ACTA ARITHMETICA
XCIII.4 (2000)

Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators

by

Harald Niederreiter and Arne Winterhof (Wien)

1. Introduction. Let $\mathbb{F}_q$ be the finite field of order $q = p^k$ with a prime p and an integer $k \ge 1$. Further let $\{\beta_1, \ldots, \beta_k\}$ be an ordered basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Define ξ_n, $n = 0, 1, \ldots, q-1$, by

$$\xi_n = n_1\beta_1 + \ldots + n_k\beta_k \tag{1}$$

if

$$n = n_1 + n_2 p + \ldots + n_k p^{k-1}, \qquad 0 \le n_i < p,\ i = 1, \ldots, k,$$

and note that $\xi_0, \xi_1, \ldots, \xi_{q-1}$ run exactly through all elements of $\mathbb{F}_q$. We obtain the sequence $\xi_0, \xi_1, \ldots$ by extending with period q ($\xi_{n+q} = \xi_n$). Moreover, let

$$\overline{\gamma} = \begin{cases} \gamma^{-1} & \text{if } \gamma \in \mathbb{F}_q^*, \\ 0 & \text{if } \gamma = 0. \end{cases}$$

For given $\alpha \in \mathbb{F}_q^*$, $\beta \in \mathbb{F}_q$, we generate a sequence $\gamma_0, \gamma_1, \ldots$ of elements of $\mathbb{F}_q$ by

$$\gamma_n = \overline{\alpha\xi_n + \beta} \qquad \text{for } n = 0, 1, \ldots \tag{2}$$

We study exponential sums over $\mathbb{F}_q$ which in the simplest case are of the form

$$\sum_{n=0}^{N-1} \chi(\gamma_n) \qquad \text{for } 1 \le N \le q,$$

where χ is a nontrivial additive character of $\mathbb{F}_q$. Upper bounds for these exponential sums are then applied to the analysis of two new inversive methods for pseudorandom number and vector generation. These new methods are defined as follows. If

$$\gamma_n = c_n^{(1)}\beta_1 + c_n^{(2)}\beta_2 + \ldots + c_n^{(k)}\beta_k \qquad \text{with all } c_n^{(i)} \in \mathbb{F}_p, \tag{3}$$

2000 *Mathematics Subject Classification*: 11K38, 11K45, 11T23, 65C10.

then we derive *digital explicit inversive pseudorandom numbers* in the interval $[0,1)$ by putting

$$y_n = \sum_{j=1}^{k} c_n^{(j)} p^{-j}$$

and *explicit inversive pseudorandom vectors* by

$$\mathbf{u}_n = \frac{1}{p}(c_n^{(1)}, c_n^{(2)}, \ldots, c_n^{(k)}) \in [0,1)^k$$

for $n = 0, 1, \ldots$ It is trivial that the sequences $y_0, y_1, \ldots$ and $\mathbf{u}_0, \mathbf{u}_1, \ldots$ are purely periodic with period q. In the special case $k = 1$ we get the explicit inversive congruential pseudorandom numbers introduced in [2].

After some auxiliary results in Section 2 we prove some new bounds for incomplete exponential sums over finite fields in Section 3 which allow us to give nontrivial results on the distribution of sequences of digital explicit inversive pseudorandom numbers and explicit inversive pseudorandom vectors. The application to digital explicit inversive pseudorandom numbers is presented in Section 4 and to explicit inversive pseudorandom vectors in Section 5. In particular, we generalize the result of [2, Theorem 1] on the statistical properties over the full period of pseudorandom numbers generated by the explicit inversive congruential method and present new results for statistical properties over parts of the period. Moreover, we extend the range for nontrivial results using the method of [9]–[11].

2. Auxiliary results. The following bound for exponential sums can be found in [5, Theorem 2].

Lemma 1. *Let χ be a nontrivial additive character of $\mathbb{F}_q$ and let f/g be a rational function over $\mathbb{F}_q$. Let v be the number of distinct roots of the polynomial g in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. Suppose that f/g is not of the form $A^p - A$, where A is a rational function over $\overline{\mathbb{F}}_q$. Then*

$$\Bigg| \sum_{\xi \in \mathbb{F}_q,\, g(\xi) \neq 0} \chi\bigg(\frac{f(\xi)}{g(\xi)}\bigg) \Bigg| \le (\max(\deg(f), \deg(g)) + v^* - 2) q^{1/2} + \delta,$$

where $v^* = v$ and $\delta = 1$ if $\deg(f) \le \deg(g)$, *and $v^* = v + 1$ and $\delta = 0$ otherwise.*

