ACTA ARITHMETICA
LXVII.3 (1994)

Bounds for exponential sums and their applications to pseudorandom numbers

by

Jürgen Eichenauer-Herrmann (Darmstadt) and
Harald Niederreiter (Wien)

1. Introduction. Let F_q be the finite field of order q, where q is an arbitrary prime power, and let F_q^* denote the set of nonzero elements of F_q. We define $\overline{c} = c^{-1} \in F_q^*$ for $c \in F_q^*$ and $\overline{c} = 0 \in F_q$ for $c = 0 \in F_q$. If $q \geq 3$, then we may equivalently put $\overline{c} = c^{q-2}$ for $c \in F_q$. We are primarily interested in complete exponential sums of the form

$$E(\chi; \mathbf{d}, \mathbf{e}) := \sum_{n \in F_q} \chi\Big(\sum_{j=1}^{s} d_j \overline{n + e_j}\Big),$$

where s is a positive integer, χ is a nontrivial additive character of F_q, and $\mathbf{d} = (d_1, \ldots, d_s) \in F_q^s$ and $\mathbf{e} = (e_1, \ldots, e_s) \in F_q^s$ are s-tuples of elements of F_q on which we will occasionally place minor restrictions to avoid trivial cases. For $q = p$ a prime, we will also consider the corresponding incomplete exponential sums

$$E_N(\chi; \mathbf{d}, \mathbf{e}) := \sum_{n=0}^{N-1} \chi\Big(\sum_{j=1}^{s} d_j \overline{n + e_j}\Big) \quad \text{for } 1 \leq N \leq p.$$

These exponential sums arise, for instance, in the analysis of a new method for pseudorandom number generation, the so-called explicit inversive congruential method, which will be described in Section 4.

In Section 2 we will deduce an upper bound for the exponential sums $E(\chi; \mathbf{d}, \mathbf{e})$ from the Bombieri–Weil bound. The corresponding incomplete exponential sums will be treated in the wider context of exponential sums with rational functions in their arguments. The average values (in the mean-square sense) of the complete and incomplete exponential sums will be calculated and lower bounds for the exponential sums will be derived in Section 3. The applications of our results to the analysis of pseudorandom numbers generated by the explicit inversive congruential method will be presented in Section 4.

2. Upper bounds for the exponential sums. We use the Bombieri–Weil bound (see [1]) in the following convenient form given by Moreno and Moreno [4, Theorem 2]. We write $\overline{F}_q$ for the algebraic closure of F_q and $\overline{F}_q(x)$ for the rational function field over $\overline{F}_q$.

LEMMA 1. *Let Q/R be a rational function over F_q which is not of the form $A^p - A$ with $A \in \overline{F}_q(x)$ and p the characteristic of F_q. Let s be the number of distinct roots of the polynomial R in $\overline{F}_q$. If χ is a nontrivial additive character of F_q, then*

$$\Big| \sum_{\substack{n \in F_q \\ R(n) \neq 0}} \chi\Big(\frac{Q(n)}{R(n)}\Big) \Big| \le (\max(\deg(Q), \deg(R)) + s^* - 2)q^{1/2} + \delta,$$

where $s^* = s$ and $\delta = 1$ if $\deg(Q) \le \deg(R)$, and $s^* = s + 1$ and $\delta = 0$ otherwise.

On the basis of this result, we can now establish an upper bound for the exponential sums $E(\chi; \mathbf{d}, \mathbf{e})$ under conditions that prevent these sums from being trivial.

THEOREM 1. *Let $\mathbf{d} \in F_q^s$ with $\mathbf{d} \neq \mathbf{0}$ and let $\mathbf{e} = (e_1, \ldots, e_s) \in F_q^s$ be such that $e_1, \ldots, e_s$ are distinct. If χ is a nontrivial additive character of F_q, then*

$$|E(\chi; \mathbf{d}, \mathbf{e})| \le (2s - 2)q^{1/2} + s + 1.$$

Proof. If $W = F_q \setminus \{-e_1, \ldots, -e_s\}$, then

$$|E(\chi; \mathbf{d}, \mathbf{e})| \le s + \Big| \sum_{n \in W} \chi\Big(\sum_{j=1}^{s} d_j \overline{n + e_j}\Big)\Big| = s + \Big| \sum_{\substack{n \in F_q \\ R(n) \neq 0}} \chi\Big(\frac{Q(n)}{R(n)}\Big)\Big|, \tag{1}$$

where Q/R is the rational function over F_q given by

$$\frac{Q(x)}{R(x)} = \sum_{j=1}^{s} \frac{d_j}{x + e_j} \quad \text{with } R(x) = \prod_{j=1}^{s} (x + e_j).$$

