

ON FAMILIES OF ADDITIVE EXPONENTIAL SUMS

ONDREJ ŠUCH

1. INTRODUCTION

In this paper we consider exponential sums of the following form

$$(1) \quad S(\mathbf{E}, f) = \sum_{x_i \in \mathbf{E}} \psi_{\mathbf{E}}(f(x_1, \dots, x_n))$$

where f is a polynomial of degree e in n variables with coefficients in a finite field \mathbf{F} of characteristic p , \mathbf{E} is an overfield of \mathbf{F} , and ψ is an additive character of \mathbf{F} .

It is interesting to ask what happens with sums $S(\mathbf{E}, f)$ when one varies \mathbf{E} , or when one varies f . In order to talk precisely about the latter, we denote by $\mathcal{P}(e, n)$ the scheme parameterizing all polynomials in n variables of degree $\leq e$ with coefficients in the algebraic closure $\bar{\mathbf{F}}$.

First, suppose one fixes the polynomial f , and varies \mathbf{E} . Then Deligne showed that if f lies in a Zariski dense subset of the parameter space $\mathcal{P}(e, n)$ the sums $S(\mathbf{E}, f)$ can be evaluated

$$(2) \quad S(\mathbf{E}, f) = (-1)^n \text{trace}(\text{Frob}^{\deg(\mathbf{E}/\mathbf{F})} | H_c^n(\mathbb{A}^n, \mathcal{F}))$$

where Frob is so called geometric Frobenius, and all eigenvalues α_i of Frob acting on the finite-dimensional vector space $H_c^n(\mathbb{A}^n, \mathcal{F})$ have absolute values $|\mathbf{E}|^{n/2}$. As a consequence,

$$(3) \quad S(\mathbf{E}, f) = (-1)^n \sum_{i=1}^N \alpha_i^{\deg(\mathbf{E}/\mathbf{F})},$$

where N is the dimension of vector space $H_c^n(\mathbb{A}^n, \mathcal{F})$. It follows that there is quite a bit of cancellation in the sum $S(\mathbf{E}, f)$ because

$$(4) \quad |S(\mathbf{E}, f)| \leq N \cdot |\mathbf{E}|^{n/2}$$

holds independently of \mathbf{E} , which contrasts with the trivial estimate $|S(\mathbf{E}, f)| \leq |\mathbf{E}|^n$. The inequality (4) is one instance of the Riemann Hypothesis for varieties over finite fields. If e is coprime to p , then one can describe explicitly one such Zariski dense subset where (2) holds, denoted $\mathcal{D}(n, e)$, by requiring the following two conditions on the highest degree form F_e of f :

- (5) F_e is nonzero
- (6) the closed subscheme of \mathbb{P}^{n-1} defined by vanishing of F_e is smooth of codimension 1

Date: August 18, 2004.

Key words and phrases. exponential sums, monodromy, additive characters.

Still with e prime to p , one can ask what happens if one varies f in $\mathcal{D}(n, e)$. To that end one can show that for any $l \neq p$ there exists a representation

$$(7) \quad \rho_l : \pi_1^{\text{arith}}(\mathcal{D}(n, e)) \rightarrow GL(N, \overline{\mathbf{Q}}_l), \quad N := (e-1)^n$$

such that for any \mathbf{E} -valued point f of the parameter space $\mathcal{D}(n, e)$ the composition

$$(8) \quad \langle \text{Frob} \rangle = \pi_1^{\text{arith}}(\text{Spec}(\mathbf{E})) \rightarrow \pi_1^{\text{arith}}(\mathcal{D}(n, e)) \rightarrow GL(N, \overline{\mathbf{Q}}_l)$$

induces linear space automorphism as in (2). The Zariski closure of the image of $\pi_1^{\text{geom}} := \pi_1(\mathcal{D}(n, e) \otimes \overline{\mathbf{E}})$ in $GL(N, \overline{\mathbf{Q}}_l)$ is called the geometric monodromy group of ρ_l and it governs the variation of $S(\mathbf{E}, f)$ when f varies. Several authors considered question of computing properties of this group and many results in this direction have been proven.

Theorem 1. (Katz) [Katz87] *The Lie algebra of the geometric monodromy group of $S(\mathbf{E}, f)$ for $\mathcal{D}(1, e)$ is $sl(e-1)$ if $p > 2e+1$.*

Theorem 2. (Šuch) [Such97, Theorem 13.2] *The Lie algebra of the geometric monodromy group of $S(\mathbf{E}, f)$ when f varies over $\mathcal{D}(1, e)$ is*

- $sp(N)$ if $p = 2$ and $e \geq 7$,
- $sl(N)$ if $p = 3$ and $e \geq 8$,
- $sl(N)$ if $p > 3$ and $e \geq (p-1)$,

where $N = e-1$.

The first result in multidimensional case came in work of Z.Feng [Feng97].

Theorem 3. (Feng) *The Lie algebra of the geometric monodromy group for $\mathcal{D}(n, e)$ is $sl(N)$ with $N = (e-1)^n$ if $p \gg e$ and $n \geq 2$.*

Recently, Katz extended Feng's result for any characteristic, based on a classification of Larsen of reductive groups having given (small) number of invariants in $V \otimes V \otimes V^\vee \otimes V^\vee$.

Theorem 4. [Katz03, Theorem 3.1.2, 2.2.3] *Let $e \geq 3$ be prime to p , set $N = (e-1)^n$ and denote G_{geom} the geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(n, e)$. Then one of the following possibilities holds*

- a) *the geometric monodromy group over $\mathcal{D}(n, e)$ is finite*
- b) *if G_{geom} is not self dual, then it contains $SL(N)$*
- c) *if G_{geom} is symplectically self dual, then it is $Sp(N)$*
- d) *if G_{geom} is orthogonally self dual, it is either $SO(N)$ or $O(N)$.*

In his work, Katz has been able to show

Theorem 5. (Katz) [Katz03, Theorem 3.1.2] *If one of the following conditions holds*

- $p \geq 7$
- $n \geq 3$
- $p = 5$ and $e \geq 4$
- $p = 3$ and $e \geq 7$
- $p = 2$ and $e \geq 7$

then the geometric monodromy over $\mathcal{D}(n, e)$ is not finite.

In the remainder of this paper we will take a closer look at the geometric monodromy groups in cases not covered by this last theorem, thus answering question raised in [Katz03, Remark 3.8.3]. To formulate our result, let $GL_k(N)$ be the group of $N \times N$ matrices with k -th power of determinant equal to 1 (so that the group $SL(N)$ is equal to $GL_1(N)$ in our notation). Then our main result can be summarized by the following theorem.

