MATHEMATICS OF COMPUTATION
Volume 80, Number 274, April 2011, Pages 1053–1061
S 0025-5718(2010)02408-1
Article electronically published on August 31, 2010

ON THE AVERAGE DISTRIBUTION OF PSEUDORANDOM NUMBERS GENERATED BY NONLINEAR PERMUTATIONS

IGOR E. SHPARLINSKI

Abstract. We modify the approach of H. Niederreiter and I. E. Shparlinski and improve one of their results on the distribution of inversive congruential pseudorandom numbers over a finite field for almost all initial values. However the main application of the new method is a similar result for pseudorandom numbers generated by iterations of a nonlinear permutation polynomial over a finite field, to which the original approach of H. Niederreiter and I. E. Shparlinski does not apply.

1. Introduction

Let p be a prime and let $\mathbb{F}_p$ be the field of p elements, which we assume to be represented by the set $\{0, \ldots, p-1\}$.

Given a map $\psi : \mathbb{F}_p \to \mathbb{F}_p$ we define $u_0(\vartheta), u_1(\vartheta), \ldots$ as the sequence of elements of $\mathbb{F}_p$ obtained by the recurrence relation

$$u_{n+1}(\vartheta) = \psi\left(u_n(\vartheta)\right), \qquad n = 0, 1, \ldots, \tag{1}$$

where $u_0(\vartheta) = \vartheta$ is the *initial value*. Such sequences are very common sources of pseudorandom numbers and are also of interest for the theory of dynamical systems; see [8, 9, 11, 13] for recent surveys of such constructions and their properties.

In particular, the distribution of sequences of points

$$\left(\frac{u_n(\vartheta)}{p}, \ldots, \frac{u_{n+s-1}(\vartheta)}{p}\right), \qquad n = 0, \ldots, N-1, \tag{2}$$

in the s-dimensional unit cube $[0,1]^s$ has been of primal interest.

Here we concentrate on the special case when the map ψ is a *permutation* of $\mathbb{F}_p$.

A very important class of permutations is given by inversions,

$$\psi(\gamma) = \begin{cases} a\gamma^{-1} + b & \text{if } \gamma \neq 0, \\ b & \text{if } \gamma = 0, \end{cases} \tag{3}$$

where $a \in \mathbb{F}_p^*$, $b \in \mathbb{F}_p$. In this case the corresponding sequence (1) is called the inversive congruential generator and has been extensively studied in the literature; see [8, 9, 13].

It is shown in [7] that for almost all initial values ϑ, the points (2), generated by ψ as in (3), are rather uniformly distributed in $[0,1]^s$. Another important class of

Received by the editor July 9, 2009 and, in revised form, December 21, 2009.
2010 *Mathematics Subject Classification.* Primary 11K45, 11T23, 65C10.
Key words and phrases. Pseudorandom numbers, inversive congruential generator, permutation polynomial.
The author was supported in part by ARC Grant DP0881473.

permutations ψ is given by permutation polynomials of low degree. Unfortunately, the method of [7] does not seem to work in this case and so analogues of the results of [7] are not known. However, here we propose a different argument, which allows us to consider the case of nonlinear permutations, and in fact we also obtain an improvement of the result of [7] as well. These estimates for almost all initial values are much stronger and hold in a much wider range than those obtained for every initial value; see [6] and [10] for the case of inversive and polynomial generators, respectively.

We note that besides being of theoretical interest, such results that apply to almost all initial values are probably most relevant for practical applications of pseudorandom generators, in both cryptography and numerical analysis.

Throughout the paper, the implied constants in the symbols 'O' and '$\ll$' may occasionally, where obvious, depend on some integer parameters d, r and s, and are absolute otherwise (we recall that $A \ll B$ is equivalent to $A = O(B)$).

2. Preparations

2.1. **Iterations of ψ.**

Let ψ^i denote the ith iterate of the permutation ψ, where ψ^0 denotes the identity map. In particular, we see from (1) that

$$u_i(\vartheta) = \psi^i(\vartheta), \qquad i = 0, 1, \ldots .$$

If ψ is given by a polynomial of degree d, then ψ^i is a polynomial of degree d^i, and thus all such iterations are pairwise distinct.

