Available online at www.sciencedirect.com
SCIENCE DIRECT®
Finite Fields and Their Applications 12 (2006) 16–25
FINITE FIELDS AND THEIR APPLICATIONS
http://www.elsevier.com/locate/ffa

Exponential sums with Dickson polynomials

Domingo Gomez-Perez[a], Jaime Gutierrez[a], Igor E. Shparlinski[b,*]

[a] *Faculty of Science, University of Cantabria, E-39071 Santander, Spain*
[b] *Department of Computing, Macquarie University Sydney, NSW 2109, Australia*

Received 24 January 2004

Abstract

We give new bounds of exponential sums with sequences of iterations of Dickson polynomials over prime finite fields. This result is motivated by possible applications to polynomial generators of pseudorandom numbers.

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 integer numbers in the above range.

Given a polynomial $F(X) \in \mathbb{F}_p[X]$, we define the *polynomial congruential generator*, (v_n) of elements of $\mathbb{F}_p$ by the recurrence relation

$$x_{n+1} \equiv F(x_n) \pmod{p}, \qquad n = 0, 1, \ldots,$$

where x_0 is the *initial value*.

* Corresponding author. Fax: +61-0-9850-9551.
E-mail addresses: gomezd@unican.es (D. Gomez-Perez), jaime.gutierrez@unican.es (J. Gutierrez), igor@ics.mq.edu.au (I.E. Shparlinski).

1071-5797/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2004.08.001

Recently [9], a new method has been invented to estimate exponential sums with such sequences for arbitrary polynomials F and thus study their distribution, see also recent surveys [8,10,11]. Unfortunately, for general polynomials, this method leads to rather weak bounds. For a special class of polynomials, namely for monomials $F(X) = X^e$ an alternative approach, producing much stronger bounds have been proposed in [2,3]. In [1] this approach has been used to obtain bounds of multiplicative character sums with iterations of the polynomial $F(X) = X^e$. In [4] it has been applied to derive bounds of additive character sums over trajectories of repeated scalar multiplication of a point on an elliptic curve over a finite fields. Here we show that this method also works for another, yet related, special class of polynomials, namely for certain *Dickson polynomials*.

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

It is easy to check that $D_e(X, 0) = X^e$, which corresponds to the case investigated in [2,3]. Here, we concentrate on another special case $\alpha = 1$. We denote for brevity $D_e(X) = D_e(X, 1)$, and consider the sequence

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

where u_0 is the *initial value*.

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

For $a \in \mathbb{F}_p$ we define the exponential sum

$$S_e(a) = \sum_{n=0}^{T-1} \mathbf{e}_p(au_n),$$

where $\mathbf{e}_p(z) = \exp(2\pi z/p)$ for $z \in \mathbb{F}_p$.

We apply the method of [2] to obtain an upper bound on sums $|S_e(a)|$. We remark, however, that several specific properties of X^e do not hold for $D_e(X)$ thus our general result is slightly weaker than that of [2]. However, in an important special case, using a new bound of exponential sums from [6], we obtain a result of the same strength as in [2].

2. Preliminaries

As usual we denote by $\varphi(q)$ the *Euler function*.
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 $h \geqslant t^{\delta}$ there exists an integer $r \in \mathcal{U}_t$ such that the congruence*

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

has

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

solutions.

We also need the bounds of some character sums. First of all we present the *Weil bound* in the following form (see [7, Chapter 5]).

Lemma 2. *For any prime p and any polynomial $f(X) \in Z[X]$ of degree $d \geqslant 1$ the bound*

$$\left| \sum_{z \in \mathbb{F}_p} \mathbf{e}_p(f(z)) \right| \leqslant dp^{1/2}$$

holds.

For a quadratic extension $\mathbb{F}_{p^2}$ of $\mathbb{F}_p$, we denote by $\mathrm{Nm}(z)$ and $\mathrm{Tr}(z)$ the *norm* and *trace* of $z \in \mathbb{F}_{p^2}$, that is,

$$\mathrm{Nm}(z) = z^{p+1} \qquad \text{and} \qquad \mathrm{Tr}(z) = z + z^p.$$

The following bound is a very special partial case of the results of [6].

Lemma 3. *For any prime p, any multiplicative character χ of $\mathbb{F}_{p^2}$ and any polynomial $f(X) \in Z[X]$ of degree $d \geqslant 1$ the bound*

$$\left| \sum_{\substack{z \in \mathbb{F}_{p^2} \\ \mathrm{Nm}(z)=1}} \chi(z) \mathbf{e}_p\left(f\left(\mathrm{Tr}(z)\right)\right) \right| \leqslant 2dp^{1/2}$$

holds.

