

PAUCITY PHENOMENA FOR POLYNOMIAL PRODUCTS

VICTOR Y. WANG AND MAX WENQIANG XU

ABSTRACT. Let $P(x) \in \mathbb{Z}[x]$ be a polynomial with at least two distinct complex roots. We prove that the number of solutions $(x_1, \dots, x_k, y_1, \dots, y_k) \in [N]^{2k}$ to the equation

$$\prod_{1 \leq i \leq k} P(x_i) = \prod_{1 \leq j \leq k} P(y_j) \neq 0$$

(for any $k \geq 1$) is asymptotically $k!N^k$ as $N \rightarrow +\infty$. This solves a question first proposed and studied by Najnudel. The result can also be interpreted as saying that all even moments of random partial sums $\frac{1}{\sqrt{N}} \sum_{n \leq N} f(P(n))$ match standard complex Gaussian moments as $N \rightarrow +\infty$, where f is the Steinhaus random multiplicative function.

1. INTRODUCTION

We are interested in counting solutions to Diophantine equations involving products of polynomial values. Let $P(x) \in \mathbb{Z}[x]$ be a polynomial. Consider the equation

$$\prod_{1 \leq i \leq k} P(x_i) = \prod_{1 \leq j \leq k} P(y_j) \neq 0 \tag{1.1}$$

for a given integer $k \geq 1$. For integers $N \geq 1$, let $[N] := \{1, 2, \dots, N\}$ and define

$$A_{P,2k}([N]) := \#\{(x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_k) \in [N]^{2k} : \text{solutions to (1.1)}\}.$$

Call a solution to (1.1) *trivial* if the first k variables x_1, \dots, x_k equal the last k variables y_1, \dots, y_k in pairs. We say (1.1) has a *paucity* of nontrivial solutions in $[N]^{2k}$ as $N \rightarrow +\infty$ if almost all solutions are trivial, or equivalently, if $\lim_{N \rightarrow +\infty} (A_{P,2k}([N])/N^k) = k!$ holds. One might expect a typical equation of the form (1.1) to have this paucity property, which is a problem raised and studied in some special cases of $P(x)$ by Najnudel in [18, §5]. A recent result of Klurman, Shkredov, and Xu [16, Proposition 1.4] confirms that such phenomena exist in the $k = 2$ case.

1.1. Main results. In this paper, we prove the paucity phenomenon occurs for all $P(x)$ satisfying mild necessary conditions. Let $P(x) \in \mathbb{Z}[x]$ have degree $d \geq 2$ and at least two distinct complex roots. Let e_P be the maximum multiplicity of any complex root of P ; then $1 \leq e_P \leq d - 1$. (For example, if $P(x) = x^2(x + 1)$, then $e_P = 2$.)

Theorem 1.1. *Let P, d, e_P be as above. Then for integers $k, N \geq 1$, we have*

$$A_{P,2k}([N]) = k!N^k + O_{P,k,\varepsilon}(N^{k-1/6e_P+\varepsilon}).$$

2020 *Mathematics Subject Classification.* Primary 11K65; Secondary 11D45, 11D57, 11D79, 11N37.

Key words and phrases. Multiplicative Diophantine equations, paucity, random multiplicative functions, Gaussian behavior.

We prove Theorem 1.1 in §2. Related paucity results (for linear $P(x) = x - \alpha$ with $\alpha \in \mathbb{C}$ *irrational*) were obtained independently by Bourgain, Garaev, Konyagin, and Shparlinski [3, Corollary 27] and Heap, Sahay, and Wooley [13, Theorems 1.1 and 1.2]. By considering certain algebraic norms, it may be possible to use our result (Theorem 1.1) to obtain a version of those results (of [3] and [13]), weaker in the error term. However, we are not aware of any known or easy implication in the other direction.

1.2. Linear case and optimality of the results. The set of polynomials P we allow in Theorem 1.1 is precisely $\mathbb{Z}[x] \setminus \{c(ax - r)^m : c, a, r \in \mathbb{Z}, m \in \mathbb{N}\}$. Since (1.1) is “homogeneous” in P , the condition $P(x) \neq c(ax - r)^m$ in Theorem 1.1 basically requires $P(x)$ to not be linear. There has been a lot of literature in the case $P(x) = x$, e.g. [1, 5–7, 9, 11, 12]; it is known that in this case, $A_{P,2k}([N])$ is larger than the number of trivial solutions by a power of $\log N$ with degree depending on k . Thus, there is no paucity phenomenon in the linear case and our mild condition is necessary.

