, such that $L(\overline{f_\delta} - g) \leqslant C_2(n)$. Consider the polynomial

$$g_\delta(x) = f_\delta(x) - \overline{f_\delta}(x) + g(x) = f(x) - \overline{f}(x) + g(x) \in \mathbb{Z}[x]$$

where, by abuse of notation, we now consider $\overline{f_\delta}(x)$, $\overline{f}(x)$ and $g(x)$ as polynomials in $\mathbb{Z}[x]$. If a denotes the leading coefficient of $f(x)$, then the leading coefficient of $g_\delta(x)$ is

$$a - \overline{a} + 1 \equiv 1 \pmod{2}.$$

In particular, $g_\delta(x)$ has degree n. Additionally, $g_\delta(x) \equiv g(x) \pmod{2}$ implies that $g_\delta(x)$ is irreducible over the rationals. Furthermore,

$$L_1(f - g_\delta) \leqslant 1 + L_1(\overline{f_\delta} - g) = 1 + L(\overline{f_\delta} - g) \leqslant 1 + C_2(n).$$

The assertion follows.

In view of the last observation above, it suffices to bound $C_2(n)$. For $n \geqslant 1$, let $C_2'(n)$ denote the smallest positive integer such that given $f(x)$ and $g(x)$ in $2[x]$ with $\deg f = n$, there is a polynomial $g_1(x) \in 2[x]$ with

$$\deg g_1 \leqslant \max\{\deg g, C_2'(n)\}, \quad L(g - g_1) \leqslant C_2'(n)$$

such that $\gcd(f(x), g_1(x)) = 1$. The better part of the paper is devoted to developing a method to establishing that $C_2'(n) \ll \log n$.

Now, suppose for the moment that we have achieved $C_2'(n) \leqslant \theta \log n$ for some $\theta > 0$. Let $\deg g = m \geqslant 1$, and set $\ell = \lfloor m/2 \rfloor$. Take $f(x)$ to be the product of all irreducible

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

polynomials of degree $\leqslant \ell$ in $2[x]$. By Lemma 3.2, [7], we have $\deg f \leqslant 2^{\ell+1}$. The hypothesis on $C_2'(n)$ would then imply that there is a polynomial $g_1(x) \in 2[x]$ with $\deg g_1 \leqslant \deg g$ and satisfies

$$L(g - g_1) \leqslant C_2'(\deg f) \leqslant \theta(\ell + 1)\log 2 \leqslant \frac{\theta(m+2)\log 2}{2}$$

such that $\gcd(f(x), g_1(x)) = 1$. The last condition implies that $g_1(x)$ has no irreducible factor of degree $\leqslant \deg g/2$. Since $\deg g_1 \leqslant \deg g$, it would then follow that $g_1(x)$ is irreducible in $2[x]$. A suitably small θ would then give a better bound on $C(m)$ than $m+2$. In fact, any $\theta < 2/\log 2 = 2.885\ldots$ would give the first non-trivial improvement on $C(m)$. Our main result establishes that $C_2'(n) \ll \log n$.

Theorem 1. *Let $f(x)$ and $g(x)$ be polynomials in $2[x]$ with $\deg f = n$. For $n \gg 1$, there is a polynomial $g_1(x) \in \mathbb{F}_2[x]$ with $\deg g_1 \leqslant \max\{\deg g, 6.7\log n\}$ and $L(g - g_1) < 6.7\log n$ such that $\gcd(f(x), g_1(x)) = 1$.*

Next, we discuss the squarefree analogue of Turán's conjecture. We refer to a polynomial $f(x) \in \mathbb{Z}[x]$ as *squarefree* if it has no multiple roots. For a positive integer n, let S_n denote the set of squarefree polynomials in V_n. Since $I_n \subset S_n$, it follows that the asymptotic density of squarefree polynomials in V_n is 1. Naturally, one is prompted to investigate the squarefree analogue Turán's problem. Dubickas and Sha [4] were the first to study this problem. For a positive integer n, let $D(n)$ denote the smallest positive integer such that given any $f(x) \in \mathbb{Z}[x]$ with $\deg f = n$, there is an $g(x) \in S_n$ with $L_1(f - g) \leqslant D(n)$. It is easily seen that $D(n) \leqslant C(n)$. Dubickas and Sha [4] conjecture that $D(n) \leqslant 2$. They further showed that $D(n) \geqslant 2$ for every $n \geqslant 15$ (in fact, their result is much more explicit). Thus, the conjectured value is $D(n) = 2$. In some contrast to $C(n) \leqslant n+2$, Filaseta and Moy [7] have obtained the bound

$$D(n) \leqslant (\log n)^{2\log 2+\varepsilon}$$

for $n \gg_\varepsilon 1$. As a simple application of Theorem 1, we will establish that $D(n) \ll \log n$.

Theorem 2. *For every $f(x) \in \mathbb{F}_2[x]$ of degree $n \gg 1$, there is a squarefree $g(x) \in 2[x]$ satisfying $\deg g = n$ and $L(f - g) \leqslant 6.7\log n$.*

Arguing as we did to establish that $C(n) \leqslant C_2(n)+1$ above (in the case that $\deg g = n$), we obtain the following.

Corollary 1. *For every $f(x) \in \mathbb{Z}[x]$ of degree $n \gg 1$, there is a squarefree $g(x) \in \mathbb{Z}[x]$ satisfying $\deg g = n$ and $L_1(f - g) \leqslant 1 + 6.7\log n < 6.8\log n$.*

The proof of Theorem 1 is based on a function field analogue of Brun–Hooley sieve (see Theorem 3, § 2). Although this is identical to the usual Brun–Hooley sieve in almost every aspect needing only minor adjustments, there is no evidence of a suitable reference in the existing literature. This prompted the authors to establish a function field analogue of the Brun–Hooley sieve in its full rigour. This is presented in § 2. For an exhaustive account of the usual Brun–Hooley sieve, the reader may refer to Halberstam–Richert [9] or Bateman–Diamond [3]. Apart from these references, the authors have found the nice exposition by Kevin Ford [8] particularly useful. For general arithmetic in function fields, we refer the reader to Rosen [10].

We clarify some of the basic notation to be followed in the remainder of the paper. Throughout, $\mathbf{A}$ denotes the ring $2[x]$. The set of non-zero elements of $\mathbf{A}$ will be denoted by $\mathbf{A}^*$. Typically, in our proofs, we will use uppercase letters A, D, F and G to denote the elements of $\mathbf{A}$ where $D \in \mathbf{A}^*$, generally, will denote a divisor of some element in $\mathbf{A}$. The letter P is reserved for a non-zero prime (irreducible) in $\mathbf{A}$. Following [10], we define the *norm* $|A|$ of $A \in \mathbf{A}^*$ as

$$|A| = 2^{\deg\, A}.$$

As it turns out, $|A|$ is the correct analogue for the size of an integer in $\mathbb{Z}$. Sometimes, for A and A' in $\mathbf{A}$, we will use (A, A') to denote $\gcd(A, A')$. The function $\nu(A)$ will denote the number of distinct prime factors of $A \in \mathbf{A}^*$ with $\nu(1) = 0$. For a squarefree $A \in \mathbf{A}^*$, the Möbius function $\mu(A) = (-1)^{\nu(A)}$. Otherwise, $\mu(A) = 0$. For a real number $x > 0$, we will denote by $\log_2 x$ the base-2 logarithm of x, and $\log x$ denotes the natural logarithm of x.

The paper is organized as follows. We develop the necessary technical details, namely the Brun–Hooley sieve for $\mathbf{A}$, in § 2. Theorem 1 and Theorem 2 are respectively proved in § 3 and § 4.