Theorem 6. *In the notation as above*

- a) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 3)(\overline{\mathbf{F}}_2)$ is $O_4^+(\mathbf{F}_3)$.*
- b) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 5)(\overline{\mathbf{F}}_2)$ is $O(16)$ in its standard representation.*
- c) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 4)(\overline{\mathbf{F}}_3)$ is $GL_6(9)$.*
- d) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 3)(\overline{\mathbf{F}}_5)$ is $GL_{10}(4)$.*

2. ELEMENTARY TRANSFORMATIONS

In the following we choose a prime $l \neq p$. We also choose a nontrivial additive character

$$\psi : \mathbf{F}_p \rightarrow \overline{\mathbf{Q}}_l^\times.$$

Such character is uniquely specified by the choice of a nontrivial p -th root of unity $\zeta_p = \psi(1)$ in $\overline{\mathbf{Q}}_l$. One extends this character to any finite overfield \mathbf{E} of \mathbf{F}_p by setting

$$\psi_{\mathbf{E}}(x) = \psi(\text{Trace}_{\mathbf{E}/\mathbf{F}_p}(x)).$$

For any element x in \mathbf{F}_p by Little Fermat's theorem $x^p = x$ and therefore $\psi(x) = \psi(x^p)$. This elementary property extends to finite extensions \mathbf{E} of \mathbf{F}_p .

Lemma 7. *For any finite overfield \mathbf{E} of \mathbf{F}_p and any element x in \mathbf{E} one has*

$$\begin{aligned} \psi_{\mathbf{E}}(x) &= \psi_{\mathbf{E}}(x^p) \\ \psi_{\mathbf{E}}(x + y) &= \psi_{\mathbf{E}}(x^p + y^p) \end{aligned}$$

Proof. Let n be the degree of \mathbf{E} over \mathbf{F}_p . The Galois group of automorphisms of \mathbf{E} over \mathbf{F}_p is cyclic, isomorphic to \mathbf{Z}/n , generated by the Frobenius automorphism $\sigma : x \mapsto x^p$. Its n -th power, that is mapping $x \mapsto x^{p^n}$ fixes all elements of \mathbf{E} therefore

$$\begin{aligned} \psi_{\mathbf{E}}(x^p) &= \psi\left(\sum_{i=0}^{n-1} \sigma^i(x^p)\right) = \psi\left(\sum_{i=0}^{n-1} (x^p)^{p^i}\right) = \psi\left(\sum_{i=0}^{n-1} x^{p^{i+1}}\right) = \psi\left(\sum_{i=1}^n x^{p^i}\right) \\ &= \psi\left(x^{p^n} + \sum_{i=1}^{n-1} x^{p^i}\right) = \psi\left(x + \sum_{i=1}^{n-1} x^{p^i}\right) = \psi\left(\sum_{i=0}^{n-1} x^{p^i}\right) = \psi\left(\sum_{i=0}^{n-1} \sigma^i(x)\right) = \psi_{\mathbf{E}}(x) \end{aligned}$$

This proves the first assertion, and the second follows by virtue of ψ being an additive character \square

A classical computation of Gauss determines the value of exponential sum for $p > 2$

$$(9) \quad \sum_{x \in \mathbf{F}_p} e^{2\pi i x^2/p}$$

More generally, sums of the kind

$$(10) \quad \sum_{x \in \mathbf{F}} \chi(x) \Psi(x)$$

where $\chi(x)$, $\Psi(x)$ are multiplicative, resp. additive character are called Gauss sums. It can be easily shown that if χ is nontrivial then

$$(11) \quad \left| \sum_{x \in \mathbf{F}} \chi(x) \Psi(x) \right| = \sqrt{q}$$

Let us denote $\chi_2(x)$ the nontrivial multiplicative character of \mathbf{E}^\times whose values is 1 on squares in \mathbf{E}^\times , and -1 on non-squares.

Lemma 8. *If $a \neq 0$, then*

$$(12) \quad \sum_{x \in \mathbf{E}} \psi_{\mathbf{E}}(ax + b) = 0$$

$$(13) \quad \sum_{x \in \mathbf{E}} \psi_{\mathbf{E}}(ax^2 + bx + c) = \chi_2(a) \psi_{\mathbf{E}}\left(c - \frac{b^2}{4a}\right) \cdot G_{\mathbf{E}} \quad \text{if } p > 2$$

$$(14) \quad \sum_{x \in \mathbf{E}} \psi_{\mathbf{E}}(ax^2 + bx + c) = \sum_{x \in \mathbf{E}} \psi_{\mathbf{E}}\left((a^{1/2} + b)x + c\right) \quad \text{if } p = 2$$

where $G_{\mathbf{E}} = \sum_{x \in \mathbf{E}} \chi_2(x) \psi_{\mathbf{E}}(x)$ is a Gauss sum independent of a, b, c .

Proof. The mapping $x \mapsto ax + b$ is a linear automorphism of \mathbf{F}_q , thus

$$\sum_{x \in \mathbf{E}} \psi_{\mathbf{E}}(ax + b) = \sum_{y \in \mathbf{E}} \psi_{\mathbf{E}}(y) := S$$

In particular

$$S = \sum_{y+1 \in \mathbf{E}} \psi_{\mathbf{E}}(y+1) = \sum_{y \in \mathbf{E}} \psi_{\mathbf{E}}(y) \psi_{\mathbf{E}}(1) = \zeta_p S$$

thus $S = 0$ which proves the first assertion.

To prove the second assertion we complete squares

$$\sum_{x \in \mathbf{E}} \psi_{\mathbf{E}}(ax^2 + bx + c) = \sum_{x \in \mathbf{E}} \psi_{\mathbf{E}}\left(a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a}\right) = \psi_{\mathbf{E}}\left(c - \frac{b^2}{4a}\right) \sum_{y \in \mathbf{E}} \psi_{\mathbf{E}}(ay^2)$$

If a is a square in the multiplicative group then ay^2 runs over same values as y^2 , namely over each nonzero square in \mathbf{E} twice thus the last sum is

$$\sum_{y \in \mathbf{E}} \psi_{\mathbf{E}}(ay^2) = \sum_{y \in \mathbf{E}} \psi_{\mathbf{E}}(y^2) = \sum_{y \in \mathbf{E}} (1 + \chi_2(y)) \psi_{\mathbf{E}}(y) = \sum_{y \in \mathbf{E}} \chi_2(y) \psi_{\mathbf{E}}(y),$$

the last equality by virtue of (12). On the other hand if a is not a square in the multiplicative group of \mathbf{E} , then ay^2 runs twice over each non-squares in \mathbf{E} , thus

$$\sum_{y \in \mathbf{E}} \psi_{\mathbf{E}}(ay^2) = \psi_{\mathbf{E}}(0) + 2 \sum_{\text{non-squares}} \psi_{\mathbf{E}}(y) = \sum_{y \in \mathbf{E}} (1 - \chi_2(y)) \psi_{\mathbf{E}}(y) = - \sum_{y \in \mathbf{E}} \chi_2(y) \psi_{\mathbf{E}}(y)$$

The last assertion follows directly from Lemma 7. \square

We can apply this lemma to deduce divisibility properties of two-variable exponential sums.

