Canad. J. Math. Vol. **66** (4), 2014 pp. 844–873
http://dx.doi.org/10.4153/CJM-2013-014-9

Multidimensional Vinogradov-type Estimates in Function Fields

Wentang Kuo, Yu-Ru Liu, and Xiaomei Zhao

Abstract. Let $\mathbb{F}_q[t]$ denote the polynomial ring over the finite field $\mathbb{F}_q$. We employ Wooley's new efficient congruencing method to prove certain multidimensional Vinogradov-type estimates in $\mathbb{F}_q[t]$. These results allow us to apply a variant of the circle method to obtain asymptotic formulas for a system connected to the problem about linear spaces lying on hypersurfaces defined over $\mathbb{F}_q[t]$.

1 Introduction

One central problem in number theory is concerned with integral points lying on hypersurfaces. In particular, for $s, k \in \mathbb{N} = \{0, 1, 2, \dots\}$ with $k \geq 2$ and $\mathbf{a} = (a_1, \dots, a_s) \in (\mathbb{Z} \setminus \{0\})^s$, we could ask how large s should be (in terms of k and independent of $\mathbf{a}$) so that the hypersurface

$$a_1 w_1^k + \cdots + a_s w_s^k = 0 \tag{1.1}$$

contains a non-trivial integral point. Additionally, establishing an asymptotic formula for the number of such points has become a substantial research area. For $P \in \mathbb{N}$, let $M_{s,k,\mathbf{a}}(P)$ denote the number of solutions of (1.1) with

$$w_j \in [-P, P] \cap \mathbb{Z}, \quad 1 \leq j \leq s.$$

A celebrated result of Wooley [10] states that, subject to a local solubility hypothesis, whenever $s \geq k \log k + O(k \log\log k)$, we have $M_{s,k,\mathbf{a}}(P) \gg P^{s-k}$. His recent groundbreaking work [12] can also be used to show that whenever $s \geq 2k^2 + 2k - 3$, we can establish an asymptotic formula for $M_{s,k,\mathbf{a}}(P)$. In [13], Wooley further improved his result and showed that if $k \geq 6$, it suffices to take $s \geq 2k^2 - 2k - 8$. In this case, no local solubility hypothesis is required (except for indefiniteness), since the result of Davenport and Lewis in [3] shows that $k^2 + 1$ variables suffice to satisfy the congruence conditions.

Because of the homogeneity of (1.1), if a non-trivial integral point lies on (1.1), then the hypersurface contains the line through the origin and that point. Thus, the above problem can be viewed as a question about linear spaces of dimension 1. It is

Received by the editors October 23, 2012; revised March 26, 2013.
Published electronically May 7, 2013.
The research of the first two authors are supported by NSERC discovery grants, and the research of the third author is supported by NSFC (11126191) and NSFC(11201163). This work was completed when the third author visited the University of Waterloo in 2012, and she would like to thank the Department of Pure Mathematics for its hospitality.
AMS subject classification: **11D45**, 11P55, 11T55.
Keywords: Vinogradov's mean value theorem, function fields, circle method.

therefore natural to consider linear spaces of higher dimension. Results concerning the existence of such spaces date back to work by Brauer [2] and Birch [1]. Asymptotic estimates for linear spaces on the hypersurface (1.1) were first established by Parsell (see [7, 8]). More precisely, for $d \in \mathbb{N}$ with $d \geq 2$, we find that the linear spaces of dimension d are in correspondence with solutions of the system

$$a_1 u_{11}^{i_1} \cdots u_{d1}^{i_d} + \cdots + a_s u_{1s}^{i_1} \cdots u_{ds}^{i_d} = 0, \quad i_1 + \cdots + i_d = k. \tag{1.2}$$

Let $M_{s,k,d,\mathbf{a}}(P)$ denote the number of solutions of (1.2) with

$$u_{lj} \in [-P, P] \cap \mathbb{Z}, \quad 1 \leq l \leq d,\ 1 \leq j \leq s,$$

and let $n_1 = \binom{k+d}{k} - 1$. A result of Parsell [8] states that, subject to a local solubility hypothesis, whenever $s \geq 2n_1 k((2/3)\log n_1 + (1/2)\log k) + O(n_1 k \log\log k)$, we can establish an asymptotic formula for $M_{s,k,d,\mathbf{a}}(P)$. By employing Wooley's new efficient congruencing method, Parsell, Prendiville, and Wooley [9] have further improved the above bound to

$$s \geq 2n_1 k + 2n_1 + 1. \tag{1.3}$$

The main result in [9] is indeed applicable to general translation-dilation invariant systems (for definition, see [9, Section 2]).

Let $\mathbb{F}_q[t]$ be the ring of polynomials over the finite field $\mathbb{F}_q$ of q elements whose characteristic is p. Since there exists remarkable similarity between $\mathbb{Z}$ and $\mathbb{F}_q[t]$, we can formulate the above questions in function fields. Let $k \in \mathbb{N}$ with $p \nmid k$. For $\mathbf{c} = (c_1, \ldots, c_s) \in (\mathbb{F}_q[t] \setminus \{0\})^s$, consider the hypersurface defined by

$$c_1 z_1^k + \cdots + c_s z_s^k = 0. \tag{1.4}$$

For $P \in \mathbb{N}$, let I_P be the subset of $\mathbb{F}_q[t]$ containing all polynomials of degree $< P$. Let $N_{s,k,\mathbf{c}}(P)$ denote the number of solutions of (1.4) with $z_j \in I_P$, $1 \leq j \leq s$. A result by Wooley and the second author [6] states that, subject to a local solubility hypothesis, whenever $s \geq (4/3)k\log k + O(k\log\log k)$, we have $N_{s,k,\mathbf{c}}(P) \gg (q^P)^{s-k}$. Moreover, under the same hypothesis, their recent work on Vinogradov's mean value theorem in function fields can be used to prove that whenever $s \geq 2n_2 k + 2n_2 + 1$, where $1 \leq n_2 = n_2(k; p) \leq k$, we can establish an asymptotic formula for $N_{s,k,\mathbf{c}}(P)$. The Lang–Tsen theory of C_i-fields (see [5, Theorem 8]) shows that (1.4) possesses a non-trivial solution whenever $s \geq k^2 + 1$. Thus, if $2n_2 k + 2n_2 \geq k^2$, then the local solubility hypothesis is automatically satisfied.

We now consider linear spaces of higher dimension in function fields. For $d \in \mathbb{N}$ with $d \geq 2$, let $\mathbf{x}_1, \ldots, \mathbf{x}_d \in \mathbb{F}_q[t]^s$ be linearly independent vectors and define

$$\mathrm{Span}\{\mathbf{x}_1, \ldots, \mathbf{x}_d\} = \left\{ \mathfrak{f}_1 \mathbf{x}_1 + \cdots + \mathfrak{f}_d \mathbf{x}_d \;\middle|\; \mathfrak{f}_1, \ldots, \mathfrak{f}_d \in \mathbb{F}_q(t) \right\}.$$

Write $\mathbf{x}_i = (x_{i1}, \ldots, x_{is})$, $1 \leq i \leq d$. Then the hypersurface (1.4) contains the d-dimensional linear space $\mathrm{Span}\{\mathbf{x}_1, \ldots, \mathbf{x}_d\}$ if and only if

$$c_1(\mathfrak{f}_1 x_{11} + \cdots + \mathfrak{f}_d x_{d1})^k + \cdots + c_s(\mathfrak{f}_1 x_{1s} + \cdots + \mathfrak{f}_d x_{ds})^k = 0.$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

By the multinomial theorem, we see that the above equation is true for every d-tuple $(\mathfrak{f}_1, \dots, \mathfrak{f}_d) \in \mathbb{F}_q(t)^d$ if and only if $\mathbf{x}_1, \dots, \mathbf{x}_d$ simultaneously satisfy the equations

$$\frac{k!}{i_1! \cdots i_d!}\left(c_1 x_{11}^{i_1} \cdots x_{d1}^{i_d} + \cdots + c_s x_{1s}^{i_1} \cdots x_{ds}^{i_d}\right) = 0, \quad i_1 + \cdots + i_d = k.$$

Since the characteristic of $\mathbb{F}_q$ is p, the above system is equivalent to the system

$$c_1 x_{11}^{i_1} \cdots x_{d1}^{i_d} + \cdots + c_s x_{1s}^{i_1} \cdots x_{ds}^{i_d} = 0, \quad (i_1, \dots, i_d) \in \mathcal{L}, \tag{1.5}$$

where the set $\mathcal{L}$ is defined by

$$\mathcal{L} = \left\{ (i_1, \dots, i_d) \in \mathbb{N}^d \;\middle|\; i_1 + \cdots + i_d = k \quad \text{and} \quad p \nmid \frac{k!}{i_1! \cdots i_d!} \right\}.$$

Let $N_{s,k,d,\mathbf{c}}(P)$ denote the number of solutions of (1.5) with

$$x_{lj} \in I_P, \quad 1 \le l \le d,\ 1 \le j \le s.$$

For $\mathbf{i} = (i_1, \dots, i_d) \in \mathbb{N}^d$, we write $|\mathbf{i}| = i_1 + \cdots + i_d$, and write $p \nmid \mathbf{i}$ if $p \nmid i_l$ for some l with $1 \le l \le d$. We abbreviate a monomial of the shape $x_1^{i_1} \cdots x_d^{i_d}$ by $\mathbf{x}^{\mathbf{i}}$. For $m \in \mathbb{N}$, write m in base p, say $m = a_0(m) + a_1(m)p + \cdots + a_D(m)p^D$, where $a_h(m) \in [0, p-1] \cap \mathbb{Z}$, $0 \le h \le D$. In order to estimate $N_{s,k,d,\mathbf{c}}(P)$, we need to estimate a Vinogradov-type system. Let

$$\mathcal{R}_0 = \left\{ \mathbf{i} \in \mathbb{N}^d \;\middle|\; \exists n \in \mathbb{N} \text{ with } a_n(k) \ge 1 \text{ and } a_h(i_1) + \cdots + a_h(i_d) \le a_{h+n}(k),\ h \in \mathbb{N} \right\}$$

and $\mathcal{R}_0' = \left\{ \mathbf{i} \in \mathcal{R}_0 \mid p \nmid \mathbf{i} \right\}$. Let $\mathcal{J}_{s,k,d}(P)$ denote the number of solutions of the system

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}}, \quad \mathbf{i} \in \mathcal{R}_0',$$

with $\mathbf{x}_j, \mathbf{y}_j \in I_P^d$ for $1 \le j \le s$. Write $\iota = \operatorname{card} \mathcal{L}$, the cardinality of the set $\mathcal{L}$, and $\mu = \operatorname{card} \mathcal{R}_0'$. A result of the third author [16] states that for $k \ge d+2$, subject to a local solubility hypothesis, whenever $s \ge 2\mu k(\log(\iota\mu k) + \log\log(\mu k) + 10)$, we can establish an asymptotic formula for $N_{s,k,d,\mathbf{c}}(P)$.

In this paper, we will employ Wooley's new efficient congruencing method to improve the aforementioned result in [16]. In addition to obtaining an upper bound for $\mathcal{J}_{s,k,d}(P)$, we will estimate a more general Vinogradov-type system. Our generalisation seems flexible and could be applied to various Diophantine problems in function fields, including the multidimensional Waring problem and the Tarry problem. We will return to these projects in future papers.

Let $\mathcal{R}$ be a finite subset of $\mathbb{N}^d$ satisfying the following condition:

Condition$*$: for each $\mathbf{j} = (j_1, \dots, j_d) \in \mathcal{R}$, if $\mathbf{l} = (l_1, \dots, l_d) \in \mathbb{N}^d$ with $p \nmid \binom{j_1}{l_1} \cdots \binom{j_d}{l_d}$, then $\mathbf{l} \in \mathcal{R}$.

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Let $J_s(\mathcal{R};P)$ denote the number of solutions of the system

$$\mathbf{u}_1^{\mathbf{j}} + \cdots + \mathbf{u}_s^{\mathbf{j}} = \mathbf{v}_1^{\mathbf{j}} + \cdots + \mathbf{v}_s^{\mathbf{j}}, \quad \mathbf{j} \in \mathcal{R}, \tag{1.6}$$

with $\mathbf{u}_j, \mathbf{v}_j \in I_P^d$, $1 \le j \le s$. We will see in Lemma 3.2 that Condition$*$ implies that $J_s(\mathcal{R};P)$ satisfies a translation invariant property. This condition also plays an important role in the process of efficient congruencing. Since p is the characteristic of $\mathbb{F}_q$, if there exist $\mathbf{i}, \mathbf{j} \in \mathcal{R}$ with $\mathbf{j} = p^\nu \mathbf{i}$ for some $\nu \in \mathbb{N} \setminus \{0\}$, then we have

$$\sum_{j=1}^{s} (\mathbf{u}_j^{\mathbf{j}} - \mathbf{v}_j^{\mathbf{j}}) = \Big(\sum_{j=1}^{s} (\mathbf{u}_j^{\mathbf{i}} - \mathbf{v}_j^{\mathbf{i}}) \Big)^{p^\nu}.$$

Thus, the equations in (1.6) are not always independent. The absence of independence suggests that Vinogradov-type estimates for integers cannot be adapted directly into a function field setting. To regain independence, we instead consider

$$\mathcal{R}' = \left\{ \mathbf{i} \in \mathbb{N}^d \mid p \nmid \mathbf{i} \quad \text{and} \quad p^\nu \mathbf{i} \in \mathcal{R} \text{ for some } \nu \in \mathbb{N} \right\}. \tag{1.7}$$

Then we see that $J_s(\mathcal{R};P)$ also counts the number of solutions of the system

$$\mathbf{u}_1^{\mathbf{i}} + \cdots + \mathbf{u}_s^{\mathbf{i}} = \mathbf{v}_1^{\mathbf{i}} + \cdots + \mathbf{v}_s^{\mathbf{i}}, \quad \mathbf{i} \in \mathcal{R}', \tag{1.8}$$

with $\mathbf{u}_j, \mathbf{v}_j \in I_P^d$, $1 \le j \le s$. By extending Wooley's efficient congruencing method, we will prove the following theorem.

Theorem 1.1 *Let $r = \operatorname{card} \mathcal{R}'$, $\phi = \max_{\mathbf{i} \in \mathcal{R}'} |\mathbf{i}|$, and $\kappa = \sum_{\mathbf{i} \in \mathcal{R}'} |\mathbf{i}|$. Suppose that $d \ge 2$, $\phi \ge 2$, and $s \ge r\phi + r$. Then for each $\epsilon > 0$, there exists a positive constant $C_1 = C_1(s, d; r, \phi, \kappa; q; \epsilon)$ such that*

$$J_s(\mathcal{R};P) \le C_1 \left(q^P\right)^{2sd - \kappa + \epsilon}.$$

We notice here that although the equations in (1.8) are independent, the set $\mathcal{R}'$ is not necessarily contained in $\mathcal{R}$. This lack of inclusion prevents the transfer of certain congruence relations between $\mathcal{R}$ and $\mathcal{R}'$. However, such a transition is necessary to proceed with efficient congruencing. We address this issue by introducing an alternative set extending $\mathcal{R}'$ in Section 4. Since the new set satisfies Condition$*$ and contains $\mathcal{R}'$, it allows successful use of efficient congruencing.

By [16, Lemma A.4], we see that $\mathcal{R}_0$ satisfies Condition$*$. It also follows from [16, Lemma 8.1] that

$$\mathcal{R}_0' = \left\{ \mathbf{i} \in \mathcal{R}_0 \;\middle|\; p \nmid \mathbf{i} \right\} = \left\{ \mathbf{i} \in \mathbb{N}^d \;\middle|\; p \nmid \mathbf{i} \quad \text{and} \quad p^\nu \mathbf{i} \in \mathcal{R}_0 \text{ for some } \nu \in \mathbb{N} \right\}.$$

In addition, a straightforward calculation shows that $k = \max_{\mathbf{i} \in \mathcal{R}_0'} |\mathbf{i}|$ as $p \nmid k$. Since $\mathcal{J}_{s,k,d}(P) = J_s(\mathcal{R}_0;P)$, we can derive the following corollary from Theorem 1.1.

