3

Weyl's inequality and Hua's inequality

The most important single tool for the investigation of Waring's problem, and indeed many other problems in the analytic theory of numbers, is Weyl's inequality. This was given, in a less explicit form, in Weyl's great memoir [96] of 1916 on the uniform distribution of sequences of numbers to the modulus 1. The explicit form for a polynomial, in terms of a rational approximation to the highest coefficient, was given by Hardy and Littlewood in P.N. I [37].

Lemma 3.1. (Weyl's Inequality) *Let $f(x)$ be a real polynomial of degree k with highest coefficient α:*

$$f(x) = \alpha x^k + \alpha_1 x^{k-1} + \cdots + \alpha_k.$$

Suppose that α has a rational approximation a/q satisfying

$$(a, q) = 1, \quad q > 0, \quad \left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}.$$

Then, for any $\varepsilon > 0$,

$$\left|\sum_{x=1}^{P} e(f(x))\right| \ll P^{1+\varepsilon}\left(P^{-\frac{1}{K}} + q^{-\frac{1}{K}} + \left(\frac{P^k}{q}\right)^{-\frac{1}{K}}\right),$$

where $K = 2^{k-1}$ and the implied constant[1] *depends only on k and ε.*

Note. The inequality gives *some* improvement on the trivial upper bound P provided that $P^\delta \leq q \leq P^{k-\delta}$ for some fixed $\delta > 0$. If $P \leq q \leq P^{k-1}$, we get the estimate $P^{1-1/K+\varepsilon}$, and it is under these

[1] We use the Vinogradov symbol $\ll$ to indicate an inequality with an unspecified 'constant' factor. In the present instance, the factor which arises is in reality independent of k, but we do not need to know this.

conditions that Weyl's inequality is most commonly applied. It is obviously impossible to extract any better estimate than this from it. Note that Weyl's inequality fails to give any useful information if q is small, and this is natural because if $f(x) = \alpha x^k$ and α is very near to a rational number with small denominator, the sum is genuinely of a size which approaches P.

Proof. The basic operation in the proof is that of squaring the absolute value of an exponential sum, and thereby relating the sum to an average of similar sums with polynomials of degree one lower. Let

$$S_k(f) = \sum_{x=P_1+1}^{P_2} e(f(x)),$$

where $0 \leq P_2 - P_1 \leq P$, and where the suffix k serves to indicate the degree of $f(x)$. Then

$$\begin{aligned} |S_k(f)|^2 &= \sum_{x_1}\sum_{x_2} e(f(x_2) - f(x_1)) \\ &= P_2 - P_1 + 2\Re \sum_{\substack{x_1,\, x_2 \\ x_2 > x_1}} e(f(x_2) - f(x_1)). \end{aligned}$$

Put $x_2 = x_1 + y$. Then $1 \leq y < P_2 - P_1$, and

$$f(x_2) - f(x_1) = f(x_1 + y) - f(x_1) = \Delta_y f(x_1),$$

with an obvious notation. Hence

$$|S_k(f)|^2 = P_2 - P_1 + 2\Re \sum_{y=1}^{P}\sum_{x} e\left(\Delta_y f(x)\right),$$

where the summation in x is over an interval depending on y but contained in $P_1 < x \leq P_2$. This interval may, for some values of y, be empty.

In particular,

$$|S_k(f)|^2 \leq P + 2\sum_{y=1}^{P} |S_{k-1}(\Delta_y f)|,$$

where the interval for S_{k-1} is of the nature just described. By repeating the argument we get

$$|S_{k-1}(\Delta_y f)|^2 \leq P + 2\sum_{z=1}^{P} |S_{k-2}\left(\Delta_{y,z} f\right)|,$$

where the interval of summation in S_{k-2} depends on both y and z but is contained in $P_1 < x \leq P_2$. The use of Cauchy's inequality enables us to substitute for S_{k-1} from the second inequality into the first:

$$\begin{aligned} |S_k(f)|^4 &\ll P^2 + P\sum_{y=1}^{P} |S_{k-1}(\Delta_y f)|^2 \\ &\ll P^3 + P\sum_{y=1}^{P}\sum_{z=1}^{P} |S_{k-2}(\Delta_{y,z} f)|. \end{aligned}$$

