

QUASI-DIAGONAL BEHAVIOUR IN CERTAIN MEAN VALUE THEOREMS OF ADDITIVE NUMBER THEORY

TREVOR D. WOOLEY

1. INTRODUCTION

Of fundamental significance in many problems of additive number theory are estimates for mean values of exponential sums over polynomial functions. In this paper we shall show that the exponential sums of greatest interest in additive number theory demonstrate quasi-diagonal behaviour, which is to say that by taking the degree of the polynomial argument sufficiently large, we can obtain upper bounds for low moments of the exponential sums arbitrarily close (in a suitable sense) to the diagonal estimate. Let us illustrate these notions by considering the situation in Vinogradov's mean value theorem.

Let s and k be positive integers, and write

$$f(\boldsymbol{\alpha}; Q) = \sum_{1 \leq x \leq Q} e(\alpha_1 x + \cdots + \alpha_k x^k), \quad (1.1)$$

where $e(\alpha)$ denotes $e^{2\pi i \alpha}$. When P is a real number, we define $J_{s,k}(P)$ by

$$J_{s,k}(P) = \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; P)|^{2s} d\boldsymbol{\alpha}, \quad (1.2)$$

where \mathbb{T}^k denotes the k -dimensional unit cube. Upper bounds for the mean value (1.2) were first considered by Vinogradov in the 1930's (see [V1]), their estimation being based on the observation that by orthogonality, $J_{s,k}(P)$ is equal to the number of solutions of the simultaneous diophantine equations

$$x_1^j + \cdots + x_s^j = y_1^j + \cdots + y_s^j \quad (1 \leq j \leq k), \quad (1.3)$$

with $1 \leq x_i, y_i \leq P$ ($1 \leq i \leq s$). Those solutions of (1.3) in which x_1, \dots, x_s is a permutation of y_1, \dots, y_s (the *diagonal solutions*) plainly contribute $\gg_s P^s$ to $J_{s,k}(P)$, and in fact when $s \leq \frac{1}{2}k(k+1)$ and $k > 2$ it is widely conjectured that $J_{s,k}(P) \ll_{s,k} P^s$. (When $s > \frac{1}{2}k(k+1)$, the conjectured bound for $J_{s,k}(P)$ takes a different shape; see, for example, [W3] for this and related results). Motivated by this conjecture, we now formulate the property of quasi-diagonal behaviour as follows. We consider a sequence $(\mathcal{S}_k)_{k=1}^\infty$ of finite sets of exponents $\mathcal{S}_k \subset \mathbb{N}$, and say that the mean value (1.2) exhibits *quasi-diagonal behaviour* for this sequence if there exists a set of real numbers $\{\delta_{s,k} : k \in \mathbb{N}, s \in \mathcal{S}_k\}$ with the property that

$$\lim_{k \rightarrow \infty} \max_{s \in \mathcal{S}_k} \delta_{s,k} = 0,$$

and for each $k \in \mathbb{N}$ and $s \in \mathcal{S}_k$ we have the bound

$$J_{s,k}(P) \ll_{s,k} P^{s+\delta_{s,k}}. \quad (1.4)$$

Moreover, we shall say that the mean value exhibits *strongly diagonal behaviour* if given $\varepsilon > 0$, for each $k \in \mathbb{N}$ and $s \in \mathcal{S}_k$ we have the bound

$$J_{s,k}(P) \ll_{s,k,\varepsilon} P^{s+\varepsilon}.$$

1991 *Mathematics Subject Classification*. 11L15, 11P08.

Research supported in part by NSF grant DMS-8610730 at the Institute for Advanced Study, and by a Rackham Faculty Fellowship at the University of Michigan.

At present we have rather limited knowledge concerning the behaviour of the solutions of the system (1.3). When $1 \leq s \leq k$, one may use elementary results on symmetric polynomials (Newton's formulae) to deduce that the only solutions of (1.3) are diagonal. Also, Hua [H, Lemma 5.4] has used divisor sum arguments to show that

$$J_{k+1,k}(P) \ll_k P^{k+1}(\log P)^{2^k-1}.$$

Then (1.2) certainly exhibits strongly diagonal behaviour when $1 \leq s \leq k+1$. However, for exponents $s > k+1$, previous estimates have not come close even to demonstrating quasi-diagonal behaviour. Indeed, until recently the best bounds available for $J_{s,k}(P)$ took the form

$$J_{rk,k}(P) \ll_{r,k} P^{2rk - \frac{1}{2}k(k+1) + \frac{1}{2}k^2(1-1/k)^r} \quad (r \in \mathbb{N}) \quad (1.5)$$

(see [W2, Theorems 1.1 and 1.2] for improvements significant for $s \gg k^2$). When put into the form (1.4), the bound (1.5) yields only $\delta_{s,k} \ll s$. Arkhipov and Karatsuba [AK] were the first to make substantial progress, establishing that (1.4) holds with $\delta_{s,k} \ll s^{3/2}/k$, and Tyrina [T] has recently improved this result to obtain $\delta_{s,k} \ll s^2/k^2$. Neither of the latter estimates establish quasi-diagonal behaviour for the non-trivial range $k+1 < s \leq \frac{1}{2}k(k+1)$. In this paper we substantially improve these estimates, in particular establishing quasi-diagonal behaviour for $1 \leq s \ll_\varepsilon k^{3/2-\varepsilon}$.

Theorem 1. *Let $k \in \mathbb{N}$, $P \in \mathbb{R}^+$ and define $\xi = \xi(s, k)$ to be the smallest positive solution of the equation*

$$4s^2\xi e^{1+4\xi/k} = k(k-2\xi)^2.$$

Then when $1 \leq s \leq k^{3/2}$, the bound (1.4) holds with

$$\delta_{s,k} \ll \xi^{-\frac{1}{2}} k^3 \left(1 - \frac{2\xi}{k}\right)^k e^{\xi+2\xi^2/k}.$$

Corollary 1.1. *The inequality (1.4) holds with*

$$\delta_{s,k} \ll sk^{3/2} \exp\left(-\frac{k^3}{4es^2} (1 + O(k^2/s^2))\right).$$

When s is small, the strength of the new bound may be discerned from the following corollary.

Corollary 1.2. *When $s = (1 + o(1))k$, the bound (1.4) holds with $\delta_{s,k} \ll e^{-\frac{k}{18}}$.*

It may be useful to illustrate the relative strengths of these results when s is a fixed multiple of k , say $s = Ck$. In such circumstances the work of Arkhipov and Karatsuba shows that $\delta_{s,k} \ll_C k^{1/2}$ is permissible, Tyrina's work gives $\delta_{s,k} \ll_C 1$, and Theorem 1 yields $\delta_{s,k} \ll e^{-Ak}$ with $A = A(C) > 0$. The superiority of our result is self-evident.

The proof of Theorem 1 is based partly on the author's recent work on Vinogradov's mean value theorem (see [W2]), and is motivated in spirit by Vaughan's work on the corresponding problem associated with Waring's problem (see [Va2]). By modifying the argument of [W2], we are able to relate the number of solutions of the simultaneous diophantine equations

$$\sum_{i=1}^t (x_i^j - y_i^j) = \sum_{l=1}^s (u_l^j - v_l^j) \quad (1 \leq j \leq k),$$

with $1 \leq x_i, y_i \leq P$ ($1 \leq i \leq t$), $1 \leq u_l, v_l \leq P$ ($1 \leq l \leq s$), to the number of solutions of the simultaneous equations

$$\sum_{i=1}^t (x_i^j - y_i^j) = p^j \sum_{l=1}^s (m_l^j - n_l^j) \quad (1 \leq j \leq k), \quad (1.6)$$

with $1 \leq m_l, n_l \leq P^{1-\theta}$ ($1 \leq l \leq s$), $1 \leq x_i, y_i \leq P$ and $x_i \equiv y_i \pmod{p^r}$ ($1 \leq i \leq t$), and where p is some fixed prime satisfying $P^\theta < p \leq 2P^\theta$. Here θ is a parameter with $0 \leq \theta < 1$, and r and t are integer parameters. In the "classical" version of Vinogradov's mean value theorem, one takes $r = t = k$

and $\theta = 1/k$, thus showing that $x_i = y_i$ ($1 \leq i \leq t$), and enabling a reduction formula to be set up which relates $J_{s+t,k}(P)$ to $J_{s,k}(P^{1-\theta})$. Arkhipov and Karatsuba [AK] observed that when s is small, the latter reduction formula can be made more efficient by taking $r = t < k$ and $\theta = 1/r$. In our method we take $r < k$, $t = k + 1 - r$ and $\theta < 1/r$, and then consider the substitution $y_i = x_i + h_i p^r$. This gives rise to efficient differences, via expressions of the form $\Psi_{i,j} = (x_i + h_i p^r)^j - x_i^j$, and we are then able to apply a Hölder's inequality argument to estimate the number of solutions of the equations (1.6) in terms of

$$\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; P^{1-\theta})|^{\frac{2sk}{k-t}} d\boldsymbol{\alpha},$$

and a suitable mean value estimate for exponential sums over the difference polynomials $\Psi_{i,j}$. Thus we are able to relate $J_{s+t,k}$ to $J_{s,k}$ and $J_{\frac{sk}{k-t},k}$, and thereby obtain bounds in terms of solutions of a set of recurrence relations of a complicated nature. Suitable bounds for the solution of these recurrence relations yield Theorem 1.

