LARGE SIEVE ESTIMATE FOR MULTIVARIATE POLYNOMIAL MODULI AND APPLICATIONS

KARIN HALUPCZOK AND MARC MUNSCH

Abstract. We prove large sieve inequalities with multivariate polynomial moduli and deduce a general Bombieri–Vinogradov type theorem for a class of polynomial moduli having a sufficient number of variables compared to its degree. This sharpens previous results of the first author in two aspects: the range of the moduli as well as the class of polynomials which can be handled. As a consequence, we deduce that there exist infinitely many primes p such that $p-1$ has a prime divisor of size $\gg p^{2/5+o(1)}$ that is the value of an incomplete norm form polynomial.

1. Introduction

The large sieve in its arithmetic form was introduced by Linnik in the early 40s to bound the number of exceptions to Vinogradov's conjecture on the size of the least quadratic non-residue. Since then it has been the object of intensive study by mathematicians such as Rényi, Roth, Bombieri and others leading to the modern presentation in its analytic form called large sieve inequality. The classic form of the large sieve inequality and its generalizations is an extremely powerful tool and has many applications in analytic number theoretical problems. For instance, as a consequence of a high dimensional version of the large sieve, Gallagher [11] proved the 'generic' irreducibility and maximality of the Galois group for integral polynomials with bounded height. A more recent focus involves the large sieve over sparse sequences of moduli, such as powers or more general polynomials (see also [4] for results on arbitrary sparse sequences). Obtaining large sieve inequalities in this context has various applications in diverse arithmetic problems. Without being exhaustive, let us mention few examples such as the distribution of primes in sparse progressions [1, 3], the existence of shifted primes divisible by a large square [18, 20], elliptic curves [5, 26] or the study of Fermat quotients [7, 25].

The case of moduli defined as values of polynomials of several variables received much less attention. However, recently the first author obtained a general result in [13] using multidimensional Weyl sum estimates and highlighted several possible applications to problems related to the multiplicative structure of consecutive integers.

Recently, the second author [22] improved in some range of the parameters the existing large sieve inequalities with polynomial moduli in one variable. A

[0]2010 Mathematics Subject Classification. Primary: 11B57, 11L07, 11N32. Secondary: 11C08, 11N36.

Key words and phrases. Large sieve, polynomial of several variables, congruence equations, Vinogradov mean value theorem, Bombieri–Vinogradov theorem, primes in polynomial progressions.

Date: October 27, 2021.

crucial ingredient was the use of bounds on the number of solutions to polynomial equations in boxes. In Section 2 we explain how this idea can be adapted in our multivariable setting to give large sieve bounds which are sharper than those of [13] in the case of a general multivariate polynomial. Additionally, these multidimensional estimates allow us to deduce interesting consequences. As an application, we obtain in Section 3 a Bombieri–Vinogradov type theorem for a general class of polynomial moduli having a sufficiently large number of variables compared to the degree. The proof involves a very careful splitting of the range of the parameters where both classical large sieve and our new results are needed. In Section 3.3, we discuss an interesting choice of polynomials that can be made and in particular, the existence of infinitely many primes p such that $p-1$ is divisible by certain divisors of multidimensional polynomial shape.

2. Multidimensional polynomial large sieve

2.1. **Notation and conventions.** Throughout the paper, the notation $U = O(V)$, $U \ll V$ and $V \gg U$ are equivalent to $|U| \leqslant cV$ for some positive constant c, which depends on the degree of the polynomials involved and, where applies, on the coefficients of the polynomials.

For any quantity $V > 1$ we write $U = V^{o(1)}$ (as $V \to \infty$) to indicate a function of V which satisfies $V^{-\varepsilon} \leq |U| \leq V^{\varepsilon}$ for any $\varepsilon > 0$, provided V is large enough. One additional advantage of using $V^{o(1)}$ is that it absorbs $\log V$ and other similar quantities without changing the whole expression.

2.2. **Setting of the problem.** In this section we consider a polynomial $P \in \mathbb{Z}[X_1, \dots, X_\ell]$ in ℓ variables of total degree $k \geq 2$. For a real number $Q \geq 1$, we consider ℓ- tuples $\mathbf{q} = (q_1, \dots, q_\ell) \sim Q$ where $\mathbf{q} \sim Q$ means that $\mathbf{q}$ is in the dyadic Q- box $\prod_{i=1}^{\ell} [Q, 2Q)$. Let $\{a_n\}_{n\geq 1}$ denote a sequence of complex numbers and M, N positive integers. We define

$$\sum_{N,Q,P} := \sum_{\mathbf{q}\sim Q} \sum_{\substack{1\leq a\leq P(\mathbf{q}) \\ (a,P(\mathbf{q}))=1}} \left| S\left(\frac{a}{P(\mathbf{q})}\right)\right|^2$$

where as usual

$$S(\theta) := \sum_{M<n\leq M+N} a_n \mathrm{e}(n\theta) \tag{2.1}$$

and $\mathrm{e}(z) = \exp(2i\pi z)$ for $z \in \mathbb{C}$. Our main goal is to obtain large sieve inequalities which are bounds of the shape

$$\sum_{N,Q,P} \ll \Delta_{k,\ell}(Q,N) \sum_{n=M+1}^{M+N} |a_n|^2, \tag{2.2}$$

where $\Delta_{k,\ell}(Q,N)$ is some function of the parameters N and Q (which could both depend on k and ℓ) and the implied constant may also depend on the parameters k and ℓ. The reader may notice that repetitions are allowed in the definition of $\sum_{N,Q,P}$ meaning that it is possible to have $P(\mathbf{q}) = P(\mathbf{q}')$ for

different ℓ- tuples $\mathbf{q}$ and $\mathbf{q}'$ [1]. To state our results we need to introduce the following function which counts the number of representations of an integer by a polynomial,

$$r_P(m,Q) := \#\{\mathbf{q} \sim Q;\ P(\mathbf{q}) = m\}, \tag{2.3}$$

and the maximum over a dyadic box,

$$r_P^*(Q) := \max_{\mathbf{q}\sim Q} \{r_P(P(\mathbf{q}),Q)\}. \tag{2.4}$$

Several estimates on $\sum_{N,Q,P}$ already follow from the classic large sieve inequality that we recall now. A set of real numbers $\{x_k;\ k = 1,\dots,K\}$, is called *δ-spaced modulo* 1 if $\|x_k - x_j\| \geq \delta$ for all $1 \leq j < k \leq K$, where $\|x\|$ denotes the distance of a real number x to its closest integer. Then by a result of Montgomery and Vaughan [21, Theorem 1], we have

$$\sum_{k=1}^{K} \left| \sum_{n=M+1}^{M+N} a_n \mathrm{e}(x_k n) \right|^2 \leq (\delta^{-1} + N) \sum_{n=M+1}^{M+N} |a_n|^2. \tag{2.5}$$

