NEW ESTIMATES FOR MEAN VALUES OF WEYL SUMS

Kevin B. Ford

1. Introduction

Let

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x$$

be a polynomial with integer coefficients, P a natural number, and let $F(\alpha)$ be the Weyl sum associated with f, defined by

$$F(\alpha) = \sum_{x=1}^{P} e(\alpha f(x)), \tag{1.1}$$

where $e(z) = e^{2\pi i z}$. In this note we develop a new method of estimating the mean values

$$I_s(P) = \int_0^1 |F(\alpha)|^{2s} d\alpha,$$

which have applications to Waring's problem. Observe that $I_s(P)$ is the number of solutions of

$$\sum_{i=1}^{s} (f(x_i) - f(y_i)) = 0$$

with $1 \leqslant x_i, y_i \leqslant P$. If $I_s(P;n)$ denotes the number of solutions of

$$\sum_{i=1}^{s} (f(x_i) - f(y_i)) = n$$

with $1 \leqslant x_i, y_i \leqslant P$, then

$$I_s(P;n) = \int_0^1 |F(\alpha)|^{2s} e(-n\alpha) d\alpha \leqslant I_s(P). \tag{1.2}$$

Similar inequalities hold for general diophantine equations (or systems of equations) of this type, and we shall refer to this by saying that the zero representation dominates. From (1.2) we obtain

$$P^{2s} = \sum_n I_s(P;n) \ll P^k I_s(P),$$

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

whence $I_s(P) \gg P^{2s-k}$, and it is conjectured that this represents the true order of magnitude of $I_s(P)$ when $s \geqslant k \geqslant 3$. We write bounds for $I_s(P)$ in the form

$$I_s(P) \ll P^{2s-k+\Delta(s,k)}, \tag{1.3}$$

and are primarily concerned with the rate at which $\Delta(s,k) \to 0$ as s becomes large.

There are only two known methods for bounding these mean values, both dating from the 1930's. In 1938, Hua [Hu38] used a Weyl-type differencing argument to show that when $1 \leqslant j \leqslant k$,

$$I_{2^{j-1}}(P) \ll P^{2^j-j+\varepsilon}. \tag{1.4}$$

Recently, Heath-Brown [HB] has refined Hua's technique when $f(x) = x^k$, $j = k$ and $k \geqslant 6$, obtaining

$$I_{7\cdot 2^{k-4}}(P) \ll P^{7\cdot 2^{k-3}-k+\varepsilon}. \tag{1.5}$$

The second method depends on estimates of the integral

$$J_{s,k}(P;\mathbf{n}) = \int_{[0,1]^k} \left| \sum_{x=1}^{P} e(\alpha_1 x + \cdots + \alpha_k x^k) \right|^{2s} e(-n_1\alpha_1 - \cdots - n_k\alpha_k) d\boldsymbol{\alpha},$$

first studied by Vinogradov in the mid-1930's. Clearly $J_{s,k}(P;\mathbf{n}) \leqslant J_{s,k}(P;\mathbf{0}) =: J_{s,k}(P)$. Since $J_{s,k}(P;\mathbf{n})$ is the number of solutions to the simultaneous diophantine equations

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

with $1 \leqslant x_i, y_i \leqslant P$, we have

$$P^{2s} = \sum_{\mathbf{n}} J_{s,k}(P;\mathbf{n}) \ll P^{k(k+1)/2} J_{s,k}(P),$$

or $J_{s,k}(P) \gg P^{2s-k(k+1)/2}$. Nontrivial upper bounds for $J_{s,k}(P)$ are now known collectively as *Vinogradov's mean value theorem* and take the form

$$J_{s,k}(P) \ll P^{2s-k(k+1)/2+\eta(s,k)}. \tag{1.6}$$

In what follows, we suppose that (1.6) holds for each pair (s,k) and take this as the "definition" of $\eta(s,k)$. We have

$$\begin{aligned} I_s(P) &= \sum_{a_1n_1+\cdots+a_kn_k=0} J_{s,k}(P;\mathbf{n}) \\ &\ll P^{k(k-1)/2} J_{s,k}(P) \\ &\ll P^{2s-k+\eta(s,k)}, \end{aligned} \tag{1.7}$$

i.e., (1.3) holds with $\Delta(s,k) = \eta(s,k)$. This represents a vast improvement over Hua's inequality for large k, since modern bounds for $J_{s,k}(P)$ have $\eta(s,k)$ very close to zero when s is of order $k^2 \log k$.

We develop a more sophisticated method of bounding $I_s(P)$ in terms of bounds (1.6) which reduces $\Delta(s,k)$ roughly by a factor of k. More precisely, we have

Theorem 1. *Let m be an integer with $1 \leqslant m \leqslant k$. Then*

$$I_s(P) \ll P^{2s-k+\frac{1}{m}\eta(s-m(m-1)/2,k)}.$$

Taking $\eta(s,k) \approx k^2 e^{-2s/k^2}$ [Wo92b], the optimal choice for m is about $k/\sqrt{2}$, and we then have approximately

$$I_s(P) \ll P^{2s-k+\frac{\sqrt{2e}}{k}\eta(s,k)}.$$

Let $\widetilde{G}(k)$ be the smallest 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,

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

where $\mathfrak{S}_{s,k}(n)$ denotes the usual singular series in Waring's problem (see [Va81, §2.6]). Roughly speaking, we have $\widetilde{G}(k) \leqslant 2s$, where s is the smallest integer for which $\Delta(s,k)$ is very small (say $< 1/\log k$). Hua's inequality implies $\widetilde{G}(k) \leqslant 2^k + 1$, and this was the best known bound for small k until recently. Vaughan [Va86a,b] showed that $\widetilde{G}(k) \leqslant 2^k$, and Heath-Brown [HB] and Boklan [Bo] used (1.5) to establish $\widetilde{G}(k) \leqslant 7 \cdot 2^{k-3}$ for $k \geqslant 6$.

