Multiplicative Character Sums of Recurring Sequences with Rédei Functions

Domingo Gomez[1] and Arne Winterhof[2]

[1] Faculty of Sciences, University of Cantabria
E-39071 Santander, Spain
domingo.gomez@unican.es
[2] Johann Radon Institute for Computational
and Applied Mathematics (RICAM)
Austrian Academy of Sciences
Altenbergerstr. 69, 4040 Linz, Austria
arne.winterhof@oeaw.ac.at

Abstract. We prove a new bound for multiplicative character sums of nonlinear recurring sequences with Rédei functions over a finite field of prime order. This result is motivated by earlier results on nonlinear recurring sequences and their application to the distribution of powers and primitive elements. The new bound is much stronger than the bound known for general nonlinear recurring sequences.

1 Introduction

Let p be a prime, $\mathbb{F}_p$ the finite field of p elements, and $F(X)$ a rational function over $\mathbb{F}_p$. Let (u_n) be the sequence of elements of $\mathbb{F}_p$ obtained by the recurrence relation

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

with some initial value $u_0 \in \mathbb{F}_p$. Obviously, this sequence eventually becomes periodic with least period $T \leq p$, but we may restrict ourselves to the case where (u_n) is purely periodic since otherwise we can consider a shift of the sequence.

Let χ be a nontrivial multiplicative character of $\mathbb{F}_p$. We consider character sums

$$S_\chi = \sum_{n=1}^{T} \chi(u_n).$$

Bounds on S_χ can be applied to obtain results on the distribution of powers and primitive roots modulo p in the sequence (u_n) in a standard way, see e.g. [8].

In the special case of *linear recurring sequences* these sums are well-studied, see [3, 4, 11].

When $F(X) \in \mathbb{F}_p[X]$ is a polynomial of degree at least 2, in [8] under some natural restrictions on $F(X)$ the general but rather weak upper bound

$$S_\chi = O\left(T^{1/2} p^{1/2} (\log p)^{-1/2}\right)$$

and an analog for sums over parts of the period were given which are nontrivial whenever $T > p(\log p)^{-1}$. Here the implied constant depends only on the degree of $F(X)$. Note that each mapping of $\mathbb{F}_p$ can be represented by a polynomial. However, a representation as rational mapping can provide much stronger results.

For example, in the special case

$$F(X) = aX^{p-2} + b, \quad a \in \mathbb{F}_p^*,\ b \in \mathbb{F}_p,$$

the much stronger result

$$S_\chi = O\left(T^{1/2}p^{1/4}\right)$$

was obtained in [7], which is nontrivial whenever $T > p^{1/2}$. Since $x^{p-2} = x^{-1}$ for all $x \in \mathbb{F}_p^*$ the sequence (u_n) can up to at most one sequence element be defined with the rational function $F(X) = aX^{-1} + b$.

In [2] we investigated another special class of nonlinear recurring sequences (1) constructed via *Dickson polynomials* $F(X) = D_e(X) \in \mathbb{F}_p[X]$ defined by the recurrence relation

$$D_e(X) = XD_{e-1}(X) - D_{e-2}(X), \qquad e = 2, 3, \dots,$$

with initial values

$$D_0(X) = 2, \qquad D_1(X) = X.$$

Under the condition $\gcd(e, p^2-1) = 1$, which characterizes the Dickson permutation polynomials, see [5, Theorem 3.2], we obtained nontrivial bounds provided that $T > p^{1/2+\varepsilon}$ and if $T = p^{1+o(1)}$ we obtained

$$S_\chi = O\left(p^{7/8+o(1)}\right).$$

This article deals with the special class of nonlinear recurring sequences (1) constructed via *Rédei functions* defined in the sequel, which have some similar properties as Dickson polynomials.

Suppose that

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

is an irreducible quadratic polynomial with the two different roots ξ 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 ξ 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 [5, p. 22] or [10]. 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 [9]. 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 [5, 9, 10].

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 $u_0 \in \mathbb{F}_p$. The sequences (u_n) are purely periodic and the period length T divides $\varphi(p+1)$, where φ denotes Euler's totient function. For details we refer to [9, Lemma 3.5].

Although we follow the same general method of bounding character sums as in [2] the details of the crucial step that a certain auxiliary polynomial, see (6) below, is not of the form $ag(X)^s$, where s denotes the order of χ, is much more intricate.

2 Preliminaries

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

We recall Lemma 2 from [1].

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

$$rk \equiv y \pmod{t}, \qquad k \in \mathcal{K},\ 0 \leq y \leq h-1,$$

has

$$L_r(h) \gg \frac{Kh}{t}$$

solutions (k, y).

We also need the *Weil bound* for character sums which we present in the following form, see e.g. [6, Theorem 5.41].

