ACTA ARITHMETICA
LXXXIII.1 (1998)

A bound for the discrepancy of digital nets and its application to the analysis of certain pseudo-random number generators

by

GERHARD LARCHER (Salzburg)

1. Introduction. The concept of digital nets is at the moment the most effective method for the construction of low-discrepancy point sets in the s-dimensional unit cube. Furthermore, by recent work it turned out that digital nets also play an important role in the analysis of certain pseudo-random number generators.

Until now the discrepancy of digital nets essentially was estimated by using discrepancy bounds valid for arbitrary nets. In this paper we give a more sensible—in some sense—discrepancy bound, especially for digital nets generated over a finite field of prime order, and we apply this bound for improving some results concerning the serial test of certain pseudo-random number generators.

The serial test is a test for the statistical independence of successive pseudo-random numbers. For a pseudo-random number sequence $x_0, x_1, \ldots, x_{N-1}$ in $[0,1)$ and a fixed dimension $s \geq 2$ let the *serial set* $(\mathbf{x}_n)_{n\geq 0}$ of dimension s be defined by $\mathbf{x}_n := (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0,1)^s$ for $n = 0, 1, \ldots, N-1$. (Here we consider the sequence $(x_n)_{n\geq 0}$ to be periodic with period N.) We then consider the usual star-discrepancy D_N^* of this sequence in $[0,1)^s$. D_N^* is defined by

$$D_N^* = \sup_B \left| \frac{A_N(B)}{N} - \lambda(B) \right|,$$

where the supremum is over all subintervals B in $[0,1)^s$ with one vertex at the origin, $A_N(B)$ denotes the number of elements of the sequence belonging to B, and $\lambda(B)$ is the s-dimensional volume of B.

Small discrepancy guarantees good statistical independence properties of the successive elements of the pseudo-random sequence.

1991 *Mathematics Subject Classification*: 11K38, 11K45.

K. F. Roth [11] has shown that for every dimension $s \geq 2$ there exists a constant $c_s > 0$ such that for every $N \geq 2$ and each sequence $y_0, y_1, \ldots, y_{N-1}$ in $[0,1)^s$, for the corresponding star-discrepancy D_N^* of the sequence we have

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

It is a famous conjecture that this still holds if the exponent $(s-1)/2$ of the logarithm is replaced by $s-1$. Until now this was only proved for the dimensions $s = 1$ and $s = 2$ (see [12]). So by "small discrepancy" we mean a discrepancy of an order $(\log N)^A/N$ with A not much larger than $s-1$.

In this paper we consider three widely used pseudo-random number generation methods: the recursive matrix method (combined with the p-adic digit method), the digital multistep method, and the generalized feedback shift-register method. These methods have the property that their serial sets show in some sense a "net property" and even a "digital net property". For the theory of nets and for more details and a discussion concerning the serial test see the excellent monograph [4] of Niederreiter, and the various references given there.

For all these generation methods we show the existence of parameters which provide pseudo-random number sequences with large period and with an extremely small discrepancy for its serial sets. We thereby improve results which are given in, or can be deduced from, [6], [3] and [2].

Note that it is not the intention of this paper to discuss or to evaluate different pseudo-random number generation methods or to give comments on advantages and disadvantages of various pseudo-random number tests.

2. A discrepancy bound for digital nets. The concept of digital nets over a certain ring is at the moment the most effective method for the construction of low-discrepancy sequences in an s-dimensional unit cube. We just mention the powerful construction methods given by Niederreiter and Xing for example in [8]–[10] which are based on the digital construction concept over a finite field. In this section we recall the notion of digital nets and we give the new discrepancy bound in Proposition 1.

Let p be a prime, let F_p be the finite field of order p and use the natural identification between the elements of the field and the digits between 0 and $p-1$.

For integers $s \geq 2$, $m \geq 2$ and $N = p^m$ the sequence $\mathbf{x}_0, \ldots, \mathbf{x}_{N-1} \in [0,1)^s$ with $\mathbf{x}_n := (x_n(1), \ldots, x_n(s))$ is called a *digital net* over F_p if there exist s $m \times m$ matrices $A_1, \ldots, A_s$ over F_p such that for all $n = 0, \ldots, N-1$ and $i = 1, \ldots, s$ we have

$$x_n(i) = \frac{1}{N} \tau(A_i \cdot \tau^{-1}(n)).$$

Here we denote by τ the following bijection between F_p^m and $\{0,\dots,p^m-1\}$:

$$\tau((a_0,\dots,a_{m-1})) := a_0 + a_1 p + \dots + a_{m-1}p^{m-1}.$$

The quality of the distribution of a digital net of course essentially depends on the properties of the defining matrices A_i (see for example Theorem 4.28 of [4]).

Let $A_1,\dots,A_s$ be given and denote by $a_j^{(i)} \in F_p^m$ with $j=1,\dots,m$ the rows of the matrix A_i for $i=1,\dots,s$. For $0 \le w \le s$, a w-tuple $(d_1,\dots,d_w)$ of non-negative integers is called *admissible with respect to* $A_1,\dots,A_s$ if the system $\{a_j^{(i)} : j=1,\dots,d_i,\ i=1,\dots,w\}$ is linearly independent over F_p. For $w=0$ we define the "zero-tuple" () to be admissible. For $w \le s-1$ and $(d_1,\dots,d_w)$ admissible we set $h(d_1,\dots,d_w) := \max\{h \ge 0 \mid (d_1,\dots,d_w,h) \text{ is admissible}\}$.

