ON VINOGRADOV'S MEAN VALUE THEOREM

TREVOR D. WOOLEY

§1. *Introduction.* The object of this paper is to obtain improvements in Vinogradov's mean value theorem widely applicable in additive number theory. Let $J_{s,k}(P)$ denote the number of solutions of the simultaneous diophantine equations

$$x_1^j + \ldots + x_s^j = y_1^j + \ldots + y_s^j \qquad (1 \leqslant j \leqslant k), \tag{1.1}$$

with $1 \leqslant x_i, y_i \leqslant P$ for $1 \leqslant i \leqslant s$. In the mid-thirties Vinogradov developed a new method (now known as *Vinogradov's mean value theorem*) which enabled him to obtain fairly strong bounds for $J_{s,k}(P)$. On writing

$$f(\boldsymbol{\alpha}; Q) = \sum_{x \leqslant Q} e(\alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_k x^k), \tag{1.2}$$

in which $e(\alpha)$ denotes $e^{2\pi i\alpha}$, we observe that

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

where T^k denotes the k-dimensional unit cube, and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$. It will therefore be readily appreciated that bounds for the mean value $J_{s,k}(P)$ provide information about the size of exponential sums involving functions to which there are reasonable polynomial approximations. Thus there are numerous applications for such bounds, and indeed Vinogradov was able to use his method with great success in areas as diverse as Waring's problem, zero-free regions for the Riemann zeta function, and obtaining bounds for the fractional parts of polynomials (see Vinogradov [**15**] and Walfisz [**16**]).

Stechkin [**9**] and Karatsuba [**7**] have obtained bounds of the form

$$J_{rk,k}(P) \leqslant D(k, r) P^{2rk - \frac{1}{2}k(k+1) + \eta(r,k)} \qquad (r \in \mathbf{N}), \tag{1.3}$$

where $D(k, r)$ is independent of P, and $\eta(r, k) = \frac{1}{2}k^2(1 - 1/k)^r$. Reductions in the permissable value of $\eta(r, k)$ have since been obtained, most recently by Turina [**10**], but these seem to be of importance only for small values of r, the savings being rapidly dissipated as r increases.

In this paper we describe a new method which permits rather substantial improvements to be made in the term $\eta(r, k)$. Roughly speaking, we are able to double the rate at which $\eta(r, k)$ diminishes with respect to r in the region of importance. The precise form of our result is given in the following theorem.

THEOREM 1.1. *Let t and k be positive integers with $t \geqslant k \geqslant 2$, and suppose that μ is a positive real number with $2t - \frac{1}{2}k(k+1) < \mu \leqslant 2t$, and satisfying the property that we have $J_{t,k}(P) \ll_{t,k} P^{\mu}$.*

[MATHEMATIKA, **39** (1992), 379-399]

For $s=t+lk$ $(l=1,2,\ldots)$, define the real numbers λ_s, Δ_s, θ_s and $\varphi(j,s,J)$ recursively as follows. Put $\Delta_t=\mu+\frac{1}{2}k(k+1)-2t$. Then for $l\geqslant 1$ and $j=1,\ldots,k$ put $\varphi(j,s,j)=1/k$, and evaluate $\varphi(j,s,J-1)$ successively for $J=j,\ldots,2$ by

$$\left.\begin{aligned}\varphi^*(j,s,J-1)&=\frac{k+(k^2+\frac{1}{2}(J-1)(J-2)-\Delta_{s-k})\varphi(j,s,J)}{2k^2}\\ \varphi(j,s,J-1)&=\min\{1/k,\varphi^*(j,s,J-1)\}\end{aligned}\right\}. \tag{1.4}$$

Finally, set

$$\theta_s=\min_{1\leqslant j\leqslant k}\varphi(j,s,1), \tag{1.5}$$

$$\Delta_s=\Delta_{s-k}(1-\theta_s)+k(k\theta_s-1), \tag{1.6}$$

$$\lambda_s=2s-\tfrac{1}{2}k(k+1)+\Delta_s. \tag{1.7}$$

Then for each $s=t+lk$ $(l=1,2,\ldots)$ we have $J_{s,k}(P)\ll P^{\lambda_s}$. (Here the implicit constant in Vinogradov's notation depends at most on s and k.)

We remark that in the statement of Theorem 1.1, the Δ_s which appear satisfy $0\leqslant\Delta_s\leqslant k^2$, and so the numbers φ are always positive. Consequently $0\leqslant\theta_s\leqslant 1/k$ for each s. Moreover, $\theta_s=1/k$ immediately yields the "classical" result, so that the superiority of Theorem 1.1 will be obvious. It is useful to have a simplification of Theorem 1.1 of use in applications. The bound which we give below could certainly be refined (along the lines of the treatment of Section 4 of Wooley [17]), but that given has the advantage of simplicity of derivation.

THEOREM 1.2. *There exists an absolute constant k_0 such that whenever $k\geqslant k_0$, we have*

$$J_{rk,k}(P)\ll_{r,k} P^{2rk-\frac{1}{2}k(k+1)+\eta(r,k)},$$

where

$$\eta(r,k)=k^2\log k\left(1-\frac{2}{k}(1-1/\log k)\right)^r \qquad 1\leqslant r\leqslant r_1(k),$$

$$\eta(r,k)=5(\log k)^3\left(1-\frac{3}{2k}(1-1/k)\right)^{r-r_1(k)} \qquad r>r_1(k),$$

in which we have written $r_1(k)=[k(\log k-\log\log k)]+1$.

The dependency on s and k in our bound for $J_{s,k}(P)$ could be found with a little effort. Indeed, it is necessary to make this constant explicit in order to establish zero-free regions for the Riemann zeta function. However, it would seem that our new results do not lead to any significant improvements in the latter, and instead we concentrate on applications of Theorem 1.1 in additive number theory. The method of proof of each of the following corollaries is in each case a simple modification of existing methods, and we go into detail only in the first two cases.

We first obtain bounds for exponential sums.

COROLLARY 1.1. *Let* $\psi(x)=\sum_{j=1}^{k}\alpha_j x^j$, *and put* $f(\boldsymbol{\alpha})=\sum_{n=1}^{P}e(\psi(n))$. *Suppose that there exist* j, a, q *with* $2\leqslant j\leqslant k$, $|\alpha_j-a/q|<q^{-2}$, $(a,q)=1$ *and* $q\leqslant P^j$. *Then if* $P\ll q\ll P^{j-1}$, *we have* $f(\boldsymbol{\alpha})\ll_{\varepsilon,k} P^{1-\sigma+\varepsilon}$, *where*

$$\sigma=\sigma(k)=\max_{s\in\mathbf{N}}\left(\frac{1-\Delta_s}{2s}\right),$$

and Δ_s *is as given in the statement of Theorem* 1.1, *but with* k *replaced by* $k-1$. *In particular,* $(2k^2\log k)\sigma(k)\geqslant 1+o(1)$ *as* $k\to\infty$.

Previously, the best exponent in such results satisfied $(4k^2\log k)\sigma(k)\geqslant 1+o(1)$ as $k\to\infty$ (see Vaughan [11], Theorem 5.3). Note that Baker's generalization of Weyl's inequality (see R. Baker [1], Theorem 5.1) leads to a "minor arc" bound $f(\boldsymbol{\alpha})\ll P^{1-\tau(k)+\varepsilon}$ with $\tau(k)=2^{1-k}$. Also, Heath-Brown [3] has obtained an improvement of the latter exponent to $\tau(k)=2^{3-k}/3$ on a more restricted set of α, at least, when $\psi(n)=\alpha n^k$ and $k\geqslant 6$. Corollary 1.1 improves on the latter exponent whenever $k\geqslant 12$. For small k, explicit values of $\sigma(k)$ are frequently required, so we take this opportunity of recording the values arising from Corollary 1.1 on applying Theorem 1.1 starting from the estimate $J_{k+1,k}(P)\ll_{\varepsilon,k} P^{k+1+\varepsilon}$ (see Hua [6], Lemma 5.4).

COROLLARY 1.1a. *Define* $\sigma(k)$ *as in Corollary* 1.1, *and put* $\rho(k)=10^4\sigma(k)$. *Then we have* $\rho(11)\geqslant 12{\cdot}416$, $\rho(12)\geqslant 9{\cdot}91907$, $\rho(13)\geqslant 8{\cdot}09323$, $\rho(14)\geqslant 6{\cdot}71884$, $\rho(15)\geqslant 5{\cdot}66022$, $\rho(16)\geqslant 4{\cdot}82792$, $\rho(17)\geqslant 4{\cdot}16423$, $\rho(18)\geqslant 3{\cdot}62526$, $\rho(19)\geqslant 3{\cdot}18243$, $\rho(20)\geqslant 2{\cdot}81440$.