Some of the techniques which we develop in the analysis of the reduction formulae alluded to above are also of use in mean value estimates related to Waring's problem. Let $S_s(P, R)$ denote the number of solutions of the equation

$$x_1^k + \cdots + x_s^k = y_1^k + \cdots + y_s^k, \quad (1.7)$$

with $x_i, y_i \in \mathcal{A}(P, R)$ ($1 \leq i \leq s$), where here, and throughout, we write

$$\mathcal{A}(P, R) = \{n \in \mathbb{Z} \cap [1, P] : p \text{ prime, } p|n \Rightarrow p \leq R\}.$$

Bounds for $S_s(P, R)$ were first systematically established by Vaughan [Va1,2], and have since been improved, especially for larger k (see [W1]). When $R = P^\eta$ with $0 < \eta < \eta_0$ one has $\text{card}(\mathcal{A}(P, R)) \gg_\eta P$, and so standard arguments yield

$$S_s(P, R) \gg P^s + P^{2s-k}$$

(here, and throughout this discussion with regards to $S_s(P, R)$, the implicit constant in Vinogradov's notation may depend on s, k, ε and η). Vaughan [Va2, Theorem 1.1] has used methods loosely related to those described above to establish quasi-diagonal behaviour for the mean value $S_s(P, R)$ when $s \ll_\varepsilon k^{1/2-\varepsilon}$ (here "quasi-diagonal" has the obvious meaning analogous to that defined for $J_{s,k}(P)$). He shows that when $\eta = \eta(\varepsilon, k)$ is a sufficiently small positive number, then

$$S_s(P, P^\eta) \ll P^{s+\gamma_{s,k}+\varepsilon}, \quad (1.8)$$

where $\gamma_{s,k}$ is a real number prescribed by a complicated formula, but bounded roughly in the form

$$\gamma_{s,k} \ll \left(k/s^2\right)^{-\frac{\log(k/s^2)}{\log 16}} + O(1).$$

Notice that in order to establish quasi-diagonal solubility in the shape (1.4), we have merely to take ε to be sufficiently small in terms of s and k . In particular, when $s = 3$, Vaughan [Va2, proof of Theorem 1.2] obtains

$$\gamma_{3,k} = \left(C_k + O(k^{-1/2})\right) k^{-\frac{\log k}{\log 16}}, \quad (1.9)$$

where $1 \ll C_k \ll 1$, and expresses the opinion that "undoubtedly refinements can be introduced which...would lead to a smaller value for C_k in (equation (1.9))". In Theorem 2 below we show that even the exponent of k may be improved a little.

Theorem 2. *Suppose that $k \in \mathbb{N}$ and $s \leq \frac{1}{2}k^{1/2}$. Suppose that $\varepsilon > 0$ is given, and let $\eta = \eta(\varepsilon, k)$ be a sufficiently small positive number. Then the bound (1.8) holds with*

$$\gamma_{s,k} \ll \frac{k}{s} \left(\frac{k}{s^2} \log\left(\frac{k}{s^2}\right)\right)^{-\alpha_{s,k}},$$

where

$$\alpha_{s,k} = \frac{\log(k/s^2) + \log \log(k/s^2)}{\log 16} + O(1).$$

In §2 we establish some preliminary lemmata required in the proof of Theorem 1. Then, in §3, we set up the fundamental lemmata which in §4 permit us to establish the recurrence relations for $\delta_{s,k}$. These we solve in §5, thereby proving Theorem 1. Next, in §6, we recall some estimates from the iterative method in Waring's problem, these enabling us to establish the recurrence relations for $\gamma_{s,k}$ in §7. The solution of these relations yields Theorem 2. Finally, in section 8 we make some remarks concerning generalisations of the above results, and consequences of the generalised *ABC*-conjecture.

The author thanks Professor G.Kolesnik for providing him with a copy of the unpublished paper [KO], in which Kolesnik and Odlyzko independently developed the methods underlying the work of Arkhipov and Karatsuba [AK]. The clarity of the formers' exposition was of great assistance. The author also thanks the referee for some helpful comments. Much of the work for this paper was completed while the author was enjoying the hospitality of the Institute for Advanced Study.

Throughout, k will denote an integer exceeding 4, and P will denote the basic parameter, a real number sufficiently large in terms of k . Also, we write $[x]$ for the integer part of x .

2. PRELIMINARY LEMMATA

We first provide a lemma which estimates the number of solutions of a certain system of congruences of similar nature to previous results of Linnik, Karatsuba and Tyrina (see [T, Lemma 6]).

Lemma 2.1. *Suppose that t and r are integers with $1 \leq r, t \leq k$ and $r + t \geq k$. Let $\mathcal{B}_t(p^r; \mathbf{u})$ denote the number of solutions (z_1, \dots, z_t) distinct $(\bmod p^r)$ of the system of congruences*

$$\sum_{i=1}^t z_i^j \equiv u_j \pmod{p^j} \quad (1 \leq j \leq k)$$

with the z_i distinct $(\bmod p)$. Then $\mathcal{B}_t(p^r; \mathbf{u}) \ll_k p^{\omega(r,t,k)}$, where

$$\omega(r, t, k) = \frac{1}{2}(r + t - k - 1)(r + t - k). \quad (2.1)$$

Proof. Let $\mathcal{C}(p; \mathbf{a})$ denote the number of solutions (z_1, \dots, z_t) distinct $(\bmod p^r)$ of the system of congruences

$$\begin{aligned} \sum_{i=1}^t z_i^j &\equiv a_j \pmod{p^r} & (k - t + 1 \leq j \leq k) \\ \sum_{i=1}^t z_i^j &\equiv a_j \pmod{p} & (1 \leq j \leq k - t), \end{aligned}$$

with the z_i distinct $(\bmod p)$. Then

$$\mathcal{B}_t(p^r; \mathbf{u}) \leq \sum_{\mathbf{a}}^* \mathcal{C}(p; \mathbf{a}) \quad (2.2)$$

where the summation is over $(a_1, \dots, a_k) \in \mathbb{Z}^k$ with

$$a_j \equiv u_j \pmod{p^{\min\{j,r\}}} \quad \text{and} \quad 1 \leq a_j \leq p^r \quad (k - t + 1 \leq j \leq k),$$

and with

$$a_j \equiv u_j \pmod{p} \quad \text{and} \quad 1 \leq a_j \leq p \quad (1 \leq j \leq k - t).$$

For a fixed \mathbf{u} , the total number of choices for \mathbf{a} is $p^{\omega(r,t,k)}$. But as in the proof, for example, of [W2, Lemma 2.2], for each p and \mathbf{b} we have $\mathcal{C}(p; \mathbf{b}) \leq t! \leq k!$, and thus the lemma follows from (2.2).

We now investigate mean value estimates for exponential sums over difference polynomials. When P and H are positive numbers, let

$$G_r(\boldsymbol{\alpha}; p; z) = \sum_{1 \leq h \leq H} e(\alpha_1 \Psi_{1,r}(z, h, p) + \dots + \alpha_k \Psi_{k,r}(z, h, p)),$$

where

$$\Psi_{i,r}(z, h, p) = (z + hp^r)^i - z^i.$$

Further, let

$$F_r(\boldsymbol{\alpha}; p) = \sum_{1 \leq z \leq P} G_r(\boldsymbol{\alpha}; p; z). \quad (2.3)$$

Lemma 2.2. *Suppose that m, r and p are positive integers and $2m \leq k$. Then*

$$\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2m} d\boldsymbol{\alpha} \ll_k (PH)^m.$$

Proof. The integral in question is bounded above by the number of solutions of the system of diophantine equations

$$\sum_{i=1}^m \left((z_i + h_i p^r)^j - z_i^j \right) = \sum_{i=1}^m \left((y_i + g_i p^r)^j - y_i^j \right) \quad (1 \leq j \leq k), \quad (2.4)$$

with $1 \leq y_i, z_i \leq P$ and $1 \leq g_i, h_i \leq H$ ($1 \leq i \leq m$). Consider any solution $\mathbf{y}, \mathbf{z}, \mathbf{g}, \mathbf{h}$ of the equations (2.4). By rearranging variables we may suppose that

$$y_1 = \min_{1 \leq i \leq m} y_i, \quad \text{and} \quad z_1 = \min_{1 \leq i \leq m} z_i. \quad (2.5)$$

Further, by Newton's formulae on the roots of polynomials, for every real number x we have

$$\prod_{i=1}^m (x - z_i - h_i p^r)(x - y_i) = \prod_{i=1}^m (x - z_i)(x - y_i - g_i p^r).$$

Then by comparing the roots of the polynomials on each side of the latter equation, we deduce that

$$(z_1 + h_1 p^r, \dots, z_m + h_m p^r, y_1, \dots, y_m)$$

is a permutation of

$$(y_1 + g_1 p^r, \dots, y_m + g_m p^r, z_1, \dots, z_m).$$

In view of (2.5), we may conclude that $y_1 = z_1$, so that from (2.4), and by considering the underlying diophantine equations, it follows that

$$\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2m} d\boldsymbol{\alpha} \ll_k \int_{\mathbb{T}^k} \sum_{1 \leq z \leq P} |G_r(\boldsymbol{\alpha}; p; z)^2 F_r(\boldsymbol{\alpha}; p)^{2m-2}| d\boldsymbol{\alpha}.$$

Therefore, by applying Hölder's inequality twice,

$$\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2m} d\boldsymbol{\alpha} \ll_k \left(P^{m-1} \sum_{1 \leq z \leq P} N_m(z) \right)^{1/m} \left(\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2m} d\boldsymbol{\alpha} \right)^{1-1/m},$$

where

$$N_m(z) = \int_{\mathbb{T}^k} |G_r(\boldsymbol{\alpha}; p; z)|^{2m} d\boldsymbol{\alpha}.$$

Hence

$$\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2m} d\boldsymbol{\alpha} \ll_k P^{m-1} \sum_{1 \leq z \leq P} N_m(z). \quad (2.6)$$

But $N_m(z)$ is the number of solutions of the system of diophantine equations

$$\sum_{i=1}^m \left((z + h_i p^r)^j - z^j \right) = \sum_{i=1}^m \left((z + g_i p^r)^j - z^j \right) \quad (1 \leq j \leq k),$$

with $1 \leq g_i, h_i \leq H$ ($1 \leq i \leq m$). Moreover, for each solution \mathbf{g}, \mathbf{h} counted by $N_m(z)$, we have

$$\sum_{i=1}^m (z + h_i p^r)^j = \sum_{i=1}^m (z + g_i p^r)^j \quad (1 \leq j \leq k),$$

so that by using Newton's formulae on the roots of polynomials once again, we may deduce that

$$(z + h_1 p^r, \dots, z + h_m p^r)$$

is a permutation of

$$(z + g_1 p^r, \dots, z + g_m p^r).$$

Consequently, (h_1, \dots, h_m) is a permutation of (g_1, \dots, g_m) , and so $N_m(z) \ll_k H^m$. The lemma now follows immediately from (2.6).