For large k, the best bounds all derive from (1.7). In a series of papers in the 1930's and 1940's, Vinogradov, Hua and others refined estimates for $J_{s,k}(P)$, leading to $\widetilde{G}(k) \leqslant (4+o(1))k^2 \log k$, proved by Hua [Hu49] in 1949. Until recently, only the $o(1)$ term has been improved. Using an "efficient differencing" technique, Wooley [Wo92b] obtained superior bounds for $J_{s,k}(P)$ which give $\widetilde{G}(k) \leqslant (2+o(1))k^2 \log k$. Combining Theorem 1 with Wooley's bounds for $J_{s,k}(P)$ produces the following improvement.

Corollary 1.1. *We have $\widetilde{G}(k) \leqslant k^2(\log k + \log\log k + O(1))$ as $k \to \infty$.*

In fact, upper bounds for $\widetilde{G}(k)$ are improved for all $k \geqslant 9$, and we record below the bounds attainable from Theorem 1 for $9 \leqslant k \leqslant 20$.

Corollary 1.2. *We have $\widetilde{G}(9) \leqslant 393$, $\widetilde{G}(10) \leqslant 551$, $\widetilde{G}(11) \leqslant 717$, $\widetilde{G}(12) \leqslant 874$, $\widetilde{G}(13) \leqslant 1050$, $\widetilde{G}(14) \leqslant 1233$, $\widetilde{G}(15) \leqslant 1434$, $\widetilde{G}(16) \leqslant 1647$, $\widetilde{G}(17) \leqslant 1881$, $\widetilde{G}(18) \leqslant 2137$, $\widetilde{G}(19) \leqslant 2412$, $\widetilde{G}(20) \leqslant 2703$.*

These bounds may be compared with the bounds $\widetilde{G}(9) \leqslant 448$ (Boklan [Bo]), and $\widetilde{G}(10) \leqslant 750$, $\widetilde{G}(11) \leqslant 975$, $\widetilde{G}(12) \leqslant 1200$, $\widetilde{G}(13) \leqslant 1450$, $\widetilde{G}(14) \leqslant 1725$, $\widetilde{G}(15) \leqslant 2026$, $\widetilde{G}(16) \leqslant 2354$, $\widetilde{G}(17) \leqslant 2708$, $\widetilde{G}(18) \leqslant 3089$, $\widetilde{G}(19) \leqslant 3497$, $\widetilde{G}(20) \leqslant 3932$ (Wooley [Wo92b]).

Any bounds for $I_s(P)$ which depend upon Vinogradov's mean value theorem are in a sense unsatisfactory, since the best possible upper bounds for $J_{s,k}(P)$ only imply $\widetilde{G}(k) \ll k^2$ (using (1.7) or Theorem 1), and it is likely that $\widetilde{G}(k) \ll k$.

The author wishes to thank Professor Bombieri for showing the author the argument sketched in the next section and Professor T. D. Wooley for supplying Lemma 3.1. The work for this paper was completed while the author was enjoying the hospitality of the Institute For Advanced Study, supported by NSF grant DMS 9304580.

2. A first iterative approach

When $f(x)=x^k$ and the range of x in (1.1) is restricted to so-called "smooth" numbers, Vaughan [Va89] has developed an iterative process for a single equation which is similar to the iteration used for a system of equations to prove Vinogradov's mean value theorem (see also [Wo92a]). The next lemma, from unpublished notes by Bombieri in 1974, represents a simple idea on how to create such an iterative process for classical Weyl sums for arbitrary polynomials f. It is included here only as a motivation for the more sophisticated method we will actually follow.

Lemma 2.1. *If $k \geqslant 3$, then*

$$I_s(P) \ll P^{2s-k+\Delta(s,k)},$$

where

$$\Delta(s,k)=\frac{k-1}{2}-\left(\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k}\right)+\frac{\eta(s-k+1,k)}{k}.$$

This is stronger than both (1.4) and (1.7) for $k\log k \ll s \leqslant (\frac{1}{2}+o(1))k^2\log k$. However, as $\eta(s,k)\to 0, \Delta(s,k)\to \frac{k}{2}-\log k+O(1)$, which is much too large for the application to Waring's problem.

Proof sketch. For simplicity, assume that $f^{(h)}(x)$ is irreducible over $\mathbb{Q}$ for $1\leqslant h\leqslant k-2$. The proof for general f follows the method given in the proof of Lemma 4.1 below. Let $p_1,\dots,p_{k-1}$ be primes with $sP^{1/r(r+1)}\leqslant p_r\leqslant 2sP^{1/r(r+1)}$, such that the congruence $\prod_{h=1}^{k-2} f^{(h)}(x)\equiv 0 \pmod{p_r}$ is insoluble. Let $q_0=1$, $q_m=p_1\cdots p_m$, and let $I_s(P;q,b)$ denote the number of solutions of

$$\sum_{i=1}^{s}(f(qx_i+b)-f(qy_i+b))=0, \tag{2.1}$$

with $0\leqslant x_i,y_i\leqslant P/q$. Our goal is to prove

$$I_s(P;q_{m-1},b)\ll p_m^{2s+m-1}\sum_{a=0}^{p_m-1} I_{s-1}(P;q_m,b+aq_{m-1}). \tag{2.2}$$

Writing $f(q_{m-1}x+b)=\sum f^{(h)}(b)(q_{m-1}x)^h/h!$, it follows from (2.1) that q_{m-1} divides

$$f'(b)\sum_{i=1}^{s}(x_i-y_i).$$

Suppose $m\geqslant 2$, so that $q_{m-1}\geqslant sP^{1/2}$. Note also that $(q_{m-1},f'(b))=1$. Because of the reduced ranges of x_i,y_i, we have

$$\left|\sum_{i=1}^{s}(x_i-y_i)\right|\leqslant sP/q_{m-1}<q_{m-1},$$

and it follows that

$$\sum_{i=1}^{s}(x_i-y_i)=0.$$

When $m \leqslant k-1$, we similarly obtain

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \qquad (1 \leqslant j \leqslant m-1), \tag{2.3}$$

using the relations $q_{m-1} \geqslant sP^{1-1/m}$ and $(f^{(h)}(b), q_{m-1}) = 1$ for $1 \leqslant h \leqslant m-1$. When $m = k$, (2.3) holds as well, except when $(f^{(k-1)}(b), q_{k-1}) > 1$. These exceptional b can be safely ignored by employing the method given in the proof of Lemma 4.1. For the remaining b, we then have

$$I_s(P; q_{k-1}, b) \leqslant J_{s,k}(P^{1/k}), \tag{2.4}$$

and this terminates the iteration.

