On the Distribution of Some New Explicit Nonlinear Congruential Pseudorandom Numbers

Harald Niederreiter[1] and Arne Winterhof[2]

[1] Department of Mathematics, National University of Singapore,
2 Science Drive 2, Singapore 117543, Republic of Singapore
nied@math.nus.edu.sg

[2] Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences,
Altenbergerstr. 69, 4040 Linz, Austria
arne.winterhof@oeaw.ac.at

Abstract. Nonlinear methods are attractive alternatives to the linear congruential method for pseudorandom number generation. We introduce a new particularly attractive explicit nonlinear congruential method and present nontrivial results on the distribution of pseudorandom numbers generated by this method over the full period and in parts of the period. The proofs are based on new bounds on certain exponential sums over finite fields.

Keywords: Pseudorandom numbers, Nonlinear method, Discrepancy.

1 Introduction

Let $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ be the finite field of prime order $p \geq 3$. Further let $\eta \in \mathbb{F}_p^*$ be an element of multiplicative order $T \geq 2$. For a given polynomial $f(X) \in \mathbb{F}_p[X]$ of positive degree D we generate a sequence $\gamma_0, \gamma_1, \ldots$ of elements of $\mathbb{F}_p$ by

$$\gamma_n = f(\eta^n) \qquad \text{for } n = 0, 1, \ldots. \tag{1}$$

This sequence is purely periodic with least period t for some $t|T$. We may restrict ourselves to the case where $t = T$ and $D < T$. If $D < T$, then we have $t = T$ if and only if, for all proper divisors d of T, the polynomial $f(X)$ is not of the form $f(X) = g(X^{T/d})$ with a polynomial $g(X) \in \mathbb{F}_p[X]$. For example, this is guaranteed if T is a prime or if $f(X)$ is a permutation polynomial of $\mathbb{F}_p$ (or more generally, $f(X)$ is injective on the group generated by η).

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

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

where χ is a nontrivial additive character of $\mathbb{F}_p$. Upper bounds for these exponential sums are then applied to the analysis of a new nonlinear method for

T. Helleseth et al. (Eds.): SETA 2004, LNCS 3486, pp. 266–274, 2005.

pseudorandom number generation. This new method is defined as follows. We derive *explicit nonlinear congruential pseudorandom numbers of period* T in the interval $[0,1)$ by putting

$$y_n = \gamma_n/p, \quad n = 0, 1, \ldots.$$

After some auxiliary results in Section 2 we prove some new bounds for complete and incomplete exponential sums over finite fields in Section 3 which allow us to give nontrivial results on the distribution of sequences of explicit nonlinear congruential pseudorandom numbers of period T. The application to explicit nonlinear congruential pseudorandom numbers is presented in Section 4.

Similar results on a different family of explicit nonlinear congruential pseudorandom numbers of period p were obtained in [13].

2 Auxiliary Results

We recall Weil's bound on additive character sums (see [8–Theorem 5.38], [19–Chapter II, Theorem 2E]).

Lemma 1. *Let* χ *be a nontrivial additive character of* $\mathbb{F}_p$ *and* g *be a nonconstant polynomial over* $\mathbb{F}_p$*. Then we have*

$$\left| \sum_{\xi \in \mathbb{F}_p} \chi(g(\xi)) \right| \le (\deg(g) - 1)p^{1/2}.$$

For the following analog on hybrid character sums see [19–Chapter II, Theorem 2G].

Lemma 2. *Let* χ *be a nontrivial additive character and* ψ *a nontrivial multiplicative character of* $\mathbb{F}_p$ *and* g *a nonconstant polynomial over* $\mathbb{F}_p$*. Then we have*

$$\left| \sum_{\xi \in \mathbb{F}_p} \chi(g(\xi))\psi(\xi) \right| \le \deg(g)p^{1/2}.$$

Lemma 3. *Let* $\gamma_0, \gamma_1, \ldots$ *be a sequence of the form (1). If* $\mu_0, \mu_1, \ldots, \mu_{s-1} \in \mathbb{F}_p$ *and*

$$\sum_{i=0}^{s-1} \mu_i \gamma_{n+i} = c, \quad 0 \le n \le T - 1,$$

for some $c \in \mathbb{F}_p$*, then either*

$$\mu_0 = \mu_1 = \ldots = \mu_{s-1} = 0$$

or

$$s \ge \mathrm{w}(f),$$

where $\mathrm{w}(f)$ *denotes the weight of* $f(X)$*, i. e., the number of nonzero coefficients of* $f(X)$*.*