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Corollary 1.2 *Let p be the characteristic of $\mathbb{F}_q$, $\mu = \operatorname{card} \mathcal{R}_0'$ and $K = \sum_{\mathbf{i}\in\mathcal{R}_0'} |\mathbf{i}|$. Let $s, k, d \in \mathbb{N}$ with $d \geq 2$, $k \geq 2$ with $p \nmid k$ and $s \geq \mu k + \mu$. Then for each $\epsilon > 0$, there exists a positive constant $C_2 = C_2(s, d; k; q; \epsilon)$ such that*

$$\mathcal{J}_{s,k,d}(P) \leq C_2\big(q^P\big)^{2sd-K+\epsilon}.$$

Let $\mathbb{F}_q(t)$ be the fraction field of $\mathbb{F}_q[t]$. For a place $w \in \mathbb{F}_q[t]$, let $\mathbb{F}_q(t)_w$ denote the completion of $\mathbb{F}_q(t)$ at w. By combining the above corollary with a variant of the Hardy–Littlewood circle method, we can significantly improve the result in [16, Theorem 1.1] as follows.

Theorem 1.3 *Let p be the characteristic of $\mathbb{F}_q$, $\iota = \operatorname{card} \mathcal{L}$ and $\mu = \operatorname{card} \mathcal{R}_0'$. Let $s, k, d \in \mathbb{N}$ with $d \geq 2$, $k \geq 2$ with $p \nmid k$ and $s \geq 2\mu k + 2\mu + 1$. Suppose that the system (1.5) has non-trivial solutions in all completions $\mathbb{F}_q(t)_w$ of $\mathbb{F}_q(t)$. Then there exist positive constants $C_3 = C_3(s, d; k; q; \mathbf{c})$ and $\eta = \eta(d; k; q)$ such that*

$$N_{s,k,d,\mathbf{c}}(P) = C_3(q^P)^{sd-\iota k} + O\big((q^P)^{sd-\iota k-\eta}\big).$$

An interested reader can find explicit calculations of ι and μ in [16, Lemmas 12.2 and 12.3]. It is worth remarking that when k is of certain form, both ι and μ are independent of k. For example, when $k = 1 + p^E$, $E \in \mathbb{N} \setminus \{0\}$, we have that $\iota = d^2$ and $\mu = d(d + 1)$. In this case, the bound for s in Theorem 1.3 is sharper than its integer analogue in (1.3). Moreover, we may save additional variables by employing a new strategy, introduced in [12–14], for transforming Vinogradov-type estimates to minor arc contributions. We will pursue this improvement in future work.

2 Preliminaries

We begin this section by introducing the Fourier analysis for function fields. Let $\mathbb{A} = \mathbb{F}_q[t]$, and let $\mathbb{K} = \mathbb{F}_q(t)$ be the fraction field of $\mathbb{A}$. Let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K}$ at ∞. We may write each element $\alpha \in \mathbb{K}_\infty$ in the shape $\alpha = \sum_{i\leq \nu} a_i(\alpha)t^i$ for some $\nu \in \mathbb{Z}$ and $a_i(\alpha) \in \mathbb{F}_q$, $i \leq \nu$. If $a_\nu(\alpha) \neq 0$, we say that $\operatorname{ord}\alpha = \nu$ and we write $\langle\alpha\rangle = q^{\operatorname{ord}\alpha}$. We adopt the convention that $\operatorname{ord} 0 = -\infty$ and $\langle 0\rangle = 0$. It is also convenient to refer to a_{-1} as being the residue of α, denoted by $\operatorname{res}\alpha$. Given that the characteristic of $\mathbb{F}_q$ is p, we are now equipped to define the exponential function on $\mathbb{K}_\infty$. Let $e(z)$ denote $e^{2\pi iz}$, and let $\operatorname{tr}\colon \mathbb{F}_q \to \mathbb{F}_p$ denote the familiar trace map. There is a non-trivial additive character $e_q\colon \mathbb{F}_q \to \mathbb{C}^\times$ defined for each $a \in \mathbb{F}_q$ by taking $e_q(a) = e(\operatorname{tr}(a)/p)$. This character induces a map $e\colon \mathbb{K}_\infty \to \mathbb{C}^\times$ by defining, for each $\alpha \in \mathbb{K}_\infty$, the value of $e(\alpha)$ to be $e_q(\operatorname{res}\alpha)$. Let $\mathbb{T} = \{\alpha \in \mathbb{K}_\infty \mid \operatorname{ord}\alpha < 0\}$. Given any Haar measure $d\alpha$ on $\mathbb{K}_\infty$, we normalise it in such a manner that $\int_{\mathbb{T}} 1\, d\alpha$. The orthogonality relation underlying the Fourier analysis of $\mathbb{F}_q[t]$, established in [4, Lemma 1], takes the shape

$$\int_{\mathbb{T}} e(x\alpha)\, d\alpha = \begin{cases} 1, & \text{when } x = 0, \\ 0, & \text{otherwise.} \end{cases}$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Thus, for $n \in \mathbb{N} \setminus \{0\}$, $(x_1, \cdots, x_n) \in \mathbb{A}^n$, and $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{K}_\infty^n$, we have

$$\int_{\mathbb{T}^n} e(x_1\alpha_1 + \cdots + x_n\alpha_n)\, d\alpha = \prod_{l=1}^{n} \int_{\mathbb{T}} e(x_l\alpha_l)\, d\alpha_l = \begin{cases} 1, & \text{when } x_l = 0\ (1 \le l \le n), \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

Let $\mathcal{R}$ be a finite subset of $\mathbb{N}^d$ satisfying Condition$*$, and let $\mathcal{R}'$ be defined as in (1.7). Recall that for $\mathbf{i} = (i_1, \ldots, i_d) \in \mathbb{N}^d$, we write $|\mathbf{i}| = i_1 + \cdots + i_d$. We also denote

$$r = \operatorname{card} \mathcal{R}', \quad \phi = \max_{\mathbf{i} \in \mathcal{R}'} |\mathbf{i}|, \quad \text{and} \quad \kappa = \sum_{\mathbf{i} \in \mathcal{R}'} |\mathbf{i}|. \tag{2.2}$$

For $X \in \mathbb{R}$, let $\widehat{X} = q^X$. For $P \in \mathbb{N}$, we recall that $I_P = \{x \in \mathbb{A} \mid \langle x \rangle < \widehat{P}\}$. Let $J_s(\mathcal{R}; P)$ be defined as in (1.8). For $\mathbf{h} = (h_\mathbf{i})_{\mathbf{i} \in \mathcal{R}'} \in \prod_{\mathbf{i} \in \mathcal{R}'} I_{|\mathbf{i}|P}$, define $J_s(P; \mathbf{h})$ to be the number of solutions of the system

$$\sum_{j=1}^{s} (\mathbf{u}_j^\mathbf{i} - \mathbf{v}_j^\mathbf{i}) = h_\mathbf{i}, \quad \mathbf{i} \in \mathcal{R}',$$

with $\mathbf{u}_j, \mathbf{v}_j \in I_P^d$, $1 \le j \le s$. Thus, $J_s(P; \mathbf{h}) = J_s(\mathcal{R}; P)$ whenever $h_\mathbf{i} = 0$, $\mathbf{i} \in \mathcal{R}'$. For $(\alpha) = (\alpha_\mathbf{i})_{\mathbf{i} \in \mathcal{R}'} \in \mathbb{K}_\infty^r$, write

$$f(\alpha; P) = \sum_{\mathbf{x} \in I_P^d} e\Big(\sum_{\mathbf{i} \in \mathcal{R}'} \alpha_\mathbf{i} \mathbf{x}^\mathbf{i} \Big).$$

By (2.1), we have

$$J_s(P; \mathbf{h}) = \int_{\mathbb{T}^r} \big| f(\alpha; P) \big|^{2s} e\Big(- \sum_{\mathbf{i} \in \mathcal{R}'} \alpha_\mathbf{i} h_\mathbf{i} \Big)\, d\alpha.$$

Since

$$J_s(P; \mathbf{h}) \le \int_{\mathbb{T}^r} \big| f(\alpha; P) \big|^{2s} d\alpha = J_s(\mathcal{R}; P),$$

it follows that

$$\widehat{P}^{2sd} \le \sum_{\mathbf{h} \in \prod_{\mathbf{i} \in \mathcal{R}'} I_{|\mathbf{i}|P}} J_s(P; \mathbf{h}) \le \sum_{\mathbf{h} \in \prod_{\mathbf{i} \in \mathcal{R}'} I_{|\mathbf{i}|P}} J_s(\mathcal{R}; P) = \widehat{P}^{\kappa} J_s(\mathcal{R}; P).$$

Thus, we have

$$J_s(\mathcal{R}; P) \ge \widehat{P}^{2sd - \kappa}. \tag{2.3}$$

For $s \in \mathbb{N}$, we say that λ_s is *admissible for* $\mathcal{R}$ if for any $\epsilon > 0$ and $P \in \mathbb{N}$ sufficiently large (in terms of s, d, r, ϕ, κ, q and ϵ), we have $J_s(\mathcal{R}; P) \ll \widehat{P}^{\lambda_s + \epsilon}$. Define λ_s^* to be the

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

infimum of the set of exponents λ_s admissible for $\mathcal{R}$. Thus, for P sufficiently large, we have

$$J_s(\mathcal{R};P) \ll \widehat{P}^{\lambda_s^*+\epsilon}.$$

Write $\eta_s = \lambda_s^* - 2sd + \kappa$. It follows from (2.3) that $\eta_s \geq 0$.

In the following, we abbreviate $J_s(\mathcal{R};P)$ as $J_s(P)$. We will focus on estimating $J_{s+r}(P)$ for $s = ru$ with some $u \in \mathbb{N}$ satisfying $u \geq \phi$. Then Theorem 1.1 can be established by showing that $\eta_{s+r} = 0$. Let $N \in \mathbb{N}$ be sufficiently large (in terms of s, d, r, ϕ, κ and q). Let $\theta = N^{-1/2}(r/s)^{N+2}$ and $\delta = (6sN)^{-(2N+3)}$. Thus, we have

$$\delta < (2s/r)^{-N}\theta/(6s). \tag{2.4}$$

By the infimal definition of λ_{s+r}^*, there exists a sequence of non-negative integers $(P_m)_{m=1}^{\infty}$, tending to ∞, such that

$$J_{s+r}(P_m) > \widehat{P_m}^{\lambda_{s+r}^*-\delta}, \quad m \in \mathbb{N}\setminus\{0\}. \tag{2.5}$$

If P_m is sufficiently large (in terms of s, d, r, ϕ, κ, q and N), then for any $Q \in \mathbb{N}$ with $\delta^2 P_m < Q \leq P_m$, we have

$$J_{s+r}(Q) < \widehat{Q}^{\lambda_{s+r}^*+\delta}$$

For N sufficiently large, we have $\delta < (2(s+r)d)^{-1}$. Thus, for $0 < Q \leq P_m$, by the trivial bound $|f(\alpha;P)| \leq \widehat{P}^d$, we have

$$J_{s+r}(Q) < \widehat{P_m}^{2(s+r)d\delta^2} + \widehat{Q}^{\lambda_{s+r}^*+\delta} < 2\widehat{P_m}^{\delta}\widehat{Q}^{2(s+r)d-\kappa+\eta_{s+r}}. \tag{2.6}$$

In what follows, we consider a fixed element $P = P_m$ of the sequence $(P_m)_{m=1}^{\infty}$, which is sufficiently large (in terms of s, d, r, ϕ, κ, q and N). Unless stated otherwise, all implicit constants below may depend at most on s, d, r, ϕ, κ, q, and N. Since our methods involve only a finite number of steps, these implicit constants are under control. In addition, for $X \in \mathbb{R}$, we write $[X]$ for the greatest integer not exceeding X. Finally, for $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{A}^n$, $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{A}^n$ and $g \in \mathbb{A}$, we write $\mathbf{a} \equiv \mathbf{b} \pmod{g}$ if $a_l \equiv b_l \pmod{g}$, $1 \leq l \leq n$. Then for $\mathbf{a}', \mathbf{b}' \in \mathbb{A}^d$, we write $(\mathbf{a}, \mathbf{a}') \equiv (\mathbf{b}, \mathbf{b}') \pmod{g}$ if $\mathbf{a} \equiv \mathbf{b} \pmod{g}$ and $\mathbf{a}' \equiv \mathbf{b}' \pmod{g}$.

We recall that $J_{s+r}(P)$ counts the number of solutions of the system

$$\sum_{i=1}^{r}\left(\mathbf{y}_i^{\mathbf{i}} - \mathbf{z}_i^{\mathbf{i}}\right) = \sum_{j=1}^{s}\left(\mathbf{u}_j^{\mathbf{i}} - \mathbf{v}_j^{\mathbf{i}}\right), \quad \mathbf{i} \in \mathcal{R}', \tag{2.7}$$

with $\mathbf{y}_i, \mathbf{z}_i, \mathbf{u}_j, \mathbf{v}_j \in I_P^d$, $1 \leq i \leq r$, $1 \leq j \leq s$. Let $w \in \mathbb{A}$ be irreducible, and let $h, n, \nu \in \mathbb{N}$. Let $(\mathbf{f})$ be a system of h many polynomials in $\mathbb{A}[t_1, \dots, t_n]$. For $\mathbf{g}_1, \dots, \mathbf{g}_\nu \in \mathbb{A}^n$, let $\mathrm{Jac}(\mathbf{f};\mathbf{g}_l)$ denote the $h \times n$ Jacobian matrix of $\mathbf{f}$ evaluated at $\mathbf{g}_l$, $1 \leq l \leq n$. We write $\mathrm{rk}\,\mathrm{Jac}(\mathbf{f};\mathbf{g}_1, \dots, \mathbf{g}_\nu; w)$ for the rank of the $h \times n\nu$ Jacobian matrix

$$\left(\mathrm{Jac}(\mathbf{f};\mathbf{g}_1), \dots, \mathrm{Jac}(\mathbf{f};\mathbf{g}_\nu)\right)$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

over $\mathbb{A}/(w)$. In addition, write $I^*(P;w)$ for the number of solutions

$$(\mathbf{y}_i, \mathbf{z}_i, \mathbf{u}_j, \mathbf{v}_j), \quad 1 \le i \le r, 1 \le j \le s,$$

counted by $J_{s+r}(P)$ for which

$$\operatorname{rk} \operatorname{Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{y}_1, \dots, \mathbf{y}_r; w\right) = r.$$

To bound $J_{s+r}(P)$ in terms of $I^*(P;w)$, we need the following lemma.

Lemma 2.1 *Let $v \in \mathbb{N}$ with $v \ge r$, and let $w \in \mathbb{A}$ be irreducible. Let $\mathcal{S}(w)$ denote the set of v-tuples $(\mathbf{g}_1, \dots, \mathbf{g}_v)$ with $\mathbf{g}_l \in \left(\mathbb{A}/(w)\right)^d$, $1 \le l \le v$, such that*

$$\operatorname{rk} \operatorname{Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{g}_1, \dots, \mathbf{g}_v; w\right) < r.$$

We have

$$\operatorname{card} \mathcal{S}(w) \ll \langle w\rangle^{v(d-1)+r-1},$$

where the implicit constant depends on v, ϕ, r, and d.