In the case that the permutation ψ is given by an inversion map (3), the situation is slightly more complicated.

As in [7], we consider the following sequence of rational functions over $\mathbb{F}_p$:

$$R_0(X) = X, \qquad R_i(X) = R_{i-1}(aX^{-1} + b), \qquad i = 1, 2, \ldots$$

associated with the map (3). It is obvious that this sequence is purely periodic. Denote by T the least period.

2.2. **Average values of some exponential sums.**

We write

$$\mathbf{e}_p(z) = \exp(2\pi i z/p).$$

For a permutation ψ of $\mathbb{F}_p$, a vector $\mathbf{h} = (h_0, \ldots, h_{s-1}) \in \mathbb{F}_p^s$ and integers $r, M \geq 1$, we define

$$V_{r,\mathbf{h},\psi}(M) = \sum_{\vartheta \in \mathbb{F}_p} \left| \sum_{m=0}^{M-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{m+j}(\vartheta) \right) \right|^{2r}.$$

In the case of $r = 1$ and the inversion map (3), such (and in fact more general) sums are estimated in [7]. In particular, a special case of [7, Lemma 1] implies the following estimate:

Lemma 1. *Assume that the permutation ψ is given by* (3) *with $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. Then for any integer M with $1 \leq M \leq T$ and nonzero vector $\mathbf{h} = (h_0, \ldots, h_{s-1}) \in \mathbb{F}_p^s$ we have*

$$V_{1,\mathbf{h},\psi}(M) \ll \begin{cases} Mp & \text{if } M \leq p^{1/2}, \\ M^2 p^{1/2} & \text{if } M > p^{1/2}. \end{cases}$$

We now use the same approach as in [7] to obtain a similar (albeit much weaker) result in the case of permutation polynomials.

Lemma 2. *Assume that the permutation ψ is given by a permutation polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \geq 2$. Then there is a constant $c > 0$, depending only on r, d and s, such for any integer $M \geq 1$ and nonzero vector $\mathbf{h} = (h_0, \dots, h_{s-1}) \in \mathbb{F}_p^s$ we have*

$$V_{r,\mathbf{h},\psi}(M) \ll \begin{cases} M^r p, & \text{if } M < c \log p, \\ M^{2r} p (\log p)^{-r}, & \text{if } M \geq c \log p. \end{cases}$$

Proof. Expanding the inner sum and changing the order of summation, we obtain

$$V_{r,\mathbf{h},\psi}(M) \\ \leq \sum_{m_1,\dots,m_r=0}^{M-1} \sum_{n_1,\dots,n_r=0}^{M-1} \left| \sum_{\vartheta \in \mathbb{F}_p} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \left(\sum_{\nu=1}^{r} \left(\psi^{m_\nu + j}(\vartheta) - \psi^{n_\nu + j}(\vartheta) \right) \right) \right) \right|.$$

If the r-tuple $(m_1, \dots, m_r)$ is a permutation of $(n_1, \dots, n_r)$, then the sum over ϑ is equal to p. Otherwise we see that

$$\sum_{j=0}^{s-1} h_j \left(\sum_{\nu=1}^{r} \left(\psi^{m_\nu + j}(\vartheta) - \psi^{n_\nu + j}(\vartheta) \right) \right) \\ = \sum_{j=0}^{s-1} h_j \left(\sum_{\nu=1}^{r} \left(f_{m_\nu + j}(\vartheta) - f_{n_\nu + j}(\vartheta) \right) \right),$$

where $f_i(X) \in \mathbb{F}_p[X]$ is a polynomial of degree d^i. Therefore, in this case the polynomial

$$\sum_{j=0}^{s-1} h_j \left(\sum_{\nu=1}^{r} \left(f_{m_\nu + j}(X) - f_{n_\nu + j}(X) \right) \right) \in \mathbb{F}_p[X]$$

is an inconstant polynomial of degree at most d^{M+s-2}. Applying the Weil bound, see [4, Theorem 5.38], we derive

$$V_{r,\mathbf{h},\psi}(M) \leq r! M^r p + M^{2r} d^{M+s-2} p^{1/2}.$$

As in [7], we also observe that because ψ is a permutation, for any integer L and any real $\tau \geq 0$, we have