The process can be continued, and the general inequality established in this way is

$$|S_k(f)|^{2^\nu} \ll P^{2^\nu - 1} + P^{2^\nu - \nu - 1} \sum_{y_1=1}^{P} \cdots \sum_{y_\nu=1}^{P} \left|S_{k-\nu}(\Delta_{y_1,\ldots,y_\nu} f)\right|. \quad (3.1)$$

This is readily proved by induction on ν, using again Cauchy's inequality together with the basic operation described above which expresses $|S_{k-\nu}|^2$ in terms of $S_{k-\nu-1}$. It is to be understood that the range of summation for x in $S_{k-\nu}$ in (3.1) is an interval depending on $y_1, \ldots, y_\nu$, but contained in $P_1 < x \leq P_2$.

At this point we interpolate a remark which will be useful in the proof of Lemma 3.2. This is that if, at the last stage of the proof of (3.1), we apply the basic operation in its original form, we get

$$|S_k(f)|^{2^\nu} \ll P^{2^\nu - 1} + P^{2^\nu - \nu - 1} \sum_{y_1=1}^{P} \cdots \sum_{y_\nu=1}^{P} \Re S_{k-\nu}(\Delta_{y_1,\ldots,y_\nu} f). \quad (3.2)$$

Here again, the range for x in $S_{k-\nu}$ depends on $y_1, \ldots, y_\nu$ and may sometimes be empty.

Returning to (3.1), we take $\nu = k-1$ and in the original S_k we take $P_1 = 0$, $P_2 = P$. We observe that

$$\Delta_{y_1,\ldots,y_{k-1}} f(x) = k!\alpha y_1 \cdots y_{k-1} x + \beta,$$

say, where β is a collection of terms independent of x. Hence

$$\left|S_1(\Delta_{y_1,\ldots,y_{k-1}} f)\right| = \left|\sum_x e(k!\alpha y_1 \cdots y_{k-1} x)\right|.$$

The sum on the right, taken over any interval of x of length at most P, is of the form

$$\left|\sum_{x=x_1}^{x_2-1} e(\lambda x)\right| \le \frac{2}{|1-e(\lambda)|} = \frac{1}{|\sin \pi\lambda|} \ll \frac{1}{\|\lambda\|},$$

where $\|\lambda\|$ denotes the distance of λ from the nearest integer. This fails if λ is an integer, and indeed gives a poor result if λ is very near to an integer, but we can supplement it by the obvious upper bound P. Hence (3.1) gives

$$|S_k(f)|^K \ll P^{K-1} + P^{K-k} \sum_{y_1=1}^{P} \cdots \sum_{y_{k-1}=1}^{P} \min(P, \|k!\alpha y_1 \cdots y_{k-1}\|^{-1}).$$

We now appeal to a result in elementary number theory, which enables us to collect together all the terms in the sum for which $k!y_1 \cdots y_{k-1}$ has a given value, say m. The number of such terms is $\ll m^\varepsilon$. To prove this, it suffices to show that

$$d(m) \ll m^\varepsilon, \tag{3.3}$$

for any integer m, where $d(m) = \sum_{d|m} 1$ is the usual divisor function. Indeed there are at most $d(m)$ possibilities for each of $y_1, \dots, y_{k-1}$. To establish (3.3) we suppose that $m = p_1^{\lambda_1} p_2^{\lambda_2} \cdots$, and note that

$$\frac{d(m)}{m^\varepsilon} = \prod_i \frac{\lambda_i + 1}{p_i^{\varepsilon\lambda_i}} \le \prod_{p_i \le 2^{1/\varepsilon}} \frac{\lambda_i + 1}{2^{\varepsilon\lambda_i}} \le C(\varepsilon),$$

since $2^{-\varepsilon\lambda}(\lambda+1)$ is bounded above for $\lambda > 0$.