Proposition 9. *Let $f(x, y)$ be a polynomial in $\mathcal{D}(3, 2)(\mathbf{F})$, where \mathbf{F} is a field of characteristic 2. Then there exists a finite extension \mathbf{F}' of \mathbf{F} such that for every extension \mathbf{E} of \mathbf{F}'*

$$(15) \quad S(\mathbf{E}, f) = |\mathbf{E}| \sum_{c \in \mathbf{E}: f_4(c)=0} \psi_{\mathbf{E}}(f_3(c)),$$

where f_4 is a polynomial of degree 4, and f_3 has degree ≤ 3 . If

$$(16) \quad f(x, y) = p_1(y)x^2 + p_2(y)x + p_3(y),$$

then we can take $f_4 = p_2^2 - p_1$ and $f_3 = p_3$.

Proof. Let F be the degree 3 form consisting of degree the three terms of f . By assumption, it is nonzero, and the subscheme of \mathbb{P}^1 defined by the vanishing of F is smooth of codimension one. By Bezout's theorem, after extending scalars to a finite extension \mathbf{F}' of \mathbf{F} , it is isomorphic to the sum of 3 distinct points. After applying an automorphism of \mathbb{P}^1 we may assume that one of them lies at $\infty := \mathbb{P}^1 \setminus \mathbb{A}^1$. Then f has form

$$f(x, y) = p_1(y)x^2 + p_2(y)x + p_3(y),$$

where $\deg p_i(y) \leq i$. We can compute

$$\sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(f(x, y)) = \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(p_1(y)x^2 + p_2(y)x + p_3(y))$$

which by Lemma 8 c) is equal to

$$= \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}\left((p_1^{1/2}(y) + p_2(y))x + p_3(y)\right).$$

By Lemma 8 a) the sum over x vanishes whenever $p_1(y) \neq p_2^2(y)$ and thus

$$= |\mathbf{E}| \sum_{y \in \mathbf{E}: p_1(y) = p_2^2(y)} \psi_{\mathbf{E}}(p_3(y))$$

It remains to prove the claim about the degree of f_4 . But that immediately follows from the following lemma.

Lemma 10. *Let*

$$F(x, y) = rxy^2 + sx^2y + tx^3$$

be a homogeneous form of degree 3 in characteristic 2 having distinct points of vanishing in \mathbb{P}^1 (i.e. satisfying (6)). Then r and s are both nonzero.

Proof. If $r = 0$, then $sx^2y + tx^3$ has double zero at $(x, y) = (0, 1)$. On the other hand if $s = 0$, then $rxy^2 + tx^3$ has double zero at $(x, y) = (r^{1/2}, t^{1/2})$. \square

\square

We can apply Lemma 8 to transform two variable exponential sums into one parameter ones.

Proposition 11. *Let $f(x, y)$ be a polynomial in $\mathcal{D}(2, 3)(\mathbf{F})$, where \mathbf{F} is a finite field of characteristic > 2 . Then there exists a finite extension \mathbf{F}' of \mathbf{F} , polynomials f_1, f_2 in $\mathbf{F}'[x]$ such that for every finite extension \mathbf{E} of \mathbf{F}'*

$$\sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(F(x, y)) = G_{\mathbf{E}} \sum_{x \in \mathbf{E}} \chi_2(f_1(x)) \psi_{\mathbf{E}}\left(\frac{f_2(x)}{f_1(x)}\right) + O(1).$$

Proof. By assumption the degree 3 form F consisting of the degree 3 terms in $f(x, y)$ is nonzero. Moreover, by assumption, it defines a smooth codimension one subscheme of \mathbb{P}^1 . Therefore this subscheme is the sum of three distinct points, one of which we may transform by an automorphism of \mathbb{P}^1 (after extension of scalars) to infinity. Then $f(x, y)$ has form

$$f(x, y) = p_1(y)x^2 + p_2(y)x + p_3(y)$$

where $\deg p_i \leq i$. We can compute

$$\sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(f(x, y)) = \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(p_1(y)x^2 + p_2(y)x + p_3(y))$$

which by Lemma 8 is equal to

$$= \sum_{\substack{y \in \mathbf{E} \\ p_1(y) \neq 0}} G_E \chi_2(p_1(y)) \psi_{\mathbf{E}} \left(p_3(y) - \frac{p_2(y)^2}{4p_1(y)} \right) + \sum_{\substack{p_1(y)=0 \\ p_2(y)=0}} \psi_{\mathbf{E}}(p_3(y))$$

By assumption of smoothness of scheme defined by vanishing of F , $p_1(y) \neq 0$, which completes the proof. \square

3. P-ADIC VALUATIONS OF TRACES

The exponential sums of type $S(\mathbf{E}, f) = \sum_{\mathbf{x} \in \mathbf{E}^n} \psi_{\mathbf{E}}(\mathbf{x})$ have a well known cohomological interpretation.

Theorem 12. [Katz03, Theorem 3.1.2] *If $e \geq 3$ is prime to p , there exists a geometrically irreducible, geometrically nonconstant lisse étale sheaf $\mathcal{M}(n, e, \psi)$ on $\mathcal{D}(n, e)$, ι -pure of weight zero, of rank $(e-1)^n$, such that for any f in $\mathcal{D}(n, e)$*

$$\text{trace}(\text{Frob}_{\mathbf{E}, f} | \mathcal{M}(n, e, \psi)) = (-1)^n |\mathbf{E}|^{-n/2} \sum_{v \in \mathbb{A}^n(\mathbf{E})} \psi_{\mathbf{E}}(f(v))$$

From this result we can conclude an explicit numerical criterion for determining if the geometric monodromy group of $\mathcal{M}(n, e, \psi)$ is not finite.

Lemma 13. *Denote by \mathfrak{p} the prime over p in $\mathbf{Q}(\zeta_p)$, and let \mathbf{F} be any finite extension of \mathbf{F}_p . Then the geometric monodromy of $\mathcal{M}(n, e, \psi)$ is finite if and only if for every finite extension \mathbf{E} of \mathbf{F} , and for every f in $\mathcal{D}(n, e)(\mathbf{E})$, $\text{Frob}_{\mathbf{E}, f}$ acting on $H_c^n(\mathbb{A}^n, \mathcal{F})$ has all its eigenvalues divisible by $|\mathbf{E}|^{n/2}$, or equivalently if for every eigenvalue α of $\text{Frob}_{\mathbf{E}, f}$ we have*

$$(17) \quad \text{ord}_{\mathfrak{p}}(\alpha) = \frac{n(p-1)}{2} \times \deg(\mathbf{E}/\mathbf{F}_p)$$

Proof. Follows directly from the numerical criterion for finiteness in [Katz90, Theorem 8.14.4] by noting that $\mathcal{M}(n, e, \psi)$ has determinant arithmetically of finite order [Katz03, Determinant Lemma 3.5.13] and using the fact that $\text{ord}_{\mathfrak{p}}(p) = p-1$. \square

With the heavy work done for us we can now embark on determination of finiteness of monodromy groups.