Then we have:

PROPOSITION 1. *Let D^* denote the star-discrepancy of the digital net $\mathbf{x}_0,\dots,\mathbf{x}_{p^m-1}$ over F_p defined by $A_1,\dots,A_s$. Then*

$$D^* \le \sum_{w=0}^{s-1}(p-1)^w \sum_{\substack{(d_1,\dots,d_w)\ admissible\\ d_i>0}} p^{-(d_1+\dots+d_w+h(d_1,\dots,d_w))}.$$

Proof. By the definitions, if $(d_1,\dots,d_w)$ is admissible and we let

$$B \subseteq [0,1]^s \quad \text{with} \quad B = \prod_{i=1}^{w}\left[\frac{a_i}{p^{d_i}},\frac{b_i}{p^{d_i}}\right) \times [0,1)^{s-w}$$

with integers $0 \le a_i < b_i \le p^{d_i}$ (we call such an interval an *admissible interval*), then B contains exactly

$$p^{m-(d_1+\dots+d_w)}\prod_{i=1}^{w}(b_i-a_i)$$

of the net points.

Let $M = \prod_{i=1}^{s}[0,\alpha_i) \subseteq [0,1)^s$ with $\alpha_i := \sum_{j=1}^{\infty}\alpha_j^{(i)}/p^j$ for $i=1,\dots,s$ be taken arbitrarily. (If the representation of some α_i is not unique then we use an infinite representation.) Then on the one hand we have

$$\widetilde{M} := \bigcup_{\substack{(d_1,\dots,d_s)\ \text{admissible}\\ d_i>0}} \prod_{i=1}^{s}\left[\sum_{j=1}^{d_i-1}\frac{\alpha_j^{(i)}}{p^j},\sum_{j=1}^{d_i}\frac{\alpha_j^{(i)}}{p^j}\right) \subseteq M.$$

The intervals in the above union are pairwise disjoint and admissible. On the other hand, we will show by induction on s that

$$M \subseteq \widetilde{M} \cup \bigcup_{w=0}^{s-1} \bigcup_{\substack{(d_1,\dots,d_w)\text{ admissible}\\ d_i>0}} \left(\prod_{i=1}^{w} \left[\sum_{j=1}^{d_i-1} \frac{\alpha_j^{(i)}}{p^j}, \sum_{j=1}^{d_i} \frac{\alpha_j^{(i)}}{p^j} \right) \times \left[\sum_{j=1}^{h(d_1,\dots,d_w)} \frac{\alpha_j^{(w+1)}}{p^j}, \sum_{j=1}^{h(d_1,\dots,d_w)} \frac{\alpha_j^{(w+1)}}{p^j} + \frac{1}{p^{h(d_1,\dots,d_w)}} \right) \times [0,1)^{s-w-1} \right).$$

(Again all intervals in the second union above are admissible.) For $s = 1$ the right hand side above is

$$\bigcup_{d_1\text{ admissible}} \left[\sum_{j=1}^{d_1-1} \frac{\alpha_j^{(1)}}{p^j}, \sum_{j=1}^{d_1} \frac{\alpha_j^{(1)}}{p^j} \right) \cup \left[\sum_{j=1}^{h()} \frac{\alpha_j^{(1)}}{p^j}, \sum_{j=1}^{h()} \frac{\alpha_j^{(1)}}{p^j} + \frac{1}{p^{h()}} \right) = \left[0, \sum_{j=1}^{h()} \frac{\alpha_j^{(1)}}{p^j} + \frac{1}{p^{h()}} \right),$$

which contains $M = [0, \alpha_1)$. Assume the assertion is true up to dimension $s-1$ and consider

$$M = \prod_{i=1}^{s-1} [0, \alpha_i) \times [0, \alpha_s).$$

By induction,

$$\prod_{i=1}^{s-1} [0, \alpha_i) \subseteq \bigcup_{\substack{(d_1,\dots,d_{s-1})\text{ admissible}\\ d_i>0}} \prod_{i=1}^{s-1} \left[\sum_{j=1}^{d_i-1} \frac{\alpha_j^{(i)}}{p^j}, \sum_{j=1}^{d_i} \frac{\alpha_j^{(i)}}{p^j} \right) \cup \bigcup_{w=0}^{s-2} \bigcup_{\substack{(d_1,\dots,d_w)\text{ admissible}\\ d_i>0}} \left(\prod_{i=1}^{w} \left[\sum_{j=1}^{d_i-1} \frac{\alpha_j^{(i)}}{p^j}, \sum_{j=1}^{d_i} \frac{\alpha_j^{(i)}}{p^j} \right) \times \left[\sum_{j=1}^{h(d_1,\dots,d_w)} \frac{\alpha_j^{(w+1)}}{p^j}, \sum_{j=1}^{h(d_1,\dots,d_w)} \frac{\alpha_j^{(w+1)}}{p^j} + \frac{1}{p^{h(d_1,\dots,d_w)}} \right) \times [0,1)^{s-w-2} \right).$$

We extend each of the $(s-1)$-dimensional intervals J on the right hand side above to an s-dimensional interval J' such that M is contained in the union of these extensions.

If J is part of the first big union above, that is, if it is of the form

$$\prod_{i=1}^{s-1}\left[\sum_{j=1}^{d_i-1}\frac{\alpha_j^{(i)}}{p^j},\sum_{j=1}^{d_i}\frac{\alpha_j^{(i)}}{p^j}\right)$$

for some admissible $(d_1,\ldots,d_{s-1})$, then we take

$$\begin{aligned}J' := &\prod_{i=1}^{s-1}\left[\sum_{j=1}^{d_i-1}\frac{\alpha_j^{(i)}}{p^j},\sum_{j=1}^{d_i}\frac{\alpha_j^{(i)}}{p^j}\right)\\ &\times\Bigg(\bigcup_{k=1}^{h(d_1,\ldots,d_{s-1})}\left[\sum_{j=1}^{k-1}\frac{\alpha_j^{(s)}}{p^j},\sum_{j=1}^{k}\frac{\alpha_j^{(s)}}{p^j}\right)\\ &\cup\left[\sum_{j=1}^{h(d_1,\ldots,d_{s-1})}\frac{\alpha_j^{(s)}}{p_j},\sum_{j=1}^{h(d_1,\ldots,d_{s-1})}\frac{\alpha_j^{(s)}}{p^j}+\frac{1}{p^{h(d_1,\ldots,d_{s-1})}}\right)\Bigg).\end{aligned}$$

If J is part of the second big union then we just extend by $[0,1)$.

