JOURNAL OF NUMBER THEORY 5, 16–23 (1973)

Hermitian Forms and the Large and Small Sieves

K. R. MATTHEWS

Department of Mathematics, University of Queensland, St. Lucia, Brisbane, Queensland, Q. 4067, Australia

Communicated by H. Halberstam

Received January 17, 1971; revised November 7, 1971

The author observes that two Hermitian forms have the same largest eigenvalue. A large sieve result of Roth–Bombieri type and Selberg's upper bound sieve with a Montgomery type error term are derived.

1. INTRODUCTION

Let

$$S(x) = \sum_{n=M+1}^{M+N} a_n e(nx) \quad (e(\Theta) = e^{2\pi i\Theta}),$$

where $a_{M+1}, \ldots, a_{M+N}$ are arbitrary complex numbers. Let $x_1, x_2, \ldots, x_R$ $(R \geqslant 2)$ be any real numbers satisfying

$$\| x_r - x_s \| \geqslant \delta > 0 \qquad \text{for} \quad r \neq s,$$

where $\| \Theta \|$ is the distance from Θ to the nearest integer.

Montgomery [1, Corollary] gave an upper bound large sieve estimate which depended on the following inequality of Bombieri and Davenport:

$$\sum_{r=1}^{R} | S(x_r)|^2 \leqslant \kappa(N, \delta^{-1}) \sum_{n=M=1}^{M+N} | a_n |^2,$$

where $\kappa(N, \delta^{-1})$ may equal $(N^{1/2} + \delta^{-1/2})^2$ or $N + C\delta^{-1}$ (see [2–5, 7]). In the present paper we study the sum $T(n)$ defined by

$$T(n) = \sum_{r=1}^{R} b_r e(nx_r),$$

where $b_1, b_2, \ldots, b_R$ are arbitrary complex numbers. (In the following,

variables r and s range over 1,..., R and variables m and n range over $M+1,\ldots, M+N$).

Starting with the inequality,

$$\sum_n |\, T(n)|^2 \leqslant \kappa(N, \delta^{-1}) \sum_r |\, b_r\,|^2$$

(Theorem (1)(i)), we shall derive Theorem 2(i), which leads almost immediately to Selberg's upper bound sieve estimate with a Montgomery error term (Section 5).

2.

We note that $\sum_r |\, S(x_r)|^2$ and $\sum_n |\, T(n)|^2$ are positive semidefinite Hermitian forms:

$$\sum_r |\, S(x_r)|^2 = \sum_m \sum_n a_m \bar{a}_n c_{mn}\,, \qquad \sum_n |\, T(n)|^2 = \sum_r \sum_s \bar{b}_r b_s a_{rs}\,,$$

where

$$c_{mn} = \sum_r e((m-n)\,x_r) \text{ and } a_{rs} = \sum_n e(n(x_s - x_r)).$$

If P is the $N \times R$ matrix defined by

$$P = [p_{jr}] = [e(jx_r)], \qquad j = 1,\ldots, N, \qquad r = 1,\ldots, R,$$

the coefficient matrix of the form $\sum_r |\, S(x_r)|^2$ is the $N \times N$ matrix $PP^* = C = [c_{jk}]$. The coefficient matrix of $\sum_n |\, T(n)|^2$ is the $R \times R$ matrix $P^*P = A = [a_{rs}]$. (P^* denotes the complex-conjugate transpose of P.)

LEMMA. *Let $\lambda_1 \leqslant \cdots \leqslant \lambda_N$ be the eigenvalues of C and $\mu_1 \leqslant \cdots \leqslant \mu_R$ be the eigenvalues of A. Then*

(i) *The nonzero eigenvalues of C and A are identical and*

(ii) *For $r = 1, 2,\ldots, R$ we have*

$$|\, \mu_r - N\,| < K\delta^{-1},$$

where K is an absolute constant.

(See Matthews [4, Lemma 3; 5], where it is shown that K may be taken to be 4.3.)