Similarly as observed by Zhao in [29], we remark that the inequality (2.5) implies (2.2) with

$$\Delta_{k,\ell}(Q,N) = \min\left\{r_P^*(Q)(Q^{2k}+N), Q^{\ell}(Q^k+N)\right\}. \tag{2.6}$$

Due to the possible repetitions of the moduli $P(\mathbf{q})$, the factor $r_P^*(Q)$ appears in the inequality. This quantity is relatively harmless (say $r_P^*(Q) = Q^{o(1)}$) for the choice of polynomials appearing in our applications (see Section 3.3 for details). Furthermore, heuristics from Zhao in [29] make clear that conjecturally, we shall have in the ℓ-dimensional case

$$\Delta_{k,\ell}(Q,N) = (QN)^{o(1)} r_P^*(Q)(Q^{\ell+k}+N), \tag{2.7}$$

but we are still far away from proving this conjecture even for polynomials in one variable. It was conjectured in [15] that for the one-dimensional case $\ell = 1$, one should be able to reach

$$\Delta_{k,1}(Q,N) = (Q^{k+1} + Q^{1+1/(k-1)} N^{1-1/k(k-1)})(QN)^{o(1)}.$$

This was proved by the second author as [22, Thm. 1.2] with $k+1$ instead of $k-1$, thus confirming [15, Conjecture 21] with $\omega = 1/k(k+1)$.

Some improvements over the bound (2.6) have been obtained by the first author using Weyl sums estimates and the recent breakthroughs in Vinogradov's mean value theorem from [6, 28] and its generalizations to general polynomials of several variables [23]. More precisely it was proved in [13, eq. (5)] that (2.2) holds with

$$\Delta_{k,\ell}(Q,N) = (Q^{\ell(k+1)} + Q^{\ell - 1/2r_0\ell k} N + Q^{\ell+1/2r_0} N^{1-1/2r_0\ell k})(QN)^{o(1)}, \tag{2.8}$$

where $r_0 = \binom{\ell k+\ell-1}{\ell} - 1$. Adapting the methods of [6], the recent impressive work [12] extends [23] and essentially removes the factor 2 from the bound in the multidimensional version of Vinogradov's mean value theorem. [2] By

[1] We could have stated our results removing repetitions or weighting every moduli by the inverse of the number of appearances. For our purpose these formulations are essentially equivalent due to the polynomials being considered in applications where we essentially have very small preimages.

[2] The result is slightly more complicated to state and gives the expected number of solutions to multidimensional Vinogradov systems. The correcting factor for applications depends also on the number of variables ℓ but is very close to 2.

this result, the factor 2 in the exponent of (2.8) could also be deleted, leading already to a slight improvement.

In this note we go further and generalize the technique used in [22], which leads to a substantial improvement of the polynomial large sieve inequality in several variables. The best available bound of [12] in the multidimensional Vinogradov's mean value theorem serves in the next section as an ingredient.

2.3. **Modular equations in boxes.** To prove our main result, we need the following result of Kerr [17, Thm. 3.1] which bounds the number of solutions to multidimensional polynomial equations in boxes. This is a generalization of a result for polynomials in one variable [9, Theorem 1]. We consider a polynomial of degree $k \geq 2$,

$$P(\mathbf{x}) = \sum_{0 \leq |\mathbf{i}| \leq k} \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}}, \ \alpha_{\mathbf{i}} \in \mathbb{Z}_m,$$

such that

$$h_P := \min_{|\mathbf{i}|=k} |\alpha_{\mathbf{i}}| = 1, \tag{2.9}$$

where $|\mathbf{i}|$ is the sum of the components of $\mathbf{i} \in \mathbb{N}_0^\ell$, and $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_\ell^{i_\ell}$. Given any positive $K_1, \ldots, K_\ell, L, H, R \geq 1$ and $(a, m) = 1$, we define by $N(H, R; K_1, \ldots, K_\ell, L)$ the number of solutions to the congruence

$$aP(\mathbf{x}) \equiv y \ (\bmod m), \tag{2.10}$$

where

$$(\mathbf{x}, y) \in \prod_{i=1}^{\ell} [K_i + 1, K_i + H] \times [L + 1, L + R].$$

Lemma 2.1. *The following bound holds uniformly over arbitrary integers $K_1, \ldots, K_\ell$ and L:*

$$N(H, R; K_1, \ldots, K_\ell, L) \ll H^\ell \left((R/m)^{1/r(k+1)} + (R/H^k)^{1/r(k+1)} \right) m^{o(1)}, \tag{2.11}$$

where

$$r = \binom{k+\ell}{\ell} - 1. \tag{2.12}$$

Note that in [17, Thm. 3.1], this result was stated with $2r$ instead of r in (2.11) since the result [23] was used. Indeed Kerr made use of [23, Theorem 1.1] asserting that Vinogradov's systems of equations have at most the expected number of solutions as soon as the number of variables is large enough. Now thanks to the improvement of [23] in [12], the number of necessary variables can be reduced by a factor 2 [3]. This impacts the improved bound (2.11), and thus our work, too.

[3] Again the correcting factor is more complicated and depends on the number of variables but is just slightly larger than 2. For a more precise description of the gain here, see [23, Theorem 3.2] and the enlightening discussion following equation (1.4) in the same paper. For our purpose and to simplify the exposition we correct by a factor 2.