By inserting we obtain

$$\begin{aligned}M\subseteq &\bigcup_{\substack{(d_1,\ldots,d_{s-1})\text{ admissible}\\ d_i>0}}\Bigg(\prod_{i=1}^{s-1}\left[\sum_{j=1}^{d_i-1}\frac{\alpha_j^{(i)}}{p^j},\sum_{j=1}^{d_i}\frac{\alpha_j^{(i)}}{p^j}\right)\\ &\times\bigcup_{k=1}^{h(d_1,\ldots,d_{s-1})}\left[\sum_{j=1}^{k-1}\frac{\alpha_j^{(s)}}{p^j},\sum_{j=1}^{k}\frac{\alpha_j^{(s)}}{p^j}\right)\Bigg)\\ &\cup\bigcup_{\substack{(d_1,\ldots,d_{s-1})\text{ admissible}\\ d_i>0}}\Bigg(\prod_{i=1}^{s-1}\left[\sum_{j=1}^{d_i-1}\frac{\alpha_j^{(i)}}{p^j},\sum_{j=1}^{d_i}\frac{\alpha_j^{(i)}}{p^j}\right)\\ &\times\left[\sum_{j=1}^{h(d_1,\ldots,d_{s-1})}\frac{\alpha_j^{(s)}}{p^j},\sum_{j=1}^{h(d_1,\ldots,d_{s-1})}\frac{\alpha_j^{(s)}}{p^j}+\frac{1}{p^{h(d_1,\ldots,d_{s-1})}}\right)\Bigg)\\ &\cup\bigcup_{w=0}^{s-2}\bigcup_{\substack{(d_1,\ldots,d_w)\text{ admissible}\\ d_i>0}}\Bigg(\prod_{i=1}^{w}\left[\sum_{j=1}^{d_i-1}\frac{\alpha_j^{(i)}}{p^j},\sum_{j=1}^{d_i}\frac{\alpha_j^{(i)}}{p^j}\right)\\ &\times\left[\sum_{j=1}^{h(d_1,\ldots,d_w)}\frac{\alpha_j^{(w+1)}}{p^j},\sum_{j=1}^{h(d_1,\ldots,d_w)}\frac{\alpha_j^{(w+1)}}{p^j}+\frac{1}{p^{h(d_1,\ldots,d_w)}}\right)\\ &\times[0,1)^{s-w-1}\Bigg),\end{aligned}$$

and the induction is finished.

So we obtain

$$\left|\frac{A_N(M)}{N} - \lambda(M)\right| \le \sum_{w=0}^{s-1}(p-1)^w \sum_{\substack{(d_1,\dots,d_w)\\ \text{admissible}\\ d_i>0}} p^{-(d_1+\dots+d_w+h(d_1,\dots,d_w))}$$

and the result follows. ■

3. The recursive matrix method. The recursive matrix method was introduced in full generality by Niederreiter in [5], and it was studied in detail for example in [6] and [7]. Here we only consider the case of recursive matrix methods of order one. This is a combination of the classical matrix method for the generation of pseudo-random vectors (see [4]), combined with a p-adic digit method.

The method is the following. Let p be a prime and let F_p be again the finite field of order p. Let m be a positive integer and let A be a non-singular $m \times m$ matrix over F_p. A sequence $\mathbf{z}_0, \mathbf{z}_1, \dots$ of row vectors from F_p^m is generated by choosing an initial vector $\mathbf{z}_0$ different from $\mathbf{0}$ and by

$$\mathbf{z}_{n+1} := \mathbf{z}_n \cdot A \quad \text{for } n = 0, 1, \dots$$

We now derive pseudo-random numbers x_n in $[0,1)$ from $\mathbf{z}_n := (z_n^{(1)}, \dots, z_n^{(m)}) \in F_p^m$ in the following way. We identify the elements $z \in F_p$ in the natural way with digits $z \in \{0, \dots, p-1\}$. Then

$$x_n := \sum_{j=1}^{m} z_n^{(j)} p^{-j} \quad \text{for } n = 0, 1, \dots$$

The sequence $(\mathbf{z}_n)_{n\ge0}$ and therefore $(x_n)_{n\ge0}$ is purely periodic because of the non-singularity of the matrix A, with (least) period at most $p^m - 1$. This maximal (least) period is attained if and only if the polynomial $\det(x \cdot I_m - A)$ of degree m is a primitive polynomial over F_p. (Here I_m is the $m \times m$ identity matrix.) This is shown for example in Theorem 10.2 of [4]. In the following we restrict ourselves to this, for practical purposes most important, case of maximal period.

Let in the following $q := p^m$. In Theorem 2 of [6] it was shown that a sequence $(\mathbf{z}_n)_{n\ge0}$ with $\mathbf{z}_n := (z_n^{(1)}, \dots, z_n^{(m)}) \in F_p^m$ is a recursive vector sequence of the above form of period $T := p^m - 1$ if and only if there is a primitive element σ of F_q and a basis $\beta_1, \dots, \beta_m$ of F_q over F_p such that $z_n^{(j)} = \mathrm{Tr}(\beta_j \sigma^n)$ for $1 \le j \le m$ and $n \ge 0$. Here Tr is the trace function from F_q to F_p.

Concerning the star-discrepancy $D_T^{*(s)}$ of the serial sets of dimension s of these sequences, the following was shown in [6].

Let $2 \le s \le m$ and let σ be a fixed primitive element of F_q. Then for $D_T^{*(s)}$ we have on the average

$$D_T^{*(s)} \le c(s)\frac{(\log T)^s}{T}$$

with an implied constant depending only on s, where the average is taken over all ordered bases of F_q over F_p.