However, we remark that in the companion paper [19] of the authors and Pandey, the analogous counting problem is solved for $P(x) = x$ with short interval support $[N, N+H]$, $H \leq N/(\log N)^{Ck^2}$,¹ and this is one of the key steps in making progress towards a recent question of Harper [10]. The “paucity” in this case comes from the “shortness” of the interval; in comparison, the “paucity” in the present paper comes from the fact that $P(x)$ is “genuinely of degree ≥ 2 ” (i.e. it has at least two distinct complex roots).

1.3. Application to random multiplicative functions. One motivation for the study of Diophantine equations of the form (1.1) (when $P(x) = x$) comes from the moments of the Steinhaus random multiplicative function: let $f(p)$ be independent random variables (for all primes p) taking values uniformly from the complex unit circle, and define $f(n)$ completely multiplicatively for all n . We can use orthogonality to derive that

$$\mathbb{E}_f \left| \sum_{n \leq N} f(n) \right|^{2k} = A_{P(n)=n,2k}([N]).$$

Computing the moments here is exactly the same as counting solutions to (1.1). As mentioned before, we have now a good understanding of the high moments of $\frac{1}{\sqrt{N}} \sum_{n \leq N} f(n)$. When the support of $f(n)$ is the full set $[N]$, these moments blow up and grow like powers of $\log N$ as k grows. Our recent work [19] with Pandey proves that when $f(n)$ is supported on short intervals $[N, N+H]$ with $H \rightarrow +\infty$ and $H \ll N/(\log N)^{Ck^2}$ as $N \rightarrow +\infty$, these moments are consistent with Gaussian moments for all $k \geq 1$.

Theorem 1.1 can be interpreted as the following moment asymptotic for the Steinhaus random multiplicative function f . Suppose that $P(n)$ has a positive leading coefficient; then there exists a constant $n_0 \geq 0$ such that $P(n) > 0$ for all $n > n_0$. Then

$$\mathbb{E}_f \left| \frac{1}{\sqrt{N}} \sum_{n_0 < n \leq N} f(P(n)) \right|^{2k} = k! + O_{k,P,\varepsilon}(N^{-1/6e_P+\varepsilon}).$$

¹Previously, Bourgain, Garaev, Konyagin, and Shparlinski [3, proof of Theorem 34] handled a range of the form $H \leq N/\exp(C_k \log N/\log \log N)$.

The moments of random sums are strongly connected to their limiting distribution. In particular, to prove the random sums have Gaussian limiting distribution, it is sufficient to show that all the moments match the Gaussian moments (although this is not a necessary condition). Thus, Theorem 1.1 potentially gives a way to establish the central limit theorem for $\frac{1}{\sqrt{N}} \sum_{n \leq N} f(P(n))$ subject to establishing the odd moments,² which could likely be done either by the methods of the present paper, or by adapting the treatment of analogous odd moments in [19, end of §3]. In fact, Klurman, Shkredov, and Xu [16] already proved that $\frac{1}{\sqrt{N}} \sum_{n \leq N} f(P(n))$ has Gaussian limiting distribution by exploiting the martingale structure, which successfully reduces the task of establishing a central limit theorem to a fourth moment estimate. There is a lot more literature on the study of the distribution when $P(n)$ is linear and we refer readers to [4, 8, 14, 20].

1.4. Notation. Our notation is standard. For any two functions $f, g : \mathbb{R} \rightarrow \mathbb{R}$, we write $f \ll g, g \gg f, g = \Omega(f)$ or $f = O(g)$ if there exists a positive constant C such that $|f| \leq Cg$. We use O_k to indicate that the implied constant depends on k . Let $\omega(n)$ be the number of distinct prime factors of n , and $\tau_k(n)$ be the number of ways to write n as an ordered product of k positive integers. We use $\lfloor x \rfloor$ to denote the largest integer $\leq x$.