When $m < k$, we separate off the variables x_1, y_1 and divide the remaining variables into residue classes modulo p_m. Using Hölder's inequality to align the residue classes yields

$$I_s(P; q_{m-1}, b) \ll p_m^{2s-3} \sum_{a=0}^{p_m-1} S(p, a),$$

where $S(P, a)$ is the number of solutions of the system

$$\begin{cases} \displaystyle\sum_{i=1}^{s-1}(f(q_m u_i + b') - f(q_m v_i + b')) = f(q_{m-1}x + b) - f(q_{m-1}y + b) \\ \displaystyle\sum_{i=1}^{s-1}((p_m u_i + a)^j - (p_m v_i + a)^j) = x^j - y^j \qquad (1 \leqslant j \leqslant m-1) \end{cases}$$

with $0 \leqslant x, y \leqslant P/q_{m-1}$, $0 \leqslant u_i, v_i \leqslant P/q_m$ and $b' = b + aq_{m-1}$. Utilizing the additional equations, one can show that

$$f(q_{m-1}x + b) - f(q_{m-1}y + b) \equiv 0 \pmod{p_m^m}, \tag{2.5}$$

and so the number of possible pairs (x, y) is $\ll p_m^{-m}(P/q_{m-1})^2$. Since the zero representation dominates, for each pair (x, y) the number of $(\mathbf{u}, \mathbf{v})$ is bounded by $I_{s-1,m}(P; q_m, b')$. Inequality (2.2) now follows from the fact that $P/q_{m-1} \ll p_m^{m+1}$, and the lemma follows by iterating (2.2) and applying (2.4) when $m = k$.

3. Preliminaries

To avoid certain technical complications, we assume that the coefficients a_j are positive. If not, replacing $f(x)$ by $f(x+c)$ for some natural number c will result in a polynomial with all coefficients positive. The effect on the mean value estimates is negligible, for if

$$F^*(\alpha) = \sum_{x=1}^{P} e(\alpha f(x+c)),$$

then

$$\int_0^1 |F(\alpha)|^{2s} d\alpha \ll \int_0^1 |F^*(\alpha)|^{2s} d\alpha + \int_0^1 c^{2s} d\alpha \ll \int_0^1 |F^*(\alpha)|^{2s} d\alpha.$$

Our improvement to the argument in the preceding section involves a more efficient use of the additional equations (2.3) which arise when q_m becomes large. Instead of separating only x_1 and y_1, we separate $x_1, \dots, x_m$ and $y_1, \dots, y_m$ and proceed in a manner analogous to the iteration used to bound $J_{s,m}(P)$ (see [Va81, §5.1]). This leads to a system of congruences in these $2m$ variables modulo powers of p_m in place of the single congruence (2.5). The number of solutions of this system is estimated by the following generalization of a result due to Linnik [Li, Lemma 1].

Lemma 3.1[Wo95]. *Let $f_1, \dots, f_d$ be polynomials in $\mathbb{Z}[x_1, \dots, x_d]$ with respective degrees $k_1, \dots, k_d$, and write*

$$J(\mathbf{f}; \mathbf{x}) = \det \left(\frac{\partial f_j(\mathbf{x})}{\partial x_i} \right)_{1 \leqslant i,j \leqslant d}.$$

Also, let p be a prime number and s be a natural number. Then the number, N, of solutions of the simultaneous congruences

$$f_j(x_1, \dots, x_d) \equiv 0 \pmod{p^s} \quad (1 \leqslant j \leqslant d)$$

with $1 \leqslant x_i \leqslant p^s$ $(1 \leqslant i \leqslant d)$ and $(J(\mathbf{f}; \mathbf{x}), p) = 1$, satisfies $N \leqslant k_1 \cdots k_d$.

The next lemma gives an explicit form for the Jacobians of the functions we will need to prove Theorem 1.

Lemma 3.1. *Suppose $h \geqslant m$, $f_j(\mathbf{x}) = x_1^j + \cdots + x_m^j$ for $1 \leqslant j \leqslant m-1$, and $f_m(\mathbf{x}) = x_1^h + \cdots + x_m^h$. Then in the notation of Lemma 3.1,*

$$J(\mathbf{f}; \mathbf{x}) = h(m-1)! K_{h,m}(\mathbf{x}) \prod_{i<j} (x_i - x_j),$$

where $K_{h,m}(\mathbf{x})$ is the sum of all monomials in $x_1, \dots, x_m$ of total degree $h - m$.

Proof. The conclusion is obvious when $m = 2$, and when $h = m$ the determinant is the Vandermonde determinant, so the lemma follows in this case as well (with $K_{h,m}(\mathbf{x}) = 1$). Now suppose $h > m > 2$ and let $J_{h,m}(\mathbf{x}) = J(\mathbf{f}; \mathbf{x})/(h(m-1)!)$. Subtracting the $i = m$ column from each of the other columns and taking out common factors gives

$$J_{h,m}(\mathbf{x}) = (x_1 - x_m) \cdots (x_{m-1} - x_m) \det(g_{ij}),$$

where $1 \leqslant i \leqslant m-1$, $j \in \{1, 2, \dots, m-2, h-1\}$, and $g_{ij} = (x_i^j - x_m^j)/(x_i - x_m)$. Expanding the terms in the $j = h-1$ row and using elementary row operations, we have

$$\det(g_{ij}) = \sum_{d=m}^{h} x_m^{h-d} J_{d-1,m-1}(x_1, \dots, x_{m-1}).$$

The lemma now follows from the identity

$$K_{h,m}(x_1, \dots, x_m) = \sum_{d=m}^{h} x_m^{h-d} K_{d-1,m-1}(x_1, \dots, x_{m-1})$$

by double induction on h and m.