THEOREM 1. *We have*

(i) $\sum_n | T(n)|^2 \leqslant \kappa(N, \delta^{-1}) \sum_r | b_r |^2$,

(ii) $\sum_n | T(n)|^2 = (N + O(\delta^{-1})) \sum_r | b_r |^2$.

Proof. A unitary transformation,

$$b_r = \sum_s \gamma_{rs} d_s ,$$

exists such that

$$\sum_n | T(n)|^2 = \sum_r \mu_r | d_r |^2.$$

From part (i) of the lemma, we have

$$\mu_r \leqslant \mu_R = \lambda_N ,$$

and it is easy to see that $\kappa(N, \delta^{-1})$ must satisfy

$$\lambda_N \leqslant \kappa(N, \delta^{-1}).$$

Hence,

$$\sum_n | T(n)|^2 \leqslant \kappa(N, \delta^{-1}) \sum_r | d_r |^2 = \kappa(N, \delta^{-1}) \sum_n | b_r |^2.$$

To prove (ii) we write $\mu_r = N + \nu_r$ where by part (ii) of the lemma we have

$$| \nu_r | < K\delta^{-1}.$$

Then

$$\begin{aligned} \sum_n | T(n)|^2 &= N \sum_r | d_r |^2 + \sum_r \nu_r | d_r |^2 \\ &= (N + O(\delta^{-1})) \sum_r | d_r |^2 \\ &= (N + O(\delta^{-1})) \sum_r | b_r |^2. \end{aligned}$$

3.

Let k be a positive integer and let $F(X, k)$ denote the set of numbers of the form $\alpha = a/q$, where $1 \leqslant a \leqslant q \leqslant X$, $(a, q) = 1$ and $(q, k) = 1$. ($F(X, 1)$ is the set of Farey fractions of order X.) Also let N' be the number of integers n lying in a given arithmetic progression $n \equiv l \pmod{k}$ and

satisfying $M + 1 \leqslant n \leqslant M + N$. Then $N' = N$ if $k = 1$, $N' = Nk^{-1} + \Theta$, $|\Theta| \leqslant 1$, if $k > 1$, and we have the following corollary.

COROLLARY 1. *Let $f(\alpha)$ be an arbitrary complex-valued function defined on $F(X, k)$. Then*

$$\text{(i)} \quad \sum_{\substack{n \\ n \equiv l (\mathrm{mod}\ k)}} \left| \sum_{\alpha \in F(X,k)} f(\alpha)\, e(n\alpha) \right|^2 \leqslant \kappa(N', X^2) \sum_{\alpha \in F(X,k)} |f(\alpha)|^2,$$

$$\text{(ii)} \quad \sum_{\substack{n \\ n \equiv l (\mathrm{mod}\ k)}} \left| \sum_{\alpha \in F(X,k)} f(\alpha)\, e(n\alpha) \right|^2 = (N' + O(X^2)) \sum_{\alpha \in F(X,k)} |f(\alpha)|^2.$$

Proof. The sum on the left of these inequalities may be written as

$$\sum_{n'=M'+1}^{M'+N'} \left| \sum_{\alpha \in F(X,k)} g(\alpha)\, e(n'k\alpha) \right|^2,$$

where $g(\alpha) = e(\alpha l) f(\alpha)$. Also it is not difficult to verify that the numbers $k\alpha$, $\alpha \in F(X, k)$ satisfy

$$\| k\alpha_1 - k\alpha_2 \| \geqslant X^{-2},$$

if $\alpha_1 \neq \alpha_2$, Theorem 1 may now be applied with $x_1, \ldots, x_R$ replaced by the numbers $k\alpha$, and $\delta = X^{-2}$.

4.