We claim that Q/R is not of the form $A^p - A$ with $A \in \overline{F}_q(x)$. For suppose we had

$$\frac{Q}{R} = \Big(\frac{K}{L}\Big)^p - \frac{K}{L}$$

with polynomials K, L over $\overline{F}_q$ and $\gcd(K, L) = 1$; then

$$L^p Q = (K^{p-1} - L^{p-1})KR. \tag{2}$$

From $\gcd(K, L) = 1$ it follows that L^p divides R, but since R has only simple roots, this can hold only if L is a nonzero constant polynomial. Since at least one d_j is nonzero, the uniqueness of the partial fraction decomposition for

rational functions implies that $Q \neq 0$. Then a comparison of degrees in (2) yields $\deg(Q) \geq \deg(R)$, and this contradiction proves the claim. Thus we can apply Lemma 1, which together with (1) establishes the theorem. ∎

Now we prove an upper bound for incomplete exponential sums over a finite prime field F_p with rational functions in their arguments.

THEOREM 2. *Let p be a prime, let Q/R be a nonzero rational function over F_p, and let s be the number of distinct roots of the polynomial R in $\overline{F}_p$. Furthermore, let χ be a nontrivial additive character of F_p and $1 \leq N < p$. If $\deg(Q) < \deg(R)$, then*

$$\Big|\sum_{\substack{n=0\\R(n)\neq 0}}^{N-1} \chi\Big(\frac{Q(n)}{R(n)}\Big)\Big| < (\deg(R)+s)p^{1/2}\Big(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\Big) + \frac{N}{p}((\deg(R)+s-2)p^{1/2}+1).$$

If $\deg(Q) \geq \deg(R)+2$, then

$$\Big|\sum_{\substack{n=0\\R(n)\neq 0}}^{N-1} \chi\Big(\frac{Q(n)}{R(n)}\Big)\Big| < (\deg(Q)+s-1)p^{1/2}\Big(\frac{4}{\pi^2}\log p + 0.38 + \frac{N+0.64}{p}\Big).$$

P r o o f. We can assume that $\deg(Q) < p$, $\deg(R) < p$, and $p \geq 5$, since the result is trivial otherwise. If S_N is the exponential sum in the theorem, then

$$S_N = \sum_{\substack{n=0\\R(n)\neq 0}}^{p-1} \chi\Big(\frac{Q(n)}{R(n)}\Big)\sum_{r=0}^{N-1}\frac{1}{p}\sum_{u=0}^{p-1}\chi(u(n-r))$$

since the sum over r is equal to 1 for $0 \leq n \leq N-1$ and equal to 0 for $N \leq n \leq p-1$. By rearranging terms, we get

$$\begin{aligned} S_N &= \frac{1}{p}\sum_{u=0}^{p-1}\Big(\sum_{r=0}^{N-1}\chi(-ur)\Big)\Big(\sum_{\substack{n\in F_p\\R(n)\neq 0}}\chi\Big(\frac{Q(n)}{R(n)}+un\Big)\Big)\\ &= \frac{1}{p}\sum_{u=1}^{p-1}\Big(\sum_{r=0}^{N-1}\chi(-ur)\Big)\Big(\sum_{\substack{n\in F_p\\R(n)\neq 0}}\chi\Big(\frac{Q(n)}{R(n)}+un\Big)\Big)\\ &\quad + \frac{N}{p}\sum_{\substack{n\in F_p\\R(n)\neq 0}}\chi\Big(\frac{Q(n)}{R(n)}\Big), \end{aligned}$$

and so

$$|S_N| \le \frac{1}{p}\sum_{u=1}^{p-1}\Big|\sum_{r=0}^{N-1}\chi(ur)\Big|\Big|\sum_{\substack{n\in F_p\\ R(n)\neq 0}}\chi\Big(\frac{Q(n)}{R(n)}+un\Big)\Big| + \frac{N}{p}\Big|\sum_{\substack{n\in F_p\\ R(n)\neq 0}}\chi\Big(\frac{Q(n)}{R(n)}\Big)\Big|. \tag{3}$$