Lemma 2. *Let f/g be a rational function over $\mathbb{F}_q$ such that g is not divisible by the pth power of a nonconstant polynomial over $\overline{\mathbb{F}}_q$, $f \neq 0$, and* $\deg(f) - \deg(g) \not\equiv 0 \bmod p$ *or* $\deg(f) < \deg(g)$. *Then f/g is not of the form $A^p - A$, where A is a rational function over $\overline{\mathbb{F}}_q$.*

Proof. Suppose we had

$$\frac{f}{g} = \left(\frac{b}{c}\right)^p - \frac{b}{c},$$

where $b, c \in \overline{\mathbb{F}}_q[x]$ and $\gcd(b,c) = 1$. Then

$$c^p f = (b^{p-1} - c^{p-1})bg.$$

From $\gcd(b,c) = 1$ it follows that c^p divides g. This divisibility relation can hold only if c is a nonzero constant. Thus,

$$f = (\omega_1 b^p + \omega_2 b)g$$

for suitable $\omega_1, \omega_2 \in \overline{\mathbb{F}}_q$ with $\omega_1\omega_2 \neq 0$. This implies that $\deg(f) - \deg(g)$ is a multiple of p and $\deg(f) \geq \deg(g)$, which is a contradiction. ■

Lemma 3. *Let χ be a nontrivial additive character of $\mathbb{F}_q$, N be an integer with $1 \leq N \leq q$, and ξ_n be defined as in* (1) *for $n = 0, \ldots, N-1$. Then*

$$\sum_{\mu \in \mathbb{F}_q^*} \Big| \sum_{n=0}^{N-1} \chi(\mu\xi_n) \Big| \leq ql\left(\frac{4}{\pi^2}\log p + 1.38\right) + N(p^{k-l} - 1),$$

where $l = \lceil (\log N)/\log p \rceil$.

Proof. We proceed as in [12, Section 3]. For $j = 0, \ldots, l-1$ define

$$M_j = \{\mu \in \mathbb{F}_q^* \mid \chi(\mu\beta_1) = \ldots = \chi(\mu\beta_j) = 1,\ \chi(\mu\beta_{j+1}) \neq 1\}$$

and

$$M_l = \{\mu \in \mathbb{F}_q^* \mid \chi(\mu\beta_1) = \ldots = \chi(\mu\beta_l) = 1\}.$$

Then we can write

$$\begin{aligned}\sum_{\mu \in \mathbb{F}_q^*} \Big| \sum_{n=0}^{N-1} \chi(\mu\xi_n) \Big| &= \sum_{j=0}^{l} \sum_{\mu \in M_j} \Big| \sum_{n=0}^{N-1} \chi(\mu\xi_n) \Big| \\ &= \sum_{j=0}^{l-1} \sum_{\mu \in M_j} \Big| \sum_{n=0}^{N-1} \chi(\mu\xi_n) \Big| + N(p^{k-l} - 1).\end{aligned}$$

Now we fix $\mu \in M_j$, $0 \leq j \leq l-1$, and consider the sum

$$\sum_{n=0}^{N-1} \chi(\mu\xi_n).$$

For $0 \leq n \leq N-1$ we have

$$\xi_n = n_1\beta_1 + \ldots + n_l\beta_l, \qquad 0 \leq n_i < p,\ 1 \leq i \leq l,$$

where $n = n_1 + n_2 p + \ldots + n_l p^{l-1}$. This yields

$$\chi(\mu\xi_n) = \chi(\mu\beta_{j+1})^{n_{j+1}} \ldots \chi(\mu\beta_l)^{n_l}$$

with $\chi(\mu\beta_{j+1}) \neq 1$. We write

$$N-1 = r_1 + r_2 p + \ldots + r_l p^{l-1}, \qquad 0 \le r_i < p,\ 1 \le i \le l.$$