THEOREM 2. *For each prime $p \leqslant X$, let $H(p)$ be a set of $\omega(p)$ distinct residues* mod p. *Let $g(q)$ be an arbitrary complex-valued function of q and define $\Omega(p, n)$ by*

$$\Omega(p, n) = \sum_{t_p} c_p(n - t_p),$$

where t_p runs over $H(p)$, and $c_q(m)$ is Ramanujan's function:

$$c_q(m) = \sum_{a \bmod q}^{*} e\left(\frac{am}{q}\right),$$

where the asterisk indicates a summation over a reduced set mod q. *Then if σ and τ are defined by*

$$\sigma = \sum_{n} \left| \sum_{q \leqslant X} \mu(q)\, g(q) \prod_{p \mid q} \Omega(p, n) \right|^2$$

and

$$\tau = \sum_{q \leqslant X} \mu^2(q) |g(q)|^2 \prod_{p \mid q} (p - \omega(p))\, \omega(p),$$

we have

(i) $\sigma \leqslant \kappa(N, X^2)\tau$,

(ii) $\sigma = (N + O(X^2))\tau$.

Proof. By the Chinese remainder theorem we can define $H(q)$ for all $q \leqslant X$ inductively:

We let $\omega(1) = 1$ and suppose $q = uv$, $(u, v) = 1$, where $H(u)$ and $H(v)$ are already defined. Then if integers m_u and m_v are defined by the congruences

$$vm_u \equiv 1 \pmod{u}, \qquad um_v \equiv 1 \pmod{v},$$

the elements t_q of $H(q)$ are given by

$$t_q = vm_u t_u + um_v t_v,$$

where t_u and t_v run independently over $H(u)$ and $H(v)$, respectively. We see that $\omega(q) = \omega(u)\,\omega(v)$; also

$$t_q \equiv t_u \pmod{u} \qquad \text{and} \qquad t_q \equiv t_v \pmod{v}.$$

If $\alpha = a/q$, $1 \leqslant a \leqslant q \leqslant X$, $(a, q) = 1$, we define $f(\alpha)$ by

$$f(\alpha) = \mu(q)\, g(q) \sum_{t_q} e(-\alpha t_q),$$

and apply Corollary 1.

We have

$$\sum_{\alpha \in F(X,1)} f(\alpha)\, e(n\alpha) = \sum_{q \leqslant X} \mu(q)\, g(q) \sideset{}{^*}\sum_{a \bmod q} e\left(\frac{na}{q}\right) \sum_{t_q} e\left(-\frac{a}{q} t_q\right)$$

$$= \sum_{q \leqslant X} \mu(q)\, g(q)\, \Omega(q, n),$$

where

$$\Omega(q, n) = \sum_{t_q} c_q(n - t_q).$$

Also

$$\sum_{\alpha \in F(X,1)} |f(\alpha)|^2 = \sum_{q \leqslant X} \mu^2(q) |g(q)|^2 A(q),$$

where

$$A(q) = \sideset{}{^*}\sum_{a \bmod q} \left| \sum_{t_q} e\left(-\frac{a}{q} t_q\right)\right|^2.$$

The proof of Theorem 2 is completed by demonstrating that $\Omega(q, n)$ and $A(q)$ are multiplicative functions of q. For then

$$\Omega(q, n) = \prod_{p|q} \Omega(p, n) \text{ and } A(q) = \prod_{p|q} A(p).$$

Moreover,

$$A(p) = \sum_{a=1}^{p-1} \left| \sum_{t_p} e\left(-\frac{a}{q} t_p\right)\right|^2$$

$$= \sum_{a=1}^{p-1} \sum_{t_p} \sum_{T_p} e\left(\frac{a}{p}(T_p - t_p)\right)$$

$$= \sum_{t_p} \sum_{T_p} c_p(T_p - t_p) = (p - \omega(p))\,\omega(p),$$

where we have used the results

$$c_p(t) = \begin{cases} p-1 & \text{if } t \equiv 0 (\text{mod } p), \\ -1 & \text{if } t \not\equiv 0 (\text{mod } p). \end{cases}$$

Hence,

$$A(q) = \prod_{p|q} (p - \omega(p))\,\omega(p).$$

To prove the multiplicative property of $\Omega(q, n)$, let $q = uv$, $(u, v) = 1$. Then

$$\Omega(q, n) = \sum_{t_q} c_q(n - t_q)$$

$$= \sum_{t_q} c_u(n - t_q)\, c_v(n - t_q)$$

$$= \sum_{t_u} \sum_{t_v} c_u(n - t_q)\, c_v(n - t_q),$$

where

$$t_q = vm_u t_u + um_v t_v,$$

as defined earlier.