Let $\tilde{G}(k)$ denote the least integer t such that for all $s\geqslant t$, and all sufficiently large natural numbers n, we have the asymptotic formula in Waring's problem, that is

$$\operatorname{card}\{\mathbf{x}\in\mathbf{N}^s: n=x_1^k+\ldots+x_s^k\}=(\mathfrak{S}_{s,k}(n)+o(1))\frac{(\Gamma(1+1/k))^s}{\Gamma(s/k)}n^{s/k-1}.$$

Here $\mathfrak{S}_{s,k}(n)$ denotes the usual singular series in Waring's problem (see Vaughan [11], Section 2.6). The first workers to obtain a bound for $\tilde{G}(k)$ were Hardy and Littlewood [2], who obtained $\tilde{G}(k)\leqslant(k-2)2^{k-1}+5$ for $k\in\mathbf{N}$. For small k, this bound has been improved on by Hua [4], who obtained $\tilde{G}(k)\leqslant 2^k+1$, and Vaughan [12, 13], who obtained $\tilde{G}(k)\leqslant 2^k$ for $k\geqslant 3$. Heath-Brown [3] has recently shown that $\tilde{G}(k)\leqslant 7\cdot 2^{k-3}+1$ for $k\geqslant 6$, and quite probably the "+1" can be saved by combining his argument with that of Vaughan [13].

It seems likely that $\tilde{G}(k)=O(k)$, and so the above bounds are clearly rather unsatisfactory, increasing exponentially with k. It was therefore of great interest when Vinogradov [14] proved that $\tilde{G}(k)\leqslant 183k^9(\log k+1)^2$. This bound was improved by Vinogradov, Hua and others, and the best bound currently known is of the form $\tilde{G}(k)<(4+o(1))k^2\log k$ as $k\to\infty$, first proved by Hua [5] in 1949. Since then only the $o(1)$ term has been improved (see Vaughan [11], Section 5.3). Using Theorem 1.1 we obtain the following improvement.

COROLLARY 1.2. *We have* $\tilde{G}(k) \leqslant 1+\min_{s \in \mathbf{N}} (2s+\Delta_s/\sigma_0)$, *where* Δ_s *is as given by Theorem* 1.1, *and* $\sigma_0 = \max\{\sigma, 2^{1-k}\}$, *in which* $\sigma = \sigma(k)$ *is the exponent given by Corollary* 1.1. *In particular, we have* $\tilde{G}(k) < (2+o(1))k^2 \log k$ *as* $k \to \infty$.

We take this opportunity to record bounds stemming from Corollaries 1.1 and 1.2 when $10 \leqslant k \leqslant 20$. Starting from the same estimate as was used for Corollary 1.1a, we obtain the following bounds.

COROLLARY 1.2a. *We have* $\tilde{G}(10) \leqslant 750$, $\tilde{G}(11) \leqslant 975$, $\tilde{G}(12) \leqslant 1200$, $\tilde{G}(13) \leqslant 1450$, $\tilde{G}(14) \leqslant 1725$, $\tilde{G}(15) \leqslant 2026$, $\tilde{G}(16) \leqslant 2354$, $\tilde{G}(17) \leqslant 2708$, $\tilde{G}(18) \leqslant 3089$, $\tilde{G}(19) \leqslant 3497$, $\tilde{G}(20) \leqslant 3932$.

These bounds may be compared with the bounds $\tilde{G}(10) \leqslant 897$ (Heath-Brown [3]), and $\tilde{G}(11) \leqslant 1520$, $\tilde{G}(12) \leqslant 1948$, $\tilde{G}(13) \leqslant 2355$, $\tilde{G}(14) \leqslant 2810$, $\tilde{G}(15) \leqslant 3309$, $\tilde{G}(16) \leqslant 3852$, $\tilde{G}(17) \leqslant 4440$, $\tilde{G}(18) \leqslant 5074$, $\tilde{G}(19) \leqslant 5754$, $\tilde{G}(20) \leqslant 6481$ (attainable by the method of Vaughan [11], Chapter 5).

The final two corollaries we give without proof.

COROLLARY 1.3. *Let* $k \geqslant 4$. *Then there is a* $J = J(k)$ *with the property that for any polynomial* $f(x) = \alpha_k x^k + \ldots + \alpha_1 x$ *and* $N > N_0(k)$, *there is a natural number* $n \leqslant N$ *with* $\|f(n)\| < N^{-1/J}$. *Further, we have* $J \leqslant (4+o(1))k^2 \log k$ *as* $k \to \infty$.

Theorem 4.5 of R. Baker [1] gives a similar "localized" result on fractional parts in which, asymptotically, 8 replaces 4 in the final conclusion.

COROLLARY 1.4. *There are positive numbers* C_1, $\delta(k)$ *and* $C_2(k, s)$ *such that whenever* $s \geqslant s_0 = \frac{5}{3}k^2(\log k + C_1 \log\log k)$, *one has*

$$J_{s,k}(X) = (C_2(k, s) + O(X^{-\delta(k)}))X^{2s-k(k+1)/2}.$$

Theorem 7.4 of Vaughan [11] gives a similar result in which for some absolute constant C_3 we have $s_0 = k^2(3 \log k + \log\log k + C_3)$.

The proof of Theorem 1.1 is motivated by the strategy adopted in the author's recent work on Waring's problem (see Wooley [17]). There we were able to exploit the arithmetic properties of a suitable set of integers $\mathscr{A}$ to set up an "efficient" Weyl differencing procedure. Thus, given a polynomial $\Psi(x)$, expressions of the form $m^{-k}(\Psi(z+hm^k) - \Psi(z))$ arise (Weyl differencing corresponds to the situation where $m = 1$). Our methods necessarily differ from those of Wooley [17], because the underlying set of integers for the equations (1.1) consists of a complete interval. However, we are nonetheless able to set up a similar form of reduction formula to that in the aforementioned paper by using the well-known "p-adic method" of Linnik-Karatsuba. Roughly speaking, we relate the number of solutions of the simultaneous equations

$$\sum_{i=1}^{k} (x_i^j - y_i^j) = \sum_{r=1}^{s} (u_r^j - v_r^j) \qquad (1 \leqslant j \leqslant k)$$

with $1 \leqslant x_i, y_i \leqslant P$ $(1 \leqslant i \leqslant k)$, $1 \leqslant u_r, v_r \leqslant P$ $(1 \leqslant r \leqslant s)$, to the number of

solutions of the simultaneous equations

$$\sum_{i=1}^{k}(x_i^j - y_i^j) = p^j \sum_{r=1}^{s}(m_r^j - n_r^j) \qquad (1 \leqslant j \leqslant k) \tag{1.8}$$

in which p is some fixed prime with $P^\theta < p \leqslant 2P^\theta$, and

$$\begin{gathered} 1 \leqslant m_r, n_r \leqslant P^{1-\theta}(1 \leqslant r \leqslant s), \qquad 1 \leqslant x_i, y_i \leqslant P, \\ x_i \equiv y_i \pmod{p^k} \qquad (1 \leqslant i \leqslant k). \end{gathered} \tag{1.9}$$

In previous applications of the method one took $\theta = 1/k$, so that the congruential condition in (1.9) implies, by permuting variables, that $x_i = y_i$ $(1 \leqslant i \leqslant k)$, and in this way $J_{s+k,k}(P)$ is related to $J_{s,k}(P^{1-\theta})$. We choose $\theta < 1/k$, and then consider the substitution $y_i = x_i + h_i p^k$. This gives rise to efficient differences, *via* expressions of the form $\Psi_{i,j} = p^{-j}((x_i + h_i p^k)^j - x_i^j)$, and we are then able to manipulate equations to obtain a new system of equations of the form

$$\sum_{i=1}^{k}(\Phi_{i,j} - \Phi'_{i,j}) = \sum_{r=1}^{s}(u_r^j - v_r^j) \qquad (1 \leqslant j \leqslant k),$$

with the $\Phi_{i,j}$ being of a form similar to the $\Psi_{i,j}$. There is then the possibility of repeating the whole process, and thus extracting efficient differences repeatedly.

One major difficulty in both the new and old methods is the possibility that there may be singular solutions to the system of congruences which arise from (1.8). In previous approaches to the problem, one fixed the choice of prime and dealt with the possibility of singular solutions *via* a separate argument. In this paper we consider a set of primes bounded in number by a power of k, and show that if there is a singularity (mod p) for each of these primes, then there is a real singularity. The latter imposes a strong restriction on the range of the variables. This treatment may be used to reduce the term $D(k, r)$ in (1.3) (such a process is executed in Wooley [**18**]).

In Section 2 we prove some preliminary lemmata before going on to prove the fundamental lemma in Section 3. The latter is then used in Section 4 to establish the efficient differencing procedure, leading to Theorem 1.1. In Section 5 we deduce Theorem 1.2 in an elementary manner from Theorem 1.1. The remainder of the paper is then taken up with proving the corollaries, which are simple applications of the main theorem through existing methods.

The author wishes to thank Professor R. C. Vaughan, for re-motivating the author with respect to this problem, and for much useful advice during the course of the author's PhD at Imperial College, London. The author thanks the Science and Engineering Research Council for a grant. This paper was revised while the author was in receipt of a US NSF grant, enjoying the hospitality of the Institute for Advanced Study. The author also greatly appreciates the detailed suggestions of the referee, which have much improved the exposition of this material.

§2. *Preliminary lemmata.* We shall derive an analogue of the fundamental lemma of Wooley [**17**] relating the numbers of solutions of two auxiliary

equations. Unfortunately, the reduction formulae which we apply generate rather complicated polynomials. We shall avoid explicit reference to these polynomials by adopting the following notational convenience.