Acknowledgement. We thank Oleksiy Klurman, Ilya Shkredov, and Igor Shparlinski for helpful comments on earlier versions of the paper, and thank Yotam Hendel for providing a reference for Lemma 2.1. We also thank the anonymous referee for their generous corrections and comments. The first author has received funding from the European Union’s Horizon 2020 research and innovation program under the Marie Skłodowska-Curie Grant Agreement No. 101034413. The second author is partially supported by the Cuthbert C. Hurd Graduate Fellowship in the Mathematical Sciences, Stanford.

2. PROOF OF THE MAIN RESULT

The proof of Theorem 1.1 shares some ideas with the authors’ recent work [19] with Pandey, particularly the use of “factored” congruence conditions and induction on k .³ But the present proof also requires a novel use of some algebra (e.g. a result of Huxley [15]) and algebraic geometry (e.g. [2, Theorem 4] of Bombieri and Pila), among other ingredients. More specifically, our argument requires us to separately consider three types of solutions: trivial solutions (for which x_i and y_j are equal in pairs), “almost-trivial” nontrivial solutions (for which some $\gcd(P(x_i), P(y_j))$ is very large), and “generic” nontrivial solutions. For the two types of nontrivial solutions, see especially Corollary 2.4 and its proof. Roughly speaking, we use [15] to show that there are relatively few “generic” nontrivial solutions, while we use [2, Theorem 4] to show that *on average* there are relatively few “almost-trivial” nontrivial solutions.

²Very recently, Besfort Shala noted that the odd moments are trivial to handle by the divisor bound.

³The work [3, proof of Lemma 22 (for Lemma 23 and Theorem 34)] also uses congruence conditions, but does not “factor” them as we do in Corollary 2.4 below (and as in [19, §2 and §3]).

We now build up to a proof of Theorem 1.1. Let P, d, e_P be as in Theorem 1.1. Furthermore, assume that P has positive leading coefficient. (Theorem 1.1 is invariant under scaling P , so we may certainly make this assumption.) Now fix an integer $n_0 \geq 0$ such that $P(n) > 0$ for all $n > n_0$. By the divisor bound, (1.1) has at most $O_\varepsilon(N^{k-1+\varepsilon})$ solutions in $[N]^{2k}$ with $\min(x_1, \dots, x_k, y_1, \dots, y_k) \leq n_0$. Therefore, we may and do restrict attention to $n > n_0$. By replacing $P(x)$ with $P(x + n_0)$, we may then assume $P(n) > 0$ for all $n > 0$, as we do from now on.

Let $Q(x) \in \mathbb{Z}[x]$ be a polynomial, with no repeated complex roots, such that

$$Q(x) \mid P(x) \mid Q(x)^{e_P}. \quad (2.1)$$

Let $\Delta_Q \neq 0$ be the discriminant of Q . (On a first reading, we suggest restricting to the special case $P(x) = x(x+1)$ considered by Najnudel in [18, §5], where $e_P = 1$ and one can take $Q(x) = x(x+1)$ with $\Delta_Q = 1$.)

The following result on polynomial congruences is due to Huxley [15]. See also the stronger result in Stewart [21, Corollary 2], and the ensuing historical discussion there.

Lemma 2.1 (Huxley). *Let P, d, e_P, Q, Δ_Q be as above. Let $\ell \geq 1$ be an integer. Then*

$$\#\{x \bmod \ell : Q(x) \equiv 0 \bmod \ell\} \leq d^{\omega(\ell)} |\Delta_Q|^{1/2}. \quad (2.2)$$

Proof. Since P has ≥ 2 distinct complex roots, the condition (2.1) implies $\deg Q \geq 2$. Since $\deg Q \geq 2$, the bound (2.2) then follows directly from [15]. \square

This result leads to the following proposition:

Proposition 2.2. *Let P, d, e_P, Q, Δ_Q be as above. Let $z, N \geq 1$ be integers. Then*

$$\#\{x \in [N] : z \mid P(x)\} \leq d^{\omega(z)} |\Delta_Q|^{1/2} \cdot (1 + N/z^{1/e_P}). \quad (2.3)$$

Proof. Let ℓ be the smallest positive integer such that $z \mid \ell^{e_P}$. Clearly $\ell \mid z$ and $\ell \geq z^{1/e_P}$.

