ON THE DENSITY OF INTEGER POINTS ON GENERALISED MARKOFF-HURWITZ HYPERSURFACES

MEI-CHU CHANG AND IGOR E. SHPARLINSKI

Abstract. We use bounds of mixed character sums modulo a square-free integer q of a special structure to estimate the density of integer points on the hypersurface

$$f_1(x_1) + \ldots + f_n(x_n) = a x_1^{k_1} \ldots x_n^{k_n}$$

for some polynomials $f_i \in \mathbb{Z}[X]$ and nonzero integers a and k_i, $i = 1, \ldots, n$. In the case of

$$f_1(X) = \ldots = f_n(X) = X^2 \qquad \text{and} \qquad k_1 = \ldots = k_n = 1$$

the above hypersurface is known as the Markoff-Hurwitz hypersurface. Our results are substantially stronger than those known for general hypersurfaces.

1. Introduction

Studying the density of integer and rational points $(x_1, \ldots, x_n)$ on hypersurfaces has always been an active area of research, where many rather involved methods have led to remarkable achievements, see [5, 6, 14, 15, 21, 22, 25, 26, 28] and references therein. More precisely, given a hypersurface

$$F(x_1, \ldots, x_n) = 0$$

defined by a polynomial $F \in \mathbb{Z}[X_1, \ldots, X_n]$ in n variables, the goal is to estimate the number $N_F(\mathfrak{B})$ of solutions $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ that fall in a hypercube $\mathfrak{B}$ of the form

$$\mathfrak{B} = [u_1 + 1, u_1 + h] \times \ldots \times [u_n + 1, u_n + h]. \qquad (1)$$

Unfortunately, even in the most favourable situation, the currently known general approaches lead only to a bound of the form $N_F(\mathfrak{B}) = O\left(h^{n-2+\varepsilon}\right)$ for any fixed $\varepsilon > 0$ or even weaker, see [6, 15, 25, 26]. For some special types of hypersurfaces the strongest known bounds are due Heath-Brown [14] and Marmon [21, 22]. For example, for

2010 *Mathematics Subject Classification.* 11D45, 11D72, 11L40.

Key words and phrases. Integer points on hypersurfaces, multiplicative character sums.

hypercubes around the origin, Marmon [22] gives a bound of the form $N_F(\mathfrak{B}) = O\left(h^{n-4+\delta_n}\right)$ for a class of hypersurfaces, with some explicit function δ_n such that $\delta_n \sim 37/n$ as $n \to \infty$. Combining this bound with some previous results and methods, for a certain class of hypersurfaces, Marmon [22] also derives the bound $N_F(\mathfrak{B}) = O\left(h^{n-4+\delta_n} + h^{n-3+\varepsilon}\right)$ which holds for an arbitrary hypercube $\mathfrak{B}$ with any fixed $\varepsilon > 0$ and the implied constant that depends only of $\deg F$, n and ε (note that $\delta_n > 1$ for $n < 29$).

Finally, we also recall that when the number of variables n is exponentially large compared to d and the highest degree form of F is nonsingular, then the methods developed as the continuation of the work of Birch [4] lead to much stronger bounds, of essentially optimal order of magnitude.

Here, we show that in some interesting special cases, to which further developments of [4] do not apply (as the highest degree form is singular and the number of variables is not large enough) a modular approach leads to stronger bounds where the saving actually grows with n (at a logarithmic rate).

More precisely we concentrate on hypersurfaces of the form

$$f_1(x_1) + \ldots + f_n(x_n) = a x_1^{k_1} \ldots x_n^{k_n} \tag{2}$$

defined by some polynomials $f_i \in \mathbb{Z}[X]$ and nonzero integers a and k_i, $i = 1, \ldots, n$. In particular, we use $N_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B})$ to denote the number of integer solutions to (2) with $(x_1, \ldots, x_n) \in \mathfrak{B}$, where $\mathbf{f} = (f_1, \ldots, f_n)$ and $\mathbf{k} = (k_1, \ldots, k_n)$.

In the case of

$$f_1(X) = \ldots = f_n(X) = X^2 \qquad \text{and} \qquad k_1 = \ldots = k_n = 1 \tag{3}$$

the equation (2) defines the *Markoff-Hurwitz hypersurface*, see [1, 2, 3, 7], where various questions related to these hypersurfaces have been investigated.

Furthermore, for

$$f_1(X) = \ldots = f_n(X) = X^n \qquad \text{and} \qquad k_1 = \ldots = k_n = 1 \tag{4}$$

the equation (2) is known as the *Dwork hypersurface*, which has been intensively studied by various authors [12, 13, 18, 19, 30], in particular, as an example of a *Calabi–Yau variety*.

We remark that solutions with at least one component $x_i = 0$, $i = 1, \ldots, n$, correspond to solutions of a diagonal equation

$$\sum_{\substack{j=1\\ j\neq i}}^{n} f_j(x_j) = -f_i(0)$$

to which one can apply the standard circle method.

To clarify our ideas and to make the exposition simpler we concentrate here on the solutions to (2) with $x_1 \ldots x_n \neq 0$. In particular, we use $N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B})$ to denote the number of such solutions. Clearly for the hypercubes $\mathfrak{B}$ of the form (1) we have

$$N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B}) = N_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B}).$$

Throughout the paper, the implied constants in the symbols "O", "$\ll$" and "$\gg$" may depend on the polynomials $\deg f_i$, the coefficient a and the exponents k_i in (2), $i = 1, \ldots, n$, and also on the integer positive parameters r and ν. We recall that the expressions $A = O(B)$, $A \ll B$ and $B \gg A$ are each equivalent to the statement that $|A| \le cB$ for some constant c.

Here, we use some ideas from [27], combined a new bound of mixed character sums, that can be of independent interest, to derive the following result:

Theorem 1. *Let $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$ be n polynomials of degrees at most d, and let $k_1, \ldots, k_n \ge 1$ be odd integers. For any fixed integer $r \ge 1$, there is a constant $C(r)$ depending only on r, such that, uniformly over all boxes $\mathfrak{B}$ of the form* (1) *with*

$$\max_{i=1,\ldots,n} |u_i| \le \exp(C(r)h^{4/9})$$

for the solutions to the equation (2)*, we have*

$$N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B}) \ll h^{n-4r/9}$$

provided that

$$n > (d+1)(d+2)2^r \max\{2r, 3r - 9/2\} + 2.$$

The proof of Theorem 1 is based on a bound of mixed character sums which combines the ideas from [9, 16].

Unfortunately Theorem 1 does not apply to the Dwork hypersurface as the degrees of the polynomials in (4) are too large for our argument to work. So here apply an alternative approach that is based on the method of Postnikov [23, 24] (see also [10] and the references therein for further developments). This leads to a much more precise bound which however applies only when the degree of the polynomials $f_1(X), \ldots, f_n(X)$ are sufficiently large.