2. Brun–Hooley sieve for $\mathbb{F}_2[x]$

Let $\mathcal{A} \subset \mathbf{A}$ with $\#\mathcal{A} = X$. Let z be a real number satisfying $2 \leqslant z \leqslant X$. Let

$$\mathscr{P} = \mathscr{P}(z) := \{P \in \mathbf{A}^* \text{ is prime} : |P| \leqslant z\}, \tag{2.1}$$

and define

$$\Pi = \Pi(z) := \prod_{P \in \mathscr{P}} P. \tag{2.2}$$

We fix a total order $\prec$ on $\mathbf{A}$. For instance, for F and G in $\mathbf{A}$, we say that $F \prec G$ if $F(2) < G(2)$ when $F(x)$ and $G(x)$ are considered as polynomials in $\mathbb{R}[x]$. Observe that F and G, when considered as polynomials in $\mathbb{R}[x]$, have coefficients in $\{0, 1\}$, so that

$$F(2) \neq G(2) \iff F(x) \neq G(x),$$

as polynomials in $\mathbb{R}[x]$. Hence, if $F \neq G$ in $\mathbf{A}$, then exactly one of $F \prec G$ and $G \prec F$ holds. It is easy to see that $\prec$ thus defined is a total order in $\mathbf{A}$. In particular, every squarefree $A \neq 1$ can be uniquely expressed as the product

$$A = P_1 P_2 \cdots P_r,$$

where P_1, P_2, …, P_r are primes in $\mathbf{A}^*$ satisfying

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

$$P_1 \prec P_2 \prec \cdots \prec P_r.$$

Additionally, for A as above, define $p^-(A) = P_1$ and $p^+(A) = P_r$. We also set $p^-(1) = 1 = p^+(1)$.

For each $D \in \mathbf{A}^*$, let

$$\mathcal{A}_D := \{A \in \mathcal{A} : D \mid A\},$$

with the understanding that $\mathcal{A}_1 = \mathcal{A}$. We suppose that there is a real-valued function ω satisfying

$$\omega(1) = 1, \quad 0 \leqslant \omega(P) \leqslant 1 \tag{Ω}$$

for every prime $P \in \mathbf{A}^*$. Next, extend ω multiplicatively to all of $\mathbf{A}^*$ by defining

$$\omega(D) := \prod_{P|D} \omega(P).$$

For a $D \in \mathbf{A}^*$, we denote by r_D the quantity

$$r_D := \#\mathcal{A}_D - \frac{\omega(D)}{|D|}X.$$

We assume that

$$|r_D| \leqslant \omega(D), \quad D \in \mathbf{A}^*. \tag{r}$$

Further, define

$$W = W(z) := \prod_{P \in \mathscr{P}} \left(1 - \frac{\omega(P)}{|P|}\right), \tag{2.3}$$

and let

$$S(\mathcal{A}; z) := \#\{A \in \mathcal{A} : (A, \Pi) = 1\}.$$

Our main result in this section is the following.

Theorem 3. *(Brun–Hooley sieve for $2[x]$) Let $\mathcal{A}$, X, z, W and $S(\mathcal{A}; z)$ be as defined above. Let ω be a multiplicative function on $\mathbf{A}^*$ satisfying (Ω) and (r). Then for $z \gg 1$, one has*

(i) $S(\mathcal{A}; z) \geqslant 0.0001XW - z^{4.6385}$ *and*
(ii) $S(\mathcal{A}; z) \leqslant eXW + z^{3.6385}$.

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

The proof of the next lemma is identical to its integer counterpart.

Lemma 1. *For every $A \in A^*$, one has*

$$\sum_{D|A} \mu(D) = \begin{cases} 1 & \text{if} \quad A = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 2. *Let $\mathfrak{f}$ be a real-valued multiplicative function defined on $\mathbf{A}^*$, and let $A \in \mathbf{A}^*$ be squarefree. Then for every integer $k \geqslant 0$, one has*

$$\sum_{\substack{D|A \\ \nu(D) \leqslant k}} \mu(D)\mathfrak{f}(D) = \sum_{D|A} \mu(D)\mathfrak{f}(D) + (-1)^k \sum_{\substack{D|A \\ \nu(D)=k+1}} \mathfrak{f}(D) \prod_{\substack{P \in \mathscr{P} \\ P \prec p^-(D)}} (1 - \mathfrak{f}(P)),$$

where an empty product is equal to 1.

Proof. Consider the terms in the sum on the right corresponding to D with $\nu(D) \geqslant k+1$. Every such D can be uniquely expressed as

$$D = D_1 D_2,$$

where $\nu(D_1) = k+1$, and D_2 is either 1 or $p^+(D_2) \prec p^-(D_1)$. It follows that

$$\begin{aligned} \sum_{D|A} \mu(D)\mathfrak{f}(D) - \sum_{\substack{D|A \\ \nu(D) \leqslant k}} \mu(D)\mathfrak{f}(D) &= \sum_{\substack{D|A \\ \nu(D) \geqslant k+1}} \mu(D)\mathfrak{f}(D) \\ &= \sum_{\substack{D_1|A \\ \nu(D_1)=k+1}} \mu(D_1)\mathfrak{f}(D_1) \sum_{\substack{D_2|A \\ p^+(D_2) \prec p^-(D_1)}} \mu(D_2)\mathfrak{f}(D_2) \\ &= (-1)^{k+1} \sum_{\substack{D|A \\ \nu(D)=k+1}} \mathfrak{f}(D) \prod_{\substack{P \in \mathscr{P} \\ P \prec p^-(D)}} (1 - \mathfrak{f}(P)). \end{aligned}$$

The lemma follows. □

Corollary 2. *Let $\mathfrak{f}$ be a multiplicative function defined on $\mathbf{A}^*$ satisfying $0 \leqslant \mathfrak{f}(P) \leqslant 1$ for every prime P, and let $A \in \mathbf{A}^*$ be squarefree. Then for every even integer $k \geqslant 0$, one has*

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

$$\sum_{D|A}\mu(D)\mathfrak{f}(D)\leqslant\sum_{\substack{D|A\\ \nu(D)\leqslant k}}\mu(D)\mathfrak{f}(D)\leqslant\sum_{D|A}\mu(D)\mathfrak{f}(D)+\sum_{\substack{D|A\\ \nu(D)=k+1}}\mathfrak{f}(D).$$

Let $z\geqslant 2$ be as defined earlier, and let $2=z_{t+1}<z_t<\cdots<z_1=z$. Partition $\mathscr{P}=\mathscr{P}_1\cup\mathscr{P}_2\cup\cdots\cup\mathscr{P}_t$ such that if $P\in\mathscr{P}_j$, then $z_{j+1}<|P|\leqslant z_j$ if $j<t$ and $z_{t+1}\leqslant|P|\leqslant z_t$ if $j=t$. Set

$$\Pi_j=\prod_{P\in\mathscr{P}_j}P,$$

so that

$$\prod_{j=1}^{t}\Pi_j=\Pi.$$

In proving Theorem 1, we will need both upper and lower bounds on $S(\mathcal{A};z)$. As is usually the case, achieving a lower bound is relatively more difficult. We next embark on this pursuit. To this end, we begin with Hooley's lemma (for proof, see Lemma 12.6, [3]), which is the key step in the usual Brun–Hooley lower bound sieve.

