The maximal large sieve

Dedicated to Professor Yoshie Katsurada on the occasion of her sixtieth anniversary

By Saburô UCHIYAMA

Let M and N be integers with $N>0$ and let $a_{M+1},\cdots,a_{M+N}$ be any real or complex numbers. Define

$$S(t)=\sum_{M<n\leqq M+N} a_n e(nt)$$

with the abbreviation $e(t)=e^{2\pi i t}$ and set

$$Z=\sum_{M<n\leqq M+N}|a_n|^2 .$$

Let $x_1,\cdots,x_R$ $(R\geqq 1)$ be any fixed real numbers which satisfy the condition

$$\|x_u-x_v\|\geqq\delta \qquad \text{when} \quad u\neq v,$$

where $\|x\|$ denotes the absolute distance between x and the nearest integer to it, and $0<\delta\leqq 1/2$.

In a recent paper [1] E. Bombieri and H. Davenport proved that

$$(1)\qquad \sum_{r=1}^{R}|S(x_r)|^2\leqq\begin{cases}(N^{1/2}+\delta^{-1/2})^2 Z\\ 2\max(N,\delta^{-1})Z\end{cases}$$

and essentially the best possible results of the type (1) have also been obtained by them in [2]. On the other hand, P. X. Gallagher [3] has given a very simple and ingenious proof of the inequality

$$(2)\qquad \sum_{r=1}^{R}|S(x_r)|^2\leqq(\pi N+\delta^{-1})Z,$$

which is slightly weaker than, but as powerful as, (1).

Now, our principal objective in this paper is to replace in these inequalities the sum $S(t)$ by the 'maximal function' $S^*(t)$ defined by

$$S^*(t)=\sup_{1\leqq n\leqq N}\Big|\sum_{M<m<M+n} a_m e(mt)\Big| .$$

Indeed, we can show that for $N\geqq 2$

$$(3)\qquad \sum_{r=1}^{R}\big(S^*(x_r)\big)^2\leqq B(N\log N+\delta^{-1}\log^2 N)Z,$$

where, and throughout in what follows, B denotes an unspecified, positive absolute constant.

However, we should like to present our main result in a form slightly more general than (3).

1. Notations.

For the sake of simplicity we shall adopt vector notations of dimension s, s being a fixed positive integer. Thus, if

$$a=(a_1,\cdots,a_s)$$

is an s-dimensional integral vector, i.e. a vector with integer components a_j $(1\leqq j\leqq s)$, we set

$$2^a=(2^{a_1},\cdots,2^{a_s}),$$

and if $b=(b_1,\cdots,b_s)$ is another s-dimensional integral vector, we define

$$ab=(a_1b_1,\cdots,a_sb_s);$$

also, we write

$$a\leqq b \quad \text{or} \quad b\geqq a$$

when

$$a_j\leqq b_j \qquad \text{for} \quad j=1,\cdots,s,$$

and write

$$a<b \quad \text{or} \quad b>a$$

when

$$a_j<b_j \qquad \text{for} \quad j=1,\cdots,s.$$

We shall often identify a scalar a with the vector $(a,\cdots,a)$; in particular,

$$0=(0,\cdots,0), \qquad 1=(1,\cdots,1).$$

Now, let M and N be s-dimensional integral vectors with $N>0$. Let the a_{M+n} $(1\leqq n\leqq N)$ be any real or complex numbers and define

$$S(t)=\sum_{M<n\leqq M+N} a_n e(<n,t>),$$

where $<n,t>$ denotes the inner product of the integral vector $n=(n_1,\cdots,n_s)$ and the vector $t=(t_1,\cdots,t_s)$ with real components t_j $(1\leqq j\leqq s)$, namely

$$\langle n,t\rangle=n_1t_1+\cdots n_st_s.$$

We set as before

$$Z=\sum_{M<n\leqq M+N}|a_n|^2.$$

Let

$$x_r=(x_{r,1},\cdots,x_{r,s}) \qquad (r=1,\cdots,R)$$

be any fixed R vectors with real components $x_{r,j}$ $(1\leqq j\leqq s)$ such that

