Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Finite monodromy of some families of exponential sums ☆

Antonio Rojas-León

Dpto. de Álgebra, Fac. de Matemáticas, Universidad de Sevilla, c/Tarfia, s/n, 41012 Sevilla, Spain

ARTICLE INFO

Article history:
Received 12 March 2018
Received in revised form 11 June 2018
Accepted 14 June 2018
Available online xxxx
Communicated by A. Pal

MSC:
11L05
11T23

Keywords:
Exponential sums
Monodromy
ℓ-Adic cohomology
Almost perfect nonlinear functions

ABSTRACT

Given a prime p and an integer $d > 1$, we give a numerical criterion to decide whether the ℓ-adic sheaf associated to the one-parameter exponential sums $t \mapsto \sum_x \psi(x^d + tx)$ over $\mathbb{F}_p$ has finite monodromy or not, and work out some explicit cases where this is computable.

1. Introduction

Consider the affine line $\mathbb{A}^1_k$ over a finite field k of characteristic $p > 0$. Let $\ell \neq p$ be a prime, and $\mathcal{F}$ an ℓ-adic sheaf on $\mathbb{A}^1_k$ of rank n, which can be regarded as a continuous representation

☆ Partially supported by MTM2016-75027-P (Ministerio de Economía y Competitividad) and FEDER.
E-mail address: arojas@us.es.

https://doi.org/10.1016/j.jnt.2018.06.012
0022-314X/

$$\rho : \pi_1(\mathbb{A}^1_k, \bar{\eta}) \to \mathrm{GL}(n, \bar{\mathbb{Q}}_\ell)$$

where $\bar{\eta}$ is a geometric generic point of $\mathbb{A}^1_k$. The arithmetic and geometric monodromy groups G^{arith} and G^{geom} of $\mathcal{F}$ are defined to be the Zariski closures of the images of ρ (resp. of its subgroup $\pi_1(\mathbb{A}^1_k, \bar{\eta})$). According to [Del80] (see [Kat88, Chapter 3] for a more explicit statement), under certain conditions (which are usually fulfilled after taking a Tate twist of $\mathcal{F}$), these groups govern the distribution of the Frobenius traces of the sheaf $\mathcal{F}$: more precisely, if $G^{geom} = G^{arith}$, the Frobenius traces are equidistributed as the traces of random elements of a maximal compact subgroup of G^{geom} as $\#k$ grows.

These groups also determine the asymptotic values of the higher moments associated to the trace function of $\mathcal{F}$, which are related to the dimension of the invariant subspaces of certain tensor powers of the given representation of G^{geom} via ρ. See [Kat05] for a detailed exposition of the topic.

In this article we will be concerned with a special class of sheaves, which are a subset of the class of so-called Airy sheaves, lisse sheaves on $\mathbb{A}^1_k$ of rank n with a single slope $\frac{n+1}{n}$ at infinity, which can also be characterized as the Fourier transform of lisse sheaves of rank 1 with slope > 1 at infinity. The monodromy of these sheaves was extensively studied by O. Šuch in [Šuc00], who gave a full classification of their possible non-finite monodromy groups [Šuc00, Propositions 11.6, 11.7].

Let $d \geq 2$ be a prime to p integer. Let $k = \mathbb{F}_p$ and let $\psi : k \to \mathbb{C}$ be the additive character given by $\psi(t) = \exp(2\pi it/p)$. Let $[d] : \mathbb{A}^1_k \to \mathbb{A}^1_k$ be the d-th power map, and $\mathcal{L}_{\psi(t^d)} = [d]^*\mathcal{L}_\psi$ the pull-back of the Artin–Schreier sheaf $\mathcal{L}_\psi$ on $\mathbb{A}^1_k$ associated to ψ. It is a lisse sheaf on $\mathbb{A}^1_k$ of rank 1, with slope d at infinity. Its Fourier transform $\mathcal{F}_d$ is then a lisse Airy sheaf on $\mathbb{A}^1_k$ of rank $d-1$ with a single slope $\frac{d}{d-1}$ at infinity [Kat90, Theorem 7.5.4]. The Frobenius trace of $\mathcal{F}_d$ at a point $t \in k$ is given (up to sign) by

$$\sum_{x \in k} \psi(x^d + tx).$$

The main goal of this article is giving a numerical criterion to determine whether the geometric monodromy (and therefore the arithmetic one after a suitable Tate twist) of $\mathcal{F}_d$ is finite. This is done in Proposition 1, and some specific cases are worked out explicitly in section 4. Moreover we show that, in the case where the monodromy is not finite, the given representation of the monodromy group is Lie irreducible, which allows to completely determine the arithmetic and geometric monodromy groups via the results in [Šuc00].