If $j \le l-2$ and $(n_{j+2}, \ldots, n_l) \neq (r_{j+2}, \ldots, r_l)$, then by fixing

$$n_1, \ldots, n_j, n_{j+2}, \ldots, n_l$$

and summing $\chi(\mu\xi_n)$ over $n_{j+1} = 0, 1, \ldots, p-1$ we get 0. Therefore, in the range of summation $n = 0, 1, \ldots, N-1$ we are left with the terms $\chi(\mu\xi_n)$ for which $(n_{j+2}, \ldots, n_l) = (r_{j+2}, \ldots, r_l)$. Thus,

$$\Big|\sum_{n=0}^{N-1} \chi(\mu\xi_n)\Big| = \Big|\sum_{n_1,\ldots,n_{j+1}} \chi(\mu\beta_{j+1})^{n_{j+1}}\Big|, \tag{4}$$

where the last sum is over all $n_1, \ldots, n_{j+1}$ with

$$n_1 + n_2 p + \ldots + n_{j+1} p^j \le r_1 + r_2 p + \ldots + r_{j+1} p^j.$$

The identity (4) holds trivially for $j = l-1$ as well. If $r_{j+1} \neq 0$, then by (4) we obtain

$$\Big|\sum_{n=0}^{N-1} \chi(\mu\xi_n)\Big| \le p^j \Big|\sum_{n_{j+1}=0}^{r_{j+1}-1} \chi(\mu\beta_{j+1})^{n_{j+1}}\Big| + p^j = p^j \left|\frac{\chi(r_{j+1}\mu\beta_{j+1}) - 1}{\chi(\mu\beta_{j+1}) - 1}\right| + p^j,$$

and this holds trivially for $r_{j+1} = 0$ as well. For fixed $0 \le j \le l-1$ this yields

$$\begin{aligned}\sum_{\mu \in M_j} \Big|\sum_{n=0}^{N-1} \chi(\mu\xi_n)\Big| &\le p^j p^{k-j-1} \sum_{u=1}^{p-1} \left|\frac{\sin(\pi r_{j+1} u/p)}{\sin(\pi u/p)}\right| + p^j p^{k-j-1}(p-1) \\ &\le p^{k-1}\left(\frac{4}{\pi^2} p \log p + 0.38p + 0.7\right) + p^{k-1}(p-1),\end{aligned}$$

where we used [12, Lemma 5] in the first step and [1, Theorem 1] in the second step. Simple calculations yield the lemma. ∎

Let $C(p)$ denote the set of integers h with $-p/2 < h \le p/2$ and let $C_k(p)$ be the set of k-dimensional points $(h_1, \ldots, h_k)$ with $h_j \in C(p)$ for $1 \le j \le k$. For $(h_1, \ldots, h_k) \in C_k(p)$ we put $Q_p(h_1, \ldots, h_k) = 1$ if $(h_1, \ldots, h_k) = \mathbf{0}$ and

$$Q_p(h_1, \ldots, h_k) = p^{-d} \csc \frac{\pi}{p}|h_d| \quad \text{ if } (h_1, \ldots, h_k) \neq \mathbf{0},$$

where $d = d(h_1, \ldots, h_k)$ is the largest j with $h_j \neq 0$. Let $C^*_{s\times k}(p)$ be the set of all nonzero $s \times k$ matrices with entries in $C(p)$. For $H = (h_{ij}) \in C^*_{s\times k}(p)$ we define

$$W_p(H) = \prod_{i=1}^{s} Q_p(h_{i1}, \ldots, h_{ik}).$$

The following lemma is obtained by using [6, Lemma 3.13] for $p = 2$ and an inequality in the proof of [8, Theorem 2] for $p > 2$.

LEMMA 4. *For any $s \geq 1$ and $k \geq 1$ we have*

$$\sum_{H \in C^*_{s\times k}(2)} W_2(H) < \left(\frac{k}{2} + 1\right)^s,$$

$$\sum_{H \in C^*_{s\times k}(p)} W_p(H) < \left(\frac{2}{\pi} k \log p + \frac{2}{5} k + 1\right)^s \qquad \textit{if } p > 2.$$

The following lemma is needed in the proof of Theorem 3 in Section 3. For nonnegative integers n and i we define $n \oplus i$ by

$$n \oplus i = j \Leftrightarrow \xi_n + \xi_i = \xi_j; \qquad 0 \leq j < q. \tag{5}$$

LEMMA 5. *For given integers L and m with $0 \leq L, m < q$, the number of integers n with $0 \leq n \leq L$ for which $n \oplus m > L$ is at most m. Furthermore, the number of integers n with $0 \leq n \leq L$ which are not of the form $r \oplus m$ for some $0 \leq r \leq L$ is at most m.*

Proof. Note that for $0 \leq n < q$ we can obtain $n \oplus m$ by adding the digit vectors (in base p) of n and m as elements of the vector space $\mathbb{F}_p^k$ and then identifying the resulting digit vector with the corresponding integer in the interval $[0, q)$. Thus, for $0 \leq n \leq L$ we have

$$n \oplus m \leq n + m \leq L + m.$$

Since $n' \oplus m \neq n'' \oplus m$ for $0 \leq n' < n'' < q$, the numbers $L+1, L+2, \ldots, L+m$ can appear as values of $n \oplus m$ for at most m values of n with $0 \leq n \leq L$. The second part is shown in a similar way. ∎