We note that it is the strongly diagonal behaviour of the mean value in Lemma 2.2 which is crucial to the argument which follows. The estimate (2.14) of [V2] plays a similar rôle in the corresponding work associated with Waring's problem. This is a point which we shall pursue further in section 8.

3. THE FUNDAMENTAL LEMMA

In order to derive the recurrence relations alluded to in the introduction, we must establish a fundamental lemma similar to [W2, Lemma 3.1]. Although the proof of this lemma is a straightforward extension of the latter, there are sufficiently many changes to warrant a complete account. We first set up some notation. In sections 3-5 implicit constants will depend only on the natural numbers k and s , unless stated otherwise.

For each $s \in \mathbb{N}$ we take $r = r_s$ and $t = t_s$ to be integers with $3 \leq r, t \leq k$ and $r + t \geq k$, and we take $\theta = \theta_s$ to be a real number with $0 < \theta_0(k) \leq \theta \leq 1/r$, to be chosen later. For convenience, we write

$$M = P^\theta, \quad H = PM^{-r}, \quad Q = PM^{-1}. \quad (3.1)$$

Let $\mathcal{P}(\theta)$ be the set consisting of the smallest $[k^2/\theta] + 1$ primes exceeding P^θ . Notice that on taking P sufficiently large, it follows from the prime number theorem that $P^\theta < p < 2P^\theta$ for each $p \in \mathcal{P}(\theta)$.

When $p \in \mathcal{P}(\theta)$ we define $\mathcal{L}_s(P; p)$ to be the number of solutions of the simultaneous equations

$$\sum_{n=1}^t (z_n^j - w_n^j) + p^j \sum_{m=1}^s (u_m^j - v_m^j) = 0 \quad (1 \leq j \leq k), \quad (3.2)$$

with

$$1 \leq z_n, w_n \leq P, \quad z_n \equiv w_n \pmod{p^r} \quad (1 \leq n \leq t), \quad (3.3)$$

and

$$1 \leq u_m, v_m \leq Q \quad (1 \leq m \leq s). \quad (3.4)$$

Lemma 3.1. *With r, t and θ satisfying the above hypotheses, there exists a prime $p \in \mathcal{P}(\theta)$ with*

$$J_{s+t,k}(P) \ll M^{2s+\omega(r,t,k)} \mathcal{L}_s(P; p).$$

Proof. Let $R_1(\mathbf{h})$ denote the number of solutions of the simultaneous equations

$$\sum_{i=1}^{s+t} x_i^j = h_j \quad (1 \leq j \leq k) \quad (3.5)$$

with $1 \leq x_i \leq P$ ($1 \leq i \leq s+t$) and with $x_j \leq 2P^\theta$ for some j . Let $R_2(\mathbf{h})$ denote the number of solutions of (3.5) with $1 \leq x_i \leq P$ ($1 \leq i \leq s+t$), with $x_j \leq 2P^\theta$ for no j , and with x_1, \dots, x_t distinct, and let $R_3(\mathbf{h})$ denote the corresponding number of solutions with x_1, \dots, x_t not distinct. Then

$$J_{s+t,k}(P) = \sum_{\mathbf{h}} (R_1(\mathbf{h}) + R_2(\mathbf{h}) + R_3(\mathbf{h}))^2 \leq 9 \max\{S_1, S_2, S_3\},$$

where $S_i = \sum_{\mathbf{h}} R_i(\mathbf{h})^2$ ($i = 1, 2, 3$). We now divide into cases.

(a) Suppose that $S_1 \geq \max\{S_2, S_3\}$. Then $J_{s+t,k}(P) \leq 9S_1$. By considering the underlying diophantine equations,

$$S_1 \ll \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; 2P^\theta)^2 f(\boldsymbol{\alpha}; P)^{2s+2t-2}| d\boldsymbol{\alpha}.$$

In this case, therefore, by Hölder's inequality,

$$\begin{aligned} J_{s+t,k}(P) &\ll \left(\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; P)|^{2s+2t} d\boldsymbol{\alpha} \right)^{1-\frac{1}{s+t}} \left(\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; 2P^\theta)|^{2s+2t} d\boldsymbol{\alpha} \right)^{\frac{1}{s+t}}, \\ &\ll (J_{s+t,k}(P))^{1-\frac{1}{s+t}} (J_{s+t,k}(2P^\theta))^{\frac{1}{s+t}}. \end{aligned}$$

Then by using a trivial estimate, and recalling that by hypothesis we have $\theta \leq \frac{1}{r} \leq \frac{1}{3}$, we deduce that

$$J_{s+t,k}(P) \ll J_{s+t,k}(2P^\theta) \ll (2P^\theta)^{2s+2t} = o(P^{s+t}).$$

However, by considering diagonal solutions alone, we have $J_{s+t,k}(P) \gg P^{s+t}$, which yields a contradiction. Thus $S_1 < \max\{S_2, S_3\}$.

(b) Suppose that $S_3 \geq \max\{S_1, S_2\}$. Then $J_{s+t,k}(P) \leq 9S_3$. By rearranging variables, we find that $R_3(\mathbf{h})$ is at most $\binom{t}{2}$ times the number of solutions of the simultaneous equations (3.5) with $x_1 = x_2$. Then by considering the underlying diophantine equations,

$$S_3 \ll \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; P)^{2s+2t-4} f(2\boldsymbol{\alpha}; P)^2| d\boldsymbol{\alpha}.$$

In this case, therefore, by Hölder's inequality,

$$\begin{aligned} J_{s+t,k}(P) &\ll \left(\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; P)|^{2s+2t} d\boldsymbol{\alpha} \right)^{1-\frac{2}{s+t}} \left(\int_{\mathbb{T}^k} |f(2\boldsymbol{\alpha}; P)|^{2s+2t} d\boldsymbol{\alpha} \right)^{\frac{1}{s+t}} \\ &\ll (J_{s+t,k}(P))^{1-\frac{1}{s+t}}. \end{aligned}$$

Then $J_{s+t,k}(P) \ll 1$, and so once again we arrive at a contradiction. Thus, in view of (a), we deduce that $S_2 \geq \max\{S_1, S_3\}$.

(c) Suppose that $S_2 \geq \max\{S_3, S_1\}$. Then $J_{s+t,k}(P) \leq 9S_2$. For a solution \mathbf{x} counted by $R_2(\mathbf{h})$, let

$$\mathcal{I} = \prod_{1 \leq i < j \leq t} (x_i - x_j).$$

Then $0 < |\mathcal{I}| \leq P^{t(t-1)/2}$, and so the number, N^* , of prime divisors $p \in \mathcal{P}(\theta)$ of \mathcal{I} is at most

$$\frac{t(t-1)}{2\theta} < \left\lceil \frac{k^2}{\theta} \right\rceil + 1 = \text{card}(\mathcal{P}(\theta)).$$

Thus $\text{card}(\mathcal{P}(\theta)) > N^*$, and hence there is a $p \in \mathcal{P}(\theta)$ with $p \nmid \mathcal{I}$. Consequently x_1, \dots, x_t are distinct (mod p). Therefore

$$R_2(\mathbf{h}) \leq \sum_{p \in \mathcal{P}(\theta)} R_4(\mathbf{h}, p),$$

where $R_4(\mathbf{h}, p)$ denotes the number of solutions of the equations (3.5) with $p \leq x_i \leq P$ ($1 \leq i \leq s+t$) and with x_1, \dots, x_t distinct (mod p). Let $I_1(p) = \sum_{\mathbf{h}} R_4(\mathbf{h}, p)^2$. Then $I_1(p)$ is the number of solutions of the simultaneous equations

$$\sum_{i=1}^{s+t} (x_i^j - y_i^j) = 0 \quad (1 \leq j \leq k),$$

with $p \leq x_i, y_i \leq P$ ($1 \leq i \leq s+t$), with x_1, \dots, x_t distinct (mod p), and likewise y_1, \dots, y_t . Further, in this case we have

$$J_{s+t,k}(P) \ll (\text{card } \mathcal{P}(\theta))^2 \max_{p \in \mathcal{P}(\theta)} I_1(p). \quad (3.6)$$

For a fixed prime p , let

$$g(\boldsymbol{\alpha}, y) = \sum_{\substack{p \leq x \leq P \\ x \equiv y \pmod{p}}} e(\alpha_1 x + \dots + \alpha_k x^k),$$

and let \mathcal{A} denote the set of t -tuples $\mathbf{a} = (a_1, \dots, a_t)$ with $0 < a_r \leq p$ and the a_r distinct. Then by considering the underlying diophantine equations, we have

$$I_1(p) = \int_{\mathbb{T}^k} \left| \sum_{\mathbf{a} \in \mathcal{A}} g(\boldsymbol{\alpha}, a_1) \dots g(\boldsymbol{\alpha}, a_t) \right|^2 \left| \sum_{0 \leq x < p} g(\boldsymbol{\alpha}, x) \right|^{2s} d\boldsymbol{\alpha}.$$