The most important case for applications is $p = 2$. In that case, we show that the monodromy of $\mathcal{F}_d$ is finite for d of the form $2^a + 1$ or $\frac{2^a+1}{2^b+1}$, and we conjecture that these are the only cases where the monodromy is finite. This case is important for its relation with *almost perfect nonlinear* and *exceptional* functions. A function $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if the equation $f(x+a) + f(x) = b$ has at most two solutions for every $a \neq 0, b \in \mathbb{F}_{2^n}$. These functions are quite useful in cryptography, see

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

e.g. [BLCCC06]. A function is *exceptional* if it is APN on $\mathbb{F}_{2^n}$ and also on infinitely many extensions of $\mathbb{F}_{2^n}$.

If the monodromy of $\mathcal{F}_d$ is not finite, then both G^{geom} and G^{arith} are the full symplectic group $\mathrm{Sp}(d-1,\mathbb{C})$. In particular, the (arithmetic) fourth moment of the trace function of $\mathcal{F}_d$ is 3. But this fourth moment can be computed explicitly, and it is equal to the number of (absolute) irreducible components of the polynomial $x^d+y^d+z^d+(x+y+z)^d \in k[x,y,z]$ minus one. So, if $\mathcal{F}_d$ does not have finite monodromy, the polynomial

$$\frac{x^d+y^d+z^d+(x+y+z)^d}{(x+y)(x+z)(y+z)}$$

is absolutely irreducible. By [AMR10] this implies that the function $f(x)=x^d$ is not almost perfect nonlinear on $\mathbb{F}_{2^n}$ for any sufficiently large n, and therefore is not exceptional. This gives a new algebro-geometric approach to the study of such problems.

The author would like to thank Daqing Wan for bringing this problem to his attention, and the anonymous referees for their useful comments and suggestions, particularly the simplified proofs of Lemma 2 and Proposition 4.

2. A numerical criterion for the finiteness of the monodromy of $\mathcal{F}_d$

Let $k=\mathbb{F}_p$ and $\mathcal{F}_d$ be as in the introduction, with $d\geq 3$ prime to p. We want to determine the values of (p,d) such that $\mathcal{F}_d$ has finite geometric monodromy.

Lemma 1. *The determinant of the Tate-twisted sheaf $\mathcal{F}_d(1/2)$ is geometrically trivial and arithmetically of finite order.*

Proof. The determinant $\det \mathcal{F}_d(1/2)$ is a lisse rank one sheaf on $\mathbb{A}^1_k$, which is geometrically trivial by [Kat87, Theorem 17]. So it is of the form α^{deg} for some ℓ-adic unit α. Then $\det \mathcal{F}_d(1/2)$ will be arithmetically of finite order over $\mathbb{A}^1_k$ if and only if α is a root of unity. In order to prove this, we will explicitly evaluate the action of Frobenius on $\det \mathcal{F}_d(1/2)$ at $t=0$, which is equal to α. By replacing k with a finite extension if necessary, we may assume that $d|q-1$, where $q=\#k$.

Let $r\geq 1$, and let k_r be the extension of k of degree r inside a fixed algebraic closure $\bar{k}$. The trace of the action of Frobenius on $\mathcal{F}_d(1/2)$ at $t=0\in k_r$ is given by

$$\frac{1}{q^{r/2}}\sum_{x\in k_r}\psi_r(x^d)$$

where $\psi_r(x)=\psi(\mathrm{Tr}_{k_r/\mathbb{F}_p}(x))$. Let $S_r:=\sum_{x\in k_r}\psi_r(x^d)$, then we have

$$S_r=\sum_{u\in k_r}\psi_r(u)\cdot\#\{x^d=u\}=\sum_{u\in k_r}\psi_r(u)\sum_{\chi^d=\mathbf{1}}\chi(u)$$

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

where the inner sum is taken over the set of multiplicative characters of k_r with trivial d-th power. Since $d|q-1$, every such character is obtained, by composition with the norm map, from one such multiplicative character of k. Then we have

$$\sum_{u\in k_r}\psi_r(u)\sum_{\chi^d=\mathbf{1}}\chi(u)=\sum_{\chi^d=\mathbf{1}}\sum_{u\in k_r}\psi_r(u)\chi(u)=-\sum_{\chi\neq\mathbf{1};\chi^d=\mathbf{1}}G(\psi_r,\chi)$$

where

$$G(\psi_r,\chi)=-\sum_{u\in k_r^\times}\psi_r(u)\chi(u)$$

is the Gauss sum associated to χ. Using the Hasse–Davenport relation $G(\psi_r,\chi)=G(\psi_1,\chi)^r$, we deduce

$$\exp\sum_{r\geq 1}S_r\frac{T^r}{r}=\exp\left(-\sum_{r\geq 1}\sum_{\chi\neq\mathbf{1};\chi^d=\mathbf{1}}\frac{(G(\psi_1,\chi)T)^r}{r}\right)=$$

$$=\prod_{\chi\neq\mathbf{1};\chi^d=\mathbf{1}}\exp\left(-\sum_{r\geq 1}\frac{(G(\psi_1,\chi)T)^r}{r}\right)=\prod_{\chi\neq\mathbf{1};\chi^d=\mathbf{1}}(1-G(\psi_1,\chi)T)$$