3. Bounds for exponential sums.

Let $\gamma_0, \gamma_1, \ldots$ be the sequence of elements of $\mathbb{F}_q$ generated by (2) and (1). For a nontrivial additive character χ of $\mathbb{F}_q$, for $\mu_0, \mu_1, \ldots, \mu_{s-1} \in \mathbb{F}_q$, and for an integer N with $1 \leq N \leq q$ we consider the exponential sums

$$S_N = \sum_{n=0}^{N-1} \chi\Big(\sum_{i=0}^{s-1} \mu_i \gamma_{n\oplus i}\Big),$$

where $\oplus$ is defined by (5).

THEOREM 1. *If $\mu_0, \mu_1, \ldots, \mu_{s-1}$ are not all* 0, *then*

$$|S_q| \leq (2s-2)q^{1/2} + s + 1.$$

Proof. We can assume that $s < q$ since otherwise the result is trivial. Then we have

$$|S_q| = \Big|\sum_{\xi\in\mathbb{F}_q}\chi\Big(\sum_{i=0}^{s-1}\mu_i\overline{\alpha(\xi+\xi_i)+\beta}\Big)\Big| \le s + \Big|\sum_{\xi\in\mathbb{F}_q,\,g(\xi)\neq 0}\chi\Big(\frac{f(\xi)}{g(\xi)}\Big)\Big|,$$

where

$$f(x) = \sum_{i=0}^{s-1}\mu_i\prod_{j=0,j\neq i}^{s-1}(\alpha(x+\xi_j)+\beta)$$

and

$$g(x) = \prod_{j=0}^{s-1}(\alpha(x+\xi_j)+\beta).$$

Since at least one μ_i is nonzero, the uniqueness of the partial fraction decomposition for rational functions implies that $f \neq 0$. Since $\deg(f) < \deg(g)$, Lemmas 1 and 2 yield the result. ■

The proof of Theorem 1 does not use the special ordering (1) of the elements of $\mathbb{F}_q$. An arbitrary but fixed ordering would be sufficient. But for $N < q$, the case treated in the next theorem, we need (1).

THEOREM 2. *If* $\mu_0,\mu_1,\ldots,\mu_{s-1}$ *are not all* 0, *then*

$$|S_N| < s(2q^{1/2}+1)\Big(\frac{4}{\pi^2}\log p^l + 1.38l + 1\Big) \qquad \textit{for } 1 \le N < q,$$

where $l = \lceil(\log N)/\log p\rceil$.

Proof. We can again assume that $s < q$. With $\sigma_n = \sum_{i=0}^{s-1}\mu_i\gamma_{n\oplus i}$ we have

$$\begin{aligned}
S_N &= \sum_{n=0}^{q-1}\chi(\sigma_n)\sum_{t=0}^{N-1}\frac{1}{q}\sum_{\mu\in\mathbb{F}_q}\chi(\mu(\xi_n-\xi_t))\\
&= \frac{1}{q}\sum_{\mu\in\mathbb{F}_q}\Big(\sum_{t=0}^{N-1}\chi(-\mu\xi_t)\Big)\Big(\sum_{n=0}^{q-1}\chi(\sigma_n+\mu\xi_n)\Big)\\
&= \frac{N}{q}\sum_{n=0}^{q-1}\chi(\sigma_n) + \frac{1}{q}\sum_{\mu\in\mathbb{F}_q^*}\Big(\sum_{t=0}^{N-1}\chi(-\mu\xi_t)\Big)\Big(\sum_{n=0}^{q-1}\chi(\sigma_n+\mu\xi_n)\Big),
\end{aligned}$$

and so

$$|S_N| \le \frac{N}{q}|S_q| + \frac{1}{q}\sum_{\mu\in\mathbb{F}_q^*}\Big|\sum_{t=0}^{N-1}\chi(\mu\xi_t)\Big|\cdot\Big|\sum_{n=0}^{q-1}\chi(\sigma_n+\mu\xi_n)\Big|.$$