2.4. **Large sieve inequality for multivariate polynomials.** To begin with, we standardly define a subset of Farey fractions

$$\mathcal{S}(Q) := \left\{ \frac{a}{P(\mathbf{q})};\ (a, P(\mathbf{q})) = 1,\ 1 \leq a < P(\mathbf{q}),\ \mathbf{q} \sim Q \right\}.$$

We would like to count the number of such fractions which are close to each other. For this purpose we define

$$M(N, Q) = \max_{x \in \mathcal{S}(Q)} \#\left\{ y \in \mathcal{S}(Q);\ \|x - y\| < 1/2N \right\}. \tag{2.13}$$

We obtain the following bound depending only on the number of variables and the degree of the polynomial P.

Lemma 2.2. *Let ℓ be a positive integer and P a polynomial of degree $k \geq 2$ with $h_P = 1$ and such that $P(\mathbf{q}) \gg Q^{k+o(1)}$ for all $\mathbf{q} \sim Q$. For any integer N with $Q^k \leq N \leq Q^{2k}$, we have*

$$M(N, Q) \ll (QN)^{o(1)} Q^{\ell + k/r(k+1)} N^{-1/r(k+1)}, \tag{2.14}$$

with r as in (2.12).

Proof. Let $x = \frac{a}{P(\mathbf{q})}$ a fixed reduced fraction. We aim to estimate the number of $(\ell+1)$- tuple $(b, \mathbf{r})$ with $(b, \mathbf{r}) = 1$ such that

$$\left\| \frac{a}{P(\mathbf{q})} - \frac{b}{P(\mathbf{r})} \right\| = \frac{|aP(\mathbf{r}) - bP(\mathbf{q})|}{P(\mathbf{q})P(\mathbf{r})} < 1/2N. \tag{2.15}$$

Setting $z = aP(\mathbf{r}) - bP(\mathbf{q})$, our problem is equivalent to estimating the number of $(\ell+1)$- tuples $(b, \mathbf{r})$ such that $|z| \ll Q^{2k}/N$. This boils down to counting the number of $(\ell+1)$- tuples $(\mathbf{r}, z)$. The number of solutions is bounded above by the number of tuples with $\mathbf{r} \sim Q$ and $|z| \ll Q^{2k}/N$ which are solutions to the congruence

$$aP(\mathbf{r}) = z \ (\bmod P(\mathbf{q})). \tag{2.16}$$

Applying Lemma 2.1 to the polynomial P with parameters $H = Q$, $R = Q^{2k}/N$, and $m = P(\mathbf{q})$ we deduce that the numbers of $(\mathbf{r}, z)$ satisfying (2.16) is bounded above by

$$Q^{\ell+\varepsilon}(Q^k/N)^{1/r(k+1)}$$

for any $\varepsilon > 0$. This concludes the proof. □

We follow a routine method to prove large sieve inequalities and deduce the following theorem.

Theorem 2.3. *Let ℓ be a positive integer and P a polynomial of degree $k \geq 2$ with $h_P = 1$. For any integer N with $Q^k \leq N \leq Q^{2k}$ we have*

$$\sum_{N,Q,P}^{*} \ll (QN)^{o(1)} Q^{\ell + k/r(k+1)} N^{1 - 1/r(k+1)} \sum_{n=M+1}^{M+N} |a_n|^2, \tag{2.17}$$

with r as in (2.12) *and where $\sum^{*}_{N,Q,P}$ denotes the sum $\sum_{N,Q,P}$ restricted over those $\mathbf{q}$ such that $P(\mathbf{q}) \gg Q^{k+o(1)}$.*

Proof. We do not reproduce the full proof which is standard. This proof follows the method used for instance in the proofs of [22, Theorem 1.2] or [29, Theorem 2] by incorporating the result of Lemma 2.2. □

Remark 2.4. *It is worth to note that general large sieve bounds have been obtained in* [4, Theorem 1.1] *in terms of the additive energy of the sequence of moduli. For specific choices of multivariate polynomials it might be possible to efficiently bound this additive energy and compare the resulting bounds with Theorem 2.3.*

Remark 2.5. *For applications the estimate* (2.17) *over "good" moduli* $\mathbf{q}$ *is sufficient. Indeed for typical* $\mathbf{q}$ *we have* $P(\mathbf{q}) \gg Q^{k+o(1)}$ *or in other words the set of "bad" moduli has small density (see Lemma 3.4 below).*

3. A Bombieri–Vinogradov-type theorem with polynomial moduli

In this section, we prove a variant of the well-known Bombieri–Vinogradov-theorem. Compared to the classical theorem, the version we look at deals with moduli that are values of polynomials P in several variables. A first result in that direction has been established as [14, Thm. 1.2], where it is also discussed that such a variant goes beyond the potential of the classical Bombieri–Vinogradov-theorem, if the number of variables of P is smaller than its degree. We obtain here an improvement of this result since it gives an extension of the moduli range and can handle a much larger class of polynomials P as described below.

Setting 3.1. *Let* $P \in \mathbb{Z}[x_1, \dots, x_\ell]$ *be a polynomial of degree* $k \geq 2$ *with* $h_P = 1$ *that is the product of* m *irreducible polynomials* $H_1, \dots, H_m \in \mathbb{Z}[x_1, \dots, x_\ell]$, *each* H_j *of degree* $k_j \geq 1$ *where* ℓ_j *denotes the number of variables in* H_j. *We assume that* $h_{H_j} = 1$ *for all* $1 \leq j \leq m$ *and also require that* $r_P^*(Q) = Q^{o(1)}$. *Define as in* (2.12)

$$r = r_{k,\ell} := \binom{k+\ell}{\ell} - 1 \text{ and } \rho = \rho_{k,\ell} := r(k+1)/(r(k+1)-1). \tag{3.1}$$

For k_j *and* ℓ_j *define the correspondent* $r_j := r_{k_j,\ell_j}$ *and* $\rho_j := \rho_{k_j,\ell_j}$.

We obtain the following theorem.