For $1 \leqslant m \leqslant k-1$, let $J_m(\mathbf{x}; q, b)$ denote the Jacobian of the functions $f_j(\mathbf{x}) = x_1^j + \cdots + x_m^j$ $(1 \leqslant j \leqslant m-1)$ and $f_m(\mathbf{x}) = \sum_{i=1}^m f(qx_i + b)$. By Lemma 3.1, we have

$$J_m(\mathbf{x}; q, b) = (m-1)! F_m(\mathbf{x}; q, b) \prod_{1 \leqslant i < j \leqslant m} (x_i - x_j), \tag{3.1}$$

where

$$F_m(\mathbf{x}; q, b) = \sum_{h=m}^{k} h q^h \sum_{i=h}^{k} a_i \binom{i}{h} b^{i-h} K_{h,m}(\mathbf{x}). \tag{3.2}$$

Let P be a large integer, and for $1 \leqslant r \leqslant k-1$, let $\mathscr{P}_r$ denote the $2sk^4$ smallest primes greater than $sP^{1/(r(r+1))}$. If P is sufficiently large, $p < 2sP^{1/(r(r+1))}$ for each $p \in \mathscr{P}_r$. For $m \geqslant 1$, let $I_{s,m}(P; q, b)$ denote the number of solutions of

$$\begin{cases} \displaystyle\sum_{i=1}^{s} (f(qx_i + b) - f(qy_i + b)) = 0 \\ \displaystyle\sum_{i=1}^{s} (x_i^j - y_i^j) = 0 \qquad (1 \leqslant j \leqslant m-1) \end{cases} \tag{3.3}$$

with $0 \leqslant x_i, y_i \leqslant P/q$. In particular, $I_s(P) \leqslant I_{s,1}(P; 1, 0)$. In mean value form,

$$I_{s,m}(P; q, b) = \int_{[0,1]^m} |F(\boldsymbol{\alpha})|^{2s} d\boldsymbol{\alpha},$$

where

$$F(\boldsymbol{\alpha}) = \sum_{0 \leqslant x \leqslant P/q} e(\alpha_1 x + \cdots + \alpha_{m-1} x^{m-1} + \alpha_m f(qx + b)).$$

4. Improved iteration procedure

We are now ready to construct the iteration which leads to Theorem 1. The proof of this lemma is similar in structure to the proof of a bound for $J_{s,k}(P)$ given in [Wo93b].

Lemma 4.1. *Suppose $k \geqslant 3$, $1 \leqslant m \leqslant k-1$, $s > m$ and $q = p_1 \cdots p_{m-1}$, where each $p_i \in \mathscr{P}_i$ (if $m = 1$ suppose $q = 1$). Also suppose b is a number satisfying $0 \leqslant b < q$ and $(f^{(j)}(b), q) = 1$ for $1 \leqslant j \leqslant k-1$. Then*

$$I_{s,m}(P; q, b) \ll \max_{p \in \mathscr{P}_m} p^{2s-2m+\frac{3}{2}m(m+1)} \max_{a \in \mathscr{B}(p)} I_{s-m,m+1}(P; pq, b + aq),$$

where $\mathscr{B}(p) = \mathscr{B}(p; q, b)$ denotes the set of a with $0 \leqslant a < p$ and $(f^{(j)}(b+aq), pq) = 1$ for $1 \leqslant j \leqslant k-1$.

Proof. For each m-tuple $\mathbf{h} = (h_1, \dots, h_m)$, let $R_1(\mathbf{h})$ denote the number of solutions of

$$(4.1)\qquad \begin{cases} \displaystyle\sum_{i=1}^{s} f(qx_i + b) = h_m \\ \displaystyle\qquad\sum_{i=1}^{s} x_i^j = h_j \qquad (1 \leqslant j \leqslant m-1) \end{cases}$$

with $0 \leqslant x_i \leqslant P/q$ and $x_1, \dots, x_m$ distinct, and let $R_2(\mathbf{h})$ denote the corresponding number of solutions with $x_1, \dots, x_m$ not distinct. Then

$$I_{s,m}(P; q, b) = \sum_{\mathbf{h}} (R_1(\mathbf{h}) + R_2(\mathbf{h}))^2 \leqslant 2(S_1 + S_2),$$

where $S_i = \sum_{\mathbf{h}} R_i(\mathbf{h})^2 \quad (i = 1, 2)$.

Suppose $S_2 \geqslant S_1$, so that $I_{s,m}(P; q, b) \leqslant 4S_2$. Then by considering the underlying diophantine equations and noting that $R_2(\mathbf{h})$ is at most $\binom{m}{2}$ times the number of solutions of (4.1) with $x_1 = x_2$, we have by Hölder's inequality,

$$\begin{aligned} I_{s,m}(P; q, b) &\leqslant m^4 \int_{[0,1]^m} |F(\boldsymbol{\alpha})^{2s-4} F(2\boldsymbol{\alpha})^2| d\boldsymbol{\alpha} \\ &\leqslant m^4 \left(\int_{[0,1]^m} |F(\boldsymbol{\alpha})|^{2s} d\boldsymbol{\alpha} \right)^{1-2/s} \left(\int_{[0,1]^m} |F(2\boldsymbol{\alpha})|^{2s} d\boldsymbol{\alpha} \right)^{1/s} \\ &= m^4 (I_{s,m}(P; q, b))^{1-1/s}, \end{aligned}$$

whence $I_{s,m}(P; q, b) \ll 1$. On the other hand, the number of solutions of (3.3) with $x_i = y_i$ for each i is $\geqslant (P/q)^s$. Therefore $S_1 \geqslant S_2$ and $I_{s,m}(P; q, b) \leqslant 4S_1$.