For $\mu \in \mathbb{F}_q^*$ we have

$$\Big|\sum_{n=0}^{q-1} \chi(\sigma_n + \mu\xi_n)\Big| = \Big|\sum_{\xi\in\mathbb{F}_q} \chi\Big(\sum_{i=0}^{s-1} \mu_i \overline{\alpha(\xi+\xi_i)+\beta} + \mu\xi\Big)\Big|$$
$$\le s + \Big|\sum_{\xi\in\mathbb{F}_q,\, g(\xi)\ne 0} \chi\Big(\frac{f(\xi)}{g(\xi)}\Big)\Big|,$$

where

$$f(x) = \mu x \prod_{j=0}^{s-1}(\alpha(x+\xi_j)+\beta) + \sum_{i=0}^{s-1} \mu_i \prod_{j=0,\, j\ne i}^{s-1} (\alpha(x+\xi_j)+\beta)$$

and

$$g(x) = \prod_{j=0}^{s-1}(\alpha(x+\xi_j)+\beta).$$

Lemmas 1–3 yield

$$\sum_{\mu\in\mathbb{F}_q^*} \Big|\sum_{t=0}^{N-1} \chi(\mu\xi_t)\Big| \cdot \Big|\sum_{n=0}^{q-1} \chi(\sigma_n + \mu\xi_n)\Big|$$
$$\le s(2q^{1/2}+1) \sum_{\mu\in\mathbb{F}_q^*} \Big|\sum_{t=0}^{N-1} \chi(\mu\xi_t)\Big|$$
$$\le s(2q^{1/2}+1)\Big(ql\Big(\frac{4}{\pi^2}\log p + 1.38\Big) + N(p^{k-l}-1)\Big),$$

where $l = \lceil(\log N)/\log p\rceil$. Hence we obtain, by Theorem 1,

$$|S_N| \le \frac{N}{q}((2s-2)q^{1/2}+s+1)$$
$$+ s(2q^{1/2}+1)\Big(\frac{4}{\pi^2}\log p^l + 1.38l + N(p^{-l}-p^{-k})\Big).$$

Simple calculations yield the theorem. ∎

Theorem 2 is nontrivial only if N is at least of the order of magnitude $sq^{1/2}\log q$. Now we prove a bound which is nontrivial for N at least of the order of magnitude $sq^{1/2}$ using a new method introduced in [9] and extended in [10] and [11].

Theorem 3. *If* $\mu_0, \mu_1, \ldots, \mu_{s-1}$ *are not all* 0, *then*

$$|S_N| < \sqrt{5}s^{1/2}N^{1/2}q^{1/4} + q^{1/2} + 1 \quad \textit{for } 1 \le N < q.$$

Proof. We can assume that $2s+1 \le 2q^{1/2}$ since otherwise the result is trivial. With $\sigma_n = \sum_{i=0}^{s-1} \mu_i\gamma_{n\oplus i}$ and any integer m with $0 \le m < q$ we have, by Lemma 5,

$$\Big|S_N - \sum_{n=0}^{N-1} \chi(\sigma_{n\oplus m})\Big| \le 2m.$$

For an integer M with $1 \le M \le q$ we use the above inequality for $m = 0, 1, \ldots, M-1$ and we get

$$M|S_N| < W + M^2, \tag{6}$$

where

$$W = \Big|\sum_{n=0}^{N-1}\sum_{m=0}^{M-1} \chi(\sigma_{n\oplus m})\Big| \le \sum_{n=0}^{N-1}\Big|\sum_{m=0}^{M-1}\chi(\sigma_{n\oplus m})\Big|.$$

By the Cauchy–Schwarz inequality we obtain

$$\begin{aligned}W^2 &\le N\sum_{n=0}^{N-1}\Big|\sum_{m=0}^{M-1}\chi(\sigma_{n\oplus m})\Big|^2 \le N\sum_{\xi\in\mathbb{F}_q}\Big|\sum_{m=0}^{M-1}\chi\Big(\sum_{i=0}^{s-1}\mu_i\overline{\alpha(\xi+\xi_i+\xi_m)+\beta}\Big)\Big|^2\\ &= N\sum_{m_1,m_2=0}^{M-1}\sum_{\xi\in\mathbb{F}_q}\chi\Big(\sum_{i=0}^{s-1}\mu_i(\overline{\alpha(\xi+\xi_i+\xi_{m_1})+\beta} - \overline{\alpha(\xi+\xi_i+\xi_{m_2})+\beta})\Big).\end{aligned}$$