Theorem 3.2 (A Bombieri–Vinogradov Theorem with polynomial moduli)**.** *Let* $A, Q, x > 1$ *be real, and* $P \in \mathbb{Z}[x_1, \dots, x_\ell]$ *a polynomial of degree* k *as in Setting 3.1. Assume that the polynomials* H_j *of degree* k_j *have pairwise disjoint sets of*

$$\ell_j \geq \Big(1 - \frac{1}{2\rho_j}\Big)k_j = \Big(1 + \frac{1}{r_j(k_j+1)}\Big)\frac{k_j}{2} \tag{3.2}$$

many variables for each $j = 1, \dots, m$. *Further suppose that*

$$Q \leq x^{1/(2k+k/2\rho)-\varepsilon} \tag{3.3}$$

for arbitrary $\varepsilon > 0$. *Let us recall the notation*

$$\psi(y; P(\mathbf{q}), a) := \sum_{\substack{n \leq y \\ n \equiv a \bmod P(\mathbf{q})}} \Lambda(n).$$

Then we have the estimate

$$\sum_{\mathbf{q} \sim Q} G_{\mathbf{q}} \frac{\varphi(P(\mathbf{q}))}{Q^\ell} \sup_{y \leq x} \max_{\substack{a \bmod P(\mathbf{q}) \\ \gcd(a, P(\mathbf{q}))=1}} |\psi(y; P(\mathbf{q}), a) - y/\varphi(P(\mathbf{q}))| \ll_{A,\ell,k,m,\varepsilon} \frac{x}{(\log x)^A},$$

where

$$G_{\mathbf{q}} := \mu^2(P(\mathbf{q}))\Lambda(H_1(\mathbf{q}))\cdots\Lambda(H_m(\mathbf{q})),$$

and where the sum runs over all $\mathbf{q}$ *with* $Q \le q_i < 2Q$, $i = 1, \dots, \ell$.

Remark 3.3. *A condition on the number of variables like* (3.2) *was not appearing in* [14] *where the result was stated only for very special polynomials and an uniform large sieve bound (equivalently a single choice of* $\Delta_{k,\ell}(Q, N)$*) was used in the proof. This new condition appears in Lemma 3.5 below and comes essentially from the use of the standard large sieve bound* (2.6) *(which does not depend on* ℓ*). It allows us to gain a substantial improvement in the level of distribution in comparison to* [14, Thm. 1.2]*, where the* Q*-exponent was around* $3k$ *whereas the exponent is here around* $5k/2$*. Note also that* [14, Thm. 1.2] *as well as Theorem 3.2 is only nontrivial in the case when* $\ell < k$*, since otherwise, the classical Bombieri–Vinogradov-theorem gives a stronger statement. It is also not hard to see that our proof works also when the condition* (3.2) *is not fulfilled producing a slightly smaller level of distribution.*

Since the proof of Theorem 3.2 follows closely Section 3 in [14], we restrict this presentation to the changes that need to be made. Briefly, the improvement comes from the sharpened polynomial large sieve inequality obtained in Theorem 2.3, together with a very careful case distinction.

Unlike in [14] we assume only that the polynomial P is the product of some irreducible polynomials with some conditions on their variable sets and degrees, that can be formulated in a much easier way. The weight $G_{\mathbf{q}}$ forces the factors $H_i(\mathbf{q})$ to attain prime values, so that all prime divisors of $P(\mathbf{q})$ are values of polynomials, too. This property allows us to apply the fundamental Lemma 3.5 below to any divisor of the polynomial P.

In order to apply Theorem 2.3, we need in the proof of Theorem 3.2 to discard the contribution of $\mathbf{q}$ such that $P(\mathbf{q})$ is small. The following simple lemma allows us to control the number of such "bad" moduli.

Lemma 3.4. *Let* $P \in \mathbb{Z}[X_1, \dots, X_\ell]$ *be a polynomial in* ℓ *variables of total degree* $k \ge 2$*. For every* $\varepsilon > 0$*, we have*

$$\#\left\{\mathbf{q} \sim Q, |P(\mathbf{q})| \le \varepsilon Q^k\right\} = O(\varepsilon^{1/k} Q^\ell),$$

where the implied constant only depends on P*,* k *and* ℓ*.*

Proof. We first prove the lemma when P contains a summand λq_1^k with $\lambda \neq 0$. Indeed, given any choice of $q_2, \dots, q_\ell \sim Q$, $P(\mathbf{q})$ is a nonzero integer polynomial of degree k in q_1. We remark by factorizing this polynomial over $\mathbb{C}$ that the inequality $|P(\mathbf{q})| \le \varepsilon Q^k$ forces q_1 to lie within $O\left(\varepsilon^{1/k} Q\right)$ of one of the (complex) roots of this polynomial. Hence, there is at most $O(\varepsilon^{1/k} Q^\ell)$ choices of such bad tuples $\mathbf{q}$. The general case boils down to this situation after applying a linear change of variables to P of the form $y_1 = q_1, y_2 = q_2 + \lambda_2 q_1, \dots, y_\ell = q_\ell + \lambda_\ell q_1$ for a suitable choice of $(\lambda_2, \dots, \lambda_\ell)$ depending only on the coefficients of P. □

Setting $\varepsilon := \varepsilon(Q) = (\log Q)^{-k(A+m+1)}$ and applying Lemma 3.4, we see that

$$\sum_{\substack{\mathbf{q}\sim Q \\ |P(\mathbf{q})|\le \varepsilon Q^k}} G_{\mathbf{q}} \frac{\varphi(P(\mathbf{q}))}{Q^\ell} \sup_{y\le x} \max_{\substack{a \bmod P(\mathbf{q}) \\ \gcd(a,P(\mathbf{q}))=1}} |\psi(y; P(\mathbf{q}), a) - y/\varphi(P(\mathbf{q}))| \ll \frac{x}{(\log x)^A},$$

where we trivially bounded $G_{\mathbf{q}}$ and $\psi(y; P(\mathbf{q}), a)$. Hence, we can always assume that $P(\mathbf{q}) \gg Q^{k+o(1)}$ in the rest of the proof and we will omit to precise it in the summations encountered.

The next Lemma is the key step in the proof and provides an improved version of the polynomial version of the mean value theorem [14, Thm. 4.1] respectively [14, Lemma 5.1].