DEFINITION. *Let d and k be integers with $0 \leqslant d \leqslant k$. Let P be a positive real parameter, and let A be a sufficiently large (but fixed) positive real number. Then we say that the k-tuple of polynomials $(\Psi) = (\Psi_1(x), \dots, \Psi_k(x)) \in \mathbb{Z}[x]^k$ is of type (d, P, A) if*

(a) *Ψ_i has degree $i-d$ for $i \geqslant d$, and is identically zero for $i < d$, and*

(b) *the coefficient of x^{i-d} in $\Psi_i(x)$ is non-zero, and bounded by AP^d $(1 \leqslant i \leqslant k)$.*

Where confusion is easily avoided, we shall frequently use such objects as (Ψ) in a generic sense.

As indicated in the introduction, our method depends fundamentally on efficient Weyl differencing. We define the modified forward difference operator Δ_i^* by

$$\Delta_i^*(f(x); h; m) = m^{-i}(f(x+hm^k) - f(x)).$$

In the following lemma we give some immediate consequences of the above definitions.

LEMMA 2.1. *Suppose that the system (Ψ) is of type (d, P, A). Then the following hold.*

(i) *Suppose that λ_{ij} $(1 \leqslant j < i \leqslant k)$ are integers, and the polynomials Φ_i are defined by*

$$\Phi_i = \Psi_i + \sum_{j=1}^{i-1} \lambda_{ij}\Psi_j \qquad (1 \leqslant i \leqslant k).$$

Then the system (Φ) is of type (d, P, A).

(ii) *Define the Jacobian $J(\Psi)$ by*

$$J(\Psi) = \det\left(\frac{\partial \Psi_i(z_j)}{\partial z_j}\right)_{d+1 \leqslant i,j \leqslant k}.$$

Then

$$J(\Psi) = V \det\,(z_j^{i-d-1})_{d+1 \leqslant i,j \leqslant k},$$

with V a non-zero integer satisfying $V \ll A^k P^{kd}$.

(iii) *Let h and m be fixed integers with $1 \leqslant hm^k \leqslant BP$, and define the polynomials $\Upsilon_i = \Upsilon_i(z)$ by*

$$\Upsilon_i = \Delta_i^*(\Psi_i(z); h; m) \qquad (1 \leqslant i \leqslant k).$$

Then the system (Υ) is of type $(d+1, P, kAB)$.

Proof. (i) Conditions (a) and (b) of the definition are satisfied almost trivially.

(ii) This follows by using row operations on the determinant.

(iii) We have that $\Upsilon_i(z)$ is of degree $i-d-1$ for $i \geqslant d+1$, and is identically zero for $1 \leqslant i \leqslant d$. Then to prove (iii) we merely note that the leading coefficient of $\Upsilon_i(z)$ is $(i-d)hm^{k-i} < kBP$ times that of $\Psi_i(z)$.

The following result on the number of solutions of certain systems of congruences should be compared with Lemma 1 of Linnik [8] (frequently attributed to Karatsuba).

LEMMA 2.2. *Suppose that the system* (Ψ) *is of type* (d, P, A). *Let* $\mathscr{B}(p; \mathbf{u}; \Psi)$ *denote the number of solutions* $(z_1, \dots, z_k)$ *distinct* $(\mathrm{mod}\ p^k)$ *of the system of congruences*

$$\sum_{i=1}^{k} \Psi_j(z_i) \equiv u_j \ (\mathrm{mod}\ p^j) \qquad (d+1 \leqslant j \leqslant k),$$

with

$$J(\Psi; \mathbf{z}) = \det\left(\frac{\partial \Psi_i(z_j)}{\partial z_j}\right)_{d+1 \leqslant i,j \leqslant k}$$

not divisible by p. Then $\mathscr{B}(p; \mathbf{u}; \Psi) \ll p^{\omega(k,d)}$, *where*

$$\omega(k, d) = \tfrac{1}{2}(k(k-1) + d(d+1)), \tag{2.1}$$

and the implicit constant depends only on k.

Proof. Let $\mathscr{C}_s(p; \mathbf{u}; \Psi)$ denote the number of solutions $(z_1, \dots, z_k)$ distinct $(\mathrm{mod}\ p^k)$ of the system of congruences

$$\sum_{i=s+1}^{k} \Psi_j(z_i) \equiv u_j \ (\mathrm{mod}\ p^k) \qquad (d+1 \leqslant j \leqslant k) \tag{2.2}$$

with $(J(\Psi; \mathbf{z}), p) = 1$.

We have

$$\mathscr{B}(p; \mathbf{u}; \Psi) = \sum_{\mathbf{a}}^{*} \mathscr{C}_0(p; \mathbf{a}; \Psi), \tag{2.3}$$

where the summation is over $a_j \equiv u_j \ (\mathrm{mod}\ p^j)$ with $1 \leqslant a_j \leqslant p^k$ $(d+1 \leqslant j \leqslant k)$. For a fixed $\mathbf{u}$, the total number of choices for $\mathbf{a}$ is $p^{\frac{1}{2}(k-d)(k-d-1)}$. Next, by taking any of the p^k possible choices for each z_i in (2.2) with $1 \leqslant i \leqslant s = d$, we have

$$\mathscr{C}_0(p; \mathbf{a}; \Psi) \leqslant p^{kd} \max_{\mathbf{b}} \mathscr{C}_d(p; \mathbf{b}; \Psi), \tag{2.4}$$

where the maximum is over all $\mathbf{b} \in (\mathbb{Z}/p^k\mathbb{Z})^{k-d}$. If we can now show that $\mathscr{C}_d(p; \mathbf{b}; \Psi)$ is bounded independently of p, then the result will follow from (2.3) and (2.4), since $\frac{1}{2}(k-d)(k-d-1) + kd = \omega(k, d)$.

We begin our investigation of $\mathscr{C}_d(p; \mathbf{b}; \Psi)$ by considering the congruences

$$\sum_{i=d+1}^{k} \Psi_j(z_i) \equiv b_j \ (\mathrm{mod}\ p) \qquad (d+1 \leqslant j \leqslant k). \tag{2.5}$$

Let $(x_{d+1}, \dots, x_k)$ be any solution of (2.5) with $(J(\Psi; \mathbf{x}), p) = 1$, and let $(y_{d+1}, \dots, y_k)$ be another such. Let

$$P(X) = \prod_{i=d+1}^{k} (X - x_i).$$

Then by Newton's formulae connecting the sums of the powers of the roots

of a polynomial with its coefficients, and by using the information on the leading coefficients of the Ψ_j given by the condition $(J(\boldsymbol{\Psi}; \mathbf{z}), p) = 1$, we have

$$P(X) \equiv \prod_{i=d+1}^{k} (X - y_i) \qquad (\mathrm{mod}\ p).$$

Then $P(y_r) \equiv 0\ (\mathrm{mod}\ p)$ for $d+1 \leqslant r \leqslant k$. Now $(\boldsymbol{\Psi})$ is of type (d, P, A), and so by Lemma 2.1(ii) we have

$$J(\boldsymbol{\Psi}; \mathbf{z}) = V \det (z_j^{i-d-1})_{d+1 \leqslant i,j \leqslant k}$$

for some non-zero integer V. But since $(J(\boldsymbol{\Psi}; \mathbf{y}), p) = (J(\boldsymbol{\Psi}; \mathbf{x}), p) = 1$, the x_r and y_r must each be distinct $(\mathrm{mod}\ p)$. We therefore conclude that the y_r are a permutation of the x_r, and hence that the number of solutions of (2.5) with $(J(\boldsymbol{\Psi}; \mathbf{z}), p) = 1$ is at most

$$(k-d)! \tag{2.6}$$

Next we use the non-singularity condition to lift the solutions $(\mathrm{mod}\ p)$ uniquely to solutions $(\mathrm{mod}\ p^k)$. Suppose that $\mathbf{z}$ is any solution counted by $\mathscr{C}_d(p; \mathbf{b}; \boldsymbol{\Psi})$, and consider all other distinct solutions $\mathbf{z}'$ such that $\mathbf{z}' \equiv \mathbf{z}\ (\mathrm{mod}\ p)$ and $(J(\boldsymbol{\Psi}; \mathbf{z}'), p) = 1$ (if any such solutions exist). We may plainly write $z_i' = z_i + \zeta_i p^\tau$ $(d+1 \leqslant i \leqslant k)$ for some integers ζ_i. Further, without loss of generality we may suppose that $(\zeta_{d+1}, \dots, \zeta_k, p) = 1$ and $1 \leqslant \tau < k$. Write $\Psi'(z)$ for $\partial \Psi(z)/\partial z$. Then on substituting $\mathbf{z}'$ for $\mathbf{z}$, by (2.2) we have

$$\sum_{i=d+1}^{k} \zeta_i \Psi_j'(z_i) \equiv 0\ (\mathrm{mod}\ p) \qquad (d+1 \leqslant i \leqslant k).$$

But $\det (\Psi_j'(z_i))_{d+1 \leqslant i,j \leqslant k} \not\equiv 0\ (\mathrm{mod}\ p)$, and hence $\zeta_i \equiv 0\ (\mathrm{mod}\ p)$ $(d+1 \leqslant i \leqslant k)$. This contradicts the assumption $(\zeta_{d+1}, \dots, \zeta_k, p) = 1$, and so we conclude from (2.6) that $\mathscr{C}_d(p; \mathbf{b}; \boldsymbol{\Psi}) \leqslant (k-d)!$ for every $\mathbf{b}$, which completes the proof of the lemma.