$$\|x_{u,j}-x_{v,j}\|\geqq\delta_j \qquad \text{when} \quad u\neq v\ (1\leqq j\leqq s),$$

where $0<\delta_j\leqq 1/2$ $(1\leqq j\leqq s)$; we put

$$\delta=(\delta_1,\cdots,\delta_s)$$

and write

$$\delta^{-1}=(\delta_1^{-1},\cdots,\delta_s^{-1}).$$

2. A theorem of E. Hlawka.

For any two s-dimensional vectors

$$\xi=(\xi_1,\cdots,\xi_s) \quad \text{and} \quad \eta=(\eta_1,\cdots,\eta_s)$$

with real components, we set

$$C_s(\xi,\eta)=\prod_{j=1}^{s}(\xi_j+\eta_j).$$

In his very interesting paper [4] E. Hlawka proved substantially the following result.

THEOREM 1. *Under the notations and conditions described above we have*

$$\sum_{r=1}^{R}|S(x_r)|^2\leqq C_s(\pi N,\delta^{-1})Z.$$

This is just an s-dimensional version of the inequality (2) of Gallagher's; we note that similar generalizations have also been given by several writers.

3. The main theorem.

We are now going to replace the sum $S(t)$ in Theorem 1 by the 'maximal function' $S^*(t)$ defined by

$$S^*(t)=\sup_{1\leqq n\leqq N}\Big|\sum_{M<m\leqq M+n}a_m e(\langle m,t\rangle)\Big|.$$

We shall prove the following

THEOREM 2. *Let N and L be s-dimensional integral vectors such that*

$$N \geqq 2 \quad \textit{and} \quad 2^{L-1} < N \leqq 2^L .$$

Then we have

$$\sum_{r=1}^{R} \left(S^*(x_r)\right)^2 \leqq C_s(L, 1)\, C_s\left(\pi 2^{L+1}, (L+1)\delta^{-1}\right) Z .$$

It is clear that for $s=1$ our Theorem 2 reduces to an inequality of the from (3).

In order to prove Theorem 2 we set

$$a_m = 0 \qquad \text{for} \quad M+N < m \leqq M+2^L$$

and put for s-dimensional integral vectors k, l with $1 \leqq k \leqq 2^l$, $0 \leqq l \leqq L$,

$$S_{k,l}(t) = \sum_{M+(k-1)2^{L-l} < m \leqq M+k2^{L-l}} a_m e(\langle m, t \rangle) .$$

If we write

$$S^*(t) = \sup_{1 \leqq k \leqq 2^l} |S_{k,l}(t)| ,$$

then we easily find that

$$S^*(t) \leqq \sum_{0 \leqq l \leqq L} S_l^*(t) ,$$

on taking account of the dyadic development of each component of an integral vector n, $1 \leqq n \leqq N$. Therefore, Cauchy's inequality gives

$$\left(S^*(t)\right)^2 \leqq C_s(L, 1) \sum_{0 \leqq l \leqq L} \left(S_l^*(t)\right)^2$$

and so

$$\sum_{r=1}^{R} \left(S^*(x_r)\right)^2 \leqq C_s(L, 1) \sum_{0 \leqq l \leqq L} \sum_{r=1}^{R} \left(S_l^*(x_r)\right)^2 ,$$

where

$$\begin{aligned} \sum_{r=1}^{R} \left(S_l^*(x_r)\right)^2 &\leqq \sum_{1 \leqq k \leqq 2^l} \sum_{r=1}^{R} |S_{k,l}(x_r)|^2 \\ &\leqq \sum_{1 \leqq k \leqq 2^l} C_s(\pi 2^{L-l}, \delta^{-1}) \sum_{M+(k-1)2^{L-l} < m \leqq M+k2^{L-l}} |a_m|^2 \\ &= C_s(\pi 2^{L-l}, \delta^{-1}) \sum_{M < m \leqq M+N} |a_m|^2 \end{aligned}$$

by Theorem 1. Hence we obtain the result in Theorem 2, on noticing that

$$\sum_{0 \leqq l \leqq L} C_s(\pi 2^{L-l}, \delta^{-1}) = C_s\left(\pi(2^{L+1}-1),\ (L+1)\delta^{-1}\right) .$$

This completes the proof of Theorem 2.