Lemma 3.5 (Polynomial Mean Value Theorem)**.** *Let $Q, x > 1$, and $P \in \mathbb{Z}[x_1, \dots, x_\ell]$ be a polynomial of degree $k \geq 2$ with $h_P = 1$, $r_P^*(Q) = Q^{o(1)}$ and such that the number of variables verifies $\ell \geq (1 - 1/2\rho)k$. For a character χ we write $\psi(x, \chi) := \sum_{n \leq x} \chi(n)\Lambda(n)$. Then we have*

$$\sum_{\mathbf{q} \sim Q} \frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))} \sideset{}{^*}\sum_{\chi \bmod P(\mathbf{q})} \sup_{y \leq x} |\psi(y, \chi)| \ll (Qx)^{o(1)} Q^{\ell} x^{1-\delta'} \tag{3.4}$$

in the range $Q^{2k+k/2\rho+\varepsilon} \leq x$ for a sufficiently small $\varepsilon > 0$, with some $\delta' > 0$ sufficiently small depending on ε.

Proof. Without loss of generality we can assume that x lies in the interval $Q^{2k+\delta_1} \leq x \leq Q^{2k+\delta}$ for some parameters $k/2\rho < \delta_1 < \delta$. We can also assume that $\delta < k$, since if $x \geq Q^{3k}$, the assertion follows already from [14, Lemma 5.1]. We follow the proof of [14, Thm. 4.1] and apply Vaughan's identity. To do so, let us introduce the parameter U as

$$U := x/Q^{k+H} \tag{3.5}$$

for an appropriate parameter $0 < H < k$ to be chosen later. To obtain (3.4), it suffices to find an upper bound for

$$S_1 := \sum_{\mathbf{q} \sim Q} \frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))} \sideset{}{^*}\sum_{\chi \bmod P(\mathbf{q})} \sum_{r \leq U} \max_{w} \Big| \sum_{w < s \leq x/r} \chi(sr) \Big|$$

and

$$S_M := \sum_{\mathbf{q} \sim Q} \frac{P(\mathbf{q})}{\varphi(P(\mathbf{q}))} \sideset{}{^*}\sum_{\chi \bmod P(\mathbf{q})} \Big| \sum_{m \sim M} \sum_{s \leq x/m} a(m) b(s) \chi(sm) \Big|,$$

for any M in the interval $U \leq M \leq W := \max(U^2, x/U)$. Here $a(n)$ and $b(n)$ are arithmetic functions depending on U only and such that $|b(n)| \leq \tau(n)$, $|a(n)| \leq \log n$ for all $n \in \mathbb{N}$.

We bound S_1 using the Pólya–Vinogradov inequality and obtain

$$S_1 \ll U Q^{\ell + 3k/2 + o(1)} = x Q^{\ell + k/2 - H + o(1)}.$$

To ensure that $S_1 \ll Q^{\ell} x^{1-\delta'}$ for some $\delta' > 0$, we need

$$k/2 < H < k. \tag{3.6}$$

Bounding S_M requires a more careful analysis and the factor $\Delta_{k,\ell}(Q, x)$ appearing in the large sieve inequality (2.2) comes into play. Applying [14, Lemma 3.2], which follows essentially from the inequality of Cauchy–Schwarz,

we obtain

$$S_M \ll Q^{o(1)}(\Delta_{k,\ell}(Q,M)M)^{1/2}(\Delta_{k,\ell}(Q,x/M)x/M)^{1/2} \tag{3.7}$$
$$= Q^{o(1)}x^{1/2}\Delta_{k,\ell}(Q,M)^{1/2}\Delta_{k,\ell}(Q,x/M)^{1/2}.$$

We split the interval $[U,W]$ into three subintervals with boundaries at Q^k and x/Q^k. In each of these subintervals, which we call here regions, we estimate S_M using different large sieve inequalities, or equivalently different values of $\Delta_{k,\ell}(Q,x)$ coming both from Theorem 2.3 and the trivial bound (2.6).

First region: $M \in [U, Q^k]$.

We apply the standard large sieve bound (2.6)

$$\Delta_{k,\ell}(Q,M) \ll Q^\ell M + Q^{\ell+k} \ll Q^{\ell+k}.$$

Since $Q^k \le x/Q^k \le x/M \le x/U = Q^{k+H} \le Q^{2k}$, we can apply Theorem 2.3 and take $\Delta_{k,\ell}(Q,x/M) = Q^{\ell+k/r(k+1)}(x/M)^{1-1/r(k+1)}$. Hence, it follows from (3.7) that

$$S_M \ll Q^{o(1)}x^{1/2}Q^{(\ell+k)/2}\cdot Q^{\ell/2+k/2r(k+1)}(x/M)^{1/2-1/2r(k+1)}$$
$$\ll Q^{o(1)}x^{1/2}Q^{\ell+k/2+k/2r(k+1)+(k+H)(1/2-1/2r(k+1))},$$

where we used that $x/M \le Q^{k+H}$ holds in this region. Inserting $x \le Q^{2k+\delta}$, we have $S_M \ll Q^{\gamma+o(1)}$ where

$$\gamma := \ell + \frac{2k+\delta}{2} + \frac{k}{2} + \frac{k+H}{2} - \frac{H}{2r(k+1)}.$$

To obtain (3.4) we need to show that $\gamma < \ell + 2k + \delta_1$. Choosing δ such that $\delta - \delta_1$ is sufficiently small, it suffices to show that $\gamma < \ell + 2k + \delta$. This holds true as soon as

$$2k + \frac{\delta}{2} + \frac{H}{2} - \frac{H}{2r(k+1)} < 2k + \delta,$$

i.e. if

$$H\Big(1 - \frac{1}{r(k+1)}\Big) = H/\rho < \delta. \tag{3.8}$$

Under this additional restriction on H, this implies $S_M \ll Q^\ell x^{1-\delta'}$ for any sufficiently small $\delta' > 0$.

Second region: $M \in [Q^k, x/Q^k]$.