Theorem 2. *Let $f_1(X), \ldots, f_n(X) \in \mathbb{Z}[X]$ be n polynomials of degrees at least d, and let $k_1, \ldots, k_n \ge 1$ be odd integers. There is an absolute constant C such that, uniformly over all boxes $\mathfrak{B}$ of the form* (1) *with*

$$\max_{i=1,\ldots,n} |u_i| \le \exp(Ch^{1/3})$$

and any fixed integer $r \ge 1$ *with*

$$r \le \min_{i=1,\ldots,n} \deg f_i$$

for the solutions to the equation (2)*, we have*

$$N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B}) \ll h^{n-r/3}$$

provided that

$$n > 2r^3 + 1.$$

Finally, in some cases the arithmetic structure of the right hand side of the equation (2) allows to derive a much stronger bound via the result of [8]. We illustrate this in the special case of the equation

$$x_1^d + \ldots + x_n^d = a x_1^{k_1} \ldots x_n^{k_n}$$

and the box $\mathfrak{B}$ aligned along the main diagonal, that is, of the form

$$\mathfrak{B} = [u+1, u+h] \times \ldots \times [u+1, u+h] \qquad (5)$$

with some integers u and h.

Theorem 3. *Let* $f_1(X) = \ldots = f_n(X) = X^d$ *and let* a, $k_1, \ldots, k_n$ *be arbitrary nonzero integers. Then, uniformly over all boxes* $\mathfrak{B}$ *of the form* (5)*, for the solutions to the equation* (2) *we have*

$$N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B}) \ll h^{d(d+1)/2+o(1)}.$$

2. Some Bounds of Classical Exponential and Character Sums

We denote

$$\mathbf{e}(z) = \exp(2\pi i z).$$

We start with recording the following trivial implication of the orthogonality of exponential functions.

For quadratic polynomials, we see that [17, Theorem 8.1] implies

Lemma 4. *For an integer* $q \ge 1$ *and any linear polynomial*

$$G(X) = aX \in \mathbb{Z}[X]$$

with $\gcd(a, q) = 1$

$$\left| \sum_{z=1}^{H} \mathbf{e}(G(z)/q) \right| \ll q.$$

For quadratic polynomials, we see that [17, Theorem 8.1] yields:

Lemma 5. *For an integer $q \ge 1$ and any quadratic polynomial*

$$G(X) = aX^2 + bX \in \mathbb{Z}[X]$$

with $\gcd(a, q) = 1$

$$\left| \sum_{z=1}^{H} \mathbf{e}(G(z)/q) \right| \ll Hq^{-1/2} + q^{1/2} \log q.$$

One of our main tools is the following very special case of a much more general bound of Wooley [29], that applies to polynomials with arbitrary real coefficients.

Lemma 6. *For any polynomial*

$$G(X) = \sum_{i=1}^{s} \frac{a_i}{q_i} X^i \in \mathbb{Q}[X]$$

of degree $s \ge 3$ with $\gcd(a_i, q_i) = 1$ *and positive integer H, for every $j = 2, \ldots, s$ we have*

$$\left| \sum_{z=1}^{H} \mathbf{e}(G(z)) \right| \ll H \left(q_j^{-1} + H^{-1} + q_j H^{-j} \right)^{\sigma}$$

where

$$\sigma = \frac{1}{2(s-1)(s-2)}.$$

Let $\mathcal{X}_q$ be the set of $\varphi(q)$ multiplicative characters modulo q, where $\varphi(q)$ is the Euler function. We also denote by let $\mathcal{X}_q^* = \mathcal{X}_q \setminus \{\chi_0\}$ the set of nonprincipal characters (we set $\chi(0) = 0$ for all $\chi \in \mathcal{X}_q$). We appeal to [17] for a background on the basic properties of multiplicative characters and exponential functions, such as orthogonality.

We use the following well-know bound that is implied by the Weil bound for mixed sums of additive and multiplicative characters, see [20, Chapter 6, Theorem 3], and a reduction between complete and incomplete sums, see [17, Section 12.2], we also derive the following well-known estimate:

Lemma 7. *For any $\chi \in \mathcal{X}_q$, $\lambda \in \mathbb{F}_p$, nonlinear polynomial $F(X) \in \mathbb{F}_p[X]$ and integers u and $h \ge p$, we have*

$$\sum_{x=u+1}^{u+h} \chi(x) \, \mathbf{e}(\lambda F(x)) \ll p^{1/2} \log p$$

provided that $(\chi, \lambda) \ne (\chi_0, 0)$.

3. Character Sums with Square-free Moduli

For a real $Q \ge 3$ and an integer $r \ge 1$ we denote by $\mathcal{P}_r(Q)$ the set of integers q of the form $q = p_1 \ldots p_r$ where $p_1, \ldots p_r \in [Q, 2Q]$ are pairwise distinct primes with

$$\gcd(k_1 \ldots k_n, p_j - 1) = 1, \qquad j = 1, \ldots, r. \tag{6}$$

Here we obtain a new bound of mixed character sums with multiplicative characters modulo $q \in \mathcal{P}_r(Q)$ which can be of independent interest. We note that recently several bounds of such sums have been obtained for prime $q = p$, see [9, 16]. However for our applications moduli $q \in \mathcal{P}_r(Q)$ are more suitable. Our result is based on the bound of [17, Theorem 12.10] and in fact can be considered as its generalisation.

As in Section 2, we use $\mathcal{X}_q$ for the set of $\varphi(q) = (p_1 - 1) \ldots (p_r - 1)$ multiplicative characters modulo $q = p_1 \ldots p_r \in \mathcal{P}_r(Q)$ and also let $\mathcal{X}_q^* = \mathcal{X}_q \setminus \{\chi_0\}$. Furthermore, we also continue to use $\mathbf{e}(z) = \exp(2\pi i z)$.

We start with recalling the bound of [17, Theorem 12.10], which we present in a somewhat simplified form adjusted to our applications. In particular, some simplifications come from the fact that the modulus $q \in \mathcal{P}_s(Q)$ is square-free.

Lemma 8. *Let $q = \ell_1 \ldots \ell_s \in \mathcal{P}_s(Q)$ for some primes $\ell_1, \ldots, \ell_s$ and let $\psi = \chi_1 \ldots \chi_s$ be a n multiplicative character of conductor q and of order t, where χ_j are arbitrary multiplicative characters of modulo ℓ_j, $j = 1, \ldots, s-1$, and χ_s is a nontrivial multiplicative character modulo ℓ_s. Assume $f(X)$ is a rational function that can be written as*

$$f(X) = \prod_{i=1}^{m} (X - v_i)^{d_i}$$

with some arbitrary integers $v_1, \ldots, v_m$ and nonzero integer $d_1, \ldots, d_m$ with

$$\gcd(d_1, \ldots, d_m, t) = 1,$$

for any integers u and h with $h \ge (2Q)^{9/4}$, we have

$$\left| \sum_{x=u+1}^{u+h} \psi(f(x)) \right| \le 4h \left(\gcd(\Delta, \ell_s) \ell_s^{-1} \right)^{2^{-s}},$$

where

$$\Delta = \prod_{m \ge i > j \ge 1} (v_i - v_j).$$

We are now ready to present one of our main technical results which can be of independent interest.

Lemma 9. *For any $r = 1, 2, \ldots$, a sufficiently large $Q \geq 1$, a modulus $q \in \mathcal{P}_r(Q)$, a polynomial $F(X) \in \mathbb{R}[X]$ of degree d and integers u and h with $h \geq (2Q)^{9/4}$, we have*

$$\max_{\chi \in \mathcal{X}_q^*} \left| \sum_{x=u+1}^{u+h} \chi(x)\, \mathbf{e}(F(x)) \right| \ll hQ^{-\gamma}$$

where

$$\gamma = \frac{1}{2^{r+1}(d+1)(d+2)}.$$

Proof. Let us fix some $\chi \in \mathcal{X}_q^*$. Without loss of generality we can write $\chi = \chi_1 \ldots \chi_r$, where χ_j is a multiplicative character modulo a prime p_j, $j = 1, \ldots, r$ and χ_r is a nonprincipal character (as before, we write $q = p_1 \ldots p_r$ for r distinct primes).