4. An application.

In this and the next sections we shall restrict ourselves to the simplest case of $s=1$. Thus, as before, we define

$$S(t)=\sum_{M<n\leqq M+N} a_n e(nt)$$

and set

$$Z=\sum_{M<n\leqq M+N} |a_n|^2,$$

where M and N are integers with $N>0$ and the a_n are any complex numbers; also, we put

$$S^*(t)=\sup_{1\leqq n\leqq N} |S_n(t)|$$

with

$$S_n(t)=\sum_{M<m\leqq M+n} a_m e(mt).$$

We shall assume throughout that $N\geqq 2$.

If

$$0<x_1<x_2<\cdots<x_R=1$$

are the Farey fractions of order Q, $Q\geqq 1$, then

$$R=\frac{3}{\pi^2}Q^2+O(Q\log 2Q)$$

and we may take

$$\delta=\min\left(\frac{1}{2}, \frac{1}{Q^2}\right).$$

It follows from (3) that

$$\sum_{q\leqq Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}\left(S^*\left(\frac{a}{q}\right)\right)^2\leqq B(N\log N+Q^2\log^2 N)Z. \tag{4}$$

If we write for integers $1\leqq n\leqq N$, $q\geqq 1$ and h

$$Z_n(q,h)=\sum_{\substack{M<m\leqq M+n\\ m\equiv h \,(\mathrm{mod}\, q)}} a_m, \tag{5}$$

then we have (cf. [5])

$$\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S_n\left(\frac{a}{q}\right)\right|^2=q\sum_{h=1}^{q}\left|\sum_{d\mid q}\frac{\mu(d)}{d}Z_n\left(\frac{q}{d},h\right)\right|^2,$$

where $\mu(d)$ is the Möbius function.

We define

$$W(q, h)=\sup_{1\leqq n\leqq N}\left|\sum_{d\mid q}\frac{\mu(d)}{d}Z_n\left(\frac{q}{d}, h\right)\right|.$$

The following theorem can be proved by the method employed in the previous section to establish Theorem 2, though the result obtained is not a direct consequence of the inequality (4).

THEOREM 3. *We have*

$$\sum_{q\leqq Q} q\sum_{h=1}^{q}\left(W(q, \mathrm{h})\right)^2\leqq B(N\log N+Q^2\log^2 N)Z.$$

Let L be the positive integer for which

$$2^{L-1}<N\leqq 2^L.$$

Setting

$$a_m=0 \qquad \text{for} \quad M+N<m\leqq +2^L,$$

we define $Z_n(q, h)$ by (5) for integers $1\leqq n\leqq 2^L$, $q\geqq 1$ and h. Put, further, for integers k, l with $1\leqq k\leqq 2^l$, $0\leqq l\leqq L$,

$$Z_{k,l}(q, h)=\sum_{\substack{m=M+(k-1)2^{L-l}+1\\ m\equiv h \pmod q}}^{M+k2^{L-l}} a_m,$$

and write

$$W_l(q, h)=\sup_{1\leqq k\leqq 2^l}\left|\sum_{d\mid q}\frac{\mu(d)}{d}Z_{k,l}\left(\frac{q}{d}, h\right)\right|.$$

