ACTA ARITHMETICA
111.3 (2004)

Multiplicative character sums for nonlinear recurring sequences

by

HARALD NIEDERREITER and ARNE WINTERHOF (Singapore)

1. Introduction. Let q be a prime power, $\mathbb{F}_q$ the finite field of q elements, and $f(X)$ a polynomial over $\mathbb{F}_q$ of degree at least 2. Let (u_n) be the sequence of elements of $\mathbb{F}_q$ obtained by the recurrence relation

$$u_{n+1} = f(u_n), \quad n \geq 0,$$

with some initial value u_0. Obviously, this sequence eventually becomes periodic with least period $t \leq q$, but we restrict ourselves to the case where (u_n) is purely periodic.

Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$, with the standard convention $\chi(0) = 0$. We prove an upper bound on the character sums

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

in Section 2. We use the method introduced in [16] and extended and refined in the series of papers [3, 6–8, 13–15, 18, 21]; see also the surveys [17, 20] of this method and the recent exposition [25] of the general theory of character sums.

In Section 3 we apply this character sum bound and obtain results on the distribution of powers and primitive elements in the sequence (u_n).

Although several similar results on linear recurring sequences [11, 24] and explicitly defined sequences [1, 2, 4, 5, 10, 22, 26–28] were obtained with other methods, for nonlinear recurring sequences nontrivial character sum bounds have been out of reach. However, for some special inversive sequences the results of this paper can be essentially improved [19].

2. A character sum bound. Define the sequence of polynomials $f_k(X) \in \mathbb{F}_q[X]$ by the recurrence relation

2000 *Mathematics Subject Classification*: 11B37, 11L40, 11T23.
Key words and phrases: nonlinear recurring sequences, multiplicative character sums, powers in finite fields, primitive elements.

$$f_0(X) = X, \quad f_k(X) = f(f_{k-1}(X)), \quad k \ge 1,$$

and let (v_n) be the sequence defined by $v_0 = 0$ and $v_{n+1} = f(v_n)$, $n \ge 0$. Even under our 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. Then we can prove the following upper bound on $S_\chi(N)$.

THEOREM 1. *Let χ be a multiplicative character of $\mathbb{F}_q$ of order $s > 1$ and let $f(X) \in \mathbb{F}_q[X]$ with $d := \deg(f) \ge 2$. If $f_k(X)$, $1 \le k < \lceil 0.4(\log q)/\log d\rceil$, is not, up to a multiplicative constant, an sth power of a polynomial, then for $1 \le N \le t$ we have*

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

where the implied constant is absolute.

Proof. We can assume $q \ge 3$. For any integer $k \ge 0$ we have

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

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

$$K|S_\chi(N)| \le W + \Big|\sum_{k=0}^{K-1}\Big(S_\chi(N) - \sum_{n=0}^{N-1}\chi(u_{n+k})\Big)\Big| < W + K^2 \tag{1}$$

with

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

By the Cauchy–Schwarz inequality we obtain

$$W^2 \le N\sum_{n=0}^{N-1}\Big|\sum_{k=0}^{K-1}\chi(u_{n+k})\Big|^2 = N\sum_{n=0}^{N-1}\Big|\sum_{k=0}^{K-1}\chi(f_k(u_n))\Big|^2.$$

Completing the outer sum, we get

$$\begin{aligned} W^2 &\le N\sum_{c\in\mathbb{F}_q}\Big|\sum_{k=0}^{K-1}\chi(f_k(c))\Big|^2 \le N\sum_{k,l=0}^{K-1}\Big|\sum_{c\in\mathbb{F}_q}\chi(f_k(c)f_l(c)^{q-2})\Big| \\ &\le KNq + 2N\sum_{\substack{k,l=0\\k>l}}^{K-1}\Big|\sum_{c\in\mathbb{F}_q}\chi(f_k(c)f_l(c)^{q-2})\Big|. \end{aligned}$$

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

$g(X) := \gcd(f_k(X), f_l(X))$ has degree at least 1 and let α be a root of $g(X)$ in some extension field of $\mathbb{F}_q$. Since

$$f_{k-l}(0) = f_{k-l}(f_l(\alpha)) = f_k(\alpha) = 0,$$

we have $k - l \equiv 0 \bmod t_0$. Now suppose $k \not\equiv l \bmod t_0$ and thus $g(X) = 1$. Hence, if $F(X)$ is (up to a multiplicative constant) an sth power, then both $f_k(X)$ and $f_l(X)$ 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 $0 \le l < k \le K-1$ 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 Weil's bound (see [12, Theorem 5.41]) and get

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

With

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

and (1) we arrive at the desired result. ∎

Remark 1. If again $d = \deg(f)$ and s does not divide $\deg(f_k) = d^k$, then $f_k(X)$ is not, up to a multiplicative constant, an sth power. Furthermore, if $f(X)$ is a permutation polynomial of $\mathbb{F}_q$, then $f_k(X)$ is also a permutation polynomial of $\mathbb{F}_q$ and cannot be, up to a multiplicative constant, an sth power.