Proposition 14. *In notation as above*

- a) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 3)(\overline{\mathbf{F}}_2)$ is finite.*
- b) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 5)(\overline{\mathbf{F}}_2)$ is not finite.*
- c) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 4)(\overline{\mathbf{F}}_3)$ is not finite.*

d) *The geometric monodromy group of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 3)(\overline{\mathbf{F}}_5)$ is not finite.*

Proof. a) It follows from Lemma 9 that for any f in $\mathcal{D}(3, 2)(\overline{\mathbf{F}}_2)$ some power of Frob has trace equal to 4. Since the dimension of $\mathcal{M}(n, e, \psi)$ is 4 by theorem 12, and all eigenvalues of Frob acting on $\mathcal{M}(n, e, \psi)$ are of absolute value 1, it follows they are all roots of unity.

To prove parts b), c), d) by [Katz03, 3.2.5] it is sufficient to exhibit explicit polynomials violating equality (17).

b) In characteristic 2 and degree 5 we can take

$$f(x, y) = x^5 + x^2y^3 + y^5$$

This polynomial belongs to $\mathcal{D}(2, 5)(\mathbf{F}_2)$ because the highest degree form is f itself, and since the polynomial $x^5 + x^2 + 1$ is irreducible over \mathbf{F}_2 , the form defines 5 distinct points in \mathbb{P}^1 (). The distribution of $\text{trace}_{\mathbf{E}}(f(x, y))$ is given by the following table

field \mathbf{E}	number of (x, y) such that $\psi_{\mathbf{E}}(f(x, y)) = 1$	number of (x, y) such that $\psi_{\mathbf{E}}(f(x, y)) = -1$
\mathbf{F}_2	1	3
\mathbf{F}_4	6	10
\mathbf{F}_8	28	36
\mathbf{F}_{16}	136	120

Denote by $\{\alpha_i\}$ the set of eigenvalues of Frob acting on finite dimensional $\overline{\mathbf{Q}}_l$ vector space $H_c^2(\mathbb{A}^2, \mathcal{F})$, and write

$$N_k = \sum_i \alpha_i^k$$

$$s_k = \sum_{\text{distinct } i_1, i_2, \dots, i_k} \alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_k}$$

From the table we infer

$$N_1 = -2$$

$$N_2 = -4$$

$$N_3 = -8$$

$$N_4 = 16$$

We can use Newton formulas to compute elementary symmetric functions s_k from the values of symmetric powers N_k . These formulae state

$$s_1 = N_1$$

$$s_2 = \frac{N_1 s_1 - N_2}{2}$$

$$s_3 = \frac{N_3 - N_2 s_1 + N_1 s_2}{3}$$

$$s_4 = \frac{N_1 s_3 - N_2 s_2 + N_3 s_1 - N_4}{4}$$

...

Thus we compute

$$\begin{aligned} s_1 &= -2 \\ s_2 &= 4 \\ s_3 &= -8 \\ s_4 &= 8 \end{aligned}$$

If all α_i were divisible by 2, then $s_4 = 8$ would be divisible by 16, but it is not. Thus by Lemma 13 the geometric monodromy is not finite.

c) In characteristic 3 and degree 4 we can take

$$f(x, y) = x^4 + x^2y^2 + xy^3 + y^4$$

The highest degree form of f is f itself, and it defines 4 distinct points in \mathbb{P}^1 , because the polynomial $x^4 + x^2 + x + 1$ is irreducible over \mathbf{F}_3 . Thus f belongs to $\mathcal{D}(2, 4)(\mathbf{F}_3)$. The distribution of $f(x, y)$ over \mathbf{F}_3 is given by the following table

c in \mathbf{F}_3	# of pairs (x, y) such that $f(x, y) = c$
0	1
1	6
2	2

Therefore

$$\begin{aligned} N_1 &= 1 + 6\zeta_3 + 2\zeta_3^2 \\ &= 4\zeta_3 - 1 = 3 + 4(\zeta_3 - 1) \end{aligned}$$

and therefore

$$\text{ord}_{\mathfrak{p}} N_1 = 1$$

and it follows from Lemma 13 that the geometric monodromy is not finite.

d) In characteristic 5 and degree 3 we can take

$$f(x, y) = x^3 + y^3 + xy^2 + y + xy$$

The highest degree form of this polynomial is $F(x, y) = x^3 + y^3 + xy^2$ and it defines 3 distinct points in \mathbb{P}^1 because the polynomial $x^3 + x + 1$ is irreducible over \mathbf{F}_5 . Therefore f belongs to $\mathcal{D}(2, 3)(\mathbf{F}_5)$. The distribution of $f(x, y)$ over \mathbf{F}_5 is given by the following table

c in \mathbf{F}_5	# of pairs (x, y) such that $f(x, y) = c$
0	8
1	2
2	6
3	5
4	4

Therefore

$$\begin{aligned} N_1 &= 8 + 2\zeta_5 + 6\zeta_5^2 + 5\zeta_5^3 + 4\zeta_5^4 \\ &= \zeta_5^3 + 2\zeta_5^2 - 2\zeta_5 + 4 \\ &= 5 + (1 - \zeta_5)(-(1 - \zeta_5)^2 - 5\zeta_5) \end{aligned}$$

and therefore

$$\text{ord}_{\mathfrak{p}} N_1 = 3$$

and again it follows from Lemma 13 that the geometric monodromy is not finite. \square

4. COMPUTATION OF FINITE MONODROMY

We already know (Proposition 14) that the geometric monodromy group Γ of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 3)(\overline{\mathbf{F}}_2)$ is finite. Now we will compute the group precisely. Let us write

$$f(x, y) = a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3 + b_0x^2 + b_1xy + b_2y^2 + c_0x + c_1y + d$$

The highest degree form of f is

$$F(x, y) = a_0x^3 + a_1x^2y + a_2xy^2 + a_3y^3$$

The discriminant form of $F(x, y)$ is

$$(18) \quad \Delta(a_0, a_1, a_2, a_3) = (a_0a_3)^2 + (a_1a_2)^2$$

and $\mathcal{D}(2, 3)$ is the subscheme of $\text{Spec}(\mathbf{F}_2[a_i, b_i, c_i, d])$ where $\Delta^{1/2} \neq 0$.