Note that S_1 is the number of solutions counted in $I_{s,m}(P; q, b)$ with $x_1, \dots, x_m$ distinct and likewise for $y_1, \dots, y_m$. Let

$$(4.2)\qquad H(x_1, \dots, x_s) = J_m(x_1, \dots, x_m; q, b) \prod_{\substack{m+1 \leqslant i \leqslant s \\ 1 \leqslant j \leqslant k-1}} f^{(j)}(qx_i + b).$$

By (3.1),(3.2) and the fact that all of the a_j are positive, for a solution $(\mathbf{x}, \mathbf{y})$ counted in S_1, we have

$$0 < |H(\mathbf{x})H(\mathbf{y})| \ll P^{m(m-1)+2k+sk^2} < P^{2sk^2}$$

if P is sufficiently large. There is some prime $p \in \mathscr{P}_m$ which does not divide $H(\mathbf{x})H(\mathbf{y})$, for otherwise $|H(\mathbf{x})H(\mathbf{y})| > P^{2sk^4/(m(m+1))} > P^{2sk^2}$. It follows that $S_1 \leqslant \sum_{p \in \mathscr{P}_m} S_1(p)$, where $S_1(p)$ denotes the number of solutions of (3.3) with $p \nmid H(\mathbf{x})H(\mathbf{y})$. For a fixed prime p, let

$$F(\boldsymbol{\alpha}, a) = \sum_{\substack{0 \leqslant x \leqslant P/q \\ x \equiv a \pmod{p}}} e(\alpha_1 x + \dots + \alpha_{m-1} x^{m-1} + \alpha_m f(qx + b)).$$

Let $\mathscr{A}$ denote the m-tuples $\mathbf{a} = (a_1, \dots, a_m)$ with $0 \leqslant a_i < p$ and $p \nmid J_m(\mathbf{a}; q, b)$. For $1 \leqslant j \leqslant k-1$, $(f^{(j)}(qx+b), q) = (f^{(j)}(b), q) = 1$ and $x \equiv a \pmod p$ implies $f^{(j)}(qx+b) \equiv f^{(j)}(b+aq) \pmod p$. Thus by (4.2),

$$S_1(p) = \int_{[0,1]^m} \left| \sum_{a \in \mathscr{B}(p)} F(\boldsymbol{\alpha}, a) \right|^{2s-2m} \left| \sum_{\mathbf{a} \in \mathscr{A}} F(\boldsymbol{\alpha}, a_1) \cdots F(\boldsymbol{\alpha}, a_m) \right|^2 d\boldsymbol{\alpha}.$$

By Hölder's inequality,

$$\left| \sum_{a \in \mathscr{B}(p)} F(\boldsymbol{\alpha}, a) \right|^{2s-2m} \leqslant p^{2s-2m-1} \sum_{a \in \mathscr{B}(p)} |F(\boldsymbol{\alpha}, a)|^{2s-2m},$$

and hence

$$S_1(p) \leqslant p^{2s-2m} \max_{a \in \mathscr{B}(p)} S_3(p, a), \tag{4.3}$$

where $S_3(p,a)$ denotes the number of solutions of

$$\begin{cases} \displaystyle\sum_{i=1}^{m} (f(qx_i+b) - f(qy_i+b)) = \sum_{i=1}^{s-m} (f(pqu_i+b+aq) - f(pqv_i+b+aq)) \\ \displaystyle\qquad\qquad\qquad \sum_{i=1}^{m} x_i^j - y_i^j = \sum_{i=1}^{s-m} (pu_i+a)^j - (pv_i+a)^j \qquad (1 \leqslant j \leqslant m-1) \end{cases}$$

with $0 \leqslant x_i, y_i \leqslant P/q$, $p \nmid J_m(\mathbf{x}; q, b) J_m(\mathbf{y}; q, b)$, and $0 \leqslant u_i, v_i \leqslant P/(qp)$. In the above system, we expand the functions in the top equation in a Taylor series about the point $b + aq$, and apply the binomial theorem to the remaining equations. If $d_h = f^{(h)}(b+aq)q^h/h!$, then $S_3(p,a)$ is the number of solutions of

$$\begin{cases} \displaystyle\sum_{h=1}^{k} d_h \sum_{i=1}^{m} ((x_i-a)^h - (y_i-a)^h) = \sum_{h=1}^{k} d_h p^h \sum_{i=1}^{s-m} (u_i^h - v_i^h) \\ \displaystyle\qquad \sum_{i=1}^{m} ((x_i-a)^j - (y_i-a)^j) = p^j \sum_{i=1}^{s-m} (u_i^j - v_i^j) \qquad (1 \leqslant j \leqslant m-1) \end{cases} \tag{4.4}$$

with the same conditions on $\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}$. Let $T(p,a)$ denote the number of $(\mathbf{x}, \mathbf{y})$ for which (4.4) is satisfied for some $(\mathbf{u}, \mathbf{v})$. Since the zero representation dominates, we have

$$S_3(p,a) \leqslant T(p,a) I_{s-m,m}(P; qp, b+aq). \tag{4.5}$$

In the top equation of (4.4), the terms with $1 \leqslant h \leqslant m-1$ cancel, so

$$\sum_{h=m}^{k} d_h \sum_{i=1}^{m} ((x_i-a)^h - (y_i-a)^h) \equiv 0 \pmod{p^m}. \tag{4.6}$$