Set $p = p_1$. Then for any positive integer M for the sum

$$S = \sum_{x=u+1}^{u+h} \chi(x)\, \mathbf{e}(F(x))$$

we have

$$\begin{aligned} S &\leq \frac{1}{M} \left| \sum_{x=u+1}^{u+h} \sum_{y=0}^{M-1} \chi(x+py)\, \mathbf{e}(F(x+py)) \right| + 2Mp \\ &\leq \frac{1}{M} \sum_{\substack{x=u+1 \\ \gcd(x,p)=1}}^{u+h} \left| \sum_{y=0}^{M-1} \psi(x+py)\, \mathbf{e}(F(x+py)) \right| + 4MQ, \end{aligned}$$

where $\psi = \chi_2 \ldots \chi_r$. We note that ψ is of conductor q/p rather that q, so this explains the condition $\gcd(x,p) = 1$ in the sum over x. We can however not simply discard this condition and write

$$S \leq \frac{1}{M} \sum_{x=u+1}^{u+h} \left| \sum_{y=0}^{M-1} \psi(x+py)\, \mathbf{e}(F(x+py)) \right| + 4MQ. \tag{7}$$

We divide the unit cube $[0,1]^{d+1}$ into

$$K = M^{(d+1)(d+2)/2}$$

cells of the form

$$\mathcal{U}_{\mathbf{a}} = \left[\frac{a_0}{M}, \frac{a_0+1}{M}\right] \times \ldots \times \left[\frac{a_d}{M^{d+1}}, \frac{a_d+1}{M^{d+1}}\right],$$

where $\mathbf{a} = (a_0, \ldots, a_{d+1}) \in \mathbb{Z}^{d+1}$ runs through the set $\mathcal{A}$ of integer vectors with components $a_\nu = 0, \ldots, M^{\nu+1} - 1$, $\nu = 0, \ldots, d+1$.

We now write

$$F(X + pY) = F_0(X) + F_1(X)Y + \ldots + F_d(X)Y^d$$

and define

$$\Omega_{\mathbf{a}} = \{x \in \{u+1, \ldots, u+h\} \ : \ (F_0(x), \ldots, F_d(x)) \in \mathcal{U}_{\mathbf{a}}\}, \quad \mathbf{a} \in \mathcal{A}.$$

It is easy to see that for $x \in \Omega_{\mathbf{a}}$ we have

$$\mathbf{e}(F(x + py)) = E_{\mathbf{a}}(y) + O(M^{-1}),$$

where

$$E_{\mathbf{a}}(y) = \mathbf{e}\left(\frac{a_0}{M} + \frac{a_1}{M^2} y + \ldots + \frac{a_d}{M^{d+1}} y^d\right).$$

Hence we see from (7) that

$$S \ll \frac{1}{M} W + h/M + QM, \tag{8}$$

where

$$W = \sum_{\mathbf{a} \in \mathcal{A}} \sum_{x \in \Omega_{\mathbf{a}}} \left| \sum_{y=0}^{M-1} \psi(x + py) E_{\mathbf{a}}(y) \right|.$$

We now fix some integer $k \geq 1$ and apply the Hölder inequality to W^{2k}, getting

$$\begin{aligned} W^{2k} &\leq \left(\sum_{\mathbf{a} \in \mathcal{A}} \sum_{x \in \Omega_{\mathbf{a}}} 1 \right)^{2k-1} \sum_{\mathbf{a} \in \mathcal{A}} \sum_{x \in \Omega_{\mathbf{a}}} \left| \sum_{y=0}^{M-1} \psi(x + py) E_{\mathbf{a}}(y) \right|^{2k} \\ &= h^{2k-1} \sum_{\mathbf{a} \in \mathcal{A}} \sum_{x \in \Omega_{\mathbf{a}}} \left| \sum_{y=0}^{M-1} \psi(x + py) E_{\mathbf{a}}(y) \right|^{2k}. \end{aligned}$$

Next, we extend the inner summation over the integers $x \in \Omega_{\mathbf{a}}$ to all $x \in \{u+1, \ldots, u+h\}$. Opening up the $2k$th power, changing the order of summations and using that $|E_{\mathbf{a}}(y)| = 1$, we derive

$$\begin{aligned} W^{2k} &\leq h^{2k-1} \sum_{\mathbf{a} \in \mathcal{A}} \sum_{y_1, \ldots, y_{2k} = 0}^{M-1} \left| \sum_{x=u+1}^{u+h} \psi\left(\prod_{\nu=1}^{k} \frac{x + py_\nu}{x + py_{k+\nu}} \right) \right| \\ &= h^{2k-1} K \sum_{y_1, \ldots, y_{2k} = 0}^{M-1} \left| \sum_{x=u+1}^{u+h} \psi\left(\prod_{\nu=1}^{k} \frac{x + py_\nu}{x + py_{k+\nu}} \right) \right|. \end{aligned}$$

Now, for $O(M^k)$ vectors $(y_1, \ldots, y_{2k})$ where each value appears at least twice we estimate the inner sum trivially as h.

For the remaining $O(M^{2k})$ vectors $(y_1, \dots, y_{2k})$ we apply Lemma 8. More precisely, we use it for $s = r-1$ with $\ell_i = p_{i+1}$. The rational function $f(X)$ after making all cancellation and combining equal terms becomes of the form

$$f(X) = \prod_{i=1}^{m} (x + pz_i)^{d_i},$$

where $1 \le z_1 < \ldots < z_m \le M$ and at least one $d_i = \pm 1$. We now assume that

$$M < Q. \tag{9}$$

Then we have $\gcd(z_i - z_j, p_r) = 1$ for $m \ge i > j \ge 1$. Hence, we also see that

$$\gcd\left(\prod_{m \ge i > j \ge 1} (pz_i - pz_j), p_r\right) = \gcd\left(\prod_{m \ge i > j \ge 1} (z_i - z_j), p_r\right) = 1.$$

With the above simplifications, the bound of Lemma 8 becomes

$$\left|\sum_{x=u+1}^{u+h} \psi\left(\prod_{\nu=1}^{k} \frac{x + py_\nu}{x + py_{k+\nu}}\right)\right| \le 4hQ^{2^{-r+1}}.$$

Therefore,

$$\begin{aligned} W^{2k} &\ll h^{2k-1} K \left(M^k h + M^{2k} h Q^{2^{-r+1}}\right) \\ &= h^{2k} M^{(d+1)(d+2)/2} \left(M^k + M^{2k} Q^{2^{-r+1}}\right), \end{aligned}$$

which after the substitution in (8) implies

$$\begin{aligned} S &\ll hM^{(d+1)(d+2)/4k} \left(M^{-1/2} + Q^{2^{-r}/k}\right) + h/M + QM \\ &\ll hM^{(d+1)(d+2)/4k} \left(M^{-1/2} + Q^{2^{-r}/k}\right) + h^{8/9} \end{aligned}$$

(since by (9) we have $QM \le Q^2 \ll h^{8/9}$, provided that $h \ge (2Q)^{9/4}$). We now choose $M = \left\lceil Q^{2^{-r+1}/k} \right\rceil$, so (9) holds, getting

$$S \ll hM^{(d+1)(d+2)/4k} Q^{2^{-r}/k} + h^{8/9} = hQ^{((d+1)(d+2)/2k-1)2^{-r}/k} + h^{8/9}.$$

Choosing $k = (d+1)(d+2)$ we conclude the proof. □

We remark, that the idea of the proof also works with a simpler shift $F(x) \to F(x+y)$, however using the shift $F(x) \to F(x+py)$ allows to reduce the conductor (from q to q/p) and thus leads to a slightly stronger bound as the conductor of ψ is now a product of only $r-1$

primes. This idea can be used in more generality leading to stronger bounds for more limited ranges of parameters.

