Multiplicative Character Sums for Nonlinear Recurring Sequences with Dickson Polynomials

Domingo Gomez
and
Arne Winterhof
Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenberger Straße 69, A-4040 Linz, Austria.
{domingo.gomez}{arne.winterhof}@oeaw.ac.at

December 15, 2009

Abstract

We give new bounds of character sums with sequences of iterations of Dickson polynomials over finite fields. This result is motivated by possible applications of nonlinear congruential pseudorandom number generators.

1 Introduction

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 $\{0, 1, \ldots, t-1\}$. As usual, we denote by $\mathcal{U}_t$ the set of invertible elements of $\mathbb{Z}_t$.

Accordingly, for a power of a prime number $q = p^r$ with $r \geq 1$, we denote by $\mathbb{F}_q$ the field of p^r elements. For $r = 1$, we have $\mathbb{F}_p \cong \mathbb{Z}_p$. In this particular case, we assume that it is represented by the set $\{0, 1, \ldots, p-1\}$. Through this article, we treat elements of $\mathbb{Z}_t$ and $\mathbb{F}_p$ as integer numbers in the above range when the meaning is clear from the context.

Given a polynomial $F(X) \in \mathbb{F}_q[X]$ of degree at least 2, we define the *Nonlinear congruential generator*, (u_n) of elements of $\mathbb{F}_q$ by the recurrence relation

$$u_{n+1} = F(u_n), \qquad n = 0, 1, \ldots,$$

where u_0 is the *Initial value*.

In [8], a new method was proposed to estimate exponential sums. The idea is applicable to character sums (see [11]) and exponential sums with such sequences for arbitrary polynomials $F(X)$, see also these surveys surveys [7, 9, 10, 12].

Unfortunately, for general polynomials, this method leads to rather weak bounds for character sums (see [11]). Here we show that this method also works for an important class of polynomials, namely for certain *Dickson polynomials*.

We recall that the family of Dickson polynomials $D_e(X, \alpha) \in \mathbb{F}_q[X]$ is defined by the following recurrence relation

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

with initial values

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

where $\alpha \in \mathbb{F}_q$ is a parameter, see [5] for many useful properties and applications of Dickson polynomials. In particular, $\deg D_e(X, \alpha) = e$.

Here we concentrate only on the cases $\alpha = 1$ and $\alpha = -1$. From now and on, we denote $D_e(X)$ either $D_e(X, 1)$ or $D_e(X, -1)$, and consider the sequence

$$u_{n+1} = D_e(u_n), \qquad n = 0, 1, \ldots, \tag{2}$$

where u_0 is the *Initial value*.

It is clear that the sequence $u_0, u_1, \ldots$ is periodic of period $T \le q$. In fact, we always assume that it is purely periodic (which can be achieved by a shift of the sequence and discarding several initial values).

We define the character sum

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

where χ is a nontrivial multiplicative character of the field $\mathbb{F}_q$.

2 Preliminaries

We recall Lemma 2 from [2].

Lemma 1. *Then for any set $\mathcal{K} \subseteq \mathcal{U}_t$ of cardinality $\#\mathcal{K} = K$, any fixed $\delta > 0$ 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.

We also need the *Weil bound* for character sums which we present in the following form (see Chapter 5 of [6]).

Lemma 2. *Let χ be a multiplicative 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 the number of distinct in its splitting field over $\mathbb{F}_q$. Under these conditions, the following inequality*

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

holds.

Finally, we need the following result on Dickson polynomials. This is a generalization of a similar Lemma in [4].

Lemma 3. *For $u \in \mathbb{F}_q$ we define the polynomial*
$F_u(X) = X^2 - uX + \beta$, $\beta = -1, 1$. Assume that either $F_u(X)$ is irreducible over $\mathbb{F}_q$ and $e \equiv f \pmod{2q+2}$ or $F_u(X)$ has two simple roots in $\mathbb{F}_q$ and $e \equiv f \pmod{q-1}$. Then

$$D_e(u) \equiv D_f(u),\ \forall u \in \mathbb{F}_q.$$

Proof. Let $F_u(X)$ be irreducible over $\mathbb{F}_q$ and let μ_1 and $\mu_2 = \mu_1^q$ be its roots in F_{q^2}. Because $\mu_1^{q+1} = \mu_1\mu_2 = 1$ or $\mu_1^{q+1} = \mu_1\mu_2 = -1$ we derive that $F_u(X) | X^{2q+2} - 1$ in this case.