Proof This proof can be carried out by replacing $\mathcal{R}_0'$ and k in the proof of [16, Lemma 7.3] with $\mathcal{R}'$ and ϕ respectively. ∎

Lemma 2.2 *Let $s = ru$ with $u \in \mathbb{N}$ and $u \ge \phi$, and let $M = [\theta P] + 1$. There exists an irreducible polynomial $w \in \mathbb{A}$ with $\langle w\rangle = \widehat{M}$ such that*

$$J_{s+r}(P) \ll I^*(P;w).$$

Proof For P sufficiently large, there exists a set $\mathcal{P}$ consisting of $[\theta^{-1}]$ irreducible polynomials of degree $[\theta P] + 1$. Let S_1 denote the number of solutions

$$(\mathbf{y}_i, \mathbf{z}_i, \mathbf{u}_j, \mathbf{v}_j), \quad 1 \le i \le r,\ 1 \le j \le s,$$

counted by $J_{s+r}(P)$ such that for all $w \in \mathcal{P}$,

$$\operatorname{rk} \operatorname{Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r; w\right) < r.$$

Let S_2 denote the number of remaining solutions, *i.e.*, the solutions for which

$$\operatorname{rk} \operatorname{Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r; w\right) = r$$

for some $w \in \mathcal{P}$. Thus, we have

$$J_{s+r}(P) = S_1 + S_2.$$

There are two cases.

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Case 1: Suppose that $S_2 \le S_1$. For every $w \in \mathcal{P}$, by taking $v = 2r$ in Lemma 2.1, we see that the number of $(\mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r) \in (\mathbb{A}/(w))^{2rd}$ with

$$\operatorname{rk}\operatorname{Jac}\big((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r; w\big) < r$$

is $O(\langle w\rangle^{2rd-r-1})$. Let $\rho = \prod_{w\in\mathcal{P}} w$. By the Chinese Remainder Theorem, in the solutions counted by S_1, the total number of choices for $(\mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r) \in (\mathbb{A}/(\rho))^{2rd}$ is $O(\langle\rho\rangle^{2rd-r-1})$. For each fixed choice $(\mathbf{g}_1, \dots, \mathbf{g}_r, \mathbf{h}_1, \dots, \mathbf{h}_r) (\mathrm{mod}\, \rho)$, there are at most $(\widehat{P}/\langle\rho\rangle)^{2rd}$ choices for the $(\mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r) \in I_P^{2rd}$ with $(\mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r) \equiv (\mathbf{g}_1, \dots, \mathbf{g}_r, \mathbf{h}_1, \dots, \mathbf{h}_r) (\mathrm{mod}\, \rho)$. Thus, the number of $(\mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r) \in I_P^{2rd}$ under consideration can be estimated by $O(\widehat{P}^{2rd}\langle\rho\rangle^{-r-1})$. Since $\langle\rho\rangle > (\widehat{P}^{\theta})^{\theta^{-1}-1} = \widehat{P}^{1-\theta}$, we have

$$\widehat{P}^{2rd}\langle\rho\rangle^{-r-1} < \widehat{P}^{2rd-(r+1)(1-\theta)}.$$

Thus, we have

$$J_{s+r}(P) \le 2S_1 \ll \widehat{P}^{2rd-(r+1)(1-\theta)} J_s(P).$$

By Hölder's inequality, we have

$$J_s(P) = \int_{\mathbb{T}^r} \big|f(\alpha; P)\big|^{2s} d\alpha \le \Big(\int_{\mathbb{T}^r} \big|f(\alpha; P)\big|^{2(s+r)} d\alpha \Big)^{s/(s+r)} = J_{s+r}(P)^{s/(s+r)}.$$

On combining the above two estimates, we see that

$$J_{s+r}(P) \ll \widehat{P}^{2rd-(r+1)(1-\theta)} J_{s+r}(P)^{s/(s+r)},$$

which implies that

$$J_{s+r}(P) \ll \widehat{P}^{2(s+r)d-(r+1)(1-\theta)(s+r)/r}.$$

Notice that $s \ge r\phi \ge \kappa$ and

$$\theta = N^{-1/2}(r/s)^{N+2} \le \phi^{-(N+2)} \le (\phi + r)\big((r+1)(\phi+1)\big)^{-1}.$$

Thus, we have

$$(r+1)(1-\theta)(s+r)/r \ge (r+1)(1-\theta)(\phi+1) = r\phi+\phi+r+1-\theta(r+1)(\phi+1) \ge \kappa+1.$$

It follows that

$$J_{s+r}(P) \ll \widehat{P}^{2(s+r)d-\kappa-1},$$

which contradicts the lower bound in (2.3).

Case 2: Suppose that $S_1 \le S_2$. On noticng that $\mathcal{P} \ll 1$, we see that there exists $w \in \mathcal{P}$ such that $S_2 \ll S_3(w)$, where $S_3(w)$ denotes the number of solutions $(\mathbf{y}_i, \mathbf{z}_i, \mathbf{u}_j, \mathbf{v}_j)$, $1 \le i \le r$, $1 \le j \le s$, counted by S_2 for which

$$\operatorname{rk}\operatorname{Jac}\big((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{y}_1, \dots, \mathbf{y}_r, \mathbf{z}_1, \dots, \mathbf{z}_r; w\big) = r.$$

After rearranging variables, we have

$$J_{s+r}(P) \ll S_3(w) \ll I^*(P; w).$$

On combining Cases 1 and 2, the lemma follows. ∎

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

In what follows, for a sufficiently large $P = P_m$ (in terms of s, d, r, ϕ, κ, q, and N), let $M = [\theta P] + 1$ and let $w \in \mathbb{A}$ satisfy all conditions in Lemma 2.2. For $g \in \mathbb{A} \setminus \{0\}$, define

$$L(g) = \left\{ (a_1, \dots, a_d) \in \mathbb{A}^d \mid \deg a_i < \deg g, \quad 1 \le i \le d \right\}.$$

For $c \in \mathbb{N}$ and $\xi \in \mathbb{A}^d$, denote by $\Xi_c(\xi; w)$ the set of r-tuples $(\xi_1, \dots, \xi_r)$ with $\xi_i \in L(w^{c+1})$ and $\xi_i \equiv \xi \pmod{w^c}$, $1 \le i \le r$, such that

$$\operatorname{rk} \operatorname{Jac} \left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'}; [\xi_1], \dots, [\xi_r]; w \right) = r,$$

where for $\eta \equiv \xi \pmod{w^c}$, write $[\eta] = [\eta]_{c,w,\xi} = w^{-c}(\eta - \xi)$. Let $R = \operatorname{card} \mathcal{R}$. In the following sections, we will frequently apply the multinomial theorem stated in Lemma 3.1 to treat certain congruence conditions. Since system (2.7) does not necessarily contain all equations that are needed to use the theorem, we consider instead the equivalent definition of $J_{s+r}(P)$ that counts the number of solutions of the system

$$\sum_{i=1}^{r} \left(\mathbf{y}_i^{\mathbf{j}} - \mathbf{z}_i^{\mathbf{j}} \right) = \sum_{j=1}^{s} \left(\mathbf{u}_j^{\mathbf{j}} - \mathbf{v}_j^{\mathbf{j}} \right), \quad \mathbf{j} \in \mathcal{R}$$

with $\mathbf{y}_i, \mathbf{z}_i, \mathbf{u}_j, \mathbf{v}_j \in I_P^d$, $1 \le i \le r$, $1 \le j \le s$. Thus, in what follows, we will integrate over $\mathbb{T}^R$ instead of $\mathbb{T}^r$. For $\alpha = (\alpha_{\mathbf{j}})_{\mathbf{j} \in \mathcal{R}} \in \mathbb{K}_\infty^R$ and $\sigma \in \Sigma_r = \{1, -1\}^r$, define

$$\mathfrak{f}_c(\alpha; \xi) = \sum_{\substack{\mathbf{x} \in I_P^d \\ \mathbf{x} \equiv \xi \pmod{w^c}}} e\Big(\sum_{\mathbf{j} \in \mathcal{R}} \alpha_{\mathbf{j}} \mathbf{x}^{\mathbf{j}} \Big)$$

and

$$\mathfrak{F}_c^\sigma(\alpha; \xi) = \sum_{(\xi_1, \dots, \xi_r) \in \Xi_c(\xi; w)} \prod_{i=1}^{r} \mathfrak{f}_{c+1}(\sigma_i \alpha; \xi_i).$$

Let $s = ru$ with $u \in \mathbb{N}$ and $u \ge \phi$. For $a, b \in \mathbb{N}$, $\xi, \eta \in \mathbb{A}^d$ and $\sigma, \tau \in \Sigma_r$, define

$$I_{a,b}^\sigma(P; \xi, \eta) = \int_{\mathbb{T}^R} \left| \mathfrak{F}_a^\sigma(\alpha; \xi)^2 \mathfrak{f}_b(\alpha; \eta)^{2s} \right| d\alpha$$

and

$$K_{a,b}^{\sigma,\tau}(P; \xi, \eta) = \int_{\mathbb{T}^R} \left| \mathfrak{F}_a^\sigma(\alpha; \xi)^2 \mathfrak{F}_b^\tau(\alpha; \eta)^{2u} \right| d\alpha.$$

We then define

$$I_{a,b}(P) = \max_{\xi \in L(w^a)} \max_{\eta \in L(w^b)} \max_{\sigma \in \Sigma_r} I_{a,b}^\sigma(P; \xi, \eta)$$

and

$$K_{a,b}(P) = \max_{\xi \in L(w^a)} \max_{\eta \in L(w^b)} \max_{\sigma, \tau \in \Sigma_r} K_{a,b}^{\sigma,\tau}(P; \xi, \eta).$$

To obtain Theorem 1.1, we will iterate among the mean values $J_{s+r}(P)$, $I_{a,b}(P)$ and $K_{a,b}(P)$. The first step is to estimate $J_{s+r}(P)$ in terms of $K_{0,1}(P)$ by imposing some

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

initial efficient congruence conditions to the variables. Then we extract stronger congruence conditions from $K_{0,1}(P)$ and estimate it in terms of $K_{a,b}(P)$ for some $b > a$. On repeating such a process, we can bound $J_{s+r}(P)$ by a sequence of mean values $K_{a,b}(P)$. A major difficulty in each stage is to well-condition the variables such that the next efficient congruence can be extracted. We overcome this difficulty by making use of the mean values $I_{a,b}(P)$.

3 The Conditioning Process

For $a, b, c \in \mathbb{N}$, the goal of this section is to associate $I_{a,b}(P)$ with $K_{a,c}(P)$ in the way that the variables are well-conditioned in view of the definition of $K_{a,c}(P)$. In addition, in Lemma 3.6, we complete the initial step by relating $J_{s+r}(P)$ to $K_{0,1}(P)$.

Lemma 3.1 *For* $\mathbf{j} = (j_1, \dots, j_d) \in \mathbb{N}^d$ *and* $\mathbf{l} = (l_1, \dots, l_d) \in \mathbb{N}^d$, *write*

$$\binom{\mathbf{j}}{\mathbf{l}} = \binom{j_1}{l_1} \cdots \binom{j_d}{l_d}.$$

For $\mathbf{j} \in \mathbb{N}^d$, *define*

$$\mathcal{R}_{\mathbf{j}} = \left\{ \mathbf{l} \in \mathbb{N}^d \;\middle|\; p \nmid \binom{\mathbf{j}}{\mathbf{l}} \right\}.$$

Then for $\mathbf{x}, \mathbf{y} \in \mathbb{A}^d$, *we have*

$$(\mathbf{x} + \mathbf{y})^{\mathbf{j}} = \sum_{\mathbf{l} \in \mathcal{R}_{\mathbf{j}}} \binom{\mathbf{j}}{\mathbf{l}} \mathbf{x}^{\mathbf{l}} \mathbf{y}^{\mathbf{j}-\mathbf{l}}.$$

Proof This is [16, Lemma 3.2]. ∎

We remark that Condition$*$ implies that $\mathcal{R}_{\mathbf{j}} \subseteq \mathcal{R}$ for each $\mathbf{j} \in \mathcal{R}$. We are now in a position to deduce a translation invariance of the Diophantine system underlying the mean value $J_n(P)$.

Lemma 3.2 *Let* $c \in \mathbb{N}$ *with* $c \leq \theta^{-1} - 1$. *For* $n \in \mathbb{N}$, *we have*

$$\max_{\xi \in L(w^c)} \int_{\mathbb{T}^R} \left| \mathfrak{f}_c(\alpha; \xi) \right|^{2n} d\alpha = J_n(P - cM).$$

Proof We observe first that for $c \leq \theta^{-1} - 1$ and $M = [\theta P] + 1$, if P is sufficiently large (in terms of s, r, N), then $P - cM > 0$. For $\xi \in L(w^c)$, by the definition of $\mathfrak{f}_c(\alpha; \xi)$, we have

$$\mathfrak{f}_c(\alpha; \xi) = \sum_{\mathbf{y} \in I^d_{P - \operatorname{ord} w^c}} e\Big(\sum_{\mathbf{j} \in \mathcal{R}} \alpha_{\mathbf{j}} (w^c \mathbf{y} + \xi)^{\mathbf{j}} \Big).$$

By (2.1), the integral $\int_{\mathbb{T}^R} \left| \mathfrak{f}_c(\alpha; \xi) \right|^{2n} d\alpha$ counts the number of solutions of the system

$$\sum_{i=1}^{n} (w^c \mathbf{y}_i + \xi)^{\mathbf{j}} = \sum_{i=1}^{n} (w^c \mathbf{z}_i + \xi)^{\mathbf{j}}, \quad \mathbf{j} \in \mathcal{R}$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

with $\mathbf{y}_i, \mathbf{z}_i \in I^d_{P-\operatorname{ord} w^c}$, $1 \le i \le n$. By Lemma 3.1 and Condition$*$, we see that the above system is equivalent to

$$\sum_{i=1}^{n} \mathbf{y}_i^{\mathbf{j}} = \sum_{i=1}^{n} \mathbf{z}_i^{\mathbf{j}}, \quad \mathbf{j} \in \mathcal{R}.$$

On recalling that $\operatorname{ord} w = M$, the lemma follows. ∎

Lemma 3.3 *Let $a, b \in \mathbb{N}$ with $b > a$. We have*

$$I_{a,b}(P) \ll K_{a,b}(P) + \widehat{M}^{2s(d-1)+r-1} I_{a,b+1}(P).$$

Proof For $\xi \in L(w^a)$, $\eta \in L(w^b)$ and $\sigma \in \Sigma_r$, we see from (2.1) that $I^{\sigma}_{a,b}(P; \xi, \eta)$ counts the number of solutions of the system

$$\sum_{i=1}^{r} \sigma_i \left(\mathbf{y}_i^{\mathbf{j}} - \mathbf{z}_i^{\mathbf{j}} \right) = \sum_{j=1}^{s} \left(\mathbf{u}_j^{\mathbf{j}} - \mathbf{v}_j^{\mathbf{j}} \right), \quad \mathbf{j} \in \mathcal{R},$$

with

$$\mathbf{y}_i, \mathbf{z}_i \in I_P^d, \quad \mathbf{y}_i \equiv \xi_i \,(\operatorname{mod} w^{a+1}), \quad \mathbf{z}_i \equiv \zeta_i \,(\operatorname{mod} w^{a+1}), \quad 1 \le i \le r,$$

for some $(\xi_1, \dots, \xi_r), (\zeta_1, \dots, \zeta_r) \in \Xi_a(\xi; w)$, and with

$$\mathbf{u}_j, \mathbf{v}_j \in I_P^d, \quad \mathbf{u}_j \equiv \mathbf{v}_j \equiv \eta \,(\operatorname{mod} w^b) \quad (1 \le j \le s).$$

For $\gamma \equiv \eta \,(\operatorname{mod} w^b)$, write $[\gamma] = w^{-b}(\gamma - \eta)$. Let T_1 denote the number of solutions $(\mathbf{y}_i, \mathbf{z}_i, \mathbf{u}_j, \mathbf{v}_j)$, $1 \le i \le r$, $1 \le j \le s$ counted by $I^{\sigma}_{a,b}(P; \xi, \eta)$ for which

$$\operatorname{rk} \operatorname{Jac} \left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'}; [\mathbf{u}_1], \dots, [\mathbf{u}_s], [\mathbf{v}_1], \dots, [\mathbf{v}_s]; w \right) < r.$$

Let T_2 denote the number of remaining solutions, *i.e.,* the solutions for which

$$\operatorname{rk} \operatorname{Jac} \left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'}; [\mathbf{u}_1], \dots, [\mathbf{u}_s], [\mathbf{v}_1], \dots, [\mathbf{v}_s]; w \right) = r.$$

Thus, we have $I^{\sigma}_{a,b}(P; \xi, \eta) = T_1 + T_2$.