If $m_1 = m_2$, then the sum over ξ is equal to q. For $m_1 \ne m_2$ let

$$f(x) = \alpha(\xi_{m_2} - \xi_{m_1})\sum_{i=0}^{s-1}\mu_i\prod_{j=0,\, j\ne i}^{s-1}(\alpha(x+\xi_j+\xi_{m_1})+\beta)(\alpha(x+\xi_j+\xi_{m_2})+\beta)$$

and

$$g(x) = \prod_{j=0}^{s-1}(\alpha(x+\xi_j+\xi_{m_1})+\beta)(\alpha(x+\xi_j+\xi_{m_2})+\beta).$$

Then

$$\begin{aligned}&\Big|\sum_{\xi\in\mathbb{F}_q}\chi\Big(\sum_{i=0}^{s-1}\mu_i(\overline{\alpha(\xi+\xi_i+\xi_{m_1})+\beta} - \overline{\alpha(\xi+\xi_i+\xi_{m_2})+\beta})\Big)\Big|\\ &\qquad\qquad\le 2s + \Big|\sum_{\xi\in\mathbb{F}_q,\, g^*(\xi)\ne 0}\chi\Big(\frac{f^*(\xi)}{g^*(\xi)}\Big)\Big|,\end{aligned}$$

where $f^* = f/(f,g)$ and $g^* = g/(f,g)$. For the application of Lemmas 1 and 2 we need that g^* is squarefree ($p = 2$!) and $f^* \ne 0$.

In $g(x)$ we can have repetition of factors only if there exist $0 \le i, j \le s-1$ with $i \ne j$ such that

$$\xi_i + \xi_{m_1} = \xi_j + \xi_{m_2}. \tag{7}$$

Then $\alpha(x+\xi_i+\xi_{m_1})+\beta$ is a common factor of f and g. Hence g^* is squarefree.

Suppose we have $f^* = 0$. Let i be an index with $\mu_i \neq 0$. Then

$$\begin{aligned}0 &= f^*(-\alpha^{-1}\beta - \xi_i - \xi_{m_1}) = f(-\alpha^{-1}\beta - \xi_i - \xi_{m_1})\\ &= \alpha(\xi_{m_2} - \xi_{m_1})\mu_i \prod_{j=0,\, j\neq i}^{s-1} \alpha(\xi_j - \xi_i)\alpha(\xi_j - \xi_i + \xi_{m_2} - \xi_{m_1})\end{aligned}$$

yields the existence of $0 \le j \le s-1$, $i \neq j$, satisfying (7). There are at most $s-1$ possible indices $m_2 \neq m_1$ satisfying (7) for given m_1 and i. For these m_2 we estimate trivially.

By Lemmas 1 and 2 we obtain

$$W^2 \le N(Msq + M^2((4s-2)q^{1/2} + 2s + 1)) \le N(Msq + 4M^2 sq^{1/2}).$$

Choosing $M = \lceil q^{1/2} \rceil$ we get

$$W^2/M^2 \le 5sNq^{1/2},$$

and thus

$$|S_N| < \sqrt{5} s^{1/2} N^{1/2} q^{1/4} + q^{1/2} + 1$$

by (6). ■

4. Digital explicit inversive pseudorandom numbers. We use the bounds for exponential sums obtained in the previous section to derive results on the distribution of sequences of digital explicit inversive pseudorandom numbers over the full period and in parts of the period.

Given a sequence $y_0, y_1, \ldots$ of digital explicit inversive pseudorandom numbers and a dimension $s \ge 1$, we consider the points

$$\mathbf{y}_n = (y_n, y_{n\oplus 1}, \ldots, y_{n\oplus(s-1)}) \in [0,1)^s \quad \text{for } n = 0, 1, \ldots$$

Then for any integer N with $1 \le N \le q$ we define the *star discrepancy*

$$D_N^{*(s)} = \sup_J |F_N(J) - V(J)|,$$

where the supremum is extended over all subintervals J of $[0,1)^s$ containing the origin, $F_N(J)$ is N^{-1} times the number of points among $\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{N-1}$ falling into J, and $V(J)$ denotes the s-dimensional volume of J. In the following we establish an upper bound for $D_N^{*(s)}$.