It is also easy to see that if $F_u(X)$ has to simple roots in $\mathbb{F}_q$ then $F_u(X)|X^{q-1}-1$, because the order of any of the two roots divides the order of $\mathbb{F}_q^*$ as a multiplicative group, which is $q-1$.

Recalling that the sequence $D_e(u), e=0,\ldots,$ satisfies a linear recurrent relation (1) with the characteristic polynomial F_u, we obtain the desired result. □

It is well known that Dickson polynomial commute with respect the composition, see for instance [5].

Lemma 4. *For any positive integers e and f, we have*

$$D_e(D_f(X)) = D_{ef}(X) = D_f(D_e(X)).$$

The factorization of Dickson polynomials is also well known. Here, we give a reduced version of Corollary 3.13 of [5].

Lemma 5. *Let n be an odd positive integers and assume that $\mathbb{F}_{p^r}$ contains a primitive $n-$th root of unity. Then*

$$D_n(X,\alpha) = X \prod_{k=1}^{(n-1)/2} (X^2 + \alpha\beta_k^2)$$

where $\beta_k = \rho^k - \rho^{-k}$.

Using the last Lemma we can proof this global result:

Lemma 6. *Let $D_{re_i^k}(X), k_i \in \mathcal{L}$ a family of Dickson polynomials where r and e are odd integers. Then, if $d_i \not\equiv 0 \pmod{s}, \forall i$ where*

$$\prod_{i=1}^{\nu} D_{re^{k_i}}(X,\alpha)^{d_i} \tag{3}$$

then the polynomial is not, up to a multiplicative constant, an $s-$th power.

Proof. Put $n = re^N = \max\{re^{k_i} | k_i \in \mathcal{L}\}$ and take $\mathbb{K}$ the splitting field of $D_n(X,\alpha)$.

Let $\rho \in \mathbb{K}$ be a primitive $n-$th root of the unity. Conditions in Lemma 5 are satisfied.

By this Lemma, we have:

$$D_{re^N}(X,\alpha) = X \prod_{k=1}^{(re^N-1)/2} (X^2 + \alpha\beta_k^2).$$

With the same notation we have:

$$D_{re^{N-1}}(X,\alpha) = X \prod_{k=1}^{(re^{N-1}-1)/2} (X^2 + \alpha\beta_{ek}^2),$$

which directly implies that $D_{re^{N-1}}(X,\alpha)|D_{re^N}(X,\alpha)$. Using this argument, we get that $D_{re^{k_i}}(X,\alpha)|D_{re^{N-1}}(X,\alpha),\ k_i \neq n$.

By Corollary 3.14 of [5], all the roots of $D_n(X,\alpha)$ are simple. Taking one root of $D_{re^N}(X,\alpha)$ which is not a root of $D_{re^{N-1}}(X,\alpha)$ we have finished. □

3 Main result

Now we have enough tools to get a general estimate for the sums S_χ with a purely periodic sequence u_n, $n = 0, 1, \ldots$, satisfying (2).

We remark that if $u_0 \neq 2$, then $F_{u_0}(X) = X^2 - u_0X + \beta,\ \beta = -1, 1$ has not multiple roots and thus Lemma 3 applies. Let us denote by t the smallest positive integer for which $D_e(u_0) \equiv D_f(u_0)$ whenever $e \equiv f \pmod t$. By Lemma 3 we have either $t|2q+2$ or $t|q-1$.

We also remark that if $u_0 \equiv 2 \pmod q$ then $u_n \equiv 2 \pmod q$ for every $n = 1, 2, \ldots$. Thus we can take $t = 1$ in this case.

It is easy to see that T is the multiplicative order of e modulo t.

Theorem 7. *For every fixed integer $\nu \geq 1$,*

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

where the implied constant depends on ν.