For fixed $u \in F_p$ we consider the rational function

$$\frac{Q_u(x)}{R(x)} = \frac{Q(x)}{R(x)} + ux.$$

We want to prove that Q_u/R is not of the form $A^p - A$ with $A \in \overline{F}_p(x)$. Suppose we have

$$\frac{Q_u}{R} = \Big(\frac{K}{L}\Big)^p - \frac{K}{L}$$

with polynomials K, L over $\overline{F}_p$ and $\gcd(K, L) = 1$. Then

$$L^p Q_u = (K^{p-1} - L^{p-1})KR.$$

From $\gcd(K, L) = 1$ it follows that L^p divides R. Since $\deg(R) < p$, this is possible only if L is a nonzero constant polynomial. Thus

$$Q_u = (\alpha K^p + \beta K)R \tag{4}$$

for suitable $\alpha, \beta \in \overline{F}_p$ with $\alpha\beta \neq 0$. We note that $Q_u(x) = Q(x) + uxR(x)$, and so $Q \neq 0$ implies that $Q_u \neq 0$ if either $\deg(Q) < \deg(R)$ or $\deg(Q) \ge \deg(R)+2$. Then (4) shows that $\deg(Q_u)-\deg(R)$ is a nonnegative multiple of p. Since $\deg(Q) < p$, this can hold only if $\deg(Q_u) = \deg(R)$, but in both cases $\deg(Q) < \deg(R)$ and $\deg(Q) \ge \deg(R) + 2$ this is seen to be impossible.

Thus, Lemma 1 can be applied to the complete exponential sums in (3). If $\deg(Q) < \deg(R)$, then this yields

$$|S_N| \le \frac{1}{p}\sum_{u=1}^{p-1}\Big|\sum_{r=0}^{N-1}\chi(ur)\Big|(\deg(R)+s)p^{1/2} + \frac{N}{p}((\deg(R)+s-2)p^{1/2}+1).$$

Now

$$\sum_{u=1}^{p-1}\Big|\sum_{r=0}^{N-1}\chi(ur)\Big| = \sum_{v=1}^{p-1}\Big|\frac{\sin(\pi vN/p)}{\sin(\pi v/p)}\Big| < \frac{4}{\pi^2}p\log p + (0.38)p + 0.64$$

by an inequality of Cochrane [2, Theorem 1], where we used $p \ge 5$. This establishes the bound in the theorem for $\deg(Q) < \deg(R)$. The bound for $\deg(Q) \ge \deg(R) + 2$ follows analogously. ∎

COROLLARY 1. *Let p be a prime, let $\mathbf{d} \in F_p^s$ with $\mathbf{d} \neq \mathbf{0}$, and let $\mathbf{e} = (e_1, \dots, e_s) \in F_p^s$ be such that $e_1, \dots, e_s$ are distinct. If χ is a nontrivial additive character of F_p and $1 \le N < p$, then*

$$|E_N(\chi; \mathbf{d}, \mathbf{e})| < 2sp^{1/2}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) + \frac{N}{p}((2s-2)p^{1/2}+1) + s.$$

Proof. Proceed as at the beginning of the proof of Theorem 1 and use the bound in Theorem 2 for the case $\deg(Q) < \deg(R)$. ∎

3. Average values and lower bounds for the exponential sums. For the applications in Section 4 we need special cases of the following results on the average values (in the mean-square sense) of the exponential sums introduced in Section 1.

THEOREM 3. *Let $1 \le k \le s$ and $\mathbf{e} \in F_q^s$. Then for every nontrivial additive character χ of F_q we have*

$$\sum_{d_1,\dots,d_k \in F_q} |E(\chi; \mathbf{d}, \mathbf{e})|^2 = q^{k+1},$$

where $\mathbf{d} = (d_1, \dots, d_s)$ with fixed $d_{k+1}, \dots, d_s \in F_q$.