If $x \in [N]$ and $z \mid P(x)$, then $z \mid Q(x)^{e_P}$ by (2.1), so $\ell \mid Q(x)$. This implies that

$$\#\{x \in [N] : z \mid P(x)\} \leq \#\{x \in [N] : \ell \mid Q(x)\}. \quad (2.4)$$

But a short calculation using Lemma 2.1 gives the bound

$$\#\{x \in [N] : \ell \mid Q(x)\} \leq d^{\omega(\ell)} |\Delta_Q|^{1/2} \cdot \lceil N/\ell \rceil \leq d^{\omega(\ell)} |\Delta_Q|^{1/2} \cdot (1 + N/\ell). \quad (2.5)$$

(For $N = \ell$, the bound (2.5) follows directly from Lemma 2.1; for $N < \ell$ it then follows by enlarging N to ℓ , while for $N > \ell$ it follows by reduction modulo ℓ .)

Since $\ell \mid z$ and $\ell \geq z^{1/e_P}$, the proposition follows from (2.4) and (2.5). \square

Remark 2.3. By using [17, Theorem 1] instead of “enlarging N to ℓ ” (in the case $N < \ell$), the right-hand side of (2.3) could be improved to $d^{\omega(z)} \cdot (1 + |\Delta_Q|^{1/2} N/z^{1/e_P})$, provided the content of Q (the greatest common divisor of the coefficients of Q) is relatively prime to ℓ . This would save roughly a factor of $|\Delta_Q|^{1/2}$ when $N \asymp z^{1/e_P}/|\Delta_Q|^{1/2}$. But (2.3) is sufficient for our purposes (and does not require the content of Q to be coprime to ℓ).

We next deduce the following general counting result. Here and later, we let

$$G_{P,\lambda}([N], z) := \#\{(x, a, b) \in [N] \times [\lambda]^2 : a \cdot z = b \cdot P(x) \text{ and } a < b\}, \quad (2.6)$$

whenever $z, N, \lambda \in \mathbb{N}$.

Corollary 2.4. *Let P, d, e_P, Q, Δ_Q be as above. Let $k, z, N \geq 1$ be integers. Let*

$$T := \#\{(x_1, x_2, \dots, x_k) \in [N]^k : z \mid P(x_1)P(x_2) \cdots P(x_k), \\ P(x_1), P(x_2), \dots, P(x_k) < z\}. \quad (2.7)$$

Then for any integer $\lambda \geq 1$, we have

$$T \leq k \cdot G_{P,\lambda}([N], z) \cdot N^{k-1} + \tau_k(z) \cdot O(d^{\omega(z)})^k |\Delta_Q|^{k/2} \cdot \left(\frac{N^k}{z^{1/e_P}} + \frac{N^{k-1}}{\lambda^{1/e_P}} + N^{k-2} \right). \quad (2.8)$$

Proof. For each $j \in [k]$, let I_j be the contribution to T from tuples (x_1, \dots, x_k) with $\gcd(P(x_j), z) \geq z/\lambda$. Note that if $x \in [N]$ has the properties $\gcd(P(x), z) \geq z/\lambda$ and $P(x) < z$, then $\gcd(P(x), z) = z/b$ for some positive integer $b \leq \lambda$ dividing z , and thus $P(x) = a \cdot z/b$ for some positive integer $a < b$, since $P(x) > 0$. It follows that for each $j \in [k]$, we have

$$I_j \leq G_{P,\lambda}([N], z) \cdot N^{k-1}. \quad (2.9)$$

Now let S be the contribution to T from tuples (x_1, \dots, x_k) with $\gcd(P(x_j), z) < z/\lambda$ for all $j \in [k]$. Given positive integers u_1, \dots, u_k with $u_1 u_2 \cdots u_k = z$, let S_{u_1, \dots, u_k} be the contribution to T from tuples (x_1, \dots, x_k) with $\gcd(P(x_j), z) < z/\lambda$ and $u_j \mid P(x_j)$ for all $j \in [k]$. Then $S_{u_1, \dots, u_k} = 0$ unless $u_1, \dots, u_k < z/\lambda$, in which case we must have $k \geq 2$ and (by Proposition 2.2)