Then we have

$$W(q, h)\leqq\sum_{l=0}^{L}W_l(q, h)$$

so that

$$\left(W(q, h)\right)^2\leqq(L+1)\sum_{l=0}^{L}\left(W_l(q, h)\right)^2.$$

It follows from this that

$$\sum_{q\leqq Q} q\sum_{h=1}^{q}\left(W(q, h)\right)^2\leqq(L+1)\sum_{l=0}^{L}\sum_{q\leqq Q} q\sum_{h=1}^{q}\left(W_l(q, h)\right)^2,$$

where

$$\sum_q q \sum_h \left(W_l(q,h)\right)^2 \leqq \sum_{k=1}^{2^l} \sum_q q \sum_h \left| \sum_{d|q} \frac{\mu(d)}{d} Z_{k,l}\left(\frac{q}{d}, h\right)\right|^2$$
$$= \sum_{k=1}^{2^l} \sum_q \sum_{(a,q)=1} \left| S_{k,l}\left(\frac{a}{q}\right)\right|^2$$

with

$$S_{k,l}(t) = \sum_{m=M+(k-1)2^{L-l}+1}^{M+k2^{L-l}} a_m e(mt).$$

Hence we obtain

$$\sum_q q \sum_h \left(W_l(q,h)\right)^2 \leqq \sum_{k=1}^{2^l} (\pi 2^{L-l} + Q^2) \sum_{m=M+(k-1)2^{L-l}+1}^{M+k2^{L-l}} |a_m|^2$$
$$= (\pi 2^{L-l} + Q^2) Z$$

by (2), and so

$$\sum_{q \leqq Q} q \sum_{h=1}^{q} \left(W(q,h)\right)^2 \leqq (L+1)\left(\pi 2^{L+1} + (L+1)Q^2\right) Z.$$

This proves Theorem 3, since

$$L+1 < \frac{3}{\log 2} \log N \qquad \text{for} \quad N \geqq 2.$$

5. A Final remark.

Again, let M and N be integers with $N>0$ and let $a_{M+1}, \cdots, a_{M+N}$ be any complex numbers. Put for each residue character $\chi \pmod{q}$, $q \geqq 1$,

$$S(\chi) = \sum_{M<n\leqq M+N} a_n \chi(n)$$

and define

$$S^*(\chi) = \sup_{1\leqq n \leqq N} \Big| \sum_{M<m\leqq M+n} a_m \chi(m) \Big|.$$

Using the inequality (cf. [3; (5)])

$$\frac{1}{\phi(q)} \sum_{\chi \,(\mathrm{mod}\, q)} |S(\chi)|^2 \leqq \frac{1}{q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left| S\left(\frac{a}{q}\right)\right|^2$$

where $\phi(q)$ is the Euler totient function and $\sum_\chi$ indicates that the sum is taken over primitive characters χ only, we can deduce from (2) that with a positive absolute constant B

$$\sum_{q\leqq Q} \frac{q}{\phi(q)} \sum_{\chi\,(\mathrm{mod}\, q)} \left(S^*(\chi)\right)^2 \leqq B(N \log N + Q^2 \log^2 N) Z, \tag{6}$$

provided $N\geqq 2$.

We write as usual

$$\psi(x, q, a)=\sum_{\substack{n\leqq x \\ n\equiv a \pmod q}} \Lambda(n),$$

where $\Lambda(n)=\log p$ if n is a power of the prime p and $=0$ otherwise. An immediate consequence of (6) is that for all real $x>1$ and any fixed $A>0$ we have

$$\sum_{q\leqq x(\log x)^{-A}} \sup_{y\leqq x} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\psi(y, q, a)-\frac{y}{\phi(q)}\right)^2 \leqq B_A \frac{x^2}{(\log x)^{A-3}},$$

$B_A>0$ being a constant depending at most on A. However, our method used in the proof of (3), combined with the method of Gallagher [3], will furnish a slightly stronger result than this inequality, namely

$$(7) \qquad \sum_{q\leqq x(\log x)^{-A}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sup_{y\leqq x} \left(\psi(y, q, a)-\frac{y}{\phi(q)}\right)^2 \leqq B_A \frac{x^2}{(\log x)^{A-3}}.$$

This last inequality may have a consequence on the magnitude in the mean of the least prime number in an arithmetic progression of integers. Thus, if we denote by $p(q, a)$ the least prime $p\equiv a \pmod q$, $(a, q)=1$, then it follows from (7) that

$$(8) \qquad \sum_{q\leqq x(\log x)^{-A}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left(\frac{\min(p(q, a), x)}{\phi(q)}\right)^2 \leqq B_A \frac{x^2}{(\log x)^{A-3}}$$

for any $A>0$ and some $B_A>0$.