We note that we do not impose any conditions on the polynomial F in Lemma 9, which, in particular can be a constant polynomial, in which case, we have the bound of of [17, Theorem 12.10].

4. Character Sums with Prime-power Moduli

Let $q = p^r$ where $r \ge 1$ is an integer and $p \ge 3$ is a prime with

$$\gcd(k_1 \dots k_n, p-1) = 1. \tag{10}$$

As in Section 2, we use $\mathcal{X}_q$ for the set of $\varphi(q) = p^{r-1}(p-1)$ multiplicative characters modulo q and let $\mathcal{X}_q^* = \mathcal{X}_q \setminus \{\chi_0\}$. We also continue to use $\mathbf{e}(z) = \exp(2\pi i z)$.

Since group of units modulo q is cyclic then so is $\mathcal{X}_q$. So we now fix a character $\chi \in \mathcal{X}_q$ that generates this group, so that

$$\mathcal{X} = \{\chi^\mu \ : \ \mu = 0, \dots, p^{r-1}(p-1) - 1\}.$$

The following result is due to Postnikov [23, 24], see also [17, Equation (12.89)].

Lemma 10. *Assume that $q = p^r$ for ana integer $r \ge 1$ and a prime $p > \max\{2, r\}$. Then for any integers y and z with $\gcd(y, p) = 1$, we have*

$$\chi(y + pz) = \chi(y)\, \mathbf{e}\left(F(pwz)/q\right)$$

for some polynomial

$$F(Z) = \sum_{k=1}^{r-1} A_k Z^k \in \mathbb{Z}[Z]$$

of degree $r-1$ and the coefficients satisfying $\gcd(A_k, p) = 1$, $k = 1, \dots, r-1$, where w is defined by

$$wy \equiv 1 \pmod q \qquad \text{and} \qquad 1 \le w < q.$$

Lemma 11. *Assume that $q = p^r$ for an integer $r \ge 1$ and a prime $p > \max\{2, r\}$. Then for a polynomial $f(X) \in \mathbb{Z}[X]$ of degree $d \ge r$ with the leading coefficient a_d satisfying $\gcd(a_d, p) = 1$ and integers u and h with $q \ge h \ge p^3$, uniformly over the integers*

$$\lambda \in \{0, \dots, p^r - 1\} \qquad \text{and} \qquad \mu \in \{0, \dots, (p-1)p^{r-1} - 1\}$$

with $\lambda + \mu > 0$, we have

$$\left| \sum_{x=u+1}^{u+h} \chi^\mu(x)\, \mathbf{e}(\lambda f(x)/q) \right| \ll h^{1-1/4r^2}.$$

Proof. Let $H = \lfloor h/p \rfloor$. Then

$$\sum_{x=u+1}^{u+h} \chi^{\mu}(x)\,\mathbf{e}(\lambda f(x)/q) = S + O(H), \tag{11}$$

where

$$S = \sum_{y=u+1}^{u+p} \sum_{z=0}^{H} \chi^{\mu}(y+pz)\,\mathbf{e}(\lambda f(y+pz)/q).$$

Therefore, using Lemma 10 we obtain

$$\begin{split} S = \sum_{\substack{y=u+1\\ \gcd(y,p)=1}}^{u+p} \chi^{\mu}(y)\,\mathbf{e}\left(\lambda f(y)/p^r\right) \\ \sum_{z=0}^{H} \mathbf{e}\left(\sum_{k=1}^{r-1} \frac{1}{p^{r-k}} \left(\mu A_k y^{-k} - \lambda f^{(k)}(y)/k!\right) z^k\right). \end{split} \tag{12}$$

Let $\mathrm{ord}_p\, t$ denote the p-adic order of an integer t (where we formally set $\mathrm{ord}_p\, 0 = \infty$). We set $m = \min\{\mathrm{ord}_p\, \lambda, \mathrm{ord}_p\, \mu\}$.

In particular, for the inner sum over z in (12) we have

$$\begin{split} \sum_{z=0}^{H} \mathbf{e}\left(\sum_{k=1}^{r-1} \frac{1}{p^{r-k}} \left(\mu A_k y^{-k} - \lambda f^{(k)}(y)/k!\right) z^k\right) \\ = \sum_{z=0}^{H} \mathbf{e}\left(\sum_{k=1}^{r-m-1} \frac{1}{p^{r-m-k}} \left(\mu^* A_k y^{-k} - \lambda^* f^{(k)}(y)/k!\right) z^k\right), \end{split} \tag{13}$$

where $\mu^* = \mu/p^m$ and $\lambda^* = \lambda/p^m$ are integers.

We now consider three different cases.

If $m = r-1$ then we see from (13) that the inner sum over z in (12) is trivial. Note that if $p^{r-1} \mid \mu$ then $\chi^{\mu}(y)$ becomes a character modulo p, and it is either a nontrivial character modulo p or $\gcd(\lambda^*, p) = 1)$.

Thus, using Lemma 7, we derive for the sum S

$$\begin{split} S = H \sum_{\substack{y=u+1\\ \gcd(y,p)=1}}^{u+p} \chi^{\mu}(y)\,\mathbf{e}\left(\lambda^* f(y)/p\right) \ll H p^{1/2} \log p \\ \ll h p^{-1/2} \log h \ll h^{1-1/2r} \log h, \end{split} \tag{14}$$

If $r-3 \le m \le r-2$ then we see that the sum (13) is a sum with either linear or quadratic polynomial in z. Let $\mathcal{Y}$ be the set of solutions the congruence

$$\mu^* A_{r-m-1} y^{-r+m+1} - \lambda^* f^{(r-m-1)}(y)/(r-m-1)! \equiv 0 \pmod p$$

where

$$y = u+1, \ldots, u+p, \qquad \gcd(y,p) = 1.$$

Recalling that $\gcd(A_{r-m-1}, p) = 1$ and the condition on the leading coefficient of f, we see that $\#\mathcal{Y} \le d$. Now, for $y \notin \mathcal{Y}$, the sum (13) is

- either a sum with a linear polynomial and a denominator p (when $m = r-2$);
- or a sum with a quadratic polynomial and a denominator p^2 (when $m = r-3$).