Lemma 3. *Suppose that $0\leqslant x_j\leqslant y_j$ for $1\leqslant j\leqslant t$. Then one has*

$$x_1x_2\cdots x_t=y_1y_2\cdots y_t-\sum_{\ell=1}^{t}(y_\ell-x_\ell)\prod_{\substack{j=1\\ j\neq\ell}}^{t}y_j.$$

Let k_1, k_2, …, k_t be a sequence of even non-negative integers. For each $j\in\{1,2,\ldots,t\}$ and $A\in\mathcal{A}$, set

$$x_j=\sum_{D|(A,\Pi_j)}\mu(D),\quad y_j=\sum_{\substack{D|(A,\Pi_j)\\ \nu(D)\leqslant k_j}}\mu(D).$$

Setting $\mathfrak{f}\equiv 1$ and $A=(A,\Pi_j)$ in Corollary 2, we find that $x_j\leqslant y_j$ for every j. Furthermore, since k_j is even, setting $\mathfrak{f}\equiv 1$ in Corollary 2 again, we get

$$y_\ell-x_\ell\leqslant\sum_{\substack{D|(A,\Pi_\ell)\\ \nu(D)=k_\ell+1}}1.$$

Thus, by Lemma 3, we have

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

$$\sum_{D|(A,\Pi)} \mu(D) \geqslant \prod_{j=1}^{t} \sum_{\substack{D|(A,\Pi_j)\\ \nu(D)\leqslant k_j}} \mu(D) - \sum_{\ell=1}^{t} \sum_{\substack{D|(A,\Pi_\ell)\\ \nu(D)=k_\ell+1}} \left(\prod_{\substack{j=1\\ j\neq \ell}}^{t} \left(\sum_{\substack{D|(A,\Pi_j)\\ \nu(D)\leqslant k_j}}^{t} \mu(D) \right) \right)$$

$$= \sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|(A,\Pi_j)\\ \nu(D_j)\leqslant k_j}} \mu(D_1D_2\cdots D_t) - \sum_{\ell=1}^{t} \left(\sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|(A,\Pi_j)\\ \nu(D_j)\leqslant k_j, j\neq \ell\\ \nu(D_\ell)=k_\ell+1}} \mu\left(\frac{D_1D_2\cdots D_t}{D_\ell}\right) \right).$$

Now, using Lemma 1 and the last lower bound above, we obtain

$$S(\mathcal{A};z) = \sum_{A\in\mathcal{A}} \sum_{D|(A,\Pi)} \mu(D)$$

$$\geqslant \sum_{A\in\mathcal{A}} \sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|(A,\Pi_j)\\ \nu(D_j)\leqslant k_j}} \mu(D_1D_2\cdots D_t) - \sum_{A\in\mathcal{A}} \sum_{\ell=1}^{t} \left(\sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|(A,\Pi_j)\\ \nu(D_j)\leqslant k_j, j\neq \ell\\ \nu(D_\ell)=k_\ell+1}} \mu\left(\frac{D_1D_2\cdots D_t}{D_\ell}\right) \right)$$

$$= \sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|\Pi_j\\ \nu(D_j)\leqslant k_j}} \mu(D_1D_2\cdots D_t)\#\mathcal{A}_{D_1D_2\cdots D_t}$$

$$- \sum_{\ell=1}^{t} \left(\sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|\Pi_j\\ \nu(D_j)\leqslant k_j, j\neq \ell\\ \nu(D_\ell)=k_\ell+1}} \mu\left(\frac{D_1D_2\cdots D_t}{D_\ell}\right) \#\mathcal{A}_{D_1D_2\cdots D_t} \right).$$

Setting above

$$\#\mathcal{A}_{D_1D_2\cdots D_t} = \frac{\omega(D_1D_2\cdots D_t)}{|D_1D_2\cdots D_t|}X + r_{D_1D_2\cdots D_t},$$

we get

$$S(\mathcal{A};z) \geqslant X\Sigma - R,$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

where

$$\Sigma = \sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j \mid \Pi_j \\ \nu(D_j) \leqslant k_j}} \prod_{j=1}^{t} \mu(D_j) \frac{\omega(D_j)}{|D_j|} - \sum_{\ell=1}^{t} \left(\sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j \mid \Pi_j \\ \nu(D_j) \leqslant k_j, j \neq \ell \\ \nu(D_\ell) = k_\ell + 1}} \frac{\omega(D_\ell)}{|D_\ell|} \prod_{\substack{j=1 \\ j \neq \ell}}^{t} \mu(D_j) \frac{\omega(D_j)}{|D_j|} \right), \tag{2.4}$$

and

$$R = \sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j \mid \Pi_j \\ \nu(D_j) \leqslant k_j}} |r_{D_1 D_2 \cdots D_t}| + \sum_{\ell=1}^{t} \left(\sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j \mid \Pi_j \\ \nu(D_j) \leqslant k_j, j \neq \ell \\ \nu(D_\ell) = k_\ell + 1}} |r_{D_1 D_2 \cdots D_t}| \right).$$

By assumptions (Ω) and (r), we have $|r_D| \leqslant \omega(D) \leqslant 1$. Therefore,

$$R \leqslant \sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j \mid \Pi_j \\ \nu(D_j) \leqslant k_j}} 1 + \sum_{\ell=1}^{t} \left(\sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j \mid \Pi_j \\ \nu(D_j) \leqslant k_j, j \neq \ell \\ \nu(D_\ell) = k_\ell + 1}} 1 \right).$$

The above sum is over all D_1, D_2, $\ldots$, D_t satisfying $D_j \mid \Pi_j$, and either $\nu(D_j) \leqslant k_j$ for all j, or $\nu(D_j) \leqslant k_j$ for all but one j for which $\nu(D_j) = k_j + 1$. This is bounded by

$$\sum_{|D| \leqslant z_1^{k_1+1} z_2^{k_2} \cdots z_t^{k_t}} \mu^2(D) < 2 z_1^{k_1+1} z_2^{k_2} \cdots z_t^{k_t}.$$

Thus,

$$R < Z := 2 z_1^{k_1+1} z_2^{k_2} \cdots z_t^{k_t}. \tag{2.5}$$

Next, for each $j \in \{1, 2, \ldots, t\}$, define

$$U_j := \sum_{\substack{D \mid \Pi_j \\ \nu(D) \leqslant k_j}} \mu(D) \frac{\omega(D)}{|D|}, \quad W_j := \sum_{D \mid \Pi_j} \mu(D) \frac{\omega(D)}{|D|} = \prod_{P \in \mathscr{P}_j} \left(1 - \frac{\omega(P)}{|P|}\right).$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Then

$$\sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|\Pi_j\\ \nu(D_j)\leqslant k_j}} \prod_{j=1}^{t} \mu(D_j)\frac{\omega(D_j)}{|D_j|} = U_1U_2\cdots U_t, \tag{2.6}$$

and

$$\sum_{\ell=1}^{t}\left(\sum_{\substack{D_1,D_2,\ldots,D_t\\ D_j|\Pi_j\\ \nu(D_j)\leqslant k_j, j\neq\ell\\ \nu(D_\ell)=k_\ell+1}} \frac{\omega(D_\ell)}{|D_\ell|}\prod_{\substack{j=1\\ j\neq\ell}}^{t}\mu(D_j)\frac{\omega(D_j)}{|D_j|}\right) = U_1U_2\cdots U_t\sum_{\ell=1}^{t}\frac{1}{U_\ell}\sum_{\substack{D_\ell|\Pi_\ell\\ \nu(D_\ell)=k_\ell+1}}\frac{\omega(D_\ell)}{|D_\ell|}. \tag{2.7}$$

From Equations (2.4), (2.6) and (2.7), we have

$$\Sigma = U_1U_2\cdots U_t\left(1-\sum_{\ell=1}^{t}\frac{1}{U_\ell}\sum_{\substack{D_\ell|\Pi_\ell\\ \nu(D_\ell)=k_\ell+1}}\frac{\omega(D_\ell)}{|D_\ell|}\right). \tag{2.8}$$

By Corollary 2,

$$U_j \geqslant W_j, \quad j = 1,2,\cdots,t,$$

so that

$$U_1U_2\cdots U_t \geqslant W_1W_2\cdots W_t := W.$$

Next, in order to estimate the expression following the negative sign in Equation (2.8), we will make use of the following lemma.