By Hölder's inequality,

$$\left| \sum_{0 \leq x < p} g(\boldsymbol{\alpha}, x) \right|^{2s} \leq p^{2s-1} \sum_{0 \leq x < p} |g(\boldsymbol{\alpha}, x)|^{2s},$$

and hence $I_1(p) \leq p^{2s} \max_{0 \leq x < p} I_2(x, p)$, where $I_2(x, p)$ denotes the number of solutions of the simultaneous equations

$$\sum_{i=1}^t (m_i^j - n_i^j) = \sum_{l=1}^s ((py_l + x)^j - (pz_l + x)^j) \quad (1 \leq j \leq k)$$

with

$$p \leq m_i, n_i \leq P \quad (1 \leq i \leq t), \quad 0 < y_l, z_l \leq (P - x)/p \quad (1 \leq l \leq s), \quad (3.7)$$

and with the m_i distinct (mod p), and likewise the n_i . An application of the binomial theorem shows that $I_2(x, p)$ is the number of solutions of the simultaneous equations

$$\sum_{i=1}^t ((m_i - x)^j - (n_i - x)^j) = \sum_{l=1}^s p^j (y_l^j - z_l^j) \quad (1 \leq j \leq k),$$

under the same conditions.

Write

$$q_i(\mathbf{z}) = z_1^i + \cdots + z_t^i \quad (1 \leq i \leq k).$$

Then on making a change of variables, $I_2(x, p)$ is bounded above by the number of solutions of the simultaneous equations

$$q_j(\mathbf{m}) - q_j(\mathbf{n}) = p^j \sum_{l=1}^s (y_l^j - z_l^j) \quad (1 \leq j \leq k), \quad (3.8)$$

with

$$1 \leq m_i, n_i \leq P \quad (1 \leq i \leq t), \quad 1 \leq y_l, z_l \leq Q \quad (1 \leq l \leq s), \quad (3.9)$$

and with the m_i distinct (mod p), and likewise the n_i . For each solution of the latter equations, we have

$$q_j(\mathbf{m}) \equiv q_j(\mathbf{n}) \pmod{p^j} \quad (1 \leq j \leq k),$$

so that each solution of (3.8) subject to (3.9) may be classified according to the common residue class (mod p^j) of $q_j(\mathbf{m})$ and $q_j(\mathbf{n})$ for each j . Let $\mathcal{B}^*(p; \mathbf{u})$ denote the set of solutions (z_1, \dots, z_t) distinct (mod p^r) of the system of congruences

$$q_i(\mathbf{z}) \equiv u_i \pmod{p^i} \quad (1 \leq i \leq k),$$

with the z_i distinct (mod p). Then by Lemma 2.1 we have $\text{card}(\mathcal{B}^*(p; \mathbf{u})) \ll p^{\omega(r, t, k)}$. Let

$$H(\boldsymbol{\alpha}; \mathbf{z}) = \sum_{\substack{1 \leq x_1 \leq P \\ x_1 \equiv z_1 \pmod{p^r}}} \cdots \sum_{\substack{1 \leq x_t \leq P \\ x_t \equiv z_t \pmod{p^r}}} e(\alpha_1 q_1(\mathbf{x}) + \cdots + \alpha_k q_k(\mathbf{x})).$$

Then $I_2(x, p) \ll V(p)$, where on writing $\boldsymbol{\alpha} p^i$ for $(\alpha_1 p, \dots, \alpha_k p^k)$,

$$V(p) = \int_{\mathbb{T}^k} H_p(\boldsymbol{\alpha}) |f(\boldsymbol{\alpha} p^i; Q)|^{2s} d\boldsymbol{\alpha}, \quad (3.10)$$

and

$$H_p(\boldsymbol{\alpha}) = \sum_{u_1=1}^p \cdots \sum_{u_k=1}^{p^k} \left| \sum_{\mathbf{z} \in \mathcal{B}^*(p; \mathbf{u})} H(\boldsymbol{\alpha}; \mathbf{z}) \right|^2.$$

But by Cauchy's inequality,

$$H_p(\boldsymbol{\alpha}) \leq \sum_{u_1=1}^p \cdots \sum_{u_k=1}^{p^k} \text{card}(\mathcal{B}^*(p; \mathbf{u})) \sum_{\mathbf{z} \in \mathcal{B}^*(p; \mathbf{u})} |H(\boldsymbol{\alpha}; \mathbf{z})|^2.$$

Therefore, by collecting the above results together with (3.10) we obtain

$$I_1(p) \ll p^{2s + \omega(r, t, k)} \sum_{z_1=1}^{p^r} \cdots \sum_{z_t=1}^{p^r} \int_{\mathbb{T}^k} |H(\boldsymbol{\alpha}; \mathbf{z})|^2 |f(\boldsymbol{\alpha} p^i; Q)|^{2s} d\boldsymbol{\alpha},$$

and the lemma now follows from (3.6) on considering the underlying diophantine equations.

4. EFFICIENT DIFFERENCING AND THE ITERATIVE PROCESS

Having prepared the ground, we are now able to extract an efficient difference in much the same way as was done in [W2, Lemma 4.1]. Thus, ultimately, we shall be able to restrict attention to the integral

$$\mathcal{M}_s(P; p) = \int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)^t f(\boldsymbol{\alpha}\mathbf{p}^i; Q)^{2s}| d\boldsymbol{\alpha}. \quad (4.1)$$

Lemma 4.1. *Whenever $p \in \mathcal{P}(\theta)$, we have*

$$\mathcal{L}_s(P; p) \ll P^t J_{s,k}(Q) + \mathcal{M}_s(P; p).$$

Proof. On writing

$$I_p(\boldsymbol{\alpha}) = \sum_{z=1}^{p^r} \left| \sum_{\substack{1 \leq x \leq P \\ x \equiv z \pmod{p^r}}} e(\alpha_1 x + \cdots + \alpha_k x^k) \right|^2,$$

we find, by considering the underlying diophantine equations, that

$$\mathcal{L}_s(P; p) = \int_{\mathbb{T}^k} I_p(\boldsymbol{\alpha})^t |f(\boldsymbol{\alpha}\mathbf{p}^i; Q)|^{2s} d\boldsymbol{\alpha}.$$

Further,

$$\mathcal{L}_s(P; p) \ll U_0 + U_1,$$

where U_0 denotes the number of solutions of the equations (3.2) subject to (3.3) and (3.4), and with $z_n = w_n$ for some n with $1 \leq n \leq t$, and U_1 denotes the corresponding number of solutions with $z_n \neq w_n$ ($1 \leq n \leq t$). We divide into cases.

(i) *Suppose that $U_0 \geq U_1$.* By considering the underlying diophantine equations,

$$U_0 \ll P \int_{\mathbb{T}^k} I_p(\boldsymbol{\alpha})^{t-1} |f(\boldsymbol{\alpha}\mathbf{p}^i; Q)|^{2s} d\boldsymbol{\alpha}.$$

An application of Hölder's inequality gives

$$\begin{aligned} \mathcal{L}_s(P; p) &\ll P \left(\int_{\mathbb{T}^k} I_p(\boldsymbol{\alpha})^t |f(\boldsymbol{\alpha}\mathbf{p}^i; Q)|^{2s} d\boldsymbol{\alpha} \right)^{1-1/t} \left(\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}\mathbf{p}^i; Q)|^{2s} d\boldsymbol{\alpha} \right)^{1/t} \\ &= P (\mathcal{L}_s(P; p))^{1-1/t} (J_{s,k}(Q))^{1/t}, \end{aligned}$$

and the result now follows in the first case.

(ii) *Suppose that $U_1 \geq U_0$.* For each solution of (3.2) counted by U_1 , we have

$$z_n \equiv w_n \pmod{p^r} \quad \text{and} \quad z_n \neq w_n \quad (1 \leq n \leq t).$$

Then for some h_n with $1 \leq |h_n| \leq H$, we have

$$w_n = z_n + h_n p^r \quad (1 \leq n \leq t). \quad (4.2)$$

On substituting (4.2) into (3.2), we deduce that

$$U_1 \leq \sum_{\eta_1} \cdots \sum_{\eta_t} U_2(\eta_1, \dots, \eta_t),$$

where the summation is over $\eta_i = \pm 1$ ($1 \leq i \leq t$), and where $U_2(\boldsymbol{\eta})$ is the number of solutions of the system of equations

$$\sum_{j=1}^t \eta_j \Psi_{i,r}(z_j, h_j, p) + p^i \sum_{m=1}^s (u_m^i - v_m^i) = 0 \quad (1 \leq i \leq k),$$

with \mathbf{z}, \mathbf{u} and \mathbf{v} satisfying (3.3) and (3.4), and $1 \leq h_j \leq H$ ($1 \leq j \leq t$). Then on recalling (2.3), and considering the underlying diophantine equations,

$$U_1 \leq \sum_{\boldsymbol{\eta}} \int_{\mathbb{T}^k} \left(\prod_{j=1}^t F_r(\eta_j \boldsymbol{\alpha}; p) \right) |f(\boldsymbol{\alpha} \mathbf{p}^i; Q)|^{2s} d\boldsymbol{\alpha},$$

where the summation is over $\boldsymbol{\eta} \in \{+1, -1\}^t$. Thus

$$U_1 \ll \int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)^t f(\boldsymbol{\alpha} \mathbf{p}^i; Q)^{2s}| d\boldsymbol{\alpha},$$

and by (4.1) the proof of the lemma is complete.