Remark 2. It is clear that the maximal value $t = q$ of the least period of (u_n) is obtained if and only if $f(X)$ is a permutation polynomial of $\mathbb{F}_q$ representing a permutation which is a cycle of length q. In this case we have $t = t_0$.

Remark 3. Let $f(X) = X^d$ with $d \ge 2$, $u_0 \ne 0$, and s be a divisor of $d-1$. Then it is clear that for a character χ of order s we have $\chi(u_n) = \chi(u_0)$ for all $n \ge 0$. This example provides some evidence that the dependence of the character sum bound on t_0 is natural.

Remark 4. Let $f(X) = (X+a)^d - a$ with $d \ge 2$, $a \in \mathbb{F}_q^*$, $u_0 = 0$. The sequence (u_n) generated by this polynomial can be obtained by subtracting a from a sequence as in Remark 3. Hence, both sequences have the same least period. For example, if q is even, $q-1$ a Mersenne prime, d the least primitive root modulo $q-1$, i.e., $d = O(\log^6(q-1))$ under ERH (see [23, Theorem 1.3]), and a is a primitive element of $\mathbb{F}_q$ (see the definition prior to Theorem 3), then we have $t = t_0 = q-2$. This shows that examples for which Theorem 1 gives a nontrivial bound can be easily constructed.

REMARK 5. From the equation

$$\sum_{c\in\mathbb{F}_q}\Big|\sum_{n=0}^{N-1}\chi(u_n+c)\Big|^2=\sum_{n,m=0}^{N-1}\sum_{c\in\mathbb{F}_q}\chi(u_n+c)\chi^{-1}(u_m+c)=N(q-N)$$

for $1\le N\le t$ and χ nontrivial, we see that for each sequence (u_n) there exists a shifted sequence (u_n+c) such that

$$\Big|\sum_{n=0}^{N-1}\chi(u_n+c)\Big|\le N^{1/2}\Big(1-\frac{N}{q}\Big)^{1/2}.$$

Furthermore, for almost all c, more precisely for all c but a fraction of $O(1/\log q)$, we have

$$\Big|\sum_{n=0}^{N-1}\chi(u_n+c)\Big|\le N^{1/2}(\log q)^{1/2}.$$

3. Distribution of powers and primitive elements. For a positive divisor s of $q-1$, an element $w\in\mathbb{F}_q^*$ is called an *sth power* if the equation $w=z^s$ has a solution in $\mathbb{F}_q$.

Let $R_s(N)$ be the number of sth powers among $u_0,u_1,\ldots,u_{N-1}$. Then, with the notation in Theorem 1, we have the following result.

THEOREM 2. *Let q be a prime power and $s>1$ be a divisor of $q-1$. If for all prime divisors r of s the polynomial $f_k(X)$, $1\le k<\lceil 0.4(\log q)/\log d\rceil$, is not, up to a multiplicative constant, an rth power of a polynomial, then*

$$R_s(N)=\frac{N}{s}+O\bigg(N^{1/2}q^{1/2}\bigg(\min\bigg(\frac{\log q}{\log d},t_0\bigg)\bigg)^{-1/2}\bigg)\quad \textit{for } 1\le N\le t.$$

Proof. Let X_s denote the set of multiplicative characters χ for which $\chi(w)=1$ for any sth power $w\in\mathbb{F}_q^*$. By [12, Theorem 5.4] we obtain

$$\frac{1}{s}\sum_{\chi\in X_s}\chi(w)=\begin{cases}1 & \text{if } w\in\mathbb{F}_q^* \text{ is an } s\text{th power},\\ 0 & \text{otherwise,}\end{cases}$$

where we used the convention $\chi_0(0)=0$ for the trivial character χ_0 of $\mathbb{F}_q$. Therefore

$$R_s(N)=\frac{1}{s}\sum_{\chi\in X_s}S_\chi(N).$$

The contribution to $R_s(N)$ of the sum corresponding to the trivial character is either $(N-1)/s$ or N/s. Therefore

$$\Big|R_s(N)-\frac{N}{s}\Big|\le\frac{1}{s}+\frac{1}{s}\sum_{\chi\in X_s\setminus\{\chi_0\}}|S_\chi(N)|,$$

and Theorem 1 implies the result. ∎

We recall that $w \in \mathbb{F}_q^*$ is a *primitive element* of $\mathbb{F}_q$ if it is not an sth power for any divisor $s > 1$ of $q-1$. For an integer $m \geq 1$ we denote by $\nu(m)$ the number of distinct prime divisors of m and by $\varphi(m)$ Euler's totient function.