Lemma 4. *We have*

$$\sum_{\substack{D|\Pi_\ell\\ \nu(D)=k_\ell+1}}\frac{\omega(D)}{|D|} \leqslant \frac{I_\ell^{k_\ell+1}}{(k_\ell+1)!},$$

where

$$I_\ell = \log\frac{1}{W_\ell} = -\sum_{P|\Pi_\ell}\log\left(1-\frac{\omega(P)}{|P|}\right).$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Proof. Let $\mathscr{P}_\ell = \{P_1, P_2, \dots, P_T\}$ with

$$P_1 \prec P_2 \prec \cdots \prec P_T.$$

For $D \mid \Pi_\ell$, set $\mathfrak{f}(D) = \omega(D)/|D|$. Thus, $0 \leqslant \mathfrak{f}(D) < 1$. By the multinomial theorem, we have

$$\begin{aligned}\left(\sum_{P\in\mathscr{P}_\ell} \mathfrak{f}(P)\right)^{k_\ell+1} &= \sum_{\substack{m_1+m_2+\cdots+m_T=k_\ell+1\\ m_j\geqslant 0}} \frac{(k_\ell+1)!}{m_1!m_2!\cdots m_T!}\prod_{j=1}^{T}\mathfrak{f}(P_j)^{m_j}\\ &> (k_\ell+1)! \sum_{P_{e_1}\prec P_{e_2}\prec\cdots\prec P_{e_{k_\ell+1}}} \mathfrak{f}(P_{e_1})\mathfrak{f}(P_{e_2})\cdots\mathfrak{f}(P_{e_{k_\ell+1}})\\ &= (k_\ell+1)! \sum_{\substack{D\mid\Pi_\ell\\ \nu(D)=k_\ell+1}} \mathfrak{f}(D).\end{aligned}$$

On the other hand, since $0 \leqslant \mathfrak{f}(P) < 1$, we have

$$\sum_{P\in\mathscr{P}_\ell} \mathfrak{f}(P) \leqslant \sum_{P\in\mathscr{P}_\ell} -(\log(1-\mathfrak{f}(P))) = \log\frac{1}{W_\ell} = I_\ell.$$

This finishes the proof of the lemma. $\square$

Now, by the estimate of Lemma 4, we have

$$\sum_{\substack{D\mid\Pi_\ell\\ \nu(D)=k_\ell+1}} \frac{\omega(D_\ell)}{|D_\ell|} \leqslant W_\ell\left(\frac{W_\ell^{-1}I_\ell^{k_\ell+1}}{(k_\ell+1)!}\right) = W_\ell\left(\frac{e^{I_\ell}I_\ell^{k_\ell+1}}{(k_\ell+1)!}\right).$$

Recalling that $U_\ell \geqslant W_\ell$, we get

$$\frac{1}{U_\ell}\sum_{\substack{d_\ell\mid\Pi_\ell\\ \nu(d_\ell)=k_\ell+1}} \frac{\omega(D_\ell)}{|D_\ell|} \leqslant \frac{e^{I_\ell}I_\ell^{k_\ell+1}}{(k_\ell+1)!}.$$

Observe that if $k_\ell = 0$ for some ℓ, then $U_\ell = 1$. Accordingly, in this case, the expression on the left side of the last display is then bounded by

$$W_\ell\left(\frac{e^{I_\ell}I_\ell^{k_\ell+1}}{(k_\ell+1)!}\right) = W_\ell e^{I_\ell}I_\ell = I_\ell.$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

From these estimates, we deduce from Equation (2.8) that

$$\Sigma \geqslant (1-E)\,W, \quad E = \sum_{\ell=1}^{t} \frac{\psi(\ell) I_\ell^{k_\ell+1}}{(k_\ell+1)!}, \tag{2.9}$$

where

$$\psi(\ell) = \begin{cases} e^{I_\ell} & \text{if} \quad k_\ell \neq 0 \\ 1 & \text{if} \quad k_\ell = 0. \end{cases} \tag{2.10}$$

As such,

$$S(\mathcal{A}; z) \geqslant X(1-E)W - Z, \tag{2.11}$$

where Z is as defined in Equation (2.5). Next, we obtain an upper bound on $S(\mathcal{A}; z)$. In this case, from Corollary 2, we have

$$\sum_{D|(a,\Pi)} \mu(D) = \prod_{j=1}^{t} \sum_{D_j|(a,\Pi_j)} \mu(D_j) \leqslant \prod_{j=1}^{t} \sum_{\substack{D_j|(a,\Pi_j) \\ \nu(D_j)\leqslant k_j}} \mu(D_j).$$

Accordingly, we have, using Lemma 1, that

$$\begin{aligned} S(\mathcal{A}; z) &= \sum_{A\in\mathcal{A}} \sum_{D|(A,\Pi)} \mu(D) \\ &\leqslant \sum_{A\in\mathcal{A}} \sum_{\substack{D_1,D_2,\ldots,D_t \\ D_j|(A,\Pi_j) \\ \nu(D_j)\leqslant k_j}} \mu(D_1 D_2 \cdots D_t) \\ &= \sum_{\substack{D_1,D_2,\ldots,D_t \\ D_j|\Pi_j \\ \nu(D_j)\leqslant k_j}} \mu(D_1 D_2 \cdots D_t) \# \mathcal{A}_{D_1 D_2 \cdots D_t} \\ &= X\Sigma + R, \end{aligned}$$

where

$$\Sigma = \sum_{\substack{D_1,D_2,\ldots,D_t \\ D_j|\Pi_j \\ \nu(D_j)\leqslant k_j}} \prod_{j=1}^{t} \mu(D_j) \frac{\omega(D_j)}{|D_j|} = \prod_{j=1}^{t} \sum_{\substack{D|\Pi_j \\ \nu(D)\leqslant k_j}} \mu(D) \frac{\omega(D)}{|D|},$$

and

$$R = \sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j | \Pi_j \\ \nu(D_j) \leqslant k_j}} \mu(D_1 D_2 \cdots D_t) r_{D_1 D_2 \cdots D_t}.$$

Working as before,

$$|R| \leqslant \sum_{\substack{D_1, D_2, \ldots, D_t \\ D_j | \Pi_j \\ \nu(D_j) \leqslant k_j}} 1 \leqslant 2 z_1^{k_1} z_2^{k_2} \cdots z_t^{k_t} = \frac{Z}{z_1} = \frac{Z}{z}.$$

Appealing again to Corollary 2, we have

$$\begin{aligned} \sum_{\substack{D_j | \Pi_j \\ \nu(D_j) \leqslant k_j}} \mu(D_j) \frac{\omega(D_j)}{|D_j|} &\leqslant \sum_{D_j | \Pi_j} \mu(D_j) \frac{\omega(D_j)}{|D_j|} + \sum_{\substack{D_j | \Pi_j \\ \nu(D_j) = k_j + 1}} \mu(D_j) \frac{\omega(D_j)}{|D_j|} \\ &= W_j + \sum_{\substack{D_j | \Pi_j \\ \nu(D_j) = k_j + 1}} \mu(D_j) \frac{\omega(D_j)}{|D_j|}. \end{aligned}$$

Proceeding as in the proof of Lemma 4, we get

$$\sum_{\substack{D_j | \Pi_j \\ \nu(D_j) = k_j + 1}} \mu(D_j) \frac{\omega(D_j)}{|D_j|} \leqslant \frac{I_j^{k_j + 1}}{(k_j + 1)!}.$$

Therefore,

$$\sum_{\substack{D_j | \Pi_j \\ \nu(D_j) \leqslant k_j}} \mu(D_j) \frac{\omega(D_j)}{|D_j|} \leqslant W_j \left(1 + \frac{e^{I_j} I_j^{k_j + 1}}{(k_j + 1)!} \right).$$

However, if $k_j = 0$ for some j, then the left side of the last display is equal to 1, and consequently, it is bounded by $W_j(1 + I_j)$ since $W_j \geqslant 1$. Thus,

$$\Sigma \leqslant \prod_{j=1}^{t} W_j \left(1 + \frac{\psi(j) I_j^{k_j + 1}}{(k_j + 1)!} \right) \leqslant W \prod_{j=1}^{t} \exp \left(\frac{\psi(j) I_j^{k_j + 1}}{(k_j + 1)!} \right) = W \exp(E),$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

where E and $\psi(j)$ are as defined by Equations (2.9) and (2.10), respectively. In conclusion,

$$S(\mathcal{A};z) \leqslant XW\exp(E) + \frac{Z}{z}, \tag{2.12}$$

where Z is as defined in Equation (2.5).