To estimate T_1, let

$$\mathcal{C} = \left\{ (\mathbf{u}_1, \dots \mathbf{u}_s, \mathbf{v}_1, \dots, \mathbf{v}_s) \pmod{w^{b+1}} \mid (\mathbf{y}_i, \mathbf{z}_i, \mathbf{u}_j, \mathbf{v}_j) \text{ counted by } T_1 \right\}$$

and

$$\mathcal{C}' = \left\{ ([\mathbf{u}_1], \dots, [\mathbf{u}_s], [\mathbf{v}_1], \dots, [\mathbf{v}_s]) \,(\operatorname{mod} w) \mid (\mathbf{u}_1, \dots, \mathbf{u}_s, \mathbf{v}_1, \dots, \mathbf{v}_s) \in \mathcal{C} \right\}.$$

Consider the bijection from $\mathcal{C}$ to $\mathcal{C}'$ defined by

$$(\mathbf{u}_1, \dots, \mathbf{u}_s, \mathbf{v}_1, \dots, \mathbf{v}_s) \longmapsto \left([\mathbf{u}_1], \dots, [\mathbf{u}_s], [\mathbf{v}_1], \dots, [\mathbf{v}_s] \right).$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

By the definition of T_1, it follows from Lemma 2.1 that

$$\operatorname{card} \mathcal{C} = \operatorname{card} \mathcal{C}' \ll \langle w \rangle^{2s(d-1)+r-1}.$$

On considering the underlying Diophantine system, we have

$$T_1 \leq \sum_{(\eta_1', \dots, \eta_{2s}') \in \mathcal{C}} \int_{\mathbb{T}^R} |\mathfrak{F}_a^\sigma(\alpha; \xi)|^2 \prod_{j=1}^{s} \mathfrak{f}_{b+1}(\alpha; \eta_j') \mathfrak{f}_{b+1}(-\alpha; \eta_{j+s}') d\alpha.$$

By Hölder's inequality, we have

$$\begin{aligned} \int_{\mathbb{T}^R} \big| \mathfrak{F}_a^\sigma(\alpha; \xi) \big|^2 \prod_{j=1}^{2s} \big| \mathfrak{f}_{b+1}(\alpha; \eta_j') \big| \, d\alpha &\leq \prod_{j=1}^{2s} \Big(\int_{\mathbb{T}^R} |\mathfrak{F}_a^\sigma(\alpha; \xi)|^2 |\mathfrak{f}_{b+1}(\alpha; \eta_j')|^{2s} d\alpha \Big)^{1/(2s)} \\ &\leq I_{a,b+1}(P). \end{aligned}$$

It follows that

$$T_1 \ll \widehat{M}^{2s(d-1)+r-1} I_{a,b+1}(P).$$

We now consider the solutions counted by T_2. Since

$$\operatorname{rk} \operatorname{Jac} \big((\mathbf{x}^{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'}; [\mathbf{u}_1], \dots, [\mathbf{u}_s], [\mathbf{v}_1], \dots, [\mathbf{v}_s]; w \big) = r,$$

after rearranging variables, we can assume that

$$\operatorname{rk} \operatorname{Jac} \big((\mathbf{x}^{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'}; [\mathbf{u}_1], \dots, [\mathbf{u}_r]; w \big) = r.$$

Thus, there exists $(\eta_1, \dots, \eta_r) \in \Xi_b(\eta; w)$ such that $\mathbf{u}_i \equiv \eta_i \pmod{w^{b+1}}$, $1 \leq i \leq r$. On considering the underlying Diophantine system, we see that

$$T_2 \ll \int_{\mathbb{T}^R} |\mathfrak{F}_a^\sigma(\alpha; \xi)|^2 \mathfrak{F}_b^{\mathbf{1}}(\alpha; \eta) \mathfrak{f}_b(\alpha; \eta)^{s-r} \mathfrak{f}_b(-\alpha; \eta)^s d\alpha,$$

where $\mathbf{1} = (1, \dots, 1) \in \Sigma_r$. On recalling that $s = ur$, it follows from Hölder's inequality that

$$T_2 \ll \Big(\int_{\mathbb{T}^R} |\mathfrak{F}_a^\sigma(\alpha; \xi)^2 \mathfrak{F}_b^{\mathbf{1}}(\alpha; \eta)^{2u}| d\alpha \Big)^{1/(2u)} \Big(\int_{\mathbb{T}^R} |\mathfrak{F}_a^\sigma(\alpha; \xi)^2 \mathfrak{f}_b(\alpha; \eta)^{2s}| d\alpha \Big)^{1-1/(2u)}.$$

Thus, we have

$$T_2 \ll \big(K_{a,b}(P) \big)^{1/(2u)} \big(I_{a,b}(P) \big)^{1-1/(2u)}.$$

On combining the above upper bounds for T_1 and T_2, we obtain

$$I_{a,b}(P) \ll \widehat{M}^{2s(d-1)+r-1} I_{a,b+1}(P) + \big(K_{a,b}(P) \big)^{1/(2u)} \big(I_{a,b}(P) \big)^{1-1/(2u)},$$

which implies that

$$I_{a,b}(P) \ll \widehat{M}^{2s(d-1)+r-1} I_{a,b+1}(P) + K_{a,b}(P).$$

This completes the proof of the lemma. ∎

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

We remark here that by repeated applications of Lemma 3.3, whenever $a, b, H \in \mathbb{N}$ with $b > a$, we have

$$I_{a,b}(P) \ll \sum_{h=0}^{H-1} \widehat{M}^{h(2s(d-1)+r-1)} K_{a,b+h}(P) + \widehat{M}^{H(2s(d-1)+r-1)} I_{a,b+H}(P). \tag{3.1}$$

Lemma 3.4 *Let $a, b, H \in \mathbb{N}$ with $0 < b - a \le H \le \theta^{-1} - 1 - b$. We have*

$$\widehat{M}^{H(2s(d-1)+r-1)} I_{a,b+H}(P) \ll \widehat{M}^{-H/2} \big(\widehat{P}/\widehat{M}^b\big)^{2sd} \big(\widehat{P}/\widehat{M}^a\big)^{2rd-\kappa+\eta_{s+r}}.$$

Proof For $\xi \in L(w^a)$, $\eta \in L(w^{b+H})$ and $\sigma \in \Sigma_r$, by the definition of $I^{\sigma}_{a,b+H}(P;\xi,\eta)$, we see that

$$I^{\sigma}_{a,b+H}(P;\xi,\eta) \le \int_{\mathbb{T}^R} |\mathfrak{f}_a(\alpha;\xi)^{2r} \mathfrak{f}_{b+H}(\alpha;\eta)^{2s}| d\alpha.$$

By Hölder's inequality and Lemma 3.2, we have

$$\begin{aligned} I^{\sigma}_{a,b+H}(P;\xi,\eta) &\le \Big(\int_{\mathbb{T}^R} |\mathfrak{f}_a(\alpha;\xi)|^{2(s+r)} d\alpha \Big)^{r/(s+r)} \Big(\int_{\mathbb{T}^R} |\mathfrak{f}_{b+H}(\alpha;\eta)|^{2(s+r)} d\alpha \Big)^{s/(s+r)} \\ &\ll \big(J_{s+r}(P - aM)\big)^{r/(s+r)} \big(J_{s+r}(P - (b+H)M)\big)^{s/(s+r)}. \end{aligned}$$

It follows from (2.6) that

$$\begin{aligned} I_{a,b+H}(P) &\ll \widehat{P}^{\delta} \big((\widehat{P}/\widehat{M}^a)^{r/(s+r)} (\widehat{P}/\widehat{M}^{b+H})^{s/(s+r)} \big)^{2(s+r)d-\kappa+\eta_{s+r}} \\ &\ll \widehat{P}^{\delta} (\widehat{P}/\widehat{M}^a)^{2rd-\kappa+\eta_{s+r}} (\widehat{P}/\widehat{M}^b)^{2sd} \Upsilon, \end{aligned}$$

where

$$\Upsilon = (\widehat{M}^{b-a+H})^{\kappa s/(s+r)} \widehat{M}^{-2sdH}.$$

Notice that $s \ge r\phi \ge \kappa$. Since $H \ge b - a$, we see that

$$\begin{aligned} &H\big(2s(d-1) + r - 1\big) + (b - a + H)\kappa s/(s+r) - 2sdH \\ &\quad \le H\big(-2s + r - 1 + 2\kappa s/(s+r)\big) \\ &\quad = -H + (-2s - r + r^2/s + 2\kappa) Hs/(s+r) \\ &\quad \le -H. \end{aligned}$$

Thus, we have

$$\widehat{P}^{\delta} \widehat{M}^{H(2s(d-1)+r-1)} \Upsilon \ll \widehat{M}^{-H/2}.$$

On combining the above estimates, the lemma follows. ∎

Lemma 3.5 *Let $a, b, H \in \mathbb{N}$ with $a < b$ and $H = b - a$. Suppose that $b + H \le \theta^{-1} - 1$. Then there exists $h \in \mathbb{N}$ with $h < H$ such that*

$$I_{a,b}(P) \ll \widehat{M}^{h(2s(d-1)+r-1)} K_{a,b+h}(P) + \widehat{M}^{-H/2} \big(\widehat{P}/\widehat{M}^b\big)^{2sd} \big(\widehat{P}/\widehat{M}^a\big)^{2rd-\kappa+\eta_{s+r}}.$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Proof By (3.1) and Lemma 3.4, the lemma follows. ∎

Lemma 3.6 *For $s = ru$ with $u \geq \phi$, we have $J_{s+r}(P) \ll \widehat{M}^{2sd} K_{0,1}(P)$.*

Proof For $\alpha \in \mathbb{K}_\infty^R$, define

$$\mathfrak{F}(\alpha) = \prod_{i=1}^{r} \mathfrak{f}_0(\alpha; \mathbf{0}) \quad \text{and} \quad I^*(P) = \int_{\mathbb{T}^R} \mathfrak{F}_0^{\mathbf{1}}(\alpha; \mathbf{0}) \mathfrak{F}(-\alpha) \big| \mathfrak{f}_0(\alpha; \mathbf{0}) \big|^{2s} d\alpha,$$

where $\mathbf{1} = (1, \ldots, 1) \in \Sigma_r$. Since the fixed $w \in \mathbb{A}$ satisfies all conditions in Lemma 2.2, we have

$$J_{s+r}(P) \ll I^*(P; w) = I^*(P).$$

By Cauchy's inequality, we obtain

$$I^*(P) \leq \Big(\int_{\mathbb{T}^R} \big| \mathfrak{F}(\alpha) \big|^2 \big| \mathfrak{f}_0(\alpha; \mathbf{0}) \big|^{2s} d\alpha \Big)^{1/2} \Big(\int_{\mathbb{T}^R} \big| \mathfrak{F}_0^{\mathbf{1}}(\alpha; \mathbf{0}) \big|^2 \big| \mathfrak{f}_0(\alpha; \mathbf{0}) \big|^{2s} d\alpha \Big)^{1/2}.$$

It follows from (2.1) that the first integral above is equal to $J_{s+r}(P)$. Thus, we have

$$J_{s+r}(P) \ll I_{0,0}^{\mathbf{1}}(P; \mathbf{0}, \mathbf{0}).$$

Notice that

$$\mathfrak{f}_0(\alpha; \mathbf{0}) = \sum_{\xi \in L(w)} \mathfrak{f}_1(\alpha; \xi).$$

By Hölder's inequality, we have

$$I_{0,0}^{\mathbf{1}}(P; \mathbf{0}, \mathbf{0}) \leq \langle w \rangle^{d(2s-1)} \sum_{\xi \in L(w)} \int_{\mathbb{T}^R} \big| \mathfrak{F}_0^{\mathbf{1}}(\alpha; \mathbf{0}) \big|^2 \big| \mathfrak{f}_1(\alpha; \xi) \big|^{2s} d\alpha,$$

which implies that

$$I_{0,0}^{\mathbf{1}}(P; \mathbf{0}, \mathbf{0}) \ll \langle w \rangle^{2sd} \max_{\xi \in L(w)} \int_{\mathbb{T}^R} \big| \mathfrak{F}_0^{\mathbf{1}}(\alpha; \mathbf{0}) \big|^2 \big| \mathfrak{f}_1(\alpha; \xi) \big|^{2s} d\alpha.$$

Since $\langle w \rangle = \widehat{M}$, we have

$$J_{s+r}(P) \ll I_{0,0}^{\mathbf{1}}(P; \mathbf{0}, \mathbf{0}) \ll \widehat{M}^{2sd} I_{0,1}(P).$$

When $a = 0$ and $b = 1$, we see that $H = b - a = 1$. Thus, by Lemma 3.5, we have

$$I_{0,1}(P) \ll K_{0,1}(P) + \widehat{M}^{-1/2} \big(\widehat{P} / \widehat{M} \big)^{2sd} \widehat{P}^{2rd - \kappa + \eta_{s+r}}.$$

By (2.4), δ is small enough such that $\widehat{M}^{1/2} > \widehat{P}^{2\delta}$. It follows that

$$J_{s+r}(P) \ll \widehat{M}^{2sd} I_{0,1}(P) \ll \widehat{M}^{2sd} K_{0,1}(P) + \widehat{P}^{2(s+r)d - \kappa + \eta_{s+r} - 2\delta}.$$

On the other hand, we see from (2.5) that

$$J_{s+r}(P) > \widehat{P}^{2(s+r)d - \kappa + \eta_{s+r} - \delta}.$$

Thus, we have

$$J_{s+r}(P) \ll \widehat{M}^{2sd} K_{0,1}(P) + \widehat{P}^{-\delta} J_{s+r}(P),$$

which implies that

$$J_{s+r}(P) \ll \widehat{M}^{2sd} K_{0,1}(P).$$

This completes the proof of the lemma. ∎

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

4 The Efficient Congruencing Process

The goal of this section is to provide an iterative relation among the mean values $K_{a,b}(P)$. Before proceeding, we need to estimate some auxiliary systems of congruences.

Proposition 4.1 *For $n, m \in \mathbb{N} \setminus \{0\}$, let $\Upsilon_1, \dots, \Upsilon_m$ be polynomials in $\mathbb{A}[z_1, \dots, z_n]$ with degrees $k_1, \dots, k_m$ in $\mathbf{z} = (z_1, \dots, z_n)$ respectively. Let $w \in \mathbb{A}$ be irreducible. For $l \in \mathbb{N} \setminus \{0\}$ and $\mathbf{a} = (a_1, \dots, a_m) \in \mathbb{A}^m$, let $\mathcal{D}_{l,m,n}(\Upsilon; \mathbf{a}; w)$ denote the set of solutions of the system of congruences*

$$\Upsilon_i(z_1, \dots, z_n) \equiv a_i \,(\mathrm{mod}\, w^l), \quad 1 \le i \le m,$$

with $z_l \in \mathbb{A}/(w^l)$, $1 \le l \le n$, and $\mathrm{rk}\,\mathrm{Jac}(\Upsilon; \mathbf{z}; w) = m$. Then we have

$$\mathrm{card}\, \mathcal{D}_{l,m,n}(\Upsilon; \mathbf{a}; w) \le C_4 \langle w^l \rangle^{n-m},$$

where $C_4 = \big(n!/(m!(n-m)!)\big)\, k_1 \cdots k_m$.