Proof. We assume that not all μ_i are zero and denote by j the largest index with $\mu_j \neq 0$ (so $0 \leq j \leq s-1$). Then we have

$$\sum_{i=0}^{j} \mu_i \gamma_{n+i} = c, \quad 0 \leq n \leq T-1, \tag{2}$$

and

$$\sum_{i=1}^{j+1} \mu_{i-1} \gamma_{n+i} = c, \quad 0 \leq n \leq T-1. \tag{3}$$

Subtracting (3) from (2) yields

$$\mu_0 \gamma_n + \sum_{i=1}^{j} (\mu_i - \mu_{i-1}) \gamma_{n+i} - \mu_j \gamma_{n+j+1} = 0, \quad 0 \leq n \leq T-1.$$

Hence, $j+1$ is at least as large as the linear complexity L of the sequence $\gamma_0, \gamma_1, \ldots$, i.e., the order of the shortest linear recurrence relation over $\mathbb{F}_p$

$$\gamma_{n+L} = \sum_{i=0}^{L-1} \sigma_i \gamma_{n+i}, \quad 0 \leq n \leq T-1,$$

satisfied by the sequence. Lemma 3 follows from the well-known result

$$L = \mathrm{w}(f) \tag{4}$$

of Blahut [1]. We refer to [7–Section 6.8] for a proof. □

Put $\mathrm{e}_T(z) = \exp(2\pi i z/T)$.

Lemma 4. *For any integer* $1 \leq N \leq T$ *we have*

$$\sum_{u=1}^{T-1} \left| \sum_{n=0}^{N-1} \mathrm{e}_T(un) \right| \leq T \left(\frac{4}{\pi^2} \log T + 0.8 \right).$$

Proof. We have

$$\begin{aligned} \sum_{u=1}^{T-1} \left| \sum_{n=0}^{N-1} \mathrm{e}_T(un) \right| &= \sum_{u=1}^{T-1} \left| \frac{\sin(\pi N u/T)}{\sin(\pi u/T)} \right| \\ &\leq \frac{4}{\pi^2} T \log T + 0.38T + 0.608 + 0.116 \frac{\gcd(N,T)^2}{T} \end{aligned}$$

by [2–Theorem 1]. □

3 Bounds for Exponential Sums

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

$$S_N = \sum_{n=0}^{N-1} \chi\left(\sum_{i=0}^{s-1} \mu_i \gamma_{n+i}\right).$$

Theorem 1. *Let* $1 \le s < \mathrm{w}(f)$ *and suppose that* $\mu_0, \mu_1, \dots, \mu_{s-1} \in \mathbb{F}_p$ *are not all* 0*. Then we have*

$$|S_T| \le \left(D - \frac{T}{p-1}\right) p^{1/2} + \frac{T}{p-1}.$$

Proof. We have

$$\begin{aligned} |S_T| &= \left|\sum_{n=0}^{T-1} \chi\left(\sum_{i=0}^{s-1} \mu_i f(\eta^{n+i})\right)\right| \\ &= \frac{T}{p-1}\left|\sum_{\xi \in \mathbb{F}_p^*} \chi\left(\sum_{i=0}^{s-1} \mu_i f(\eta^i \xi^{(p-1)/T})\right)\right|. \end{aligned}$$

Since at least one μ_i is nonzero and $s < \mathrm{w}(f)$, Lemma 3 implies that

$$\sum_{i=0}^{s-1} \mu_i f(\eta^i X^{(p-1)/T})$$

is not constant and the result follows by Lemma 1. □

Theorem 2. *Let* $1 \le s < \mathrm{w}(f)$ *and suppose that* $\mu_0, \mu_1, \dots, \mu_{s-1} \in \mathbb{F}_p$ *are not all* 0*. Then we have*

$$|S_N| < D p^{1/2}\left(\frac{4}{\pi^2} \log T + 1.8\right) \qquad \textit{for } 1 \le N < T.$$