In the next lemma we combine Lemmata 3.1 and 4.1 in order to estimate $J_{s+t,k}(P)$ in terms of $J_{s,k}(Q)$ and $\mathcal{M}_s(P; p)$. The latter may be bounded by means of Lemma 2.2. It transpires, in the analysis of the recurrence relations which follows, that our analysis is simplified by proving a slightly weaker result in this lemma than is in fact attainable. This ensures that certain parameters which arise are integral.

Lemma 4.2. *Let $l = [k/2]$ and $u = \left[s \left(1 - \frac{t}{2l} \right)^{-1} + 1 \right]$. Suppose that r and t are as in the hypotheses at the start of section 3, and further $t < 2l$. Then*

$$J_{s+t,k}(P) \ll M^{2s+\omega(r,t,k)} \left(P^t J_{s,k}(Q) + (PH)^{t/2} (J_{u,k}(Q))^{s/u} \right).$$

Proof. By applying Hölder's inequality to (4.1), we obtain

$$\mathcal{M}_s(P; p) \ll \left(\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2l} d\boldsymbol{\alpha} \right)^{\frac{t}{2l}} \left(\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha} \mathbf{p}^i; Q)|^{2u} d\boldsymbol{\alpha} \right)^{\frac{s}{u}} \left(\int_{\mathbb{T}^k} d\boldsymbol{\alpha} \right)^{1 - \frac{t}{2l} - \frac{s}{u}}. \quad (4.3)$$

(Notice here that $\frac{t}{2l} + \frac{s}{u} \leq \frac{t}{2l} + 1 - \frac{t}{2l} = 1$). But by Lemma 2.2, we have

$$\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2l} d\boldsymbol{\alpha} \ll (PH)^l, \quad (4.4)$$

and further, by considering the underlying diophantine equations,

$$\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha} \mathbf{p}^i; Q)|^{2u} d\boldsymbol{\alpha} = \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; Q)|^{2u} d\boldsymbol{\alpha} = J_{u,k}(Q). \quad (4.5)$$

The lemma now follows by combining (4.3)-(4.5) with Lemmata 3.1 and 4.1.

In order to consider the values which we should assign to the free parameters, we shall set up some notation. We shall say that a sequence of real numbers $(\delta_s) = (\delta_{s,k})$ is *permissible* whenever the sequence has the property that

$$J_{s,k}(P) \ll P^{s+\delta_{s,k}} \quad (1 \leq s \leq k^3).$$

We record some elementary properties of permissible sequences in the following lemma.

Lemma 4.3. *Permissible sequences $(\delta_{s,k})$ exist with $0 \leq \delta_s \leq s$, and satisfying the property that whenever $u \geq s$, we have $u\delta_s \leq s\delta_u$.*

Proof. Permissible sequences certainly exist, since for each s the estimate $J_{s,k}(P) \ll P^{2s}$ is trivial. Moreover, this bound shows that for each s we may take $\delta_s \leq s$ in any permissible sequence. Next, on noting that the diagonal solutions $x_i = y_i$ ($1 \leq i \leq s$) of (1.3) give $\gg P^s$ solutions, we deduce that for each s we have $\delta_s \geq 0$ in any permissible sequence. Finally, whenever $u \geq s$, we may apply Hölder's inequality to deduce that

$$\int_0^1 |f(\boldsymbol{\alpha}; P)|^{2s} d\boldsymbol{\alpha} \leq \left(\int_0^1 |f(\boldsymbol{\alpha}; P)|^{2u} d\boldsymbol{\alpha} \right)^{s/u},$$

and hence that in any permissible sequence, $\delta_s \leq \frac{s}{u}\delta_u$. This completes the proof of the lemma.

Now consider the conclusion of Lemma 4.2. Suppose that $(\delta_{s,k})$ is a sequence of permissible exponents. Let us choose θ so that

$$P^t Q^{s+\delta_s} = (PH)^{t/2} (Q^{u+\delta_u})^{s/u}.$$

On recalling (3.1), we therefore put

$$\frac{1}{2}rt\theta = \left(\frac{s}{u}\delta_u - \delta_s\right)(1-\theta),$$

and hence

$$\theta = \frac{2(s\delta_u - u\delta_s)}{urt + 2(s\delta_u - u\delta_s)}. \quad (4.6)$$

Notice that by Lemma 4.3 we may suppose that θ is positive. Suppose, for the moment, that $\theta < 1/r$. Then by Lemma 4.2, with this choice of θ ,

$$J_{s+t,k}(P) \ll M^{2s+\omega(r,t,k)} P^t (P/M)^{s+\delta_s}. \quad (4.7)$$

Define the real number δ'_{s+t} by

$$\delta'_{s+t} = \delta_s(1-\theta) + (s + \omega(r,t,k))\theta,$$

with θ defined by (4.6). Then by (4.7) we have the estimate

$$J_{s+t,k}(P) \ll P^{s+t+\delta'_{s+t}}. \quad (4.8)$$

Naturally, the implicit constant in (4.8) may be larger than that associated with δ_{s+t} . For the values of s which concern us in this paper, the optimum choice for r_s is $k+1-t_s$. Then by (2.1) and a little calculation, the conclusion (4.8) holds with

$$\delta'_{s+t} = \delta_s(1-\theta) + s\theta, \quad (4.9)$$

and

$$\theta = \frac{2s\delta_u}{ut(k+1-t)}. \quad (4.10)$$

For the application at hand we shall replace (4.9) by the weaker (implicit) bound

$$\delta'_{s+t} = \delta_s + s\theta. \quad (4.11)$$

This simplification reduces the technical complexity of our argument a little, and would appear to cause no significant loss for the values of s which concern us.

We now consider the possibility that the value of θ given by (4.6) exceeds $1/r$. In this case we take $\theta = 1/r$. Then by (3.2), (3.3) and (3.4), for $p \in \mathcal{P}(\theta)$ we have

$$\mathcal{L}_s(P;p) \ll P^t J_{s,k}(Q),$$

and so by Lemma 3.1,

$$J_{s+t,k}(P) \ll M^{2s+\omega(r,t,k)} P^t Q^{s+\delta_s}.$$

Take $r = k+1-t$. Then $\omega(r,t,k) = 0$, and so

$$J_{s+t,k}(P) \ll P^{s+t+\delta_s} M^{s-\delta_s} \ll P^{s+t+\delta'_{s+t}},$$

with

$$\delta'_{s+t} = \delta_s(1-1/r) + s/r. \quad (4.12)$$

But for any ϕ exceeding $1/r$ we have

$$\delta_s(1-1/r) + s/r \leq \delta_s + s/r \leq \delta_s + s\phi,$$

and hence (4.10) and (4.11) generate a permissible sequence even in this case.

The above strategy permits us to set up an iterative process (cf. [VW, section 2]) in the following manner. Suppose that the sequence (δ_s) is permissible. We define a new sequence of real numbers (δ'_s) as follows. When $1 \leq s \leq k$ we put $\delta'_s = 0$, and for each $s > k$ we define δ'_s by means of the recurrence relations

$$\delta'_{s+t} = \delta'_s + s\theta, \quad (4.13)$$

where θ is given by (4.10). Then by the above arguments, the sequence (δ'_s) is permissible. We may now substitute (δ'_s) for (δ_s) , and repeat the whole process.

5. THE RECURRENCE RELATIONS

We must now attend to the matter of solving the recurrence relations implicit in the treatment of the preceding section. In order to start the iteration process, we could simply use the trivial estimate $\delta_s = s$ ($1 \leq s \leq k^3$). However, we can do better by using the recurrence sequence (4.12) with $t = \lfloor \frac{1}{2}(k+1) \rfloor$ and $r = k+1-t$, thereby obtaining a result of similar strength to that of [T, Theorem 1]. We may take $\delta_s = 0$ ($1 \leq s \leq k$), so by repeated use of (4.12) we find that the sequence (δ'_s) is permissible, where

$$\delta'_s = \sum_{l=1}^{\lfloor s/t \rfloor} \frac{s-lt}{r} = \frac{s}{r} \left\lfloor \frac{s}{t} \right\rfloor - \frac{t}{2r} \left\lfloor \frac{s}{t} \right\rfloor \left(\left\lfloor \frac{s}{t} \right\rfloor + 1 \right) < \frac{2s^2}{k^2}. \quad (5.1)$$

Although our method is effective when k is small, for the sake of simplicity of exposition, we shall suppose that $k \geq 20$. We proceed in an inductive manner. Suppose that α , β and C are positive real numbers with $2 \leq \alpha \leq k/2e$ and $\beta \geq \alpha$, and satisfying the property that the sequence (δ_s) , with $\delta_s = Cs^\alpha k^{-\beta}$, is permissible. Let $l = \lfloor k/2 \rfloor$, and let t be a positive integer with $t < 2l$. Then by the conclusions of section 4 the sequence (δ'_s) is permissible, where $\delta'_s = 0$ ($1 \leq s \leq k$), and δ'_s is defined for $s > k$ by

$$\delta'_{s+t} = \delta'_s + s\theta, \quad (5.2)$$

where

$$\theta = \frac{2s}{ut(k+1-t)} Cu^\alpha k^{-\beta}, \quad (5.3)$$

and $u = \left\lfloor s \left(1 - \frac{t}{2l}\right)^{-1} + 1 \right\rfloor$. Take $t = \lfloor 2l/\alpha \rfloor$. Then the hypotheses on t and r at the start of section 3 are satisfied, since

$$4 \leq \left\lfloor \frac{k-1}{k/2e} \right\rfloor \leq t \leq \frac{1}{2}k.$$

We note also that

$$\frac{\alpha}{2l} \leq t^{-1} \leq \frac{\alpha}{k} \left(1 - \frac{\alpha+1}{k}\right)^{-1}, \quad (5.4)$$

and

$$u \leq s(1-1/\alpha)^{-1} + 1 \leq s(1-1/\alpha)^{-1}(1+1/s). \quad (5.5)$$

By some elementary analysis, when $\alpha \geq 2$ we have

$$(1-1/\alpha)^{-\alpha} \leq \exp\left(1 + \frac{1}{2\alpha-2}\right) \leq e\left(1 + \frac{1}{2\alpha-3}\right), \quad (5.6)$$

and $(1+1/s)^\alpha \leq e^{\alpha/s}$. On substituting (5.4)-(5.6) into (5.3), we deduce that

$$\theta \leq 2\alpha C \frac{s^\alpha e^{1+\alpha/s}}{k^{\beta+2}} \left(\frac{2\alpha-2}{2\alpha-3}\right) \left(1 - \frac{\alpha+1}{k}\right)^{-1}.$$