Moreover, these polynomials have the leading coefficient which is relatively prime to p. In the case of linear polynomial (that is, $m = r-2$), by Lemma 4 we bound this sum as $O(p)$. In the case of a quadratic polynomial (that is, $m = r-3$), we bound this sums as $O\left(Hp^{-1} + p\log p\right)$, which dominates the previous bound. Thus, estimating the sum (13) trivially as H for $y \in \mathcal{Y}$, we derive

$$\begin{aligned} S &\ll H + p\left(Hp^{-1} + p\log p\right) \ll H + p^2 \log p \\ &\ll h/p + h^{2/3}\log h \ll h^{1-1/r}\log h. \end{aligned} \tag{15}$$

Finally, assume that $m \le r-4$. For

$$j = \left\lceil \frac{r-m}{2} \right\rceil \ge 2,$$

let $\mathcal{Y}$ be the set of solutions to the congruence

$$\mu^* A_j y^{-j} - \lambda^* f^{(j)}(y)/j! \equiv 0 \pmod p,$$

where

$$y = u+1, \ldots, u+p, \qquad \gcd(y,p) = 1.$$

Recalling that $\gcd(A_j, p) = 1$ and the condition on the leading coefficient of f we see that $\#\mathcal{Y} \le d$. Furthermore, for $y \notin \mathcal{Y}$, we estimate the inner sum over z by Lemma 6 with $s = r-m-1 \ge 3$ and $q_j = p^{r-m-j}$, getting for the sum (13):

$$\begin{aligned} \sum_{z=0}^{H} \mathbf{e}\left(\sum_{k=1}^{r-m-1} \frac{1}{p^{r-m-k}} \left(\mu^* A_k y^{-k} - \lambda^* f^{(k)}(y)/k!\right) z^k\right) \\ \ll H(p^{-r+m+j} + H^{-1} + p^{r-m-j}H^{-j})^{\sigma}, \end{aligned} \tag{16}$$

where

$$\sigma = \frac{1}{2(r-m-2)(r-m-3)}.$$

Since $H \ge p^2$ and $j \ge (r-m)/2$ we have

$$p^{r-m-j}H^{-j} \le p^{r-m-3j} \le p^{-(r-m)/2}.$$

On the other hand, since $j \le (r-m+1)/2$, we also have

$$p^{-r+m+j} \le p^{-(r-m-1)/2}.$$

Therefore, the bound (16) implies that

$$\sum_{z=0}^{H} \mathbf{e}\left(\sum_{k=1}^{r-m-1} \frac{1}{p^{r-m-k}} \left(\mu^* A_k y^{-k} - \lambda^* f^{(k)}(y)/k!\right) z^k\right) \ll H(p^{-(r-m-1)/2} + H^{-1})^{\sigma}. \tag{17}$$

We now note that for $m \le r-4$ we have

$$\frac{r-m-1}{2}\sigma = \frac{r-m-1}{4(r-m-2)(r-m-3)} \ge \frac{1}{4r}.$$

and also

$$\frac{2}{3}\sigma = \frac{1}{3(r-m-2)(r-m-3)} \ge \frac{1}{3r^2}.$$

Since $p \ge h^{1/r}$ and $H \gg h/p \ge h^{2/3}$, we finally obtain

$$\sum_{z=0}^{H} \mathbf{e}\left(\sum_{k=1}^{r-m-1} \frac{1}{p^{r-m-k}} \left(\mu^* A_k y^{-k} - \lambda^* f^{(k)}(y)/k!\right) z^k\right) \ll Hh^{-1/4r^2}. \tag{18}$$

So, estimating the sum (13) trivially for $y \in \mathcal{Y}$ and using (18) for $y \notin \mathcal{Y}$, we derive

$$S \ll H + pHh^{-1/4r^2} \ll h^{1-1/r} + h^{1-1/4r^2} \ll h^{1-1/4r^2} \tag{19}$$

Comparing (14), (15) and (19), we see that the bound (19) dominates, and the result follows. □

5. Multiplicative Congruences and Equations

We also use the following result of Cochrane and Shi [11] which generalises several previous results, which we present in the following slightly less precise form.

Lemma 12. *For arbitrary integers u and $h \le q$, the number of solutions to*

$$wx \equiv yz \pmod q$$

in variables

$$w, x, y, z \in \{u+1, \dots, u+h\} \qquad \text{and} \qquad \gcd(wxyz, q) = 1,$$

is bounded by $h^4 q^{-1+o(1)} + h^{2+o(1)}$.

Note that in Lemma 12 no assumptions on the modulus q is made (although we apply it only for $q \in \mathcal{P}_r(Q)$).

We also need a bound of [8, Proposition 3] on the number of divisors in short intervals.

Lemma 13. *For any integers $h \ge 0$, $u \ge 1$ and $z \ge 1$*

$$\#\{(x_1, \ldots, x_n) \in \mathcal{I}^n \ : \ z = x_1 \ldots x_n\} \le \exp\left(C_n \frac{\log h}{\log \log h}\right)$$

where C_n is some absolute constant depending only on n.

6. Sets in Reduced Residue Classes

We need the following simple statement

Lemma 14. *Let $H \ge 3$ be a real number and let $\mathcal{S}$ be arbitrary set of nonzero integers with $|s| \le H$ for $s \in \mathcal{S}$. For any integer $r \ge 1$ there exists a constant $c(r)$ depending only on r, such that for any sufficiently large real $Q \ge c(r) \log H$, there exists $q \in \mathcal{P}_r(Q)$ with*

$$\#\{s \in \mathcal{S} \ : \ \gcd(s, q) = 1\} \ge \frac{1}{2} \#\mathcal{S}.$$

Proof. We have

$$\begin{aligned} \sum_{q \in \mathcal{P}_r(Q)} & \#\{s \in \mathcal{S} \ : \ \gcd(s, q) > 1\} \\ & \le \sum_{s \in \mathcal{S}} \sum_{\substack{q \in \mathcal{P}_r(Q) \\ \gcd(s,q)>1}} 1 \le r \sum_{s \in \mathcal{S}} \omega(s) \sum_{q \in \mathcal{P}_{r-1}(Q)} 1, \end{aligned}$$

where as usual, $\omega(s)$ denotes the number of prime divisors of $s \neq 0$. We now use that,

$$\omega(s) \ll \frac{\log |s|}{\log(2 + \log |s|)} \ll \frac{\log H}{\log \log H}$$

(since, trivially $\omega(s)! \le s$) and also that by the asymptotic formula for the number of primes in an arithmetic progression, we have

$$\left(\frac{Q}{\log Q}\right)^{\nu} \ll \#\mathcal{P}_\nu(Q) \ll \left(\frac{Q}{\log Q}\right)^{\nu}, \qquad \nu = 1, 2, \ldots.$$

Thus, we derive

$$\sum_{q \in \mathcal{P}_r(Q)} \#\{s \in \mathcal{S} \ : \ \gcd(s, q) > 1\} \ll \#\mathcal{S} \frac{\log H}{\log \log H} \left(\frac{Q}{\log Q}\right)^{r-1}.$$

Therefore,

$$\frac{1}{\#\mathcal{P}_r(Q)} \sum_{q\in\mathcal{P}_r(Q)} \#\{s \in \mathcal{S} \ : \ \gcd(s,q) > 1\} \ll \#\mathcal{S}\frac{\log H}{\log\log H} \cdot \frac{\log Q}{Q}$$

and the result now follows. □

7. Proof of Theorem 1

Take $Q = 0.5h^{4/9}$. By the condition on $\mathfrak{B}$ and Lemma 14 (applied to the set of all coordinates of all $N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B})$ solutions) there exists $q \in \mathcal{P}_r(Q)$ such that we have

$$N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B}) \le 2T, \tag{20}$$

where T is the number of solutions to the congruence

$$f_1(x_1) + \ldots + f_n(x_n) \equiv a x_1^{k_1} \ldots x_n^{k_n} \pmod q \tag{21}$$

with

$$(x_1,\ldots,x_n) \in \mathfrak{B} \qquad \text{and} \qquad \gcd(x_1\ldots x_n, q) = 1.$$

Hence it is now sufficient to estimate T.

