ACTA ARITHMETICA
C.4 (2001)

Averages of short exponential sums, II

by

Alexandru Zaharescu (Bucureşti and Urbana, IL)

1. Introduction. Exponential sums have proved to be very useful in many problems in number theory. The most powerful results obtained so far in this area are concerned with exponential sums in finite fields. There are many important results on this topic in the literature (see Weil [9], Bombieri [2], [3], Deligne [4], [5], Serre [8], Katz [6]). The theory works fine for complete exponential sums. By a standard procedure of expressing an incomplete exponential sum in terms of complete ones, it also works for incomplete sums. However, the quality of such results depends on the size of the range of summation of the given incomplete exponential sum, and it is getting worse when this size is small.

A technique devised to estimate certain averages of short exponential sums is presented in [10]. To be precise, let $\varepsilon > 0$, let $N \le M \le P$ be positive integers and let $r(X) = f(X)/g(X)$ be a rational function which is not a polynomial, with integer coefficients bounded by P^{K_1} and with $\deg f, \deg g < K_2$, where K_1 and K_2 are some positive constants. Then for almost all pairs (p, m) with p prime, $p \in [P, 2P]$ and $m \in \{1, \dots, M\}$ one has

$$\Big| \sideset{}{^*}\sum_{1 \le n \le N} e\Big(\frac{mr(n)}{p}\Big) \Big| \ll_{\varepsilon, K_1, K_2} N^{1/2} P^{\varepsilon}. \tag{1.1}$$

Here and in what follows "almost all" means that the exceptional set has density $< P^{-\varepsilon}$, $r(n)$ is computed modulo p and $\sum^*$ denotes a sum over values of n for which $g(n)$ is nonzero modulo p. The above result was obtained via the following second moment estimate. Under the same assumptions one has

$$\sum_{P \le p \le 2P} \sum_{1 \le m \le M} \Big| \sideset{}{^*}\sum_{1 \le n \le N} e\Big(\frac{mr(n)}{p}\Big) \Big|^2 \ll_{\varepsilon, K_1, K_2} NMP^{1+\varepsilon}. \tag{1.2}$$

2000 *Mathematics Subject Classification*: 11L07, 11L05, 11T23.

In order to prove (1.2) one brings into play the pair correlation of the sets

$$\mathcal{N}_p = \left\{ \frac{r(n) \pmod p}{p} : 1 \le n \le N \right\}$$

and use them to provide upper bounds for the short moments:

$$M_2(N, M, r, p) = \sum_{1 \le m \le M} \left| \sideset{}{^*}\sum_{1 \le n \le N} e\Big(\frac{mr(n)}{p}\Big) \right|^2$$

for each p individually. Next, an alternative way of estimating the pair correlations is introduced, which produces the required amount of cancellation in these pair correlations when p varies in the interval $[P, 2P]$. Thus the point was to average the correlations rather than the exponential sums.

In this paper we present a generalization of the above results to rational functions of several variables $r(X_1, \dots, X_k)$. Here the new feature is the appearance of an obstruction caused by a certain Diophantine equation, the size of the set of solutions of which controls the size of our exponential sums. Quite interestingly, this is a Diophantine equation over $\mathbb{Z}$ as is the case with our original rational function $r(X_1, \dots, X_k)$, although the exponential sums under consideration are defined modulo p, with p varying in an interval $[P, 2P]$. More precisely, given a rational function $r(X_1, \dots, X_k) \in \mathbb{Q}(X_1, \dots, X_k)$ we consider, in the affine space $\mathbb{A}^{2k+1}$, the hypersurface H_r which consists of points $(x_1, \dots, x_k, y_1, \dots, y_k, z)$ satisfying the equation

$$z = r(x_1, \dots, x_k) - r(y_1, \dots, y_k). \tag{1.3}$$

We call H_r the *pair correlation hypersurface* associated to r. For any k-tuple $(N_1, \dots, N_k)$ of positive integers define

$$\mathcal{A}(r, N_1, \dots, N_k) = \{(x_1, \dots, x_k, y_1, \dots, y_k, z) \in \mathbb{Z}^{2k+1} \cap H_r : 1 \le x_j, y_j \le N_j, 1 \le j \le k\}.$$

Note that (1.3) has "diagonal solutions" $z = 0, x_1 = y_1, \dots, x_k = y_k$, therefore $\mathcal{A}(r, N_1, \dots, N_k)$ has at least $N_1 \dots N_k$ elements. Under the assumption that the number of integer solutions to (1.3) is not much larger than the number of diagonal solutions we obtain a generalization of (1.2) which again produces square root cancellation on average in the corresponding exponential sums.