Next, we choose the parameters z_2, z_3, …, z_t and k_1, k_2, …, k_t optimally to obtain explicit upper and lower bounds on $S(\mathcal{A};z)$ suitable for our purposes. Set $c = 0.26249$. For each $j \in \{1, 2, \ldots, t\}$, set

$$\alpha_j = \exp\left(c(j-1)^2\right),$$

and $z_j = z^{1/\alpha_j}$. Let t be the maximal positive integer such that

$$z^{1/\alpha_t} > 2.$$

That is,

$$t = \left\lceil \sqrt{\frac{1}{c}\log\log_2 z} \right\rceil,$$

where, for a real number x, we denote by $\lceil x \rceil$, the integer m satisfying $m-1 < x \leqslant m$. Next, set $k_j = 2(j-1)$. In order to make the bounds (2.11) and (2.12) explicit, we need to find suitable upper bounds on E and Z. To this end, we begin by estimating I_ℓ.

Lemma 5. *We have*

$$I_\ell \leq \begin{cases} \sum_{\log_2 z_{\ell+1} < \deg\ P \leqslant \log_2 z_\ell} \frac{1}{|P|} + \frac{1}{|P|^2} & \textit{if} \quad \ell < t \\ \sum_{1 \leqslant \deg\ P \leqslant \log_2 z_\ell} \frac{1}{|P|} + \frac{1}{|P|^2} & \textit{if} \quad \ell = t. \end{cases}$$

Proof. Since $|P| \geqslant 2$ for every $P \in \mathscr{P}_\ell$, we have

$$\log\left(1 - \frac{\omega(P)}{|P|}\right)^{-1} = \omega(P)\sum_{j=1}^{\infty}\frac{1}{j|P|^j} \leqslant \frac{1}{|P|} + \frac{1}{|P|^2}.$$

The lemma follows after recalling the definition of I_ℓ. □

For an integer $d \geqslant 1$, recall that M_d, the number of irreducible polynomials in $\mathbf{A}$ of degree d, satisfies $M_d \leqslant 2^d/d$. Since $z_{\ell+1} \geqslant 2$, it follows from Lemma 5 that for every $\ell < t$,

$$
\begin{aligned}
I_\ell &\leqslant \sum_{\log_2 z_{\ell+1} < d \leqslant \log_2 z_\ell} \left(\frac{1}{d} + \frac{1}{d 2^d} \right) \\
&\leqslant \log \frac{\alpha_{\ell+1}}{\alpha_\ell} + \sum_{\log_2 z_{\ell+1} < d \leqslant \log_2 z_\ell} \int_0^{1/2} x^{d-1} \, \mathrm{d}x \\
&\leqslant c(2\ell - 1) + \sum_{\log_2 z_{\ell+1} < d \leqslant \log_2 z_\ell} \int_0^{1/2} x^{d-1} \, \mathrm{d}x.
\end{aligned}
$$

We estimate the second sum above as follows. For $x \in (0, 1/2]$, one has

$$
\sum_{\log_2 z_{\ell+1} < d \leqslant \log_2 z_\ell} x^{d-1} \leqslant 2 x^{\log_2 z_{\ell+1} - 1}.
$$

Thus,

$$
\begin{aligned}
\sum_{\log_2 z_{\ell+1} < d \leqslant \log_2 z_\ell} \int_0^{1/2} x^{d-1} \, \mathrm{d}x &= \int_0^{1/2} \left(\sum_{\log_2 z_{\ell+1} < d \leqslant \log_2 z_\ell} x^{d-1} \right) \mathrm{d}x \\
&\leqslant 2 \int_0^{1/2} x^{\log_2 z_{\ell+1} - 1} \, \mathrm{d}x \\
&= \frac{2}{z_{\ell+1} \log_2 z_{\ell+1}} \\
&\leqslant \frac{2}{z_{\ell+1}},
\end{aligned}
$$

since $z_{\ell+1} \geqslant 2$. It follows that

$$
I_\ell \leqslant c(2\ell - 1) + \frac{2}{z_{\ell+1}}. \tag{2.13}
$$

Working similarly, for $\ell = t$, we obtain from Lemma 5 that

$$
\begin{aligned}
I_t &\leqslant \sum_{1 \leqslant \deg P \leqslant \log_2 z_t} \left(\frac{1}{|P|} + \frac{1}{|P|^2} \right) \\
&\leqslant \sum_{1 \leqslant d \leqslant \frac{\log_2 z}{\alpha_t}} \left(\frac{1}{d} + \frac{1}{d 2^d} \right) \\
&< 2 + (\log \log_2 z - \log \alpha_t) \\
&= 2 + \left(\log \log_2 z - c(t-1)^2 \right).
\end{aligned}
$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Next, recall that

$$t = \left\lceil \sqrt{\frac{1}{c}\log\log_2 z} \right\rceil \geqslant \sqrt{\frac{1}{c}\log\log_2 z},$$

so that

$$ct^2 > \log\log_2 z.$$

Using the last estimate, we deduce that

$$I_t \leqslant 2 + c(2t-1) < 0.27(2t-1),$$

for $t \gg 1$. Thus, for $z \gg 1$ (so that $t \gg 1$), the contribution of $\ell = t$ in the sum for E in Equation (2.9) is bounded by

$$\frac{e^{0.27(2t-1)}\left(0.27(2t-1)\right)^{2t-1}}{(2t-1)!} < \left(0.27e^{1.27}\right)^{2t-1} < (0.97)^{2t-1}, \tag{2.14}$$

where, we have used that $(2t-1)^{2t-1}/(2t-1)! < e^{2t-1}$.