Then on using (5.2), when $s \geq l$ we have

$$\delta'_{s+t} \leq \delta'_s + 2\alpha C e^{1+\alpha/l} \frac{s^{\alpha+1}}{k^{\beta+2}} \left(\frac{2\alpha-2}{2\alpha-3}\right) \left(1 - \frac{\alpha+1}{k}\right)^{-1}.$$

Therefore, on recalling that we may assume that $\delta'_s = 0$ ($1 \leq s \leq k$), and solving the simple recurrence relation, we obtain

$$\delta'_s \leq \frac{2\alpha C e^{1+\alpha/l}}{k^{\beta+2}} \left(\frac{2\alpha-2}{2\alpha-3}\right) \left(1 - \frac{\alpha+1}{k}\right)^{-1} \sum_{1 \leq l < \lfloor s/t \rfloor} (s-lt)^{\alpha+1}. \quad (5.7)$$

But

$$\sum_{1 \leq l < \lfloor s/t \rfloor} (s-lt)^{\alpha+1} < t^{\alpha+1} \int_0^{s/t} \left(\frac{s}{t} - x\right)^{\alpha+1} dx = \frac{s^{\alpha+2}}{t(\alpha+2)}.$$

Then on noting that

$$\frac{\alpha(2\alpha - 2)}{(2\alpha - 3)(\alpha + 2)} \leq 1 \quad (\alpha \geq 2),$$

and recalling (5.4), we deduce from (5.7) that

$$\delta'_s < \frac{2\alpha C e^{1+\alpha/l} s^{\alpha+2}}{k^{\beta+3}} \left(1 - \frac{\alpha+1}{k}\right)^{-2}. \quad (5.8)$$

We now construct a sequence of sequences, $(\delta_s^{(I)})$ ($1 \leq I \leq k/4e$), as follows. We take $\delta_s^{(1)} = 2s^2/k^2$ ($1 \leq s \leq k^3$), and for $I \geq 1$ we take

$$\delta_s^{(I)} = C_I s^{\alpha_I} k^{-\beta_I},$$

where $\alpha_I = 2I$, $\beta_I = 3I - 1$, and

$$\begin{aligned} C_I &= 2 \prod_{i=1}^{I-1} \left(2\alpha_i e^{1+\alpha_i/l} \left(1 - \frac{\alpha_i+1}{k}\right)^{-2} \right) \\ &= 2^{2I-1} e^{(I-1)(1+I/l)} (I-1)! \prod_{i=1}^{I-1} \left(1 - \frac{2i+1}{k}\right)^{-2}. \end{aligned}$$

Then $(\delta_s^{(1)})$ is permissible, by the argument leading to (5.1). Also, by iterating (5.8), each sequence $(\delta_s^{(I)})$ ($I \geq 1$) is permissible. Next we observe that

$$\prod_{i=1}^{I-1} \left(1 - \frac{2i+1}{k}\right)^{-1} \leq k^{I-1} \prod_{i=1}^{I-1} (2l - 2i - 1)^{-1} \leq \left(\frac{1}{2}k\right)^{I-1} \frac{(l-I)!}{(l-2)!}.$$

Thus

$$C_I \leq 2e^{(I-1)(1+I/l)} (I-1)! k^{2I-2} \left(\frac{(l-I)!}{(l-2)!}\right)^2.$$

But by Stirling's formula,

$$\log((I-1)!) = (I - \frac{1}{2}) \log I - I + O(1),$$

and

$$\log\left(\frac{(l-I)!}{(l-2)!}\right) = (l + \frac{1}{2}) \log\left(1 - \frac{I}{l}\right) - I \log(l-I) + I + 2 \log l + O(1).$$

Therefore,

$$\log \delta_s^{(I)} = I \log\left(\frac{e^2 s^2 I}{k(l-I)^2}\right) + \log\left(k^3 I^{-\frac{1}{2}}\right) + (2l+1) \log\left(1 - \frac{I}{l}\right) + \frac{I(I-1)}{l} + O(1).$$

An elementary optimisation reveals that we should choose I to be the integer closest to ξ , where ξ is the smallest positive root of the equation

$$4s^2 \xi e^{1+4\xi/k} = k(k - 2\xi)^2. \quad (5.9)$$

Thus $I = \xi(1 + O(s^2/k^3))$, and indeed $I < \frac{k^3}{4es^2} < \frac{k}{4e}$ in the non-trivial range $s > k$. Consequently, the optimum choice of I occurs in the interval which we have considered. A little calculation reveals that with this choice of I , we have

$$\log \delta_s^{(I)} = \log\left(\xi^{-\frac{1}{2}} k^3\right) + \xi + 2\xi^2/k + (2l+1) \log\left(1 - \frac{\xi}{l}\right) + O(1), \quad (5.10)$$

and Theorem 1 now follows on exponentiation.

To establish Corollary 1.1, we merely observe that the smallest positive root of the equation (5.9) satisfies

$$\xi = \frac{k^3}{4es^2} \left(1 + O\left(\frac{k^2}{s^2}\right)\right).$$

Hence in (5.10),

$$\xi + 2\xi^2/k + (2l + 1) \log \left(1 - \frac{\xi}{l} \right) = - \left(1 + O \left(\frac{k^2}{s^2} \right) \right) \xi,$$

and therefore,

$$\delta_{s,k} = \xi^{-1/2} k^3 \exp \left(- \frac{k^3}{4es^2} \left(1 + O \left(\frac{k^2}{s^2} \right) \right) \right)$$

is a permissible exponent. Finally, to establish Corollary 1.2 we observe that when $s = (1 + o(1))k$, the smaller root of the equation (5.9) is $(\zeta + o(1))k$, where ζ is the smaller root of the equation

$$4e^{1+4\zeta}\zeta = (1 - 2\zeta)^2.$$

A little computation reveals that $\zeta = 0.057320\dots$. Then by (5.10), it follows that

$$\delta_{s,k}^{(I)} \ll \exp \left((\zeta + 2\zeta^2 + \log(1 - 2\zeta) + o(1))k \right),$$

and the desired conclusion follows with a modicum of computation.

6. ITERATIVE SCHEMES IN WARING'S PROBLEM

We now turn our attention to mean value theorems for exponential sums arising from the new iterative methods in Waring's problem. The basic plan of attack follows closely the treatment of [Va2]. It is in the derivation and treatment of the recurrence relations that our approach differs. We start by recalling some of the methods developed in previous work (see [Va1,2, VW, W1]).

Throughout, s will denote a positive integer, and ε and η will denote sufficiently small positive numbers. We take P to be a large positive real number depending at most on k , s , ε and η . Implicit constants will depend at most on k , s , ε and η . In order to simplify our analysis, we adopt the following convention concerning the numbers ε and R . Whenever ε or R appear in a statement, either implicitly or explicitly, we assert that for each $\varepsilon > 0$, there exists a positive number $\eta_0(\varepsilon, s, k)$ such that the statement holds whenever $R = P^\eta$, with $0 < \eta \leq \eta_0(\varepsilon, s, k)$. Note that the "value" of ε , and η_0 , may change from statement to statement, and hence also the dependency of implicit constants on ε and η .

For each $s \in \mathbb{N}$ we take $\theta = \theta_s$ to be a real number with $0 \leq \theta \leq 1/k$, to be chosen later. We then take

$$M = P^\theta, \quad H = PM^{-k}, \quad Q = PM^{-1}. \quad (6.1)$$

Let

$$\Psi = \Psi(z; h; m) = m^{-k} \left((z + hm^k)^k - (z - hm^k)^k \right).$$

Write

$$f(\alpha) = \sum_{x \in \mathcal{A}(Q, R)} e(\alpha x^k).$$

Also, write

$$F(\alpha) = \sum_{z, h, m} e(\alpha \Psi(z, h, m)),$$

where the summation is over z, h, m with

$$1 \leq z \leq P, \quad M < m \leq MR, \quad 1 \leq h \leq H.$$

We let $S_s(P, R)$ denote the number of solutions of the equation (1.7), as in section 1. Suppose that the real numbers λ_s have the property that

$$S_s(P, R) \ll P^{\lambda_s + \varepsilon}.$$

Such numbers certainly exist, since we may trivially take $\lambda_s = 2s$. We now provide a lemma with which to better estimate the λ_s .

Lemma 6.1. *We have*

$$S_{s+1}(P, R) \ll P^\varepsilon M^{2s-1} \left(PMQ^{\lambda_s} + (PMHQ^{\lambda_{2s}})^{1/2} \right).$$

Proof. By [VW, Lemma 2.1], we have

$$S_{s+1}(P, R) \ll P^\varepsilon M^{2s-1} (PMQ^{\lambda_s} + I),$$

where

$$I = \int_0^1 |F(\alpha)f(\alpha)^{2s}| d\alpha.$$

But by [Va2, (2.14)] (which is essentially the last line of Lemma 2.1 of that paper), we have

$$\int_0^1 |F(\alpha)|^2 d\alpha \ll P^{1+\varepsilon} MH.$$

Then by Schwarz's inequality,

$$I^2 \ll P^{1+\varepsilon} MH \int_0^1 |f(\alpha)|^{4s} d\alpha \ll P^{1+\varepsilon} MHQ^{\lambda_{2s}},$$

and the lemma follows.