Lemma 2. *Let χ be a multiplicative character of $\mathbb{F}_p$ of order $s > 1$ and let $F(X) \in \mathbb{F}_p[X]$ be a polynomial of positive degree that is not, up to a multiplicative constant, an sth power of a polynomial. Let d be the number of distinct roots of $F(X)$ in its splitting field over $\mathbb{F}_p$. Then we have*

$$\left| \sum_{x \in \mathbb{F}_p} \chi\left(F(x)\right) \right| \leq (d-1)p^{1/2}.$$

3 Main result

Let t be the smallest positive integer for which $R_e(u_0) = R_f(u_0)$ whenever $e \equiv f \pmod{t}$. Note that $t|p+1$ and T is the multiplicative order of e modulo t.

Theorem 1. *For every fixed integer $\nu \geq 1$ and nontrivial multiplicative character χ of $\mathbb{F}_p$ we have*

$$S_\chi = O\left(T^{1-\frac{2\nu+1}{2\nu(\nu+1)}} t^{\frac{1}{2(\nu+1)}} p^{\frac{\nu+2}{4\nu(\nu+1)}}\right),$$

where the implied constant depends only on ν.

Proof. We put

$$h = \left\lceil t^{\frac{\nu}{\nu+1}} T^{\frac{-\nu}{\nu+1}} p^{\frac{1}{2(\nu+1)}} \right\rceil .$$

Because $t \geq T$, for this choice of h we obtain $h \geq p^{1/2(\nu+1)}$, thus Lemma 1 applies.

Because the sequence (u_n) is purely periodic, for any $k \in \mathbb{Z}_t$, we have:

$$S_\chi = \sum_{n=1}^{T} \chi(R_{e^{n+k}}(u_0)). \tag{4}$$

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

$$LS_\chi = \sum_{n=1}^{T} \sum_{k\in\mathcal{L}} \chi\left(R_{e^{n+k}}(u_0)\right).$$

Applying the Hölder inequality, we derive

$$L^{2\nu}|S_\chi|^{2\nu} \leq T^{2\nu-1} \sum_{n=1}^{T} \left| \sum_{k\in\mathcal{L}} \chi\left(R_{e^{n+k}}(u_0)\right) \right|^{2\nu}. \tag{5}$$

Let $1 \leq r' \leq t-1$, be defined by the congruence $rr' \equiv 1 \pmod{t}$. By (3) we obtain

$$R_{e^{n+k}}(u_0) \equiv R_{e^{n+k}rr'}(u_0) \equiv R_{re^k}\left(R_{r'e^n}(u_0)\right) \pmod{p}.$$

Obviously, the values of $r'e^n$, $n = 1, \ldots, T$, are pairwise distinct modulo t. Thus, from the definition of t, we see that the values of $R_{r'e^n}(u_0)$ are pairwise distinct. Therefore, from (5) we derive

$$L^{2\nu}|S_\chi|^{2\nu} \leq T^{2\nu-1} \sum_{u\in\mathbb{F}_p} \left| \sum_{k\in\mathcal{L}} \chi\left(R_{re^k}(u)\right) \right|^{2\nu}.$$

Denoting $\mathcal{F} = \{re^k \mid k \in \mathcal{L}\}$ we deduct

$$\begin{aligned} L^{2\nu}|S_\chi|^{2\nu} &\leq T^{2\nu-1} \sum_{u \in \mathbb{F}_p} \left| \sum_{f \in \mathcal{F}} \chi\left(R_f(u)\right) \right|^{2\nu} \\ &\leq T^{2\nu-1} \sum_{f_1,\ldots,f_{2\nu} \in \mathcal{F}} \sum_{u \in \mathbb{F}_p} \chi\left(\prod_{j=1}^{\nu} \left(R_{f_j}(u) \left(R_{f_{\nu+j}}(u)\right)^{p-2} \right) \right). \end{aligned}$$

For the case that no integer in the set $(f_1, \ldots, f_{\nu+1}, \ldots, f_{2\nu})$ appears only once we use the trivial bound p for the inner sum. Since in this case there are at most ν different values in $(f_1, \ldots, f_{\nu+1}, \ldots, f_{2\nu})$ there are at most L^ν such cases, which gives the total contribution

$$O(L^\nu p).$$

Otherwise, to apply Lemma 2 we have to show that the polynomial

$$\Psi_{f_1,\ldots,f_{2\nu}}(X) = \prod_{j=1}^{\nu} \left(g_{f_j}(X) h_{\nu+j}(X) (h_j(X) g_{f_{\nu+j}}(X))^{p-2} \right) \tag{6}$$

is not, up to a multiplicative constant, an sth-power of a polynomial, where $s > 1$ denotes the order of χ. We cancel all elements which appear in both sets $\{f_1, \ldots, f_\nu\}$ and $\{f_{\nu+1}, \ldots, f_{2\nu}\}$. Let $f > 1$ be the largest number in $\{f_1, \ldots, f_{2\nu}\}$ which is not eliminated. We may assume $f < p$. We show that $g_f(X)$ has a zero which is neither a zero of any $h_{f'}(X)$ with $f' < f$ nor a zero of any $g_{f'}(X)$ with $f' \leq f$.