Since $P/q < p^{m+1}$, the number of possibilities for $y_1, \dots, y_m$ is at most $p^{m(m+1)}$. By (4.4) and (4.6) we deduce that

$$T(p,a) \leqslant p^{m(m+1)} \max_{\mathbf{c}} V(\mathbf{c}),$$

where $V(\mathbf{c})$ is the number of solutions of the simultaneous congruences

$$\begin{cases} \sum_{h=m}^{k} d_h \sum_{i=1}^{m} (x_i - a)^h \equiv c_m \pmod{p^m} \\ \qquad\quad \sum_{i=1}^{m} (x_i - a)^j \equiv c_j \pmod{p^j} \qquad (1 \leqslant j \leqslant m-1) \end{cases}$$

with $0 \leqslant x_i < p^{m+1}$ and $p \nmid J_m(\mathbf{x}; q, b)$. For a given $\mathbf{c}$, there are at most $p^{m(m+1)/2}$ possibilities modulo p^{m+1} for the right sides of these congruences. We now reverse course, extending the sum on h in the top congruence down to $h = 0$ and applying the binomial theorem to the lower $m-1$ congruences. It follows that

$$\max_{\mathbf{c}} V(\mathbf{c}) \leqslant p^{m(m+1)/2} \max_{\mathbf{c}} W(\mathbf{c}),$$

where $W(\mathbf{c})$ is the number of solutions of

$$\begin{cases} \sum_{i=1}^{m} f(qx_i + b) \equiv c_m \pmod{p^{m+1}} \\ \qquad\quad \sum_{i=1}^{m} x_i^j \equiv c_j \pmod{p^{m+1}} \qquad (1 \leqslant j \leqslant m-1) \end{cases}$$

with $0 \leqslant x_i < p^{m+1}$ and $p \nmid J_m(\mathbf{x}; q, b)$. Lemma 3.1 implies $W(\mathbf{c}) \leqslant k(m-1)!$ for every $\mathbf{c}$, and thus

$$T(p,a) \ll p^{\frac{3}{2}m(m+1)}.$$

By (4.3) and (4.5), the lemma will follow upon showing

$$I_{s-m,m}(P; qp, b + aq) = I_{s-m,m+1}(P; qp, b + aq)$$

when $a \in \mathscr{B}(p)$. That is, we must show that every solution $(\mathbf{x}, \mathbf{y})$ counted in $I_{s-m,m}(P; qp; b + aq)$ satisfies

$$X_m := \sum_{i=1}^{s-m} (x_i^m - y_i^m) = 0. \tag{4.7}$$

By (3.3),

$$\sum_{h=m}^{k} d_h p^h \sum_{i=1}^{s-m} (x_i^h - y_i^h) = 0.$$

Thus, pq divides $f^{(m)}(b+aq)X_m$, and by the definition of $\mathscr{B}(p)$, $(f^{(m)}(b+aq), pq) = 1$. Equation (4.7) now follows since $|X_m| \leqslant s(P/qp)^m < qp$.

The next lemma provides a simple method of transitioning to Vinogradov's mean value theorem at any stage of the iteration.

Lemma 4.1. *If* $1 \leqslant m \leqslant k$, $q \leqslant (sP^m)^{1/(m+1)}$ *and* $(f^{(j)}(b), q) = 1$ $(1 \leqslant j \leqslant k-1)$, *then*

$$I_{s,m}(P; q, b) \ll \prod_{j=m}^{k-1} \frac{1}{q}\left(\frac{P}{q}\right)^j J_{s,k}(P/q).$$

Proof. When $m = k$, the equations (3.3) imply

$$\sum_{i=1}^{s}(x_i^k - y_i^k) = 0,$$

and thus

$$I_{s,k}(P; q, b) \ll J_{s,k}(P/q).$$

The variables x_i, y_i start at 1 in the definition of $J_{s,k}(P)$, which explains why the above is not a strict inequality. Now suppose $m \leqslant k-1$. The system (3.3), plus the conditions on b, imply that

$$\sum_{i=1}^{s}(x_i^m - y_i^m) \equiv 0 \pmod{q}. \tag{4.8}$$

On the other hand,

$$\left|\sum_{i=1}^{s}(x_i^m - y_i^m)\right| \leqslant s(P/q)^m.$$

There are thus at most $s(P/q)^m q^{-1}$ possible values for the sum in (4.8). Since the zero representation dominates,we have

$$I_{s,m}(P; q, b) \leqslant \frac{s}{q}\left(\frac{P}{q}\right)^m I_{s,m+1}(P; q, b),$$

and the lemma follows by induction on m.

If b and q satisfy the conditions of Lemma 4.1, then

$$I_{s-\frac{1}{2}m(m-1),m}(P; q, b) \ll P^{\frac{2s}{m(m+1)}+\frac{1}{2}} \max_{p\in\mathscr{P}_m} \max_{a\in\mathscr{B}(p)} I_{s-\frac{1}{2}m(m+1),m+1}(P; pq; b + aq).$$

Iterating this expression, starting with $m = 1$ and terminating with Lemma 4.1 at $m = r$ gives

$$\begin{aligned} I_s(P) &\ll P^{2s(1-\frac{1}{r})+\frac{r-1}{2}+\sum_{j=r}^{k-1}(\frac{j-1}{r}-1)} J_{s-\frac{1}{2}r(r-1),k}(P^{1/r}) \\ &\ll P^{2s-k+\frac{1}{r}\eta(s-\frac{1}{2}r(r-1),k)}, \end{aligned}$$

and Theorem 1 is proved.

We conclude this section by mentioning that Lemma 4.1 may be generalized in the following manner. In the estimation of $I_{s,m}$, we choose a parameter h, $1 \leqslant h \leqslant m$ and separate the variables $x_1, \ldots, x_h, y_1, \ldots, y_h$ to the left side of the equations defining $S_3(p, a)$. Thus, taking $h = m$ yields Lemma 4.1 and taking $h = 1$ at each stage gives Lemma 2.1. This generalization does lead to improvements in bounds for $I_s(P)$ for values of s smaller than those required for Waring's problem, but the author has yet to find an application for these bounds.

5. The asymptotic formula in Waring's problem

The methods of bounding $\widetilde{G}(k)$ using estimates for $I_s(P)$ are well known, and we refer the reader to Chapters 4 and 5 of [Va81]. We first require upper bound estimates for Vinogradov's integral as well as minor arc bounds for Weyl sums. The next lemma, a simplified version of Theorem 1.1 of [Wo92b], gives an upper bound for $J_{s+k,k}(P)$ given a bound for $J_{s,k}(P)$.

