Multiplicative Character Sums with Counter-Dependent Nonlinear Congruential Pseudorandom Number Generators

Domingo Gomez *

Faculty of Sciences
University of Cantabria
Avd. Los Castros, Santander, Spain.
domingo.gomez@unican.es

Abstract. Nonlinear congruential pseudorandom number generators can have unexpectedly short periods. Shamir and Tsaban introduced the class of counter-dependent generators which admit much longer periods. In this paper we present a bound for multiplicative character sums for nonlinear sequences generated by counter-dependent generators.

1 Introduction

Let $q = p^r$, where p is a prime number. In this paper we study a multiplicative character sum related with the distribution properties of the powers and primitive elements of *counter-dependent nonlinear congruential pseudorandom number generators*. This class of generators was introduced by [16] and it is defined by a recurrence of the form

$$u_{n+1} = f(u_n, n), \quad u_n \in \mathbb{F}_q, \qquad n = 0, 1, \ldots, \tag{1}$$

with some *initial value* u_0, where $f(X, Y) \in \mathbb{F}_q[X, Y]$ is a polynomial over the field $\mathbb{F}_q$ of q elements of local degree in X at least 2. It is well-known that the problem of studying the distribution of primitive roots and powers can be reduced to bound a multiplicative character sum, see, for example [9].

It is obvious that the sequence (1) eventually becomes periodic with some period $t \leq qp$. Throughout this paper we assume that this sequence is *purely periodic*, that is, $u_n = u_{n+t}$ beginning with $n = 0$, otherwise we consider a shift of the original sequence.

The case $f(X, Y) = h(X) \in \mathbb{F}_q[X]$, which does not depend on the second variable, is the well-studied *nonlinear congruential pseudorandom number generators*, see [5, 8, 11], the surveys [18, 19] and references therein. A bound in the corresponding multiplicative character sum was given in [10]. On the other hand,

* This work was partially supported by the Spanish Government. Research Grant MTM 2004-07086. Also, I want to thank A. W. for his time and patience.

these generators have their own limits, for example the period t is at most q. So, it is interesting to study more general pseudorandom number generators.

The *counter-assisted nonlinear congruential pseudorandom number generators* were defined in [16]. They are defined by the following linear recurrence:

$$u_{n+1} = h(u_n) + n \pmod p \quad 0 \le u_n \le p-1, \qquad n = 0, 1, \dots ,$$

where $h(X) \in \mathbb{F}_p[X]$. For this specific class, the linear complexity and exponential sums were studied in [2]. These generators are related to *nonlinear congruential pseudorandom number generators of order* 2 defined by

$$u_{n+2} = f(u_{n+1}, u_n) \pmod p, \quad 0 \le u_n \le p-1, \qquad n = 0, 1, \dots$$

Nonlinear congruential pseudorandom number generators of order $m \ge 2$ have been analyzed in [3, 4] in particular cases and solve for the general case in [13]. The results in these papers treat the distribution of values, not distribution of powers. The linear complexity was studied in [17], so this shows that the problem is not trivial at all.

A general class of pseudorandom number generators of higher orders has been studied in [12, 14]. This class has attracted a lot of attention, however to get a bound on the corresponding multiplicative character sum can only be done under certain conditions, see [15].

2 Definitions and Auxiliary Results

All the needed results are adapted, but the general properties of resultants and their proofs can be found in [1]. We use the classical abbreviation of $\deg_X$ to refer to the degree of a polynomial in the variable X.

The resultant is a classical concept that arises from commutative algebra. We suppose that we are working in $\mathbb{K}[X, Y]$, the ring of bivariate polynomials with coefficients in a field $\mathbb{K}$. Given two polynomials $f(X, Y), g(X, Y) \in \mathbb{K}[X, Y]$, where

$$f(X, Y) = \sum_{i=0}^{d_1} f_i(Y) X^i, \qquad g(X, Y) = \sum_{i=0}^{d_2} g_i(Y) X^i.$$

the *Sylvester matrix respect the variable* X is

$$\begin{pmatrix}
f_0(Y) & f_1(Y) & \dots & f_{d_1}(Y) & 0 & \dots & 0 & 0 \\
0 & f_0(Y) & f_1(Y) & \dots & f_{d_1}(Y) & 0 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & 0 & 0 & \dots & f_0(Y) & \dots & f_{d_1-1}(Y) & f_{d_1}(Y) \\
g_0(Y) & g_1(Y) & \dots & g_{d_2}(Y) & 0 & \dots & 0 & 0 \\
0 & g_0(Y) & g_1(Y) & \dots & g_{d_2}(Y) & 0 & \dots & 0 \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\
0 & 0 & 0 & \dots & g_0(Y) & \dots & g_{d_2-1}(Y) & g_{d_2}(Y)
\end{pmatrix}.$$