We now recall the following property of the group of characters of an abelian group.

Lemma 4. *Let $\mathcal{H}$ be an abelian group and let $\widehat{\mathcal{H}} = \mathrm{Hom}(\mathcal{H}, \mathbb{C}^*)$ be its dual group. Then for any character χ of $\mathcal{H}$,*

$$\frac{1}{|\mathcal{H}|} \sum_{h \in \mathcal{H}} \chi(h) = \begin{cases} 1 \ \text{if} \ \chi = \chi_0, \\ 0 \ \text{if} \ \chi \neq \chi_0, \end{cases}$$

where $\chi_0 \in \widehat{\mathcal{H}}$ is the trivial character.

Lemma 5. *For any prime p, any element $\gamma \in \mathbb{F}_{p^2}$ of multiplicative order t and with $\mathrm{Nm}(\gamma) = 1$, and any polynomial $f(X) \in Z[X]$ of degree $d \geqslant 1$ the bound*

$$\left| \sum_{m=1}^{t} \mathbf{e}_p \left(f \left(\mathrm{Tr}(\gamma^m) \right) \right) \right| \leqslant 2 d p^{1/2}$$

holds.

Proof. Let $\mathcal{G} \subset \mathbb{F}_{p^2}^*$ be the group of elements $z \in \mathbb{F}_{p^2}$ with $\mathrm{Nm}(z) = 1$ and let $\mathcal{H}$ be a subgroup of $\mathcal{G}$ generated by γ. We denote by $\mathcal{X}$ be the set of all multiplicative characters of $\mathcal{G}$, trivial on $\mathcal{H}$. Using Lemma 4, we write

$$\begin{aligned} \sum_{m=1}^{t} \mathbf{e}_p \left(f \left(\mathrm{Tr}(\gamma^m) \right) \right) &= \frac{1}{\#\mathcal{X}} \sum_{z \in \mathcal{G}} \mathbf{e}_p \left(f \left(\mathrm{Tr}(z) \right) \right) \sum_{\chi \in \mathcal{X}} \chi(z) \\ &= \frac{1}{\#\mathcal{X}} \sum_{\chi \in \mathcal{X}} \sum_{z \in \mathcal{G}} \chi(z) \mathbf{e}_p \left(f \left(\mathrm{Tr}(z) \right) \right). \end{aligned}$$

Applying the inequality of Lemma 3, we obtain the desired estimate. □

Finally, we need the several results on Dickson polynomials.

For $u \in \mathbb{F}_p$ we define the polynomial

$$F_u(X) = X^2 - uX + 1. \tag{3}$$

Lemma 6. *Assume that either $F_u(X)$ is irreducible over $\mathbb{F}_p$ and $e \equiv f \pmod{p+1}$ or $F_u(X)$ has two simple roots in $\mathbb{F}_p$ and $e \equiv f \pmod{p-1}$. Then*

$$D_e(u) \equiv D_f(u) \pmod{p}.$$

Proof. Let $F_u(X)$ be irreducible over $\mathbb{F}_p$ and let γ_1 and $\gamma_2 = \gamma_1^p$ be its roots in $\mathbb{F}_{p^2}$. Because $\gamma_1^{p+1} = \gamma_1\gamma_2 = F(0) = 1$ and $\gamma_2^{p+1} = \gamma_1^{(p+1)p} = 1$ we derive that $F_u(X) \mid X^{p+1} - 1$ in this case.

It is also easy to see that if $F_u(X)$ has two simple roots in $\mathbb{F}_p$ then $F_u(X) \mid X^{p-1} - 1$, see for instance [7].

Recalling that the sequence $D_e(u)$, $e = 0, 1 \ldots$, satisfies a linear recurrent relation (1) with the characteristic polynomial F_u, we obtain the desired result, see [7]. □

Lemma 7. *Assume that either $F_u(X)$ is irreducible over $\mathbb{F}_p$ and let $\gamma \in \mathbb{F}_{p^2}$ be one of the roots of $F_u(X)$. Then*

$$D_e(u) \equiv \mathrm{Tr}(\gamma^e) \pmod{p}.$$

Proof. As in the proof of Lemma 6 we note that the sequence $D_e(u)$, $e = 0, 1 \ldots$, satisfies a linear recurrent relation (1) with the characteristic polynomial F_u, which immediately implies that $D_e(u) \equiv \mathrm{Tr}(\lambda\gamma^e) \pmod{p}$ for some uniquely defined $\lambda \in \mathbb{F}_{p^2}$, see [7]. Remarking that $\mathrm{Tr}(1) = 2 = D_0(u)$ and $\mathrm{Tr}(\gamma) = u = D_1(u)$ we conclude that $\lambda = 1$. □

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

Lemma 8. *For any positive integers e and f, we have*

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

3. Main results

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

We remark that if $u_0 \neq 2$, then $F_{u_0}(X) = X^2 - u_0X + 1$ does not have multiple roots and thus Lemma 6 applies. Let us denote by t the smallest positive integer for which $D_e(u_0) \equiv D_f(u_0) \pmod{p}$ whenever $e \equiv f \pmod{t}$. By Lemma 6 we have either $t \mid p - 1$ or $t \mid p + 1$.