THEOREM 4. *For any sequence of digital explicit inversive pseudorandom numbers, for any dimension $s \ge 1$, and for any $1 \le N < q$ the star discrepancy $D_N^{*(s)}$ satisfies*

$$D_N^{*(s)} = O(\min(N^{-1}q^{1/2}\log q, N^{-1/2}q^{1/4})(\log q)^s).$$

Proof. For $H = (h_{ij}) \in C^*_{s\times k}(p)$ we define the exponential sum

$$S_N(H) = \sum_{n=0}^{N-1} e\biggl(\frac{1}{p}\sum_{i=0}^{s-1}\sum_{j=1}^{k} h_{ij}c_{n\oplus i}^{(j)}\biggr),$$

where $e(u) = \exp(2\pi\sqrt{-1}u)$ for all real u and the $c_{n\oplus i}^{(j)} \in \mathbb{F}_p$ are as in (3). Then by a general discrepancy bound in [3, Theorem 1(ii) and Lemma 3(iii)] (see also [6, Theorem 3.12] for a slightly weaker version) we obtain

$$D_N^{*(s)} \le 1 - \biggl(1-\frac{1}{q}\biggr)^s + \frac{1}{N}\sum_{H\in C^*_{s\times k}(p)} W_p(H)|S_N(H)|. \tag{8}$$

Let $\{\delta_1,\ldots,\delta_k\}$ be the dual basis of the given ordered basis $\{\beta_1,\ldots,\beta_k\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then by a well-known principle (see [4, p. 55]) we have

$$c_n^{(j)} = \mathrm{Tr}(\delta_j\gamma_n) \quad \text{for } 1\le j\le k \text{ and } n\ge 0,$$

where Tr denotes the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$. Therefore

$$\begin{aligned} S_N(H) &= \sum_{n=0}^{N-1} e\biggl(\frac{1}{p}\sum_{i=0}^{s-1}\sum_{j=1}^{k} h_{ij}\,\mathrm{Tr}(\delta_j\gamma_{n\oplus i})\biggr) \\ &= \sum_{n=0}^{N-1} e\biggl(\frac{1}{p}\,\mathrm{Tr}\Bigl(\sum_{i=0}^{s-1}\sum_{j=1}^{k} h_{ij}\delta_j\gamma_{n\oplus i}\Bigr)\biggr) = \sum_{n=0}^{N-1}\chi\Bigl(\sum_{i=0}^{s-1}\mu_i\gamma_{n\oplus i}\Bigr), \end{aligned}$$

where χ is the canonical additive character of $\mathbb{F}_q$ and $\mu_i = \sum_{j=1}^{k} h_{ij}\delta_j \in \mathbb{F}_q$ for $0\le i\le s-1$. Since H is not the zero matrix and $\{\delta_1,\ldots,\delta_k\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, it follows that $\mu_0,\ldots,\mu_{s-1}$ are not all 0. Hence we may apply the results of Section 3.

We have by (8), Theorem 2, Theorem 3, and Lemma 4,

$$\begin{aligned} D_N^{*(s)} &< \frac{s}{q} + \frac{1}{N}\biggl(\frac{k}{2}+1\biggr)^s \\ &\quad\times \min\biggl(s(2q^{1/2}+1)\biggl(\frac{4}{\pi^2}\log p^l + 1.38l + 1\biggr), \sqrt{5}s^{1/2}N^{1/2}q^{1/4} + q^{1/2} + 1\biggr) \end{aligned}$$

if $p = 2$, and

$$\begin{aligned} D_N^{*(s)} &< \frac{s}{q} + \frac{1}{N}\biggl(\frac{2}{\pi}\log q + \frac{2}{5}k + 1\biggr)^s \\ &\quad\times \min\biggl(s(2q^{1/2}+1)\biggl(\frac{4}{\pi^2}\log p^l + 1.38l + 1\biggr), \sqrt{5}s^{1/2}N^{1/2}q^{1/4} + q^{1/2} + 1\biggr) \end{aligned}$$

if $p > 2$. ■

Theorem 5. *For any sequence of digital explicit inversive pseudorandom numbers and for any dimension $s \ge 1$ the star discrepancy $D_q^{*(s)}$ satisfies*

$$D_q^{*(s)} = O(q^{-1/2}(\log q)^s).$$

Proof. The theorem follows by (8), Theorem 1, and Lemma 4 with the same arguments as in the proof of the previous theorem. ■

5. Explicit inversive pseudorandom vectors. Statistical independence properties of pseudorandom vectors are customarily assessed by the discrete discrepancy (see [6, Section 10.2]). Given a sequence $\mathbf{u}_0, \mathbf{u}_1, \ldots$ of explicit inversive pseudorandom vectors and an integer $s \ge 1$, we consider the ks-dimensional points

$$\mathbf{v}_n = (\mathbf{u}_n, \mathbf{u}_{n\oplus 1}, \ldots, \mathbf{u}_{n\oplus(s-1)}) \in [0,1)^{ks} \quad \text{for } n = 0, 1, \ldots$$

Then for any integer N with $1 \le N \le q$ we define the *discrete discrepancy*

$$E_{N,p}^{(s)} = \max_J |F_N(J) - V(J)|,$$

where the maximum is over all subintervals J of $[0,1)^{ks}$ of the form

$$J = \prod_{i=1}^{ks} \left[\frac{a_i}{p}, \frac{b_i}{p}\right)$$

with integers a_i, b_i for $1 \le i \le ks$, where $F_N(J)$ is N^{-1} times the number of points $\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{N-1}$ falling into J and $V(J)$ denotes the ks-dimensional volume of J.