In this region we have $Q^k \le x/M \le x/Q^k \le Q^{2k}$, since we assumed $x \le Q^{3k}$. Then Theorem 2.3 applies to both the sum over the intervals of size M and x/M. From (3.7), this yields the bound

$$S_M \ll Q^{o(1)}x^{1/2}\Delta_{k,\ell}(Q,M)^{1/2}\Delta_{k,\ell}(Q,x/M)^{1/2}$$
$$\ll Q^{o(1)}x^{1/2}Q^{\ell+k/r(k+1)}M^{1/2-1/2r(k+1)}(x/M)^{1/2-1/2r(k+1)}$$
$$= Q^{o(1)}x^{1-1/2r(k+1)}Q^{\ell+k/r(k+1)} = Q^{o(1)}xQ^\ell(Q^{2k}/x)^{1/2r(k+1)},$$

and having $Q^{2k+\delta_1} \le x$, the last term is $\ll Q^\ell x^{1-\delta'}$ for any sufficiently small $\delta' > 0$, as was to be shown.

Third region: $M \in [x/Q^k, W]$ with $W = \max\{U^2, x/U\}$.

• Consider first the case $W = x/U$, so that $M \leq W \leq Q^{2k}$ by the choice of U. Theorem 2.3 can be applied for the sum over $m \sim M$, and we use the standard bound $\Delta_{k,\ell}(Q, x/M) \ll Q^{\ell+k}$ following from (2.6) and $x/M \ll Q^k$. Remark that this situation is symmetric to the one in the first region. Therefore we use (3.7) from above which yields the bound

$$\begin{aligned} S_M &\ll Q^{o(1)} x^{1/2} \Delta_{k,\ell}(Q, M)^{1/2} \Delta_{k,\ell}(Q, x/M)^{1/2} \\ &\ll Q^{o(1)} x^{1/2} Q^{(\ell+k)/2} \cdot Q^{\ell/2+k/2r(k+1)} M^{1/2-1/2r(k+1)}. \end{aligned}$$

Now inserting $M \leq W = x/U = Q^{k+H}$, we get the same upper bound for S_M as in the first region, so we are done in this case by symmetry.

• If otherwise $W = U^2$, then we use again the standard bound $\Delta_{k,\ell}(Q, x/M) \ll Q^{\ell+k}$ from (2.6). Also from (2.6), we know the bound

$$\Delta_{k,\ell}(Q, M) \ll r_P^*(Q)(M + Q^{2k}) \ll Q^{o(1)}(M + Q^{2k}).$$

We split further the discussion into two subcases depending on whether $M \leq Q^{2k}$ or not. In the former case we have

$$S_M \ll Q^{o(1)} x^{1/2} \Delta_{k,\ell}(Q, M)^{1/2} \Delta_{k,\ell}(Q, x/M)^{1/2} \ll Q^{o(1)} x^{1/2} Q^k Q^{(\ell+k)/2}.$$

Inserting $x \leq Q^{2k+\delta}$, we have $S_M \ll Q^{\gamma_1+o(1)}$ where

$$\gamma_1 := \frac{1}{2}(3k + \delta - \ell) + \ell + k.$$

To infer (3.4), we argue as in the first region and thus we need to show that $\gamma_1 < \ell + 2k + \delta$. A quick computation reveals that this is equivalent to

$$k - \ell < \delta.$$

This holds true under the hypothesis $\ell \geq (1 - 1/2\rho)k$ and $\delta > k/2\rho$.

In the latter case $M \geq Q^{2k}$, recall that $M \ll U^2 = x^2 Q^{-2k-2H}$. As before, using (3.7), we arrive at

$$S_M \ll Q^{o(1)} x^{1/2} Q^{(\ell+k)/2} M^{1/2} \ll Q^{o(1)} x^{1/2} Q^{(\ell+k)/2} x Q^{-k-H}.$$

Inserting $x \leq Q^{2k+\delta}$, we have $S_M \ll Q^{\gamma_2+o(1)}$ where

$$\gamma_2 := 2k + \delta + \ell/2 + k/2 + \delta/2 - H.$$

Arguing as above, to deduce (3.4), we need to show that $\gamma_2 < \ell + 2k + \delta$. This holds if

$$k/2 + \delta/2 - H < \ell/2,$$

i.e.

$$H > \delta/2 + (k - \ell)/2. \tag{3.9}$$

Under this additional restriction on H, this implies $S_M \ll Q^\ell x^{1-\delta'}$ for any sufficiently small $\delta' > 0$.

To finish the proof we need to choose the parameter H subject to the restrictions (3.6), (3.8) and (3.9). The hypothesis $\delta_1 > k/2\rho$ ensures that both (3.6) and (3.8) can hold together. Now under the condition $\ell \geq (1 - 1/2\rho)k$ we have $\delta/2 + (k - \ell)/2 < \delta$ so (3.9) holds too. This concludes the proof.

□

3.1. **Conjectural level of distribution.** The question arises of the level of distribution that can be expected under the assumption of the multidimensional analogue (2.7) of Zhao's conjecture. We give some hints about the changes to be made under this assumption. The application of Theorem 2.3 in the proof of Lemma 3.5 is then replaced by the application of (2.7). Hence in the first region, we get $\Delta_{k,\ell}(Q, x/M) \ll (Q^{\ell+k}+Q^{k+H})Q^{o(1)} \ll Q^{k+\max\{\ell,H\}}Q^{o(1)}$ and $\gamma = k+\delta/2+(k+\ell)/2+k/2+\max\{\ell,H\}/2$, which is $< \ell+2k+\delta$ if we choose

$$H < \ell + \delta. \tag{3.10}$$

This new condition on H replaces condition (3.8). In the third region with $W = U^2$, the bound $\Delta_{k,\ell}(Q,M) \ll (Q^{\ell+k}+M)Q^{o(1)}$ leads to the new subcase distinction $M \le Q^{\ell+k}$ and $M > Q^{\ell+k}$. In the former case, $\gamma_1 = \ell+2k+\delta/2$ is already admissible, and the treatment of the second case does not change. To guarantee that H can be chosen subject to the restrictions (3.6), (3.9) and (3.10) we need that $\delta+\ell > k/2$ as well as $\delta+\ell > \delta/2+(k-\ell)/2$, leading to $\delta > \max\{k/2-\ell, k-3\ell\}$. Therefore when $\ell \ge k/2$, we can choose any $\delta > 0$ and (2.7) leads to an analogue of Lemma 3.5 in the range

$$Q^{2k+\varepsilon} \le x \tag{3.11}$$

reaching the optimal expected range. It is worth to notice that the method for $\ell = 1$ seems to lead to a Bombieri–Vinogradov theorem in the range $Q^{2k+\varepsilon} \le x$ only when $k = 2$ (it was also proved unconditionally by Baker [2]), while heuristically this range should be reached for any degree.

