Exponential sums of nonlinear congruential pseudorandom number generators with Rédei functions

Jaime Gutierrez a,*, Arne Winterhof b

a Faculty of Sciences, University of Cantabria, E-39071 Santander, Spain
b Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria

Received 31 October 2006; revised 11 March 2007
Available online 7 April 2007
Communicated by Gary L. Mullen

Dedicated to Peter M. Gruber on the occasion of his 65th birthday

Abstract

The nonlinear congruential method is an attractive alternative to the classical linear congruential method for pseudorandom number generation. We give new bounds of exponential sums with sequences of iterations of Rédei functions over prime finite fields, which are much stronger than bounds known for general nonlinear congruential pseudorandom number generators.

© 2007 Elsevier Inc. All rights reserved.

Keywords: Exponential sums; Nonlinear congruential generator; Rédei functions; Cryptography

1. Introduction

For an integer $q > 1$ we denote by $\mathbb{Z}_q$ the residue ring modulo $q$ and always assume that it is represented by the set $\{0, 1, \ldots, q - 1\}$. As usual, we denote by $\mathcal{U}_q$ the set of invertible elements of $\mathbb{Z}_q$.

Accordingly, for a prime $p$, we denote by $\mathbb{F}_p \cong \mathbb{Z}_p$ the field of $p$ elements and as before, we assume that it is represented by the set $\{0, 1, \ldots, p - 1\}$. In particular, sometimes, where obvious, we treat elements of $\mathbb{Z}_q$ and $\mathbb{F}_p$ as integers in the above range.

* Corresponding author.
E-mail addresses: jaime.gutierrez@unican.es (J. Gutierrez), arne.winterhof@oeaw.ac.at (A. Winterhof).
Given a polynomial \( F(X) \in \mathbb{F}_p[X] \) of degree at least 2, we define the nonlinear congruential generator \((x_n)\) of elements of \( \mathbb{F}_p \) by the recurrence relation

\[
x_{n+1} \equiv F(x_n) \pmod{p}, \quad n = 0, 1, \ldots, \tag{1}
\]

with some initial value \( x_0 \).

Recently in [7], a new method has been invented to study the distribution of such sequences for arbitrary polynomials \( F(X) \) by estimating exponential sums, see also recent surveys [6,9,10,13]. Unfortunately, for general polynomials, this method leads to rather weak bounds. However, in the special case of the inversive congruential generator this method leads to a much stronger bound [8]. For two other special classes of polynomials, namely for monomials and Dickson polynomials an alternative approach, producing much stronger bounds has been proposed in [1–3].

This article deals with another special case of the nonlinear congruential pseudorandom number generator constructed via Rédei functions defined in the sequel.

Suppose that

\[
r(X) = X^2 - \alpha X - \beta \in \mathbb{F}_p[X]
\]

is an irreducible quadratic polynomial with the two different roots \( \xi \) and \( \zeta = \xi^p \) in \( \mathbb{F}_{p^2} \). Then any polynomial \( b(X) \in \mathbb{F}_{p^2}[X] \) can uniquely be written in the form \( b(X) = g(X) + h(X)\xi \) with \( g(X), h(X) \in \mathbb{F}_p[X] \). For a positive integer \( e \) we consider the elements

\[
(X + \xi)^e = g_e(X) + h_e(X)\xi. \tag{2}
\]

Note that \( g_e(X) \) and \( h_e(X) \) do not depend on the choice of the root \( \xi \) of \( r(X) \). Evidently, \( e \) is the degree of the polynomial \( g_e(X) \), and \( h_e(X) \) has degree at most \( e - 1 \), where equality holds if and only if \( \gcd(e, p) = 1 \) (see also [4, p. 22], [12]). The Rédei function \( R_e(X) \) of degree \( e \) is then given by

\[
R_e(X) = \frac{g_e(X)}{h_e(X)}.
\]

The following facts can be found in [11]. The Rédei function \( R_e(X) \) is a permutation of \( \mathbb{F}_p \) if and only if \( \gcd(e, p + 1) = 1 \), the set of these permutations is a group with respect to the composition which is isomorphic to the group of units of \( \mathbb{Z}_{p+1} \). In particular for indices \( m, n \) with \( \gcd(m, p + 1) = \gcd(n, p + 1) = 1 \) we have

\[
R_m(R_n(u)) = R_{mn}(u) = R_n(R_m(u)) \quad \text{for all } u \in \mathbb{F}_p. \tag{3}
\]

For further background on Rédei functions we refer to [4,11,12].

We consider generators \((u_n)\) defined by

\[
u_{n+1} = R_e(u_n), \quad n \geq 0, \quad \gcd(e, p + 1) = 1,
\]

with a Rédei permutation \( R_e(X) \) and some initial element \( u_0 \in \mathbb{F}_p \). Note that each mapping over \( \mathbb{F}_p \) can be uniquely represented by a polynomial of degree at most \( p - 1 \) and therefore the generator \((u_n)\) belongs to the class of nonlinear congruential pseudorandom number generators (1).
The sequences \((u_n)\) are purely periodic, the period length \(T\) divides \(\varphi(p + 1)\), where \(\varphi\) denotes Euler’s totient function. For details we refer to [11, Lemma 3.5].