$$S_{u_1, \dots, u_k} \leq O(d^{\omega(z)})^k |\Delta_Q|^{k/2} \cdot \frac{N^k}{\prod_{j \in [k]} \min(N, u_j^{1/e_P})} \\ \leq O(d^{\omega(z)})^k |\Delta_Q|^{k/2} \cdot \left(N^{k-2} + \frac{N^{k-1}}{\min_{i \in [k]} (z/u_i)^{1/e_P}} + \frac{N^k}{z^{1/e_P}} \right),$$

because $\prod_{j \in [k]} \min(N, u_j^{1/e_P})$ is either $\geq N^2$, or equal to $N \prod_{j \in [k] \setminus \{i\}} u_j^{1/e_P} = N(z/u_i)^{1/e_P}$, or else equal to $\prod_{j \in [k]} u_j^{1/e_P} = z^{1/e_P}$. Therefore,

$$S_{u_1, \dots, u_k} \leq O(d^{\omega(z)})^k |\Delta_Q|^{k/2} \cdot \left(N^{k-2} + \frac{N^{k-1}}{\lambda^{1/e_P}} + \frac{N^k}{z^{1/e_P}} \right), \quad (2.10)$$

since we may assume $u_1, \dots, u_k < z/\lambda$. As $S \leq \sum_{u_1 u_2 \cdots u_k = z} S_{u_1, \dots, u_k}$, we conclude that

$$S \leq \tau_k(z) \cdot O(d^{\omega(z)})^k |\Delta_Q|^{k/2} \cdot \left(N^{k-2} + \frac{N^{k-1}}{\lambda^{1/e_P}} + \frac{N^k}{z^{1/e_P}} \right). \quad (2.11)$$

Since $T \leq I_1 + \cdots + I_k + S$, the desired result follows from (2.9) and (2.11). \square

To further estimate the upper bound in (2.8) for the quantity (2.7), we show that on average over certain values of z , the quantity $G_{P,\lambda}([N], z)$ appearing in (2.8) is not large. We show this in Lemma 2.7, with Lemma 2.5 and Lemma 2.6 as preparations.

Lemmas 2.5 and 2.6 imply that when $a \neq b$, the polynomial $a \cdot P(y) - b \cdot P(x)$ has no linear factor, and therefore has few integral zeros in boxes. Lemma 2.6 is a well-known counting result due to Bombieri and Pila [2, Theorem 4], which is also used in [16].

Lemma 2.5. *Let P, d be as above. Let a, b be distinct positive integers. Then the polynomial $a \cdot P(y) - b \cdot P(x)$ has no factor in $\mathbb{C}[x, y]$ of degree 1.*

Proof. Suppose for contradiction that $a \cdot P(y) - b \cdot P(x)$ has a linear factor, say $fx + gy + h$ (with $f, g, h \in \mathbb{C}$ and $(f, g) \neq (0, 0)$). By symmetry, we may assume $g \neq 0$. By scaling, we may then assume $g = -1$. The factor theorem in $(\mathbb{C}[x])[y]$ now implies

$$aP(fx + h) = bP(x).$$

Thus $f^d = b/a$ (so $|f| = (b/a)^{1/d} \notin \{0, 1\}$), and the (invertible) affine map $L(x) := fx + h$ on \mathbb{C} permutes the roots of P . Thus each root of P is fixed by L^d . But since $|f| \neq 1$, the map $L^d = f^d x + O_{d,f,h}(1)$ has at most one fixed point. Thus P has at most one root, contradicting our original requirement that P have at least two distinct roots. \square

Lemma 2.6 (Bombieri–Pila [2, Theorem 4]). *Let \mathcal{C} be an absolutely irreducible curve (over the rationals) of degree $r \geq 2$. If $N \geq \exp(r^6)$, then the number of integral points on \mathcal{C} and inside the square $[0, N] \times [0, N]$ does not exceed $N^{1/r} \exp(12\sqrt{r} \log N \log \log N)$.*

Recall the definition of $G_{P,\lambda}([N], z)$ from (2.6). The following lemma shows that $G_{P,\lambda}([N], P(y))$ is not large when we average over y .