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

$$\left(\frac{x_0 + \xi}{x_0 + \zeta} \right)^k = 1, \tag{7}$$

i.e., $(x_0 + \xi)/(x_0 + \zeta)$ is a k-th root of unity. Similarly using

$$\zeta(X + \xi)^k - \xi(X + \zeta)^k = (\zeta - \xi) g_k(X)$$

we get $g_k(x_0) = 0$ if and only if

$$\left(\frac{x_0 + \xi}{x_0 + \zeta} \right)^k = \frac{\xi}{\zeta} = \zeta^{p-1}.$$

Let $\alpha > 1$ be the order of ζ^{p-1}, i.e., $\alpha | p+1$, put $l = \alpha f$ and let ρ be a suitable primitive lth root of unity in an appropriate extension field of $\mathbb{F}_p$, which exists since $f < p$ and thus $\gcd(l, p) = 1$, such that

$$z_0 = \frac{\xi - \rho\zeta}{\rho - 1}$$

is a root of $g_f(X)$. Obviously we have $g_{f'}(z_0) \neq 0$ for $f' < f$. It can easily be seen with (7) that $h_{f'}(z_0) \neq 0$ for $f' \leq f$ since otherwise we had $\rho^{f'} = 1$.

Taking into account that the number of distinct roots of $\Psi_{f_1,\dots,f_{2\nu}}(X)$ is less than $2\nu h$ and it cannot be an sth-power, Lemma 2 applies. We obtain that the total contribution from such terms is $O(L^{2\nu} h p^{1/2})$. Hence

$$L^{2\nu}|S_\chi|^{2\nu} = O\left(T^{2\nu-1}\left(L^\nu p + L^{2\nu} h p^{1/2}\right)\right).$$

So this leads us to the bound

$$|S_\chi|^{2\nu} = O\left(T^{2\nu-1}\left(L^{-\nu} p + h p^{1/2}\right)\right).$$

Recalling that $L \gg hT/t$, we derive

$$|S_\chi|^{2\nu} = O\left(T^{2\nu-1}\left(t^\nu T^{-\nu} h^{-\nu} p + h p^{1/2}\right)\right).$$

Substituting the selected value of h, which balances both terms in the above estimate, we finish the proof. □

Remark. As for the bound for Dickson polynomials we mention the following simplifications.

Assuming that $T = t^{1+o(1)}$, the bound of Theorem 1 takes the form

$$S_\chi = O\left(T^{1-1/2\nu+o(1)} p^{(\nu+2)/4\nu(\nu+1)}\right).$$

Therefore for any $\delta > 0$, choosing a sufficiently large ν we obtain a nontrivial bound provided $T \geq p^{1/2+\delta}$.

On the other hand, if $t \geq T = p^{1+o(1)}$, then taking $\nu = 1$ we obtain

$$|S_\chi| = O\left(p^{7/8+o(1)}\right).$$

Acknowledgment

Parts of this paper were written during a pleasant stay of D.G. to Linz. He wishes to the Radon Institute for its hospitality. A.W. was supported in part by the Austrian Science Fund (FWF) Grant P19004-N18.

References

1. J. B. Friedlander, J. Hansen and I. E. Shparlinski, On character sums with exponential functions, *Mathematika* **47** (2000), 75–85.
2. D. Gomez and A. Winterhof, Character sums for sequences of iterations of Dickson polynomials, *Lecture Notes in Comput. Sci.*, to appear.
3. 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).

4. N. M. Korobov, *Exponential sums and their applications*, Mathematics and its Applications (Soviet Series), 80. Kluwer Academic Publishers Group, Dordrecht, 1992.
5. R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Math., Longman, London-Harlow-Essex, (1993).
6. R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, (1997).
7. H. Niederreiter and I. E. Shparlinski, On the distribution of power residues and primitive elements in some nonlinear recurring sequences, *Bull. London Math. Soc.* **35** (2003), 522–528.
8. H. Niederreiter and A. Winterhof, Multiplicative character sums for nonlinear recurring sequences, *Acta Arith.* **111** (2004), 299-305.
9. R. Nöbauer, Rédei-Permutationen endlicher Körper, in: J. Czermak et al. (Eds.), Contributions to General Algebra 5, Hölder-Pichler-Tempsky, Vienna, 1987, pp. 235–246.
10. L. Rédei, Über eindeutig umkehrbare Polynome in endlichen Körpern, *Acta Sci. Math.* **11** (1946), 85–92.
11. I. E. Shparlinskiĭ, Distribution of nonresidues and primitive roots in recurrent sequences, *Matem. Zametki* **24** (1978), 603–613 (in Russian).