We also remark that is $u_0 \equiv 2 \pmod{p}$ then $u_n \equiv 2 \pmod{p}$ 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 9. *For every fixed integer $v \geqslant 1$,*

$$\max_{(a,p)=1} |S_e(a)| = O\left(T^{1-(2v+1)/2v(v+1)} t^{1/2(v+1)} p^{(v+2)/4v(v+1)}\right).$$

Proof. We put

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

Because $t \geqslant T$, for this choice of h we obtain $h \geqslant p^{1/2(v+1)}$, 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:

$$S_e(a) = \sum_{n=1}^{T} \mathbf{e}_p(aD_{e^{n+k}}(u_0)). \tag{4}$$

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

$$LS_e(a) = \sum_{n=1}^{T} \sum_{k \in \mathcal{L}} \mathbf{e}_p\left(aD_{e^{n+k}}(u_0)\right).$$

Applying the Hölder inequality, we derive

$$L^{2v}|S_e(a)|^{2v} \leqslant T^{2v-1} \sum_{n=1}^{T} \left| \sum_{k \in \mathcal{L}} \mathbf{e}_p\left(aD_{e^{n+k}}(u_0)\right) \right|^{2v}. \tag{5}$$

Let s, $1 \leqslant s \leqslant t-1$, be defined by the congruence $rs \equiv 1 \pmod{t}$. By Lemma 8 we obtain

$$D_{e^{n+k}}(u_0) \equiv D_{e^{n+k}rs}(u_0) \equiv D_{re^k}\left(D_{se^n}(u_0)\right) \pmod{p}. \tag{6}$$

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 $D_{se^n}(u_0)$ are pairwise distinct modulo p. Therefore, from (5) we derive

$$L^{2v}|S_e(a)|^{2v} \leqslant T^{2v-1} \sum_{u \in \mathbb{F}_p} \left| \sum_{k \in \mathcal{L}} \mathbf{e}_p\left(aD_{re^k}(u)\right) \right|^{2v}.$$

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

$$L^{2v}|S_e(a)|^{2v} \leqslant T^{2v-1} \sum_{u\in\mathbb{F}_p} \left| \sum_{f\in\mathcal{F}} \mathbf{e}_p\left(aD_f(u)\right)\right|^{2v}$$

$$\leqslant T^{2v-1} \sum_{f_1,\dots,f_{2v}\in\mathcal{F}} \sum_{u\in\mathbb{F}_p} \mathbf{e}_p\left(a\sum_{j=1}^{v}\left(D_{f_j}(u) - D_{f_{v+j}}(u)\right)\right).$$

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

Otherwise, taking into account that $\deg D_f = f$, we conclude that the polynomial

$$\Psi_{f_1,\dots,f_{2v}}(X) = \sum_{j=1}^{v}\left(D_{f_j}(X) - D_{f_{v+j}}(X)\right)$$

is a nonconstant polynomial of degree

$$\deg \Psi_{f_1,\dots,f_{2v}} \leqslant \max_{j=1,\dots,2v} f_j \leqslant \max_{f\in\mathcal{F}} f \leqslant h.$$

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

$$L^{2v}|S_e(a)|^{2v} = O\left(T^{2v-1}\left(L^v p + L^{2v}hp^{1/2}\right)\right).$$

So this leads us to the bound

$$|S_e(a)|^{2v} = O\left(T^{2v-1}\left(L^{-v}p + hp^{1/2}\right)\right).$$

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

$$|S_e(a)|^{2v} = O\left(T^{2v-1}\left(t^v T^{-v}h^{-v}p + hp^{1/2}\right)\right).$$

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

We now show that if $t \mid p+1$, that is, if the polynomial $F_u(X)$, given by (3), is irreducible then Theorem 9 can be improved up to the level of the results of [2].