THEOREM 1. *Let $\varepsilon > 0$, let $N_1, \dots, N_k \le P$ and M be positive integers and let $r(X) = f(X_1, \dots, X_k)/g(X_1, \dots, X_k)$ be a rational function with integer coefficients bounded by P^{K_1} and with $\deg f, \deg g < K_2$, where K_1 and K_2 are some positive constants. Assume that*

$$\#\mathcal{A}(r, N_1, \dots, N_k) \ll_{\varepsilon, k, K_1, K_2} N_1 \dots N_k P^{\varepsilon}. \tag{1.4}$$

Then

$$\sum_{P\le p\le 2P}\sum_{1\le m\le M}\Big|\sum_{1\le n_1\le N_1}\dots\sideset{}{^*}\sum_{1\le n_k\le N_k} e\Big(\frac{mr(n_1,\dots,n_k)}{p}\Big)\Big|^2 \ll_{\varepsilon,k,K_1,K_2} N_1\dots N_k(MP+PN_1\dots N_k+N_1\dots N_kM)P^{\varepsilon}. \tag{1.5}$$

As a consequence, if $N_1\dots N_k\le \min\{P,M\}$ then we get square root cancellation on average in the above exponential sums:

Corollary 1. *Under the hypotheses of Theorem* 1, *if* $N_1\dots N_k\le \min\{P,M\}$ *then for almost all pairs* (p,m) *with* p *prime*, $p\in[P,2P]$ *and* $m\in\{1,\dots,M\}$ *one has*

$$\Big|\sum_{1\le n_1\le N_1}\dots\sideset{}{^*}\sum_{1\le n_k\le N_k} e\Big(\frac{mr(n_1,\dots,n_k)}{p}\Big)\Big| \ll_{\varepsilon,k,K_1,K_2} N_1^{1/2}\dots N_k^{1/2}P^{\varepsilon}. \tag{1.6}$$

In practice, in order to apply the above results one first needs to check whether the given rational function $r(X_1,\dots,X_k)$ satisfies the above condition (1.4). Let us remark that if two rational functions $r_1(X_1,\dots,X_k)$ and $r_2(X_1,\dots,X_k)$ differ by a polynomial, that is,

$$r_1(X_1,\dots,X_k)-r_2(X_1,\dots,X_k)\in\mathbb{Z}[X_1,\dots,X_k],$$

then for any k-tuple $(N_1,\dots,N_k)$ one has

$$\#\mathcal{A}(r_1,N_1,\dots,N_k)=\#\mathcal{A}(r_2,N_1,\dots,N_k).$$

Therefore (1.4) holds for $r_1(X_1,\dots,X_k)$ if and only if it holds for $r_2(X_1,\dots,X_k)$. In case $k=1$ the relation (1.4) holds for any $r(X)$ which is not a polynomial (see [10], Section 3). For functions of several variables this is no longer the case. For example, if $k\ge 2$ and b is a nonzero integer then (1.4) fails for the rational function

$$r(X_1,\dots,X_k)=\frac{b}{X_1+\dots+X_k}. \tag{1.7}$$

Indeed, in this case any $(2k+1)$-tuple $(x_1,\dots,x_k,y_1,\dots,y_k,0)$ with $x_1,\dots,x_k,y_1,\dots,y_k\in\mathbb{Z}$, $1\le x_j,y_j\le N_j$ for $1\le j\le k$ and $x_1+\dots+x_k=y_1+\dots+y_k$ will be an element of $\mathcal{A}(r,N_1,\dots,N_k)$. If we replace the sum from the denominator of the right hand side of (1.7) by the product $X_1\dots X_k$ then the condition (1.4) will hold true. By the above remark this condition will continue to hold if a polynomial is added to our rational function. In particular if we take

$$r(X_1,\dots,X_k)=a_1X_1+\dots+a_kX_k+\frac{b}{X_1\dots X_k}$$

then (1.4) holds and we obtain square root cancellation in certain averages of short hyper-Kloosterman sums:

COROLLARY 2. *Let $K, \varepsilon > 0$, let $P, M, N_1, \dots, N_k$ be positive integers such that $N_1 \dots N_k < \min\{P, M\}$ and let $b \neq 0$ and $a_1, \dots, a_k$ be integers bounded by P^K. Then for almost all pairs (p, m) with p prime, $p \in [P, 2P]$ and $1 \leq m \leq M$ one has*

$$\left| \sum_{1 \leq n_1 \leq N_1} \dots \sum_{1 \leq n_k \leq N_k} e\left(\frac{m(a_1 n_1 + \dots + a_k n_k + b\overline{n_1 \dots n_k})}{p} \right) \right| \ll_{\varepsilon, k, K} N_1^{1/2} \dots N_k^{1/2} P^{\varepsilon}, \tag{1.8}$$

where $\overline{n_1 \dots n_k}$ denotes the inverse of $n_1 \dots n_k$ modulo p.

As was pointed out by the referee, our results have a similarity to the Large Sieve Inequality. In fact, in case $r(n) = n$ (which is not covered by our results) the left hand side of (1.2) can be written in the form $\sum_{j=1}^{R} |S(\alpha_j)|^2$, where $S(\alpha) = \sum_{n=1}^{N} e(n\alpha)$ and $\{\alpha_1, \dots, \alpha_R\}$ is the set of fractions m/p with $1 \leq m \leq M$ and $P \leq p \leq 2P$, p prime. The Large Sieve Inequality (see Montgomery [7]) gives an upper bound of the form

$$\sum_{j=1}^{R} |S(\alpha_j)|^2 \leq \Delta(N, \delta) \sum_{n=M+1}^{M+N} |a_n|^2$$

for any trigonometric polynomial with complex coefficients

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha)$$

and any real numbers $\alpha_1, \dots, \alpha_R$ which are well spaced (mod 1) in the sense that $\|\alpha_j - \alpha_s\| \geq \delta$ for $j \neq s$, where $\|\cdot\|$ denotes the distance to the nearest integer. Here one can take $\Delta(N, \delta) = N - 1 + \delta^{-1}$. Our method also works with weights a_n or, in general, $a(n_1, \dots, n_k)$ attached to the sums. The results are presented in Section 4.4 below.

Acknowledgements. The author is grateful to the referee whose comments led to the results presented in Section 4.4.

2. Exponential sums and pair correlations. Let $\mathcal{N} = \{x_n : 1 \leq n \leq N\}$ be a finite sequence of points in the interval $[0, 1]$ and let M be a positive integer. An upper bound for the second moment

$$M_2(\mathcal{N}, M) := \sum_{1 \leq m \leq M} \left| \sum_{1 \leq n \leq N} e(mx_n) \right|^2$$

is provided in [10], Section 2, in terms of the pair correlation of the set $\mathcal{N}$. The result is

$$M_2(\mathcal{N}, M) \ll ME(\mathcal{N}, M) \tag{2.1}$$

where

$$E(\mathcal{N}, M) = \#\{1 \le n, n' \le N : \|x_n - x_{n'}\| \le 1/M\}.$$

Now let $r(X_1, \dots, X_k)$ be a rational function as in the statement of Theorem 1 and let p be a prime number in the interval $[P, 2P]$. Choose positive integers $N_1, \dots, N_k$ less than p and let $B(r, p, N_1, \dots, N_k)$ be the set of k-tuples $(n_1, \dots, n_k)$ of positive integers with $n_j \le N_j$, $1 \le j \le k$, for which $g(n_1, \dots, n_k)$ is nonzero modulo p. Denote by $\mathcal{N}(r, p, N_1, \dots, N_k)$ the set of values of $r(n_1, \dots, n_k) \pmod p/p$, counted with multiplicities, as $(n_1, \dots, n_k)$ varies in $B(r, p, N_1, \dots, N_k)$. From (2.1) applied to $\mathcal{N} = \mathcal{N}(r, p, N_1, \dots, N_k)$ we get

$$\sum_{1 \le m \le M} \Big| \sum_{1 \le n_1 \le N_1} \cdots \sideset{}{^*}\sum_{1 \le n_k \le N_k} e\Big(\frac{mr(n_1, \dots, n_k)}{p}\Big)\Big|^2 \ll ME(\mathcal{N}(r, p, N_1, \dots, N_k), M) \tag{2.2}$$

where

$$\begin{aligned} &E(\mathcal{N}(r, p, N_1, \dots, N_k), M) \\ &\quad = \#\{(n_1, \dots, n_k), (n'_1, \dots, n'_k) \in B(r, p, N_1, \dots, N_k) : \\ &\qquad r(n_1, \dots, n_k) - r(n'_1, \dots, n'_k) \equiv h \pmod p,\ |h| \le p/M\}. \end{aligned}$$