Let Z_3 be the closed subscheme of $\mathcal{D}(3, 2)$ where $a_3 = 0$. In terms of previously introduced coordinates, on Z_3 we have

$$\Delta(a_0, a_1, a_2, a_3) = (a_1a_2)^2$$

so that

$$Z_3 = \text{Spec}(\mathbf{F}_2[a_0, a_1, a_2, b_i, c_i, d, \frac{1}{a_1}, \frac{1}{a_2}])$$

Over Z_3 we can write

$$f(x, y) = p_1(x)y^2 + p_2(x)y + p_3(x)$$

where

$$p_1(x) = a_2x + b_2$$

$$p_2(x) = a_1x^2 + b_1x + c_1$$

$$p_3(x) = a_0x^3 + b_0x^2 + c_0x + d$$

Then, over Z_3 , we can express the trace function using (12) and (14) of Lemma 8.

$$(19) \quad \begin{aligned} & \text{trace}(\text{Frob}_{\mathbf{E}, \bar{f}} | \mathcal{M}(2, 3, \psi)(-1)) = \\ &= \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(p_1(x)y^2 + p_2(x)y + p_3(x)) \\ &= \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}\left((p_1^{1/2}(x) + p_2(x))y + p_3(x)\right) \\ &= |E| \sum_{x' \in \mathbf{E}: p_1^{1/2}(x) = p_2(x)} \psi_{\mathbf{E}}(p_3(x)) \\ &= |E| \sum_{x' \in \mathbf{E}: p_1(x) = p_2^2(x)} \psi_{\mathbf{E}}(p_3(x)) \end{aligned}$$

Let us denote by R the ring

$$\overline{\mathbf{F}}_2[a_0, a_1, a_2, b_i, c_i, d, \frac{1}{a_1}, \frac{1}{a_2}],$$

so that $Z_3 \otimes \overline{\mathbf{F}}_2 = \text{Spec}R$. Then p_1, p_2, p_3 are elements of $R[x]$. Consider now the polynomial $A(z)$ over the field of fractions $K(R)$ of R

$$(20) \quad A(z) := p_2^2(z) - p_1(z) = a_1^2z^4 + b_1^2z^2 + a_2z + (c_1^2 + b_2)$$

Lemma 15. *Over $K(R)$ the polynomial $A(z)$ is*

- a) of degree 4,
- b) separable over $K(R)$,
- c) irreducible over $K(R)$,
- d) its Galois group over $K(R)$ is S_4 .

Proof. Part a) follows from the fact, that p_2 is of degree 2. Part b) follows since p_1 is of degree 1.

To prove part c), consider $A(z)$ over the one parameter curve in Z_3 given by

$$\begin{aligned} a_1 &= 1 \\ b_1 &= 0 & a_2 &= t \\ c_1 &= 0 & b_2 &= t & p_3(x) &= 0 \end{aligned}$$

The polynomial $A(z)$ is then of form

$$A(z) = z^4 + tz + t$$

and we conclude that the above specialization of $A(z)$ is irreducible by Eisenstein's criterion over the completion of $\overline{\mathbf{F}}_2(t)$ with respect to valuation at $t = 0$. A fortiori, $A(z)$ is irreducible over $K(R)$, which proves c).

Now we proceed to determine the Galois group of the splitting field of $A(z)$. Since most authors describe the standard procedure of solving quartic equations only in characteristic $\neq 2, \neq 3$, we proceed with detailed explanation. Say $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ are roots of $A(z)$. Then

$$\begin{aligned} \beta_1 &= -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\ \beta_2 &= -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\ \beta_3 &= -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3) \end{aligned}$$

are quantities that are fixed by the Klein's Viergruppe inside S_4 , and S_4 permutes them. One computes that

$$\beta_1 + \beta_2 + \beta_3 = -\sum_{i \neq j} 2\alpha_i \alpha_j = 0,$$

since we are in characteristic 2. Since $\sum_i \alpha_i = 0$, we can also compute

$$\begin{aligned} \beta_1 \beta_2 + \beta_1 \beta_3 + \beta_2 \beta_3 &= \left(\sum_{i \neq j} \alpha_i^2 \alpha_j^2 \right) + (3\alpha_1 \alpha_2 \alpha_3 \sum_i \alpha_i) + 6\alpha_1 \alpha_2 \alpha_3 \alpha_4 \\ &= \left(\frac{b_1^2}{a_1^2} \right)^2 \end{aligned}$$

Finally, $\beta_1 \beta_2 \beta_3$ is a symmetric function in α_i , thus it can be represented as a polynomial in the elementary symmetric functions s_i so that

$$(21) \quad \beta_1 \beta_2 \beta_3 = f_1(s_2 s_4) + f_2 s_3^2 + f_3 s_2^3$$

for some constants f_1, f_2, f_3 in \mathbf{F}_2 . Since $\beta_1 \beta_2 \beta_3$ vanishes whenever two of the roots α_i coincide, looking at

$$(22) \quad (z^2 - \sigma^2)(z^2 - \tau^2) = z^4 + (\sigma^2 + \tau^2)z^2 + \sigma^2 \tau^2$$

we conclude that

$$0 = (\sigma^2 + \tau^2)(f_1 \sigma^2 \tau^2 + f_3 (\sigma^2 + \tau^2)^2)$$

for any choice of σ and τ . It follows that $f_1 = f_3 = 0$. Since $\beta_1\beta_2\beta_3$ is not identically 0, we must have $f_2 = 1$ and thus

$$\beta_1\beta_2\beta_3 = s_3^2 = \frac{a_2^2}{a_1^4}$$

Therefore the splitting field of $A(z)$ contains also the splitting field of

$$B(z) := (z - \beta_1)(z - \beta_2)(z - \beta_3) = z^3 + \frac{b_1^4}{a_1^4}z + \frac{a_2^2}{a_1^4}$$

This is so called resolvent cubic of $A(z)$. Using the same specialization values as before, we see that

$$B(z) = z^3 + t^2$$

defines a completely ramified extension of degree 3 in the completion of $\overline{\mathbf{F}}_2(t)$ with respect to $t = 0$, and thus the resolvent cubic $B(z)$ is irreducible. One then sets

$$\begin{aligned}\gamma_1 &= \beta_1 + \zeta_3\beta_2 + \zeta_3^2\beta_3 \\ \gamma_2 &= \beta_1 + \zeta_3^2\beta_2 + \zeta_3\beta_3\end{aligned}$$

and checks that

$$\begin{aligned}\gamma_1\gamma_2 &= \beta_1^2 + \beta_2^2 + \beta_3^2 + (\zeta_3 + \zeta_3^2)(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3) \\ &= (\beta_1 + \beta_2 + \beta_3)^2 - 3(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3) \\ &= \left(\frac{b_1^2}{a_1^2}\right)^2\end{aligned}$$

and

$$\begin{aligned}\gamma_1^3 + \gamma_2^3 &= (\beta_1 + \zeta_3\beta_2 + \zeta_3^2\beta_3)^3 + (\beta_1 + \zeta_3^2\beta_2 + \zeta_3\beta_3)^3 \\ &= (\beta_1 + \zeta_3\beta_2 + \zeta_3^2\beta_3)^3 + (\beta_1 + \zeta_3^2\beta_2 + \zeta_3\beta_3)^3 + (\beta_1 + \beta_2 + \beta_3)^3 \\ &= 3(\beta_1^3 + \beta_2^3 + \beta_3^3) + 18\beta_1\beta_2\beta_3\end{aligned}$$