So the Frobenius eigenvalues at $t=0\in k$ are $G(\psi_1,\chi)$ for the $d-1$ non-trivial multiplicative characters χ of k such that $\chi^d=\mathbf{1}$. The determinant is then the product of these Gauss sums. Using the well-known relation $G(\psi_1,\chi)G(\psi_1,\chi^{-1})=\chi(-1)q$ we see that this product is $\pm q^{(d-1)/2}$ if d is odd, or $\pm q^{(d-2)/2}G(\psi_1,\rho)$ if d is even, where in the latter case ρ denotes the unique order 2 multiplicative character. Since $G(\psi_1,\rho)^2=G(\psi_1,\rho)G(\psi_1,\rho^{-1})=\rho(-1)q$, in both cases the product is $q^{(d-1)/2}$ times a root of unity. So Frobenius acts on $\det\mathcal{F}_d(1/2)=(\det\mathcal{F}_d)((d-1)/2)$ by multiplication by a root of unity. □

The following corollary is simply a restatement of [Kat90, Theorem 8.14.4]:

Corollary 1. *The sheaf $\mathcal{F}_d(1/2)$ has finite arithmetic monodromy if and only if it has finite geometric monodromy, if and only if for every finite extension k_r of k and every $t\in k_r$, the trace of the action of Frobenius on $\mathcal{F}_d(1/2)$ at t is an algebraic integer.*

The last condition is equivalent to the trace of the action of Frobenius on $\mathcal{F}_d$ being a multiple of $\sqrt{q}$ as an algebraic integer. Let us spell out what this means explicitly:

Corollary 2. *The sheaf $\mathcal{F}_d$ has finite geometric monodromy if and only if for every $r\geq 1$ and every $t\in k_r$, $\sum_{x\in k_r}\psi_r(x^d+tx)$ is divisible by $p^{r/2}$ as an algebraic integer.*

For our purposes we will need the following equivalent statement:

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

Proposition 1. *The sheaf $\mathcal{F}_d$ has finite geometric monodromy if and only if for every $r \geq 1$ the sum $\sum_{x \in k_r} \psi_r(x^d)$ is divisible by $p^{r/2}$ as an algebraic integer and, for every non-trivial multiplicative character $\chi : k_r^\times \to \mathbb{C}^\times$, $G_r(\chi) \cdot \sum_{x \in k_r^\times} \psi_r(x^d)\bar{\chi}(x)$ is divisible by $p^{r/2}$ as an algebraic integer. It is sufficient that the condition holds for every r which is a multiple of a certain $r_0 \geq 1$.*

Proof. This is an explicit version of [Kat90, Theorem 8.14.6]. Suppose that for every $r \geq 1$ and every $t \in k_r$, $\sum_{x \in k_r} \psi_r(x^d + tx)$ is divisible by $p^{r/2}$ as an algebraic integer. Then, in particular, $\sum_{x \in k_r} \psi_r(x^d)$ is divisible by $p^{r/2}$. Furthermore, for every non-trivial multiplicative character $\chi : k_r^\times \to \mathbb{C}^\times$, the sum

$$\sum_{t \in k_r^\times} \chi(t) \sum_{x \in k_r} \psi_r(x^d + tx) = \sum_{x \in k_r} \psi_r(x^d) \sum_{t \in k_r^\times} \chi(t)\psi_r(tx) = -G_r(\chi) \cdot \sum_{x \in k_r^\times} \psi_r(x^d)\bar{\chi}(x)$$

is also divisible by $p^{r/2}$.

Conversely, if $\sum_{x \in k_r^\times} \psi_r(x^d)$ is divisible by $p^{r/2}$, so is

$$\sum_{t \in k^\times} \sum_{x \in k_r^\times} \psi_r(x^d + tx) = \sum_{t \in k} \sum_{x \in k_r^\times} \psi_r(x^d + tx) - \sum_{x \in k_r^\times} \psi_r(x^d) = p^r - \sum_{x \in k_r^\times} \psi_r(x^d)$$

Since $\sum_{t \in k_r^\times} \chi(t) \sum_{x \in k_r} \psi_r(x^d + tx)$ is also divisible by $p^{r/2}$ for every non-trivial $\chi : k_r^\times \to \mathbb{C}^\times$, by Fourier inversion $\sum_{x \in k_r} \psi_r(x^d + tx)$ is divisible by $p^{r/2}$ for every $t \in k_r^\times$.