$$\begin{aligned} &\sum_{\vartheta \in \mathbb{F}_p} \left| \sum_{m=L}^{L+M-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{m+j}(\vartheta) \right) \right|^\tau \\ &\qquad = \sum_{\vartheta \in \mathbb{F}_p} \left| \sum_{m=0}^{M-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{m+j}(\psi^L(\vartheta)) \right) \right|^\tau \\ &\qquad = \sum_{\vartheta \in \mathbb{F}_p} \left| \sum_{m=0}^{M-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{m+j}(\vartheta) \right) \right|^\tau . \end{aligned} \tag{4}$$

In particular,

$$\sum_{\vartheta \in \mathbb{F}_p} \left| \sum_{n=L}^{L+M-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{n+j}(\vartheta) \right) \right|^{2r} = V_{r,\mathbf{h},\psi}(N).$$

Therefore, separating the inner sum into at most $M/K+1$ subsums of length at most K, for any integer $1 \le K \le M$ we have

$$\begin{aligned} V_{r,\mathbf{h},\psi}(M) &\ll \left(K^r p + K^{2r} d^{K+s-2} p^{1/2}\right) M^{2r} K^{-2r} \\ &= M^{2r}\left(pK^{-r} + d^{K+s-2} p^{1/2}\right). \end{aligned}$$

Thus, selecting $K = \min\{M, \lfloor c \log p \rfloor\}$ for an appropriate constant c, in particular such that

$$pK^{-r} \ge d^{K+s-2} p^{1/2},$$

we obtain the desired result. □

2.3. **Discrepancy.** For a sequence of N points

$$\Gamma = (\gamma_{0,n}, \ldots, \gamma_{s-1,n})_{n=1}^{N} \tag{5}$$

of the half-open interval $[0,1)^s$, denote by D_Γ its *discrepancy*, that is,

$$D_\Gamma = \sup_{B \subseteq [0,1)^s} \left| \frac{T_\Gamma(B)}{N} - |B| \right|,$$

where $T_\Gamma(B)$ is the number of points of the sequence Γ which hit the box

$$B = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0,1)^s$$

and the supremum is taken over all such boxes.

For a vector $\mathbf{h} = (h_0, \ldots, h_{s-1}) \in \mathbb{Z}^s$ we put

$$|\mathbf{h}| = \max_{j=0,\ldots,s-1} |h_j|, \qquad \rho(\mathbf{h}) = \prod_{j=0}^{s-1} \max\{|h_j|, 1\}. \tag{6}$$

We need the *Koksma–Szüsz inequality* [3, 12] (see also [2, Theorem 1.21]) for the discrepancy of a sequence of points of the s-dimensional unit cube, which we present in the following form.

Lemma 3. *For any integer $H \ge 1$, the discrepancy D_Γ of a sequence of points* (5) *satisfies*

$$D_\Gamma \ll \frac{1}{H} + \frac{1}{N} \sum_{0 < |\mathbf{h}| \le H} \frac{1}{\rho(\mathbf{h})} \left| \sum_{n=1}^{N} \exp\left(2\pi i \sum_{j=0}^{s-1} h_j \gamma_{j,n}\right) \right|,$$

where $|\mathbf{h}|$ and $\rho(\mathbf{h})$ are defined by (6) *and the sum is taken over all integer vectors*

$$\mathbf{h} = (h_0, \ldots, h_{s-1})$$

with $0 < |\mathbf{h}| \le H$.

3. Main results

3.1. **Notation.** For a permutation ψ, we denote by $D_{s,\psi}(\vartheta; N)$ the *s-dimensional discrepancy* of the points (2).

Our results show that for almost all $\vartheta \in \mathbb{F}_p$, the discrepancy $D_{s,\psi}(\vartheta; N)$ is small for every admissible N. We note that it is much stronger than a result (which usually admits a simpler proof) that asserts that for every admissible N, the discrepancy is small for almost all $\vartheta \in \mathbb{F}_p$.

3.2. **Discrepancy bound for inversions.** The number T is defined as in the beginning of Section 2.1.