We will next estimate E by separately considering the contributions from terms corresponding to $\ell < t$ for which $\alpha_{\ell+1} \leqslant \sqrt{\log z}$ and $\alpha_{\ell+1} > \sqrt{\log z}$. First, consider the case that $\alpha_{\ell+1} \leqslant \sqrt{\log z}$. In this case,

$$z_{\ell+1} = z^{1/\alpha_{\ell+1}} \geqslant z^{1/\sqrt{\log z}} = e^{\sqrt{\log z}}.$$

Thus, from Equation (2.13) and the above, we get that

$$I_\ell \leqslant c(2\ell-1) + \frac{2}{e^{\sqrt{\log z}}}.$$

Additionally, $\alpha_{\ell+1} \leqslant \sqrt{\log z}$ implies that $c\ell^2 \leqslant (\log\log z)/2$. That is,

$$\ell \leqslant 1.5\sqrt{\log\log z}.$$

Let ψ be as defined in Equation (2.10). Note that $\psi(1) = 1$. For $1 < \ell \leqslant 1.5\sqrt{\log\log z}$ and for $z \gg 1$, using the estimates for I_ℓ from Equation (2.13), we have

$$\begin{aligned}
\frac{\psi(\ell)I_\ell^{2\ell-1}}{(2\ell-1)!} &\leqslant e^{2/\exp(\sqrt{\log z})}e^{c(2\ell-1)}\frac{\left(c(2\ell-1)+\frac{2}{e^{\sqrt{\log z}}}\right)^{2\ell-1}}{(2\ell-1)!}\\
&\leqslant e^{c(2\ell-1)}\left(1+O(e^{-\sqrt{(\log z)}})\right)\frac{\left((c(2\ell-1))^{2\ell-1}+(2\ell-1)^{2\ell-1}e^{-\sqrt{\log z}}3^{2\ell-1}\right)}{(2\ell-1)!}\\
&\leqslant e^{c(2\ell-1)}\left(1+O(e^{-\sqrt{(\log z)}})\right)\left(\frac{(c(2\ell-1))^{2\ell-1}}{(2\ell-1)!}+O(e^{3(2\ell-1)}e^{-\sqrt{\log z}})\right)\\
&= e^{c(2\ell-1)}\left(1+O(e^{-\sqrt{(\log z)}})\right)\left(\frac{(c(2\ell-1))^{2\ell-1}}{(2\ell-1)!}+O(e^{-\sqrt{\log z}/2})\right)\\
&= \frac{e^{c(2\ell-1)}(c(2\ell-1))^{2\ell-1}}{(2\ell-1)!}+O(e^{-\sqrt{\log z}/3}),
\end{aligned}$$

where, to obtain the bound in the second line above, we have used the binomial theorem as follows:

$$\begin{aligned}
\left(c(2\ell-1)+\frac{2}{e^{\sqrt{\log z}}}\right)^{2\ell-1} &\leqslant (c(2\ell-1))^{2\ell-1}+\sum_{j=1}^{2\ell-1}\binom{2\ell-1}{j}(c(2\ell-1))^{2\ell-1-j}2^j\\
&< (c(2\ell-1))^{2\ell-1}+(2\ell-1)^{2\ell-1}(2+c)^{2\ell-1}\\
&< (c(2\ell-1))^{2\ell-1}+(2\ell-1)^{2\ell-1}3^{2\ell-1}.
\end{aligned}$$

Thus, the contribution to the sum E from the terms corresponding to $\alpha_{\ell+1}\leqslant\sqrt{\log z}$ is bounded above by

$$\begin{aligned}
&I_1+\sum_{\ell>1}\frac{e^{c(2\ell-1)}(c(2\ell-1))^{2\ell-1}}{(2\ell-1)!}+O(\sqrt{\log\log z}e^{-\sqrt{\log z}/3}) \qquad (2.15)\\
&< c+\sum_{\ell>1}\frac{e^{c(2\ell-1)}(c(2\ell-1))^{2\ell-1}}{(2\ell-1)!}+O(e^{-\sqrt{\log z}/4})\\
&< 0.9997+O(e^{-\sqrt{\log z}/4}).
\end{aligned}$$

Next, consider the case that $\alpha_{\ell+1}>\sqrt{\log z}$. In this case, $\ell>\sqrt{\log\log z}$. Since $z_{\ell+1}\geqslant 2$, for $\sqrt{\log\log z}<\ell<t$, we have from Equation (2.13) that

$$I_\ell\leqslant c(2\ell-1)+\frac{2}{z_{\ell+1}}\leqslant c(2\ell-1)+1,$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

since $z_{\ell+1} \geqslant 2$. Thus, for ℓ as above and z sufficiently large, we have

$$\frac{\psi(\ell) I_\ell^{2\ell-1}}{(2\ell-1)!} \leqslant e^{c(2\ell-1)+1} \frac{(c(2\ell-1)+1)^{2\ell-1}}{(2\ell-1)!}$$
$$< e^{0.27(2\ell-1)} \frac{(0.27(2\ell-1))^{2\ell-1}}{(2\ell-1)!}$$
$$< (0.27 e^{1.27})^{2\ell-1} < 0.97^{2\ell-1}.$$

Thus, the contribution to the sum E from the terms corresponding to the ℓ under consideration is less than

$$\sum_{\ell > \sqrt{\log\log z}} (0.97)^{2\ell-1} = O(0.97^{\sqrt{\log\log z}}).$$

From the last estimate above and Equation (2.15), we deduce that

$$E < 0.9999$$

for $z \gg 1$.

It remains to estimate

$$Z := 2 z_1^{k_1+1} z_2^{k_2} \cdots z_t^{k_t} = 2\exp\left(\log z \left(\frac{1}{\alpha_1} + \frac{2}{\alpha_2} + \cdots + \frac{2(t-1)}{\alpha_t}\right)\right).$$

The exponent of z above is bounded by

$$1 + \sum_{n=1}^{\infty} \frac{2n}{\exp(0.26249 n^2)} < 4.63833.$$

We now obtain (i) and (ii) of Theorem 3 by putting the estimates $E < 0.9999$ and $Z < z^{4.6385}$ (for $z \gg 1$) in Equations (2.11) and (2.12), respectively.

3. A proof of Theorem 1

Let $f(x)$ and $g(x)$ be as stated in Theorem 1 with $\deg f = n$. Let $t := \lfloor 4.64 \log_2 n \rfloor$, and set $X := 2^t$. Observe that $t \leqslant 4.64 \log_2 n < 6.7 \log n$. For future reference, we make a note of the fact that

$$n < 2^{\frac{t+1}{4.64}} < 2X^{\frac{1}{4.64}}.$$

Let

$$\mathcal{A} := \{g + u : u \in \mathbf{A}, \deg u < t\}.$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Thus, $\#\mathcal{A} = X$. We will establish that for $n \gg 1$, there is some $g_1 \in \mathcal{A}$ satisfying $\gcd(f, g_1) = 1$. If $g_1 = g + u$, then

$$\deg\, g_1 \leqslant \max\{\deg\, g, \deg\, u\} \leqslant \max\{\deg\, g, 6.7 \log n\},$$

and

$$L(g - g_1) = L(u) \leqslant \deg\, u + 1 \leqslant t < 6.7 \log n,$$

as is required to be shown.

Let $P \in \mathbf{A}^*$ be irreducible. If $P \mid f$, and $\deg\, P > t$, then P divides at most one polynomial in $\mathcal{A}$. Thus, at most n polynomials in $\mathcal{A}$ have a common prime factor of degree greater than t with f.

For every irreducible $P \in \mathbf{A}^*$ with $\deg\, P \leqslant t$, we define $\omega(P) = 1$ if P divides some element of $\mathcal{A}$, and $\omega(P) = 0$, otherwise. We extend ω multiplicatively to all of $\mathbf{A}^*$ by defining

$$\omega(D) := \prod_{P \mid D} \omega(P), \quad D \in \mathbf{A}^*.$$

For $D \in \mathbf{A}^*$, let

$$\mathcal{A}_D := \{A \in \mathcal{A} : D \mid A\}.$$

Observe that if $\deg\, D \leqslant t$, then $\omega(D) = 1$ implies that

$$\#\mathcal{A}_D = 2^{t - \deg\, D} = \frac{\omega(D)}{|D|} X.$$

If $\deg\, D > t$ and $\omega(D) = 1$, then $\#\mathcal{A}_D = 1$; while, $\omega(D) = 0$ implies $\#\mathcal{A}_D = 0$. Define

$$r_D := |\mathcal{A}_D| - \frac{\omega(D)}{|D|} X.$$

Then $r_D = 0$ if either $\deg\, D \leqslant t$ or $\omega(D) = 0$. If $\deg\, D > t$ and $\omega(D) = 1$, then

$$r_D = 1 - 2^{t - \deg\, D} < 1.$$

Thus, in any case, $0 \leqslant r_D \leqslant \omega(D)$. In particular, $\omega(D)$ and r_D satisfy (Ω) and (r). Let

$$\mathcal{P}_f = \{P \text{ is irreducible} : P \mid f, \omega(P) = 1\},$$

and

$$\Pi_f = \prod_{P \in \mathcal{P}_f} P.$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Note that $\deg \Pi_f \leqslant \deg f$, and if $A \in \mathcal{A}$, then $(f, A) = 1$ if and only if $(A, \Pi_f) = 1$. So, without loss of any generality, we may and do assume that $f = \Pi_f$. Specifically, $\omega(P) = 1$ for every $P \mid f$.