The last statement is a consequence of the fact that having finite geometric monodromy is invariant under extension of scalars to a finite extension of the base field. □

Lemma 2. *Let $z \in k_r^\times$ and $\chi : k_r^\times \to \mathbb{C}^\times$ be a multiplicative character. Then*

$$\sum_{x | x^d = z} \chi(x) = \sum_{\eta | \eta^d = \chi} \eta(z).$$

Proof. Let $\Phi, \Psi : k_r^\times \times \widehat{k_r^\times} \to \mathbb{C}^\times$ be the functions defined by

$$\Phi(z, \chi) = \sum_{x | x^d = z} \chi(x), \ \Psi(z, \chi) = \sum_{\eta | \eta^d = \chi} \eta(\zeta).$$

We will show that their Fourier transforms coincide as functions on $\widehat{k_r^\times} \times k_r^\times$, so $\Phi = \Psi$. The Fourier transform of Φ is given by

$$(\xi, y) \mapsto \sum_{z, \chi} \xi(z)\chi(y) \sum_{x^d = z} \chi(x) = \sum_{x, \chi} \xi(x^d)\chi(xy) = (p^r - 1)\xi(y^{-d})$$

and, similarly, the Fourier transform of Ψ is

$$(\xi, y) \mapsto \sum_{z,\chi} \xi(z)\chi(y) \sum_{\eta^d=\chi} \eta(z) = \sum_{z,\eta} \xi(z)\eta(y^d z) = (p^r - 1)\xi(y^{-d}). \quad \square$$

Using this lemma, we get

$$\sum_{x\in k_r^\times} \psi_r(x^d)\bar{\chi}(x) = \sum_{z\in k_r^\times} \psi_r(z) \sum_{x^d=z} \bar{\chi}(x) = \sum_{z\in k_r^\times} \psi_r(z) \sum_{\eta^d=\chi} \bar{\eta}(z) = -\sum_{\eta^d=\chi} G_r(\bar{\eta})$$

and

$$\sum_{x\in k_r} \psi_r(x^d) = 1 + \sum_{z\in k_r^\times} \psi_r(z)\#\{x|x^d = z\} = 1 + \sum_{z\in k_r^\times} \psi_r(z) \sum_{\eta^d=\mathbf{1}} \eta(z) =$$
$$= 1 + \sum_{\eta^d=\mathbf{1}} \sum_{z\in k_r^\times} \psi_r(z)\eta(z) = -\sum_{\eta\neq\mathbf{1},\eta^d=\mathbf{1}} G_r(\eta)$$

This allows us to give yet another criterion for finite monodromy:

Proposition 2. *The sheaf $\mathcal{F}_d$ has finite geometric monodromy if and only if for every $r \geq 1$ and every non-trivial multiplicative character $\eta : k_r^\times \to \mathbb{C}^\times$, the Gauss sum $G_r(\eta)$ is divisible by $p^{r/2}$ if η^d is trivial, and the product $G_r(\eta)G_r(\bar{\eta}^d)$ is divisible by $p^{r/2}$ if η^d is non-trivial. It is sufficient that the condition holds for every r which is a multiple of a certain $r_0 \geq 1$.*

Proof. By Proposition 1 and the previous remark, if these products of Gauss sums are divisible by $p^{r/2}$ then $\mathcal{F}_d$ has finite monodromy. Conversely, suppose that $\mathcal{F}_d$ has finite monodromy. Then for every $r \geq 1$ and every non-trivial $\chi : k_r^\times \to \mathbb{C}^\times$, the sums $A_r = \sum_{\eta\neq\mathbf{1},\eta^d=\mathbf{1}} G_r(\eta)$ and $B_r(\chi) = \sum_{\eta^d=\chi} G_r(\chi)G_r(\bar{\eta})$ are divisible by $p^{r/2}$ as algebraic integers. We need to show that the individual summands are also divisible by $p^{r/2}$. By the Hasse–Davenport relation, by passing to a finite extension of k_r we may assume that $d|p^r - 1$. Then for every $m \geq 1$ there are either 0 (in which case there is nothing to prove) or d characters η of $k_{rm}^\times$ such that $\eta^d = \chi$, which are obtained from those of $k_r^\times$ by composition with the norm map. By the Hasse–Davenport relation we have that $A_{rs} = \pm\sum_{\eta\neq\mathbf{1},\eta^d=\mathbf{1}} G_r(\eta)^s$ and $B_{rs}(\chi) = \sum_{\eta^d=\chi} G_r(\chi)^s G_r(\bar{\eta})^s$ are divisible by $p^{rs/2}$ as algebraic integers. The result is then a consequence of the following lemma. $\square$

Lemma 3. *Let $\alpha_1, \ldots, \alpha_d$ be algebraic integers such that $\alpha_1^s + \cdots + \alpha_d^s$ is divisible by $p^{s/2}$ for every $s \geq 1$. Then α_i is divisible by $p^{1/2}$ for every $i = 1, \ldots, d$.*