Lemma 5.1 (Wooley). *Suppose $J_{s,k}(P) \ll P^{2s-k(k+1)/2+\eta}$ and $\frac{1}{2}(j-1)(j-2) \leqslant \eta$. Let $\phi_j = 1/k$ and for $J = j, \dots, 2$ set*

$$\phi_{J-1} = \frac{k + (k^2 + \frac{1}{2}(J-1)(J-2) - \eta)\phi_J}{2k^2}.$$

If $\phi = \phi_1$, then

$$J_{s+k,k}(P) \ll P^{2(s+k)-k(k+1)/2+\eta(1-\phi)+k(k\phi-1)}.$$

Lemma 5.1. *If k is sufficiently large, and $1 \leqslant r \leqslant k(\log k - \log\log k)$, then (1.6) holds with*

$$\eta(rk, k) = k^2 e^{-2r/k}.$$

Proof. This follows by combining the estimation techniques of [Wo92b, §5] and [Wo93a, §2]. Let $\delta(1) = \frac{1}{2}(1 - 1/k)$ and define $\delta(r)$ iteratively as follows. If $\delta(r-1) < (\log k/k)^2$ then set $\delta(r) = \delta(r-1)$. Otherwise apply Lemma 5.1 with $j = [\log^{1/4} k] + 1$ and $\eta = k^2\delta(r-1)$ and set $\delta(r) = \delta(r-1)(1-\phi) + \phi - 1/k$. Starting with the classical estimate $J_{k,k}(P) \ll P^k$, it follows from Lemma 5.1 by induction that $J_{rk,k}(P) \ll P^{2s-k(k+1)/2+k^2\delta(r)}$ for each r. The lemma will follow upon showing that

$$\delta(r) < e^{-2r/k}. \tag{5.1}$$

Note that (5.1) holds if $\delta(r) < (\log k/k)^2$ because of the restriction on r. Thus we may assume that $\delta = \delta(r-1) \geqslant (\log k/k)^2$. In the notation of Lemma 5.1, we have $\eta > (j-1)(j-2)\log^{3/2} k$, and hence if $1 \leqslant J \leqslant j$,

$$k^2 + \frac{1}{2}(J-1)(J-2) - \eta < k^2(1-\delta'),$$

where

$$\delta' = \delta(1 - \log^{-3/2} k).$$

Therefore,

$$\phi_{J-1} < \frac{k + k^2(1-\delta')\phi_J}{2k^2} = \frac{1}{2k} + \frac{1-\delta'}{2}\phi_J.$$

Since $\phi_j = 1/k$, by induction on J we have

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

In particular,

$$\phi_1 < \frac{1}{k(1+\delta')}(1+2^{1-j}\delta') < \frac{1}{k(1+\delta)}(1+2\delta\log^{-3/2}k).$$

Thus

$$\begin{aligned}\delta(r) = \delta - 1/k + (1-\delta)\phi_1 &< \delta - \frac{1}{k} + \frac{1-\delta}{k(1+\delta)}(1+2\delta\log^{-3/2}k)\\ &= \delta\left(1 - \frac{2-\omega}{k(1+\delta)}\right),\end{aligned}$$

where $\omega = 2(1-\delta)\log^{-3/2}k$. It follows that

$$\begin{aligned}\delta(r) + \log\delta(r) &< \delta - \frac{\delta(2-\omega)}{k(1+\delta)} + \log\delta - \frac{2-\omega}{k(1+\delta)}\\ &< \delta + \log\delta - \frac{2}{k} + \frac{2}{k\log^{3/2}k}.\end{aligned}$$

Since $\delta(1) + \log\delta(1) < 1/2 - \log 2 - 3/(2k)$, it follows by induction that whenever $\delta(r-1) > (\log k/k)^2$,

$$\begin{aligned}\delta(r) + \log\delta(r) &< -\frac{2r}{k} + \frac{1}{2} - \log 2 + \frac{1}{2k} + \frac{2r-2}{k\log^{3/2}k}\\ &< -\frac{2r}{k}.\end{aligned} \tag{5.2}$$

Inequality (5.1) now follows by exponentiating (5.2).

Bounds for Vinogradov's integral lead to minor arc bounds for Weyl sums as provided in the next lemma, which collects together the estimates from Weyl's inequality (Lemma 2.4 of [Va81]), Theorem 5.2 of [Va81], and Theorems 1 and 2 of [Wo94b].

Lemma 5.1. *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 a, q with $|\alpha_k - a/q| < q^{-2}$, $(a,q) = 1$ and $P \leqslant q \leqslant P^{k-1}$. Then $f(\boldsymbol{\alpha}) \ll_{\epsilon,k} P^{1-\sigma(k)+\epsilon}$, where*

$$\begin{aligned}\sigma(k) &= \max\left(2^{1-k}, \sigma_1(k), \sigma_2(k)\right),\\ \sigma_1(k) &= \max_{s\geqslant 1}\left(\frac{1-\eta(s,k-1)}{2s}\right),\\ \sigma_2(k) &= \max_{1\leqslant r\leqslant k/2}\left(\min(\sigma_3(k,r), \sigma_4(k,r))\right),\\ \sigma_3(k,r) &= \max_{s\geqslant k(k-1)/2}\left(\frac{r-\eta(s,k-1)}{2rs}\right),\\ \sigma_4(k,r) &= \max_{t\geqslant 1}\left(\frac{k-r(1+\eta(t,k))}{2tk}\right).\end{aligned}$$

In particular, $1/\sigma(k) \leqslant (3/2 + o(1))k^2\log k$.