As before, we use $\mathcal{X}_q$ to denote the set of multiplicative characters modulo q and also let $\mathcal{X}_q^* = \mathcal{X}_q \setminus \{\chi_0\}$ be the set of nonprincipal characters.

We now proceed as in the proof of [27, Theorem 3.2]. Let

$$S_i(\chi;\lambda) = \sum_{x=u_i+1}^{u_i+h} \chi^{k_i}(x)\,\mathbf{e}\left(\lambda f_i(x)/q\right), \quad i = 1,\ldots,n.$$

We also introduce the Gauss sums

$$G(\chi,\lambda) = \sum_{y=1}^{q} \chi(y)\,\mathbf{e}(\lambda y/q), \qquad \chi \in \mathcal{X}_q,\ \lambda \in \mathbb{Z},$$

Clearly, we can assume that at least one of the polynomials $f_1,\ldots,f_n$ is not a constant polynomial as otherwise the result is immediate.

Without loss of generality, we can now assume that $\deg f_1 \ge 1$. Furthermore, we can also assume that h is sufficiently large so that $\gcd(a,q) = 1$ and also the leading coefficients of the polynomial f_n is relatively prime to q (recall that q is composed out of primes in the interval $[Q, 2Q]$).

We now introduce one more variable y that runs through the reduced residue system modulo q and rewrite (21) as a system of congruences

$$\begin{aligned} &f_1(x_1) + \ldots + f_n(x_n) \equiv y \pmod q,\\ &a x_1^{k_1} \ldots x_n^{k_n} \equiv y \pmod q. \end{aligned}$$

Then exactly as in [27, Equation (3.3)], we write

$$T = \frac{1}{q\varphi(q)} \sum_{\lambda=1}^{q} \sum_{\chi \in \mathcal{X}_q} \overline{G}(\chi, \lambda) \prod_{i=1}^{n} |S_i(\chi, \lambda)|,$$

where, as before, $\varphi(q)$ is the Euler function and $\overline{G}(\chi, \lambda)$ is the complex conjugate of the Gauss sum.

As in the proof of [27, Theorem 3.2], we see that, under the condition (6), we have:

$$T \ll \frac{1}{q\varphi(q)} (R_1 + R_2), \tag{22}$$

where

$$R_1 = \sum_{\lambda=1}^{q} \sum_{\chi \in \mathcal{X}_q^*} |G(\chi, \lambda)| \prod_{i=1}^{n} |S_i(\chi, \lambda)|,$$
$$R_2 = \sum_{\lambda=1}^{q} |G(\chi_0, \lambda)| \prod_{i=1}^{n} |S_i(\chi_0, \lambda)|,$$

To estimate R_1 we first use Lemma 9 for $n-2$ sums and infer that

$$R_1 \ll h^{(1-4\gamma/9)(n-2)} \sum_{\lambda=1}^{q} \sum_{\chi \in \mathcal{X}_q^*} |G(\chi, \lambda)||S_1(\chi; \lambda)||S_2(\chi; \lambda)|, \tag{23}$$

where γ is as in Lemma 9.

Using the Hölder inequality, and then expanding the summation to all $\chi \in \mathcal{X}_q$, we obtain

$$\begin{aligned} &\sum_{\lambda=1}^{q} \sum_{\chi \in \mathcal{X}_q} |G(\chi, \lambda)||S_1(\chi; \lambda)||S_2(\chi; \lambda)| \\ &\qquad \le \sum_{\lambda=1}^{q} \left(\sum_{\chi \in \mathcal{X}_q} |G(\chi, \lambda)|^2 \right)^{1/2} \\ &\qquad\qquad \left(\sum_{\chi \in \mathcal{X}_q} |S_1(\chi; \lambda)|^4 \right)^{1/4} \left(\sum_{\chi \in \mathcal{X}_q} |S_2(\chi; \lambda)|^4 \right)^{1/4}. \end{aligned} \tag{24}$$

Using the orthogonality of multiplicative characters we see that

$$\sum_{\chi\in\mathcal{X}_q} |S_1(\chi;\lambda)|^4 = q \sum_{\substack{w,x,y,z=u_1+1\\ \gcd(wxyz,q)=1\\ wx\equiv yz \pmod q}}^{u_1+h} \mathbf{e}\left(\frac{\lambda}{q}\left(f_1(w)+f_1(x)-f_1(y)-f_1(z)\right)\right) \le qW,$$

where W is the number of solutions to

$$wx \equiv yz \pmod q$$

in variables

$$w,x,y,z \in \{u_1+1,\dots,u_1+h\} \qquad \text{and} \qquad \gcd(wxyz,q)=1.$$

Using Lemma 12, we obtain

$$\sum_{\chi\in\mathcal{X}_q} |S_1(\chi;\lambda)|^4 \le h^4 q^{o(1)} + h^{2+o(1)} q.$$

Similarly we obtain the same inequality for the 4th moment of the sums $S_2(\chi;\lambda)$, and also

$$\sum_{\chi\in\mathcal{X}_q} |G(\chi,\lambda)|^2 \ll q^2.$$

Thus, collecting these bounds together which together with (23) and (24), we derive

$$\begin{aligned} R_1 &\ll h^{(1-4\gamma/9)(n-2)} q^2 \left(h^2 q^{o(1)} + h^{1+o(1)} q^{1/2}\right) \\ &= h^{n-4\gamma(n-2)/9-1}\left(hq^{2+o(1)} + q^{5/2+o(1)}\right). \end{aligned} \tag{25}$$

For R_2, using the trivial bound

$$|S_i(\chi_0;\lambda)| \le h, \qquad i=1,\dots,n-1,$$

we write

$$R_2 \le h^{n-1} \sum_{\lambda=1}^{q} |G(\chi_0;\lambda)||S_1(\chi_0;\lambda)|.$$

We remark that

$$G(\chi_0;\lambda) = \sum_{\substack{y=1\\ \gcd(y,q)=1}}^{q} \mathbf{e}(\lambda y/q)$$

is the *Ramanujan sum* and thus for a square-free q we obtain

$$|G(\chi_0;\lambda)| = \varphi(\gcd(\lambda,q))$$

see [17, Section 3.2]. Collecting together the values of λ with the same $\gcd(\lambda, q) = q/s$, where s runs over all 2^r divisors of q, and then using the Cauchy inequality, we obtain

$$\begin{aligned} R_2 &\le h^{n-1} q \sum_{s|q} \frac{1}{s} \sum_{\mu=1}^{s} |S_1(\chi_0; \mu q/s)| \\ &\le h^{n-1} q \sum_{s|q} \frac{1}{s} \sum_{\mu=1}^{s} \left| \sum_{\substack{x=u_1+1 \\ \gcd(x,q)=1}}^{u_1+h} \mathbf{e}\left(\mu f_1(x)/s\right) \right| \\ &\le h^{n-1} q \sum_{s|q} \frac{1}{s^{1/2}} \left(\sum_{\mu=1}^{s} \left| \sum_{\substack{x=u_1+1 \\ \gcd(x,q)=1}}^{u_1+h} \mathbf{e}\left(\mu f_1(x)/s\right) \right|^2 \right)^{1/2} . \end{aligned}$$