§3. *The fundamental lemma.* In the remainder of this paper we consider P to be the basic parameter, a sufficiently large real number. Implicit constants will depend only on the natural numbers $k \geqslant 2$ and r, unless stated otherwise.

Suppose that $(\Psi_1, \dots, \Psi_k)$ is of type (d, P, A). Taking $J(\boldsymbol{\Psi}; \mathbf{z})$ to be as in the statement of Lemma 2.2, we can find a positive integer, $l = l(A, k)$, independent of P, such that

$$\sup_{\mathbf{z}} \left(\frac{\log |J(\boldsymbol{\Psi}; \mathbf{z})|}{\log P} \right) < k^l,$$

where the supremum is over $\mathbf{z}$ with $1 \leqslant z_i \leqslant P$ $(d+1 \leqslant i \leqslant k)$ subject to $J(\boldsymbol{\Psi}; \mathbf{z}) \neq 0$.

Let θ be a real number with $0 < \theta \leqslant 1/k$. We take $\mathscr{P}(\theta)$ to be the set consisting of the smallest $[2k^l/\theta]+1$ primes exceeding P^θ. Notice that on taking P sufficiently large, we have $P^\theta < p < 2P^\theta$ for each $p \in \mathscr{P}(\theta)$.

Define $K_s(P, Q; \Psi)$ to be the number of solutions of the simultaneous equations

$$\sum_{n=1}^{k} (\Psi_i(z_n) - \Psi_i(z'_n)) + \sum_{m=1}^{s} (x_m^i - y_m^i) = 0 \qquad (1 \leqslant i \leqslant k), \tag{3.1}$$

with

$$0 < z_n, z'_n \leqslant P \quad (1 \leqslant n \leqslant k), \qquad \text{and} \qquad 0 < x_m, y_m \leqslant Q \quad (1 \leqslant m \leqslant s). \tag{3.2}$$

Also, for $p \in \mathscr{P}(\theta)$ we define $L_s(P, Q; \theta; p; \Psi)$ to be the number of solutions of the simultaneous equations

$$\sum_{n=1}^{k} (\Psi_i(z_n) - \Psi_i(z'_n)) + p^i \sum_{m=1}^{s} (u_m^i - v_m^i) = 0 \qquad (1 \leqslant i \leqslant k) \tag{3.3}$$

with $\mathbf{z}, \mathbf{z}'$ satisfying (3.2), and

$$0 < u_m, v_m \leqslant QP^{-\theta} \ (1 \leqslant m \leqslant s), \qquad z_n \equiv z'_n \pmod{p^k} \qquad (1 \leqslant n \leqslant k). \tag{3.4}$$

We then write

$$L_s(P, Q; \theta; \Psi) = \max_{p \in \mathscr{P}(\theta)} L_s(P, Q; \theta; p; \Psi).$$

We are now in a position to state and prove the fundamental lemma.

LEMMA 3.1. *Suppose that* $s \geqslant d$, $0 < P^\theta \leqslant Q \leqslant P$, *and that the system* $(\Psi_1, \ldots, \Psi_k)$ *is of type* (d, P, A). *Then there exists a system* $(\Phi_1, \ldots, \Phi_k)$ *of type* (d, P, A) *such that*

$$K_s(P, Q; \Psi) \ll_{\theta, A} P^k J_{s,k}(Q) + P^{(2s+\omega(k,d-1))\theta} L_s(P, Q; \theta; \Phi),$$

where $\omega(k, d)$ *is given by* (2.1).

Proof. In the proof of this lemma implicit constants may depend on θ and A. Let $R_1(\mathbf{w})$ denote the number of solutions of the simultaneous equations

$$\sum_{n=1}^{k} \Psi_i(z_n) + \sum_{m=1}^{s} x_m^i = w_i \qquad (1 \leqslant i \leqslant k) \tag{3.5}$$

with $\mathbf{w}$ fixed, and with $\mathbf{z}, \mathbf{x}$ satisfying (3.2), and the additional condition that the z_n be distinct. Also, let $R_2(\mathbf{w})$ denote the corresponding number of solutions with the z_n not distinct.

We have

$$K_s(P, Q; \Psi) = \sum_{\mathbf{w}} (R_1(\mathbf{w}) + R_2(\mathbf{w}))^2,$$

where the summation is over $\mathbf{w} \in \mathbb{Z}^k$. Then $K_s(P, Q; \Psi) \leqslant 4(S_1 + S_2)$, where $S_i = \sum_{\mathbf{w}} R_i(\mathbf{w})^2$ $(i = 1, 2)$.

We divide into two cases.

(i) *Suppose that* $S_2 \geqslant S_1$. Then we have $K_s(P, Q; \Psi) \leqslant 8S_2$. Let $f(\boldsymbol{\alpha}; Q)$ be defined as in (1.2), and

$$F(\boldsymbol{\alpha}) = \sum_{z \leqslant P} e(\alpha_1 \Psi_1(z) + \ldots + \alpha_k \Psi_k(z)).$$

On noting that S_2 counts solutions of (3.1) in which the z_n are not distinct, and likewise the z_n', by considering the underlying diophantine equations we deduce that

$$S_2 \ll \int_{\mathfrak{T}^k} |F(2\boldsymbol{\alpha})^2 F(\boldsymbol{\alpha})^{2k-4} f(\boldsymbol{\alpha}; Q)^{2s}| d\boldsymbol{\alpha}.$$

Then by applying Hölder's inequality twice, we obtain

$$K_s(P, Q; \boldsymbol{\Psi}) \ll \left(\int_{\mathfrak{T}^k} |F(\boldsymbol{\alpha})^{2k} f(\boldsymbol{\alpha}; Q)^{2s}| d\boldsymbol{\alpha} \right)^{1-2/k} \left(\int_{\mathfrak{T}^k} |F(2\boldsymbol{\alpha})^k f(\boldsymbol{\alpha}; Q)^{2s}| d\boldsymbol{\alpha} \right)^{2/k}.$$

By making a trivial estimate, we therefore have

$$K_s(P, Q; \boldsymbol{\Psi}) \ll (K_s(P, Q; \boldsymbol{\Psi}))^{1-2/k} \left(P^k \int_{\mathfrak{T}^k} |f(\boldsymbol{\alpha}; Q)|^{2s} d\boldsymbol{\alpha} \right)^{2/k},$$

and the result follows in the first case.

(ii) *Suppose that* $S_1 \geqslant S_2$. Then we have $K_s(P, Q; \boldsymbol{\Psi}) \leqslant 8S_1$. For a solution $\mathbf{z}, \mathbf{x}$ counted by $R_1(\mathbf{w})$, consider the Jacobian $J(\boldsymbol{\Psi}; \mathbf{z})$. Since $(\boldsymbol{\Psi})$ is of type (d, P, A), by Lemma 2.1(ii) we have

$$J(\boldsymbol{\Psi}; \mathbf{z}) = V \det (z_j^{i-d-1})_{d+1 \leqslant i,j \leqslant k}$$

for some non-zero integer V. Then since the z_j are distinct, we have $J(\boldsymbol{\Psi}; \mathbf{z}) \neq 0$. Hence the number, $N^*(\mathbf{z})$, of prime divisors p of $J(\boldsymbol{\Psi}; \mathbf{z})$ with $p \geqslant P^\theta$ satisfies

$$N^*(\mathbf{z}) \leqslant \frac{\log |J(\boldsymbol{\Psi}; \mathbf{z})|}{\theta \log P} < k! \theta^{-1}.$$

But then card $(\mathscr{P}(\theta)) > N^*(\mathbf{z}) + N^*(\mathbf{z}')$, and hence there is a prime $p \in \mathscr{P}(\theta)$ with p dividing neither $J(\boldsymbol{\Psi}; \mathbf{z})$ nor $J(\boldsymbol{\Psi}; \mathbf{z}')$. It therefore follows that $S_1 \leqslant \sum_{p \in \mathscr{P}(\theta)} S_3(p)$, where $S_3(p)$ denotes the number of solutions of the equations (3.1) subject to (3.2), and in addition with the z_n distinct (mod p), and likewise the z_n'.

Consider any solution $\mathbf{z}, \mathbf{z}', \mathbf{x}, \mathbf{y}$ counted by $S_3(p)$. Since $\boldsymbol{\Psi}$ is of type (d, P, A), we have

$$\sum_{m=1}^{s} (x_m^i - y_m^i) = 0 \qquad (1 \leqslant i \leqslant d).$$

Let $\mathscr{B}(\mathbf{w})$ denote the set of solutions distinct (mod p) of the system of congruences

$$\sum_{m=1}^{s} x_m^i \equiv w_i \pmod{p} \qquad (1 \leqslant i \leqslant d).$$

It is a simple exercise to show that when $s \geqslant d$, we have card $(\mathscr{B}(\mathbf{w})) \ll p^{s-d}$ (the number of singular solutions of this system of congruences is particularly easy to estimate).