For \(a \in \mathbb{F}_p^*\) we define the exponential sum

\[
S_e(a) = \sum_{n=0}^{T-1} e_p(au_n),
\]

where \(e_p(z) = \exp(2\pi iz/p)\) for \(z \in \mathbb{F}_p\).

We apply the method of [1,3] to obtain an upper bound on sums \(|S_e(a)|\). We remark, however, that several specific properties of \(X_e\) do not hold for \(R_e(X)\) thus our result is slightly weaker than that of [1]. Although we follow the same general method of bounding exponential sums as in [3] the details of the crucial step that a certain auxiliary mapping, see (6) below, is not constant is much more intricate.

2. Preliminaries

We recall Lemma 2 from [1].

Lemma 1. For any set \(K \subseteq \mathcal{U}_t\) of cardinality \(\#K = K\), any fixed \(1 \leq \delta > 0\) and any integer \(t \geq h \geq t^\delta\) there exists an integer \(r \in \mathcal{U}_t\) such that the congruence

\[rk \equiv y \pmod{t}, \quad k \in K, \quad 0 \leq y \leq h - 1,\]

has

\[L_r(h) \gg \frac{Kh}{t}\]

solutions \((k, y)\).

Note that each \(k\) corresponds at most one solution \((k, y)\).

We also need the following bound on exponential sums [5, Theorem 2].

Lemma 2. Let \(p\) be a prime and \(f/g\) 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

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

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

3. Main result

Let \(t\) be the smallest positive integer for which \(R_e(u_0) \equiv R_f(u_0) \pmod{p}\) whenever \(e \equiv f \pmod{t}\). Note that \(t \mid p + 1\) and \(T\) is the multiplicative order of \(e\) modulo \(t\).
Theorem 3. For every fixed integer \( v \geq 1 \),
\[
\max_{a \in \mathbb{F}_p^*} |S_e(a)| = O\left(T^{1-\frac{2v+1}{2v+3+1}} p^{\frac{1}{2v+4+1}} \right),
\]
where the implied constant depends only on \( v \).

Proof. We put
\[
h = \left\lceil t^{\frac{v}{v+1}} T^{\frac{v}{v+1}} p^{\frac{1}{2v+4+1}} \right\rceil.
\]
Since otherwise the result is trivial we may assume \( h < p^{-1/2} T < t \). Because \( t \geq T \), for this choice of \( h \) we obtain \( h \geq p^{1/2(v+1)} \), thus Lemma 1 applies.

Because the sequence \((u_n)\) is purely periodic, for any \( k \in \mathbb{Z}_t \), we have:
\[
S_e(a) = \sum_{n=1}^{T} e_p(a R_{e^{n+k}}(u_0)).
\]

Let \( \mathcal{K} \) be the subgroup of \( \mathcal{U}_t \) generated by \( e \). Thus \( \#\mathcal{K} = T \). We select \( r \) as in Lemma 1 and let \( \mathcal{L} \) be the subset of \( \mathcal{K} \) which satisfies the corresponding congruence. We denote \( L = \#\mathcal{L} \). In particular, \( L \gg hT/t \).

By (4) we have
\[
LS_e(a) = \sum_{n=1}^{T} \sum_{k \in \mathcal{L}} e_p(a R_{e^{n+k}}(u_0)).
\]

Applying the Hölder inequality, we derive
\[
L^{2v} |S_e(a)|^{2v} \leq T^{2v-1} \sum_{n=1}^{T} \left| \sum_{k \in \mathcal{L}} e_p(a R_{e^{n+k}}(u_0)) \right|^{2v}.
\]

Let \( 1 \leq s \leq t - 1 \), be defined by the congruence \( rs \equiv 1 \pmod{t} \). By (3) we obtain
\[
R_{e^{n+t}}(u_0) \equiv R_{e^{n+krs}}(u_0) \equiv R_{re^s} R_{se^r}(u_0) \pmod{p}.
\]

Obviously, the values of \( se^n \), \( n = 1, \ldots, T \), are pairwise distinct modulo \( t \). Thus, from the definition of \( t \), we see that the values of \( R_{se^r}(u_0) \) are pairwise distinct modulo \( p \). Therefore, from (5) we derive
\[
L^{2v} |S_e(a)|^{2v} \leq T^{2v-1} \sum_{u \in \mathbb{F}_p} \left| \sum_{k \in \mathcal{L}} e_p(a R_{re^k}(u)) \right|^{2v}.
\]