Proof It follows from similar arguments as in [11, Theorem 1]. For more details, see also [15, Appendix]. ∎

We recall that $J_s(\mathcal{R}; P)$ counts the number of solutions of the system

$$\mathbf{u}_1^{\mathbf{j}} + \cdots + \mathbf{u}_s^{\mathbf{j}} = \mathbf{v}_1^{\mathbf{j}} + \cdots + \mathbf{v}_s^{\mathbf{j}}, \quad \mathbf{j} \in \mathcal{R},$$

with $\mathbf{u}_j, \mathbf{v}_j \in I_P^d$, $1 \le j \le s$. It also represents the number of solutions of the system

$$\mathbf{u}_1^{\mathbf{i}} + \cdots + \mathbf{u}_s^{\mathbf{i}} = \mathbf{v}_1^{\mathbf{i}} + \cdots + \mathbf{v}_s^{\mathbf{i}}, \quad \mathbf{i} \in \mathcal{R}',$$

with $\mathbf{u}_j, \mathbf{v}_j \in I_P^d$, $1 \le j \le s$. Although the second system consists of independent equations, it does not necessarily contain all equations of certain auxiliary congruences that are used to well-condition variables. More precisely, since $\mathcal{R}'$ is not necessarily contained in $\mathcal{R}$, for any $g \in \mathbb{A} \setminus \{0\}$, the system of congruences

$$\mathbf{u}_1^{\mathbf{j}} + \cdots + \mathbf{u}_s^{\mathbf{j}} \equiv \mathbf{v}_1^{\mathbf{j}} + \cdots + \mathbf{v}_s^{\mathbf{j}} \,(\mathrm{mod}\, g), \quad \mathbf{j} \in \mathcal{R},$$

does not always imply that

$$\mathbf{u}_1^{\mathbf{i}} + \cdots + \mathbf{u}_s^{\mathbf{i}} \equiv \mathbf{v}_1^{\mathbf{i}} + \cdots + \mathbf{v}_s^{\mathbf{i}} \,(\mathrm{mod}\, g), \quad \mathbf{i} \in \mathcal{R}'.$$

To resolve the difficulty, we consider an alternative system. We recall that $\phi = \max_{\mathbf{i} \in \mathcal{R}'} |\mathbf{i}|$. Let

$$\mathcal{S} = \left\{ p^n \mathbf{i} \mid \mathbf{i} \in \mathcal{R}', \quad n \in \mathbb{N}, \quad \text{and} \quad p^n |\mathbf{i}| \le \phi \right\}.$$

In Lemma 4.2 we will prove that $\mathcal{S}$ satisfies Condition$*$. In addition, since $\mathcal{R}' \subseteq \mathcal{S}$, we see that the above system of congruence shares the same solutions with the system of congruences

$$\mathbf{u}_1^{\mathbf{j}} + \cdots + \mathbf{u}_s^{\mathbf{j}} \equiv \mathbf{v}_1^{\mathbf{j}} + \cdots + \mathbf{v}_s^{\mathbf{j}} \,(\mathrm{mod}\, g), \quad \mathbf{j} \in \mathcal{S}.$$

This equivalence is essential in our proof of Lemma 4.3.

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Lemma 4.2 *For each* $\mathbf{j} = (j_1, \dots, j_d) \in \mathcal{S}$, *if* $\mathbf{l} = (l_1, \dots, l_d) \in \mathbb{N}^d$ *with* $p \nmid \binom{j_1}{l_1} \cdots \binom{j_d}{l_d}$, *then* $\mathbf{l} \in \mathcal{S}$.

Proof Let $\mathbf{j} = (j_1, \dots, j_d) \in \mathcal{S}$. Then there exist $\mathbf{i} \in \mathcal{R}'$ and $n \in \mathbb{N}$ such that $\mathbf{j} = p^n\mathbf{i}$. Let $\mathbf{l} = (l_1, \dots, l_d) \in \mathbb{N}^d$ with $p \nmid \binom{j_1}{l_1} \cdots \binom{j_d}{l_d}$. By Lucas' criterion, we have

$$a_h(l_1) \le a_h(j_1), \dots, a_h(l_d) \le a_h(j_d), \quad h \in \mathbb{N}. \tag{4.1}$$

Since $a_h(j_1) = \cdots = a_h(j_d) = 0$, $0 \le h \le n-1$, we see from (4.1) that

$$a_h(l_1) = \cdots = a_h(l_d) = 0, \quad 0 \le h \le n-1.$$

It follows that $p^n | l_1, \dots, p^n | l_d$, *i.e.*, there exists $\mathbf{m} = (m_1, \dots, m_d) \in \mathbb{N}^d$ such that $\mathbf{l} = p^n\mathbf{m}$. Since $\mathbf{j} = p^n\mathbf{i}$ and $\mathbf{l} = p^n\mathbf{m}$, we obtain

$$a_{h+n}(j_1) = a_h(i_1), \dots, a_{h+n}(j_d) = a_h(i_d), \quad h \in \mathbb{N}$$

and

$$a_{h+n}(l_1) = a_h(m_1), \dots, a_{h+n}(l_d) = a_h(m_d) \quad h \in \mathbb{N}.$$

Then it follows from (4.1) that

$$a_h(m_1) \le a_h(i_1), \dots, a_h(m_d) \le a_h(i_d), \quad h \in \mathbb{N}.$$

Since $\mathbf{i} \in \mathcal{R}'$, there exists $\nu \in \mathbb{N}$ such that $p^\nu\mathbf{i} \in \mathcal{R}$. It follows from the above inequalities that

$$a_h(p^\nu m_1) \le a_h(p^\nu i_1), \dots, a_h(p^\nu m_d) \le a_h(p^\nu i_d), \quad h \in \mathbb{N},$$

which implies that

$$p \nmid \binom{p^\nu i_1}{p^\nu m_1} \cdots \binom{p^\nu i_d}{p^\nu m_d}.$$

In view of the property of $\mathcal{R}$, since $p^\nu\mathbf{i} \in \mathcal{R}$, we have $p^\nu\mathbf{m} \in \mathcal{R}$. Thus, there exist $\mathbf{u} \in \mathcal{R}'$ and $c \in \mathbb{N}$ such that $p^\nu\mathbf{m} = p^c\mathbf{u}$. Since $p \nmid \mathbf{u}$, we have $\nu \le c$ and $\mathbf{m} = p^{c-\nu}\mathbf{u}$. This implies that $\mathbf{l} = p^n\mathbf{m} = p^{n+c-\nu}\mathbf{u}$. On recalling (4.1), we have $|\mathbf{l}| \le |\mathbf{j}| \le \phi$ and hence $\mathbf{l} \in \mathcal{S}$. This completes the proof of the lemma. ∎

Let $\mathcal{R}_\mathbf{j}$ be defined as in Lemma 3.1. We remark that by Lemma 4.2, we have $\mathcal{R}_\mathbf{j} \subseteq \mathcal{S}$ for each $\mathbf{j} \in \mathcal{S}$.

Lemma 4.3 *Let* $a, b \in \mathbb{N}$ *with* $b > a$, *and let* $w \in \mathbb{A}$ *be irreducible. For* $\sigma \in \Sigma_r$, $\mathbf{m} = (m_\mathbf{i})_{\mathbf{i} \in \mathcal{R}'} \in \mathbb{A}^r$, $\xi \in L(w^a)$ *and* $\eta \in L(w^b)$, *let* $\mathcal{B}_{a,b}^\sigma(\mathbf{m}; \xi, \eta; w)$ *denote the set of solutions of the system of congruences*

$$\sum_{i=1}^{r} \sigma_i(\mathbf{z}_i - \eta)^\mathbf{i} \equiv m_\mathbf{i} \pmod{w^{|\mathbf{i}|b}}, \quad \mathbf{i} \in \mathcal{R}',$$

with $\mathbf{z}_i \in L(w^{\phi b})$ *and* $\mathbf{z}_i \equiv \xi_i \pmod{w^{a+1}}$, $1 \le i \le r$, *for some* $(\xi_1, \dots, \xi_r) \in \Xi_a(\xi; w)$. *Then we have*

$$\operatorname{card} \mathcal{B}_{a,b}^\sigma(\mathbf{m}; \xi, \eta; w) \le C_5 \langle w \rangle^{(r\phi d - \kappa)b + (\kappa - rd)a},$$

where $C_5 = ((rd)!/(r!(rd-r)!)) \prod_{\mathbf{i} \in \mathcal{R}'} |\mathbf{i}|$.

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Proof Let $\mathcal{D}_1(\mathbf{n})$ denote the set of solutions of the system of congruences

$$\sum_{i=1}^{r} \sigma_i(\mathbf{z}_i - \eta)^{\mathbf{i}} \equiv n_{\mathbf{i}} \,(\mathrm{mod}\, w^{\phi b}), \quad \mathbf{i} \in \mathcal{R}',$$

with $\mathbf{z}_i \in L(w^{\phi b})$ and $\mathbf{z}_i \equiv \xi_i \,(\mathrm{mod}\, w^{a+1})$, $1 \le i \le r$, for some $(\xi_1, \dots, \xi_r) \in \Xi_a(\xi; w)$. Define

$$\mathcal{N} = \left\{ \mathbf{n} = (n_{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'} \mid n_{\mathbf{i}} \in \mathbb{A},\ \deg n_{\mathbf{i}} < \deg w^{\phi b} \text{ and } n_{\mathbf{i}} \equiv m_{\mathbf{i}} \,(\mathrm{mod}\, w^{|\mathbf{i}|b}), \quad \mathbf{i} \in \mathcal{R}' \right\}.$$

By (2.2), we have

$$\mathrm{card}\, \mathcal{B}^{\sigma}_{a,b}(\mathbf{m}; \xi, \eta; w) \le \sum_{\mathbf{n} \in \mathcal{N}} \mathrm{card}\, \mathcal{D}_1(\mathbf{n}) \le \langle w \rangle^{(r\phi - \kappa)b} \max_{\mathbf{n} \in \mathcal{N}} \mathrm{card}\, \mathcal{D}_1(\mathbf{n}).$$

It remains to estimate $\mathcal{D}_1(\mathbf{n})$. Let $(\mathbf{z}_1, \dots, \mathbf{z}_r) \in \mathcal{D}_1(\mathbf{n})$ and write

$$\mathbf{z}_i = w^a \mathbf{h}_i + \xi, \quad 1 \le i \le r.$$

Since $\mathbf{z}_i \equiv \xi_i \,(\mathrm{mod}\, w^{a+1})$, $1 \le i \le r$, for some $(\xi_1, \dots, \xi_r) \in \Xi_a(\xi; w)$, we see that

$$w^{-a}(\mathbf{z}_i - \xi) \equiv w^{-a}(\xi_i - \xi) \,(\mathrm{mod}\, w).$$

Thus, we have

$$\mathrm{rk\,Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'}; \mathbf{h}_1, \dots, \mathbf{h}_r; w \right) = \mathrm{rk\,Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i} \in \mathcal{R}'}; [\xi_1], \dots, [\xi_r]; w \right) = r,$$

where $[\xi_i] = w^{-a}(\xi_i - \xi)$, $1 \le i \le r$. Let $(\mathbf{y}_1, \dots, \mathbf{y}_r) \in \mathcal{D}_1(\mathbf{n})$ and write $\mathbf{y}_i = w^a \mathbf{g}_i + \xi$, $1 \le i \le r$. We have

$$\sum_{i=1}^{r} \sigma_i(w^a \mathbf{h}_i + \xi - \eta)^{\mathbf{i}} \equiv \sum_{i=1}^{r} \sigma_i(w^a \mathbf{g}_i + \xi - \eta)^{\mathbf{i}} \,(\mathrm{mod}\, w^{\phi b}), \quad \mathbf{i} \in \mathcal{R}'.$$

Let $\mathcal{S}$ be defined as in Lemma 4.2. We see from the definition of $\mathcal{S}$ that the above system implies that

$$\sum_{i=1}^{r} \sigma_i(w^a \mathbf{h}_i + \xi - \eta)^{\mathbf{j}} \equiv \sum_{i=1}^{r} \sigma_i(w^a \mathbf{g}_i + \xi - \eta)^{\mathbf{j}} \,(\mathrm{mod}\, w^{\phi b}), \quad \mathbf{j} \in \mathcal{S}.$$

On combining Lemma 3.1 with Lemma 4.2, since $\mathcal{R}' \subseteq \mathcal{S}$, the above system implies that

$$\sum_{i=1}^{r} \sigma_i \mathbf{h}_i^{\mathbf{i}} \equiv \sum_{i=1}^{r} \sigma_i \mathbf{g}_i^{\mathbf{i}} \,(\mathrm{mod}\, w^{\phi b - |\mathbf{i}|a}), \quad \mathbf{i} \in \mathcal{R}'.$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

For $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'} \in \mathbb{A}^r$, we write $\mathcal{D}_2(\mathbf{u})$ for the set of solutions of the system of congruences

$$\sum_{i=1}^{r} \sigma_i \mathbf{h}_i^{\mathbf{i}} \equiv u_{\mathbf{i}} \,(\mathrm{mod}\, w^{\phi b-|\mathbf{i}|a}), \quad \mathbf{i} \in \mathcal{R}',$$

with $\mathbf{h}_i \in L(w^{\phi b-a})$ and $\mathrm{rk\,Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{h}_1, \dots, \mathbf{h}_r; w\right) = r$. Then it follows from the above argument that there exists some $\mathbf{u}$ such that $\mathrm{card}\,\mathcal{D}_1(\mathbf{n}) \le \mathrm{card}\,\mathcal{D}_2(\mathbf{u})$. Define

$$\mathcal{V} = \left\{\mathbf{v} = (v_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'} \mid v_{\mathbf{i}} \in \mathbb{A}, \deg v_{\mathbf{i}} < \deg w^{\phi b-a} \text{ and } v_{\mathbf{i}} \equiv u_{\mathbf{i}} (\mathrm{mod}\, w^{\phi b-|\mathbf{i}|a}) (\mathbf{i} \in \mathcal{R}')\right\}.$$

For $\mathbf{v} \in \mathcal{V}$, denote by $\mathcal{D}_3(\mathbf{v})$ the set of solutions of the system of congruences

$$\sum_{i=1}^{r} \sigma_i \mathbf{h}_i^{\mathbf{i}} \equiv v_{\mathbf{i}} \,(\mathrm{mod}\, w^{\phi b-a}), \quad \mathbf{i} \in \mathcal{R}',$$

with $\mathbf{h}_i \in L(w^{\phi b-a})$ and $\mathrm{rk\,Jac}\left((\mathbf{x}^{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}; \mathbf{h}_1, \dots, \mathbf{h}_r; w\right) = r$. Thus, we have

$$\mathrm{card}\,\mathcal{D}_2(\mathbf{u}) \le \langle w\rangle^{(\kappa-r)a} \max_{\mathbf{v}\in\mathcal{V}} \mathrm{card}\,\mathcal{D}_3(\mathbf{v}).$$

By Proposition 4.1, we have

$$\mathrm{card}\,\mathcal{D}_3(\mathbf{v}) \le C_5 \langle w^{\phi b-a}\rangle^{rd-r},$$

where $C_5 = ((rd)!/(r!(rd-r)!)) \prod_{\mathbf{i}\in\mathcal{R}'} |\mathbf{i}|$. On combining the above estimates we have

$$\mathrm{card}\,\mathcal{B}_{a,b}^{\sigma}(\mathbf{m}; \xi, \eta; w) \le C_5 \langle w\rangle^{(r\phi-\kappa)b+(\kappa-r)a+(\phi b-a)(rd-r)} = C_5 \langle w\rangle^{(r\phi d-\kappa)b+a(\kappa-rd)}.$$

This completes the proof of the lemma. ∎

Lemma 4.4 *Let $a, b \in \mathbb{N}$ with $a < b \le \theta^{-1} - 1$. We have*

$$K_{a,b}(P) \ll \widehat{M}^{(r\phi d-\kappa)b+a(\kappa-rd)} \widehat{M}^{(\phi b-a)dr} \left(J_{s+r}(P - bM)\right)^{1-r/s} \left(I_{b,\phi b}(P)\right)^{r/s}.$$