Proof. With $\mathbf{e} = (e_1, \dots, e_s)$ we get

$$\begin{aligned}
&\sum_{d_1,\dots,d_k \in F_q} |E(\chi; \mathbf{d}, \mathbf{e})|^2 \\
&\quad = \sum_{d_1,\dots,d_k \in F_q} \sum_{n,m \in F_q} \chi\Big(\sum_{j=1}^{s} d_j(\overline{n+e_j} - \overline{m+e_j})\Big) \\
&\quad = \sum_{n,m \in F_q} \chi\Big(\sum_{j=k+1}^{s} d_j(\overline{n+e_j} - \overline{m+e_j})\Big) \\
&\qquad \times \prod_{j=1}^{k}\Big(\sum_{d \in F_q} \chi(d(\overline{n+e_j} - \overline{m+e_j}))\Big) \\
&\quad = \sum_{\substack{n,m \in F_q \\ n=m}} q^k = q^{k+1},
\end{aligned}$$

where we used the orthogonality relations for additive characters in the penultimate step. ∎

COROLLARY 2. *Let $\mathbf{e} = (e_1, e_2) \in F_q^2$ with $e_1 \neq e_2$ and $\mathbf{d} = (d_1, d_2) \in F_q^2$ with fixed $d_2 \in F_q^*$. Let χ be a nontrivial additive character of F_q. Let $0 <$*

$t \le \sqrt{q/(q-1)}$ *and*

$$A_q(t) := \frac{q^2 - (q-1)qt^2}{(2q^{1/2}+3)^2 - qt^2}.$$

Then there exist more than $A_q(t)$ *values of* $d_1 \in F_q^*$ *with*

$$|E(\chi; \mathbf{d}, \mathbf{e})| \ge tq^{1/2}.$$

Proof. Suppose that there exist at most $A_q(t)$ values of $d_1 \in F_q^*$ with $|E(\chi; \mathbf{d}, \mathbf{e})| \ge tq^{1/2}$, i.e., there exist at least $q - 1 - A_q(t)$ values of $d_1 \in F_q^*$ with $|E(\chi; \mathbf{d}, \mathbf{e})| < tq^{1/2}$. Now an application of Theorem 1 (with $s = 2$) implies that $|E(\chi; \mathbf{d}, \mathbf{e})| \le 2q^{1/2} + 3$ for every $d_1 \in F_q^*$. Hence, observing that $E(\chi; \mathbf{d}, \mathbf{e}) = 0$ for $d_1 = 0$, we obtain

$$\begin{aligned}\sum_{d_1 \in F_q} |E(\chi; \mathbf{d}, \mathbf{e})|^2 &= \sum_{d_1 \in F_q^*} |E(\chi; \mathbf{d}, \mathbf{e})|^2 \\ &< (q - 1 - A_q(t))t^2 q + A_q(t)(2q^{1/2}+3)^2 = q^2,\end{aligned}$$

which contradicts Theorem 3 (with $s = 2$ and $k = 1$). ∎

Theorem 4. *Let* p *be a prime,* $1 \le N < p$, *and* $1 \le k \le s$. *Then for every* $\mathbf{e} \in F_p^s$ *and every nontrivial additive character* χ *of* F_p *we have*

$$\sum_{d_1, \ldots, d_k \in F_p} |E_N(\chi; \mathbf{d}, \mathbf{e})|^2 = Np^k,$$

where $\mathbf{d} = (d_1, \ldots, d_s)$ *with fixed* $d_{k+1}, \ldots, d_s \in F_p$.

Proof. With $\mathbf{e} = (e_1, \ldots, e_s)$ we get

$$\begin{aligned}&\sum_{d_1, \ldots, d_k \in F_p} |E_N(\chi; \mathbf{d}, \mathbf{e})|^2 \\ &= \sum_{d_1, \ldots, d_k \in F_p} \sum_{n,m=0}^{N-1} \chi\Big(\sum_{j=1}^{s} d_j(\overline{n + e_j} - \overline{m + e_j})\Big) \\ &= \sum_{n,m=0}^{N-1} \chi\Big(\sum_{j=k+1}^{s} d_j(\overline{n + e_j} - \overline{m + e_j})\Big) \prod_{j=1}^{k} \Big(\sum_{d \in F_p} \chi(d(\overline{n + e_j} - \overline{m + e_j}))\Big) \\ &= \sum_{\substack{n,m=0 \\ n=m}}^{N-1} p^k = Np^k,\end{aligned}$$

where we used again the orthogonality relations for additive characters in the penultimate step. ∎