3. Averaging over p. We add the inequalities (2.2) for all primes $p \in [P, 2P]$ to obtain

$$\sum_{P \le p \le 2P} \sum_{1 \le m \le M} \Big| \sum_{1 \le n_1 \le N_1} \cdots \sideset{}{^*}\sum_{1 \le n_k \le N_k} e\Big(\frac{mr(n_1, \dots, n_k)}{p}\Big)\Big|^2 \ll M \sum_{P \le p \le 2P} E(\mathcal{N}(r, p, N_1, \dots, N_k), M). \tag{3.1}$$

Note that the sum on the right hand side equals the number of $(2k+2)$-tuples $(n_1, \dots, n_k, n'_1, \dots, n'_k, h, p)$ satisfying the following conditions:

$$\begin{aligned} &p \text{ prime}, \quad P \le p \le 2P, \\ &h \in \mathbb{Z}, \quad |h| \le p/M, \\ &n_1, \dots, n_k, n'_1, \dots, n'_k \in \mathbb{Z}, \\ &1 \le n_j, n'_j \le N_j, \quad 1 \le j \le k, \\ &g(n_1, \dots, n_k),\ g(n'_1, \dots, n'_k) \text{ nonzero } (\mathrm{mod}\, p), \\ &r(n_1, \dots, n_k) - r(n'_1, \dots, n'_k) \equiv h \pmod p. \end{aligned} \tag{3.2}$$

The last condition in (3.2) is equivalent to

$$g(n_1',\dots,n_k')f(n_1,\dots,n_k)-f(n_1',\dots,n_k')g(n_1,\dots,n_k) \equiv hg(n_1',\dots,n_k')g(n_1,\dots,n_k) \pmod p. \tag{3.3}$$

For any solution $(n_1,\dots,n_k,n_1',\dots,n_k',h,p)$ to (3.2) consider the integer

$$A = g(n_1',\dots,n_k')f(n_1,\dots,n_k)-f(n_1',\dots,n_k')g(n_1,\dots,n_k) - hg(n_1',\dots,n_k')g(n_1,\dots,n_k).$$

We count separately the solutions with $A=0$ and those with $A\neq 0$. Let $(n_1,\dots,n_k,n_1',\dots,n_k',h,p)$ be a solution with $A=0$. Then

$$r(n_1,\dots,n_k)-r(n_1',\dots,n_k')=h$$

in $\mathbb{Q}$, hence $(n_1,\dots,n_k,n_1',\dots,n_k',h)$ is an integer point on the hypersurface H_r. Moreover, from (3.2) we see that this point belongs to $\mathcal{A}(r,N_1,\dots,N_k)$. By our assumption (1.4), the number of elements of $\mathcal{A}(r,N_1,\dots,N_k)$ is $\ll_{\varepsilon,k,K_1,K_2} N_1\dots N_kP^{\varepsilon}$. Any such $(2k+1)$-tuple $(n_1,\dots,n_k,n_1',\dots,n_k',h)$ appears in less than P solutions $(n_1,\dots,n_k,n_1',\dots,n_k',h,p)$ to (3.2), therefore the number of solutions with $A=0$ is

$$\ll_{\varepsilon,k,K_1,K_2} N_1\dots N_kP^{1+\varepsilon}.$$

We now count the solutions to (3.2) for which $A\neq 0$. Choose a $(2k+1)$-tuple $(n_1,\dots,n_k,n_1',\dots,n_k',h)$ which appears in such a solution. The point here is that A cannot have too many prime divisors. More precisely, from the hypotheses of Theorem 1 we see that

$$A \ll_{k,K_2} P^{2K_1}(\max\{N_1,\dots,N_k\})^{2K_2}\max\{P/M,1\} \ll P^{2K_1+2K_2+1}.$$

It follows that the number of primes $p\in[P,2P]$ which divide A is bounded by a constant which depends on k, K_1 and K_2 only.