Proof For $\xi \in L(w^a)$, $\eta \in L(w^b)$ and $\sigma, \tau \in \Sigma_r$, we see from (2.1) that $K_{a,b}^{\sigma,\tau}(P; \xi, \eta)$ counts the number of solutions of the system

$$\sum_{i=1}^{r} \sigma_i \left(\mathbf{y}_i^{\mathbf{j}} - \mathbf{z}_i^{\mathbf{j}}\right) = \sum_{l=1}^{u} \sum_{m=1}^{r} \tau_m \left(\mathbf{u}_{l,m}^{\mathbf{j}} - \mathbf{v}_{l,m}^{\mathbf{j}}\right), \quad \mathbf{j} \in \mathcal{R}, \tag{4.2}$$

with

$$\mathbf{y}_i, \mathbf{z}_i \in I_P^d, \quad \mathbf{y}_i \equiv \xi_i \,(\mathrm{mod}\, w^{a+1}), \quad \mathbf{z}_i \equiv \gamma_i \,(\mathrm{mod}\, w^{a+1}) \quad (1 \le i \le r)$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

for some $(\xi_1,\dots,\xi_r)$, $(\gamma_1,\dots,\gamma_r)\in \Xi_a(\xi;w)$, and with

$$\mathbf{u}_{l,m},\mathbf{v}_{l,m}\in I_P^d,\quad \mathbf{u}_{l,m}\equiv \eta_{l,m}\,(\mathrm{mod}\, w^{b+1}),$$
$$\mathbf{v}_{l,m}\equiv \nu_{l,m}(\mathrm{mod}\, w^{b+1}),\quad 1\le l\le u,\ 1\le m\le r,$$

for some $(\eta_{l,1},\dots,\eta_{l,r})$, $(\nu_{l,1},\dots,\nu_{l,r})\in \Xi_b(\eta;w)$. On combining Lemma 3.1 with Condition$*$, we see that (4.2) is equivalent to the system

$$\sum_{i=1}^{r}\sigma_i\big((\mathbf{y}_i-\eta)^{\mathbf{j}}-(\mathbf{z}_i-\eta)^{\mathbf{j}}\big)=\sum_{l=1}^{u}\sum_{m=1}^{r}\tau_m\big((\mathbf{u}_{l,m}-\eta)^{\mathbf{j}}-(\mathbf{v}_{l,m}-\eta)^{\mathbf{j}}\big),\quad \mathbf{j}\in\mathcal{R}.$$

Then by the definition of $\mathcal{R}'$, it follows that

$$\sum_{i=1}^{r}\sigma_i\big((\mathbf{y}_i-\eta)^{\mathbf{i}}-(\mathbf{z}_i-\eta)^{\mathbf{i}}\big)=\sum_{l=1}^{u}\sum_{m=1}^{r}\tau_m\big((\mathbf{u}_{l,m}-\eta)^{\mathbf{i}}-(\mathbf{v}_{l,m}-\eta)^{\mathbf{i}}\big),\quad \mathbf{i}\in\mathcal{R}'.$$

Given a solution $(\mathbf{y}_i,\mathbf{z}_i,\mathbf{u}_{l,m},\mathbf{v}_{l,m})$, $1\le i\le r$, $1\le l\le u$, $1\le m\le r$, counted by $K_{a,b}^{\sigma,\tau}(P;\xi,\eta)$, we have $\mathbf{u}_{l,m}\equiv\mathbf{v}_{l,m}\equiv\eta\,(\mathrm{mod}\, w^b)$. Thus, the above system implies that

$$\sum_{i=1}^{r}\sigma_i(\mathbf{y}_i-\eta)^{\mathbf{i}}\equiv\sum_{i=1}^{r}\sigma_i(\mathbf{z}_i-\eta)^{\mathbf{i}}\,(\mathrm{mod}\, w^{|\mathbf{i}|b}),\quad \mathbf{i}\in\mathcal{R}'. \tag{4.3}$$

Let $\mathcal{B}(\mathbf{m})=\mathcal{B}_{a,b}^{\sigma}(\mathbf{m};\xi,\eta;w)$ be defined as in Lemma 4.3. Write

$$\mathfrak{G}_{a,b}^{\sigma}(\alpha;\xi,\eta;\mathbf{m})=\sum_{(\zeta_1,\dots,\zeta_r)\in\mathcal{B}(\mathbf{m})}\prod_{i=1}^{r}\mathfrak{f}_{\phi b}(\sigma_i\alpha;\zeta_i).$$

Notice that for each $\mathbf{m}=(m_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}'}\in\mathbb{A}^r$, the integral

$$\int_{\mathbb{T}^R}\big|\,\mathfrak{G}_{a,b}^{\sigma}(\alpha;\xi,\eta;\mathbf{m})^2\mathfrak{F}_b^{\tau}(\alpha;\eta)^{2u}\big|\,d\alpha$$

denotes the number of solutions $(\mathbf{y}_i,\mathbf{z}_i,\mathbf{u}_{l,m},\mathbf{v}_{l,m})$, $1\le i\le r$, $1\le l\le u$, $1\le m\le r$, counted by $K_{a,b}^{\sigma,\tau}(P;\xi,\eta)$ in which $(\mathbf{y}_1,\dots,\mathbf{y}_r)\,(\mathrm{mod}\, w^{\phi b})$ and $(\mathbf{z}_1,\dots,\mathbf{z}_r)\,(\mathrm{mod}\, w^{\phi b})$ lie in $\mathcal{B}(\mathbf{m})$. Thus, by (4.3), we have

$$K_{a,b}^{\sigma,\tau}(P;\xi,\eta)\le\sum_{\substack{\deg m_{\mathbf{i}}<\deg w^{|\mathbf{i}|b}\\ \mathbf{i}\in\mathcal{R}'}}\int_{\mathbb{T}^R}\big|\,\mathfrak{G}_{a,b}^{\sigma}(\alpha;\xi,\eta;\mathbf{m})^2\mathfrak{F}_b^{\tau}(\alpha;\eta)^{2u}\big|\,d\alpha.$$

By Lemma 4.3 and Cauchy's inequality, we have

$$\begin{aligned}\big|\,\mathfrak{G}_{a,b}^{\sigma}(\alpha;\xi,\eta;\mathbf{m})\big|^2&\le \operatorname{card}\mathcal{B}(\mathbf{m})\sum_{(\zeta_1,\dots,\zeta_r)\in\mathcal{B}(\mathbf{m})}\prod_{i=1}^{r}\big|\,\mathfrak{f}_{\phi b}(\alpha;\zeta_i)\big|^2\\&\ll \widehat{M}^{(r\phi d-\kappa)b+(\kappa-rd)a}\sum_{(\zeta_1,\dots,\zeta_r)\in\mathcal{B}(\mathbf{m})}\prod_{i=1}^{r}\big|\,\mathfrak{f}_{\phi b}(\alpha;\zeta_i)\big|^2.\end{aligned}$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

It follows that

$$\begin{aligned}
&K_{a,b}^{\sigma,\tau}(P;\xi,\eta)\\
&\ll \widehat{M}^{(r\phi d-\kappa)b+(\kappa-rd)a} \sum_{\substack{\deg m_{\mathbf{i}}<\deg w^{|\mathbf{i}|b}\\ \mathbf{i}\in\mathcal{R}'}} \sum_{(\zeta_1,\dots,\zeta_r)\in\mathcal{B}(\mathbf{m})} \int_{\mathbb{T}^R}\\
&\qquad \Big(\prod_{i=1}^{r}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta_i)\big|^2\Big)\big|\mathfrak{F}_b^{\tau}(\alpha;\eta)\big|^{2u}d\alpha\\
&\ll \widehat{M}^{(r\phi d-\kappa)b+(\kappa-rd)a} \sum_{\substack{\zeta_i\in L(w^{\phi b})\\ \zeta_i\equiv\xi \pmod{w^a}\\ 1\le i\le r}} \int_{\mathbb{T}^R}\Big(\prod_{i=1}^{r}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta_i)\big|^2\Big)\big|\mathfrak{F}_b^{\tau}(\alpha;\eta)\big|^{2u}d\alpha.
\end{aligned}$$

By Hölder's inequality, we see that

$$\begin{aligned}
\sum_{\substack{\zeta_i\in L(w^{\phi b})\\ \zeta_i\equiv\xi \pmod{w^a}\\ 1\le i\le r}}\prod_{i=1}^{r}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta_i)\big|^2 &= \Big(\sum_{\substack{\zeta\in L(w^{\phi b})\\ \zeta\equiv\xi \pmod{w^a}}}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta)\big|^2\Big)^r\\
&\le \langle w\rangle^{d(\phi b-a)(r-1)}\sum_{\substack{\zeta\in L(w^{\phi b})\\ \zeta\equiv\xi \pmod{w^a}}}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta)\big|^{2r}.
\end{aligned}$$

Thus, we have

$$K_{a,b}^{\sigma,\tau}(P;\xi,\eta) \ll \widehat{M}^{(r\phi d-\kappa)b+(\kappa-rd)a}\widehat{M}^{rd(\phi b-a)}\max_{\zeta\in L(w^{\phi b})}\int_{\mathbb{T}^R}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta)^{2r}\mathfrak{F}_b^{\tau}(\alpha;\eta)^{2u}\big|\,d\alpha. \tag{4.4}$$

On recalling that $s = ru$, it follows from Hölder's inequality that

$$\int_{\mathbb{T}^R}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta)^{2r}\mathfrak{F}_b^{\tau}(\alpha;\eta)^{2u}\big|\,d\alpha \le U_1^{1-r/s}U_2^{r/s},$$

where

$$U_1 = \int_{\mathbb{T}^R}\big|\mathfrak{F}_b^{\tau}(\alpha;\eta)\big|^{2u+2}d\alpha \qquad \text{and} \qquad U_2 = \int_{\mathbb{T}^R}\big|\mathfrak{F}_b^{\tau}(\alpha;\eta)^2\mathfrak{f}_{\phi b}(\alpha;\zeta)^{2s}\big|\,d\alpha.$$

On considering the underlying Diophantine system, we can deduce from Lemma 3.2 that

$$U_1 \le \int_{\mathbb{T}^R}\big|\mathfrak{f}_b(\alpha;\eta)\big|^{2s+2r}d\alpha \ll J_{s+r}(P-bM).$$

On noticing that $U_2 = I_{b,\phi b}^{\tau}(P;\eta,\xi)$, we have

$$\int_{\mathbb{T}^R}\big|\mathfrak{f}_{\phi b}(\alpha;\zeta)^{2r}\mathfrak{F}_b^{\tau}(\alpha;\eta)^{2u}\big|\,d\alpha \le \big(J_{s+r}(P-bM)\big)^{1-r/s}\big(I_{b,\phi b}(P)\big)^{r/s}.$$

On combing the above estimate with (4.4), the lemma follows. ∎

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

For $a, b \in \mathbb{N}$ with $a < b$, we define the normalised magnitude of $K_{a,b}(P)$ as follows:

$$[\![K_{a,b}(P)]\!] = K_{a,b}(P)(\widehat{P}/\widehat{M}^b)^{-2sd}(\widehat{P}/\widehat{M}^a)^{\kappa-2rd}.$$

Lemma 4.5 *Let $a, b \in \mathbb{N}$ with $a < b \le \theta^{-1} - 1$. We have*

$$[\![K_{a,b}(P)]\!] \ll \widehat{P}^{\eta_{s+r}+\delta}(\widehat{M}^{b-a})^{\kappa}.$$

Proof For $\xi \in L(w^a)$, $\eta \in L(w^b)$ and $\sigma, \tau \in \Sigma_r$, on considering the underlying Diophantine system, we see from Hölder's inequality that

$$\begin{aligned} K_{a,b}^{\sigma,\tau}(P;\xi,\eta) &\le \int_{\mathbb{T}^R} \big|\mathfrak{f}_a(\alpha;\xi)^{2r}\mathfrak{f}_b(\alpha;\eta)^{2s}\big|\,d\alpha \\ &\le \Big(\int_{\mathbb{T}^R} \big|\mathfrak{f}_a(\alpha;\xi)\big|^{2(s+r)}d\alpha\Big)^{r/(s+r)}\Big(\int_{\mathbb{T}^R} \big|\mathfrak{f}_b(\alpha;\eta)\big|^{2(s+r)}d\alpha\Big)^{s/(s+r)}. \end{aligned}$$

Since $a < b \le \theta^{-1} - 1$, by Lemma 3.2, we have

$$K_{a,b}(P) \le \big(J_{s+r}(P - aM)\big)^{r/(s+r)}\big(J_{s+r}(P - bM)\big)^{s/(s+r)}.$$

Thus, it follows from (2.6) that

$$\begin{aligned} [\![K_{a,b}(P)]\!] &= K_{a,b}(P)(\widehat{P}/\widehat{M}^b)^{-2sd}(\widehat{P}/\widehat{M}^a)^{\kappa-2rd} \\ &\ll \widehat{P}^{\delta}\big((\widehat{P}/\widehat{M}^a)^{r/(s+r)}(\widehat{P}/\widehat{M}^b)^{s/(s+r)}\big)^{2(s+r)d-\kappa+\eta_{s+r}}(\widehat{P}/\widehat{M}^b)^{-2sd}(\widehat{P}/\widehat{M}^a)^{\kappa-2rd} \\ &\ll \widehat{P}^{\eta_{s+r}+\delta}(\widehat{M}^{b-a})^{\kappa s/(s+r)}. \end{aligned}$$

This completes the proof of the lemma. ∎

Lemma 4.6 *Let $a, b, H \in \mathbb{N}$ with $a < b \le (2\phi\theta)^{-1}$ and $H = (\phi - 1)b$. Then there exists $h \in \mathbb{N}$ with $h < H$ such that*

$$[\![K_{a,b}(P)]\!] \ll \big(\widehat{P}/\widehat{M}^b\big)^{\eta_{s+r}}\widehat{M}^{-rH/(3s)} + \widehat{P}^{\delta}\widehat{M}^{-(2s-r+1)hr/s}\big(\widehat{P}/\widehat{M}^b\big)^{\eta_{s+r}(1-r/s)}[\![K_{b,\phi b+h}(P)]\!]^{r/s}.$$

Proof It follows from Lemma 4.4 that

$$\begin{aligned} [\![K_{a,b}(P)]\!] &= K_{a,b}(P)(\widehat{P}/\widehat{M}^b)^{-2sd}(\widehat{P}/\widehat{M}^a)^{\kappa-2rd} \\ &\ll (\widehat{M}^b)^{2sd}(\widehat{M}^a)^{2rd-\kappa}\widehat{M}^{(r\phi d-\kappa)b+(\kappa-rd)a}\widehat{M}^{(\phi b-a)dr}V_1^{1-r/s}V_2^{r/s}, \end{aligned}$$

where

$$V_1 = J_{s+r}(P - bM)\widehat{P}^{\kappa-2(s+r)d} \quad \text{and} \quad V_2 = I_{b,\phi b}(P)\widehat{P}^{\kappa-2(s+r)d}.$$

By (2.6), we see that

$$V_1 < \widehat{P}^{\delta}(\widehat{M}^{-b})^{2(s+r)d-\kappa}(\widehat{P}/\widehat{M}^b)^{\eta_{s+r}}.$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Since $H = (\phi - 1)b$, we have

$$\phi b + H = \phi b + (\phi - 1)b \leq 2\phi b - 1 \leq \theta^{-1} - 1.$$

It follows from Lemma 3.5 that there exists $h \in \mathbb{N}$ with $h < H$ such that

$$V_2 \ll \widehat{M}^{h(2s(d-1)+r-1)} K_{b,\phi b+h}(P) \widehat{P}^{\kappa-2(s+r)d} + \widehat{M}^{-H/2} \big(\widehat{P}/\widehat{M}^{b\phi}\big)^{2sd} \big(\widehat{P}/\widehat{M}^{b}\big)^{2rd-\kappa+\eta_{s+r}} \widehat{P}^{\kappa-2(s+r)d}.$$