We are now ready to bound $\widetilde{G}(k)$ in terms of $\eta(s,k)$ and $\sigma(k)$. Let $f(x) = x^k$ and suppose that for each s we have bounds (1.3). It follows from the analysis of section 5.3 of [Va81] that

$$\widetilde{G}(k) \leqslant 1 + \min_s(2s + \Delta(s,k)/\sigma(k)). \tag{5.3}$$

Theorem 1 then implies

Lemma 5.1. *We have*

$$\widetilde{G}(k) \leqslant 1 + \min_{\substack{1\leqslant m\leqslant k\\ s\geqslant 1}} \left(m(m-1) + 2s + \frac{\eta(s,k)}{m\sigma(k)} \right).$$

To prove Corollary 1.1, let $m = k$ and $s = rk$, where

$$r = \left[\frac{k}{2}(\log k + \log\log k) \right] + 1.$$

By Lemma 5.1, $\eta(rk, k) \leqslant k(\log k)^{-1}$, and thus Lemmas 5.1 and 5.1 imply

$$\widetilde{G}(k) \leqslant k^2(\log k + \log\log k + O(1)).$$

To bound $\widetilde{G}(k)$ when k is small, we apply Lemma 5.1 with values for $\eta(s,k)$ obtained by combining Lemma 5.1 with the technique of [Wo94a].

Lemma 5.1[Wo94a, Lemma 4.2]**.** *Let $l = [k/2]$ and $u = [s(1-t/2l)^{-1}]+1$. Suppose that r and t are natural numbers satisfying $r \geqslant 3$, $t < 2l$ and $r + t \geqslant k$. If $0 < \theta \leqslant 1/r$ then*

$$J_{s+t,k}(P) \ll P^{(2s+\omega(r,t,k))\theta} \left(P^t J_{s,k}(P^{1-\theta}) + P^{(t/2)(2-k\theta)} (J_{u,k}(P^{1-\theta}))^{s/u} \right),$$

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

This lemma provides superior bounds for $J_{s,k}(P)$ when s is small (up to about $k^{3/2}$), but the improvements become negligible for large s and would only improve the $O(1)$ term in Corollary 1.1. Using these bounds as a starting point, Lemma 5.1 provides bounds for larger s. Because the bound for $J_{s+t,k}(P)$ arising from Lemma 5.1 depends on a bound of $J_{u,k}(P)$ and usually $u \geqslant s + t$, the best bounds are obtained by iterating these two lemmas. For $k \leqslant 20$, the values of $\eta(s,k)$ obtained this way are 1-2% smaller than those arising from Lemma 5.1 alone. Using these bounds in Lemma 5.1 produces values of $\sigma(k)$ recorded in the next lemma. For $k \leqslant 10$, we take $\sigma(k) = 2^{1-k}$, for $11 \leqslant k \leqslant 13$ we take $\sigma(k) = \sigma_1(k)$ and for $k \geqslant 14$ we take $\sigma(k) = \sigma_2(k)$ (the optimal value of r being $r = 2$ in each case).

Lemma 5.1. *Let $\rho(k) = 1/\sigma(k)$. We have $\rho(11) \leqslant 802.131$, $\rho(12) \leqslant 1005.037$, $\rho(13) \leqslant 1230.216$, $\rho(14) \leqslant 1432.688$, $\rho(15) \leqslant 1646.279$, $\rho(16) \leqslant 1872.185$, $\rho(17) \leqslant 2127.695$, $\rho(18) \leqslant 2450.788$, $\rho(19) \leqslant 2795.532$, $\rho(20) \leqslant 3168.424$.*

As a concluding remark, combining Theorem 1 with an application of the circle method leads to the estimate

$$I_s(P) \sim C(f,s)P^{2s-k} \tag{5.4}$$

for some constant $C(f,s)$, valid for $s \geqslant \frac{1}{2}k^2(\log k + \log\log k + c)$, where c is an absolute constant (see, for example, Lemma 7.12 of [Hu65]). By comparison, using (1.7) with Lemma 5.1, we may only conclude that (5.4) holds for $s \geqslant k^2(\log k + \frac{1}{2}\log\log k + c)$.

References

[Bo] K. D. Boklan, *The asymptotic formula in Waring's problem*, Mathematika **41** (1994), 329–347.

[HB] D. R. Heath-Brown, *Weyl's inequality, Hua's inequality, and Waring's problem*, J. London Math. Soc. (2) **38** (1988), 216–230.

[Hu38] L.-K. Hua, *On Waring's problem*, Quart. J. Math. Oxford **9** (1938), 199–202.

[Hu49] ———, *An improvement in Vinogradov's mean value theorem and several applications*, Quart. J. Math. Oxford **20** (1949), 48–61.

[Hu65] ———, *Additive theory of prime numbers*, Amer. Math. Soc., Providence, RI, 1965.

[Li] Yu. V. Linnik, *On Weyl's sums*, Mat. Sbornik (Rec. Math.) N.S. **12** (1943), 23–39.

[Va81] R. C. Vaughan, *The Hardy-Littlewood method*, University Press, Cambridge, 1981.

[Va86a] ———, *On Waring's problem for cubes*, J. Reine Angew. Math. **365** (1986), 122–170.

[Va86b] ———, *On Waring's problem for smaller exponents. II.*, Mathematika **33** (1986), 6–22.

[Va89] ———, *A new iterative method in Waring's problem*, Acta Math. **162** (1989), 1–71.

[Wo92a] T. D. Wooley, *Large improvements in Waring's problem*, Ann. of Math. **135** (1992), 131–164.

[Wo92b] ———, *On Vinogradov's mean value theorem*, Mathematika **39** (1992), 379–399.

[Wo93a] ———, *The application of a new mean value theorem to the fractional parts of polynomials*, Acta Arith. **65** (1993), 163–179.

[Wo93b] ———, *On Vinogradov's mean value theorem, II*, Michigan Math. J. **40** (1993), 175–180.

[Wo94a] ———, *Quasi-diagonal behavior in certain mean value theorems of additive number theory*, J. Amer. Math. Soc. **7** (1994), 221–245.

[Wo94b] ———, *New estimates for Weyl sums*, Quart. J. Math. Oxford (to appear).

[Wo95] ———, *Note on simultaneous congruences*, (manuscript).

School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540
E-mail address: `ford@math.ias.edu`