As in §4, we set up some notation in order to consider the values which we should assign to the free parameters. We shall now say that a sequence of real numbers $(\gamma_{s,k})$ is *permissible* whenever the sequence has the property that

$$S_s(P, R) \ll P^{s+\gamma_{s,k}+\varepsilon} \quad (1 \leq s \leq k^2).$$

Permissible sequences certainly exist, since the estimate $S_s(P, R) \ll P^{2s}$ is trivial for each s . Thus, for each s we may take $\gamma_s \leq s$ in any permissible sequence. Furthermore, on noting that the diagonal solutions $x_i = y_i$ ($1 \leq i \leq s$) of (1.7) give $\gg P^s$ solutions, we deduce that for each s we have $\gamma_s \geq 0$ in any permissible sequence. Also, an application of Schwarz's inequality shows that we may assume that $\gamma_s \leq \frac{1}{2}\gamma_{2s}$ for each s in any permissible sequence.

Now consider the conclusion of Lemma 6.1. Suppose that $(\gamma_{s,k})$ is a sequence of permissible exponents. Let us choose θ so that

$$PMQ^{s+\gamma_s} = (PMHQ^{2s+\gamma_{2s}})^{1/2}.$$

On recalling (6.1), we therefore put

$$\frac{1}{2}(k+1)\theta = \left(\frac{1}{2}\gamma_{2s} - \gamma_s\right)(1-\theta),$$

and hence

$$\theta = \frac{\gamma_{2s} - 2\gamma_s}{k+1 + \gamma_{2s} - 2\gamma_s}.$$

Notice that the assumption $\gamma_s \leq \frac{1}{2}\gamma_{2s}$ ensures that θ is positive. By Lemma 6.1, with this choice of θ we have

$$S_{s+1}(P, R) \ll M^{2s} P^{1+\varepsilon} (P/M)^{s+\gamma_s},$$

the possibility that $\theta > 1/k$ being discarded as with the treatment of Vinogradov's mean value theorem. Define the real number γ'_{s+1} by

$$\gamma'_{s+1} = \gamma_s(1-\theta) + s\theta,$$

where θ is defined as above. Then we have the estimate

$$S_{s+1}(P, R) \ll P^{s+1+\gamma'_{s+1}+\varepsilon}.$$

The above strategy permits us to set up an iterative process. Suppose that the sequence (γ_s) is permissible. We define a new sequence of real numbers (γ'_s) as follows. When $s = 1, 2$ we put $\gamma'_s = 0$, and for each $s > 2$ we define γ'_s by means of the recurrence relations

$$\gamma'_{s+1} = \gamma'_s(1-\theta) + s\theta, \tag{6.2}$$

where

$$\theta = \frac{\gamma_{2s}}{k+1}. \tag{6.3}$$

Then by the above arguments, the sequence (γ'_s) is permissible. We may now substitute (γ'_s) for (γ_s) , and repeat the whole process.

7. MORE RECURRENCE RELATIONS

We now attend to the matter of solving the recurrence relations implicit in the treatment of the preceding section. We start with the trivial estimate $\gamma_s = s$ ($1 \leq s \leq k^2$), and proceed inductively. Suppose that the sequence (γ_s) , with $\gamma_s = Cs^\alpha k^{-\beta}$, is permissible for some fixed α and β . Then by the conclusions of §6, the sequence γ'_s is permissible, where $\gamma'_s = 0$ ($s = 1, 2$), and for $s > 2$, by (6.2) and (6.3), γ'_s is defined by

$$\gamma'_{s+1} = \gamma'_s(1 - \theta) + s\theta,$$

where

$$\theta \leq C(2s)^\alpha k^{-\beta-1}.$$

Then

$$\gamma'_{s+1} \leq \gamma'_s + 2^\alpha Cs^{\alpha+1} k^{-\beta-1}.$$

Therefore, on using this last relation inductively, we deduce that

$$\gamma'_s \leq \frac{2^\alpha C}{k^{\beta+1}} \sum_{l=0}^{s-1} l^{\alpha+1} \leq \frac{2^\alpha Cs^{\alpha+2}}{(\alpha+2)k^{\beta+1}}. \quad (7.1)$$

We now construct a sequence of sequences $(\gamma_s^{(I)})$ as follows. We take $\gamma_s^{(1)} = s$, and

$$\gamma_s^{(I)} = C_I s^{\alpha_I} k^{-\beta_I},$$

where

$$\alpha_I = 2I - 1, \quad \beta_I = I - 1,$$

and

$$C_I = \prod_{i=1}^{I-1} \frac{2^{2i-1}}{2i+1} = \frac{2^{I(I-1)}(I-1)!}{(2I-1)!}.$$

Then by (7.1), each sequence $(\gamma_s^{(I)})$ is permissible. We now apply Stirling's formula to obtain the estimate

$$\log \left(\frac{(I-1)!}{(2I-1)!} \right) = (I - \frac{1}{2}) \log(I-1) - (2I - \frac{1}{2}) \log(2I-1) + I + O(1).$$

Therefore,

$$\log \gamma_s^{(I)} = I(I-1) \log 2 + I \log(s^2/k) - \log(s/k) + I - 2I \log 2 - I \log I + O(1).$$

A simple optimisation reveals that we should take I to be the integer nearest the real number ξ , where

$$(2 \log 2)\xi = \log(k/s^2) + \log \log(k/s^2) + O(1).$$

Using this value of I , we find that

$$\log \gamma_s^{(I)} = \log(k/s) - \xi^2 \log 2 + O(\xi).$$

is permissible, and Theorem 2 follows immediately.

8. REMARKS ON GENERALISATIONS, AND THE *ABC*-CONJECTURE

The methods of this paper may be generalised to demonstrate quasi-diagonal behaviour in mean values of exponential sums of the form

$$f_{\mathbf{k}}(\boldsymbol{\alpha}; P) = \sum_{x \in \mathcal{A}(P, R)} e(\alpha_1 x^{k_1} + \dots + \alpha_m x^{k_m}),$$

where k_i ($1 \leq i \leq m$) are integers satisfying $1 \leq k_1 < \dots < k_m = k$. Suitable estimates for the mean values

$$U_s(P, R) = \int_{\mathbb{T}^t} |f_{\mathbf{k}}(\boldsymbol{\alpha}; Q)|^{2s} d\boldsymbol{\alpha} \quad (8.1)$$

may be established through a generalisation of the iterative method of [W1] developed in [W4]. Furthermore, the main result of [St] implies that when $1 \leq s \leq m$, the only solutions in positive numbers of the system of equations

$$\sum_{i=1}^s (x_i^{k_j} - y_i^{k_j}) = 0 \quad (1 \leq j \leq m), \quad (8.2)$$

are the trivial solutions in which the x_i are a permutation of the y_j (I thank Professor A. Schinzel for pointing out the existence of the latter result). Thus a generalisation of Lemma 2.2 suitable for treating the mean value (8.1) follows almost immediately, and we may proceed to establish recurrence relations as in sections 4 and 5. The precise nature of the ensuing results depends very much on the distribution of the k_i throughout the interval $[1, k]$. However, if the distribution is relatively uniform, and $m \asymp k^\theta$ with $0 < \theta < 1$, then roughly speaking, the methods alluded to above will establish quasi-diagonal behaviour for the mean value (8.1) whenever $s \leq c_1 m k^{1/2}$, for a suitable constant c_1 . Furthermore, when $s \leq Am$ these methods will establish bounds of the type

$$U_s(P, R) \ll_{\varepsilon, A} P^{s+\beta_{s,k}+\varepsilon},$$

where $\beta_{s,k}$ behaves like $\exp(-c_2 m \log(k/m))$, for a suitable positive $c_2 = c_2(A)$.

At the end of section 2 we observed that strongly diagonal behaviour lies at the core of our argument. Indeed, if a system exhibits almost totally diagonal behaviour for a given number of variables, then one may establish quasi-diagonal behaviour (for the corresponding mean value) in a rather larger number of variables. This is a principle we shall illustrate through the following hypothesis. We recall that a solution of the system (8.2) is diagonal if the x_i are a permutation of the y_j .