From this we at once deduce the following. Let $2 \le s \le m$, let σ be a fixed primitive element of F_q and let $\mathcal{B}$ be the set of ordered bases of F_q over F_p. Let $0 < \gamma < 1$ be given. Then the number of bases $B \in \mathcal{B}$ for which for the discrepancy $D_T^{*(s)}(B)$ of the s-dimensional serial set of the corresponding sequence we have

$$D_T^{*(s)}(B) \le \frac{1}{1-\gamma}c(s)\frac{(\log T)^s}{T}$$

is at least $\gamma|\mathcal{B}|$.

We improve this result (at least for small p) by almost one logarithmic factor in the following way:

THEOREM 1. *Let $2 \le s \le m$, let σ be a primitive element of F_q and let $\mathcal{B}$ be the set of ordered bases of F_q over F_p. Let $0 < \gamma < 1$ be given. Then the number of bases $B \in \mathcal{B}$ for which for the discrepancy $D_T^{*(s)}(B)$ of the s-dimensional serial set $\mathbf{x}_0, \dots, \mathbf{x}_{T-1}$ of the corresponding sequence we have*

$$\begin{aligned} D_T^{*(s)}(B) &\le \frac{1}{T} + \frac{1}{p^m}\sum_{w=0}^{s-1}(p-1)^w\binom{m}{w} \\ &\quad \times \Bigg[(s-1)\left(\frac{p}{p-1}\right)^2\frac{2}{1-\gamma}{}_p\log m \\ &\quad + \left(\frac{p}{p-1}\right)^2\frac{2}{1-\gamma}\left(1+{}_p\log\frac{4}{1-\gamma}\right)+\frac{1+\gamma}{1-\gamma}\Bigg] \\ &= \mathcal{O}\left(\frac{(\log T)^{s-1}\log\log T}{T}\right) \end{aligned}$$

is at least $\gamma|\mathcal{B}|$. (Here we denote by ${}_p\log$ the logarithm to base p.)

Remark 1. Note that the constant in the $\mathcal{O}$-result of Theorem 1 does also depend on p.

Remark 2. For example, in the case $p = 2$ for at least half the bases B in $\mathcal{B}$, we have

$$D_T^{*(s)}(B) \le 68\frac{1}{2^m}\sum_{w=0}^{s-1}\binom{m}{w} + 16(s-1)\frac{{}_2\log m}{2^m}\sum_{w=0}^{s-1}\binom{m}{w}.$$

Remark 3. The above discrepancy estimates coincide up to the $\log\log T$ factors with the conjectured general lower bound for the discrepancy of point sets in $[0,1)^s$.

Proof of Theorem 1. Let the recursive matrix sequence $x_0,\ldots,x_{T-1}$ be defined by the primitive element σ of F_q and by the ordered basis $B=\{\beta_1,\ldots,\beta_m\}$ of F_q over F_p. The β_i are viewed as vectors of F_q over F_p. By Theorem 5 of [6], the set $\mathbf{0},\mathbf{x}_0,\mathbf{x}_1,\ldots,\mathbf{x}_{T-1}$ forms a digital net over F_p which is generated by certain matrices, say $C_1,\ldots,C_s$. Let $c_j^{(i)}\in F_p^m$ for $1\le j\le m$ be rows of C_i for $1\le i\le s$.

It is shown in the proof of that Theorem 5 that these $C_1,\ldots,C_s$ have the following property: for any non-negative integers $d_i\le m,\ i=1,\ldots,s$, the system of vectors $\{c_j^{(i)}:1\le j\le d_i,\ 1\le i\le s\}$ is linearly dependent over F_p if and only if the system $\{\beta_j\sigma^{i-1}:1\le j\le d_i,\ 1\le i\le s\}$ is. In the following we consider admissible w-tuples of integers with respect to the matrices $A_i(B)$ with rows $\beta_j\sigma^{i-1}$, $j=1,\ldots,m$, for $i=1,\ldots,s$ and we call them (for fixed σ) *admissible for* B. Then by Proposition 1 for the star-discrepancy $D_T^{*(s)}(B)$ of the set $\mathbf{0},\mathbf{x}_0,\mathbf{x}_1,\ldots,\mathbf{x}_{T-1}$ we have

$$D_T^{*(s)}(B)\le\sum_{w=0}^{s-1}(p-1)^w\sum_{\substack{(d_1,\ldots,d_w)\\ \text{admissible for } B\\ d_i>0}}p^{-(d_1+\ldots+d_w+h(d_1,\ldots,d_w))}.$$

For a non-negative integer c let $\mathcal{M}(c)$ be the set of $B\in\mathcal{B}$ such that there exist positive integers $d_1,\ldots,d_s$ with $d_1+\ldots+d_s=m-c$ and with $\beta_j\sigma^{i-1},\ j=1,\ldots,d_i,\ i=1,\ldots,s$, linearly dependent over F_p. We have

$$|\mathcal{M}(c)|\le\sum_{\substack{\mathbf{d}:=(d_1,\ldots,d_s)\\ d_1+\ldots+d_s=m-c\\ d_i>0}}\ \sum_{\substack{\lambda:=(\lambda_1,\ldots,\lambda_{m-c})\in\\ F_p^{m-c}\setminus\{\mathbf{0}\}}}|\mathcal{M}(\lambda,\mathbf{d})|$$

with

$$\mathcal{M}(\lambda,\mathbf{d}):=\{B\in\mathcal{B}\mid\lambda_1\beta_1\sigma^0+\ldots+\lambda_{d_1}\beta_{d_1}\sigma^0+\ldots$$
$$\ldots+\lambda_{d_1+\ldots+d_{s-1}+1}\beta_1\sigma^{s-1}+\ldots+\lambda_{m-c}\beta_{d_s}\sigma^{s-1}=0\}.$$