Theorem 4. *Assume that the permutation ψ is given by* (3) *with $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. Then for any integer $s \geq 1$ and real $\Delta > 0$, for all initial values $\vartheta \in \mathbb{F}_p$, except at most $O(\Delta p)$ of them, we have*

$$D_{s,\psi}(\vartheta; N) \ll \left(\Delta^{-2/3}N^{-1/3} + \Delta^{-1}p^{-1/4}\right)(\log N)^s \log T$$

for all N with $1 \leq N \leq T$.

Proof. Let

$$N_\nu = 2^\nu, \qquad \text{and} \qquad M_\nu = \left\lceil \Delta^{-2/3} N_\nu^{2/3} \right\rceil, \qquad \nu = 0, \ldots, J,$$

where

$$J = \left\lceil \frac{\log T}{\log 2} \right\rceil .$$

We define $k \geq 1$ by the condition $N_{k-1} < N \leq N_k$.

From Lemma 3 with $H = \lfloor N/2 \rfloor$ we derive

$$D_{s,\psi}(\vartheta; N) \ll \frac{1}{N} + \frac{1}{N} \sum_{0<|\mathbf{h}|\leq N/2} \frac{1}{\rho(\mathbf{h})} \left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j u_{n+j-1}(\vartheta) \right) \right| . \tag{7}$$

Clearly

$$\sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j u_{n+m+j-1}(\vartheta) \right) = \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j u_{n+j-1}(\vartheta) \right) + O(m)$$

for any integer $m \geq 0$. Thus,

$$\begin{aligned} &\left| \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j u_{n+j-1}(\vartheta) \right) \right| \\ &\qquad = \frac{1}{M_k} \left| \sum_{m=0}^{M_k-1} \sum_{n=0}^{N-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j u_{n+m+j-1}(\vartheta) \right) \right| + O(M_k) \\ &\qquad \ll \frac{1}{M_k} \sum_{n=0}^{N-1} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j u_{n+m+j-1}(\vartheta) \right) \right| + M_k \\ &\qquad = \frac{1}{M_k} \sum_{n=0}^{N_k-1} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta) \right) \right| + M_k. \end{aligned}$$

Combining the above estimate with (7), and using that $N \leq N_k < 2N$, we obtain

$$D_{s,\psi}(\vartheta; N) \ll \frac{M_k}{N_k} + \frac{1}{N_k} R_{k,s,\psi}(\vartheta), \tag{8}$$

where

$$R_{k,s,\psi}(\vartheta) = \frac{1}{M_k} \sum_{0<|\mathbf{h}|\leq N_k/2} \frac{1}{\rho(\mathbf{h})} \sum_{n=0}^{N_k-1} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta) \right) \right| . \tag{9}$$

We now show that for all but $O(\Delta p)$ elements $\vartheta \in \mathbb{F}_p$, the values of $R_{k,s,\psi}(\vartheta)$ satisfy

$$R_{k,s,\psi}(\vartheta) < \Delta^{-1}(M_k^{-1/2}N_k + N_k p^{-1/4})(\log N_k)^s \log T, \tag{10}$$

for every $k = 1, \ldots, J$.

In order to prove this, we estimate the average value

$$Q_{k,s,\psi} = \sum_{\vartheta \in \mathbb{F}_p} R_{k,s,\psi}(\vartheta).$$

We have

$$Q_{k,s,\psi} = \frac{1}{M_k} \sum_{0<|\mathbf{h}|\le N_k/2} \frac{1}{\rho(\mathbf{h})} \sum_{n=0}^{N_k-1} \sum_{\vartheta\in\mathbb{F}_p} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta)\right)\right|.$$

As in the proof of Lemma 2, see (4), we see that

$$\sum_{\vartheta\in\mathbb{F}_p} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta)\right)\right| = \sum_{\vartheta\in\mathbb{F}_p} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} h_j \psi^{m+j-1}(\vartheta)\right)\right|.$$

Thus

$$Q_{k,s,\psi} = \frac{N_k}{M_k} \sum_{0<|\mathbf{h}|\le N_k/2} \frac{1}{\rho(\mathbf{h})} \sum_{\vartheta\in\mathbb{F}_p} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} h_j \psi^{m+j-1}(\vartheta)\right)\right|.$$