This matrix is a $(d_1 + d_2) \times (d_1 + d_2)$ matrix, the first row is the coefficients of $f(X, Y)$ depending on Y, adding zeros to fill the $(d_1 + d_2)$ positions. Notice that the next $d_2 - 1$ rows are shifts of the first row. The other rows are built using the polynomial $g(X, Y)$.

The determinant of this matrix is known as the resultant of the polynomials f and g respect of the variable X. We will denote it by $Res_X(f(X, Y), g(X, Y))$. The following Lemma shows the relation between resultant and common factors. It is a Corollary of [1, Proposition 1, Section 3.6].

Lemma 1 *Given* $f(X, Y), g(X, Y) \in \mathbb{F}_q[X, Y]$ *then*

$$\deg_X(\gcd(f(X, Y), g(X, Y))) \geq 1$$

if and only if

$$Res_X(f(X, Y), g(X, Y)) = 0.$$

In [6, Corollary 5.1], the author presented a relation between the composition of polynomials and resultants. His result is very general, so here is an adapted version for the proofs.

Lemma 2 *Let* $f(X, Y),\ g(X, Y),\ h(X, Y) \in \mathbb{K}[X, Y]$ *be polynomials such as* $\deg_X(f(X, Y)), \deg_X(g(X, Y)),\ \deg_X(h(X, Y)) \geq 1$ *then,*

$$Res_X(f(h(X, Y), Y), g(h(X, Y), Y)) = Res_X(f(X, Y), g(X, Y))^{\deg_X(h(X,Y))}.$$

The next Lemma is a weaker version of the Bezout Theorem.

Lemma 3 *Let* $f(X, Y), g(X, Y) \in \mathbb{K}[X, Y]$, *with* $\gcd(f(X, Y), g(X, Y)) = 1$ *then the number of common roots is at most the product of the degrees of the polynomials.*

For a polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$ of total degree d we define the sequence of polynomials $f_k(X, Y) \in \mathbb{F}_q[X, Y]$ by the recurrence relation

$$f_{k+1}(X, Y) = f_k\left(f(X, Y), Y + 1\right), \qquad k = 0, 1, \ldots, \tag{2}$$

where $f_0(X, Y) = X$. It is clear that $\deg(f_k(X, Y)) \leq d^k$ and for the sequence define in (1) that

$$u_{n+k} = f_k\left(u_n, n\right). \tag{3}$$

The following property will be necessary in the proof of the main theorem:

Lemma 4 *Given the sequence* $f_k(X, Y) \in \mathbb{F}_q[X, Y]$ *defined in* (2) *and if*

$$\deg_X(\gcd(f_k(X, Y), f_l(X, Y))) \geq 1$$

then

$$\deg_X(\gcd(f_{k-i}(X, Y), f_{l-i}(X, Y))) \geq 1, \quad \forall i \leq \min(k, l).$$

Proof. Now, we regard the polynomials $f_k(X,Y),\ f_l(X,Y)$ as polynomials in the variable X whose coefficients are in the ring $\mathbb{F}_q[Y]$ and let

$$H(Y) = Res_X(f_{k-1}(X,Y), f_{l-1}(X,Y)).$$

Using simple properties of the Sylvester Matrix, we have:

$$Res_X(f_{k-1}(X,Y+1), f_{l-1}(X,Y+1)) = H(Y+1)$$

and, using Lemma 2, we get that:

$$Res_X(f_{k-1}(f(X,Y),Y+1), f_{l-1}(f(X,Y),Y+1) = H(Y+1)^{\deg_X(f(X,Y))}.$$

Applying the Lemma 1,

$$H(Y+1)^{\deg_X(f(X,Y))} = Res_X(f_k(X,Y), f_l(X,Y)) = 0.$$

This clearly implies that $H(Y) = 0$, therefore, again by Lemma 1 we get

$$\gcd(f_{k-1}(X,Y), f_{l-1}(X,Y)) = H_1(X,Y),\ \deg_X(H_1(X,Y)) \geq 1.$$

Applying the same argument i times, we get the result. □

Now, we are going to introduce some notation. Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$, with the standard convention $\chi(0) = 0$. We want to prove an upper bound on this character sum