By the orthogonality of exponential functions,

$$\sum_{\mu=1}^{s} \left| \sum_{\substack{x=u_1+1 \\ \gcd(x,q)=1}}^{u_1+h} \mathbf{e}\left(\mu f_1(x)/s\right) \right|^2 \le s U_s.$$

Where U_s is the number of solutions to the congruence

$$f_1(x) \equiv f_1(y) \pmod s, \qquad x, y \in \{u_1 + 1, \ldots, u_1 + h\}.$$

Since the leading coefficient of $f_1(X)$ is relatively prime to q, using the Chinese Remainder Theorem we obtain

$$U_s \ll h^2/s + h.$$

Collecting the above inequalities, yields the bound

$$R_2 \ll h^{n-1} q \sum_{s|q} \frac{1}{s^{1/2}} \left(h^2 + hs\right)^{1/2} \le h^n q. \tag{26}$$

Substituting the bounds (25) and (26) in (22) and using that $\varphi(q) \gg q$ for $q \in \mathcal{P}_r(Q)$ and also that $q \gg h^{4r/9}$ we obtain

$$\begin{aligned} T &\ll h^{n-4\gamma(n-2)/9-1} \left(h + q^{1/2}\right) q^{o(1)} + h^n q^{-1} \\ &\ll \left(h^{n-4\gamma(n-2)/9} + h^{n-4\gamma(n-2)/9-1+2r/9}\right) q^{o(1)} + h^{n-4r/9}. \end{aligned} \tag{27}$$

Clearly, if

$$-4\gamma(n-2)/9 < -4r/9 \qquad \text{and} \qquad -4\gamma(n-2)/9 - 1 < -2r/3$$

or, equivalently

$$n > \max\left\{2^{r+1}(d+1)(d+2)r, 2^{r+1}(d+1)(d+2)(3r/2-9/4)\right\}+2,$$

then the last term dominates in (27). Using (20) we conclude the proof.

8. Proof of Theorem 2

Take $Q = \lfloor 0.5h^{1/3} \rfloor$. By the condition on $\mathfrak{B}$ and Lemma 14 (applied to the set of all coordinates of all $N^*_{a,\mathbf{f},\mathbf{k}}(\mathfrak{B})$ solutions and the set $\mathcal{P}_1(Q)$) there exists a prime $p \in [Q, 2Q]$ such that we have the bound (20) where now T is the number of solutions to the congruence

$$f_1(x_1) + \ldots + f_n(x_n) \equiv a x_1^{k_1} \ldots x_n^{k_n} \pmod{p^r} \tag{28}$$

with

$$(x_1, \ldots, x_n) \in \mathfrak{B} \qquad \text{and} \qquad \gcd(x_1 \ldots x_n, p) = 1.$$

Hence it is now sufficient to estimate T.

As before, we use $\mathcal{X}_{p^r}$ to denote the set of multiplicative characters modulo p^r and also let $\mathcal{X}^*_{p^r} = \mathcal{X}_{p^r} \setminus \{\chi_0\}$ be the set of nonprincipal characters.

We now proceed as in the proof of [27, Theorem 3.2]. Let

$$S_i(\chi;\lambda) = \sum_{x=u_i+1}^{u_i+h} \chi^{k_i}(x)\, \mathbf{e}\left(\lambda f_i(x)/p^r\right), \quad i = 1, \ldots, n.$$

We also introduce the Gauss sums

$$G(\chi,\lambda) = \sum_{y=1}^{p^r} \chi(y)\, \mathbf{e}(\lambda y/p^r), \qquad \chi \in \mathcal{X}_p^r,\ \lambda \in \mathbb{Z},$$

Clearly, we can assume that at least one of the polynomials $f_1, \ldots, f_n$ is not a constant polynomial as otherwise the result is immediate.

Without loss of generality, we can now assume that $\deg f_1 \geq 1$. Furthermore, we can also assume that h is sufficiently large so that $\gcd(a,p) = 1$ and also the leading coefficients of the polynomial f_n is relatively prime to p (recall that $p \in [Q, 2Q]$).

We now introduce one more variable y that runs through the reduced residue system modulo q and rewrite (28) as a system of congruences

$$\begin{aligned} &f_1(x_1) + \ldots + f_n(x_n) \equiv y \pmod{p^r}, \\ &a x_1^{k_1} \ldots x_n^{k_n} \equiv y \pmod{p^r}. \end{aligned}$$

Then exactly as in [27, Equation (3.3)], we write

$$T = \frac{1}{p^r \varphi(p^r)} \sum_{\lambda=1}^{p^r} \sum_{\chi \in \mathcal{X}_{p^r}} \overline{G}(\chi,\lambda) \prod_{i=1}^{n} |S_i(\chi,\lambda)|,$$

where, as before, $\varphi(q)$ is the Euler function and $\overline{G}(\chi,\lambda)$ is the complex conjugate of the Gauss sum.

We see that the contribution from the term corresponding to $\lambda = p^r$ and the principal character $\chi = \chi_0$ is $O(h^n/p^r)$. so the under the condition (10), we have:

$$T \ll h^n/p^r + \frac{1}{p^r\varphi(p^r)} R \tag{29}$$

where

$$R = \sum_{\substack{1\le\lambda\le p^r,\ \chi\in\mathcal{X}_{p^r}\\ (\lambda,\chi)\ne(p^r,\chi_0)}}\sum |G(\chi,\lambda)| \prod_{i=1}^{n} |S_i(\chi,\lambda)|$$

To estimate R we first use Lemma 11 for $n-2$ sums and infer that

$$R \ll h^{(1-1/4r^2)(n-2)} \sum_{\lambda=1}^{q} \sum_{\chi\in\mathcal{X}_q^*} |G(\chi,\lambda)||S_1(\chi;\lambda)||S_2(\chi;\lambda)|.$$

We now proceed exactly as in estimating R_1 in the proof of Theorem 1, getting instead of (25) the bound

$$R \ll h^{(1-1/4r^2)(n-2)} p^{2r} \left(h^2 p^{o(1)} + h^{1+o(1)} p^{r/2}\right).$$

Since $h^{1/3} \gg p \gg h^{1/3}$ and $r \ge 6$, this simplifies as

$$R \ll h^{(1-1/4r^2)(n-2)+1+o(1)} p^{5r/2} \tag{30}$$

Substituting the bound (30) in (29), we obtain

$$\begin{aligned} T &\ll h^{n-1-(n-2)/4r^2+o(1)} p^{r/2} + h^n/p^r \\ &\ll h^{n-1-(n-2)/4r^2+r/6+o(1)} + h^{n-r/3}. \end{aligned} \tag{31}$$

Clearly, if

$$r^3 \le \frac{n-2}{2}$$

or, equivalently

$$n \ge 2r^3 + 2$$

then the last term dominates in (31). Using (20) we conclude the proof.