Lemma 2.7. *Let P, d be as above. Let $N, \lambda \geq 1$ be integers. Then*

$$\sum_{y \in [N]} G_{P,\lambda}([N], P(y)) \ll_{d,\varepsilon} \lambda^2 \cdot N^{1/2+\varepsilon}.$$

Proof. Plugging in (2.6), we see that the lemma concerns the number of solutions $(x, y) \in [N]^2$ to $a \cdot P(y) = b \cdot P(x)$ in total over positive integers $a, b \leq \lambda$ with $a < b$. Consider any such integers a, b . By Lemma 2.5, each irreducible complex component of the curve $a \cdot P(y) - b \cdot P(x) = 0$ has degree ≥ 2 , and thus by Lemma 2.6, at most $O_{d,\varepsilon}(N^{1/2+\varepsilon})$ integral points $(x, y) \in [N]^2$. The lemma follows upon summing over a, b . \square

With Corollary 2.4 and Lemma 2.7, we are ready to prove Theorem 1.1. The proof proceeds by using a “symmetry, congruence condition, and induction” strategy.

Proof of Theorem 1.1. We call a solution to (1.1) *trivial* if (x_1, \dots, x_k) equals a permutation of (y_1, \dots, y_k) . Also, as explained near the beginning of §2, we assume $P(n) > 0$ for $n > 0$. Therefore, the contribution to $A_{P,2k}([N])$ from trivial solutions is

$$k!N^k + O_k(N^{k-1}), \tag{2.12}$$

since it is at most $k!N^k$ and at least $k!N(N-1)\cdots(N-k+1)$. It remains to bound $N_{P,2k}([N])$, the number of nontrivial solutions $(x_1, \dots, x_k, y_1, \dots, y_k) \in [N]^{2k}$ to (1.1).

Let $R_{P,2k}([N])$ be the contribution to $N_{P,2k}([N])$ from tuples $(x_1, \dots, x_k, y_1, \dots, y_k)$ satisfying

$$y_k = \max(y_1, \dots, y_k) = \max(x_1, \dots, x_k) = x_k.$$

Let $N'_{P,2k}([N])$ be the contribution to $N_{P,2k}([N])$ from tuples $(x_1, \dots, x_k, y_1, \dots, y_k)$ with

$$y_k = \max(y_1, \dots, y_k) > \max(x_1, \dots, x_k). \quad (2.13)$$

Then by symmetry,

$$N_{P,2k}([N]) \leq k^2 \cdot R_{P,2k}([N]) + 2k \cdot N'_{P,2k}([N]). \quad (2.14)$$

Since $R_{P,2k}([N]) \leq N \cdot N_{P,2k-2}([N])$ and $R_{P,2}([N]) = 0$, it follows from (2.14) that

$$N_{P,2k}([N]) \leq k \cdot \max_{1 \leq j \leq k} ((k^2 N)^{k-j} \cdot 2j \cdot N'_{P,2j}([N])). \quad (2.15)$$

We now bound $N'_{P,2k}([N])$. Let $M(P)$ be a positive integer (depending only on P) such that for all integers $n \geq M(P)$, we have

$$P(n) > \max(P(0), P(1), \dots, P(n-1)) \quad \text{and} \quad P(n) \geq n^d/2. \quad (2.16)$$

Let $M \geq M(P)$ and $\lambda \geq 1$ denote integers to be chosen later. Then by Corollary 2.4 (applied with $z := P(y_k)$ for $y_k \geq M$, using the conditions (2.13) and (2.16)) and the divisor bound, the quantity $N'_{P,2k}([N])$ is at most

$$M^{2k} + O_{k,d,\Delta_Q,\varepsilon}(N^\varepsilon) \cdot \sum_{M \leq y \leq N} \left(N^{k-1} G_{P,\lambda}([N], P(y)) + \frac{N^k}{y^{d/e_P}} + \frac{N^{k-1}}{\lambda^{1/e_P}} + N^{k-2} \right). \quad (2.17)$$

By Lemma 2.7, we conclude that

$$N'_{P,2k}([N]) \leq M^{2k} + O_{k,d,\Delta_Q,\varepsilon}(N^\varepsilon) \cdot (\lambda^2 N^{k-1/2} + N^k M^{1-d/e_P} + N^k \lambda^{-1/e_P} + N^{k-1}). \quad (2.18)$$

Choosing $M := \lfloor M(P) \cdot N^{1/4} \rfloor$ (say) and $\lambda := \lfloor N^{1/6} \rfloor$, we get (since $1 - d/e_P \leq -1/e_P$)

$$N'_{P,2k}([N]) \leq O_{k,d,\Delta_Q,M(P),\varepsilon}(N^\varepsilon) \cdot (N^{k/2} + N^{k-1/4e_P} + N^{k-1/6e_P}) \ll_{k,P,\varepsilon} N^{k-1/6e_P+\varepsilon}. \quad (2.19)$$