Denoting \( \mathcal{F} = \{ re^k \mid k \in \mathcal{L} \} \) we deduct
\[ L^{2v} \left| S_v(a) \right|^{2v} \leq T^{2v-1} \sum_{u \in \mathbb{F}_p} \left| \sum_{f \in \mathcal{F}} e_p(a R_f(u)) \right|^{2v} \]
\[ \leq T^{2v-1} \sum_{f_1, \ldots, f_{2v} \in \mathcal{F}} \sum_{u \in \mathbb{F}_p} e_p \left( a \sum_{j=1}^{v} (R_{f_j}(u) - R_{f_{v+j}}(u)) \right). \]

For the case that \((f_{v+1}, \ldots, f_{2v})\) is a permutation of \((f_1, \ldots, f_v)\), we use the trivial bound for the inner sum over \(u\), which gives the total contribution \(O(L^v p)\).

Otherwise, we claim that the rational function

\[ \Psi_{f_1, \ldots, f_{2v}}(X) = \sum_{j=1}^{v} \left( R_{f_j}(X) - R_{f_{v+j}}(X) \right) \]

is non-constant. In fact, there exist \(\{k_1, \ldots, k_U\} \subset \{f_1, \ldots, f_v, f_{v+1}, \ldots, f_{2v}\}\) and \(c_1, \ldots, c_U \in \mathbb{F}_p^*\) with

\[ 1 \leq k_1 < k_2 < \cdots < k_U, \quad 1 < U \leq 2v, \]

satisfying

\[ \Psi_{f_1, \ldots, f_{2v}}(X) = \sum_{i=1}^{U} c_ig_{k_i}(X) \]

Multiplying with

\[ H(X) = \prod_{i=1}^{U} h_{k_i}(X) \]

we get the polynomial

\[ G(X) = \sum_{i=1}^{U} c_ig_{k_i}(X) \prod_{j \neq i} h_{k_j}(X). \]

With (2) we obtain

\[ (X + \xi)^k - (X + \zeta)^k = (\xi - \zeta)h_k(X). \]

Hence, \(h_k(x_0) = 0\) if and only if

\[ \left( \frac{x_0 + \xi}{x_0 + \zeta} \right)^k = 1. \]
i.e., \((x_0 + \xi)/(x_0 + \zeta)\) is a \(k\)th root of unity. We may assume \(k_U \leq f_{2\nu} < p\). Let \(\rho\) be a primitive \(k_U\)th root of unity in an appropriate extension field of \(\mathbb{F}_p\). We note by (7) that \(\rho \neq 1\). Then

\[
x_0 = \frac{\xi - \rho \zeta}{\rho - 1}
\]

is a root of \(h_{k_U}\) and \(h_{k_j}(x_0) \neq 0\) for the remaining \(h_{k_j}\) that appear in \(H(X)\), and

\[
G(x_0) = c_U g_{k_U}(x_0) \prod_{1 \leq j < U} h_{k_j}(x_0).
\]

It can easily be seen with (2) that \(g_{k_U}(x_0) \neq 0\), thus \(G(x_0) \neq 0\) and hence \(G(X)\) is not the zero polynomial. Taking into account that \(\deg g_f = f\), \(\deg h_f \leq f - 1\) and

\[
\max_{j=1, \ldots, 2\nu} f_j \leq \max_{f \in \mathcal{F}} f < h
\]

we have

\[
\Psi_{f_1, \ldots, 2\nu}(X) = G(X)/H(X), \quad \deg H, \deg G < 2\nu h.
\]

Since \(G(x_0) \neq 0\) but \(H(x_0) = 0\) the rational function \(G(X)/H(X)\) cannot be constant and Lemma 2 applies. We obtain that the total contribution from such terms is \(O(L^{2\nu} h p^{1/2})\). Hence

\[
L^{2\nu} |S_e(a)|^{2\nu} = O\left(T^{2\nu-1} \left(L^\nu p + L^{2\nu} h p^{1/2}\right)\right).
\]

So this leads us to the bound

\[
|S_e(a)|^{2\nu} = O\left(T^{2\nu-1} \left(L^{-\nu} p + h p^{1/2}\right)\right).
\]

Recalling that \(L \gg hT/t\), we derive

\[
|S_e(a)|^{2\nu} = O\left(T^{2\nu-1} \left(t^\nu T^{-\nu} h^{-\nu} p + h p^{1/2}\right)\right).
\]

Substituting the selected value of \(h\), which balances both terms in the above estimate, we finish the proof. \(\square\)

**Acknowledgments**

The first author is partially supported by the research project MTM2004-07086 of the Spanish Ministry of Science and Technology. The second author is supported by the Austrian Academy of Sciences and by the grant P19004-N18 of the Austrian Science Fund (FWF). Parts of the paper were written during a visit of A.W. to the University of Cantabria. He wishes to thank for the hospitality and financial support. He also wishes to thank the doctors and nurses of the University Hospital of Valdecilla.
References