3.2. **Proof of Theorem 3.2.** Due to the assigned weight $G_{\mathbf{q}}$, each $P(\mathbf{q})$ on the left hand side of the assertion is squarefree. The tuple $\mathbf{q}$ has therefore the property that each $H_j(\mathbf{q})$ equals to a prime, and these primes $H_1(\mathbf{q}), \dots, H_m(\mathbf{q})$ are pairwise different.

Therefore, a divisor d of $P(\mathbf{q})$ must be $d = 1$ or $d = \tilde{P}(\mathbf{q})$ for some polynomial $\tilde{P}$ that divides P in $\mathbb{Z}[\mathbf{x}]$.

Following the proof of [14, Thm. 1.2], our task is reduced to give a proof of the bound

$$\sum_{\substack{\tilde{P}\mid P\\ \tilde{P}\neq 1}} \sum_{\mathbf{q}\sim Q} G_{\mathbf{q}} Q^{-\ell} \sideset{}{^*}\sum_{\chi \bmod \tilde{P}(\mathbf{q})} \sup_{y\le x} |\psi(y,\chi)| \ll x^{1-\delta} \tag{3.12}$$

for any small $\delta > 0$, where χ runs through the primitive characters mod $\tilde{P}(\mathbf{q})$, denoted by the star at the sum.

The key observation is that Lemma 3.5 can be applied to each nonconstant $\tilde{P} \mid P$ (remark that for divisors of degree 1, it follows directly from the classical Bombieri–Vinogradov theorem). Indeed, we need to verify the hypotheses of Lemma 3.5. First of all, a short calculation shows that

$$1/(2k+k/2\rho) \le 1/(2\tilde{k}+\tilde{k}/2\tilde{\rho}) \tag{3.13}$$

holds true for all nonconstant $\tilde{P} \mid P$ with corresponding degree $\tilde{k} \le k$. Hence the variable Q belongs to the admissible range. Denote by $\tilde{\ell}$ the number of

variables of $\tilde{P}$. Our assumption (3.2) and the fact that we know that the H_j have disjoint sets of variables implies by additivity

$$\tilde{\ell} \geq \Big(1 - \frac{1}{2\tilde{\rho}}\Big)\tilde{k} = \Big(1 + \frac{1}{\tilde{r}(\tilde{k}+1)}\Big)\frac{\tilde{k}}{2}$$

for any nonconstant factor $\tilde{P} \mid P$.

Hence, the application of Lemma 3.5 is possible and we can bound the left hand side of (3.12) by

$$\sum_{\tilde{P}|P} x^{1-\delta'}(\log x)^m \ll_m x^{1-\delta}$$

for any small $\delta > 0$, where we used that there are only $\ll_m 1$ many divisor polynomials of P in $\mathbb{Z}[\mathbf{x}]$. The theorem follows.

3.3. **Choice of admissible polynomials.** In order to be meaningful, our result needs to be applied to polynomials H_j taking a lot of prime values. In one variable, the Bunyakovsky conjecture states that, under mild conditions, any irreducible polynomial should take infinitely many prime values. Its quantitative version, the Bateman–Horn conjecture, predicts the frequency of prime values in polynomial sequences. Even though such a statement remains widely open for any fixed polynomial of degree greater than 2, it has been recently proved that Bateman-Horn conjecture holds for 100% of polynomials [27]. For polynomials of several variables, the situation is different and only a few examples of polynomials taking infinitely many prime values are known. For instance, this has been proved using sieve methods by Friedlander and Iwaniec [10] for $x^2 + y^4$ or by Heath-Brown [16] for $x^3 + 2y^3$.

The reader might wonder if any such good choice is possible for our problem. Indeed, we can choose the polynomials H_j explicitly as norm form polynomials, i.e. $H_j(\mathbf{x}_j) = N_K(\mathbf{x}_j)$, for a certain number field K over $\mathbb{Q}$ and a set of ℓ_j many variables. Inspired by the aforementioned works, Maynard proved in [19] that these polynomials takes the expected number of prime values when $\ell_j \geq 3k_j/4$. Precisely, the number of $\mathbf{q}_j \sim Q$ such that $H_j(\mathbf{q}_j) = N_K(\mathbf{q}_j)$ is prime is $\gg Q^\ell/\log Q$ by [19, Thm. 1.1]. (Note that our condition $\ell_j \geq (1 - 1/2\rho_j)k_j$ holds true assuming $\ell_j > 3k_j/4$.)

Thus, this result shows that for this choice of polynomials the number of moduli that are admissible in Theorem 3.2 is $\gg Q^\ell/\log Q$. This prevents Theorem 3.2 to follow trivially from an application of the classical Bombieri–Vinogradov-Theorem. Furthermore these polynomials verify the hypothesis $r^*_{N_K}(Q) \ll Q^{o(1)}$ of Setting 3.1 on the number of possible repetitions. Indeed, the specific structure of the polynomials N_K written as a norm allows to apply the divisor bound in number fields [4] [8, Proposition 2.5] or more precise results by Schmidt [24, Theorem 3] on norm form equations. As a consequence, let us mention the following result:

Corollary 3.6. *Let n, k be positive integers. Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial of degree n with root $\omega \in \mathbb{C}$. Let $K = \mathbb{Q}(\omega)$ be the*

[4] See also the discussion on mathoverflow: https://mathoverflow.net/questions/68437/the-divisor-bound-in-number-fields

corresponding number field of degree n, and let $N_K \in \mathbb{Z}[X_1, \dots, X_{n-k}]$ be the incomplete norm form

$$N_K(q_1, \dots, q_{n-k}) = N_{K/\mathbb{Q}}\left(\sum_{i=1}^{n-k} q_i \omega^{i-1}\right).$$

Then if $n \geq 4k$, there exist infinitely many primes p such that $p-1$ has a prime divisor $d = N_K(q_1, \dots, q_{n-k})$ of size $\gg p^{2/5+o(1)}$.