Hypothesis $D_{\mathbf{k},m}(S)$ (totally diagonal behaviour). *Let k_i ($1 \leq i \leq m$) be positive integers with $k_1 < k_2 < \dots < k_m$, and let s be an integer with $1 \leq s \leq S$. Denote by $D_s(P)$ the number of diagonal solutions of the system (8.2) in which*

$$1 \leq x_i, y_i \leq P \quad (1 \leq i \leq s). \quad (8.3)$$

Then the number, $V_s(P)$, of solutions of the equations (8.2) with (8.3) satisfies

$$V_s(P) - D_s(P) \ll_{s,k} P^{s/2}.$$

For the purposes of this discussion, we shall consider only the situation in which $(k_1, k_2, \dots, k_m) = (1, 2, \dots, k)$. First note that under the assumption of Hypothesis $D_{\mathbf{k},m}(S)$, the argument of the proof of Lemma 2.2 may be refined easily to show that with $w = \lfloor S/2 \rfloor$, we have

$$\int_{\mathbb{T}^k} |F_r(\boldsymbol{\alpha}; p)|^{2w} d\boldsymbol{\alpha} \ll_{k,w} (PH)^w.$$

The conclusion of Lemma 4.2 may therefore be strengthened so that l is replaced by w in its conclusion. We now pursue the same argument as previously, but with the following important observation. Since now

$$u = \left[s \left(1 - \frac{t}{2w} \right)^{-1} + 1 \right],$$

we can exploit the full power of equation (4.6), rather than the simplified form (4.10). Thus, with $\delta_s = Cs^\alpha k^{-\beta}$, we discover that

$$s\delta_u - u\delta_s = s\delta_u (1 - (s/u)^{\alpha-1}) = \left(\frac{(\alpha-1)t}{2w} + O\left(\frac{\alpha^2 t^2}{w^2}\right) \right) s\delta_u.$$

It will now be apparent that the expression for θ in (4.10) can be improved by a factor of order $\alpha t/w$. This, when pushed through the machinery of section 5, leads to improvements in the consequent bounds for $\delta_{s,k}$ as follows. If for some $\omega > 0$ we have $S \gg k^\omega$, then one obtains a bound of the form

$$\delta_{s,k} \ll \exp(-Bk^{2+\omega}/s^2)$$

for a suitable positive constant B , and quasi-diagonal behaviour for $s \ll k^{(2+\omega)/2}$. There are similar consequences for the mean value $S_s(P, R)$ discussed in sections 6 and 7, so that, for example, if one has totally diagonal behaviour with s out to around k^ϕ , then one may deduce quasi-diagonal behaviour with s out to around $k^{(1+\phi)/2}$.

At present we know only that Hypothesis $D_{\mathbf{k},m}(S)$ holds for $S = m$, and any improvement, even contingent on a reasonable hypothesis, would be of interest. When $m = 1$, the Hypothesis $D_{\mathbf{k},1}(S)$ may be established for substantially larger S on the assumption of a suitable generalisation of the *ABC*-conjecture. Since there is considerable debate over precisely what the latter conjecture should say, at this point we shall state the conjecture in a rather weak form (which, we note, differs somewhat from that given by Schmidt [**Sc**, end of Epilogue]). I thank, in particular, Professors David Masser and Andrew Granville for interesting conversations concerning this topic. We write $s_0(n)$ for the square-free kernel of n , which is to say

$$s_0(n) = \prod_{p|n} p.$$

Conjecture *ABC*(τ). *Suppose that a_i ($1 \leq i \leq s$) are non-zero integers which are mutually coprime (which is to say that $(a_1, \dots, a_s) = 1$). Suppose also that $a_1 + a_2 + \dots + a_s = 0$. Then either some subsum of the a_i vanishes, or else*

$$\max_{1 \leq i \leq s} |a_i| \ll_{s,\varepsilon} (s_0(a_1 \dots a_s))^{\tau(s)+\varepsilon}. \quad (8.4)$$

The consensus amongst the *cognoscenti* seems to be that the correct exponent $\tau(s)$ in this conjecture should satisfy

$$\tau(s) \leq \frac{1}{2}(s-1)(s-2). \quad (8.5)$$

By way of justification we shall merely mention that this conjecture arises by analogy with corresponding theorems in the function field case (see [**BM**]), and has important consequences for a number of diophantine problems (see, for example, [**L**]). A standard argument yields the following conclusion.

Theorem 8.1. *Suppose that Conjecture *ABC*(τ) holds with $\tau(s)$ an increasing function of s . Suppose also that $2S\tau(2S) < k$. Then Hypothesis $D_{\mathbf{k},1}(S)$ holds.*

Proof. We prove that for each $s \leq S$, with at most finitely many exceptions, the only solutions of the equation

$$x_1^k + \dots + x_s^k = y_1^k + \dots + y_s^k \quad (8.6)$$

are the diagonal solutions. We proceed by induction, noting that the case $s = 1$ is trivial. Suppose then that the assertion holds with $2t$ variables for each $t < s$, and that \mathbf{x}, \mathbf{y} is a solution of the equation (8.6). Consider the subsum in which the fewest variables occur (which may contain $2s$ variables), and rewrite this subsum as

$$u_1^k + \dots + u_r^k - v_1^k - \dots - v_t^k = 0,$$

where r and t are integers with $1 \leq r \leq t \leq s$. If $r = t = 1$ we remove two variables from equation (8.6), and then the inductive hypothesis implies that we have only finitely many non-diagonal solutions. Thus we may suppose that $3 \leq r + t \leq 2s$, so that by Conjecture *ABC*(τ) we have

$$\max_{i,j} (|u_i|^k, |v_j|^k) \ll_{s,\varepsilon} s_0(u_1 \dots u_r v_1 \dots v_t)^{\tau(r+t)+\varepsilon}.$$

Therefore

$$|u_1 \dots u_r v_1 \dots v_t|^k \ll_{s,\varepsilon} s_0(u_1 \dots u_r v_1 \dots v_t)^{(r+t)(\tau(r+t)+\varepsilon)}.$$

On taking ε sufficiently small, if $k > 2s\tau(2s) \geq (r+t)\tau(r+t)$, it follows that the u_i and v_i , and consequently the x_i and y_i , are bounded absolutely in terms of ε, s, k . This completes the induction, and the theorem follows immediately.

For an exponent $\tau(s)$ satisfying (8.5), Theorem 8.1 implies that Hypothesis $D_{\mathbf{k},1}(S)$ holds conditionally with $S \gg k^{1/3}$, and consequently the mean value $S_s(P, R)$ exhibits quasi-diagonal solubility for s up to about $k^{2/3}$.

We note that if the coprimality hypothesis of Conjecture *ABC*(τ) is strengthened, then it is expected that the conclusion (8.4) ought to hold for a smaller value of $\tau(s)$. Indeed, by considering the analogous result in the function field case (see [**BM**, Lemma 2]), Andrew Granville and myself expect the following conclusion.

Conjecture. Suppose that a_i ($1 \leq i \leq s$) are non-zero integers with $a_1 + a_2 + \cdots + a_s = 0$. For each prime p , define α_p by

$$\alpha_p = \text{card}\{1 \leq j \leq s : p \nmid a_j\},$$

and β_p by $\beta_p = \frac{1}{2}((s-1)(s-2) - (\alpha_p - 1)(\alpha_p - 2))$. Then either some subsum of the a_i vanishes, or else

$$\max_{1 \leq i \leq s} |a_i| \ll_{s,\varepsilon} \prod_{p|a_1 \dots a_s} p^{\beta_p + \varepsilon}.$$

We note that a fairly standard argument using exponential sums shows that the latter conjecture implies strongly diagonal behaviour for the mean value $S_s(P, P)$ when $s < \frac{1}{2}k^{1/2}$.

By way of a concluding remark, we observe that the generalised *ABC*-conjecture fails to effectively exploit the constraints imposed by simultaneous equations, and thus more precise results are required in order to establish suitable results of the form of Hypothesis $D_{\mathbf{k},m}(S)$ when m is large. At present there appears to be no analogue of the *ABC*-conjecture for simultaneous equations, even in the function field case. Rather than pursue here the likely form of such a result, we merely point out that a strengthening of conclusions concerning quasi-diagonal solubility would follow for the mean value $J_{s,k}(P)$ just as in the above treatment of $S_s(P, R)$.

REFERENCES

- [AK] G. I. Arkhipov and A. A. Karatsuba, *A new estimate of an integral of I.M. Vinogradov*, *Izv. Akad. Nauk SSSR Ser. Mat.* **42** (1978), 751–762; English transl. in *Math. USSR Izv.* **13** (1979).
- [BM] W. D. Brownawell and D. W. Masser, *Vanishing sums in function fields*, *Math. Proc. Camb. Phil. Soc.* **100** (1986), 427–434.
- [H] L.-K. Hua, *Additive theory of prime numbers*, Providence, 1965.
- [KO] G. Kolesnik and A. M. Odlyzko, *An improvement of I.M. Vinogradov's mean value theorem*, Unpublished.
- [L] S. Lang, *Old and new conjectured diophantine inequalities*, *Bull. Am. Math. Soc.* **23** (1990), 37–75.
- [Sc] W. M. Schmidt, *Diophantine approximations and diophantine equations. Lecture notes in mathematics*, Berlin: Springer-Verlag, vol. 1467.
- [St] J. Steinig, *On some rules of Laguerre's, and systems of equal sums of like powers*, *Rend. Mat.* **4** (1971), 629–644.
- [T] O. V. Tyrina, *A new estimate for a trigonometric integral of I.M. Vinogradov*, *Izv. Akad. Nauk SSSR, Ser. Mat.* **51** (1987); English transl. in *Math. USSR Izv.* **30** (1988), 337–351.
- [Vi] I. M. Vinogradov, *New estimates for Weyl sums*, *Dokl. Akad. Nauk SSSR* **8** (1935), 195–198.
- [Va1] R. C. Vaughan, *A new iterative method in Waring's problem*, *Acta Math.* **162** (1989), 1–71.
- [Va2] ———, *A new iterative method in Waring's problem, II*, *J. Lond. Math. Soc.* (2) **39** (1989), 219–230.
- [VW] ——— and T. D. Wooley, *Further improvements in Waring's problem*, Submitted for publication.
- [W1] T. D. Wooley, *Large improvements in Waring's problem*, *Annals of Math.* **135** (1992), 131–164.
- [W2] ———, *On Vinogradov's mean value theorem*, *Mathematika* **39** (1992), 379–399.
- [W3] ———, *A note on symmetric diagonal equations*, *Number theory with an emphasis on the Markoff spectrum* (A. D. Pollington and W. Moran, eds.), Marcel Dekker, 1993, pp. 317–321.
- [W4] ———, *Exponential sums over smooth numbers: bounds and applications*, In preparation.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI48109-1003
E-mail address: wooley@math.lsa.umich.edu