Theorem 6. *For any sequence of k-dimensional inversive pseudorandom vectors, for any $s \ge 1$, and for any $1 \le N < q = p^k$ the discrete discrepancy $E_{N,p}^{(s)}$ satisfies*

$$E_{N,p}^{(s)} = O(\min(N^{-1}q^{1/2}\log q, N^{-1/2}q^{1/4})(\log p)^{ks}).$$

Proof. Let $C_{ks}^*(p)$ be the set of nonzero vectors in $C_{ks}(p)$. For $\mathbf{h} \in C_{ks}^*(p)$ we define the exponential sum

$$S_N(\mathbf{h}) = \sum_{n=0}^{N-1} e(\mathbf{h}\cdot\mathbf{v}_n),$$

where the dot denotes the standard inner product. By [7, Corollary 3] we get

$$E_{N,p}^{(s)} \le \frac{1}{N} \max_{\mathbf{h}\in C_{ks}^*(p)} |S_N(\mathbf{h})| \left(\frac{4}{\pi^2}\log p + 1.41 + \frac{0.61}{p}\right)^{ks}.$$

For a fixed $\mathbf{h} \in C^*_{ks}(p)$ we write

$$\mathbf{h} = (\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{s-1})$$

with $\mathbf{h}_i \in C_k(p)$ for $0 \le i \le s-1$, where not all $\mathbf{h}_i$ are $\mathbf{0}$. Then we have

$$S_N(\mathbf{h}) = \sum_{n=0}^{N-1} e\Big(\sum_{i=0}^{s-1} \mathbf{h}_i \cdot \mathbf{u}_{n\oplus i}\Big) = \sum_{n=0}^{N-1} e\bigg(\frac{1}{p}\sum_{i=0}^{s-1}\sum_{j=1}^{k} h_{ij} c^{(j)}_{n\oplus i}\bigg),$$

where $\mathbf{h}_i = (h_{i1}, \ldots, h_{ik})$ for $0 \le i \le s-1$ and all $h_{ij} \in C(p)$. As in the proof of Theorem 4 we get

$$S_N(\mathbf{h}) = \sum_{n=0}^{N-1} \chi\Big(\sum_{i=0}^{s-1} \mu_i \gamma_{n\oplus i}\Big)$$

and thus the result. ■

THEOREM 7. *For any sequence of k-dimensional inversive pseudorandom vectors and for any $s \ge 1$ the discrete discrepancy $E^{(s)}_{q,p}$ with $q = p^k$ satisfies*

$$E^{(s)}_{q,p} = O(q^{-1/2}(\log p)^{ks}).$$

Proof. The theorem follows with the same arguments as in the proof of the previous theorem by Theorem 1. ■

References

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

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

[3] P. Hellekalek, *General discrepancy estimates: the Walsh function system*, Acta Arith. 67 (1994), 209–218.

[4] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, revised ed., Cambridge Univ. Press, Cambridge, 1994.

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

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

[7] —, *Pseudorandom vector generation by the inversive method*, ACM Trans. Modeling and Computer Simulation 4 (1994), 191–212.

[8] —, *Improved bounds in the multiple-recursive matrix method for pseudorandom number and vector generation*, Finite Fields Appl. 2 (1996), 225–240.

[9] H. Niederreiter and I. E. Shparlinski, *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, Math. Comp., to appear.

[10] —, —, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers*, Finite Fields Appl. 5 (1999), 246–253.

[11] —, —, *On the distribution of pseudorandom numbers and vectors generated by inversive methods*, Appl. Algebra Engrg. Comm. Comput., to appear.

[12] A. Winterhof, *On the distribution of powers in finite fields*, Finite Fields Appl. 4 (1998), 43–54.

Institute of Discrete Mathematics
Austrian Academy of Sciences
Sonnenfelsgasse 19
A-1010 Wien, Austria
E-mail: niederreiter@oeaw.ac.at
arne.winterhof@oeaw.ac.at

Received on 3.12.1999 (3722)