Assume now that $A>3$. Let b be any fixed number satisfying $0<b<1$. It then follows from (8) that the number of positive integers $q\leqq x(\log x)^{-A}$ such that one has

$$p(q, a)\geqq x$$

for more than $b\phi(q)$ incongruent values of $a \pmod q$ with $(a, q)=1$, does not exceed

$$\frac{B_A}{b}\frac{x}{(\log x)^{2A-3}}=o\left(\frac{x}{(\log x)^A}\right) \qquad (x\to\infty).$$

(The exponent $2A-3$ of $\log x$ could be improved to $2A-1$ in the denominator on the left side of this inequality, if use were made of [3; Theorem 3] instead of (8); however, the present result will suffice for our purposes). Hence, if we possibly remove all such integers q from the interval

$$(9) \qquad \frac{x}{(\log x)^{A+\epsilon}}<q\leqq\frac{x}{(\log x)^A},$$

ε being an arbitrary but fixed real number with $0<\varepsilon<(A-3)/2$, then the number of remaining integers q in (9) for which

$$p(q,a)\geqq\phi(q)(\log q)^A$$

holds for more than $(1-b)c\phi(q)$ incongruent a's (mod q) with $(a,q)=1$, where c is any number satisfying $0<c<1$, is not greater than

$$\frac{B_A}{(1-b)c}\frac{x}{(\log x)^{2A-3-2\varepsilon}}=o\left(\frac{x}{(\log x)^A}\right)\qquad(x\to\infty)$$

by (8) again.

Therefore, for all but possibly $o(x(\log x)^{-A})$ positive integers $q\leqq x(\log x)^{-A}$ one must have

$$p(q,a)<\phi(q)(\log q)^A$$

for at least $(1-b)(1-c)\phi(q)$ incongruent a's (mod q) with $(a,q)=1$. Rewriting c for $(1-b)(1-c)$, we thus have proved the following

THEOREM 4. *Let A be an arbitrary real number greater than* 3 *and c be any number with* $0<c<1$. *Then, for almost all positive integers q we have*

$$p(q,a)<\phi(q)(\log q)^A$$

for at least $c\phi(q)$ incongruent values of a (mod q) *with* $(a,q)=1$.

Here, 'almost all' means 'all but possibly a set of density zero'.

We note that a celebrated theorem due to Ju. V. Linnik states that there exists an absolute constant $C>0$ such that

$$p(q,a)<q^C$$

holds true for all $q>1$ and all a with $(a,q)=1$ (cf. e.g. [6; Chap. X]).

NOTE. The results of the present paper have been announced partly in the Seminar on Modern Methods in Number Theory, August 30–September 4, 1971, held at the Institute of Statistical Mathematics, Tokyo.

Department of Mathematics,
Okayama University

References

[1] E. BOMBIERI and H. DAVENPORT: On the large sieve method. Number Theory and Analysis (Edited by P. Turán), Plenum Press, New York, and VEB Deutscher Verl. der Wiss., Berlin (1969), 11–22.

[2] E. BOMBIERI and H. DAVENPORT: Some inequalities involving trigonometrical polynomials. Ann. Scuola Norm. Sup. Pisa, Ser. III, 23 (1969), 223–241.

[3] P. X. Gallagher: The large sieve. Mathematika, 14 (1967), 14–20.
[4] E. HLAWKA: Bemerkungen zum grossen Sieb von Linnik. Österreich. Akad. Wiss. Math.-Natur. Kl. S.-B. II 178 (1970), 13–18.
[5] H. L. MONTGOMERY: A note on the lage sieve. J. London Math. Soc., 43 (1968), 93–98.
[6] K. PRACHAR: Primzahlverteilung. Springer-Verl., Berlin-Göttingen-Heidelberg. (1957).

(Received December 2, 1971)