Proof. The method to prove such a result from a Bombieri–Vinogradov theorem is classical and can be found for instance in [1, Thm. 5]. Hence, we will not give all the details. Mainly speaking, it is sufficient to consider the following sum

$$\sum_{x<n\leq 2x} \Lambda(n+1) \sum_{\substack{\mathbf{q}\sim Q \\ N_K(\mathbf{q})\mid n}} \Lambda(N_K(\mathbf{q}))$$

and switch the summation. Then [19, Thm. 1] asserts that the polynomial N_K takes the expected number of prime values and we can conclude using Theorem 3.2 in the admissible range $Q \leq x^{2/5n+o(1)}$. □

A similar result could have been stated for primes p such that $p-1$ has a prime divisor $d = x^3 + 2y^3 \gg p^{72/179+o(1)}$ using Heath-Brown's result combined with Theorem 3.2. Here the exponent $72/179$ comes from the explicit computation of $1/(2k + k/2\rho)$ in Theorem 3.2 and gives a slight improvement over $2/5$.

Acknowledgements

The second author would like to thank the Max Planck Institute for Mathematics, Bonn, and the University of Düsseldorf for support and hospitality during his work on this project. The second author also acknowledges support of the Austrian Science Fund (FWF), stand-alone project P 33043 "Character sums, L-functions and applications".

Data availability statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

[1] S. Baier and L. Zhao. Bombieri-Vinogradov type theorems for sparse sets of moduli. *Acta Arith.*, 125(2):187–201, 2006.

[2] R. Baker. Primes in arithmetic progressions to spaced moduli. III. *Acta Arith.*, 179(2):125–132, 2017.

[3] R. C. Baker. Primes in arithmetic progressions to spaced moduli. *Acta Arith.*, 153(2):133–159, 2012.

[4] R. C. Baker, M. Munsch and I. E. Shparlinski. Additive energy and a large sieve inequality for sparse sequences. *Preprint*, https://arxiv.org/abs/2103.12659.

[5] W. D. Banks, F. Pappalardi, and I. E. Shparlinski. On group structures realized by elliptic curves over arbitrary finite fields. *Exp. Math.*, 21(1):11–25, 2012.

[6] J. Bourgain, C. Demeter, and L. Guth. Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three. *Ann. of Math. (2)*, 184(2):633–682, 2016.

[7] J. Bourgain, K. Ford, S. V. Konyagin, and I. E. Shparlinski. On the divisibility of Fermat quotients. *Michigan Math. J.*, 59(2):313–328, 2010.

[8] M. Chang. Factorization in generalized arithmetic progressions and application to the Erdős-Szemerédi sum-product problems. *Geometric Functional Analysis GAFA*, 13(4):720–736, 2003.
[9] J. Cilleruelo, M. Z. Garaev, A. Ostafe, and I. E. Shparlinski. On the concentration of points of polynomial maps and applications. *Math. Z.*, 272(3-4):825–837, 2012.
[10] J. Friedlander and H. Iwaniec. The polynomial $X^2 + Y^4$ captures its primes. *Ann. of Math. (2)*, 148(3):945–1040, 1998.
[11] P. X. Gallagher. The large sieve and probabilistic Galois theory. In *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pages 91–101, 1973.
[12] S. Guo and R. Zhang. On integer solutions of Parsell-Vinogradov systems. *Invent. Math.*, 218(1):1–81, 2019.
[13] K. Halupczok. Large sieve inequalities with general polynomial moduli. *Q. J. Math.*, 66(2):529–545, 2015.
[14] K. Halupczok. A Bombieri-Vinogradov theorem with products of Gaussian primes as moduli. *Funct. Approx. Comment. Math.*, 57(1):77–91, 2017.
[15] K. Halupczok. Bounds for discrete moments of Weyl sums and applications. *Acta Arith.*, 194(1):1–28, 2020.
[16] D. R. Heath-Brown. Primes represented by $x^3 + 2y^3$. *Acta Math.*, 186(1):1–84, 2001.
[17] B. Kerr. Solutions to polynomial congruences in well-shaped sets. *Bull. Aust. Math. Soc.*, 88(3):435–447, 2013.
[18] K. Matomäki. A note on primes of the form $p = aq^2 + 1$. *Acta Arith.*, 137(2):133–137, 2009.
[19] J. Maynard. Primes represented by incomplete norm forms. *Forum Math. Pi*, 8:e3, 128, 2020.
[20] J. Merikoski. On the largest square divisor of shifted primes. *Acta Arith.*, 196(4):349–386, 2020.
[21] H. L. Montgomery and R. C. Vaughan. The large sieve. *Mathematika*, 20(2):119–14, 1973.
[22] M. Munsch. A large sieve inequality for power moduli. *Acta Arith.*, 197(2):207–211, 2021.
[23] S. T. Parsell, S. M. Prendiville, and T. D. Wooley. Near-optimal mean value estimates for multidimensional Weyl sums. *Geom. Funct. Anal.*, 23(6):1962–2024, 2013.
[24] W. M. Schmidt. The number of solutions of norm form equations. *Transactions of the American Mathematical Society*, 317(1):197–227, 1990.
[25] I. E. Shparlinski. Fermat quotients: exponential sums, value set and primitive roots. *Bull. Lond. Math. Soc.*, 43(6):1228–1238, 2011.
[26] I. E. Shparlinski and L. Zhao. Elliptic curves in isogeny classes. *J. Number Theory*, 191:194–212, 2018.
[27] A. N. Skorobogatov and E. Sofos. Schinzel hypothesis with probability 1 and rational points. *Preprint*, https://arxiv.org/abs/2005.02998.
[28] T. D. Wooley. Vinogradov's mean value theorem via efficient congruencing. *Ann. of Math. (2)*, 175(3):1575–1627, 2012.
[29] L. Zhao. Large sieve inequality with characters to square moduli. *Acta Arith.*, 112(3):297–308, 2004.