Thus, we have

$$V_2 \ll \big(\widehat{M}^{-\phi b}\big)^{2sd} \big(\widehat{M}^{-b}\big)^{2rd-\kappa} V_3,$$

where

$$V_3 = \widehat{M}^{h(-2s+r-1)} [\![K_{b,\phi b+h}(P)]\!] + \widehat{M}^{-H/2} \big(\widehat{P}/\widehat{M}^{b}\big)^{\eta_{s+r}}.$$

On combining the above upper bounds for $[\![K_{a,b}(P)]\!]$, V_1 and V_2, we have

$$[\![K_{a,b}(P)]\!] \ll \widehat{M}^{\Omega} \widehat{P}^{\delta} \big(\widehat{P}/\widehat{M}^{b}\big)^{(\eta_{s+r})(1-r/s)} V_3^{r/s},$$

where

$$\Omega = b(2sd) + a(2rd - \kappa) + (r\phi d - \kappa)b + (\kappa - rd)a + (\phi b - a)dr + (-b)\big(2(s+r)d - \kappa\big)(1 - r/s) + \big(- (\phi b)(2sd) - b(2rd - \kappa)\big)(r/s).$$

A straightforward computation shows that $\Omega = 0$. Thus, we obtain

$$[\![K_{a,b}(P)]\!] \ll \widehat{P}^{\delta} \big(\widehat{P}/\widehat{M}^{b}\big)^{\eta_{s+r}} \big(\widehat{M}^{-H/2}\big)^{r/s} + \widehat{P}^{\delta} \widehat{M}^{(-2s+r-1)hr/s} \big(\widehat{P}/\widehat{M}^{b}\big)^{\eta_{s+r}(1-r/s)} [\![K_{b,\phi b+h}(P)]\!]^{r/s}.$$

By (2.4), we have $\delta < \theta/(6s)$ and hence $\widehat{P}^{\delta} < \widehat{M}^{rH/(6s)}$. Thus, we have

$$[\![K_{a,b}(P)]\!] \ll \big(\widehat{P}/\widehat{M}^{b}\big)^{\eta_{s+r}} \widehat{M}^{-rH/(3s)} + \widehat{P}^{\delta} \widehat{M}^{-(2s-r+1)hr/s} \big(\widehat{P}/\widehat{M}^{b}\big)^{\eta_{s+r}(1-r/s)} [\![K_{b,\phi b+h}(P)]\!]^{r/s}.$$

This completes the proof of the lemma. ∎

5 Proof of Theorem 1.1

We begin by establishing the following iterative process.

Lemma 5.1 *Let $a, b \in \mathbb{N}$ with $a < b \leq (2\phi\theta)^{-1}$. Suppose that there exist $\psi \geq 0$, $\gamma \geq 0$, and $c \geq 0$ with $c \leq (2s/r)^N$ such that*

$$\widehat{P}^{\eta_{s+r}(1+\psi\theta)} \ll \widehat{P}^{c\delta} \widehat{M}^{-\gamma} [\![K_{a,b}(P)]\!].$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Then there exists $h \in \mathbb{N}$ with $h \le (\phi-1)b$ such that

$$\widehat{P}^{\eta_{s+r}(1+\psi'\theta)} \ll \widehat{P}^{c'\delta}\widehat{M}^{-\gamma'}[[K_{a',b'}(P)]],$$

where

$$\psi' = (s/r)\psi + (s/r-1)b, \qquad c' = (s/r)(c+1), \qquad \gamma' = (s/r)\gamma + (2s-r+1)h,$$

$$a' = b \quad \text{and} \quad b' = \phi b + h.$$

Proof By Lemma 4.6, there exists $h \in \mathbb{N}$ with $h < (\phi-1)b$ such that

$$[[K_{a,b}(P)]] \ll \widehat{P}^{\eta_{s+r}}\widehat{M}^{-1/(3s)} + \widehat{P}^{\delta}\widehat{M}^{-(2s-r+1)hr/s}\big(\widehat{P}/\widehat{M}^{b}\big)^{\eta_{s+r}(1-r/s)}[[K_{b,\phi b+h}(P)]]^{r/s}.$$

Since $\theta = N^{-1/2}(r/s)^{N+2}$, by (2.4), we have $c\delta < \theta/(6s)$ and hence $\widehat{P}^{c\delta} < \widehat{M}^{1/(6s)}$. We also have $\delta < \theta/(6s)$ and hence $\widehat{P}^{\delta} < \widehat{M}^{1/(6s)}$. Then by the hypothesis on $\widehat{P}^{\eta_{s+r}(1+\psi\theta)}$, we see that

$$\widehat{P}^{\eta_{s+r}(1+\psi\theta)} \ll \widehat{P}^{\eta_{s+r}-\delta} + \widehat{P}^{(c+1)\delta}\widehat{M}^{-\gamma-(2s-r+1)hr/s}\big(\widehat{P}/\widehat{M}^{b}\big)^{\eta_{s+r}(1-r/s)}[[K_{b,\phi b+h}(P)]]^{r/s}.$$

Thus, we have

$$\widehat{P}^{\eta_{s+r}(r/s+(\psi+(1-r/s)b)\theta)} \ll \widehat{P}^{(c+1)\delta}\widehat{M}^{-\gamma-(2s-r+1)hr/s}[[K_{b,\phi b+h}(P)]]^{r/s},$$

which implies that

$$\widehat{P}^{\eta_{s+r}(1+\psi'\theta)} \ll \widehat{P}^{c'\delta}\widehat{M}^{-\gamma'}[[K_{b,\phi b+h}(P)]].$$

This completes the proof of the lemma. ∎

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1 We recall that to prove the theorem, it suffices to show that for $d \ge 2$, $\phi \ge 2$, and $s \ge r\phi$, we have $\eta_{s+r} = 0$. By (2.3), we have $\eta_{s+r} \ge 0$ for $s \ge r\phi$.

We first consider the cases that $s = ru$ with $u \in \mathbb{N}$ and $u \ge \phi$. Suppose that $\eta_{s+r} > 0$. Define the sequences of non-negative integers $(a_n)_{n=0}^{N}$ and $(b_n)_{n=0}^{N}$ by setting $a_0 = 0$ and $b_0 = 1$. Then for $0 \le n < N$, we fix $h_n \in \mathbb{N}$ (which will be chosen later) with $h_n \le (\phi-1)b_n$ and define

$$a_{n+1} = b_n \quad \text{and} \quad b_{n+1} = \phi b_n + h_n.$$

We now define the auxiliary sequences of non-negative real numbers $(\psi_n)_{n=0}^{N}$, $(c_n)_{n=0}^{N}$, $(\gamma_n)_{n=0}^{N}$ by setting $\psi_0 = 0$, $c_0 = 1$ and $\gamma_0 = 0$. Then for $0 \le n < N$, we define

$$\psi_{n+1} = (s/r)\psi_n + (s/r-1)b_n, \quad c_{n+1} = (s/r)(c_n+1), \quad \gamma_{n+1} = (s/r)\gamma_n + (2s-r+1)h_n.$$

The above sequences satisfy the following properties.

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Claim

(a) $\psi_n \geq n(\phi-1)\phi^{n-1}$, $0 \leq n \leq N$.
(b) $c_n \leq (n+1)(s/r)^n$, $0 \leq n \leq N$.
(c) $\gamma_n \geq (2s-r+1)(b_n-\phi^n)$, $0 \leq n \leq N$.
(d) For N sufficiently large (in terms of s and r), there exists a sequence (h_n) such that for $0 \leq n \leq N$, we have

$$b_n < \sqrt{N}(s/r)^n \tag{5.1}$$

and

$$\widehat{P}^{\eta_{s+r}(1+\psi_n\theta)} \ll \widehat{P}^{c_n\delta}\widehat{M}^{-\gamma_n}[[K_{a_n,b_n}(P)]]. \tag{5.2}$$

Proof of the Claim (a) Notice that $b_n \geq \phi^n$, $0 \leq n \leq N$. Since $s \geq r\phi$, we have

$$\psi_{n+1} \geq \phi\psi_n + (\phi-1)b_n \geq \phi\psi_n + (\phi-1)\phi^n.$$

By induction, the result follows.

(b) The upper bounds follow from a straightforward inductive argument.

(c) Since $b_{n+1} = \phi b_n + h_n$, we see that

$$\gamma_{n+1} - (s/r)\gamma_n = (2s-r+1)(b_{n+1} - \phi b_n).$$

On recalling that $s/r \geq \phi$, we have

$$\gamma_{n+1} - (2s-r+1)b_{n+1} = (s/r)\gamma_n - \phi(2s-r+1)b_n \geq \phi\big(\gamma_n - (2s-r+1)b_n\big).$$

Since $b_0 = 1$ and $\gamma_0 = 0$, it follows by induction that

$$\gamma_n \geq (2s-r+1)b_n + \phi^n\big(\gamma_0 - (2s-r+1)b_0\big) = (2s-r+1)\big(b_n - \phi^n\big), \quad 0 \leq n \leq N.$$

(d) We now apply an inductive argument on (5.1) and (5.2) simultaneously. Recall that $a_0 = 0$, $b_0 = 1$, $\psi_0 = 0$, $c_0 = 1$, and $\gamma_0 = 0$. On combining (2.3) with Lemma 3.6, we have

$$\widehat{P}^{\eta_{s+r}} < \widehat{P}^{\delta-2(s+r)d+\kappa}J_{s+r}(P) \ll \widehat{P}^{\delta-2(s+r)d+\kappa}\widehat{M}^{2sd}K_{0,1}(P) = \widehat{P}^{\delta}[[K_{0,1}(P)]].$$

Thus, (5.2) is true for $n = 0$. We notice that (5.1) is also true for $n = 0$ as $b_0 = 1$. Suppose that (5.1) and (5.2) are true for n with $0 \leq n < N$. By Claim (b), we have $c_n < (2s/r)^n$. On recalling that $\theta = N^{-1/2}(r/s)^{N+2}$, we see from the hypothesis of (5.1) that

$$\phi b_n\theta \leq \phi(s/r)^{-N-2+n} < \phi^{-1} \leq 1/2,$$

which implies that $b_n \leq (2\phi\theta)^{-1}$. Thus, it follows from Lemma 5.1 and the hypothesis of (5.2) that there exists $h \in \mathbb{N}$ with $h < (\phi-1)b_n$ such that

$$\widehat{P}^{\eta_{s+r}(1+\psi'\theta)} \ll \widehat{P}^{c'\delta}\widehat{M}^{-\gamma'}[[K_{a',b'}(P)]], \tag{5.3}$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

where

$$\psi' = (s/r)\psi_n + (s/r-1)b_n, \quad c' = (s/r)(c_n+1), \quad \gamma' = (s/r)\gamma_n + (2s-r+1)h,$$
$$a' = b_n \quad \text{and} \quad b' = \phi b_n + h.$$

Notice that $\psi' = \psi_{n+1}$, $c' = c_{n+1}$, and $a' = a_{n+1}$. By taking $h_n = h$, we also have $\gamma' = \gamma_{n+1}$ and $b' = b_{n+1}$. Thus, we see from (5.3) that (5.2) is true for $n+1$. We now consider (5.1) for $n+1$, with $h_n = h$ chosen as above. Suppose that $b_{n+1} \geq \sqrt{N}(s/r)^{n+1}$. Since $s/r \geq \phi$, we see from Claim (c) that

$$\begin{aligned}
\gamma_{n+1} &= (s/r)\gamma_n + (2s-r+1)(b_{n+1} - \phi b_n) \\
&\geq (s/r)\big((2s-r+1)b_n - (2s-r+1)(s/r)^n\big) + (2s-r+1)\big(b_{n+1} - (s/r)b_n\big) \\
&\geq (2s-r+1)\big(b_{n+1} - (s/r)^{n+1}\big) \\
&\geq (2s-r+1)(1-1/\sqrt{N})b_{n+1}.
\end{aligned}$$

Since

$$b_{n+1} = \phi b_n + h \leq 2\phi b_n - 1 \leq \theta^{-1} - 1,$$

it follows from Lemma 4.5 that

$$[\![K_{a_{n+1},b_{n+1}}(P)]\!] \ll \widehat{P}^{\eta_{s+r}+\delta}(\widehat{M}^{b_{n+1}})^{\kappa}.$$

Thus, we see from (5.3) that

$$\widehat{P}^{\eta_{s+r}(1+\psi_{n+1}\theta)} \ll \widehat{P}^{\eta_{s+r}+(c_{n+1}+1)\delta}\big(\widehat{M}^{b_{n+1}}\big)^{\kappa-(2s-r+1)(1-1/\sqrt{N})}.$$

Since $\kappa \leq r\phi \leq s$ and $\phi \geq 2$, we have

$$\begin{aligned}
\kappa - (2s-r+1)(1-1/\sqrt{N}) &\leq s - (2s-r+1) + (2s-r+1)/\sqrt{N} \\
&= -s + r - 1 + (2s-r+1)/\sqrt{N}.
\end{aligned}$$

Thus, when N is sufficiently large, we obtain

$$\kappa - (2s-r+1)(1-1/\sqrt{N}) < -1.$$

By Claim (b), we see from (2.4) that δ is small enough such that $(c_{n+1}+1)\delta < \theta/2$ and hence

$$\widehat{P}^{\eta_{s+r}\psi_{n+1}\theta} \ll \widehat{P}^{-\theta b_{n+1}/2}.$$

Since $\psi_{n+1} > 0$, $\theta > 0$ and $b_{n+1} > 0$, the above inequality implies that $\eta_{s+r} = 0$, which leads to a contradiction. Thus, we conclude that $b_{n+1} < \sqrt{N}(s/r)^{n+1}$ and hence (5.1) is also true for $n+1$. This completes the proof of Claim (d). ∎

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

Since $\theta = N^{-1/2}(r/s)^{N+2}$ and $r/s \le 1/\phi \le 1/2$, by Claim (d), we see that $b_N\theta < (r/s)^2 < 1-\theta$ and hence $b_N \le \theta^{-1} - 1$. Since $b_N \ge \phi^N$, it follows from Claim (c) that $\gamma_N \ge 0$. By Claim (d) and Lemma 4.5, for N is sufficiently large, we have

$$\widehat{P}^{\eta_{s+r}(1+\psi_N\theta)} \ll \widehat{P}^{\eta_{s+r}+(c_N+1)\delta}\widehat{M}^{b_N\kappa} \ll \widehat{P}^{\eta_{s+r}+r\phi}.$$

By Claim (a), we have

$$\eta_{s+r} \le r\phi/(\psi_N\theta) \le r\phi/(N(\phi-1)\phi^{N-1}\theta).$$

In particular, on taking $s = r\phi$, we see that $\theta = N^{-1/2}\phi^{-N-2}$ and hence

$$\eta_{r\phi+r} \le r\phi^{N+3}/(\sqrt{N}(\phi-1)\phi^{N-1}) \le r\phi^4/\sqrt{N}.$$

Since we can take N as large as possible (in terms of s and r), we have $\eta_{r\phi+r} = 0$.

We now consider general $s \in \mathbb{N}$ with $s \ge r\phi$. By the trivial bound $|f(\alpha;P)| \le \widehat{P}^d$, we have

$$J_{s+r}(P) \le \widehat{P}^{2(s-r\phi)d}\int_{\mathbb{T}^R} |f(\alpha;P)|^{2(r\phi+r)d}d\alpha = \widehat{P}^{2(s-r\phi)d}J_{r\phi+r}(P),$$

which implies that $\eta_{s+r} \le \eta_{r\phi+r}$ for $s \ge r\phi$. Thus, $\eta_{s+r} = 0$ for $s \ge r\phi$. This completes the proof of the theorem. ∎

6 Proof of Theorem 1.3

Let $k \in \mathbb{N}$ with $p \nmid k$, and let $\mathcal{L}$ and $\mathcal{R}_0'$ be defined as in Section 1. We write $\iota = \operatorname{card}\mathcal{L}$ and $\mu = \operatorname{card}\mathcal{R}_0'$.