Newton formulae state

$$3s_3 = S_3 - S_2s_1 + S_1s_2,$$

and since $s_1 = S_1 = \sum_i \beta_i = 0$, we conclude that

$$\gamma_1^3 + \gamma_2^3 = \beta_1\beta_2\beta_3 = \frac{a_2^2}{a_1^4}.$$

It follows that the splitting field of $B(z)$ (and a fortiori of $A(z)$) contains roots of

$$C(z) = (z - \gamma_1^3)(z - \gamma_2^3) = z^2 + \frac{a_2^2}{a_1^4}z + \left(\frac{b_1^2}{a_1^2}\right)^6$$

and since a_2, a_1 are invertible by Lemma 10, we can change variables,

$$z' = \frac{a_1^2}{a_2^2}z$$

to arrive at equation

$$C'(z') = z'^2 - z' + \frac{b_1^{12}}{a_2^4 a_1^8}.$$

By Artin-Schreier theory, this equation is reducible if and only if its constant term is of the form $f^2 - f$ for some element f in $K(R)$. Suppose that was the case, so that

$$\frac{b_1^{12}}{a_2^4 a_1^8} = f^2 - f$$

Then

$$\begin{aligned} \frac{b_1^3}{a_2 a_1^2} &= \frac{b_1^{12}}{a_2^4 a_1^8} + f^2 - f - \frac{b_1^3}{a_2 a_1^2} \\ \frac{b_1^3}{a_2 a_1^2} &= \left(f + \frac{b_1^6}{a_2^2 a_1^4} + \frac{b_1^3}{a_2 a_1^2}\right)^2 - \left(f + \frac{b_1^6}{a_2^2 a_1^4} + \frac{b_1^3}{a_2 a_1^2}\right) \end{aligned}$$

so that there is g in $K(R)$ for which

$$\frac{b_1^3}{a_2 a_1^2} = g^2 - g$$

Looking at one parameter family in Z_3 given by

$$\begin{aligned} a_1 &= 1 \\ b_1 &= 1 & a_2 &= t \\ c_1 &= 0 & b_2 &= t & p_3(x) &= 0 \end{aligned}$$

we see that $g^2 - g$ has a simple pole at $t = 0$, which is impossible. Thus $C(z)$ is an irreducible polynomial over $\overline{\mathbf{F}}_2(t)$ and a fortiori over $K(R)$.

We have shown, that $A(z), B(z), C(z)$ are all irreducible. Therefore the Galois group of $C(z)$ is S_2 . Since the splitting field of $B(z)$ contains roots of $C(z)$, and $B(z)$ is irreducible, the Galois group of $B(z)$ is S_3 . Finally, since the splitting field of $A(z)$ contains all roots of $B(z)$, and $A(z)$ is irreducible, it follows that the Galois group of $A(z)$ is S_4 . \square

Define Z_C to be the normalization of Z_3 in the splitting field K_C of $C(z)$ (equivalently of $C'(z)$). Similarly define Z_B, Z_A to be the normalizations of Z_3 in the splitting fields K_B, K_A of $B(z), A(z)$ respectively.

Lemma 16. Z_A is étale over Z_3 . Elements α_i of the field of functions of U_A extend to sections of the structural sheaf of Z_A .

Proof. The normalization of a normal base in a finite separable extension is automatically finite, so it is sufficient to show that the normalization is unramified. To prove this it is sufficient to look at the discriminant of $A(z)$, which is $a_2^4 a_1^4$. Since both are invertible on Z_3 , the map is unramified. Since α_i are roots of $A(z)$, it follows they are defined over all of Z_A . \square

Let \mathcal{L}_3 be the universal degree 2 cover of $\mathbb{A}^4 \times \mathbb{A}^1$ given by the lisse sheaf with trace function

$$(23) \quad \text{trace}(\text{Frob}_{(j_3, j_2, j_1, j_0; x), \mathbf{E}}) | \mathcal{L}_3 = \psi_{\mathbf{E}}(j_3 x^3 + j_2 x^2 + j_1 x + j_0)$$

Lemma 17. If $n_A : Z_A \rightarrow Z_3$ denotes the canonical map, then $n_A^* \mathcal{M}(2, 3)$ is the sum of four geometrically distinct, nontrivial characters. Natural action of $\text{Gal}(K_A/K(R))$ on Z_A permutes them.

Proof. The elements α_i define maps $p_i : Z_A \rightarrow \mathbb{A}^1$. Let r be the map $Z_3 \rightarrow \mathbb{A}^4$ given by

$$\begin{aligned} j_3 &\mapsto a_0 \\ j_2 &\mapsto b_0 \\ j_1 &\mapsto c_0 \\ j_0 &\mapsto d \end{aligned}$$

Define $\rho_i : Z_A \rightarrow \mathbb{A}^4 \times \mathbb{A}^1$ to be the map $(r \circ n_A) \times p_i$. Then computation (19) shows that on Z_A sheaves $n_A^* \mathcal{M}(2, 3)$ and $\oplus_i \rho_i^* \mathcal{L}_3$ have identical trace functions, and since they are semisimple, they must be isomorphic.

Suppose that some $\rho_i^* \mathcal{L}_3$ would be trivial, say $\rho_1^* \mathcal{L}_3$. Then also its restrictions to closed subscheme $n_A^* r^*((0, 0, 1, 0))$ would be trivial. On this subscheme of Z_A , the trace of $\rho_1^* \mathcal{L}_3$ is

$$\psi_{\mathbf{E}}(\alpha_1).$$

To claim this sheaf is trivial is to say, that α_1 is Artin-Schreier equivalent to 0, that is of the form $f^2 - f$. Now consider the one parameter family in Z_3 given by

$$\begin{aligned} a_1 &= t \\ b_1 &= 0 & a_2 &= t^2 \\ c_1 &= 0 & b_2 &= t \end{aligned}$$

Over this family, equations defining the splitting of $A(z)$ have the form

$$\begin{aligned} A(z) &= t^2 z^4 + t^2 z + t \\ B(z) &= z^3 + 1 \\ C(z) &= z^2 + t^2 z \end{aligned}$$

We see that the place $t = 0$ is totally ramified by splitting $A(z)$ of index 4. Since $\frac{1}{\alpha_1}$ is the solution of

$$w^4 + tw^3 + t = 0,$$

it follows that $\frac{1}{\alpha_1}$ has valuation 1 in the splitting field of $A(z)$, hence α_1 has a pole of odd order 1 in the splitting field of $A(z)$, hence it cannot be of the form $f^2 - f$. It follows that characters $\rho_i^* \mathcal{L}_3$ are all nontrivial.