Let

$$f_p(\boldsymbol{\alpha}; y) = \sum_{\substack{0<x\leqslant Q \\ x\equiv y \pmod p}} e(\alpha_1 x + \ldots + \alpha_k x^k),$$

and

$$G(\boldsymbol{\alpha}) = \sum_{z_1\leqslant P} \ldots \sum_{\substack{z_k\leqslant P \\ (J(\boldsymbol{\Psi};\mathbf{z}),p)=1}} e(\alpha_1 s_1(\mathbf{z}) + \ldots + \alpha_k s_k(\mathbf{z})),$$

in which we have written

$$s_i(\mathbf{z}) = \Psi_i(z_1) + \ldots + \Psi_i(z_k).$$

Then by considering the underlying diophantine equations, we have

$$S_3(p) \leqslant \int_{\mathsf{T}^k} |G(\boldsymbol{\alpha})|^2 \sum_{w_1=1}^{p} \ldots \sum_{w_d=1}^{p} |U(\boldsymbol{\alpha}; \mathbf{w})|^2 d\boldsymbol{\alpha},$$

where

$$U(\boldsymbol{\alpha}; \mathbf{w}) = \sum_{\mathbf{u}\in\mathscr{B}(\mathbf{w})} f_p(\boldsymbol{\alpha}; u_1) \ldots f_p(\boldsymbol{\alpha}; u_s).$$

But by Cauchy's inequality, followed by an application of the arithmetic-geometric mean inequality, we have

$$|U(\boldsymbol{\alpha}; \mathbf{w})|^2 \leqslant \operatorname{card}(\mathscr{B}(\mathbf{w})) \sum_{\mathbf{u}\in\mathscr{B}(\mathbf{w})} |f_p(\boldsymbol{\alpha}; u_1) \ldots f_p(\boldsymbol{\alpha}; u_s)|^2$$

$$\ll p^{s-d} \sum_{\mathbf{u}\in\mathscr{B}(\mathbf{w})} \sum_{i=1}^{s} |f_p(\boldsymbol{\alpha}; u_i)|^{2s}.$$

Hence

$$S_3(p) \ll p^{2s-d} \max_{1\leqslant x\leqslant p} S_4(x, p), \tag{3.6}$$

where

$$S_4(x, p) = \int_{\mathsf{T}^k} |G(\boldsymbol{\alpha})^2 f_p(\boldsymbol{\alpha}; x)^{2s}| d\boldsymbol{\alpha}.$$

But $S_4(x, p)$ is the number of solutions of the simultaneous equations

$$\sum_{n=1}^{k} (\Psi_i(z_n) - \Psi_i(z'_n)) + \sum_{m=1}^{s} ((py_m + x)^i - (py'_m + x)^i) = 0 \qquad (1\leqslant i\leqslant k), \tag{3.7}$$

with $\mathbf{z}, \mathbf{z}'$ satisfying (3.2) subject to

$$(J(\boldsymbol{\Psi}; \mathbf{z}), p) = (J(\boldsymbol{\Psi}; \mathbf{z}'), p) = 1, \tag{3.8}$$

and

$$-x/p < y_m, y'_m \leqslant (Q-x)/p. \tag{3.9}$$

Then on noting that by the binomial theorem,

$$\sum_{j=0}^{i} \binom{i}{j} (py_m + x)^j (-x)^{i-j} = (py_m)^i,$$

we deduce that for each solution $\mathbf{z}, \mathbf{z}', \mathbf{y}, \mathbf{y}'$ of (3.7), we have

$$\sum_{n=1}^{k} (\Phi_i(z_n) - \Phi_i(z_n')) + p^i \sum_{m=1}^{s} (y_m^i - y_m'^i) = 0 \qquad (1 \leqslant i \leqslant k), \tag{3.10}$$

where

$$\Phi_i(z) = \sum_{j=0}^{i} \binom{i}{j} \Psi_j(z)(-x)^{i-j}.$$

Conversely, each solution $\mathbf{z}, \mathbf{z}', \mathbf{y}, \mathbf{y}'$ of (3.10) satisfies (3.7). Then $S_4(x, p)$ is the number of solutions of the system (3.10) with $\mathbf{z}, \mathbf{z}'$ satisfying (3.2) subject to (3.8), and with $\mathbf{y}, \mathbf{y}'$ satisfying (3.9). Further, by Lemma 2.1(i) the system $(\boldsymbol{\Phi})$ is of type (d, P, A), and in particular, by using row operations on the implicit determinant we have $J(\boldsymbol{\Phi}; \mathbf{z}) = J(\boldsymbol{\Psi}; \mathbf{z})$.

Now, on recalling definition (1.2), and abbreviating $(\alpha_1 p, \ldots, \alpha_k p^k)$ to $\boldsymbol{\alpha}\mathbf{p}^i$, we have

$$\left| \sum_{0 \leqslant y \leqslant Y} e(\alpha_1 p y + \ldots + \alpha_k p^k y^k) \right|^{2s} \ll 1 + |f(\boldsymbol{\alpha}\mathbf{p}^i; Y)|^{2s}.$$

Let

$$H(\boldsymbol{\alpha}) = \sum_{\substack{z_1 \leqslant P \\ (J(\boldsymbol{\Phi};\mathbf{z}), p) = 1}} \cdots \sum_{z_k \leqslant P} e(\alpha_1 t_1(\mathbf{z}) + \ldots + \alpha_k t_k(\mathbf{z})),$$

in which we have written

$$t_i(\mathbf{z}) = \Phi_i(z_1) + \ldots + \Phi_i(z_k).$$

Then by considering the underlying diophantine equations, and semi-diagonal solutions of these equations, we have

$$S_4(x, p) \ll \int_{\mathsf{T}^k} |H(\boldsymbol{\alpha})^2 f(\boldsymbol{\alpha}\mathbf{p}^i; QP^{-\theta})^{2s}| d\boldsymbol{\alpha}. \tag{3.11}$$

The integral on the right hand side of (3.11) is equal to the number of solutions of the equations (3.10) with the variables satisfying (3.2),

$$(J(\boldsymbol{\Phi}; \mathbf{z}), p) = (J(\boldsymbol{\Phi}; \mathbf{z}'), p) = 1, \tag{3.12}$$

and

$$1 \leqslant y_m, y_m' \leqslant QP^{-\theta}. \tag{3.13}$$

Now $\Phi_i(z)$ is independent of z for $1 \leqslant i \leqslant d$. Also, for each solution counted by $S_4(x, p)$ we have

$$t_i(\mathbf{z}) \equiv t_i(\mathbf{z}') \pmod{p^i} \qquad (d+1 \leqslant i \leqslant k),$$

so that each solution of (3.10) subject to (3.12) and (3.13) may be classified according to the common residue class (mod p^i) of $t_i(\mathbf{z})$ and $t_i(\mathbf{z}')$ for each i.

Let $\mathscr{B}^*(p; \mathbf{u}; \boldsymbol{\Psi})$ denote the set of solutions $(z_1, \ldots, z_k)$ distinct (mod p^k) of the system of congruences

$$t_i(\mathbf{z}) \equiv u_i \pmod{p^i} \qquad (d+1 \leqslant i \leqslant k),$$

with $(J(\boldsymbol{\Phi}; \mathbf{z}), p) = 1$. Then by Lemma 2.2 we have card $(\mathscr{B}^*(p; \mathbf{u}; \boldsymbol{\Psi})) \ll p^{\omega(k,d)}$.

Let

$$H(\boldsymbol{\alpha}; \mathbf{z}) = \sum_{\substack{x_1 \leqslant P \\ x_1 \equiv z_1 \pmod{p^k}}} \cdots \sum_{\substack{x_k \leqslant P \\ x_k \equiv z_k \pmod{p^k}}} e(\alpha_1 t_1(\mathbf{x}) + \ldots + \alpha_k t_k(\mathbf{x})).$$

Then we have

$$S_4(x, p) \ll V(p), \tag{3.14}$$

where

$$V(p) = \int_{\mathsf{T}^k} H_p(\boldsymbol{\alpha}) |f(\hat{\boldsymbol{\alpha}}\mathbf{p}^{\mathbf{i}}; QP^{-\theta})|^{2s} d\boldsymbol{\alpha}, \tag{3.15}$$

and

$$H_p(\boldsymbol{\alpha}) = \sum_{u_{d+1}=1}^{p^d} \cdots \sum_{u_k=1}^{p^k} \Big| \sum_{\mathbf{z} \in \mathscr{B}^*(p; \mathbf{u}; \boldsymbol{\Psi})} H(\boldsymbol{\alpha}; \mathbf{z}) \Big|^2.$$

But by Cauchy's equality,

$$H_p(\boldsymbol{\alpha}) \leqslant \sum_{u_{d+1}=1}^{p^d} \cdots \sum_{u_k=1}^{p^k} \operatorname{card}(\mathscr{B}^*(p; \mathbf{u}; \boldsymbol{\Psi})) \sum_{\mathbf{z} \in \mathscr{B}^*(p; \mathbf{u}; \boldsymbol{\Psi})} |H(\boldsymbol{\alpha}; \mathbf{z})|^2.$$

Then by (3.6), (3.14) and (3.15), we have

$$S_3(p) \ll p^{2s+\omega(k,d-1)} \sum_{z_1=1}^{p^k} \cdots \sum_{z_k=1}^{p^k} \int_{\mathsf{T}^k} |H(\boldsymbol{\alpha}; \mathbf{z})^2 f(\boldsymbol{\alpha}\mathbf{p}^i; QP^{-\theta})^{2s}| d\boldsymbol{\alpha},$$

and the lemma now follows in the second case, on considering the underlying diophantine equations.