Finally, plug (2.19) into (2.15) to get $N_{P,2k}([N]) \ll_{k,P,\varepsilon} N^{k-1/6e_P+\varepsilon}$. This, plus the estimate (2.12) for trivial solutions, establishes the theorem. \square

REFERENCES

- [1] V. V. Batyrev and Y. Tschinkel. Manin's conjecture for toric varieties. *J. Algebraic Geom.*, 7(1):15–53, 1998.
- [2] E. Bombieri and J. Pila. The number of integral points on arcs and ovals. *Duke Math. J.*, 59(2):337–357, 1989.
- [3] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski. Multiplicative congruences with variables from short intervals. *J. Anal. Math.*, 124:117–147, 2014.
- [4] S. Chatterjee and K. Soundararajan. Random multiplicative functions in short intervals. *Int. Math. Res. Not. IMRN*, 3:479–492, 2012.
- [5] R. de la Bretèche. Compter des points d'une variété torique. *J. Number Theory*, 87(2):315–331, 2001.
- [6] R. de la Bretèche. Estimation de sommes multiples de fonctions arithmétiques. *Compositio Math.*, 128(3):261–298, 2001.

- [7] A. Granville and K. Soundararajan. Large character sums. *J. Amer. Math. Soc.*, 14(2):365–397, 2001.
- [8] A. J. Harper. On the limit distributions of some sums of a random multiplicative function. *J. Reine Angew. Math.*, 678:95–124, 2013.
- [9] A. J. Harper. Moments of random multiplicative functions, II: High moments. *Algebra Number Theory*, 13(10):2277–2321, 2019.
- [10] A. J. Harper. A note on character sums over short moving intervals, 2022. arXiv:2203.09448.
- [11] A. J. Harper, A. Nikeghbali, and M. Radziwill. A note on Helson’s conjecture on moments of random multiplicative functions. In *Analytic number theory*, pages 145–169. Springer, Cham, 2015.
- [12] W. Heap and S. Lindqvist. Moments of random multiplicative functions and truncated characteristic polynomials. *Q. J. Math.*, 67(4):683–714, 2016.
- [13] W. Heap, A. Sahay, and T. D. Wooley. A paucity problem associated with a shifted integer analogue of the divisor function. *J. Number Theory*, 242:660–668, 2023.
- [14] B. Hough. Summation of a random multiplicative function on numbers having few prime factors. *Math. Proc. Cambridge Philos. Soc.*, 150(2):193–214, 2011.
- [15] M. N. Huxley. A note on polynomial congruences. In *Recent progress in analytic number theory, Vol. 1 (Durham, 1979)*, pages 193–196. Academic Press, London-New York, 1981.
- [16] O. Klurman, I. D. Shkredov, and M. W. Xu. On the random Chowla conjecture. *Geom. Funct. Anal.*, 33(3):749–777, 2023.
- [17] S. V. Konyagin and T. Steger. Polynomial congruences. *Mat. Zametki*, 55(6):73–79, 158, 1994.
- [18] J. Najnudel. On consecutive values of random completely multiplicative functions. *Electron. J. Probab.*, 25:Paper No. 59, 28, 2020.
- [19] M. Pandey, V. Y. Wang, and M. W. Xu. Partial sums of typical multiplicative functions over short moving intervals. *Algebra Number Theory*, 18(2):389–408, 2024.
- [20] K. Soundararajan and M. W. Xu. Central limit theorems for random multiplicative functions. *J. Anal. Math.*, 151(1):343–374, 2023.
- [21] C. L. Stewart. On the number of solutions of polynomial congruences and Thue equations. *J. Amer. Math. Soc.*, 4(4):793–835, 1991.

COURANT INSTITUTE, 251 MERCER STREET, NEW YORK 10012, USA

IST AUSTRIA, AM CAMPUS 1, 3400 KLOSTERNEUBURG, AUSTRIA

Email address: vywang@alum.mit.edu

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, STANFORD, CA, USA

Email address: maxxu@stanford.edu