A STRATIFICATION RESULT
FOR AN EXPONENTIAL SUM MODULO $p^2$

KOSTADINKA LAPKOVA AND STANLEY YAO XIAO

Abstract. In this note we consider algebraic exponential sums over the values of homogeneous nonsingular polynomials $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ in the quotient ring $\mathbb{Z}/p^2\mathbb{Z}$. We provide an estimate of this exponential sum and a corresponding stratification of the space $\mathbb{A}_n^p$, which in particular illustrates a general stratification theorem of Fouvry and Katz.

1. Introduction

Let $F(x) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a polynomial of degree $d \geq 1$ and let $V_F$ be the hypersurface defined by $F(x) = 0$. Denote by $K$ a finite field or a quotient ring of size $q$. We are interested in the exponential sums

$$S_F(h; K) = \sum_{x \in V_F(K)} \exp\left(\frac{h_1x_1 + \cdots + h_nx_n}{q}\right),$$

where we use the notation $\exp(x) := e^{2\pi ix}$. In this note we address the estimate of $S_F(h, \mathbb{Z}/p^2\mathbb{Z})$ for large primes $p$.

A fundamental work in the estimation of general algebraic exponential sums is the paper of Fouvry and Katz [3]. When we drop a multiplicative character factor from the sums considered in [3], and take not a general nontrivial additive character but only $\exp \pmod{q}$, we arrive at sums similar to $S_F(h, \mathbb{F}_p)$, thus our result would be a special case of the sums considered in [3], but with the modulus being squares of primes rather than primes. An analogous algebraic exponential sum was treated by Fouvry and our main theorem resembles [2, Proposition 1.0] in the special case when the subscheme considered is a smooth hypersurface.

One significant aspect of the results of Fouvry and Fouvry-Katz [2, 3] is that they establish the existence of a decreasing filtration of subschemes (stratification) $\mathbb{A}_Z^2 \supset G_1 \supset G_2 \supset \cdots \supset G_n$ of codimension $\geq j$, such that whenever $h \notin G_j(\mathbb{F}_p)$ we have

$$S_F(h, \mathbb{F}_p) \ll p^{(n-1)/2+(j-1)/2}.$$

Thus the deviation from the bound $p^{(n-1)/2}$, which amounts to square-root cancellation and is the best that can be expected in general, is tamed by the fact that the dimensions of the subschemes $G_j$ for $j \geq 1$ are small. However, the construction of this stratification is ineffective and inaccessible for non-specialists. Furthermore, the verifying of certain criteria that allow to apply the theorems of Fouvry-Katz [3] constitutes a separate problem, see for example [1]. Also see [14] for a certain generalization.

Date: February 27, 2020.
A further overview of the topic is given in the excellent review by P. Michel \cite{11}.

On the other hand, Stepanov \cite{12} focuses not on the stratification but rather constructs a subset of the good locus $\mathcal{G}_1$ in which the optimal bound $S_F(h, \mathbb{F}_q) \ll q^{(n-1)/2+\epsilon}$ holds for any finite field and not only for fields of prime order. Heath-Brown \cite{4} treats the special case $q = p^2$ and $F \equiv 1$.

We show that in the specific case considered in (1.1) the expected estimate holds and we give an explicitly constructed stratification.

For a given vector $h \in \mathbb{Z}^n$ consider the auxiliary affine variety $W_{F,h}$ given by the equations defined over $\mathbb{F}_p$

\begin{equation}
F(y) = 0
\end{equation}

\begin{equation}
h_i \frac{\partial F}{\partial x_j}(y) = h_j \frac{\partial F}{\partial x_i}(y), \quad 1 \leq i, j \leq n, i \neq j.
\end{equation}

Note that this is the singular locus of the variety $\{F(y) = 0, h \cdot y = 0\}$. Now put $G_{F,j}$ for the set given by

\begin{equation}
G_{F,j} = \{h \in \mathbb{F}_p^n : \dim(W_{F,h}) \geq j\}.
\end{equation}

We have the following theorem, which can be viewed as an extension to Theorem 1.2 of Fouvry-Katz \cite{3} to $V(\mathbb{Z}/p^2\mathbb{Z})$ in a restricted setting.