§4. *Successive differencing.* Here we shall set up the apparatus necessary to achieve the efficient differencing process mentioned in the introduction.

LEMMA 4.1. *Suppose that* $1 < P^\theta \leqslant Q \leqslant P$, *and that the system* $(\Phi_1, \ldots, \Phi_k)$ *is of type* (d, P, A). *Write* $H = P^{1-k\theta}$. *Then there exist* $p \in \mathscr{P}(\theta)$ *and* h *satisfying* $1 \leqslant h \leqslant H$ *such that the system* $(\Upsilon_1, \ldots, \Upsilon_k)$, *given by*

$$\Upsilon_i = \Delta_i^*(\Phi_i(z); h; p) \qquad (1 \leqslant i \leqslant k),$$

satisfies the property that

$$L_s(P, Q; \theta; \boldsymbol{\Phi}) \ll_A P^k J_{s,k}(QP^{-\theta}) + H^k (K_s(P, QP^{-\theta}; \boldsymbol{\Upsilon}) J_{s,k}(QP^{-\theta}))^{1/2}.$$

Furthermore, $(\boldsymbol{\Upsilon})$ *is of type* $(d+1, P, k2^k A)$.

Proof. In the proof of this lemma implicit constants may depend on A. We shall prove the bound in the lemma with $L_s = L_s(P, Q; \theta; p; \boldsymbol{\Phi})$ in place of $L_s(P, Q; \theta; \boldsymbol{\Phi})$, and remove the maximum implicit in the conclusion. The lemma then follows easily.

Let

$$I_p(\boldsymbol{\alpha}) = \sum_{z=1}^{p^k} \left| \sum_{x \leqslant p} e(\alpha_1 \Phi_1(x) + \ldots + \alpha_k \Phi_k(x)) \right|^2.$$

We have $L_s \ll U_0 + U_1$, where U_0 denotes the number of solutions of the equations (3.3) subject to (3.4), and with $z_n = z_n'$ for some n with $1 \leqslant n \leqslant k$, and U_1 denotes the corresponding number of solutions with $z_n \neq z_n'$ $(1 \leqslant n \leqslant k)$.

We divide into cases.

(i) *Suppose that* $U_0 \geqslant U_1$. We have

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

An application of Hölder's inequality gives

$$\begin{aligned} L_s(P, Q; \theta; p; \boldsymbol{\Phi}) &\ll P \left(\int_{\mathsf{T}^k} (I_p(\boldsymbol{\alpha}))^k |f(\boldsymbol{\alpha}\mathbf{p}^i; QP^{-\theta})|^{2s} d\boldsymbol{\alpha} \right)^{1-1/k} \\ &\quad \times \left(\int_{\mathsf{T}^k} |f(\boldsymbol{\alpha}\mathbf{p}^i; QP^{-\theta})|^{2s} d\boldsymbol{\alpha} \right)^{1/k} \\ &= P(L_s(P, Q; \theta; p; \boldsymbol{\Phi}))^{1-1/k} (J_{s,k}(QP^{-\theta}))^{1/k}, \end{aligned}$$

and the result now follows in the first case.

(ii) *Suppose that* $U_1 \geqslant U_0$. For each solution of (3.3) counted by U_1, we have $z_n \equiv z_n' \pmod{p^k}$ and $z_n \neq z_n'$ $(1 \leqslant n \leqslant k)$. Then for some h_n with $1 \leqslant |h_n| \leqslant H$, we have

$$z_n' = z_n + h_n p^k \qquad (1 \leqslant n \leqslant k). \tag{4.1}$$

On substituting (4.1) into (3.3), we deduce that

$$U_1 \leqslant \sum_{\eta_1} \ldots \sum_{\eta_k} U_2(\eta_1, \ldots, \eta_k),$$

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

$$\sum_{j=1}^{k} \eta_j \Upsilon_i(z_j; h_j; p) + \sum_{m=1}^{s} (u_m^i - v_m^i) = 0 \qquad (1 \leqslant i \leqslant k)$$

with $\mathbf{z}$ satisfying (3.2), $0 < u_m, v_m \leqslant QP^{-\theta}$ $(1 \leqslant m \leqslant s)$, and $1 \leqslant h_j \leqslant H$ $(1 \leqslant j \leqslant k)$. Further, the system $(\boldsymbol{\Upsilon})$ is of type $(d+1, P, k2^k A)$ by Lemma 2.1(iii).

Define

$$W(\boldsymbol{\alpha}; h) = \sum_{z \leqslant P} e(\alpha_1 \Upsilon_1(z; h; p) + \ldots + \alpha_k \Upsilon_k(z; h; p)).$$

Then by considering the underlying diophantine equations, we have

$$U_1 \leqslant \sum_{\boldsymbol{\eta}} \int_{\mathsf{T}^k} \left(\prod_{j=1}^{k} \sum_{h \leqslant H} W(\eta_j \boldsymbol{\alpha}; h) \right) |f(\boldsymbol{\alpha}; QP^{-\theta})|^{2s} d\boldsymbol{\alpha},$$

where the summation is over $\boldsymbol{\eta} \in \{+1, -1\}^k$. But by Hölder's inequality we have

$$\sum_{\boldsymbol{\eta}} \left(\prod_{j=1}^{k} \sum_{h \leqslant H} W(\eta_j \boldsymbol{\alpha}; h) \right) \ll H^{k-1} \sum_{h \leqslant H} |W(\boldsymbol{\alpha}; h)|^k.$$

Then by the Cauchy-Schwarz inequalities we have

$$U_1 \ll \left(\int_{\mathsf{T}^k} |f(\boldsymbol{\alpha}; QP^{-\theta})|^{2s} d\boldsymbol{\alpha} \right)^{1/2} \times \left(H^{2k-1} \int_{\mathsf{T}^k} \sum_{h \leqslant H} |W(\boldsymbol{\alpha}; h)^{2k} f(\boldsymbol{\alpha}; QP^{-\theta})^{2s}| d\boldsymbol{\alpha} \right)^{1/2},$$

which leads to the desired conclusion in the second case, on considering the underlying diophantine equations.

This completes the proof of the lemma.

Combining the conclusions of Lemmata 3.1 and 4.1 gives us a means of relating $K_s(P, Q; \boldsymbol{\Psi})$ to $K_s(P, QP^{-\theta}; \boldsymbol{\Upsilon})$, where $\boldsymbol{\Upsilon}$ behaves like $\Delta^* \boldsymbol{\Psi}$. We are therefore able to take differences repeatedly, and this enables us to obtain estimates for $J_{s+k,k}(P)$ in terms of $J_{s,k}(Q)$. Theorem 1.1 supplies us with a bound of the form $J_{s,k}(P) \ll P^{\lambda_s}$.

The proof of Theorem 1.1. Before starting the proof of the theorem, we make some comments concerning the variables in its statement. Notice first that for each j, s and J, we have $\varphi(j, s, J) \leqslant 1/k$. Therefore $\theta_s \leqslant 1/k$, and hence

$$\Delta_s \leqslant \max\{0, \Delta_{s-k}\} \leqslant k(k+1)/2 < k^2,$$

by a trivial induction. Then (1.4) yields positive values for the φ and φ^*, and thus $\theta_s > 0$. Also, (1.7) gives $\lambda_s \leqslant 2s$.

We prove the result by induction, the case $s = t$ being assumed. So suppose that the result holds with $s' = t + mk$ for each $0 \leqslant m \leqslant l$, and let $s = t + lk$. We write λ for λ_s.

Let j be the least integer with $1 \leqslant j \leqslant k$ such that $\theta_{s+k} = \varphi(j, s+k, 1)$. For $J = 1, \ldots, j$ define $\varphi_J = \varphi(j, s+k, J)$ as in the statement of the theorem. Then if $\varphi_J = 1/k$ for some $J < j$, we have $\varphi(j, s+k, J) = \varphi(J, s+k, J)$, and one finds successively that $\varphi(j, s+k, r) = \varphi(J, s+k, r)$ for $r = J, J-1, \ldots, 1$, contradicting the minimality of j. Thus $\varphi_J < 1/k$ for $J < j$. We adopt the notation of writing

$$M_i = P^{\varphi_i}, \qquad H_i = PM_i^{-k}, \qquad Q_i = P(M_1 \ldots M_i)^{-1} \qquad (1 \leqslant i \leqslant j),$$

and adopt the convention that $Q_0 = P$. We shall also take A_j to be a series of sufficiently large (but fixed) real numbers with each ratio A_j/A_{j-1} also sufficiently large.