We estimate the number of elements of $\mathcal{M}(\lambda,\mathbf{d})$. There is an $i\in\{1,\ldots,m-c\}$ with $\lambda_i\ne0$. Without loss of generality assume $\lambda_1\ne0$. Since $s\le m$ and since σ is primitive, we have $\lambda_1\sigma^0+\ldots+\lambda_{d_1+\ldots+d_{s-1}+1}\sigma^{s-1}\ne0$. So for arbitrarily chosen linearly independent $\beta_2,\ldots,\beta_m$ (there are $(p^m-1)\ldots(p^m-p^{m-2})$ such choices) there is at most one β_1 such that $(\beta_1,\ldots,\beta_m)\in\mathcal{B}$. Consequently,

$$|\mathcal{M}(\lambda,\mathbf{d})|\le(p^m-1)(p^m-p)\ldots(p^m-p^{m-2})=|\mathcal{B}|\frac{1}{p^m-p^{m-1}}$$

and therefore

$$|\mathcal{M}(c)| \leq |\mathcal{B}| \frac{1}{p^c} \cdot \frac{p}{p-1} \binom{m-c-1}{s-1}.$$

Let $\overline{\mathcal{M}}(c) := \mathcal{B} \setminus \mathcal{M}(c)$. Then

$$|\overline{\mathcal{M}}(c)| \geq |\mathcal{B}|(1 - R(c)) \quad \text{with} \quad R(c) := \frac{1}{p^c} \cdot \frac{p}{p-1} \binom{m-c-1}{s-1}.$$

For a positive integer c we now consider

$$\begin{aligned}
\sum := \frac{1}{|\overline{\mathcal{M}}(c)|} & \sum_{B \in \overline{\mathcal{M}}(c)} D_T^{*(s)}(B) \\
\leq \frac{1}{|\overline{\mathcal{M}}(c)|} & \sum_{B \in \overline{\mathcal{M}}(c)} \sum_{w=0}^{s-1} (p-1)^w \sum_{\substack{d_1, \ldots, d_w \\ \text{admissible for } B \\ d_i > 0}} p^{-(d_1 + \ldots + d_w + h(d_1, \ldots, d_w))} \\
\leq \frac{1}{|\overline{\mathcal{M}}(c)|} & \sum_{w=0}^{s-1} (p-1)^w \sum_{B \in \overline{\mathcal{M}}(c)} \sum_{\substack{d_1, \ldots, d_w \\ \text{admissible for } B \\ d_i > 0}} p^{-(d_1 + \ldots + d_w)} \\
& \times \left(\left(\sum_{i = m-(d_1+\ldots+d_w)-c+1}^{m-(d_1+\ldots+d_w)} \sum_{\lambda}{}^{*} \frac{p}{p-1} \cdot \frac{1}{p_i} \right) + \frac{1}{p^{m-(d_1+\ldots+d_w)}} \right).
\end{aligned}$$

Here $\sum_\lambda^*$ means summation over all

$$\lambda := (\lambda_1, \ldots, \lambda_{d_1+\ldots+d_w+i}) \in F_p^{d_1+\ldots+d_w+i} \setminus \{\mathbf{0}\}$$

for which

$$\begin{aligned}
\lambda_1 \beta_1 + \ldots + \lambda_{d_1} \beta_{d_1} + \ldots + \lambda_{d_1+\ldots+d_{w-1}+1} \beta_1 \sigma^{w-1} + \ldots + \lambda_{d_1+\ldots+d_w} \beta_{d_w} \sigma^{w-1} \\
+ \lambda_{d_1+\ldots+d_w+1} \beta_1 \sigma^w + \ldots + \lambda_{d_1+\ldots+d_w+i} \beta_i \sigma^w = 0.
\end{aligned}$$

The summand $1/p^{m-(d_1+\ldots+d_w)}$ comes from the case where $h(d_1, \ldots, d_w) = m-(d_1+\ldots+d_w)$ and the factor $p/(p-1)$ comes from the fact that whenever for given w, B, $(d_1, \ldots, d_w)$ and i there is a possible summand λ then there are at least $p-1$ such λ.

Therefore

$$\sum \le \frac{1}{p^m}\sum_{w=0}^{s-1}(p-1)^w\binom{m}{w}$$
$$+\frac{1}{|\overline{\mathcal{M}}(c)|}\cdot\frac{p}{p-1}\sum_{w=0}^{s-1}(p-1)^w\sum_{\substack{d_1,\ldots,d_w>0\\ d_1+\ldots+d_w\le m}}p^{-(d_1+\ldots+d_w)}$$
$$\times\sum_{i=\max(0,m-(d_1+\ldots+d_w)-c+1)}^{m-(d_1+\ldots+d_w)}\frac{1}{p^i}\sum_{\lambda\in F_p^{d_1+\ldots+d_w+i}\setminus\{\mathbf{0}\}}|\mathcal{M}(\lambda,\mathbf{d},w)|,$$

where $\mathcal{M}(\lambda,\mathbf{d},w)$ is defined like $\mathcal{M}(\lambda,\mathbf{d})$ above but with w instead of $s-1$. Estimating $|\mathcal{M}(\lambda,\mathbf{d},w)|$ in the same way as $|\mathcal{M}(\lambda,\mathbf{d})|$ above, we obtain $|\mathcal{M}(\lambda,\mathbf{d},w)|\le|\mathcal{B}|/(p^m-p^{m-1})$, and

$$\sum \le \frac{1}{p^m}\sum_{w=0}^{s-1}(p-1)^w\binom{m}{w}$$
$$+\frac{1}{|\overline{\mathcal{M}}(c)|}\cdot\frac{p}{p-1}\cdot c\cdot\frac{|\mathcal{B}|}{p^m-p^{m-1}}\sum_{w=0}^{s-1}(p-1)^w\binom{m}{w}$$
$$=\frac{1}{p^m}\sum_{w=0}^{s-1}(p-1)^w\binom{m}{w}\left[1+\left(\frac{p}{p-1}\right)^2 c\frac{|\mathcal{B}|}{|\overline{\mathcal{M}}(c)|}\right]=:A(c).$$

Therefore for $\Gamma\ge 1$ the number of $B\in\mathcal{B}$ with $D_T^{*(s)}(B)\le\Gamma A(c)$ is at least $(1-1/\Gamma)(1-R(c))|\mathcal{B}|$.