**Theorem 1.1.** Let $F$ be a non-singular homogeneous polynomial in $\mathbb{Z}[x_1, \ldots, x_n]$. Let $V_F$ be the hypersurface defined by $F$. Further, suppose that $F$ is non-singular modulo $p$. For $h \in \mathbb{Z}^n$ let $S(h; p^2)$ be the exponential sum

\begin{equation}
S(h; p^2) = \sum_{x \in V_F(\mathbb{Z}/p^2\mathbb{Z})} \exp \left( \frac{h_1 x_1 + \cdots + h_n x_n}{p^2} \right).
\end{equation}

Then the sets defined in (1.4) are varieties satisfying $G_{F,0} = \mathbb{A}_p^n \supseteq G_{F,1} \supseteq \cdots \supseteq G_{F,n}$, where the codimension of each $G_{F,j}$ is $\geq j$, and we have the estimate

\[ S(h; p^2) = O_F \left( p^{n+j-2} \right) \]

whenever $h \notin G_{F,j}(\mathbb{F}_p)$.

The interest in this theorem is that unlike in the situation considered by Fouvry and Katz, a priori we have relatively little access to tools from algebraic geometry. This is because the base ring we consider is $\mathbb{Z}/p^2\mathbb{Z}$ which is not a field, so many of the basic facts one takes for granted from algebraic geometry do not necessarily hold. Nevertheless, we are able to reduce to a case where we once again consider things over a field.

When $n = 2$ and $F$ is non-singular of degree $d \geq 2$, we have $\dim W_{F,h} = 1$ if and only if the equation $h_2 \frac{\partial F}{\partial x_1}(y) = h_1 \frac{\partial F}{\partial x_2}(y)$ is redundant. If $h_1, h_2$ are not both zero then this implies that $F$ shares a component with a curve of strictly smaller degree, which violates the assumption that $F$ is non-singular. Therefore the only way to
have \( \dim W_{F,h} = 1 \) is for \( h_1 = h_2 = 0 \) and so any non-singular \( F \in \mathbb{Z}[x_1, x_2] \) we have square-root cancellation, and obtain the bound
\[
S(h; p^2) \ll p^{n-1}.
\]

We will soon see in the proof that this essentially follows from the Weil bound resolving the Riemann Hypothesis for curves, where for any (higher) dimension of \( V_F \) we apply the theorem of Lang-Weil.

In many sieving problems (see for example [7]) one applies a result like that of Fouvry-Katz [3] to use congruence conditions modulo somewhat large primes to show paucity of contributions, which results in sums of the shape
\[
\sum_{x_1 < p < x_2} \left( \frac{B^n}{p} + 1 \right).
\]

Notice that the sum over the lead terms \( 1/p \) diverges, so in such a case the size of \( x_1 \) is not relevant. On the other hand, if we apply our Theorem instead, then one would end up with a sum over \( 1/p^2 \) which is then convergent, so the sum would then be sensitive to the size of \( x_1 \). This is crucial if one wishes to obtain asymptotic formulae. Similar arguments could lead to some of the potential applications of our theorem.

2. Proof of Theorem 1.1

Write \( x = y + pz \). Then we have
\[
(2.1) \quad F(x) = F(y) + p \left( \sum_{i=1}^{n} z_i \frac{\partial F}{\partial x_i}(y) \right) + p^2 H_F(y; z) \equiv F(y) + pz \cdot \nabla F(y) \quad (\text{mod } p^2).
\]

Now restrict \( y \in \mathbb{F}_p \). Then \( y + pz \in V(\mathbb{Z}/p^2\mathbb{Z}) \) if and only if \( y \in V(\mathbb{F}_p) \) and
\[
z \cdot \nabla F(y) \equiv -F(y)/p \quad (\text{mod } p).
\]

Then (1.5) becomes
\[
\sum_{y \in V(\mathbb{F}_p)} \exp \left( \frac{h_1 y_1 + \cdots + h_n y_n}{p^2} \right) \sum_{z \equiv (\text{mod } p)} \exp \left( \frac{h_1 z_1 + \cdots + h_n z_n}{p} \right).
\]