Collecting terms as mentioned above, we get

$$|S_k(f)|^K \ll P^{K-1} + P^{K-k+\varepsilon} \sum_{m=1}^{k!P^{k-1}} \min(P, \|\alpha m\|^{-1}).$$

It remains to estimate the last sum in terms of the rational approximation a/q to α which was mentioned in the enunciation. We divide the sum over m into blocks of q consecutive terms (with perhaps one incomplete block), the number of such blocks being

$$\ll \frac{P^{k-1}}{q} + 1.$$

Consider the sum over any one block, which will be of the form

$$\sum_{m=0}^{q-1} \min(P, \|\alpha(m_1 + m)\|^{-1}),$$

where m_1 is the first number in the block. We have

$$\alpha(m_1 + m) = \alpha m_1 + \frac{am}{q} + O\left(\frac{1}{q}\right),$$

since $|\alpha - a/q| \le q^{-2}$ and $0 \le m < q$. As m goes from 0 to $q-1$, the number am runs through the complete set of residues (mod q). Putting $am \equiv r \pmod q$, the sum is

$$\sum_{r=0}^{q-1} \min\left(P, \frac{1}{\|(r+b)/q + O(1/q)\|}\right),$$

where we have taken b to be the integer nearest to $q\alpha m_1$. There are $O(1)$ values of r in the sum for which the second expression in the minimum is useless, namely those for which the absolutely least residue of $r+b$ (mod q) is small. For these, we must take P. For the other values of r, if s denotes the absolutely least residue of $r+b$ (mod q) we have

$$\left\|\frac{r+b}{q} + O\left(\frac{1}{q}\right)\right\| \gg \frac{s}{q}.$$

Hence the above sum is

$$\ll P + \sum_{s=1}^{q/2} \frac{q}{s} \ll P + q\log q.$$

Allowing for the number of blocks, we obtain

$$|S_k(f)|^K \ll P^{K-1} + P^{K-k+\varepsilon}\left(\frac{P^{k-1}}{q} + 1\right)(P + q\log q).$$

We can absorb the factor $\log q$ in P^ε, since we can suppose $q \le P^k$, as otherwise the result of the lemma is trivial. Thus the right-hand side is

$$\ll P^{K+\varepsilon}\left(P^{-1} + q^{-1} + P^{-k}q\right),$$

giving the result. □

Note. If k is large, then Vinogradov has given a much better estimate, in which (roughly speaking) 2^{k-1} is replaced by $4k^2\log k$ [49, Chapter 6].

Corollary (to Lemma 3.1). *Let*

$$S_{a,q} = \sum_{z=1}^{q} e(az^k/q),$$

where a, q are relatively prime integers and $q > 0$. Then

$$S_{a,q} \ll q^{1-1/K+\varepsilon}.$$

This is a special case of Lemma 3.1 with $\alpha = a/q$ and $P = q$. We shall later (Lemma 6.4) prove the more precise estimate $q^{1-1/k}$ instead of $q^{1-1/K+\varepsilon}$, but the above suffices for the time being.

Lemma 3.2. (Hua's Inequality [48]) *If*

$$T(\alpha) = \sum_{x=1}^{P} e(\alpha x^k),$$

then

$$\int_0^1 |T(\alpha)|^{2^k} \, d\alpha \ll P^{2^k-k+\varepsilon}$$

for any fixed $\varepsilon > 0$.

Proof. Write

$$I_\nu = \int_0^1 |T(\alpha)|^{2^\nu} \, d\alpha.$$

We prove, by induction on ν, that

$$I_v \ll P^{2^\nu-\nu+\varepsilon}, \quad \text{for } \nu = 1, \dots, k, \tag{3.4}$$

the case $\nu = k$ being the result asserted in the lemma.

For $\nu = 1$, the estimate is immediate. We have

$$I_1 = \int_0^1 \sum_{x_1} e(\alpha x_1^k) \sum_{x_2} e(-\alpha x_2^k) \, d\alpha = P,$$

since the integral over α is 1 if $x_1 = x_2$ and 0 otherwise.

Now suppose (3.4) holds for a particular integer $\nu \le k-1$; we have to deduce the corresponding result when ν is replaced by $\nu + 1$. We recall the inequality (3.2) of the preceding proof; with $T(\alpha)$ in place of $S_k(f)$ it states that

$$|T(\alpha)|^{2^\nu} \ll P^{2^\nu-1} + P^{2^\nu-\nu-1} \Re \sum_{y_1=1}^{P} \cdots \sum_{y_\nu=1}^{P} S_{k-\nu},$$

where

$$S_{k-\nu} = \sum_x e(\alpha \Delta_{y_1,\dots,y_\nu}(x^k)).$$

Note that the range of summation for x depends on the values of $y_1, \ldots, y_\nu$, but is contained in $[1, P]$.