Next, set $z = X^{\frac{1}{4.64}}$ in Theorem 3. We have

$$z = 2^{\frac{t}{4.64}} = 2^{\frac{\lfloor 4.64 \log_2 n \rfloor}{4.64}} \leqslant n.$$

Let $\mathscr{P}$, Π and W have the same meaning as implied in Equations (2.1), (2.2) and (2.3), respectively. Then the conclusion (i) of Theorem 3 implies that

$$S(\mathcal{A}; X^{\frac{1}{4.64}}) \geqslant 0.0001XW - X^{\frac{4.6385}{4.64}}, \tag{3.1}$$

for $n \gg 1$. Let $\mathcal{A}'$ denote the set $\{A \in \mathcal{A} : (A, \Pi) = 1\}$. Thus, the norm of each irreducible factor of every polynomial in $\mathcal{A}'$ is $\geqslant X^{\frac{1}{4.64}}$, and $\#\mathcal{A}' = S(\mathcal{A}; X^{\frac{1}{4.64}})$.

If $A \in \mathcal{A}'$ has a common prime factor P with f, then

$$\deg P \geqslant \log_2 X^{\frac{1}{4.64}} = \frac{\log_2 X}{4.64}.$$

Let S_1 denote the number of elements in $\mathcal{A}'$ that have a common prime factor of degree $\geqslant \frac{2\log_2 X}{4.64}$ with f, and S_2 the same for prime factors having degrees in $\left[\frac{\log_2 X}{4.64}, \frac{2\log_2 X}{4.64}\right)$. If n_d denotes the number of distinct irreducible factors of f of degree d, then

$$\begin{aligned} S_1 &\leqslant \sum_{\substack{\deg P \geqslant \frac{2\log_2 X}{4.64} \\ P \mid f}} \#\mathcal{A}_P \\ &= \sum_{\substack{\frac{2\log_2 X}{4.64} \leqslant \deg P \leqslant t \\ P \mid f}} \#\mathcal{A}_P + \sum_{\substack{\deg P > t \\ P \mid f}} \#\mathcal{A}_P \\ &\leqslant X \sum_{\substack{\frac{2\log_2 X}{4.64} \leqslant \deg P \leqslant t \\ P \mid f}} \frac{1}{|P|} + n \\ &\leqslant X \sum_{d \geqslant \frac{2\log_2 X}{4.64}} \frac{n_d}{2^d} + n \\ &\leqslant \frac{X}{2^{\frac{2\log_2 X}{4.64}}} \sum_{d \geqslant \frac{2\log_2 X}{4.64}} n_d + n \\ &\leqslant X^{\frac{2.64}{4.64}} \frac{4.64n}{2\log_2 X} + n \\ &< \frac{4.64 X^{\frac{3.64}{4.64}}}{\log_2 X} + 2X^{\frac{1}{4.64}} < \frac{5X^{\frac{3.64}{4.64}}}{\log_2 X}, \end{aligned} \tag{3.2}$$

for $n \gg 1$.

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

We now turn to estimating S_2. We begin by observing that

$$\frac{2\log_2 X}{4.64} = \frac{2t}{4.64} < t,$$

so that if deg $P < \frac{2\log_2 X}{4.64}$, then

$$\#\mathcal{A}_P = \frac{\omega(P)}{|P|}X.$$

We will apply Theorem 3, (ii) to the sets $\mathcal{A}_P$ where P is a prime factor of f with deg P in $\left[\frac{\log_2 X}{4.64}, \frac{2\log_2 X}{4.64}\right)$. In what follows, we assume that $P \mid f$ with deg $P \in \left[\frac{\log_2 X}{4.64}, \frac{2\log_2 X}{4.64}\right)$. Observe that for every P under consideration, we have $\omega(P) = 1$ so that

$$\#\mathcal{A}_P = \frac{X}{|P|} > X^{\frac{2.64}{4.64}} > z.$$

Let $\omega(D)$ be as defined earlier in this section. For $D \in \mathbf{A}^*$, define

$$r'_D := \#\mathcal{A}_{DP} - \frac{\omega(D)}{|D|}\#\mathcal{A}_P = \#\mathcal{A}_{DP} - \frac{\omega(D)}{|D|}\frac{X}{|P|}.$$

If $P \mid D$, then $\omega(DP) = \omega(D)$ whence, $r'_D = r(DP)$. Next, consider that $P \nmid D$. If $\omega(D) = 1$, then since $\omega(P) = 1$, we have

$$\omega(DP) = \omega(D)\omega(P) = 1 = \omega(D).$$

Conversely, if $\omega(DP) = 1$, then obviously $\omega(D) = 1$. It follows that $\omega(DP) = \omega(D)$, and as such,

$$r'_D = r_{DP}.$$

Thus,

$$|r'_D| = |r_{DP}| \leqslant \omega(DP) = \omega(D).$$

Thus, $\mathcal{A}_P$ and ω satisfy all the assumptions of Theorem 3. By Theorem 3 (ii), we now have for $n \gg 1$ that

$$S(\mathcal{A}_P; X^{\frac{1}{4.64}}) \leqslant e\frac{X}{|P|}W + X^{\frac{3.6385}{4.64}}.$$

Since $|P| > 2^{\frac{\log_2 X}{4.64}}$, hence

$$S(\mathcal{A}_P; X^{\frac{1}{4.64}}) \leqslant eX^{\frac{3.64}{4.64}}W + X^{\frac{3.6385}{4.64}}. \tag{3.3}$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Thus,

$$\begin{aligned} S_2 &= \sum_{\substack{P|f \\ \frac{\log_2 X}{4.64} \leqslant \deg\, P < \frac{2\log_2 X}{4.64}}} S(\mathcal{A}_P; X^{\frac{1}{4.64}}) \\ &\leqslant \left(eX^{\frac{3.64}{4.64}} W + X^{\frac{3.6385}{4.64}}\right) \sum_{\substack{P|f \\ \frac{\log_2 X}{4.64} \leqslant \deg\, P < \frac{2\log_2 X}{4.64}}} 1 \\ &\leqslant \left(eX^{\frac{3.64}{4.64}} W + X^{\frac{3.6385}{4.64}}\right) \frac{4.64n}{\log_2 X} \\ &\leqslant 10e\frac{XW}{\log_2 X} + 10\frac{X^{\frac{4.6385}{4.64}}}{\log_2 X}, \end{aligned} \tag{3.4}$$

since $n \leqslant 2X^{\frac{1}{4.64}}$. Now, from Equations (3.2) and (3.4), we have

$$S_1 + S_2 \leqslant 10e\frac{XW}{\log_2 X} + 15\frac{X^{\frac{4.6385}{4.64}}}{\log_2 X}. \tag{3.5}$$

If every polynomial in $\mathcal{A}'$ has a non-trivial gcd with f, then

$$S_1 + S_2 \geqslant \#\mathcal{A}' = S(\mathcal{A}; X^{\frac{1}{4.64}}).$$

Substituting from Equations (3.1) and (3.5) in the last estimate above, we get

$$10e\frac{XW}{\log_2 X} + 15\frac{X^{\frac{4.6385}{4.64}}}{\log_2 X} \geqslant 0.0001XW - X^{\frac{4.6385}{4.64}}.$$