We shall first prove inductively that for $J = j-1, j-2, \ldots, 0$, all systems $(\boldsymbol{\Phi})$ of type (J, P, A_J) satisfy

$$L_s(P, Q_J; \varphi_{J+1}; \boldsymbol{\Phi}) \ll P^k Q_{J+1}^{\lambda}. \tag{4.2}$$

First notice that if (Ψ) is of type (j, P, A), then a trivial estimate gives

$$K_s(P, Q_j; \Psi) \ll P^{2k} J_{s,k}(Q_j).$$

Then by Lemma 4.1, for all systems (Φ) of type $(j-1, P, A_{j-1})$ we have

$$L_s(P, Q_{j-1}; \varphi_j; \Phi) \ll P^k J_{s,k}(Q_j) + P^k H_j^k J_{s,k}(Q_j).$$

But we have $\varphi(j, s+k, j) = 1/k$, and hence $H_j = 1$. Thus the result follows in the case $J = j-1$.

We shall now suppose that (4.2) holds for J, and deduce the corresponding result for $J-1$. We have just established (4.2) when $J = j-1$, so we may assume that $J \leqslant j-1$. Then by Lemma 3.1, all systems (Ψ) of type (J, P, A_J) satisfy

$$K_s(P, Q_J; \Psi) \ll P^k J_{s,k}(Q_J) + M_{J+1}^{2s+\omega(k,J-1)} P^k Q_{J+1}^{\lambda}.$$

But since $\lambda \leqslant 2s$, we have, by our inductive hypothesis,

$$J_{s,k}(Q_J) \ll Q_J^{\lambda} = (M_{J+1} Q_{J+1})^{\lambda} \leqslant M_{J+1}^{2s} Q_{J+1}^{\lambda},$$

and hence

$$\begin{aligned} K_s(P, Q_J; \Psi) &\ll P^k M_{J+1}^{2s} Q_{J+1}^{\lambda} + M_{J+1}^{2s+\omega(k,J-1)} P^k Q_{J+1}^{\lambda} \\ &\ll M_{J+1}^{2s+\omega(k,J-1)} P^k Q_{J+1}^{\lambda}. \end{aligned}$$

We therefore deduce from Lemma 4.1 that for all systems (Φ) of type $(J-1, P, A_{J-1})$ we have

$$L_s(P, Q_{J-1}; \varphi_J; \Phi) \ll T_3 + T_4^{1/2}, \tag{4.3}$$

where

$$T_3 = P^k Q_J^{\lambda}, \tag{4.4}$$

and

$$T_4 = P^k M_{J+1}^{2s+\omega(k,J-1)} H_J^{2k} Q_J^{\lambda} Q_{J+1}^{\lambda}. \tag{4.5}$$

We have assumed that $\varphi_J < 1/k$ for $J < j$, and hence that $\varphi_J = \varphi^*(j, s+k, J)$. Then by (1.7) and (1.4) we have

$$\begin{aligned} (2s + \omega(k, J-1))\varphi_{J+1} - \lambda\varphi_{J+1} &= (k^2 + \tfrac{1}{2}J(J-1) - \Delta_s)\varphi(j, s+k, J+1) \\ &= 2k^2\varphi_J - k. \end{aligned}$$

Then by (4.5) we deduce that $T_4^{1/2} = P^k Q_J^{\lambda}$, and hence from (4.3), (4.4) and (4.5) that

$$L_s(P, Q_{J-1}; \varphi_J; \Phi) \ll P^k Q_J^{\lambda}.$$

Thus (4.2) follows with $J-1$ replacing J, and our second assertion holds for $J = 0, \ldots, j-1$.

It therefore follows that all systems (Φ) of type $(0, P, A_0)$ satisfy

$$L_s(P, Q_0; \varphi_1; \Phi) \ll P^k Q_1^{\lambda},$$

so that by Lemma 3.1, for all systems (Ψ) of type $(0, P, A_0)$, we have

$$K_s(P, Q_0; \Psi) \ll P^{k+\lambda} + M_1^{2s+\omega(k,-1)} P^k Q_1^{\lambda}.$$

Then

$$J_{s+k,k}(P) \ll K_s(P, P; \Psi) \ll P^{k+\lambda} + P^{\lambda'},$$

where by (1.5), (1.6) and (1.7) we have

$$\begin{aligned}\lambda' &= \lambda(1-\theta_{s+k}) + k + (2s + \tfrac{1}{2}k(k-1))\theta_{s+k} \\ &= 2(s+k) - \tfrac{1}{2}k(k+1) + \Delta_{s+k}.\end{aligned}$$

On noting that $\lambda' \geqslant \lambda + k$, since $\lambda \leqslant 2s$ and $\theta_{s+k} > 0$, we find that the inductive hypothesis follows for $s+k$ in place of s.

This completes the proof of the theorem.

§5. *A simplified result.* We give here an elementary argument which leads to a bound asymptotically of similar strength to Theorem 1.1. We shall suppose throughout that k is a sufficiently large integer, and therefore write such statements as $k > 8(\log k)^2$ without comment. We adopt the same notation as in the statement of Theorem 1.1.

We have $0 \leqslant \theta_s \leqslant 1/k$, so that if $0 < \Delta_{s-k} \leqslant k^2$ is positive, then by (1.6) we have

$$\Delta_s = \Delta_{s-k}(1-1/k) + (k^2 - \Delta_{s-k})(\theta_s - 1/k) \leqslant \Delta_{s-k}(1-1/k).$$

Then Δ_{rk} is a decreasing function of r for $r \geqslant 1$, and on noting the simple estimate $J_{k,k}(P) \ll P^k$ (giving $\Delta_k = \frac{1}{2}k(k-1)$) we recover the "classical" bound

$$\Delta_{rk} \leqslant \tfrac{1}{2}k^2\left(1 - \frac{1}{k}\right)^r. \tag{5.1}$$

By working somewhat harder we shall obtain Theorem 1.2.

Let $u(k) = [k \log\log k] + 1$ and $v(k) = [k(\log k - \log\log k)] + 1$. We shall prove inductively that when $r \leqslant v(k)$, we have

$$J_{rk,k}(P) \ll P^{2rk - \frac{1}{2}k(k+1) + \eta(r,k)}, \tag{5.2}$$

where the implicit constant depends at most on r and k, and

$$\eta(r, k) = \tfrac{3}{5}k^2 \log k\left(1 - \frac{2}{k}(1 - 1/\log k)\right)^r. \tag{5.3}$$

First notice that

$$(1-1/k)^r\left(1 - \frac{2}{k}(1-1/\log k)\right)^{-r} < (1+1/k)^r.$$

For $r \geqslant 1$ the latter is at most $e^{(r-1)/k}(1+1/k)$. Then for $r \leqslant u(k)$, by (5.1) we have

$$\Delta_{rk} < \tfrac{1}{2}k^2(1+1/k)\, e^{\log\log k}\left(1 - \frac{2}{k}(1-1/\log k)\right)^r,$$

and so (5.3) follows in this case.

Suppose now that $u(k) \leqslant r < v(k)$, and that (5.2) holds with (5.3) for each $r' \leqslant r$. We apply Theorem 1.1 with $t = rk$,

$$\Delta_t = \tfrac{3}{5}k^2 \log k \left(1 - \frac{2}{k}(1 - 1/\log k)\right)^r,$$

and $\mu = 2t - \frac{1}{2}k(k+1) + \Delta_t$. By elementary analysis, for each $x \geqslant 2$ we have $e^{-1-2/x} < (1-1/x)^x < e^{-1}$, and hence

$$\begin{aligned}\Delta_t &< \tfrac{3}{5}k^2 \log k \left(1 - \frac{2}{k}(1 - 1/\log k)\right)^{k \log\log k} \\ &< \tfrac{3}{5}k^2 \log k \exp(-2 \log\log k(1 - 1/\log k)) < \frac{2k^2}{3 \log k}, \end{aligned} \tag{5.4}$$

and

$$\begin{aligned}\Delta_t &> \tfrac{3}{5}k^2 \log k (1 - 2/k)^{k(\log k - \log\log k)} \\ &> \tfrac{3}{5}k^2 \log k \exp(-2(1 + 4/k)(\log k - \log\log k)) > (\log k)^2. \end{aligned} \tag{5.5}$$

We take

$$j = \left[\frac{\log(8 \log k)}{\log 2}\right] + 1,$$

and abbreviating the notation of the statement of Theorem 1.1, we write φ_J for $\varphi(j, rk+k, J)$ when $1 \leqslant J \leqslant j$, and $\Delta = \Delta_{rk}$. By (5.5) we have $\Delta > 4(j-1)(j-2) \log k$, and hence

$$k^2 + \tfrac{1}{2}(J-1)(J-2) - \Delta < k^2 - \Delta',$$

where

$$\Delta' = \Delta\left(1 - \frac{1}{8 \log k}\right). \tag{5.6}$$

Therefore, by (1.4) we have

$$\varphi^*(j, rk+k, J-1) < (2k^2)^{-1}(k + (k^2 - \Delta')\varphi_J)$$

for $2 \leqslant J \leqslant j$. But $\varphi_j = 1/k$, and hence, by the obvious downwards induction argument (as in the proof of Lemma 3.2 of Wooley [17]) we have

$$\varphi_J \leqslant \frac{k}{k^2 + \Delta'} + \left(\frac{1}{k} - \frac{k}{k^2 + \Delta'}\right)\left(\frac{k^2 - \Delta'}{2k^2}\right)^{j-J} \qquad (1 \leqslant J \leqslant j).$$