Proof. This is a well known result, see e.g. [Ax64]. Let K be the completion of $\mathbb{Q}(\alpha_1, \ldots, \alpha_d)$ at a prime over p. Since $\alpha_1^s + \cdots + \alpha_d^s$ is divisible by $p^{s/2}$, the power series

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

$$g(T) := \sum_{s=0}^{\infty} (\alpha_1^s + \cdots + \alpha_d^s) T^s$$

converges for $|T|_p < p^{1/2}$, so all the poles x must have $|x|_p \geq p^{1/2}$, that is, $(p^{1/2}x)^{-1}$ are p-adic integers. But the poles are $\alpha_1^{-1}, \ldots, \alpha_d^{-1}$, since

$$g(T) = \frac{1}{1-\alpha_1 T} + \cdots + \frac{1}{1-\alpha_d T}.$$

So $(p^{1/2}\alpha_i^{-1})^{-1} = p^{-1/2}\alpha_i$ is an algebraic integer for all $i = 1, \ldots, d$, that is, α_i is divisible by $p^{1/2}$. □

Finally we can make this more explicit thanks to Stickelberger's theorem. Fix $r \geq 1$. For every integer $1 \leq x \leq p^r - 1$ let $[x]_{p,r}$ be the sum of the p-adic digits of x. It is an integer between 1 and $r(p-1)$: for instance, $[1]_{p,r} = [p]_{p,r} = 1$, and $[p^r - 1]_{p,r} = r(p-1)$. If x is an arbitrary integer, we define $[x]_{p,r} := [y]_{p,r}$, where $1 \leq y \leq p^r - 1$ is the unique integer such that $x \equiv y \pmod{p^r - 1}$.

It is easy to see from this definition that $[px]_{p,r} = [x]_{p,r}$ and $[-x]_{p,r} = r(p-1) - [x]_{p,r}$ for every $x \in \mathbb{Z}$ which is not a multiple of $p^r - 1$. If x is not a multiple of $p^r - 1$ we have the following well-known explicit formula for $[x]_{p,r}$, where $\{x\}$ denotes the fractional part of a real number x:

$$[x]_{p,r} = (p-1) \sum_{i=0}^{r-1} \left\{ \frac{p^i x}{p^r - 1} \right\}.$$

Theorem 1. *The sheaf $\mathcal{F}_d$ has finite geometric monodromy if and only if for every $r \geq 1$ and every integer $1 \leq x \leq p^r - 2$, we have*

$$[dx]_{p,r} \leq [x]_{p,r} + \frac{r(p-1)}{2}.$$

It is sufficient that the condition holds for every r which is a multiple of a certain $r_0 \geq 1$.

Proof. Fix $r \geq 1$. The Gauss sums on $k_r^\times$ take values in the finite extension of $\mathbb{Q}$ generated by the $p(p^r-1)$-th roots of unity. By the Stickelberger theorem [BEW98, Theorem 11.2.1], if ω denotes the Teichmüller character of $k_r^\times$ (which generates the character group), the p-adic valuation of the Gauss sum associated to ω^j for $1 \leq j \leq p^r - 2$ is given by $\frac{1}{p-1}[j]_{p,r}$.

Applying this to the criterion of Proposition 2, we get that $\mathcal{F}_d$ has finite monodromy if and only if for every $1 \leq j \leq p^r - 2$ we have $[j]_{p,r} \geq \frac{r(p-1)}{2}$ if dj is divisible by $p^r - 1$, and $[j]_{p,r} + [-dj]_{p,r} \geq \frac{r(p-1)}{2}$ otherwise.

If dj is divisible by $p^r - 1$ this can be rewritten as

$$[dj]_{p,r} = r(p-1) \leq [j]_{p,r} + \frac{r(p-1)}{2}$$

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

and, if dj is not a multiple of $p-1$, it is equivalent to

$$[dj]_{p,r} = r(p-1) - [-dj]_{p,r} \leq r(p-1) + [j]_{p,r} - \frac{r(p-1)}{2} = [j]_{p,r} + \frac{r(p-1)}{2}. \quad \square$$

For computational purposes, it is convenient to have a sufficient condition for the monodromy of $\mathcal{F}_d$ to be finite. We have the following criterion, which is a generalization of [Kat07, Lemma 13.5].

Proposition 3. *For $r \geq 1$ an integer, let $f_r : [0,1] \to \mathbb{R}$ be the piecewise linear function defined by*

$$f_r(x) = \sum_{i=0}^{r-1} \{p^i x\} + \sum_{i=0}^{r-1} \{-dp^i x\}.$$

Suppose that for some integer $r_0 \geq 1$ we have

1. $f_{r_0}(\frac{a}{d}) \geq \frac{r_0}{2}$ *for* $a = 1, \ldots, d-1$
2. $\lim_{x \to \frac{a}{p^{r_0-1}d}^-} f_{r_0}(x) \geq \frac{r_0}{2}$ *for* $a = 1, \ldots, p^{r_0-1}d$

Then the monodromy of $\mathcal{F}_d$ is finite.