Taking into account that by (3.2) the $(2k+1)$-tuple $(n_1,\dots,n_k,n_1',\dots,n_k',h)$ takes at most $N_1^2\dots N_k^2\max\{2P/M,1\}$ values, we find that the number of solutions to (3.2) with $A\neq 0$ is

$$\ll_{\varepsilon,k,K_1,K_2} \frac{N_1^2\dots N_k^2(P+M)}{M}.$$

Therefore the total number of solutions to (3.2) is

$$\ll_{\varepsilon,k,K_1,K_2} N_1\dots N_kP^{1+\varepsilon}+\frac{N_1^2\dots N_k^2(P+M)}{M}.$$

Using this bound for the sum on the right hand side of (3.1) we obtain (1.5), which completes the proof of Theorem 1.

4. Further remarks, applications and generalizations

4.1. In order to prove Corollary 2 we need to check that $r(X_1,\dots,X_k) = b/(X_1\dots X_k)$ satisfies (1.4). Let us count the number of $(2k+1)$-tuples

$(x_1, \dots, x_k, y_1, \dots, y_k, z)$ in $\mathcal{A}(r, N_1, \dots, N_k)$ with $x_1, \dots, x_k$ fixed. Multiplying (1.3) by $x_1 \dots x_k$ we find that $bx_1 \dots x_k/(y_1 \dots y_k)$ is an integer. This almost fixes $y_1, \dots, y_k$ since the number of divisors of the nonzero integer $bx_1 \dots x_k$ is $O_{\varepsilon,k,K_1}(P^\varepsilon)$. Next, with $(x_1, \dots, x_k, y_1, \dots, y_k)$ fixed, z is uniquely determined by (1.3). Thus $r(X_1, \dots, X_k)$ satisfies (1.4).

4.2. Under the hypotheses of Corollary 1, assume also that all the elements $(x_1, \dots, x_k, y_1, \dots, y_k, z)$ of $\mathcal{A}(r, N_1, \dots, N_k)$ satisfy

$$|z| < P/M. \tag{4.1}$$

Note that for any $(x_1, \dots, x_k, y_1, \dots, y_k, z)$ in $\mathcal{A}(r, N_1, \dots, N_k)$ one has

$$\begin{aligned} |z| &\le |f(x_1, \dots, x_k)| + |f(y_1, \dots, y_k)| \\ &\le 2P^{K_1}(K_2+1)^k(\max\{N_1, \dots, N_k\})^{K_2}, \end{aligned}$$

therefore (4.1) will hold if we assume that $K_1 < 1$ and

$$P^{1-K_1} > 2M(\max\{N_1, \dots, N_k\})^{K_2}.$$

Under the above assumptions the condition (1.4) besides being sufficient is also necessary in order to have square root cancellation on average in the exponential sums under consideration. Indeed, on the one hand by an appropriate modification of the argument which gives (2.1) one also obtains an upper bound for $ME(\mathcal{N}, M)$ in terms of exponential sums:

$$ME(\mathcal{N}, M) \ll \sum_{|m| \le M} \Big| \sum_{1 \le n \le N} e(mx_n) \Big|^2$$

(see for example Chapter 2 of Baker [1]). This provides an upper bound for the sum on the right hand side of (3.1), and hence also for the number, call it l, of solutions of the system (3.2), in terms of exponential sums. On the other hand, following the proof of Theorem 1 and using also (4.1) we see that each element of $\mathcal{A}(r, N_1, \dots, N_k)$ in combination with each admissible prime p produce a solution to (3.2), and this gives a lower bound for l. Now if $r(X_1, \dots, X_k)$ does not satisfy (1.4), this lower bound will be too large to still have square root cancellation on average in the exponential sums appearing in the above upper bound for l.