Let now $\Gamma=(1+\gamma)/(1-\gamma)$ and choose $c\ge 1$ such that $R(c)\le(1-\gamma)/2$, that is,

$$\frac{1}{p^c}\cdot\frac{p}{p-1}\binom{m-c-1}{s-1}\le\frac{1-\gamma}{2},$$

which is satisfied for

$$c\ge\left\lceil {}_p\log\left(\frac{2p}{(1-\gamma)(p-1)}m^{s-1}\right)\right\rceil$$

(here $\lceil x\rceil$ means the smallest integer larger than or equal to x). By inserting the choices for c and Γ and by noting that the discrepancies of the point sets $\mathbf{x}_0,\ldots,\mathbf{x}_{T-1}$ and $\mathbf{0},\mathbf{x}_0,\ldots,\mathbf{x}_{T-1}$ differ by at most $1/T$, we obtain the result. ∎

4. Shift-register sequences. In this section we consider both the digital multistep method and the generalized feedback shift-register (GFSR) method. For details see again [4], especially Chapter 9.

(a) *The digital multistep method*. This method was introduced by Tausworthe in [13]. Let p be a prime, let $k \geq 2$ be an integer and generate a kth order linear recurring sequence $y_0, y_1, \ldots \in F_p$ by

$$y_{n+k} \equiv \sum_{l=0}^{k-1} a_l y_{n+l} \pmod{p} \quad \text{for } n = 0, 1, \ldots$$

where $y_0, \ldots, y_{k-1}$ are initial values not all zero, and where the coefficients $a_0, \ldots, a_{k-1} \in F_p$ are chosen in such a way that the characteristic polynomial $f(x) := x^k - \sum_{l=0}^{k-1} a_l x^l \in F_p[x]$ is a primitive polynomial over F_p. We then have a maximal possible period of length $p^k - 1$ for the sequence $(y_n)_{n\geq 0}$.

In the digital multistep method we construct a pseudo-random number sequence $x_0, x_1, \ldots$ in $[0, 1)$ by choosing an integer m with $2 \leq m \leq k$ and by putting

$$x_n := \sum_{j=1}^{m} y_{mn+j} p^{-j} \quad \text{for } n = 0, 1, \ldots$$

This sequence has a period $(p^k - 1)/(m, p^k - 1)$. (See [4], Lemma 9.1.) For various reasons it is most convenient to choose $m = k$ and to choose k such that $(k, p^k - 1) = 1$. For given k and m the sequences $(x_n)_{n\geq 0}$ are uniquely determined by the primitive polynomial f and by the initial values $y_0, \ldots, y_{k-1}$. Concerning the star-discrepancy $D_T^{*(s)}(f)$ of the s-dimensional serial set $\mathbf{x}_n := (x_n, \ldots, x_{n+s+1})$, $n = 0, \ldots, T-1$, it was shown in [3] that for $m = k$ and $(k, p^k - 1) = 1$ (and therefore $T = p^k - 1$), and initial values $y_0, \ldots, y_{k-1}$ not all zero, we have, on the average,

$$D_T^{*(s)}(f) \leq c(s, p) \frac{(\log T)^{s+1} \log\log T}{T}$$

with an implied constant depending only on p and s, where the average is taken over all primitive polynomials f over F_p of degree k. From this for arbitrary γ, $0 < \gamma < 1$, we again immediately get the following. Let $\mathcal{Q}$ be the set of primitive polynomials f over F_p of degree k. Then the number of $f \in \mathcal{Q}$ for which the discrepancy $D_T^{*(s)}(f)$ of the s-dimensional serial set of the corresponding sequence satisfies

$$D_T^{*(s)}(f) \leq \frac{1}{1-\gamma} c(s, p) \frac{(\log T)^{s+1} \log\log T}{T}$$

is at least $\gamma|\mathcal{Q}|$.

We improve this result in the following:

THEOREM 2. *For a prime p let $s \geq 2$, $m = k$ and $T := p^k - 1$ with $(k, T) = 1$ and $y_0, \ldots, y_{k-1}$ in F_p, not all zero, be given. For fixed γ, $0 < \gamma < 1$, the number of $f \in \mathcal{Q}$ for which the star-discrepancy $D_T^{*(s)}(f)$ of the* *s-dimensional serial set of the corresponding digital multistep shift-register sequence defined by f and the initial values $y_0, \ldots, y_{k-1}$ satisfies*

$$\begin{aligned}
D_T^{*(s)}(f) &\le \frac{1}{T} + \frac{1}{p^k}\sum_{w=0}^{s-1}(p-1)^w\binom{k}{w} \\
&\quad \times \Bigg[s(s-1)\frac{p}{p-1}\cdot\frac{2}{1-\gamma}k\frac{p^k}{\phi(T)}{}_p\log\left(k\frac{p^k}{\phi(T)}\right) \\
&\quad + (s-1)\frac{p}{p-1}\cdot\frac{2}{1-\gamma}k\frac{p^k}{\phi(T)}\left(1+{}_p\log\frac{2(s-1)}{1-\gamma}\right)+\frac{1+\gamma}{1-\gamma}\Bigg] \\
&= \mathcal{O}\left(\frac{(\log T)^s(\log\log T)^2}{T}\right)
\end{aligned}$$

is at least $\gamma|\mathcal{Q}|$. (Here ϕ is Euler's totient function.)

Proof. The proof runs along the same lines as the proof of Theorem 1. So it suffices to give the following details.