Proof. Since the function f_r is piecewise linear with constant negative slope and its points of discontinuity are $\frac{a}{p^{r-1}d}$ for $a = 1, \ldots, p^{r-1}d$, the two conditions imply that $f_{r_0}(x) \geq \frac{r_0}{2}$ for every $x \in \mathbb{Z}_{(p)} \cap (0,1)$.

Let r be a multiple of r_0, and $1 \leq x \leq p^r - 1$ an integer. Then

$$f_r\left(\frac{x}{p^r-1}\right) = f_{r_0}\left(\frac{x}{p^r-1}\right) + f_{r_0}\left(\frac{p^{r_0}x}{p^r-1}\right) + \cdots + f_{r_0}\left(\frac{p^{(r/r_0-1)r_0}x}{p^r-1}\right) \geq$$
$$\geq \frac{r}{r_0}\frac{r_0}{2} = \frac{r}{2}.$$

Then, if dx is a multiple of $p^r - 1$,

$$[x]_{p,r} = (p-1)\sum_{i=0}^{r-1}\left\{\frac{p^i x}{p^r-1}\right\} = (p-1)f_r\left(\frac{x}{p^r-1}\right) \geq (p-1)\frac{r}{2},$$

and otherwise,

$$[x]_{p,r} + [-dx]_{p,r} = (p-1)f_r\left(\frac{x}{p^r-1}\right) \geq (p-1)\frac{r}{2},$$

so $\mathcal{F}_d$ has finite monodromy by Theorem 1. $\square$

For instance, for $p = 2$, $d = 5$ satisfies the condition for $r = 4$, as one can easily check.

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

3. Explicit results

In this section we will use Theorem 1 to give some explicit results. First of all, we can recover the known fact [Kat87, Proposition 5] that, if $p > 2d-1 \geq 5$, then the monodromy is not finite.

Corollary 3. *Suppose that $p \geq 2d+1 \geq 7$. Then $\mathcal{F}_d$ does not have finite monodromy.*

Proof. Let $p = qd+r$ with $q \geq 2$ and $1 \leq r \leq d$. We claim that $[dq]_{p,1} > [q]_{p,1} + \frac{p-1}{2}$, so $\mathcal{F}_d$ can not have finite monodromy by Theorem 1.

Since $q < dq \leq p-1$, $[dq]_{p,1} = dq$ and $[q]_{p,1} = q$. So the inequality is equivalent to $2(d-1)q > p-1 = qd+r-1$ or, equivalently, $q(d-2) > r-1$. Now

$$q(d-2) \geq 2(d-2) = d+d-4 \geq d-1 \geq r-1$$

with equality if and only if $d = r = 3, q = 2$, in which case $p = 9$ is not prime. □

Lemma 4. *For every $r \geq 1$ and $x, y \in \mathbb{Z}$ we have $[x+y]_{p,r} \leq [x]_{p,r} + [y]_{p,r}$.*

Proof. It suffices to prove it for $1 \leq x, y \leq p^r - 1$. First of all, it is clear that, if an integer $z \geq 1$ can be written as a sum of m powers of p, then $[z]_{p,r} \leq m$ for every $r \geq 1$. Conversely, if $1 \leq z \leq p^r - 1$, then z can be written as a sum of $[z]_{p,r}$ powers of p.

So x (resp. y) can be written as a sum of $[x]_{p,r}$ (resp. $[y]_{p,r}$ powers of p), and therefore $x+y$ can be written as a sum of $[x]_{p,r} + [y]_{p,r}$ powers of p. We conclude that $[x+y]_{p,r} \leq [x]_{p,r} + [y]_{p,r}$. □

Corollary 4. *Let $d = p^a + 1$ for some integer $a \geq 1$. Then $\mathcal{F}_d$ has finite monodromy.*

Proof. We need to show that $[dx]_{p,r} \leq [x]_{p,r} + \frac{r(p-1)}{2}$ for every $r \geq 1$ and every $1 \leq x \leq p^r - 2$. If $[x]_{p,r} \geq \frac{r(p-1)}{2}$ this is obvious, since $[dx]_{p,r} \leq r(p-1)$. Suppose that $[x]_{p,r} \leq \frac{r(p-1)}{2}$. Then

$$[dx]_{p,r} = [(p^a+1)x]_{p,r} \leq [p^a x]_{p,r} + [x]_{p,r} = 2[x]_{p,r} \leq [x]_{p,r} + \frac{r(p-1)}{2}$$

for every $1 \leq x \leq p^r - 2$. □

Corollary 5. *Let $d = \frac{p^a+1}{p^b+1}$, with $a > b \geq 1$. Then $\mathcal{F}_d$ has finite monodromy.*