4.3. As in Theorem 3 of [10], we may combine Theorem 1 above with the Erdős–Turán inequality to obtain a square root saving on average in the discrepancy of the sets

$$\begin{aligned} \mathcal{N}(r, p, m, N_1, \dots, N_k) := \{mr(n_1, \dots, n_k)/p : 1 \le n_j \le N_j,\ 1 \le j \le k, \\ g(n_1, \dots, n_k) \not\equiv 0 \pmod p\}. \end{aligned}$$

The result is

THEOREM 2. *Under the hypotheses of Theorem* 1, *assume also that* $N_1 \dots \dots N_k \le \min\{P, M\}$ *and that* (1.4) *holds with* r *replaced by* mr *for any* $1 \le m \le N_1 \dots N_k$. *Then for almost all pairs* (p, m) *with* p *prime*, $p \in [P, 2P]$ *and* $1 \le m \le M$ *one has*

$$D(\mathcal{N}(r, p, m, N_1, \dots, N_k)) \ll_{\varepsilon,k,K_1,K_2} N_1^{1/2} \dots N_k^{1/2} P^{\varepsilon}.$$

Here the *discrepancy* $D(\mathcal{N})$ of a finite sequence $\mathcal{N} = \{x_n : 1 \le n \le N\}$ of points in $[0, 1]$ is defined by

$$D(\mathcal{N}) = \sup_{0 \le \alpha < \beta \le 1} |\#(\mathcal{N} \cap [\alpha, \beta]) - N(\beta - \alpha)|.$$

The proof of the above theorem goes along the same lines as that of Theorem 3 of [10]. As a consequence of Theorem 2 we have the following

COROLLARY 3. *Under the hypotheses of Theorem* 2, *for almost all pairs* (p, m) *with* p *prime*, $p \in [P, 2P]$ *and* $1 \le m \le M$ *and for any* $\beta \in [0, 1]$ *there exist* $1 \le n_1 \le N_1, \dots, 1 \le n_k \le N_k$ *such that*

$$\left| \left\{ \frac{mr(n_1, \dots, n_k) \pmod p}{p} \right\} - \beta \right| \ll_{\varepsilon,k,K_1,K_2} N_1^{-1/2} \dots N_k^{-1/2} P^{\varepsilon}.$$

4.4. One can generalize the inequalities (1.2) and (1.5) by attaching weights a_n, respectively $a(n_1, \dots, n_k)$ to the corresponding exponential sums. We are looking for an upper bound for the sum

$$S := \sum_{P \le p \le 2P} \sum_{|m| \le M} \left| \sum_{1 \le n_j \le N_j,\, 1 \le j \le k}^{*} a(n_1, \dots, n_k) e\left(\frac{mr(n_1, \dots, n_k)}{p} \right) \right|^2$$

where the weights $a(n_1, \dots, n_k)$ are arbitrary complex numbers. In this case instead of the number of elements in the set $\mathcal{A}(r, N_1, \dots, N_k)$ we consider the weighted sum

$$\sigma = \sum_{(\mathbf{x}, \mathbf{y}, z) \in \mathcal{A}(r, N_1, \dots, N_k)} |a(x_1, \dots, x_k) a(y_1, \dots, y_k)| \tag{4.2}$$

where we have set $\mathbf{x} = (x_1, \dots, x_k)$, $\mathbf{y} = (y_1, \dots, y_k)$. One has the following generalization of Theorem 1.

THEOREM 3. *Let* $K_1, K_2, \varepsilon > 0$, *let* $N_1, \dots, N_k \le P$ *and* M *be positive integers*, *let* $a(n_1, \dots, n_k)$ *with* $1 \le n_j \le N_j$, $1 \le j \le k$, *be complex numbers and let* $r(X) = f(X_1, \dots, X_k)/g(X_1, \dots, X_k)$ *be a rational function with integer coefficients bounded by* P^{K_1} *and with* $\deg f, \deg g \le K_2$. *Then*

$$|S| \ll_{\varepsilon,k,K_1,K_2} PM\sigma + P^{\varepsilon}(P+M) \Big(\sum_{1 \le n_j \le N_j,\, 1 \le j \le k} |a(n_1, \dots, n_k)| \Big)^2. \tag{4.3}$$

Taking into account the contribution of the diagonal terms $\mathbf{x} = \mathbf{y}$ in (4.2) we see that one always has

$$\sigma \geq \sum_{1 \leq n_j \leq N_j,\, 1 \leq j \leq k} |a(n_1, \dots, n_k)|^2. \tag{4.4}$$

In case $k = 1$ and $r(X) = f(X)/g(X)$ is not a polynomial, reasoning in terms of the resultant $R(f, g)$ as in Section 3 of [10] one finds that σ is not much larger than the right hand side of (4.4); more precisely,

$$\sigma \ll_{\varepsilon, K_1, K_2} P^{\varepsilon} \sum_{1 \leq n \leq N} |a_n|^2.$$

Hence we obtain the following result.