But

$$c_u(n - t_q) = c_u(n - t_u) \quad \text{and} \quad c_v(n - t_q) = c_v(n - t_v).$$

Consequently,

$$\Omega(q, n) = \sum_{t_u} \sum_{t_v} c_u(n - t_u)\, c_v(n - t_v)$$

$$= \Omega(u, n)\, \Omega(v, n).$$

The proof for $A(q)$ is similar, noting the identity

$$A(q) = \sum_{t_q} \Omega(q, t_q).$$

5. An Upper Estimate for Selberg's Quadratic Form

The form under consideration is

$$\sum_{n} \Big(\sum_{\substack{d \leqslant X \\ n \in H(d)}} \lambda(d) \Big)^2. \tag{1}$$

Here

$$\lambda(d) = \mu(d)\, \tau^{-1} \prod_{p \mid d} \Big(1 - \frac{1}{f(p)}\Big)^{-1} \sum_{\substack{q \leqslant X/d \\ (q,d)=1}} \frac{\mu^2(q)}{f_1(q)},$$

where

$$f(d) = d/\omega(d), \qquad f_1(d) = f(d) \prod_{p \mid d} \Big(1 - \frac{1}{f(p)}\Big)$$

and

$$\tau = \sum_{q \leqslant X} \mu^2(q) \prod_{p \mid q} \frac{\omega(p)}{p - \omega(p)}.$$

See Prachar [6, Satz 3.1, p. 38].

Taking $g(p) = (p - \omega(p))^{-1}$ in inequality (i) of Theorem 2, we obtain

$$\sum_{n} \Big(\sum_{q \leqslant X} \mu(q) \prod_{p \mid q} \frac{\Omega(p, n)}{p - \omega(p)} \Big)^2 \leqslant \kappa(N, X^2)\, \tau, \tag{2}$$

where

$$\Omega(p, n) = \sum_{t_p} c_p(n - t_p).$$

It is now a straightforward exercise to verify the following identity:

$$\sum_{q \leqslant X} \mu(q) \prod_{p \mid q} \frac{\Omega(p, n)}{p - \omega(p)} = \tau \sum_{\substack{d \leqslant X \\ n \in H(d)}} \lambda(d). \tag{3}$$

Inequalities (2) and (3) then give the following upper estimate for the quadratic form (1):

$$\sum_{n} \Big(\sum_{\substack{d \leqslant X \\ n \in H(d)}} \lambda(d) \Big)^2 \leqslant \tau^{-1} \kappa(N, X^2).$$

ACKNOWLEDGMENT

In conclusion, the author wishes to express his great indebtedness to Dr. Martin Huxley for pointing out the significance of (3). The author also wishes to thank Professor C. S. Davis and Dr. B. D. Jones for their encouragement and advice.

REFERENCES

1. H. L. MONTGOMERY, A note on the large sieve, *J. London Math. Soc.* **43** (1968), 93–98.
2. E. BOMBIERI AND H. DAVENPORT, On the large sieve method, *Abhandlungen aus Zahlentheorie und Analysis zur Erinnerung an Edmund Landau*, VEB Deutscher Verlag der Wissenschaften, Berlin (1968), 11–22.
3. E. BOMBIERI AND H. DAVENPORT, Some inequalities involving trigonometric polynomials, *Ann. Scuola norm. sup. Pisa, Sci. fis. mat.*, Ser. III, **23** (1969), 223–241.
4. K. R. MATTHEWS, On an inequality of Davenport and Halberstam, *J. London Math. Soc.* **4** (1972), 638–642.
5. K. R. MATTHEWS, On a bilinear form associated with the large sieve, *J. London Math. Soc.* **5** (1972), 568–570.
6. K. PRACHAR, "Primzahlverteilung," Springer, Berlin, 1957.
7. E. BOMBIERI, A note on the large sieve, *Acta Arith.* **XVIII** (1971), 401–404.