9. Proof of Theorem 3

Clearly for $(x_1,\ldots,x_n) \in \mathfrak{B}$ where $\mathfrak{B}$ is of the form (5) we have

$$x_1^d + \ldots + x_n^d \in \mathcal{Z},$$

where

$$\mathcal{Z} = \left\{ \sum_{\nu=0}^{d} \binom{d}{\nu} z_\nu u^{d-\nu} \ :\ z_\nu \in [0, nh^\nu],\ \nu = 0,\ldots,d \right\}.$$

In particular, $\#\mathcal{Z} \ll h^{d(d+1)/2}$. Applying Lemma 13 to every $z \in \mathcal{Z}$, we obtain the result.

10. Comments

We remark that Theorem 1 applies to the Markoff-Hurwitz hypersurface corresponding to (3). in which case the condition on n becomes

$$n > 12 \cdot 2^r \max\{2r, 3r - 9/2\} + 2.$$

We note that the condition of Theorem 1 requires n to be only quadratic in d, while the saving grows with n as

$$\frac{4 \log n}{9 \log 2} > 0.64 \log n,$$

when d is fixed and n tends to infinity.

On the other hand, Theorem 1 does not apply to the Dwork hypersurface, but Theorem 2 and leads to the saving that grows with n as

$$\frac{(n/2)^{1/3}}{3} > 0.26 n^{1/3}.$$

It is also easy to see that our methods also works for a more general form of (2), namely for the equation

$$(f_1(x_1) + \ldots + f_n(x_n))^m = a x_1^{k_1} \ldots x_n^{k_n}$$

with a nonzero integer m.

One can easily remove the condition on the parity of $k_1, \ldots, k_n$ at the cost of essentially only typographical changes. Indeed, if some of $k_1, \ldots, k_n$ are even that we take all our primes p to satisfy

$$p \equiv 3 \pmod{2k_1 \ldots k_n}$$

instead of (6) and (10), and then we deal with contribution from characters or order 2 as we have done for the principal character.

Finally, we note that using the bounds of mixed sums from [16] within our method leads to weaker estimates, but makes them fully uniform with respect to the box $\mathfrak{B}$. That is, the conditions on $\max_{i=1,\ldots,n} |u_i|$ in Theorems 1 and 2 can be removed at the cost of weakening the final bound.

Acknowledgment

The authors are grateful to Oscar Marmon for many useful comments. The authors also would like to thank Roger Heath-Brown and Lillian Pierce for informing them about their work [16] when it was still in progress and then sending them a preliminary draft.

During the preparation of this paper, the first author was supported by the NSF Grant DMS 1301608 and the second author by the ARC Grant DP130100237. The second author would also to thank CIRM, Luminy, for support and hospitality during his work on this project.

References

[1] A. Baragar, 'Asymptotic growth of Markoff-Hurwitz numbers', *Compositio Math.* , **94** (1994), 1–18.

[2] A. Baragar, 'The exponent for the Markoff-Hurwitz equations', *Pacific J. Math.*, **182** (1998), 1–21.

[3] A. Baragar, 'The Markoff-Hurwitz equations over number fields', *Rocky Mountain J. Math.*, **35** (2005), 695–712.

[4] B. J. Birch, 'Forms in many variables', *Proc. Roy. Soc. Ser. A*, **265** (1961), 245–263.

[5] T. D. Browning, *Quantitative arithmetic of projective varieties*, Progress in Mathem., vol. 277. Birkhäuser Verlag, Basel, 2009.

[6] T. D. Browning, R. Heath-Brown and P. Salberger, 'Counting rational points on algebraic varieties', *Duke Math. J.*, **132** (2006), 545–578.

[7] W. Cao, 'On generalized Markoff-Hurwitz-type equations over finite fields', *Acta Appl. Math.*, **112** (2010), 275–281.

[8] M.-C. Chang, 'Factorization in generalized arithmetic progressions and applications to the Erdős-Szemerédi sum-product problems', *Geom. Funct. Anal.*, **13** (2003), 720–736.

[9] M.-C. Chang, 'An estimate of incomplete mixed character sums', *An Irregular Mind*, Bolyai Society Math. Studies, vol. 21, Springer, Berlin, 2010, 243–250.

[10] M.-C. Chang, 'Short character sums for composite moduli', *J. d'Analyse Math.*, (to appear).

[11] T. Cochrane and S. Shi, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod m$ and mean values of character sums', *J. Number Theory*, **130** (2010), 767–785.

[12] P. Goutet, 'An explicit factorisation of the zeta functions of Dwork hypersurfaces', *Acta Arith.*, **144** (2010), 241–261.

[13] M. Harris, N. Shepherd-Barron and R. Taylor, 'A family of Calabi–Yau varieties and potential automorphy', *Annals Math.*, **171** (2010), 779–813.

[14] D. R. Heath-Brown, 'The density of rational points on nonsingular hypersurfaces', *Proc. Indian Acad. Sci. Math. Sci.*, **104** (1994), 13–29.

[15] D. R. Heath-Brown and L. Pierce, 'Counting rational points on smooth cyclic covers', *J. Number Theory*, **132** (2012), 1741–1757.

[16] D. R. Heath-Brown and L. Pierce, 'Burgess bounds for short mixed character sums', *Preprint*, 2014, (available from `http://arxiv.org/abs/1404.1677`).

[17] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[18] N. M. Katz, 'Another look at the Dwork family', *Algebra, Arithmetic, and Geometry: In honor of Yu. I. Manin.*. Vol. II, Progr. Math., 270, Birkhäuser Boston, Inc., Boston, MA, 2009, 89–126,

[19] R. Kloosterman, 'The zeta function of monomial deformations of Fermat hypersurfaces', *Algebra Number Theory*, **1** (2007), 421–450.

[20] W.-C. W. Li, *Number theory with applications*, World Scientific, Singapore, 1996.

[21] O. Marmon, 'The density of integral points on complete intersections', *Q. J. Math.*, **59** (2008), 29–53.

[22] O. Marmon, 'The density of integral points on hypersurfaces of degree at least four', *Acta Arith.*, **141** (2010), 211–240.

[23] A. G. Postnikov, 'On the sum of characters with respect to a modulus equal to a power of a prime number', *Izv. Akad. Nauk SSSR. Ser. Mat.*, **19** (1955), 11–16 (in Russian).

[24] A. G. Postnikov, 'On Dirichlet L-series with the character modulus equal to the power of a prime number', *J. Indian Math. Soc.*, **20** (1956), 217–226.

[25] P. Salberger, 'On the density of rational and integral points on algebraic varieties', *J. Reine Angew. Math.*, **606** (2007), 123–147.

[26] P. Salberger, 'Counting rational points on projective varieties', *Preprint*, 2013.

[27] I. E. Shparlinski, 'On the distribution of points on the generalised Markoff-Hurwitz and Dwork hypersurfaces', *Intern. J. Number Theory*, **10** (2014), 151–160.

[28] Y. Tschinkel, 'Algebraic varieties with many rational points', *Arithmetic Geometry*, Clay Math. Proc., vol. 8, Amer. Math. Soc., Providence, RI, 2009, 243–334.

[29] T. D. Wooley, 'Translation invariance, exponential sums, and Warings problem', *Preprint*, 2014, (available from `http://arxiv.org/abs/1404.3508`).

[30] Y.-D. Yu, 'Variation of the unit root along the Dwork family of Calabi–Yau varieties', *Math. Ann.*, **343** (2009), 53–78.

Department of Mathematics, University of California, Riverside, CA 92521, USA

E-mail address: `mcc@math.ucr.edu`

Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia

E-mail address: `igor.shparlinski@unsw.edu.au`