Proof. With $\sigma_n = \sum_{i=0}^{s-1} \mu_i \gamma_{n+i}$ we have

$$\begin{aligned} S_N &= \sum_{n=0}^{T-1} \chi(\sigma_n) \sum_{t=0}^{N-1} \frac{1}{T} \sum_{u=0}^{T-1} \mathrm{e}_T(u(n-t)) \\ &= \frac{1}{T} \sum_{u=0}^{T-1} \left(\sum_{t=0}^{N-1} \mathrm{e}_T(-ut)\right) \left(\sum_{n=0}^{T-1} \chi(\sigma_n) \mathrm{e}_T(un)\right) \\ &= \frac{N}{T} \sum_{n=0}^{T-1} \chi(\sigma_n) + \frac{1}{T} \sum_{u=1}^{T-1} \left(\sum_{t=0}^{N-1} \mathrm{e}_T(-ut)\right) \left(\sum_{n=0}^{T-1} \chi(\sigma_n) \mathrm{e}_T(un)\right), \end{aligned}$$

and so

$$|S_N| \le \frac{N}{T}|S_T| + \frac{1}{T}\sum_{u=1}^{T-1}\left|\sum_{t=0}^{N-1} \mathrm{e}_T(ut)\right|\left|\sum_{n=0}^{T-1}\chi(\sigma_n)\mathrm{e}_T(un)\right|.$$

For $1 \le u \le T-1$ we define the nontrivial multiplicative character ψ_u of $\mathbb{F}_p$ by

$$\psi_u(\vartheta^n) = \mathrm{e}_T(un), \quad 0 \le n \le p-2,$$

with a primitive element ϑ of $\mathbb{F}_p$. Then we have

$$\begin{aligned}\left|\sum_{n=0}^{T-1}\chi(\sigma_n)\mathrm{e}_T(un)\right| &= \frac{T}{p-1}\left|\sum_{\xi\in\mathbb{F}_p^*}\chi\left(\sum_{i=0}^{s-1}\mu_i f(\eta^i\xi^{(p-1)/T})\right)\psi_u(\xi)\right| \\ &\le Dp^{1/2}\end{aligned}$$

by Lemma 2. Lemma 4 yields

$$\begin{aligned}\sum_{u=1}^{T-1}\left|\sum_{t=0}^{N-1}\mathrm{e}_T(ut)\right|\left|\sum_{n=0}^{T-1}\chi(\sigma_n)\mathrm{e}_T(un)\right| &\le Dp^{1/2}\sum_{u=1}^{T-1}\left|\sum_{t=0}^{N-1}\mathrm{e}_T(ut)\right| \\ &\le Dp^{1/2}T\left(\frac{4}{\pi^2}\log T + 0.8\right).\end{aligned}$$

Hence we obtain by Theorem 1,

$$\begin{aligned}|S_N| \le \frac{N}{T}&\left(\left(D - \frac{T}{p-1}\right)p^{1/2} + \frac{T}{p-1}\right) \\ &+Dp^{1/2}\left(\frac{4}{\pi^2}\log T + 0.8\right).\end{aligned}$$

Simple calculations yield the theorem. □

4 Discrepancy Bound

We use the bounds for exponential sums obtained in Theorems 1 and 2 to derive results on the distribution of sequences of explicit nonlinear congruential pseudorandom numbers of period T over the full period and in parts of the period.

Let $\gamma_0/p, \gamma_1/p, \ldots$ be a sequence of explicit nonlinear congruential pseudorandom numbers of least period $T \ge 2$ obtained from (1) with a polynomial $f(X)$ of degree $D \ge 1$. For any integer $1 \le N \le T$ we define the *s-dimensional (extreme) discrepancy*

$$D_s(N) = \sup_J \left|\frac{A_N(J)}{N} - V(J)\right|,$$

where the supremum is extended over all subintervals J of $[0,1)^s$, $A_N(J)$ is the number of points

$$(\gamma_n/p, \dots, \gamma_{n+s-1}/p) \in [0,1)^s, \quad 0 \leq n \leq N-1,$$

falling into J, and $V(J)$ denotes the s-dimensional volume of J.

In the following we establish an upper bound for $D_s(N)$.

Theorem 3. *For any fixed integer* $1 \leq s < \mathrm{w}(f)$*, the* s*-dimensional discrepancy* $D_s(N)$ *satisfies*

$$D_s(N) < 1 - \left(1 - \frac{1}{p}\right)^s + \frac{Dp^{1/2}}{N}\left(\frac{4}{\pi^2}\log T + 1.8\right)\left(\frac{4}{\pi^2}\log p + 1.72\right)^s$$

for $1 \leq N < T$ *and*

$$D_s(T) \leq 1 - \left(1 - \frac{1}{p}\right)^s + \left(\left(D - \frac{T}{p-1}\right)\frac{p^{1/2}}{T} + \frac{1}{p-1}\right)\left(\frac{4}{\pi^2}\log p + 1.72\right)^s.$$