Proof. We put

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

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

It is easy to see that T is the multiplicative order of e modulo t. Because the sequence u_n, $n = 0, 1, \ldots$, is purely periodic, for any $k \in \mathbb{Z}_t$, we have:

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

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

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

Applying the Hölder inequality, we derive

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

Let r', $1 \le r' \le t-1$, be defined by the congruence $rr' \equiv 1 \pmod{t}$. By Lemma 4 we obtain

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

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 $D_{r'e^n}(u_0)$ are pairwise distinct modulo q. Therefore, from (5) we derive

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

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

$$\begin{aligned} L^{2\nu}|S_\chi|^{2\nu} &\le T^{2\nu-1} \sum_{u \in \mathbb{F}_q} \left| \sum_{f \in \mathcal{F}} \chi\left(D_f(u)\right) \right|^{2\nu} \\ &\le T^{2\nu-1} \sum_{f_1, \ldots, f_{2\nu} \in \mathcal{F}} \sum_{u \in \mathbb{F}_q} \chi\left(\prod_{j=1}^{\nu} D_{f_j}(u) (D_{f_{\nu+j}}(u))^{q-2} \right). \end{aligned}$$

For the case that no $f_{i_k} \in \{f_1, \ldots, f_{\nu+1}, \ldots, f_{2\nu}\}$ appears only once then there are at most μ differents values in $\{f_1, \ldots, f_{\nu+1}, \ldots, f_{2\nu}\}$. Hence, there are at most L^μ possible cases. For those selections, we shall use the trivial bound, which gives the total contribution $O(L^\nu q)$.

Otherwise, taking into account that $\deg D_f = f$ and eliminating all the $s-$th powers, we conclude that the polynomial

$$\Psi_{f_1,\ldots,f_{2\nu}}(X) = \prod_{j=1}^{\nu} \left(D_{f_j}(X)(D_{f_{\nu+j}}(X))^{q-2}\right)$$

is, up to a multiplicative constant, not an s-th power by Lemma 6. Now, we calculate a bound on the number of possible distinct roots of the polynomial:

$$\deg \Psi_{f_1,\ldots,f_{2\nu}} \le \max_{j=1,\ldots,2\nu} f_j \le \max_{f\in\mathcal{F}} f \le h.$$

Using Lemma 2, we obtain that the total contribution from such terms is $O(L^{2\nu}hq^{1/2})$. Hence

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

So this leads us to the bound

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

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

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

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

4 Remarks

Assuming that $T = t^{1+o(1)}$, the bound of Theorem 7 takes the form

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

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

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

$$|S_\chi| = O\left(q^{7/8+o(1)}\right). \tag{6}$$

We want also to remark that, the case when e is even, the polynomial $D_e(X)$ is not divisible by X. So, this case is covered by the results of [1].

References

[1] S. Cohen, M. Dewar, J. B. Friedlander, D. Panario and I. E. Shparlinski, 'Polynomial Gauss sums', *Proc. Amer. Math. Soc.*, **133** (2005), 2225–2231.

[2] J. B. Friedlander, J. Hansen and I. E. Shparlinski, 'On character sums with exponential functions', *Mathematika*, **47** (2000), 75–85.

[3] J. B. Friedlander and I. E. Shparlinski, 'On the distribution of the power generator', *Math. Comp.*, **70** (2001), 1575–1589.

[4] D. Gomez, J. Gutierrez and I. Shparlinski, 'Exponential sums with Dickson polynomials', *Finite Fields and Their Applications,* **12** (2006), 16–25.

[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, 'Design and analysis of nonlinear pseudorandom number generators', *Monte Carlo Simulation*, A.A. Balkema Publishers, Rotterdam, (2001), 3–9.

[8] H. Niederreiter and I. E. Shparlinski, 'On the distribution and lattice structure of nonlinear congruential pseudorandom numbers', *Finite Fields and Their Applications*, **5** (1999), 246–253.

[9] H. Niederreiter and I. E. Shparlinski, 'Recent advances in the theory of nonlinear pseudorandom number generators', *Proc. Conf. on Monte Carlo and Quasi-Monte Carlo Methods, 2000*, (2002), 86–102.

[10] H. Niederreiter and I. E. Shparlinski, 'Dynamical systems generated by rational functions', *Lect. Notes in Comp. Sci.*,**2643** (2003), 6–17.

[11] H. Niederreiter and A. Winterhof, 'Multiplicative character sums for nonlinear recurring sequences', *Acta Arith.*, **111** (2004), 299-305 .

[12] A. Topuzoğlu and A. Winterhof 'On the linear complexity profile of nonlinear congruential pseudorandom number generators of higher orders' *Appl. Algebra Engrg. Comm. Comput.* **16** (2005), 219–228.