Corollary 3. *Let* p *be a prime,* $\mathbf{e} = (e_1, e_2) \in F_p^2$ *with* $e_1 \ne e_2$, *and* $\mathbf{d} = (d_1, d_2) \in F_p^2$ *with fixed* $d_2 \in F_p^*$. *Let* χ *be a nontrivial additive character*

of F_p. Let N be an integer with

$$\frac{1}{p}\biggl(2p^{1/2}\biggl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\biggr)+2\biggr)^2<N<p,$$

let

$$\tau_N:=\frac{p}{p-1}-\frac{1}{N(p-1)}\biggl(2p^{1/2}\biggl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\biggr)+2\biggr)^2,$$

and for $0<t\le\sqrt{\tau_N}$ put

$$A_N(t):=\frac{N(p-1)(\tau_N-t^2)}{\bigl(4p^{1/2}\bigl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\bigr)+\frac{N}{p}(2p^{1/2}+1)+2\bigr)^2-Nt^2}.$$

Then there exist more than $A_N(t)$ values of $d_1\in F_p^*$ with

$$|E_N(\chi;\mathbf{d},\mathbf{e})|\ge tN^{1/2}.$$

P r o o f. Suppose that there exist at most $A_N(t)$ values of $d_1\in F_p^*$ with $|E_N(\chi;\mathbf{d},\mathbf{e})|\ge tN^{1/2}$, i.e., there exist at least $p-1-A_N(t)$ values of $d_1\in F_p^*$ with $|E_N(\chi;\mathbf{d},\mathbf{e})|<tN^{1/2}$. Now an application of Corollary 1 (with $s=2$) implies that

$$|E_N(\chi;\mathbf{d},\mathbf{e})|<4p^{1/2}\biggl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\biggr)+\frac{N}{p}(2p^{1/2}+1)+2$$

for every $d_1\in F_p^*$. Moreover, we can deduce from Corollary 1 (with $s=1$) that

$$|E_N(\chi;\mathbf{d},\mathbf{e})|<2p^{1/2}\biggl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\biggr)+2$$

for $d_1=0$. Hence, we obtain

$$\begin{aligned}
&\sum_{d_1\in F_p}|E_N(\chi;\mathbf{d},\mathbf{e})|^2\\
&<\sum_{d_1\in F_p^*}|E_N(\chi;\mathbf{d},\mathbf{e})|^2+\biggl(2p^{1/2}\biggl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\biggr)+2\biggr)^2\\
&<(p-1-A_N(t))Nt^2\\
&\quad+A_N(t)\biggl(4p^{1/2}\biggl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\biggr)+\frac{N}{p}(2p^{1/2}+1)+2\biggr)^2\\
&\quad+\biggl(2p^{1/2}\biggl(\frac{4}{\pi^2}\log p+0.38+\frac{0.64}{p}\biggr)+2\biggr)^2\\
&=Np,
\end{aligned}$$

which contradicts Theorem 4 (with $s=2$ and $k=1$). ∎

COROLLARY 4. *Let p be a prime and $e \in F_p$. Let χ be a nontrivial additive character of F_p. Let $1 \le N < p, 0 < t \le \sqrt{(p-N)/(p-1)}$, and*

$$B_N(t) := \frac{N(p-N) - N(p-1)t^2}{\left(2p^{1/2}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) + \frac{N}{p} + 1\right)^2 - Nt^2}.$$

Then there exist more than $B_N(t)$ values of $d \in F_p^*$ with

$$|E_N(\chi; d, e)| \ge tN^{1/2}.$$

Proof. Suppose that there exist at most $B_N(t)$ values of $d \in F_p^*$ with $|E_N(\chi; d, e)| \ge tN^{1/2}$, i.e., there exist at least $p-1-B_N(t)$ values of $d \in F_p^*$ with $|E_N(\chi; d, e)| < tN^{1/2}$. Now an application of Corollary 1 (with $s = 1$) implies that

$$|E_N(\chi; d, e)| < 2p^{1/2}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) + \frac{N}{p} + 1$$

for every $d \in F_p^*$. Hence, observing that $E_N(\chi; 0, e) = N$, we obtain

$$\begin{aligned}
&\sum_{d \in F_p} |E_N(\chi; d, e)|^2 \\
&\quad = \sum_{d \in F_p^*} |E_N(\chi; d, e)|^2 + N^2 \\
&\quad < (p - 1 - B_N(t))Nt^2 \\
&\qquad + B_N(t)\left(2p^{1/2}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) + \frac{N}{p} + 1\right)^2 + N^2 \\
&\quad = Np,
\end{aligned}$$

which contradicts Theorem 4 (with $s = 1$ and $k = 1$). ∎

THEOREM 5. *Let p be a prime and $1 \le N < p$. Then for every $\mathbf{e} = (e_1, e_2) \in F_p^2$ with $e_1 \ne e_2$ and every nontrivial additive character χ of F_p we have*