THEOREM 4. *Let $K_1, K_2, \varepsilon > 0$, let $N \leq P$ and M be positive integers, let a_n with $1 \leq n \leq N$ be complex numbers and let $r(X) = f(X)/g(X)$ be a rational function with integer coefficients bounded by P^{K_1} and with $\deg f, \deg g \leq K_2$, $r(X)$ not a polynomial. Then*

$$\sum_{P \leq p \leq 2P} \sum_{|m| \leq M} \Big| \sum_{1 \leq n \leq N}^{*} a_n e\Big(\frac{mr(n)}{p}\Big)\Big|^2 \ll_{\varepsilon, K_1, K_2} P^{1+\varepsilon}\Big[M \sum_{1 \leq n \leq N} |a_n|^2 + \Big(\sum_{1 \leq n \leq N} |a_n|\Big)^2\Big]. \tag{4.5}$$

Here we applied Cauchy's inequality in order to get rid of the term $P^{\varepsilon} M (\sum_{1 \leq n \leq N} |a_n|)^2$. Applying it one more time we obtain the following generalization of (1.2).

COROLLARY 4. *Under the hypotheses of Theorem* 4, *assume also that $N \leq M$. Then*

$$\sum_{P \leq p \leq 2P} \sum_{|m| \leq M} \Big| \sum_{1 \leq n \leq N}^{*} a_n e\Big(\frac{mr(n)}{p}\Big)\Big|^2 \ll_{\varepsilon, K_1, K_2} P^{1+\varepsilon} M \sum_{1 \leq n \leq N} |a_n|^2.$$

Returning to Theorem 3, its proof uses the following lemma.

LEMMA 1. *For any real numbers $x_1, \dots, x_N$, any complex numbers $a_1, \dots, a_N$ and any positive integer M one has*

$$\sum_{|m| \leq M} \Big| \sum_{1 \leq n \leq N} a_n e(m x_n)\Big|^2 \ll M \sum_{\substack{1 \leq n,\, n' \leq N \\ \|x_n - x_{n'}\| \leq 1/M}} |a_n a_{n'}|.$$

The proof of Lemma 1 goes along the same lines as the proof of (2.1) given in [10]: reasoning in terms of the real and imaginary part of a_n we may assume that the a_n's are real; next, by putting together the positive, respectively negative weights one further reduces the problem to the case

when the a_n's are positive numbers. Then the positivity argument from Section 2 of [10] works and the lemma is proved.

If we use Lemma 1 instead of (2.1) in the above relations (2.2) and (3.1) the result is that in (3.2) we have to count each solution $(n_1, \dots, n_k, n'_1, \dots \dots n'_k, h, p)$ with a weight given by $|a(n_1, \dots, n_k)a(n'_1, \dots, n'_k)|$. Note that the congruence (3.3) does not depend on the weights, so we have the same two classes of solutions to (3.2) as before, according as $A = 0$ or $A \neq 0$. The contribution of solutions with $A = 0$ to the right hand side of (4.3) is captured in the term $PM\sigma$, while the contribution of solutions with $A \neq 0$ is bounded by the other term, and this proves Theorem 3.

References

[1] R. C. Baker, *Diophantine Inequalities*, Oxford Univ. Press, New York, 1986.
[2] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.
[3] —, *On exponential sums in finite fields. II*, Invent. Math. 47 (1978), 29–39.
[4] P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. 43 (1974), 273–307.
[5] —, *La conjecture de Weil. II*, ibid. 52 (1980), 137–252.
[6] N. M. Katz, *Sommes exponentielles*, Astérisque 79 (1980).
[7] H. L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. 84 (1978), 547–567.
[8] J. P. Serre, *Majoration de sommes exponentielles*, Astérisque 41–42 (1977), 111–126.
[9] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207.
[10] A. Zaharescu, *Averages of short exponential sums*, Acta Arith. 88 (1999), 223–231.

Institute of Mathematics of the Romanian Academy
P.O. Box 1-764
RO-70700 Bucureşti, Romania

Department of Mathematics
University of Illinois
at Urbana-Champaign
Altgeld Hall
1409 W. Green Street
Urbana, IL 61801, U.S.A.
E-mail: zaharesc@math.uiuc.edu

Received on 24.1.2000
and in revised form on 22.3.2001 (3746)