Theorem 10. *If $t \mid p+1$ and $t \geqslant p^{1/2+\varepsilon}$ then for every fixed integer $v \geqslant 1$,*

$$\max_{(a,p)=1} |S_e(a)| = O\left(T^{1-(2v+1)/2v(v+1)} t^{1/2v} p^{1/4(v+1)}\right).$$

Proof. We use the notation and proceed as in the proof of Theorem 9 but put

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

Because $t \geqslant T$, for this choice of h we obtain $h \geqslant t^{1/(v+1)} p^{-1/2(v+1)} \geqslant p^{\varepsilon/(v+1)}$ thus again Lemma 1 applies.

Also, as in the proof of Theorem 9, we note that the values of se^n, $n = 1, \ldots, T$ in (6) are pairwise distinct modulo t. Thus from (5) we derive

$$\begin{aligned} L^{2v}|S_e(a)|^{2v} &\leqslant T^{2v-1} \sum_{m=1}^{t} \left| \sum_{k \in \mathcal{L}} \mathbf{e}_p\left(a D_{re^k}(D_m(u_0))\right) \right|^{2v} \\ &\leqslant T^{2v-1} \sum_{f_1,\ldots,f_{2v} \in \mathcal{F}} \sum_{m=1}^{t} \mathbf{e}_p\left(a \Psi_{f_1,\ldots,f_{2v}}((D_m(u_0)))\right). \end{aligned}$$

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 m, which gives the total contribution $O(L^v t)$ (instead of $O(L^v p)$ used in Theorem 9).

Otherwise, using Lemma 3 in a combination with Lemma 7, we obtain that the total contribution from such terms is $O(L^{2v} h p^{1/2})$. Hence

$$L^{2v}|S_e(a)|^{2v} = O\left(T^{2v-1}\left(L^v t + L^{2v} h p^{1/2}\right)\right).$$

So this leads us to the bound

$$|S_e(a)|^{2v} = O\left(T^{2v-1}\left(L^{-v} t + h p^{1/2}\right)\right).$$

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

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

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 9 takes form

$$\max_{(a,p)=1} |S_e(a)| = O\left(T^{1-1/2v+o(1)} p^{(v+2)/4v(v+1)}\right).$$

Accordingly under the same condition, the bound of Theorem 10 takes form

$$\max_{(a,p)=1} |S_e(a)| = O\left(T^{1-1/2(v+1)+o(1)} p^{1/4(v+1)}\right).$$

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

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

$$\max_{(a,p)=1} |S_e(a)| = O\left(p^{7/8+o(1)}\right). \tag{7}$$

As we have remarked, the bound of Theorem 9 is slightly weaker than the corresponding result of [2] (which is of the same form as Theorem 10). However, in many interesting cases they are of about the same strength. For example, the above nontriviality range in the case $T = t^{1+o(1)}$ and bound (7) are exactly the same as the corresponding statements from [2].

Finally, we remark that it would be interesting to extend this result to other classes of polynomials, for example, to arbitrary Dickson polynomials.

Acknowledgments

The authors wish to thank Winnie Li for many useful conversations and also informing us about her recent results [6] which have allowed us to improve our original results.

References

[1] S. Cohen, M. Dewar, J.B. Friedlander, D. Panario, I.E. Shparlinski, Polynomial Gauss sums, Proc. Amer. Math. Soc., to appear.
[2] J.B. Friedlander, J. Hansen, I.E. Shparlinski, On character sums with exponential functions, Mathematika 47 (2000) 75–85.
[3] J.B. Friedlander, I.E. Shparlinski, On the distribution of the power generator, Math. Comp. 70 (2001) 1575–1589.
[4] T. Lange, I.E. Shparlinski, Certain exponential sums and random walks on elliptic curves, Preprint, 2003, pp. 1–17.
[5] R. Lidl, G.L. Mullen, G. Turnwald, Dickson polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics, Longman, London-Harlow-Essex, 1993.

[6] W.-C.W. Li, Character sum estimates over norm groups, Finite Fields Appl., to appear.
[7] R. Lidl, H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.
[8] H. Niederreiter, Design and analysis of nonlinear pseudorandom number generators, in: Monte Carlo Simulation, A.A. Balkema Publishers, Rotterdam, 2001, pp. 3–9.
[9] H. Niederreiter, I.E. Shparlinski, On the distribution and lattice structure of nonlinear congruential pseudorandom numbers, Finite Fields Appl. 5 (1999) 246–253.
[10] H. Niederreiter, I.E. Shparlinski, Recent advances in the theory of nonlinear pseudorandom number generators, in: Proceedings of the Conference on Monte Carlo and Quasi-Monte Carlo Methods, 2000, Springer, Berlin, 2002, pp. 86–102.
[11] H. Niederreiter, I.E. Shparlinski, Dynamical systems generated by rational functions, Lecture Notes in Computer Science, vol. 2643, Springer, Berlin, 2003, pp. 6–17.