$$\sum_{d \in F_p} |E_N(\chi; (d, -d), \mathbf{e})|^2 \ge p(2N - 1).$$

Proof. We get

$$\begin{aligned}
&\sum_{d \in F_p} |E_N(\chi; (d, -d), \mathbf{e})|^2 \\
&\quad = \sum_{d \in F_p} \sum_{n,m=0}^{N-1} \chi(d(\overline{n + e_1} - \overline{n + e_2} - \overline{m + e_1} + \overline{m + e_2}))
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{n,m=0}^{N-1} \sum_{d\in F_p} \chi(d(\overline{n+e_1} - \overline{n+e_2} - \overline{m+e_1} + \overline{m+e_2})) \\
&= p\,\#\{(n,m) \in \{0,1,\dots,N-1\}^2 : \overline{n+e_1} - \overline{n+e_2} = \overline{m+e_1} - \overline{m+e_2}\} \\
&\ge p\,\#\{(n,m) \in \{0,1,\dots,N-1\}^2 : n = m \text{ or } n = -(m+e_1+e_2)\} \\
&\ge p(2N-1),
\end{aligned}
$$

where we used once more the orthogonality relations for additive characters. ∎

Corollary 5. *Let p be a prime, $1 \le N < p$, and $\mathbf{e} = (e_1, e_2) \in F_p^2$ with $e_1 \ne e_2$. Let χ be a nontrivial additive character of F_p, let*

$$\sigma_N := 1 + \frac{(p-N)(N-1)}{(p-1)N},$$

and for $0 < t \le \sqrt{\sigma_N}$ put

$$C_N(t) := \frac{N(p-1)(\sigma_N - t^2)}{\big(4p^{1/2}\big(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\big) + \frac{N}{p}(2p^{1/2}+1) + 2\big)^2 - Nt^2}.$$

Then there exist more than $C_N(t)$ values of $d \in F_p^*$ with

$$|E_N(\chi; (d,-d), \mathbf{e})| \ge tN^{1/2}.$$

Proof. Suppose that there exist at most $C_N(t)$ values of $d \in F_p^*$ with $|E_N(\chi;(d,-d),\mathbf{e})| \ge tN^{1/2}$, i.e., there exist at least $p-1-C_N(t)$ values of $d \in F_p^*$ with $|E_N(\chi;(d,-d),\mathbf{e})| < tN^{1/2}$. Now an application of Corollary 1 (with $s=2$) implies that

$$|E_N(\chi;(d,-d),\mathbf{e})| < 4p^{1/2}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) + \frac{N}{p}(2p^{1/2}+1) + 2$$

for every $d \in F_p^*$. Hence, observing that $E_N(\chi;\mathbf{0},\mathbf{e}) = N$, we obtain

$$
\begin{aligned}
&\sum_{d\in F_p} |E_N(\chi;(d,-d),\mathbf{e})|^2 \\
&\quad = \sum_{d\in F_p^*} |E_N(\chi;(d,-d),\mathbf{e})|^2 + N^2 \\
&\quad < (p-1-C_N(t))Nt^2 \\
&\qquad + C_N(t)\left(4p^{1/2}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) + \frac{N}{p}(2p^{1/2}+1) + 2\right)^2 + N^2 \\
&\quad = p(2N-1),
\end{aligned}
$$

which contradicts Theorem 5. ∎

4. Applications to pseudorandom numbers. In Niederreiter [6], [7] the following *explicit inversive congruential method* for generating parallel streams of uniform pseudorandom numbers was introduced on the basis of an earlier proposal of explicit inversive methods for pseudorandom number generation by Eichenauer-Herrmann [3]. Let p be a prime, let $a_1, \ldots, a_s \in F_p^*$, and let $b_1, \ldots, b_s \in F_p$ be such that $b_1\overline{a}_1, \ldots, b_s\overline{a}_s \in F_p$ are distinct. We identify F_p with the set $\{0, 1, \ldots, p-1\}$ of integers. Let $y_n^{(j)} = \overline{a_j n + b_j} \in F_p$ and $x_n^{(j)} = y_n^{(j)}/p$ for $1 \le j \le s$ and $n \ge 0$. Then the sequences $(x_n^{(j)})_{n\ge 0}$, $1 \le j \le s$, can be viewed as s parallel streams of pseudorandom numbers in the interval $[0, 1)$. The statistical independence of these streams, which is of crucial importance for stochastic simulations, can be assessed by the discrepancy of the s-tuples