Proof. By Lemma 4, $[(p^b+1)z]_{p,r} \leq 2[z]_{p,r}$ for every $z \in \mathbb{Z}$. Taking $z = -dx$ and using that $[-x]_{p,r} = r(p-1) - [x]_{p,r}$, we get

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

$$r(p-1)-[(p^a+1)x]_{p,r}=r(p-1)-[(p^b+1)dx]_{p,r}=[-(p^b+1)dx]_{p,r}\leq$$
$$\leq 2[-dx]_{p,r}=2r(p-1)-2[dx]_{p,r}\Rightarrow$$
$$\Rightarrow [dx]_{p,r}\leq \frac{r(p-1)}{2}+\frac{1}{2}[(p^a+1)x]_{p,r}\leq [x]_{p,r}+\frac{r(p-1)}{2}. \quad \square$$

Remark 1. In the situation of the previous corollary, a must be of the form bc with c odd. Indeed, let $a=bc+r$ with $0\leq r<b$. Since p^a+1 is a multiple of p^b+1, we have

$$0\equiv p^a+1=p^{bc}p^r+1\equiv(-1)^c p^r+1(\text{mod } p^b+1).$$

Since $|(-1)^c p^r+1|<|p^b+1|$, we conclude that $(-1)^c p^r=-1$, that is, $r=0$ and c is odd.

In the case $p=2$ we conjecture that the only cases where the monodromy is finite are the ones covered in the previous corollaries. This has been checked to be true computationally for d up to 10000.

Conjecture 1. *Let $p=2$. Then $\mathcal{F}_d$ has finite monodromy if and only if d has the form 2^a+1 for some $a\geq 1$ or $\frac{2^a+1}{2^b+1}$ for some $b\geq 1$ and $a=bc$ with odd $c\geq 3$.*

4. The monodromy in the non-finite case

In this section we will completely determine the geometric monodromy group of $\mathcal{F}_d$ in the case where it is infinite. By [Šuc00, Proposition 11.1], if the monodromy is not finite, then $\mathcal{F}_d$ is either Lie-irreducible or Artin–Schreier induced. We will see that the latter case is not possible.

Proposition 4. *Suppose that the monodromy of $\mathcal{F}_d$ is not finite. Then $\mathcal{F}_d$ is Lie-irreducible.*

Proof. Suppose that $\mathcal{F}_d$ were Artin–Schreier induced. Then the proof of [Šuc00, Proposition 11.1] shows that $\mathcal{F}_d\otimes\widehat{\mathcal{F}}_d$ contains an Artin–Schreier subsheaf $\mathcal{L}_{\psi(at)}$ for some $a\in\bar{k}^*$. That is,

$$\text{Hom}(\mathcal{F}_d\otimes\widehat{\mathcal{F}}_d,\mathcal{L}_{\psi(at)})\neq 0$$

for some $a\in\bar{k}^*$ or, equivalently (since $\mathcal{F}_d$ is irreducible),

$$\mathcal{F}_d\cong\mathcal{F}_d\otimes\mathcal{L}_{\psi(at)}.$$

By taking Fourier transform this implies

$$\mathcal{L}_{\psi(t^d)}\cong\tau_a^*\mathcal{L}_{\psi(t^d)}=\mathcal{L}_{\psi((t+a)^d)}$$

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012

where $\tau_a : \mathbb{A}^1_{\bar{k}} \to \mathbb{A}^1_{\bar{k}}$ is the translation by a. Then $\mathcal{L}_{\psi(t^d-(t+a)^d)}$ would be geometrically trivial, which is only possible if $t^a - (t+a)^d$ is Artin–Schreier equivalent to a constant, that is, $x^d - (x+a)^d = g(x)^p - g(x)$ for some $g(x) \in \bar{k}[x]$.

Since $x^d - (x+a)^d = -\sum_{i=1}^{d} \binom{d}{i} a^i x^{d-i}$ has degree $\leq d-1$, such a polynomial g would have degree $\leq \frac{d-1}{p}$. In particular, every monomial with non-zero coefficient in f of degree $> \frac{d-1}{p}$ would have degree a multiple of p. In other words, for every $i < d - \frac{d-1}{p}$ such that $d-i$ is not a multiple of p, the binomial coefficient $\binom{d}{i}$ would be a multiple of p.