Let $Q(N)$ be the number of primitive elements of $\mathbb{F}_q$ among $u_0, u_1, \ldots, u_{N-1}$. Then, with the notation in Theorem 1, we have the following result.

THEOREM 3. *If for all prime divisors r of $q-1$, the polynomial $f_k(X)$, $1 \leq k < \lceil 0.4(\log q)/\log d \rceil$, is not, up to a multiplicative constant, an rth power of a polynomial, then for $1 \leq N \leq t$ we have*

$$Q(N) = \frac{\varphi(q-1)}{q-1}\, N + O\biggl(2^{\nu(q-1)} N^{1/2} q^{1/2} \biggl(\min\left(\frac{\log q}{\log d}, t_0\right)\biggr)^{-1/2}\biggr).$$

Proof. From Vinogradov's formula (see [9, Lemma 7.5.3], [12, Exercise 5.14]) we obtain

$$Q(N) = \frac{\varphi(q-1)}{q-1} \sum_{s|(q-1)} \biggl(\frac{\mu(s)}{\varphi(s)} \sum_{\chi \in Y_s} S_\chi(N)\biggr),$$

where μ denotes the Möbius function and Y_s the set of multiplicative characters of $\mathbb{F}_q$ of order s. The rest follows from Theorem 1. ∎

REMARK 6. The theorem is only nontrivial if $2^{\nu(q-1)}$ is small. However, the sequence considered in Remark 4 above is an example for which Theorem 3 yields a nontrivial result.

REMARK 7. For any $\varepsilon > 0$ we can show that for all but a fraction of $O(q^{-\varepsilon})$ shifted sequences $(u_n + c)$ we have

$$Q(N) = \frac{\varphi(q-1)}{q-1}\, N + O(q^{\varepsilon} \max(Nq^{-1/4}, N^{1/2})).$$

For any divisor $s > 1$ of $q-1$ put

$$T_{N,s}(c) := \frac{1}{\varphi(s)} \sum_{\chi \in Y_s} \sum_{n=0}^{N-1} \chi(u_n + c).$$

Then we get

$$\sigma_{N,s} := \sum_{c \in \mathbb{F}_q} |T_{N,s}(c)|^2 = \frac{1}{\varphi(s)^2} \sum_{\chi,\psi \in Y_s} \sum_{n,m=0}^{N-1} \sum_{c \in \mathbb{F}_q} \chi(u_n + c)\psi^{-1}(u_m + c).$$

If $\chi = \psi$, then the inner sum is equal to -1 for $n \neq m$ and to $q-1$ for $n = m$. If $\chi \neq \psi$, then the inner sum can be estimated by $q^{1/2}$ by Weil's bound. Altogether, we get

$$\sigma_{N,s} < Nq + N^2 q^{1/2} \leq 2\max(Nq, N^2 q^{1/2}).$$

Thus, the number of $c \in \mathbb{F}_q$ with

$$|T_{N,s}(c)| > \sqrt{2}\, q^{2\varepsilon/3} \max(N^{1/2}, Nq^{-1/4})$$

is at most $q^{1-4\varepsilon/3}$. Now we have to consider the $2^{\nu(q-1)}-1 = O(q^{\varepsilon/3})$ different divisors $s > 1$ of $q-1$ with $\mu(s) \neq 0$ and get for all $c \in \mathbb{F}_q$ but $q^{1-\varepsilon}$ the bound

$$|T_{N,s}(c)| \leq \sqrt{2}\, q^{2\varepsilon/3} \max(N^{1/2}, Nq^{-1/4}) \quad \text{for all } s > 1 \text{ with } \mu(s) \neq 0.$$

Hence,

$$\begin{aligned} Q(N) - \frac{\varphi(q-1)}{q-1} N &= \frac{\varphi(q-1)}{q-1} \sum_{\substack{s|(q-1) \\ s>1}} \mu(s) T_{N,s}(c) \\ &= O(q^{\varepsilon} \max(N^{1/2}, Nq^{-1/4})) \end{aligned}$$

for almost all $c \in \mathbb{F}_q$.

Acknowledgments. The research of the authors is supported by the DSTA research grant R-394-000-011-422. The authors thank Jaime Gutierrez and Igor Shparlinski for useful discussions on the topic of this paper.