$$\mathbf{x}_n = (x_n^{(1)}, \ldots, x_n^{(s)}) \in [0,1)^s, \qquad n \ge 0.$$

For N arbitrary points $\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1} \in [0,1)^s$ the *discrepancy* is defined by

$$D_N(\mathbf{t}_0, \mathbf{t}_1, \ldots, \mathbf{t}_{N-1}) = \sup_J |G_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0,1)^s$, $G_N(J)$ is N^{-1} times the number of $0 \le n \le N-1$ with $\mathbf{t}_n \in J$, and $V(J)$ denotes the s-dimensional volume of J. Subsequently, for $1 \le N \le p$ the abbreviation

$$D_N^{(s)} = D_N(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1})$$

is used. It has been proved in [7, Theorems 2 and 3] that

$$D_p^{(s)} = O(p^{-1/2}(\log p)^s)$$

and

$$D_N^{(s)} = O(N^{-1}p^{1/2}(\log p)^{s+1}) \quad \text{for } 1 \le N < p.$$

It should be observed that upper bounds of the same form can also be derived from Theorem 1, Corollary 1, and [5, Corollary 3.11]. In this section, lower bounds for the discrepancies $D_N^{(s)}$ with $1 \le N \le p$ will be established.

First, for $s \ge 2$ an application of [5, Corollary 3.17 with $\mathbf{h}=(1,1,0,\ldots,0) \in \mathbb{Z}^s$] implies that

$$\begin{aligned} D_N^{(s)} &\ge \frac{1}{2(\pi+2)N}\Big|\sum_{n=0}^{N-1} e(x_n^{(1)} + x_n^{(2)})\Big| \\ &= \frac{1}{2(\pi+2)N}\Big|\sum_{n=0}^{N-1} \chi(\overline{a_1 n + b_1} + \overline{a_2 n + b_2})\Big| \\ &= \frac{1}{2(\pi+2)N}|E_N(\chi; \mathbf{d}, \mathbf{e})| \end{aligned}$$

with $\mathbf{d} = (\overline{a}_1, \overline{a}_2) \in F_p^2$ and $\mathbf{e} = (b_1\overline{a}_1, b_2\overline{a}_2) \in F_p^2$, where $e(t) = e^{2\pi it}$ for $t \in \mathbb{R}$ and $\chi(u) = e(u/p)$ for $u \in F_p$. Similarly, it follows from [5, Corollary 3.17 with $\mathbf{h} = (1, 0, \ldots, 0) \in \mathbb{Z}^s$] that for $s \geq 1$ we have

$$D_N^{(s)} \geq \frac{1}{2N}|E_N(\chi; \overline{a}_1, b_1\overline{a}_1)|.$$

Therefore, the following results are immediate consequences of Corollaries 2, 3, and 4.

COROLLARY 6. *Let $a_2 \in F_p^*, b_2 \in F_p$, and $c \in F_p \setminus \{b_2\overline{a}_2\}$ be fixed. Let $0 < t \leq \sqrt{p/(p-1)}$, and let $A_p(t)$ be defined as in Corollary 2 (with $q = p$). Then there exist more than $A_p(t)$ values of $a_1 \in F_p^*$ such that for any corresponding explicit inversive congruential pseudorandom numbers with $b_1 = a_1c$ and $s \geq 2$ we have*

$$D_p^{(s)} \geq \frac{t}{2(\pi+2)}p^{-1/2}.$$

COROLLARY 7. *Let $a_2 \in F_p^*, b_2 \in F_p, c \in F_p \setminus \{b_2\overline{a}_2\}$, and an integer N with*

$$\frac{1}{p}\left(2p^{1/2}\left(\frac{4}{\pi^2}\log p + 0.38 + \frac{0.64}{p}\right) + 2\right)^2 < N < p$$

be fixed. Let τ_N and $A_N(t)$ for $0 < t \leq \sqrt{\tau_N}$ be defined as in Corollary 3. Then there exist more than $A_N(t)$ values of $a_1 \in F_p^*$ such that for any corresponding explicit inversive congruential pseudorandom numbers with $b_1 = a_1c$ and $s \geq 2$ we have