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

Next, we recall the classical Weil bound on multiplicative character sums (see [7, Chapter 5]) for univariate polynomials.

Lemma 5 *Let χ be a character of $\mathbb{F}_q$ of order s and let $F(X) \in \mathbb{F}_q[X]$ be a polynomial of positive degree that is not, up to a multiplicative constant, an sth power of a polynomial. Let d be a bound on the number of distinct roots in its splitting field over $\mathbb{F}_q$. Under these conditions, the following inequality*

$$\left| \sum_{x \in \mathbb{F}_q} \chi\left(F(x)\right) \right| \leq dq^{1/2}$$

holds.

With this Lemma we can prove another result that we will use through later.

Lemma 6 *Let χ be a character of $\mathbb{F}_q$ of order s and let $F(X,Y) \in \mathbb{F}_q[X,Y]$ be a polynomial of positive degree such that $F(X,Y)$ is not, up to a multiplicative constant, an sth power of a polynomial. Let $F(X,Y) = F_1(X,Y)^{d_1} \cdots F_h(X,Y)^{d_h}$*

the decomposition of the polynomial in a product of irreducible polynomials. Let D be a bound on the total degree of $F_1(X,Y)\cdots F_h(X,Y)$. Under these conditions, the following inequality holds

$$\left|\sum_{x,y\in\mathbb{F}_q}\chi\left(F(x,y)\right)\right| \leq 2Dq^{3/2}.$$

Proof. This Lemma is trivial when $2D \geq q^{1/2}$ so suppose that $2D \leq q^{1/2}$. Without loss of generality, d_1 is not an integer multiple of s, because $F(X,Y)$ is not an sth power of a polynomial up to a multiplicative constant. Next,

$$\left|\sum_{x,y\in\mathbb{F}_q}\chi\left(F_1(x,y)^{d_1}\ldots F_h(x,y)^{d_h}\right)\right| \leq \sum_{y\in\mathbb{F}_q}\left|\sum_{x\in\mathbb{F}_q}\chi\left(F_1(x,y)^{d_1}\ldots F_h(x,y)^{d_h}\right)\right|.$$

Our aim is to apply Lemma 5 to each of the sums for y fixed. We have to count how many times we can not apply Lemma 5. The special cases are:

- When the polynomial $F(X,y)$ is a constant polynomial.
- When the polynomial $F(X,y)$ is an sth power.

There are, at most, D different values y where the polynomial $F(X,y)$ could be a constant polynomial.

Now, we consider in which cases the polynomial $F(X,y)$ is an sth power of a polynomial and how these cases will be counted.

First of all, we remark that $F(X,Y)$ is not an sth power of a polynomial, so if $F(X,y)$ is an sth power of a polynomial then we have this two possible nonexclusive situations:

- $F_1(X,y)^{d_1}$ is an sth power, so because d_1 is not an s multiple then we must have that $F_1(X,b)$ has, at least, one multiple root. This is only possible if $F_1(X,b)$ and the first derivative of the polynomial have a common root. $F_1(X,Y)$ is an irreducible polynomial, so Lemma 3 applies. We remark that the first derivative is a nonzero polynomial. Otherwise $F_1(X,Y)$ is a power of a polynomial, thus reducible. This can only happen in $\deg_X(F_1)(\deg_X(F_1)-1)$ cases.
- $F_1(X,b)$ and $F_s(X,b)$ have a common root and, by the same argument, there are at most $\deg_X(F_1)\deg_X(F_s)$ possible values where it happens.