By Theorem 9.5 of [4], the p^k points $\mathbf{0}, \mathbf{x}_0, \ldots, \mathbf{x}_{T-1}$ form a digital net over F_p defined by s matrices $C_1, \ldots, C_s$ with rows $c_j^i \in F_p^k$ with $1 \le j \le k$ for $1 \le i \le s$ with the following property: for non-negative integers $d_i \le k$, $i = 1, \ldots, s$, the system of vectors $\{c_j^i : 1 \le j \le d_i,\ 1 \le i \le s\}$ is linearly dependent over F_p if and only if the system $\{\alpha^{(i-1)k+j-1} : 1 \le j \le d_i,\ 1 \le i \le s\}$ is. Here α is a root of f in F_{p^k}, viewed as an element of the vector space F_{p^k} over F_p. In the following we consider admissible w-tuples of integers with respect to the matrices $A_i(f)$ with rows $\alpha^{(i-1)k+j}$, $j = 0, \ldots, k-1$, for $i = 1, \ldots, s$. For a non-negative integer c, for an s-tuple of non-negative integers $\mathbf{d} := (d_1, \ldots, d_s)$ with $d_1 + \ldots + d_s = k - c$ and $\lambda := (\lambda_1, \ldots, \lambda_{k-c}) \in F_p^{k-c}\backslash\{\mathbf{0}\}$ let $\mathcal{M}(c, \lambda, \mathbf{d})$ be the set of $f \in \mathcal{Q}$ satisfying

$$\begin{aligned}
&\lambda_1\alpha^0 + \ldots + \lambda_{d_1}\alpha^{d_1-1} + \lambda_{d_1+1}\alpha^k + \ldots + \lambda_{d_1+d_2}\alpha^{k+d_2-1} + \ldots \\
&\qquad \ldots + \lambda_{d_1+\ldots+d_{s-1}+1}\alpha^{(s-1)k} + \ldots + \lambda_{d_1+\ldots+d_s}\alpha^{(s-1)k+d_s-1} = 0.
\end{aligned}$$

Then

$$|\mathcal{M}(c, \lambda, \mathbf{d})| \le \left[\frac{(s-1)k+k-1}{k}\right] = s-1.$$

This follows from the fact that the equation in the definition of $\mathcal{M}(c, \lambda, \mathbf{d})$ has at most $(s-1)k + d_s - 1$ solutions α, and that for every such solution α, all k simple roots of the defining primitive polynomial f of α satisfy the equation.

Therefore, by proceeding quite analogously to the proof of Theorem 1, and since $|\mathcal{Q}| = \phi(p^k-1)/k$, letting $\mathcal{M}(c)$ be the set of $f \in \mathcal{Q}$ such that there exist $d_1, \ldots, d_s > 0$ with $d_1 + \ldots + d_s = k - c$ and with $\alpha^0, \ldots, \alpha^{d_1-1}, \alpha^k, \ldots$ $\ldots, \alpha^{k+d_2-1}, \ldots, \alpha^{(s-1)k}, \ldots, \alpha^{(s-1)k+d_s-1}$ linearly dependent over F_p, we have

$$|\mathcal{M}(c)| \le |\mathcal{Q}| \frac{p^k}{\phi(p^k-1)} k(s-1) p^{-c} \binom{k-c-1}{s-1} =: |\mathcal{Q}| R(c).$$

Let $\overline{\mathcal{M}}(c) := \mathcal{Q} \setminus \mathcal{M}(c)$. Then $|\overline{\mathcal{M}}(c)| \ge |\mathcal{Q}|(1-R(c))$. Proceeding as in the proof of Theorem 1 we get

$$\begin{aligned} \sum &:= \frac{1}{|\overline{\mathcal{M}}(c)|} \sum_{f \in \overline{\mathcal{M}}(c)} D_T^{*(s)}(f) \\ &\le \frac{1}{p^k} \sum_{w=0}^{s-1} (p-1)^w \binom{k}{w} \left[\frac{p^k}{|\overline{\mathcal{M}}(c)|} c(s-1) \frac{p}{p-1} + 1 \right] =: A(c). \end{aligned}$$

We then easily finish the proof like the proof of Theorem 1. The $\mathcal{Q}$-result comes from the fact that $x/\phi(x) = \mathcal{O}(\log\log x)$. ■

(b) *The GFSR method*. This method is due to Lewis and Payne [1]. Let p be a prime, and let $k \ge 2$ be an integer. For a primitive characteristic polynomial f of degree k over F_p we define the sequence $(y_n)_{n=0,\dots,T-1}$ of period $T = p^k - 1$ as in the digital multistep method. For $m \ge 2$ we then choose integers $h_1, \dots, h_m \ge 0$ and we put

$$x_n := \sum_{j=1}^{m} y_{n+h_j} p^{-j} \quad \text{for } n = 0, 1, \dots$$

This GFSR sequence has period T. In the following we again consider the case $m = k$.

It was shown in [2] (see also Theorem 9.17 of [4]) that for given f of degree $k \ge s \ge 2$ and given initial values $y_0, \dots, y_{k-1}$ not all zero (and for $m = k$), for the star-discrepancy $D_T^{*(s)}(h_1, \dots, h_k)$ of the s-dimensional serial set $\mathbf{x}_n := (x_n, x_{n+1}, \dots, x_{n+s-1})$, $n = 0, \dots, T-1$, of the corresponding GFSR sequence $(x_n)_{n=0,\dots,T-1}$ we have on the average

$$D_T^{*(s)}(h_1, \dots, h_k) \le c(p,s) \frac{(\log T)^s}{T}$$

with an implied constant depending only on p and s, where the average is taken over all $H = (h_1, \dots, h_k)$ with $0 \le h_j \le T-1$ for $1 \le j \le k$. Let $\mathcal{H}$ be the system of all such k-tuples H. Then again for every γ with $0 < \gamma < 1$, the number of H for which $D_T^{*(s)}(H)$ satisfies

$$D_T^{*(s)}(H) \le \frac{1}{1-\gamma} c(s,p) \frac{(\log T)^s}{T}$$

is at least $\gamma|\mathcal{H}|$. The following Theorem 3 is an improvement of this result:

THEOREM 3. *For a prime p let $s \ge 2$, $m = k \ge s$, a primitive polynomial f of degree k over F_p, and initial values $y_0, \dots, y_{k-1}$, not all zero, be given.*

Let $T := p^k - 1$. For fixed γ, $0 < \gamma < 1$, the number of $H \in \mathcal{H}$ for which the star-discrepancy $D_T^{*(s)}(H)$ of the s-dimensional serial set of the GFSR sequence defined by f, H and the initial values satisfies

$$\begin{aligned} D_T^{*(s)}(B) \le \frac{1}{T} + \frac{1}{p^k} \sum_{w=0}^{s-1} (p-1)^w \binom{k}{w} \\ \times \Big[(s-1)\Big(\frac{p}{p-1}\Big)^2 \frac{2}{1-\gamma} {}_p\log k \\ + \Big(\frac{p}{p-1}\Big)^2 \frac{2}{1-\gamma} \Big(1 + {}_p\log \frac{4}{1-\gamma}\Big) + \frac{1+\gamma}{1-\gamma} \Big] \\ = \mathcal{O}\Big(\frac{(\log T)^{s-1} \log\log T}{T} \Big) \end{aligned}$$

is at least $\gamma|\mathcal{H}|$.

Proof. Again (see Theorem 9.14 of [4]), $\mathbf{0}, \mathbf{x}_0, \ldots, \mathbf{x}_{T-1}$ form a digital net over F_p with the matrices $A_i(h)$ with rows α^{i-1+h_j}, $j = 1, \ldots, k$, $i = 1, \ldots, s$ (α a root of f in F_{p^k}), playing the role of $A_i(B)$ and $A_i(f)$ in the proofs of Theorems 1 and 2, respectively.

For a non-negative c we define the sets $\mathcal{M}(\lambda, \mathbf{d})$ and $\mathcal{M}(c)$ as in the proofs of the above theorems. The equation in the definition of $\mathcal{M}(\lambda, \mathbf{d})$ is then equivalent to

$$\sum_{j=1}^{k} \xi_j \alpha^{h_j} = 0 \quad \text{with} \quad \xi_j := \sum_{i=0}^{s-1} \lambda_{d_1+\ldots+d_i+j} \alpha^j.$$

Since $s \le k$ and since α is a primitive element in F_{p^k}, we see that for $\lambda \ne \mathbf{0}$ not all ξ_j are zero and therefore (again since α generates F_{p^k} and since $0 \le h_j \le p^k - 2$ for all j) we have $|\mathcal{M}(\lambda, \mathbf{d})| \le T^{k-1}$. Consequently,

$$|\mathcal{M}(c)| \le |\mathcal{H}| \binom{k-c-1}{s-1} p^{k-c} \frac{1}{T} =: |\mathcal{H}| R(c)$$

and with $\overline{\mathcal{M}}(c) := \mathcal{H} \setminus \mathcal{M}(c)$ we get

$$\begin{aligned} \frac{1}{|\overline{\mathcal{M}}(c)|} \sum_{H \in \mathcal{H}} D_T^{*(s)}(H) \\ \le \frac{1}{p^k} \sum_{w=0}^{s-1} (p-1)^w \binom{k}{w} \Big[1 + \frac{|\mathcal{H}|}{|\overline{\mathcal{M}}(c)|} \cdot \frac{p}{p-1} \cdot \frac{1}{1 - 1/p^k} c \Big] \\ =: A(c). \end{aligned}$$

We finish the proof like the proofs of Theorems 1 and 2. ∎

References

[1] T. G. Lewis and W. H. Payne, *Generalized feedback shift register pseudorandom number algorithm*, J. Assoc. Comput. Mach. 20 (1973), 456–468.

[2] H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987), 273–337.

[3] —, *The serial test for digital k-step pseudorandom numbers*, Math. J. Okayama Univ. 30 (1988), 93–119.

[4] —, *Random Number Generation and Quasi-Monte Carlo Methods*, CBMS-NSF Regional Conf. Ser. in Appl. Math. 63, SIAM, Philadelphia, 1992.

[5] —, *Factorization of polynomials and some linear-algebra problems over finite fields*, Linear Algebra Appl. 192 (1993), 301–328.

[6] —, *The multiple recursive matrix method for pseudorandom number generation*, Finite Fields Appl. 1 (1995), 3–30.

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

[8] H. Niederreiter and C. P. Xing, *Low-discrepancy sequences obtained from algebraic function fields over finite fields*, Acta Arith. 72 (1995), 281–298.

[9] —, —, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. 2 (1996), 241–273.

[10] —, —, *Quasirandom points and global function fields*, in: S. Cohen and H. Niederreiter (eds.), Finite Fields and Applications (Glasgow, 1995), London Math. Soc. Lecture Note Ser. 233, Cambridge Univ. Press, Cambridge, 1996, 269–296.

[11] K. F. Roth, *On irregularities of distribution*, Mathematika 1 (1954), 73–79.

[12] W. M. Schmidt, *Irregularities of distribution*, *VII*, Acta Arith. 21 (1972), 45–50.

[13] R. C. Tausworthe, *Random numbers generated by linear recurrence modulo two*, Math. Comp. 19 (1965), 201–209.

Institut für Mathematik
Universität Salzburg
Hellbrunnerstr. 34
A-5020 Salzburg, Austria
E-mail: Gerhard.Larcher@sbg.ac.at
Web: http://www.mat.sbg.ac.at/people/larcher.html

Received on 8.10.1996
and in revised form on 4.4.1997 (3056)