$$D_N^{(s)} \geq \frac{t}{2(\pi+2)}N^{-1/2}.$$

COROLLARY 8. *Let $c \in F_p$ and $1 \leq N < p$ be fixed. Let $0 < t \leq \sqrt{(p-N)/(p-1)}$, and let $B_N(t)$ be defined as in Corollary 4. Then there exist more than $B_N(t)$ values of $a_1 \in F_p^*$ such that for any corresponding explicit inversive congruential pseudorandom numbers with $b_1 = a_1c$ and $s \geq 1$ we have*

$$D_N^{(s)} \geq \frac{t}{2}N^{-1/2}.$$

Finally, the statistical independence of successive pseudorandom numbers within one stream will be assessed by the discrepancy of the s-tuples

$$\mathbf{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0,1)^s, \qquad n \geq 0,$$

where $x_n = y_n/p$ and $y_n = \overline{an+b} \in F_p$ for $n \geq 0$ with $a \in F_p^*$ and $b \in F_p$.

For $1 \le N \le p$ the abbreviation

$$D_N^{(s)} = D_N(\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_{N-1})$$

is used once again. It has been proved in [3, Theorems 1 and 2] that

$$D_p^{(s)} = O(p^{-1/2}(\log p)^s),$$

and that this upper bound is in general best possible up to the logarithmic factor. Moreover, it follows from [7, Theorem 3] that

$$D_N^{(s)} = O(N^{-1}p^{1/2}(\log p)^{s+1})$$

for $1 \le N < p$. We now establish a lower bound for the discrepancy $D_N^{(s)}$ with $1 \le N < p$.

First, for $s \ge 2$ an application of [5, Corollary 3.17 with $\mathbf{h} = (1, -1, 0, \ldots, 0) \in \mathbb{Z}^s$] implies that

$$\begin{aligned} D_N^{(s)} &\ge \frac{1}{2(\pi+2)N}\Big|\sum_{n=0}^{N-1} e(x_n - x_{n+1})\Big| \\ &= \frac{1}{2(\pi+2)N}\Big|\sum_{n=0}^{N-1} \chi(\overline{an+b} - \overline{an+b+a})\Big| \\ &= \frac{1}{2(\pi+2)N}\Big|E_N(\chi; (\overline{a}, -\overline{a}), (b\overline{a}, b\overline{a}+1))\Big|, \end{aligned}$$

where again $\chi(u) = e(u/p)$ for $u \in F_p$. Therefore, the following result is an immediate consequence of Corollary 5.

COROLLARY 9. *Let $c \in F_p$ and $1 \le N < p$ be fixed. Let σ_N and $C_N(t)$ for $0 < t \le \sqrt{\sigma_N}$ be defined as in Corollary 5. Then there exist more than $C_N(t)$ values of $a \in F_p^*$ such that for the corresponding explicit inversive congruential pseudorandom numbers with $b = ac$ and $s \ge 2$ we have*

$$D_N^{(s)} \ge \frac{t}{2(\pi+2)} N^{-1/2}.$$

References

[1] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.

[2] T. Cochrane, *On a trigonometric inequality of Vinogradov*, J. Number Theory 27 (1987), 9–16.

[3] J. Eichenauer-Herrmann, *Statistical independence of a new class of inversive congruential pseudorandom numbers*, Math. Comp. 60 (1993), 375–384.

[4] C. J. Moreno and O. Moreno, *Exponential sums and Goppa codes: I*, Proc. Amer. Math. Soc. 111 (1991), 523–531.

[5] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, 1992.

[6] —, *New methods for pseudorandom number and pseudorandom vector generation*, in: Proc. 1992 Winter Simulation Conference (Arlington, Va., 1992), IEEE Press, Piscataway, N.J., 1992, 264–269.

[7] —, *On a new class of pseudorandom numbers for simulation methods*, J. Comput. Appl. Math., to appear.

FACHBEREICH MATHEMATIK
TECHNISCHE HOCHSCHULE DARMSTADT
SCHLOSSGARTENSTRASSE 7
D-64289 DARMSTADT, GERMANY

INSTITUT FÜR INFORMATIONS-
VERARBEITUNG
ÖSTERREICHISCHE AKADEMIE
DER WISSENSCHAFTEN
SONNENFELSGASSE 19
A-1010 WIEN, AUSTRIA
E-mail: NIED@QIINFO.OEAW.AC.AT

Received on 13.12.1993 (2540)