We already know that for d of the form p^r+1 the monodromy of $\mathcal{F}_d$ is finite, so the result is then a consequence of the following lemma. □

Lemma 5. *Suppose that d is not of the form p^r+1 for some $r \geq 1$. Then there exists some positive integer $l < d - \frac{d-1}{p}$ such that $d-l$ is not a multiple of p and $\binom{d}{l}$ is not a multiple of p.*

Proof. Let $r = \mathrm{ord}_p(d-1)$. We will see that $l = p^r$ satisfies the stated conditions. Since $d-1$ is not a power of p, we have $d-1 \geq 2p^r = 2l$, so

$$l \leq \frac{d-1}{2} = d - \frac{d+1}{2} < d - \frac{d-1}{2} \leq d - \frac{d-1}{p}.$$

Also, $d-l$ is not a multiple of p: if $r=0$ then $d-l = d-1$ is not a multiple of p by definition of r. If $r>0$ then $d-l = (d-1)-l+1$ with $d-1$ and l multiples of p, so d is not a multiple of p. It remains to check that $\binom{d}{l}$ is not a multiple of p. That is, that $\mathrm{ord}_p(d(d-1)\cdots(d-l+1)) = \mathrm{ord}_p((d-1)\cdots(d-l+1)) = \mathrm{ord}_p(l!)$.

In fact, we will check that $\mathrm{ord}_p(d-1-j) = \mathrm{ord}_p(l-j)$ for every $j = 0, 1, \ldots, l-2$. For $j=0$ it is clear by definition of l. For $j \geq 1$, since $j < l = p^r$, we have $\mathrm{ord}_p(j) < r$, so $\mathrm{ord}_p(l-j) = \mathrm{ord}_p(j) = \mathrm{ord}_p(d-1-j)$. □

Using results of Katz and Šuch, this allows to completely determine the geometric monodromy groups in the non-finite case

Corollary 6. *Let G be the geometric monodromy group of $\mathcal{F}_d$. If G is not finite, then*

1. *If $p=2$, then $G = \mathrm{Sp}_{d-1}$.*
2. *If $p \neq 2$ and d is odd, then $G = \mathrm{Sp}_{d-1}$.*
3. *If $p \neq 2$ and d is even, then $G = \mathrm{SL}_{d-1}$.*

Proof. By Proposition 4, G is Lie-irreducible in its given representation. If $p=2$, then $\mathcal{F}_d$ is self-dual (as it has real Frobenius traces), so by [Šuc00, Proposition 11.7], the Lie algebra of G is either $\mathfrak{sp}_{d-1}$ in its standard representation or $\mathfrak{e}_7$ in its 56-dimensional representation. But for $d = 57 = \frac{2^9+1}{2^3+1}$ the monodromy of $\mathcal{F}_d$ is finite by Corollary 4, so

we must be in the former case. So the identity component G^0 of G must be Sp_{d-1}, and therefore $G = \mathrm{Sp}_{d-1}$ by self-duality of $\mathcal{F}_d$.

Suppose now that $p \neq 2$. By [Šuc00, Proposition 11.6], G^0 is then either Sp_{d-1} or SL_{d-1} in their standard representations. If d is even the former case is not possible, so $G^0 = \mathrm{SL}_{d-1}$ and $G = \det^{-1}(\det(G))$. But by [Kat87, Theorem 17], the determinant of $\mathcal{F}_d$ is geometrically trivial, so $G = \mathrm{SL}_{d-1}$. If d is odd, then $\mathcal{F}_d$ is again self-dual (as it has real Frobenius traces), so by the previous argument G must be Sp_{d-1}. □

References

[AMR10] Y. Aubry, G. McGuire, F. Rodier, A few more functions that are not APN infinitely often, Contemp. Math. 518 (2010) 23–31.

[Ax64] J. Ax, Zeros of polynomials over finite fields, Amer. J. Math. 86 (1964) 255–261.

[BLCCC06] Thierry P. Berger, Yann Laigle-Chapuy, Anne Canteaut, Pascale Charpin, On almost perfect nonlinear functions over f_2^n, IEEE Trans. Inform. Theory 52 (9) (2006) 4160–4170.

[BEW98] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley, 1998.

[Del80] Pierre Deligne, La conjecture de Weil. II, Publ. Math. IHÉS 52 (1) (1980) 137–252.

[Kat87] Nicholas M. Katz, On the monodromy groups attached to certain families of exponential sums, Duke Math. J. 54 (1987).

[Kat88] Nicholas M. Katz, Gauss Sums, Kloosterman Sums, and Monodromy Groups, Annals of Mathematics Studies, vol. 116, Princeton University Press, 1988.

[Kat90] Nicholas M. Katz, Exponential Sums and Differential Equations, Annals of Mathematics Studies, vol. 124, Princeton University Press, 1990.

[Kat05] Nicholas M. Katz, Moments, Monodromy, and Perversity: A Diophantine Perspective, Princeton University Press, 2005.

[Kat07] Nicholas M. Katz, g_2 and hypergeometric sheaves, Finite Fields Appl. 13 (2) (2007) 175–223.

[Šuc00] O. Šuch, Monodromy of Airy and Kloosterman sheaves, Duke Math. J. 103 (3) (2000) 397–444.

Please cite this article in press as: A. Rojas-León, Finite monodromy of some families of exponential sums, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2018.06.012