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), 179–192.

[2] —, *On Dirichlet characters of polynomials*, ibid. 13 (1963), 537–548.

[3] S. D. Cohen, H. Niederreiter, I. E. Shparlinski and M. Zieve, *Incomplete character sums and a special class of permutations*, J. Théor. Nombres Bordeaux 13 (2001), 53–63.

[4] H. Davenport, *On primitive roots in finite fields*, Quart. J. Math. 8 (1937), 308–312.

[5] H. Davenport and D. J. Lewis, *Character sums and primitive roots in finite fields*, Rend. Circ. Mat. Palermo (2) 12 (1963), 129–136.

[6] F. Griffin, H. Niederreiter and I. 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), Lecture Notes in Comput. Sci. 1719, Springer, Berlin, 1999, 87–93.

[7] J. Gutierrez and D. Gomez-Perez, *Iterations of multivariate polynomials and discrepancy of pseudorandom numbers*, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci. 2227, Springer, Berlin, 2001, 192–199.

[8] J. Gutierrez, H. Niederreiter and I. E. Shparlinski, *On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period*, Monatsh. Math. 129 (2000), 31–36.

[9] D. Jungnickel, *Finite Fields*: *Structure and Arithmetics*, Bibliographisches Institut, Mannheim, 1993.

[10] A. A. Karacuba, *Character sums and primitive roots in finite fields*, Soviet Math. Dokl. 9 (1968), 755–757; transl. from Dokl. Akad. Nauk SSSR 180 (1968), 1287–1289.

[11] N. M. Korobov, *The distribution of non-residues and of primitive roots in recurrence series*, Dokl. Akad. Nauk SSSR 88 (1953), 603–606 (in Russian).
[12] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, Cambridge, 1997.
[13] H. Niederreiter and I. E. Shparlinski, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers*, Finite Fields Appl. 5 (1999), 246–253.
[14] —, —, *Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus*, Acta Arith. 92 (2000), 89–98.
[15] —, —, *On the distribution of pseudorandom numbers and vectors generated by inversive methods*, Appl. Algebra Engrg. Comm. Comput. 10 (2000), 189–202.
[16] —, —, *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, Math. Comp. 70 (2001), 1569–1574.
[17] —, —, *Recent advances in the theory of nonlinear pseudorandom number generators*, in: Monte Carlo and Quasi-Monte Carlo Methods 2000, K.-T. Fang, F. J. Hickernell and H. Niederreiter (eds.), Springer, Berlin, 2002, 86–102.
[18] —, —, *On the average distribution of inversive pseudorandom numbers*, Finite Fields Appl. 8 (2002), 491–503.
[19] —, —, *On the distribution of power residues and primitive elements in some nonlinear recurring sequences*, Bull. London Math. Soc. 35 (2003), 522–528.
[20] —, —, *Dynamical systems generated by rational functions*, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Toulouse, 2003), Lecture Notes in Comput. Sci. 2643, Springer, Berlin, 2003, 6–17.
[21] H. Niederreiter and A. Winterhof, *On the distribution of compound inversive congruential pseudorandom numbers*, Monatsh. Math. 132 (2001), 35–48.
[22] G. I. Perel'muter and I. E. Shparlinskiĭ, *Distribution of primitive roots in finite fields*, Russian Math. Surveys 45 (1990), no. 1, 223–224; transl. from Uspekhi Mat. Nauk 45 (1990), no. 1, 185–186.
[23] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. 58 (1992), 369–380.
[24] I. E. Shparlinskiĭ [I. E. Shparlinski], *Distribution of nonresidues and primitive roots in recurrent sequences*, Mat. Zametki 24 (1978), 603–613 (in Russian).
[25] —, *Exponential sums in coding theory*, *cryptology and algorithms*, in: Coding Theory and Cryptology, H. Niederreiter (ed.), World Scientific, Singapore, 2002, 323–383.
[26] A. Winterhof, *On the distribution of powers in finite fields*, Finite Fields Appl. 4 (1998), 43–54.
[27] —, *Some estimates for character sums and applications*, Des. Codes Cryptogr. 22 (2001), 123–131.
[28] —, *Character sums*, *primitive elements*, *and powers in finite fields*, J. Number Theory 91 (2001), 153–163.

Department of Mathematics
National University of Singapore
2 Science Drive 2
Singapore 117543, Republic of Singapore
E-mail: nied@math.nus.edu.sg

Temasek Laboratories
National University of Singapore
10 Kent Ridge Crescent
Singapore 119260, Republic of Singapore
E-mail: tslwa@nus.edu.sg

Received on 18.4.2003 (4515)