Furthermore, by the Cauchy-Schwarz inequality, we have

$$\begin{aligned}\left(\sum_{\vartheta=0}^{p-1} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} h_j \psi^{m+j-1}(\vartheta)\right)\right|\right)^2 \\ \le p \sum_{\vartheta=0}^{p-1} \left| \sum_{m=0}^{M_k-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} h_j \psi^{m+j-1}(\vartheta)\right)\right|^2 = pV_{1,\mathbf{h},\psi}(M_k).\end{aligned}$$

Hence

$$\begin{aligned} Q_{k,s,\psi} &\le \frac{N_k p^{1/2} V_{1,\mathbf{h},\psi}(M_k)^{1/2}}{M_k} \sum_{0<|\mathbf{h}|\le N_k/2} \frac{1}{\rho(\mathbf{h})} \\ &\ll \frac{N_k p^{1/2} V_{1,\mathbf{h},\psi}(M_k)^{1/2}}{M_k} (\log N_k)^s. \end{aligned}$$

Clearly, Lemma 1 is equivalent to the estimate

$$V_{1,\mathbf{h},\psi}(M) \ll Mp + M^2 p^{1/2}.$$

Therefore,

$$Q_{k,s,\psi} \ll (M_k^{-1/2} N_k p + N_k p^{3/4})(\log N_k)^s. \tag{11}$$

Let Ω_k be the set of $\vartheta \in \mathbb{F}_p$ with

$$R_{k,s,\psi}(\vartheta) \ge \Delta^{-1}(M_k^{-1/2}N_k + N_k p^{-1/4})(\log N_k)^s \log T.$$

Then

$$\#\Omega_k \Delta^{-1}(M_k^{-1/2}N_k + N_k p^{-1/4})(\log N_k)^s \log T \le Q_{k,s,\psi}$$

and using (11) we obtain

$$\#\Omega_k \ll \Delta p (\log T)^{-1}.$$

Thus for

$$\Omega = \bigcup_{k=1}^{J} \Omega_k$$

we obtain

$$\#\Omega \ll \Delta p.$$

On the other hand, for $\vartheta \in \mathbb{F}_p \setminus \Omega$, the bound (10) holds, and we derive from (8) that

$$D_{s,\psi}(\vartheta; N) \ll \frac{M_k}{N_k} + \Delta^{-1}(M_k^{-1/2} + p^{-1/4})(\log N_k)^s \log T$$

for every $k = 1, \dots, J$. Recalling the choice of M_k, we conclude the proof. □

We note that [7, Theorem 3] gives the estimate

$$D_{s,\psi}(\vartheta; N) \ll \Delta^{-1}\left(N^{-1/2} + p^{-1/4}\right)(\log N)^{s+1} \log T$$

under the same conditions and with the same estimate on the size of the exceptional set as in Theorem 4. Clearly, Theorem 4 improves this result by a factor of $\log N$, provided that $T \ge N \ge \Delta p^{3/4}$.

3.3. **Discrepancy bound for permutation polynomials.** In the case of polynomials we slightly modify the scheme of the proof of Theorem 4, although we reuse some of its arguments.

Theorem 5. *Assume that the permutation ψ is given by a permutation polynomial $f(X) \in \mathbb{F}_p[X]$ of degree $d \ge 2$. Then for any integer $s \ge 1$ and real $\delta > 0$ and $A > 0$, for all initial values $\vartheta \in \mathbb{F}_p$, except at most $O(p(\log p)^{-A})$ of them, we have*

$$D_{s,\psi}(\vartheta; N) \ll (\log p)^{-1/2+\delta}$$

for all N with $(\log p)^{3/2+\delta} \le N \le p$.

Proof. We put

$$r = \left\lceil 2\delta^{-1}(A + s + 1)\right\rceil.$$

Let

$$N_\nu = 2^\nu, \qquad \nu = 0, \dots, J,$$

where

$$J = \left\lceil \frac{\log p}{\log 2} \right\rceil$$

and

$$M_0 = \lfloor c \log p \rfloor,$$

where $c > 0$ is the constant of Lemma 2 for the above choice of r (as well as of d and s).