Suppose now, that two of the characters, say $\rho_1^* \mathcal{L}_3$ and $\rho_2^* \mathcal{L}_3$, were geometrically isomorphic. Then their difference $\phi := \rho_1^* \mathcal{L}_3 (\rho_2^* \mathcal{L}_3)^{-1}$ would be geometrically trivial. Hence its restriction to the closed subscheme $n_A^* r^*((0, 0, 1, 0))$ would be trivial. On this subscheme of Z_A , the trace of ϕ is

$$\psi_{\mathbf{E}}(\alpha_1 - \alpha_2)$$

and to say character with this trace is trivial means that $\alpha_1 - \alpha_2$ would be Artin-Schreier equivalent to zero, that is, of the form $f^p - f$ for some f in K_A . Consider

the one parameter family in Z_3 given by

$$\begin{aligned} a_1 &= t \\ b_1 &= 0 & a_2 &= t \\ c_1 &= 0 & b_2 &= t \end{aligned}$$

Over this family, equations defining the splitting field of $A(z)$ have the form

$$\begin{aligned} A(z) &= t^2 z^4 + tz + t \\ B(z) &= z^3 + \frac{1}{t^2} \\ C(z) &= z^2 + z \end{aligned}$$

We can multiply $A(z)$ by $t^{-2/3}$ to obtain equation

$$(24) \quad 0 = t^{4/3} z^4 + t^{1/3} z + t^{1/3}$$

and setting $\omega = t^{1/3} z$ we have

$$(25) \quad 0 = \omega^4 + \omega + t^{1/3}$$

It follows that the place $t = 0$, tamely ramified in $K(B)$, splits completely in K_A/K_B . Since all roots of $A(z)$ are units in this place, it follows that over any place \mathfrak{t} in K_A over $t = 0$, ω is a uniformizing parameter in \mathfrak{t} . If α_1 is one solution of (25) then all remaining solutions are of the form $\alpha_1 + \zeta_3^i$. But then,

$$\alpha_1 - \alpha_2 = t^{-1/3} \zeta_3^i$$

But $t^{-1/3}$ has simple pole at any place \mathfrak{t} over $t = 0$, thus it can't be Artin-Schreier equivalent to 0. It follows that all characters $\rho_i^* \mathcal{L}_3$ are geometrically distinct.

The statement about Galois action of $\text{Gal}(K_A/K(R))$ follows from the fact, that $\text{Gal}(K_A/K(R))$ permutes α_i . \square

Proposition 18. *The geometric monodromy group Γ' of $S(\mathbf{E}, f)$ over $Z_3(\overline{\mathbf{F}}_2)$ has order 384.*

Proof. From Lemma 17 it follows that K_A is the smallest etale cover of Z_3 over which $\mathcal{M}(2, 3)$ splits into the sum of four characters induced by roots α_i of $A(z)$. We have thus an exact sequence

$$\{1\} \rightarrow (\mathbf{Z}/2)^4 \rightarrow \Gamma' \rightarrow S_4 \rightarrow \{1\},$$

and the statement about the group size follows. \square

Theorem 19. *The geometric monodromy group Γ of $S(\mathbf{E}, f)$ over $\mathcal{D}(2, 3)(\overline{\mathbf{F}}_2)$ is $O_4^+(\mathbf{F}_3)$.*

Proof. The group Γ is a subgroup of $GL(4, \mathbf{Z}_l)$ for any $l \neq 2$, in particular of $GL(4, \mathbf{Z}_3)$. It is a finite group by Proposition 14. Since the reduction homomorphism

$$GL(4, \mathbf{Z}_3) \rightarrow GL(4, \mathbf{F}_3)$$

has no elements of finite order in its kernel, it is a subgroup of $GL(4, \mathbf{F}_3)$. In fact since the sheaf $\mathcal{M}(2, 3)$ is orthogonally selfdual (Lemma 20), it is a subgroup of one of two general orthogonal group over \mathbf{F}_3 . (Over the field of 3 elements there are actually two groups that preserve an orthogonal quadratic form.) In

GAP notation [GAP], the two groups are `GeneralOrthogonalGroup (1,4,3)` and `GeneralOrthogonalGroup (-1,4,3)`, of orders 1152 and 1440 respectively. The group Γ contains the monodromy group Γ' which we know by the previous proposition has order 384. It follows it is a subgroup of $O_4^+(\mathbf{F}_3)=\text{GeneralOrthogonalGroup}(1,4,3)$ of index either 1 or 3.

Suppose Γ were of index 3 in $O_4^+(\mathbf{F}_3)$. There are 6 subgroups of size 384 in $O_4^+(\mathbf{F}_3)$, all of them isomorphic to `SmallGroup(384, 5602)`. One can use GAP to check that none of the irreducible 4 dimensional representations V of `SmallGroup(384, 5602)` has 3 dimensional space of invariants in $V^{\otimes 4}$. This contradicts [Katz03, Higher Moment Theorem 1.22.22] and concludes our proof. \square

5. COMPUTATION OF INFINITE MONODROMIES

Our goal in this chapter is to conclude the proof of our main result, Theorem 6. Part a) is proved in Proposition 18, and now we deal with the infinite cases. In those it is important to determine the type of duality of sheaf $\mathcal{M}(n, e)$. That is accomplished by the following result of Katz.

Lemma 20. [Katz03, 3.12] *Sheaf $\mathcal{M}(n, e, \psi)$ is not self dual if $p > 2$. If $p = 2$ it is symplectic if n is odd, and it's orthogonal if n is even.*

Theorem 21. [Katz03, Corollary 6.8.31] *Suppose that $e \geq 3$ is prime to p , and that $n \geq 2$. If ne is even, then the geometric monodromy group for $\mathcal{M}(n, e, \psi)$ contains an element of determinant -1 .*

Lemma 22. [Katz03, Lemma 6.8.13] *Suppose $e \geq 3$ is prime to p . If in addition $e - 1$ is prime to p , then for any $n \geq 1$, the geometric monodromy group for $\mathcal{M}(n, e, \psi)$ on $\mathcal{D}(n, e)$ contains an element whose determinant is a primitive p -th root of unity*

Proof of Theorem 6, parts b), c), d). Proposition 14 states that monodromy groups in cases b), c), d) are infinite. Combining Theorem 4, and Lemma 20 we conclude that in cases

- b) the geometric monodromy group is $O(16)$ or $SO(16)$,
- c) the geometric monodromy group contains $SL(9)$,
- d) the geometric monodromy group contains $SL(4)$.