Proof. By a general discrepancy bound in [14–Corollary 3.11] we obtain

$$D_s(N) \leq 1 - \left(1 - \frac{1}{p}\right)^s + \frac{B}{N}\left(\frac{4}{\pi^2}\log p + 1.72\right)^s,$$

where B is the maximum over all $(\mu_0, \dots, \mu_{s-1}) \in \mathbb{F}_p^s \setminus (0, \dots, 0)$ of the exponential sums S_N. The result follows from Theorems 1 and 2. □

5 Final Remarks

For $1 \leq D \leq T-1$ with $\gcd(D, p-1) = 1$ and $a, b \in \mathbb{F}_p^*$, the polynomial

$$f(X) = a(X+b)^D = a\sum_{i=0}^{D}\binom{D}{i}b^{D-i}X^i \tag{5}$$

of weight $D+1$ is a permutation polynomial of $\mathbb{F}_p$, and so the sequence (1) has least period T. It has linear complexity $D+1$ by (4). Therefore and by [17–Section 2] it passes the D-dimensional lattice test introduced by Marsaglia (see [9]). In contrast to sequences defined with a general polynomial of large weight, it can be rather efficiently generated.

Theorem 3 is nontrivial only if D is at most of the order of magnitude $Tp^{-1/2}(\log p)^{-s}$. However, for polynomials of the form (5) with D close to $p-2$ (in case $T = p-1$), or more generally for rational functions of the form

$$f(X) = a(X+b)^{-d}$$

(with the convention $0^{-1} = 0$) with small d, we can obtain similar results using the following analogs of Lemmas 1 and 2 for rational functions which can be found in [12, 18].

Lemma 5. *Let χ be a nontrivial additive character of $\mathbb{F}_p$ and let f/g be a rational function over $\mathbb{F}_p$. Let v be the number of distinct roots of the polynomial g in the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. Suppose that f/g is not constant. Then*

$$\left| \sum_{\substack{\xi \in \mathbb{F}_p \\ g(\xi) \neq 0}} \chi\left(\frac{f(\xi)}{g(\xi)}\right) \right| \leq (\max(\deg(f), \deg(g)) + v^* - 2)p^{1/2} + \delta,$$

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

Lemma 6. *Let χ be a nontrivial additive character and ψ a nontrivial multiplicative character of $\mathbb{F}_p$ and let f/g be a rational function over $\mathbb{F}_p$. Let v be the number of distinct roots of the polynomial g in the algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. Then*

$$\left| \sum_{\substack{\xi \in \mathbb{F}_p^* \\ g(\xi) \neq 0}} \chi\left(\frac{f(\xi)}{g(\xi)}\right) \psi(\xi) \right| \leq (\max(\deg(f), \deg(g)) + v^* - 1)p^{1/2},$$

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

The particularly interesting case $d = 1$ is investigated in [20]. In this case we have the following main character sum bound.

Theorem 4. *If $\mu_1, \mu_2, \ldots, \mu_s$ are not all 0, then we have*

$$|S_N| < s\left(2p^{1/2} + 1\right)\left(\frac{4}{\pi^2}\log T + 1.8\right) \text{ for } 1 \leq N < T.$$

These *inversive generators* have also desirable structural properties (see [3, 4, 10]).

Mordell [11] established the bound

$$\left| \sum_{\xi \in \mathbb{F}_p} \mathrm{e}_p(f(\xi)) \right| \leq (k_1 k_2 \cdots k_w \gcd(p-1, k_1, k_2, \ldots, k_w))^{1/2w} p^{1-1/2w}$$

for polynomials of the type

$$f(X) = c_1 X^{k_1} + \cdots + c_w X^{k_w}, \quad 1 \leq k_1 < \ldots < k_w < p-1, \ p \nmid c_1 \cdots c_w.$$

This bound is nontrivial for a restricted set of polynomials of large degree and can be used to obtain nontrivial discrepancy bounds for these particular polynomials.

For the p-periodic sequences $\gamma_0, \gamma_1, \ldots$ defined by

$$\gamma_n = f(n) \quad \text{for } n = 0, 1, \ldots$$

we have discrepancy bounds of the same order of magnitude as in Theorem 3 for all dimensions s with $2 \leq s \leq \deg(f)$ (see [13]). For the analogous results on the inversive sequence

$$\gamma_n = (an + b)^{-1} \quad \text{for } n = 0, 1, \ldots$$

see [5]. Appropriate bounds for corresponding sequences over arbitrary finite fields were obtained in [16].