Rearranging terms, we have

$$XW\left(0.0001 - \frac{10e}{\log_2 X}\right) \leqslant 16X^{\frac{4.6385}{4.64}}. \tag{3.6}$$

Observe that

$$W \geqslant V := \prod_{P\in\mathscr{P}} \left(1 - \frac{1}{|P|}\right).$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Now, if M_d denotes the number of irreducible polynomials in $\mathbf{A}$ of degree d, then

$$\begin{aligned}
-\log V &= \sum_{\substack{P-\text{a prime}\\ |P|\leqslant z}} -\log\left(1-\frac{1}{|P|}\right)\\
&= \sum_{\substack{P-\text{a prime}\\ |P|\leqslant z}} \sum_{j=1}^{\infty}\frac{1}{j|P|^j}\\
&= \sum_{d\leqslant \log_2 z} M_d \sum_{j=1}^{\infty}\frac{1}{j2^{dj}}.
\end{aligned}$$

Using an earlier estimate that $M_d \leqslant 2^d/d$, we get

$$\begin{aligned}
-\log V &\leqslant \sum_{d\leqslant \log_2 z} \frac{2^d}{d}\sum_{j=1}^{\infty}\frac{1}{j2^{dj}}\\
&= \sum_{d\leqslant \log_2 z}\frac{1}{d}+E',
\end{aligned}$$

where

$$\begin{aligned}
E' &= \sum_{d\leqslant \log_2 z} \frac{2^d}{d}\sum_{j=2}^{\infty}\frac{1}{j2^{dj}}\\
&< \sum_{d\leqslant \log_2 z} \frac{2^d}{2d}\sum_{j=2}^{\infty}\frac{1}{2^{dj}}\\
&= \sum_{d\leq \log_2 z} \frac{2^d}{2d}\frac{1}{2^d(2^d-1)}\\
&< \sum_{d\leqslant \log_2 z} \frac{1}{d2^d} < 1.
\end{aligned}$$

Therefore,

$$-\log V < \sum_{d\leqslant \log_2 z}\frac{1}{d}+1 < \log(\log_2 z)+2.$$

Upon exponentiating, we get

$$V > \frac{1}{e^2\log_2 z} = \frac{4.64}{e^2\log_2 X} > \frac{0.6}{\log_2 X}.$$

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press

Now, using the above estimate in Equation (3.6), we obtain

$$\frac{0.6X}{\log_2 X}\left(0.0001 - \frac{10e}{\log_2 X}\right) \leqslant 16X^{\frac{4.6385}{4.64}}.$$

The last inequality is impossible for $n \gg 1$ (whence $X \gg 1$). Therefore, for $n \gg 1$, there is an $g_1 = g + u$ in $\mathcal{A}$ such that $\gcd(f, g_1) = 1$, as asserted. This concludes the proof of Theorem 1.

4. A proof of Theorem 2

Let $f(x) \in \mathbb{F}_2[x]$ with $\deg f = n$. There are unique polynomials $f_e(x)$ and $f_o(x)$ in $2[x]$ such that $f(x)$ can be expressed as

$$f(x) = f_e(x^2) + x f_o(x^2).$$

Let $m := \max\{\deg f_e, \deg f_o\} = \lfloor n/2 \rfloor$. The proof of Theorem 2 rests upon the following result (Lemma 5.1) from [4] (also see Lemma 3.1, [7]).

Lemma 6. *Let $h(x) \in \mathbb{F}_2[x]$ be of degree at least 2. Then $h(x)$ is squarefree if and only if* $\gcd(h_e(x), h_o(x)) = 1$.

Let $u(x) \in \{f_e(x), f_o(x)\}$ be defined as

$$u(x) = \begin{cases} f_e(x) & \text{if} \quad \deg f \equiv 0 \pmod 2 \\ f_o(x) & \text{if} \quad \deg f \equiv 1 \pmod 2). \end{cases}$$

Thus, $\deg u = m$. Let $v(x) \in \{f_e(x), f_o(x)\}$ denote the other polynomial. By Theorem 1, for $n \gg 1$, there is an $v_1(x) \in \mathbb{F}_2[x]$ with $\deg v_1 \leqslant \max\{\deg v, 6.7 \log n\}$ and $L(v - v_1) < 6.7 \log m$ such that $\gcd(u(x), v_1(x)) = 1$. In particular, $\deg v_1 \leqslant \deg v \leqslant \deg u = m$. Set

$$g(x) = \begin{cases} u(x^2) + x v_1(x^2) & \text{if} \quad u(x) = f_e(x) \\ v_1(x^2) + x u(x^2) & \text{if} \quad u(x) = f_o(x). \end{cases}$$

Then $g(x)$ is squarefree by Lemma 6. Furthermore,

$$L(f - g) = L(v - v_1) < 6.7 \log m < 6.7 \log n,$$

as required. We conclude by clarifying that $\deg g = \deg f$. Assuming $\deg f = 2m$ is even, we have $u(x) = f_e(x)$ with $\deg f_e = m$. Furthermore, $\deg v < m$ in this case.

Consequently deg $v_1 < m$ (for $n \gg 1$). It follows that

$$\deg g = \max\{2\deg u, 1 + 2\deg v_1\} = \max\{2m, 1 + 2\deg v_1\} = 2m.$$

Similarly, if deg f is odd, say, deg $f = 2m + 1$, then $u(x) = f_o(x)$ with deg $f_o = m$. Then,

$$\deg g = \max\{2\deg v_1, 1 + 2\deg u\} = 2m + 1 = \deg f.$$

Acknowledgements. The authors express their sincere gratitude to the referee for identifying several critical errors. The referee's suggestions have greatly contributed to enhancing the quality of our presentation.

The first author's research was partially supported by MATRICS grant no. MTR/2021/000015 of SERB, India.

Competing interests. The authors declare none.

References

(1) A. Bérczes and L. Hajdu, Computational experiences on the distances of polynomials to irreducible polynomials, *Math. Comp.* **66**(217): (1997), 391–398.

(2) A. Bérczes and L. Hajdu, *On a Problem of Pál Turán Concerning Irreducible Polynomials*, pp. 95–100 (de Gruyter, Berlin, 1998) In: Number Theory (Eger, 1996).

(3) P. T. Batemann and H. G. Diamond, Analytic number theory, an introductory course. *Monographs in Number Theory*, Volume 1 (World Scientific Publishing Co. Pte. Ltd, Hackensack NJ, 2004).

(4) A. Dubickas and M. Sha, The distance to square-free polynomials, *Acta Arith.* **186**(3): (2018), 243–256.

(5) M. Filaseta, Is every polynomial with integer coefficients near an irreducible polynomial? *Elem. Math* **69**(3): (2014), 130–143.

(6) M. Filaseta and M. J. Mossinghoff, Distance to an irreducible polynomial II, *Math. Comp.* **81**(279): (2012), 1571–1585.

(7) M. Filaseta and R. Moy, The distance to a squarefree polynomial over F_2[x], *Acta Arith* **193**(4): (2020), 419–427.

(8) K. Ford, *Sieve methods lecture notes, spring 2023*, https://ford126.web.illinois.edu/sieve2023.pdf.

(9) H. Halberstam and H. E. Richert, Sieve methods. *London Mathematical Society Monographs* (Academic Press, London-New York, 1974) 4.

(10) M. Rosen, Number theory in function fields. *Graduate Text in Mathematics, 210* (Springer-Verlag, New York, 2002).

https://doi.org/10.1017/S0013091524000464 Published online by Cambridge University Press