Applying Theorem 21 proves part b). Since traces on sheaf $\mathcal{M}(n, e)$ lie in the field $\mathbf{Q}(\zeta_p)$, the determinant in each case also lies in the field $\mathbf{Q}(\zeta_p)$ and since its of finite order, its $2p$ -th power must be 1. Applying Lemma 22, this proves d).

To prove case c) where hypothesis of Lemma 22 is not fulfilled we compute explicitly on computer, that if

$$(26) \quad G_1(x, y) = (x - 1)y^3 + (x^2 - x - 1)y^2 + (x^3 + x^2 + x)y + x^4 + x^3 + x - 1$$

$$(27) \quad G_2(x, y) = (x - 1)y^3 + (x^2 - x + 1)y^2 + (x^3 + x^2 - x - 1)y + x^4 + x^2$$

then $\det(\text{Frob}_{\mathbf{F}_3, G_1}) \times \det(\text{Frob}_{\mathbf{F}_3, G_2}^{-1})$ is a primitive 3rd root of unity. Since the geometric monodromy group contains an element with determinant -1 , it follows that the group is $GL_6(9)$ in case c). \square

Remark 23. Of multiple ways to compute determinants in (26) we used the one based on (13). Write $G(x, y) = p_1(x)y^3 + p_2(x)y^2 + p_3(x)y + p_4(x)$. Then

$$\begin{aligned} \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(G(x, y)) &= \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(p_1(x)y^3 + p_2(x)y^2 + p_3(x)y + p_4(x)) \\ &= \sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}\left(p_2(x)y^2 + (p_3(x) + p_1^{1/3}(x))y + p_4(x)\right) \end{aligned}$$

assuming that $p_2(x)$ and $p_3(x) + p_1^{1/3}(x)$ have no common zeroes we can write

$$= G_{\mathbf{E}} \sum_{\substack{x \in \mathbf{E} \\ p_2(x) \neq 0}} \chi_2(p_2(x)) \psi_{\mathbf{E}}\left(p_4(x) - \frac{(p_3(x) + p_1^{1/3}(x))^2}{4p_2(x)}\right)$$

for a polynomial $p(x) = \sum_i a_i x^i$ let us define $p^\vee(x) = \sum_i a_i^{1/3} x^i$ so we can simplify

$$\begin{aligned} &= G_{\mathbf{E}} \sum_{\substack{x^3 \in \mathbf{E} \\ p_2(x^3) \neq 0}} \chi_2(p_2(x^3)) \psi_{\mathbf{E}}\left(p_4(x^3) - \frac{(p_3(x^3) + p_1^\vee(x))^2}{p_2(x^3)}\right) \\ &= G_{\mathbf{E}} \sum_{\substack{x^3 \in \mathbf{E} \\ p_2(x^3) \neq 0}} \chi_2(p_2(x^3)) \psi_{\mathbf{E}}\left(p_4^\vee(x) - \frac{(p_3(x^3) + p_1^\vee(x))^2}{p_2(x^3)}\right) \end{aligned}$$

Remark 24. If one sets

$$h(x) = p_4^\vee(x) - \frac{(p_3^\vee(x))^2}{p_2^\vee(x)} + \frac{p_1^\vee(x)(p_3(x^3) - p_1^\vee(x))}{p_2(x^3)}$$

so that

$$\sum_{x, y \in \mathbf{E}} \psi_{\mathbf{E}}(G(x, y)) = G_{\mathbf{E}} \sum_{\substack{x^3 \in \mathbf{E} \\ p_2(x^3) \neq 0}} \chi_2(g(x)) \psi_{\mathbf{E}}(h(x))$$

then condition on $G(x, y)$ belonging to $\mathcal{D}(2, 4)(\overline{\mathbf{F}}_3)$ is equivalent to $p_1(x)$ being of degree 1, and $h(x)$ having a pole of order 4 at ∞ .

Remark 25. The complete vector of elementary symmetric functions of roots of $\text{Frob}_{\mathbf{F}_3, G_1}$ acting on $\mathcal{M}(2, 3, \psi)(1/2)$ equals

$$\begin{aligned} (s_i) &= (-2, 2 + \zeta_3, -3(1 + \zeta_3), \\ &\quad 6 + 3\zeta_3, -9, 9(1 - \zeta_3), \\ &\quad -27, 54(2 + \zeta_3), -81(2 + \zeta_3)) \end{aligned}$$

One can check, that each root satisfies one of the following equations

$$\begin{aligned} x^6 + 4x^5 + 10x^4 + 21x^3 + 30x^2 + 36x + 27 &= 0, \\ x^2 + 3x + 3 &= 0, \\ x^2 - 3x + 3 &= 0, \\ x^4 + 3x^2 + 9 &= 0, \end{aligned}$$

namely 3 roots satisfy the first one, and 2 roots each satisfy each of the last three equations. Similarly, for $\text{Frob}_{\mathbf{F}_3, G_2}$ the symmetric functions have values

$$(s_i) = (-2, 1 - \zeta_3, 3\zeta_3, \\ 3(1 - \zeta_3), 9\zeta_3, 9(1 - \zeta_3), \\ 27\zeta_3, -54(1 + 2\zeta_3), 81(1 + 2\zeta_3))$$

One can check, that seven roots satisfy equation

$$x^{14} - 2x^{13} + 4x^{12} - 3x^{11} + 3x^{10} + 9x^9 - 9x^8 + 27x^7 \\ - 27x^6 + 81x^5 + 81x^4 - 243x^3 + 972x^2 - 1458x + 2187 = 0$$

and two of the roots equation

$$x^2 + 3x + 3 = 0$$

REFERENCES

- [Feng97] Z.T. Feng, *On Certain Families of Multivariable Exponential Sums and Their Monodromy Groups*, Ph.D. thesis, 1997, Princeton University
- [GAP] Lehrstuhl D für Mathematik, RWTH Aachen, GAP, computer program available from <http://www-gap.dcs.st-and.ac.uk/gap>
- [Katz87] N.M. Katz, *On the monodromy groups attached to certain families of exponential sums*, Duke Math. J. **54** (1987), 41-56
- [Katz90] N.M. Katz *Exponential sums and differential equations*, Annals of Mathematics Studies; no. 124, Princeton University Press, 1990
- [Katz03] N.M. Katz *Moments, Monodromy and Perversity: A Diophantine Perspective*, book preprint distributed at Princeton conference, December 2003
- [Such97] O. Šuch, *Monodromy of Airy and Kloosterman sheaves*, Duke Math. J. **103** (2000), 397-444

INSTITUTE OF MATHEMATICS AND COMPUTER SCIENCE, SEVERNÁ 5, 974 01 BANSKÁ BYSTRICA,
SLOVAK REPUBLIC,
E-mail address: ondrejs@savbb.sk