As before, we define $k \ge 1$ by the condition $N_{k-1} < N \le N_k$.

Applying Lemma 3 with $H = \lfloor \log p \rfloor$, we obtain the following analogue of the relations (8) and (9):

$$D_{s,\psi}(\vartheta; N) \ll \frac{1}{\log p} + \frac{M_0}{N_k} + \frac{1}{N_k} S_{k,s,\psi}(\vartheta), \tag{12}$$

where

$$S_{k,s,\psi}(\vartheta) = \frac{1}{M_0} \sum_{0<|\mathbf{h}|\le \log p} \frac{1}{\rho(\mathbf{h})} \sum_{n=0}^{N_k-1} \left| \sum_{m=0}^{M_0-1} \mathbf{e}_p\left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta)\right)\right|. \tag{13}$$

For $k = 1, \ldots, J$ and a vector $\mathbf{h} \in \mathbb{Z}^s$, we denote by $\Omega_k(\mathbf{h})$ the set of $\vartheta \in \mathbb{F}_p$ with

$$\sum_{n=0}^{N_k-1} \left| \sum_{m=0}^{M_0-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta) \right) \right| \ge N_k M_0 (\log p)^{-1/2+\delta/2}.$$

Clearly, for any integer $r \ge 1$,

$$\Omega_k(\mathbf{h}) (N_k M_0 (\log p)^{-1/2+\delta/2})^{2r} \le T_{r,k,s,\psi}(\mathbf{h}), \tag{14}$$

where

$$T_{r,k,s,\psi}(\mathbf{h}) = \sum_{\vartheta \in \mathbb{F}_p} \left(\sum_{n=0}^{N_k-1} \left| \sum_{m=0}^{M_0-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta) \right) \right| \right)^{2r}.$$

Using the Hölder inequality and recalling (4), we derive

$$\begin{aligned} T_{r,k,s,\psi}(\mathbf{h}) &\le N_k^{2r-1} \sum_{\vartheta \in \mathbb{F}_p} \sum_{n=0}^{N_k-1} \left| \sum_{m=0}^{M_0-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{n+m+j-1}(\vartheta) \right) \right|^{2r} \\ &= N_k^{2r} \sum_{\vartheta \in \mathbb{F}_p} \left| \sum_{m=0}^{M_0-1} \mathbf{e}_p \left(\sum_{j=0}^{s-1} h_j \psi^{m+j-1}(\vartheta) \right) \right|^{2r} = N_k^{2r} V_{r,\mathbf{h},\psi}(M_0). \end{aligned}$$

Therefore, by Lemma 2, we have

$$T_{r,k,s,\psi}(\mathbf{h}) \ll N_k^{2r} M_0^{2r} p (\log p)^{-r},$$

which after inserting in (14) yields

$$\Omega_k(\mathbf{h}) \le p (\log p)^{-\delta r/2}.$$

Thus for

$$\Omega = \bigcup_{k=1}^{J} \bigcup_{0 < |\mathbf{h}| \le \log p} \Omega_k(\mathbf{h}),$$

recalling the choice of r, we obtain

$$\#\Omega \ll p (\log p)^{-\delta r/2+s+1} \ll p (\log p)^{-A}.$$

On the other hand, for $\vartheta \in \mathbb{F}_p \setminus \Omega$, we derive from (13) that

$$S_{k,s,\psi}(\vartheta) \ll N_k (\log p)^{-1/2+\delta/2} (\log \log p)^s \ll N_k (\log p)^{-1/2+\delta}$$

for every $k = 1, \ldots, J$.

Now, recalling the choice of M_0 and the inequality $N \le N_k$, we see from (12) that

$$\begin{aligned} D_{s,\psi}(\vartheta; N) &\ll \frac{1}{\log p} + \frac{M_0}{N_k} + (\log p)^{-1/2+\delta} \\ &\ll \frac{\log p}{N} + (\log p)^{-1/2+\delta} \ll (\log p)^{-1/2+\delta}, \end{aligned}$$

for $(\log p)^{3/2+\delta} \le N \le p$, which concludes the proof. □

Certainly, using the full power of Lemma 2 one can obtain nontrivial estimates on $D_{s,\psi}(\vartheta; N)$ for smaller values of N as well.