In particular, on writing

$$\varphi' = \frac{k}{k^2 + \Delta'}\left(1 + 2^{1-j}\frac{\Delta'}{k^2}\right),$$

we have $\varphi_1 \leqslant \varphi'$. But by (1.5) we have $\theta_{rk+k} \leqslant \varphi_1$. Then once more noting that

$\Delta \leqslant k^2$, by (1.6) and (5.6) we have $\Delta_{rk+k} \leqslant \Delta^*$, with

$$\Delta^* = \Delta(1-\varphi_1) + k(k\varphi_1 - 1) = \Delta - k + (k^2 - \Delta)\varphi_1 \leqslant \Delta - k + (k^2 - \Delta)\varphi'$$

$$= \Delta(1-\varphi') + k(k\varphi' - 1) \leqslant \Delta\left(1 - \frac{k}{k^2+\Delta'}\right) - \frac{k\Delta'(1-2^{1-j})}{k^2+\Delta'}$$

$$\leqslant \Delta\left(1 - \frac{k}{k^2+\Delta'} 2(1-2^{-j})\left(1 - \frac{1}{8\log k}\right)\right).$$

But by (5.4) we have

$$(1-2^{-j})\left(1-\frac{1}{8\log k}\right)\frac{k}{k^2+\Delta'} > \frac{1}{k}\frac{(1-1/8\log k)^2}{(1+2/3\log k)} > \frac{1}{k}\left(1-\frac{1}{\log k}\right).$$

Then

$$\Delta_{rk+k} < \Delta\left(1 - \frac{2}{k}\left(1 - \frac{1}{\log k}\right)\right),$$

and by (5.3) the induction is complete.

To complete the proof of Theorem 1.2 we apply Theorem 1.1 with $j = 2$. First note that

$$k^2 \log k \left(1 - \frac{2}{k}\left(1 - \frac{1}{\log k}\right)\right)^{v(k)}$$

$$< k^2 \log k \exp\left(-2\left(1 - \frac{1}{\log k}\right)(\log k - \log\log k)\right) < e^2(\log k)^3.$$

Then by (5.2) and (5.3), we have $\Delta_{rk} < 5(\log k)^3$ when $r = v(k)$, and an inductive argument shows that this bound holds whenever $r \geqslant v(k)$. Next, for each s we have $\varphi(2, s, 2) = 1/k$, and by (1.4),

$$\varphi(2, s, 1) = \frac{1}{k} - \frac{\Delta_{s-k}}{2k^3}.$$

Then by (1.5) and (1.6),

$$\Delta_s = \Delta_{s-k}\left(1 - \frac{1}{k} + \frac{\Delta_{s-k}}{2k^3}\right) - \frac{\Delta_{s-k}}{2k},$$

and so

$$\Delta_{rk+k} < \Delta_{rk}\left(1 - \frac{3}{2k}\left(1 - \frac{1}{k}\right)\right).$$

The theorem is then completed by an inductive argument.

§6. *The asymptotic formula in Waring's problem.* We now prove Corollaries 1.1 and 1.2 to Theorem 1.1. For this purpose we use the simplification of Theorem 1.1 embodied in Theorem 1.2. We note that a procedure similar to that employed in Section 4 of Wooley [17] could be used to improve the lower order terms in the bounds given by these corollaries. However, the

analysis would necessarily be more difficult, and in any case would seem to be of little value. The methods for bounding $\tilde{G}(k)$ using estimates from Vinogradov's mean value theorem are well known, and we shall therefore be rather brief in our treatment. We refer the reader to Sections 5.2 and 5.3 of Vaughan [11].

The proof of Corollary 1.1. Let $f(x)=\sum_{j=1}^{k}\alpha_j x^j$, and suppose that there exist j, a, q with $2\leqslant j\leqslant k$, $|\alpha_j-a/q|<q^{-2}$, $(a,q)=1$ and $q\leqslant P^j$. Then by Vaughan [11], Theorem 5.2, we have

$$\sum_{n=1}^{P} e(f(n))\ll (J_{s,k-1}(2P)P^{\frac{1}{2}k(k-1)}(qP^{-j}+P^{-1}+q^{-1}))^{1/2s}\log(2P)$$

for each natural number s. In particular, if $P\ll q\ll P^{j-1}$, then on writing Δ_s' for the quantity Δ_s appearing in the statement of Theorem 1.1 with k replaced by $k-1$, we have

$$\sum_{n=1}^{P} e(f(n))\ll P^{1-\sigma+\varepsilon},$$

where

$$\sigma=\sigma(k)=\max_{l\in\mathbf{N}}\frac{1-\Delta'_{l(k-1)}}{2(k-1)l}. \tag{6.1}$$

Now apply Theorem 1.2. We obtain

$$\sigma\geqslant\max_{r\in\mathbf{N}}\frac{1}{2(k-1)(r+r_1)}\left(1-5(\log(k-1))^3\left(1-\frac{3}{2(k-1)}\left(1-\frac{1}{k-1}\right)\right)^r\right),$$

in which $r_1=[(k-1)(\log(k-1)-\log\log(k-1))]+1$.

A standard optimization shows that the maximum occurs when $r\ll k\log\log k$, and so

$$2k^2(\log k+O(\log\log k))\sigma\geqslant 1. \tag{6.2}$$

This completes the proof of Corollary 1.1.

The proof of Corollary 1.2. The argument of Section 5.3 of Vaughan [11] shows that

$$\tilde{G}(k)\leqslant 1+\min_{r\in\mathbf{N}}(2kr+\Delta_{kr}/\sigma_0),$$

where Δ_{kr} is as given in Theorem 1.1, and $\sigma_0=\max\{\sigma, 2^{1-k}\}$, where σ is the exponent given by (6.1). We again apply Theorem 1.2, noting that from Corollary 1.1 we have

$$\sigma_0\geqslant(2k^2(\log k+O(\log\log k)))^{-1}.$$

Then

$$\tilde{G}(k)\leqslant 1+\min_{r\in\mathbf{N}}\left(2k(r+r_2)+\frac{5(\log k)^3}{\sigma_0}\left(1-\frac{3}{2k}\left(1-\frac{1}{k}\right)\right)^r\right),$$

in which $r_2=[k(\log k-\log\log k)]+1$. A standard optimization shows that

the minimum occurs when $r \ll k \log\log k$, and so

$$\tilde{G}(k) \leqslant 2k^2(\log k + O(\log\log k)).$$

This completes the proof of Corollary 1.2.

References

1. R. C. Baker. *Diophantine Inequalities.* L.M.S. Monographs, New Series (Oxford, 1986).
2. G. H. Hardy and J. E. Littlewood. Some problems of "Partitio Numerorum": IV. *Math. Zeit.*, 12 (1922), 161-188.
3. D. R. Heath-Brown. Weyl's inequality, Hua's inequality, and Waring's problem. *J. Lond. Math. Soc.* (2), 38 (1988), 216-230.
4. L.-K. Hua. On Waring's problem. *Quart. J. Math. Oxford*, 9 (1938), 199-202.
5. L.-K. Hua. An improvement of Vinogradov's mean value theorem and several applications. *Quart. J. Math. Oxford*, 20 (1949), 48-61.
6. L.-K. Hua. *Additive Theory of Prime Numbers* (Providence, 1965).
7. A. A. Karatsuba. The mean value of the modulus of a trigonometric sum. *Izv. Akad. Nauk SSSR*, 37 (1973), 1203-1227.
8. Yu. V. Linnik. On Weyl's sums. *Mat. Sbornik (Rec. Math.)*, 12 (1943), 23-39.
9. S. B. Stechkin. On mean values of the modulus of a trigonometric sum. *Trudy Mat. Inst. Steklov.*, 134 (1975), 283-309.
10. O. V. Turina. A new estimate for a trigonometric integral of I. M. Vinogradov. *Izv. Akad. Nauk SSSR, Ser. Mat.*, 51 (1987), No. 2. *Translated in Math. USSR Izvestiya*, 30 (1988), 2, 337-351.
11. R. C. Vaughan. *The Hardy-Littlewood Method* (Cambridge University Press, 1981).
12. R. C. Vaughan. On Waring's problem for cubes. *J. Reine Angew. Math.*, 365 (1986), 122-170.
13. R. C. Vaughan. On Waring's problem for smaller exponents, II. *Mathematika*, 33 (1986), 6-22.
14. I. M. Vinogradov. New estimates for Weyl sums. *Dokl. Akad. Nauk SSSR*, 8 (1935), 195-198.
15. I. M. Vinogradov. The method of trigonometrical sums in the theory of numbers. *Trav. Inst. Steklov*, 23 (1947).
16. A. Z. Walfisz. *Weylsche Exponentialsummen in der neueren Zahlentheorie.* Math. Forsch., XV (Berlin, 1963).
17. T. D. Wooley. Large improvements in Waring's problem. *Annals of Math.*, 135 (1992), 131-164.
18. T. D. Wooley. On Vinogradov's mean value theorem, II. *Mich. Math. J.* to appear.

Professor T. D. Wooley,
Department of Mathematics,
University of Michigan,
Ann Arbor, MI 48109-1003,
U.S.A.

11P05: *NUMBER THEORY; Additive number theory, partitions; Waring's problem.*

Received on the 9th of September, 1990.