So, for each value of $y\in\mathbb{F}_q$, we apply Lemma 6 if the two previous cases do not occur. In the other cases, we apply the trivial bound,

$$\begin{aligned}\sum_{y\in\mathbb{F}_q}\left|\sum_{x\in\mathbb{F}_q}\chi\left(F(x,y)\right)\right| &\leq Dq + q\deg_X(F_1)\sum_{i=1}^{h}\deg_X(F_i) + Dq^{3/2}\\ &\leq (D^2+D)q + Dq^{3/2} \leq 2Dq^{3/2}.\end{aligned}$$

The last inequality holds because $2 \leq 2D \leq q^{1/2}$ and this remark finishes the proof. □

We call the sequence (v_n), given by (1) with $v_0 = 0$. Note that under the assumption that (u_n) is purely periodic, the sequence (v_n) need not be purely periodic. Let t_0 be the least period of the sequence (v_n) if it is purely periodic and put $t_0 = \infty$ otherwise. We are ready to prove the principal theorem:

Theorem 7. *Let the sequence (u_n), given by (1) with a polynomial $f(X,Y)$ with coefficients in $\mathbb{F}_q[X,Y]$ and total degree $d \geq 2$ be purely periodic with period t and $t \geq N \geq 1$. If $f_k(X,Y), 1 \leq k \leq \lceil 0.4(\log q)/\log d \rceil$ is not, up to a multiplicative constant, an sth power of a polynomial, then the bound*

$$S_\chi(N) = O\left(N^{1/2} q \left(\min\left(\frac{\log q}{\log d}, t_0\right)\right)^{-1/2}\right)$$

holds, where the implied constant is absolute.

Proof. We can suppose that $q \geq 3$. For any integer $k \geq 0$ we have

$$\left| S_\chi(N) - \sum_{n=0}^{N-1} \chi(u_{n+k}) \right| \leq 2k,$$

so for any $K \geq 1$ and summing over $k = 0, 1 \ldots, K-1$, we get

$$K|S_\chi(N)| \leq W + \left| \sum_{k=0}^{K-1} \left(S_\chi(N) - \sum_{n=0}^{N-1} \chi(u_{n+k}) \right) \right| \leq W + K^2$$

where

$$W = \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi(u_{n+k}) \right|.$$

By the Cauchy-Schwarz inequality and (3) we obtain

$$W^2 \leq N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi(u_{n+k}) \right|^2 = N \sum_{n=0}^{N-1} \left| \sum_{k=0}^{K-1} \chi(f_k(u_n, n)) \right|^2$$

$$\leq N \sum_{x,y \in \mathbb{F}_q} \left| \sum_{k=0}^{K-1} \chi(f_k(u_n, n)) \right|^2 \leq N \sum_{k,l=0}^{K-1} \left| \sum_{x,y \in \mathbb{F}_q} \chi(f_k(x,y)) \overline{\chi}(f_l(x,y)) \right|$$

where $\overline{\chi}(f_l(x,y))$ denotes the conjugate of $\chi(f_l(x,y))$.

Because χ is a multiplicative character it is trivial to see that $\chi(a^{q-2}) = \overline{\chi}(a)$, $\forall a \in \mathbb{F}_q$.

Substituting the conjugates, we get the following inequality:

$$W^2 \leq N \sum_{k,l=0}^{K-1} \left| \sum_{x,y \in \mathbb{F}_q} \chi(f_k(x,y) f_l(x,y)^{q-2}) \right|.$$

Next we have to show that for $0 \leq l \leq k \leq K-1$ the polynomial $F(X,Y) = f_k(X,Y) f_l(X,Y)^{q-2}$, $k \geq l$ is, up to a multiplicative constant, an sth power of a polynomial only if $k \equiv l \mod t_0$, where $k \equiv l \mod \infty$ means $k = l$.

Suppose $g(X,Y) = \gcd(f_k(X,Y), f_l(X,Y))$ has degree at least 1 in X. By Lemma 4, $\gcd(f_0(X,Y) = X, f_{k-l}(X,Y))$ is a non constant polynomial in X. Because X is a prime polynomial, we have that the greatest common divisor between $f_0(X,Y)$ and $f_{k-l}(X,Y)$ is X so $v_{k-l} = 0$ and, consequently, $k - l \equiv 0 \mod t_0$.