Recursively defined generators

$$\gamma_{n+1} = f(\gamma_n) \quad \text{for } n = 0, 1, \ldots$$

with some initial value u_0 were investigated in [15]. However, the results are much weaker than for the explicitly defined sequences. For the particular case of inversive sequences

$$\gamma_{n+1} = a\gamma_n^{-1} + b \quad \text{for } n = 0, 1, \ldots$$

much better results were proven in [6]. The character sum bounds are of the order of magnitude $O(N^{1/2}p^{1/4})$ (vs. $O(p^{1/2} \log p)$ in Theorem 4 or in [5]). The method of [6, 15] can also be applied to explicit generators yielding character sum bounds of the order of magnitude $O(N^{1/2}p^{1/4})$.

Acknowledgments

Parts of this paper were written during a visit of the second author to the National University of Singapore. He wishes to thank the Department of Mathematics for the hospitality. The second author is supported by the Austrian Academy of Sciences and by the Austrian Science Fund (FWF) grant S8313. The research of the first author is partially supported by the grant R-394-000-011-422 with Temasek Laboratories in Singapore.

References

1. Blahut, R.E.: Theory and Practice of Error Control Codes. Addison-Wesley, Reading, MA (1983)
2. Cochrane, T.: On a trigonometric inequality of Vinogradov. J. Number Theory **27** (1987) 9–16
3. Dorfer, G., Winterhof, A.: Lattice structure and linear complexity profile of nonlinear pseudorandom number generators. Appl. Algebra Engrg. Comm. Comput. **13** (2003) 499–508
4. Dorfer, G., Winterhof, A.: Lattice structure of nonlinear pseudorandom number generators in parts of the period. In: Niederreiter, H. (ed.): Monte Carlo and Quasi-Monte Carlo Methods 2002. Springer-Verlag, Berlin (2004) 199–211
5. Eichenauer-Herrmann, J.: Statistical independence of a new class of inversive congruential pseudorandom numbers. Math. Comp. **60** (1993) 375–384

6. Gutierrez, J., Niederreiter, H., Shparlinski, I.: On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period. Monatsh. Math. **129** (2000) 31–36
7. Jungnickel, D.: Finite Fields: Structure and Arithmetics. Bibliographisches Institut, Mannheim (1993)
8. Lidl, R., Niederreiter, H.: Finite Fields. Cambridge University Press, Cambridge (1997)
9. Marsaglia, G.: The structure of linear congruential sequences. In: Zaremba, S.K. (ed.): Applications of Number Theory to Numerical Analysis. Academic Press, New York (1972) 249–285
10. Meidl, W., Winterhof, A.: On the linear complexity profile of some new explicit inversive pseudorandom numbers. J. Complexity **20** (2004) 350–355
11. Mordell, L.J.: On a sum analogous to a Gauss's sum. Quart. J. Math. **3** (1932) 161–167
12. Moreno, C.J., Moreno, O.: Exponential sums and Goppa codes: I. Proc. Amer. Math. Soc. **111** (1991) 523–531
13. Niederreiter, H.: Statistical independence of nonlinear congruential pseudorandom numbers. Monatsh. Math. **106** (1988) 149–159
14. Niederreiter, H.: Random Number Generation and Quasi-Monte Carlo Methods. SIAM, Philadelphia (1992)
15. Niederreiter, H., Shparlinski, I.: On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. Finite Fields Appl. **5** (1999) 246–253
16. Niederreiter, H., Winterhof, A.: Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators. Acta Arith. **93** (2000) 387–399
17. Niederreiter, H., Winterhof, A.: Lattice structure and linear complexity of nonlinear pseudorandom numbers. Appl. Algebra Engrg. Comm. Comput. **13** (2002) 319–326
18. Perel'muter, G.I.: Estimate of a sum along an algebraic curve (Russian). Mat. Zametki **5** (1969) 373–380; Engl. transl. Math. Notes **5** (1969) 223–227
19. Schmidt, W.M.: Equations over Finite Fields. Lecture Notes in Mathematics, Vol. 536. Springer, Berlin (1976)
20. Winterhof, A.: On the distribution of some new explicit inversive pseudorandom numbers and vectors. In: Niederreiter, H., Talay, D. (eds.): Monte Carlo and Quasi-Monte Carlo Methods 2004, Springer, Berlin, to appear