4. Comments

One can easily obtain an analogue of Lemma 1 for $V_{r,\mathbf{h},\psi}(M)$ with any $r \geq 1$. More precisely, a quick inspection of the proof of [7, Lemma 1] reveals that it can be used to derive the estimate

$$V_{r,\mathbf{h},\psi}(M) \ll \begin{cases} M^r p & \text{if } M \leq p^{1/2}, \\ M^{2r} p^{1/2} & \text{if } M > p^{1/2}, \end{cases}$$

for ψ given by (3). The above bound, as well as Lemma 2, can easily be obtained with explicit dependence on r. In particular, as in [10], one can take r as a slightly growing function of p and obtain a better estimate on the size of the exceptional set in Theorem 5.

Our technique applies to several other related problems as well. In particular, one can obtain an improvement of the estimates of [1] for multiplicative character sums with sequences generated by inversions and permutation polynomials. It is also likely to work for such constructions as those in [5].

Finally, the same arguments also apply in the case of similar generators considered in residue rings; however, the Weil bound has to be replaced by an appropriate estimate of exponential sums which is valid in this particular ring (thus one expects much weaker results in the settings of residue rings).

References

[1] A. Çeşmelioğlu and A. Winterhof, 'On the average distribution of power residues and primitive elements in inversive and nonlinear recurring sequences', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **5203** (2008), 60–70.

[2] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997. MR1470456 (98j:11057)

[3] J. F. Koksma, 'Some theorems on Diophantine inequalities', *Math. Centrum Scriptum no. 5*, Amsterdam, 1950. MR0038379 (12:394c)

[4] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge Univ. Press, Cambridge, 1997. MR1429394 (97i:11115)

[5] H. Niederreiter and I.E. Shparlinski, 'On the distribution of pseudorandom numbers and vectors generated by inversive methods', *Applicable Algebra Engrg. Comm. Computing*, **10** (2000), 189–202. MR1751430 (2001f:11130)

[6] H. Niederreiter and I. E. Shparlinski, 'On the distribution of inversive congruential pseudorandom numbers in parts of the period', *Math. Comp.*, **70** (2001), 1569–1574. MR1836919 (2002e:11104)

[7] H. Niederreiter and I. E. Shparlinski, 'On the average distribution of inversive pseudorandom numbers', *Finite Fields and Their Appl.*, **8** (2002), 491–503. MR1933620 (2003g:11085)

[8] H. Niederreiter and I.E. Shparlinski, 'Recent advances in the theory of nonlinear pseudorandom number generators', *Monte Carlo and Quasi-Monte Carlo Methods 2000*, Springer-Verlag, Berlin, 2002, 86–102. MR1958848 (2003k:65005)

[9] H. Niederreiter and I. Shparlinski, 'Dynamical systems generated by rational functions', *Lect. Notes in Comp. Sci.*, Springer-Verlag, Berlin, **2643** (2003), 6–17. MR2042407 (2005a:94047)

[10] H. Niederreiter and A. Winterhof, 'Exponential sums for nonlinear recurring sequences', *Finite Fields Appl.*, **14** (2008), 59–64. MR2381476 (2008m:11166)

[11] I. E. Shparlinski, 'On some dynamical systems in finite fields and residue rings', *Discr. and Cont. Dynam. Syst., Ser.A*, **17** (2007), 901–917. MR2276481 (2007j:11098)

[12] P. Szüsz, 'On a problem in the theory of uniform distribution', *Comptes Rendus Premier Congrès Hongrois*, Budapest, 1952, 461–472 (in Hungarian). MR0056036 (15:15c)

[13] A. Topuzoğlu and A. Winterhof, 'Pseudorandom sequences', *Topics in Geometry, Coding Theory and Cryptography*, Springer-Verlag, 2006, 135–166. MR2278037 (2007m:11106)

Department of Computing, Macquarie University, NSW 2109, Australia
E-mail address: igor.shparlinski@mq.edu.au