Now suppose $k \not\equiv l \bmod t_0$ and thus $g(X,Y) = 1$. Hence, if $F(X,Y)$ is (up to a multiplicative constant) an sth power, then both $f_k(X,Y)$ and $f_l(X,Y)$ are (up to multiplicative constants) sth powers, which is a contradiction to our assumption provided that K is small enough (this will be guaranteed by the subsequent choice of K). Now the number of pairs $(k,l) \in \mathbb{Z}^2$ with $0 \leq l < k \leq K-1$ and $k \equiv l \bmod t_0$ is at most $K^2/(2t_0)$. For these pairs (k,l) we estimate the inner sum in the last bound on W^2 trivially by q. For all other pairs we can use Lemma 6 and get

$$W^2 < KNq^2 + K^2 N \left(\frac{q^2}{t_0} + 2d^{K-1} q^{3/2} \right).$$

With

$$K := \left\lceil 0.4 \frac{\log q}{\log d} \right\rceil$$

we get the result and this finishes the proof. □

References

1. David Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, New York, third edition, 2007. An introduction to computational algebraic geometry and commutative algebra.
2. Edwin El-Mahassni and Arne Winterhof. On the distribution and linear complexity of counter-dependent nonlinear congruential pseudorandom number generators. *Journal of Algebra, Number Theory and Applications*, 2:1–6, 2006.
3. Frances Griffin, Harald Niederreiter, and Igor E. Shparlinski. On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Comput. Sci.*, pages 87–93. Springer, Berlin, 1999.
4. Jaime Gutierrez and Domingo Gomez-Perez. Iterations of multivariate polynomials and discrepancy of pseudorandom numbers. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 192–199. Springer, Berlin, 2001.

5. Jaime Gutierrez, Igor E. Shparlinski, and Arne Winterhof. On the linear and nonlinear complexity profile of nonlinear pseudorandom number-generators. *IEEE Trans. Inform. Theory*, 49(1):60–64, 2003.
6. Hoon Hong. Subresultants under composition. *J. Symbolic Comput.*, 23(4):355–365, 1997.
7. Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.
8. Harald Niederreiter and Igor E. Shparlinski. On the distribution and lattice structure of nonlinear congruential pseudorandom numbers. *Finite Fields Appl.*, 5(3):246–253, 1999.
9. Harald Niederreiter and Igor E. Shparlinski. On the distribution of power residues and primitive elements in some nonlinear recurring sequences. *Bull. London Math. Soc.*, 35(4):522–528, 2003.
10. Harald Niederreiter and Arne Winterhof. Multiplicative character sums for nonlinear recurring sequences. *Acta Arith.*, 111(3):299–305, 2004.
11. Harald Niederreiter and Arne Winterhof. Exponential sums for nonlinear recurring sequences. *Finite Fields Appl.*, 14(1):59–64, 2008.
12. Alina Ostafe. Multivariate permutation polynomial systems and nonlinear pseudorandom number generators. *Finite Fields and Their Applications*, 16(3):144–154, 2010.
13. Alina Ostafe, Elena Pelican, and Igor E. Shparlinski. On pseudorandom numbers from multivariate polynomial systems. *Finite Fields and their Applications (to appear)*, 2010.
14. Alina Ostafe and Igor E. Shparlinski. On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators. *Math. Comp.*, 79(269):501–511, 2010.
15. Alina Ostafe, Igor E. Shparlinski, and Arne Winterhof. Multiplicative character sums of a class of nonlinear recurrence vector sequences. *Preprint*, 2010.
16. Adi Shamir and Boaz Tsaban. Guaranteeing the diversity of number generators. *Inform. and Comput.*, 171(2):350–363, 2001.
17. Alev Topuzoğlu and Arne Winterhof. On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders. *Appl. Algebra Engrg. Comm. Comput.*, 16(4):219–228, 2005.
18. Alev Topuzoğlu and Arne Winterhof. Pseudorandom sequences. In *Topics in geometry, coding theory and cryptography*, volume 6 of *Algebr. Appl.*, pages 135–166. Springer, Dordrecht, 2007.
19. Arne Winterhof. Recent results on recursive nonlinear pseudorandom number generators. In *Sequences and their Applications SETA 2010*, Lecture Notes in Comput. Sci. Springer, 2010.