Multiply both sides of the inequality by $|T(\alpha)|^{2^\nu}$ and integrate from 0 to 1. We get

$$I_{\nu+1} \ll P^{2^\nu - 1} I_\nu + P^{2^\nu - \nu - 1} \sum_{y_1, \ldots, y_\nu} \Re \int_0^1 S_{k-v} |T|^{2^\nu} \, d\alpha.$$

The last integral is

$$\int_0^1 \sum_x e\left(\alpha \Delta_{y_1, \ldots, y_\nu}(x^k)\right) \sum_{\substack{u_1, \ldots, u_{2^\nu - 1} \\ v_1, \ldots, v_{2^\nu - 1}}} e(\alpha u_1^k + \cdots) e(-\alpha v_1^k - \cdots) \, d\alpha,$$

where the u_i and v_i go from 1 to P. This integral equals the number of solutions of

$$\Delta_{y_1, \ldots, y_\nu}(x^k) + u_1^k + \cdots - v_1^k - \cdots = 0. \tag{3.5}$$

Summation over $y_1, \ldots, y_\nu$ gives the number of solutions in all the variables. Hence

$$I_{\nu+1} \ll P^{2^\nu - 1} I_\nu + P^{2^\nu - \nu - 1} N, \tag{3.6}$$

where N denotes the number of solutions of (3.5) in all the variables, these being now any integers in $[1, P]$.

It is important now to observe that since $y_1, \ldots, y_\nu$ and x are positive, we have

$$\Delta_{y_1, \ldots, y_\nu}(x^k) > 0.$$

Also, this number is divisible by each of $y_1, \ldots, y_\nu$. Thus, if we give $u_1, \ldots, u_{2^\nu - 1}$ and $v_1, \ldots, v_{2^\nu - 1}$ any values, the number of possibilities for each of $y_1, \ldots, y_\nu$ is $\ll P^\varepsilon$ by (3.3). Then there is at most one possibility for x, since $\Delta_{y_1, \ldots, y_\nu}(x^k)$ is a strictly increasing function of x (note that $\nu \leq k - 1$). The number of possibilities for the u_i and v_i is $\ll P^{2^\nu}$, whence it follows that

$$N \ll P^{2^\nu + \nu\varepsilon}.$$

Substituting in (3.6) and using the inductive hypothesis, we obtain

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

This is (3.4) with $\nu + 1$ for ν, except for the change in ε which is of no significance. $\square$

Note. It is of interest to examine the information given by Lemma 3.2 when $k = 3$. Let $\lambda(m)$ denote the lower bound of the exponents λ for which it is true that

$$\int_0^1 |T(\alpha)|^{2m}\, d\alpha \ll P^{\lambda}.$$

It follows from Cauchy's inequality that

$$\lambda\left(\frac{m_1+m_2}{2}\right) \le \frac{1}{2}(\lambda(m_1)+\lambda(m_2)),$$

so that the graph of $\lambda(m)$ as a function of m is convex. Lemma 3.2 tells us that

$$\lambda(1) \le 1, \quad \lambda(2) \le 2, \quad \lambda(4) \le 5,$$

and it can be proved that actually there is equality in all these. Thus the graph lies on or below the two line segments joining $(1,1)$, $(2,2)$, $(4,5)$. It seems likely that the graph is strictly below the segment for $2 < m < 4$, but this has never been proved. If it could be proved, one could establish the asymptotic formula for eight cubes instead of for nine cubes ($9 = 2^k + 1$). It would be enough to prove, for example, that

$$\int_0^1 |T(\alpha)|^{6}\, d\alpha \ll P^{7/2-\delta}$$

for some positive δ. This is equivalent to the assertion that the total number of solutions of

$$x_1^3 + x_2^3 + x_3^3 = y_1^3 + y_2^3 + y_3^3,$$

with all the variables between 0 and P, is $\ll P^{7/2-\delta}$.