Lemma 6.1 *For $k \ge 2$, $\alpha = (\alpha_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}_0'} \in \mathbb{K}_\infty^\mu$ and $P \in \mathbb{N}\setminus\{0\}$, define*

$$F(\alpha;P) = \sum_{\mathbf{x}\in I_P^d} e\Big(\sum_{\mathbf{i}\in\mathcal{R}_0'}\alpha_{\mathbf{i}}\mathbf{x}^{\mathbf{i}}\Big).$$

For $Q \in \mathbb{N}\setminus\{0\}$ with $Q \le P$, let $a, g \in \mathbb{A}$ with g monic, $\gcd(a,g) = 1$ and $\langle g\rangle \le \widehat{Q}^k$. For a fixed $\mathbf{l} \in \mathcal{L}$, suppose that $\langle g\alpha_{\mathbf{l}} - a\rangle < \widehat{Q}^{-k}$ and that either $\langle g\alpha_{\mathbf{l}} - a\rangle \ge \widehat{Q}\widehat{P}^{-k}$ or $\langle g\rangle > \widehat{Q}$. Then we have

$$\big|F(\alpha;P)\big| \ll \langle g\rangle^{\epsilon}\widehat{P}^{d+\epsilon}\Big(\widehat{Q}^{-1}\big(1+\langle g\rangle(\widehat{P}/\widehat{Q})^{-k}\big)\Big)^{1/(2\mu(k+1))}.$$

Proof By Corollary 1.2 and [16, Lemma 9.1], the lemma follows by replacing M with Q and taking $s = \mu(k+1)$ and $\Delta_s = \epsilon$. ∎

For $\mathbf{c} = (c_1,\dots,c_s) \in (\mathbb{A}\setminus\{0\})^s$, we recall that $N_{s,k,d,\mathbf{c}}(P)$ counts the number of the solutions of the system

$$c_1\mathbf{x}_1^{\mathbf{l}} + \cdots + c_s\mathbf{x}_s^{\mathbf{l}} = 0, \quad \mathbf{l} \in \mathcal{L},$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

with $\mathbf{x}_j \in I_P^d$, $1 \le j \le s$. For $\alpha = (\alpha_{\mathbf{l}})_{\mathbf{l}\in\mathcal{L}} \in \mathbb{K}_\infty^\iota$ and $P \in \mathbb{N} \setminus \{0\}$, define

$$f_j(\alpha) = f_j(\alpha; P) = \sum_{\mathbf{x}\in I_P^d} e\Big(\sum_{\mathbf{l}\in\mathcal{L}} c_j \alpha_{\mathbf{l}} \mathbf{x}^{\mathbf{l}} \Big), \quad 1 \le j \le s.$$

By (2.1), we see that

$$N_{s,k,d,\mathbf{c}}(P) = \int_{\mathbb{T}^\iota} \prod_{j=1}^{s} f_j(\alpha) d\alpha.$$

We now apply the Hardy–Littlewood circle method to analyze the above integral. We begin by dividing $\mathbb{T}^\iota$ into major and minor arcs as follows: given $\mathbf{a} = (a_{\mathbf{l}})_{\mathbf{l}\in\mathcal{L}} \in \mathbb{A}^\iota$, $g \in \mathbb{A}$ monic with $\gcd(a_{\mathbf{l}}, g) = 1, \mathbf{l} \in \mathcal{L}$, we define the *Farey arc* $\mathfrak{M}(g, \mathbf{a})$ about $\mathbf{a}/g$ by

$$\mathfrak{M}(g, \mathbf{a}) = \Big\{ \alpha \in \mathbb{T}^\iota \;\Big|\; \langle g\alpha_{\mathbf{l}} - a_{\mathbf{l}} \rangle < \widehat{P}^{1/2} \widehat{P}^{-k}, \mathbf{l} \in \mathcal{L} \Big\}.$$

Write $\langle \mathbf{c} \rangle = \max\big\{ \langle c_j \rangle \mid 1 \le j \le s \big\}$. The set of *major arcs* $\mathfrak{M}$ is defined to be the union of all $\mathfrak{M}(g, \mathbf{a})$ with $\mathbf{a} = (a_{\mathbf{l}})_{\mathbf{l}\in\mathcal{L}} \in \mathbb{A}^\iota$ and $g \in \mathbb{A}$ monic, which satisfy $\gcd(a_{\mathbf{l}}, g) = 1$ and $0 \le \langle a_{\mathbf{l}} \rangle < \langle g \rangle \le \langle \mathbf{c} \rangle \widehat{P}^{1/2}, \mathbf{l} \in \mathcal{L}$. Then we write $\mathfrak{m} = \mathbb{T}^\iota \setminus \mathfrak{M}$ for the complementary set of *minor arcs*. We now estimate the contribution over minor arcs.

Lemma 6.2 *Let $k \ge 2$. For each j with $1 \le j \le s$, we have*

$$\sup_{\alpha\in\mathfrak{m}} |f_j(\alpha)| \ll \widehat{P}^{d-1/(4\iota\mu(k+1))+\epsilon}.$$

Proof Let $\alpha \in \mathfrak{m}$ and $Q = [P/(2\iota)]$. By [4, Lemma 3], for each $\mathbf{l} \in \mathcal{L}$, there exist $a_{\mathbf{l}} \in \mathbb{A}$ and $g_{\mathbf{l}} \in \mathbb{A}$ monic, which satisfy $\gcd(a_{\mathbf{l}}, g_{\mathbf{l}}) = 1$, $0 \le \langle a_{\mathbf{l}} \rangle < \langle g_{\mathbf{l}} \rangle \le \widehat{Q}^k$ and $\langle g_{\mathbf{l}} c_j \alpha_{\mathbf{l}} - a_{\mathbf{l}} \rangle < \widehat{Q}^{-k}$. Using the same argument as in [16, Lemma 10.1], there exists $\mathbf{l} \in \mathcal{L}$ such that $\langle g_{\mathbf{l}} \rangle > \widehat{Q}$ or $\langle g_{\mathbf{l}} c_j \alpha_{\mathbf{l}} - a_{\mathbf{l}} \rangle \ge \widehat{Q}\widehat{P}^{-k}$. By Lemma 6.1, we have

$$|f_j(\alpha)| \ll \widehat{P}^{d-1/(4\iota\mu(k+1))+\epsilon}.$$

This completes the proof of the lemma. ∎

Let $I_{m,k,d}(P)$ denote the number of solutions of the system

$$\mathbf{x}_1^{\mathbf{l}} + \cdots + \mathbf{x}_m^{\mathbf{l}} = \mathbf{y}_1^{\mathbf{l}} + \cdots + \mathbf{y}_m^{\mathbf{l}}, \quad \mathbf{l} \in \mathcal{L},$$

with $\mathbf{x}_n, \mathbf{y}_n \in I_P^d$, $1 \le n \le m$. For $\mathbf{h} = (h_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}_0'} \in \prod_{\mathbf{i}\in\mathcal{R}_0'} I_{|\mathbf{i}|P}$, write $\mathcal{J}_{m,k,d}(P; \mathbf{h})$ for the number of solutions of the system

$$\big(\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_m^{\mathbf{i}}\big) - \big(\mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_m^{\mathbf{i}}\big) = h_{\mathbf{i}}, \quad \mathbf{i} \in \mathcal{R}_0',$$

with $\mathbf{x}_n, \mathbf{y}_n \in I_P^d$, $1 \le n \le m$. By [16, Lemma A.2], we have $\mathcal{L} \subseteq \mathcal{R}_0'$ and hence

$$I_{m,k,d}(P) = \sum_{\mathbf{h}} \mathcal{J}_{m,k,d}(P, \mathbf{h}),$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

where the summation is over $\mathbf{h} = (h_{\mathbf{i}})_{\mathbf{i}\in\mathcal{R}_0'} \in \prod_{\mathbf{i}\in\mathcal{R}_0'} I_{|\mathbf{i}|P}$ with $h_{\mathbf{i}} = 0$ when $\mathbf{i} \in \mathcal{L}$. Let $K = \sum_{\mathbf{i}\in\mathcal{R}_0'} |\mathbf{i}|$. It follows from Corollary 1.2 that for $m \geq \mu k + \mu$, we have

$$I_{m,k,d}(P) \leq \widehat{P}^{K-\iota k} \mathcal{J}_{m,k,d}(P) \ll \widehat{P}^{K-\iota k} \widehat{P}^{2md-K+\epsilon} = \widehat{P}^{2md-\iota k+\epsilon}, \tag{6.1}$$

where the implicit constants depend on m, d, k and q.

Lemma 6.3 *Let $k \geq 2$ and $s \geq 2\mu k + 2\mu + 1$. We have*

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} \big| f_j(\alpha) \big| d\alpha \ll \widehat{P}^{sd-\iota k-1/(8\iota\mu(k+1))}.$$

Proof Write $m_0 = \mu k + \mu$ and $s_0 = 1 + 2m_0$. By Hölder's inequality, we have

$$\begin{aligned}\int_{\mathfrak{m}} \prod_{j=1}^{s_0} \big| f_j(\alpha) \big| d\alpha &\leq \sup_{\alpha\in\mathfrak{m}} \big| f_1(\alpha) \big| \int_{\mathbb{T}^\iota} \prod_{j=2}^{s_0} \big| f_j(\alpha) \big| d\alpha \\ &\leq \sup_{\alpha\in\mathfrak{m}} \big| f_1(\alpha) \big| \prod_{j=2}^{s_0} \Big(\int_{\mathbb{T}^\iota} \big| f_j(\alpha) \big|^{2m_0} d\alpha \Big)^{1/(2m_0)}.\end{aligned}$$

On considering the underlying Diophantine equations, by (6.1), we have

$$\int_{\mathbb{T}^\iota} \big| f_j(\alpha) \big|^{2m_0} d\alpha = I_{m_0,k,d}(P) \ll \widehat{P}^{2m_0 d-\iota k+\epsilon}, \quad 2 \leq j \leq s_0.$$

Thus, we see from Lemma 6.2 that

$$\int_{\mathfrak{m}} \prod_{j=1}^{s_0} \big| f_j(\alpha) \big| d\alpha \ll \widehat{P}^{d-1/(4\iota\mu(k+1))+\epsilon} \widehat{P}^{2m_0 d-\iota k+\epsilon} \ll \widehat{P}^{s_0 d-\iota k-1/(8\iota\mu(k+1))}.$$

Then by using the trivial bound that $\big| f_j(\alpha) \big| \ll \widehat{P}^d$, $s_0 + 1 \leq j \leq s$, it follows that

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} \big| f_j(\alpha) \big| d\alpha \ll \widehat{P}^{(s-s_0)d} \int_{\mathfrak{m}} \prod_{j=1}^{s_0} \big| f_j(\alpha) \big| d\alpha \ll \widehat{P}^{sd-\iota k-1/(8\iota\mu(k+1))}.$$

This completes the proof of the lemma. ∎

We are now ready to prove Theorem 1.3.

Proof of Theorem 1.3 When $s \geq 2\mu k + 2\mu + 1$, it follows from Lemma 6.3 that there exists $\eta = \eta(d; k; q) > 0$ such that

$$\int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\alpha) d\alpha = O\big(\widehat{P}^{sd-\iota k-\eta} \big).$$

When $s \geq 2(\iota+1)k+1$, by [16, Theorem 6.1], subject to a local solubility hypothesis, we have

$$\int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\alpha) d\alpha = C_3 \widehat{P}^{sd-\iota k} + O\big(\widehat{P}^{sd-\iota k-\eta} \big),$$

https://doi.org/10.4153/CJM-2013-014-9 Published online by Cambridge University Press

where $C_3 = C_3(s, d; k; q; \mathbf{c}) > 0$. Recall that

$$N_{s,k,d,\mathbf{c}}(P) = \int_{\mathbb{T}^\iota} \prod_{j=1}^{s} f_j(\alpha) d\alpha = \int_{\mathfrak{M}} \prod_{j=1}^{s} f_j(\alpha) d\alpha + \int_{\mathfrak{m}} \prod_{j=1}^{s} f_j(\alpha) d\alpha.$$

Since $\mu \geq \iota + 1$, on combining the above estimates, the theorem follows. ■

Acknowledgment The authors are grateful to the referee for valuable suggestions about this paper.

References

[1] B. J. Birch, *Homogeneous forms of odd degree in a large number of variables*. Mathematika **4**(1957), 102–105. http://dx.doi.org/10.1112/S0025579300001145
[2] R. Brauer, *A note on systems of homogeneous algebraic equations*. Bull. Amer. Math. Soc. **51**(1945), 749–755. http://dx.doi.org/10.1090/S0002-9904-1945-08440-7
[3] H. Davenport and D. J. Lewis, *Homogeneous additive equations*. Proc. Roy. Soc. Ser. A. **274**(1963), 443–460. http://dx.doi.org/10.1098/rspa.1963.0143
[4] R. M. Kubota, *Waring's problem for* $\mathbb{F}_q[x]$. Ph. D. Thesis, University of Michigan, Ann Arbor, 1971.
[5] S. Lang, *On quasi-algebraic closure*. Ann. of Math. **55**(1952), 373–390. http://dx.doi.org/10.2307/1969785
[6] Y.-R. Liu and T. D. Wooley, *Waring's problem in function fields*. J. Reine Angew. Math. **638**(2010), 1–67. http://dx.doi.org/10.1515/crelle.2010.001
[7] S. T. Parsell, *A generalization of Vinogradov's mean value theorem*. Proc. London Math. Soc. (3) **91**(2005), no. 1, 1–32. http://dx.doi.org/10.1112/S002461150501525X
[8] ———, *Asymptotic estimates for rational linear spaces on hypersurfaces*. Trans. Amer. Math. Soc. **361**(2009), no. 6, 2929–2957. http://dx.doi.org/10.1090/S0002-9947-09-04821-1
[9] S. T. Parsell, S. M. Prendivlle, and T. D. Wooley, *Near-optimal mean value estimates for multidimensional Weyl sums*. arxiv:1205.6331
[10] T. D. Wooley, *Large improvements in Waring's problem*. Ann. of Math. **135**(1992), no. 1, 131–164. http://dx.doi.org/10.2307/2946566
[11] ———, *A note on simultaneous congruences*. J. Number Theory **58**(1996), no. 2, 288–297. http://dx.doi.org/10.1006/jnth.1996.0078
[12] ———, *Vinogradov's mean value theorem via efficient congruencing*. Ann. of Math. **175**(2012), no. 3, 1575–1627. http://dx.doi.org/10.4007/annals.2012.175.3.12
[13] ———, *Vinogradov's mean value theorem via efficient congruencing. II*. Duke Math. J. **162**(2013), no. 4, 673–730. http://dx.doi.org/10.1215/00127094-2079905
[14] ———, *The asymptotic formula in Waring's problem*. Int. Math. Res. Not. IMRN **2012**, no. 7, 1485–1504.
[15] X. Zhao, *A note on multiple exponential sums in function fields*. Finite Fields Appl. **18**(2012), no. 1, 35–55. http://dx.doi.org/10.1016/j.ffa.2011.06.003
[16] ———, *Asymptotic estimates for rational spaces on hypersurfaces in function fields*. Proc. Lond. Math. Soc.(3) **104**(2012), no. 2, 287–322. http://dx.doi.org/10.1112/plms/pdr031

Department of Pure Mathematics, Faculty of Mathematics, University of Waterloo, Waterloo, ON N2L 3G1
e-mail: wtkuo@math.uwaterloo.ca yrliu@math.uwaterloo.ca

School of Mathematics and Statistics, Central China Normal University, Wuhan, Hubei, China 430079
e-mail: x8zhao@gmail.com