We examine the inner sum in detail. Let us introduce the notation
\[
T_p(a, b, c) := \sum_{z \equiv (\text{mod } p)} \exp \left( \frac{a \cdot z}{p} \right).
\]

We claim that the exponential sum \( T_p(a, b, c) = 0 \) every time there exists a pair \((i, j)\) with \( 1 \leq i, j \leq n \) and \( i \neq j \), such that \( a_i b_j \neq a_j b_i \) (mod \( p \)). Indeed, if the latter holds, we can assume that \( b_i \neq 0 \), since \( b_i = b_j = 0 \) contradicts the assumption. We can assume that \( i = n \). We write
\[
z_n \equiv -b_n^{-1} (b_1 z_1 + \cdots + b_{n-1} z_{n-1} - c) \quad (\text{mod } p)
\]
and then $T_p(a, b, c)$ equals
\[
\sum_{z_1, \ldots, z_{n-1} \pmod{p}} \exp \left( \frac{a_1z_1 + \ldots + a_{n-1}z_{n-1} - a_nb_n^{-1}(b_1z_1 + \ldots + b_{n-1}z_{n-1} - c)}{p} \right) = 
\sum_{z_1, \ldots, z_{n-1} \pmod{p}} \exp \left( \frac{\sum_{1 \leq j \leq n-1}(a_j - a_nb_n^{-1}b_j)z_j + a_nb_n^{-1}c}{p} \right).
\]

As we assumed that for some $j \in [1, n-1]$ we have $a_j - a_nb_n^{-1}b_j \not\equiv 0 \pmod{p}$, it follows that $T_p(a, b, c) = 0$. On the other hand, if $a_i b_j \equiv a_j b_i \pmod{p}$ for every $1 \leq i, j \leq n$ and $i \neq j$, we have trivially $|T_p(a, b, c)| = p^{n-1}$.

Now we conclude that (1.5) is equal to
\[
\sum_{y \in V(F_p)} \exp \left( \frac{h \cdot y}{p^2} \right) T_p(h, \nabla F(y), -F(y)/p)
\]
and this is bounded from above by
\[
p^{n-1} \# \left\{ y \in \mathbb{F}_p^n : F(y) = 0, \text{rank} \left( \frac{h}{\nabla F(y)} \right) < 2 \right\} = p^{n-1} \sum_{y \in W_{F,h}(\mathbb{F}_p)} 1.
\]
If $h \not\in G_{F,j}(\mathbb{F}_p)$, then
\[
\dim(W_{F,h}) \leq j - 1.
\]
By the Lang-Weil theorem, it follows that
\[
\sum_{y \in W_{F,h}(\mathbb{F}_p)} 1 \ll d,n p^{j-1}
\]
and the estimate of the exponential sum $S(h, p^2)$ follows. It remains to deal with the dimensions of the sets $G_{F,j}$.

The following lemma is reminiscent of Heath-Brown’s Lemma 2 in [5], proved using the method of dimension counting via incidence geometry. In [5] he constructs a stratification similar to ours, but for exponential sums modulo $p$. The lemma will help us estimate the dimensions of $G_{F,j}$, which turn out to be affine varieties.

**Lemma 2.1.** Let $F \in K[x_1, \ldots, x_n]$ be a non-singular homogenous polynomial of degree $d$ in $n$ variables defined over a field $K$. For a given $z \in K^n$ let
\[
V_z = \text{sing}(X \cap H_z),
\]
where $X = \{F(x) = 0\} \subset \mathbb{P}_K^{n-1}$ and $H_z = \{z \cdot x = 0\} \subset \mathbb{P}_K^{n-1}$. Let
\[
T_s = \{z = [z] \in \mathbb{P}_K^{n-1} : \dim(V_z) \geq s\}, \quad s \geq -1.
\]
Then $T_s$ is a projective variety of dimension at most $n - 2 - s$.

**Proof.** Consider the variety
\[
I = \left\{ (z, x) \in \mathbb{P}_K^{n-1} \times X : \text{rank} \left( \frac{z}{\nabla F(x)} \right) < 2 \right\}.
\]
The projection \( \pi_2 : I \to X \) is onto, since \( [\nabla F(x)] \) is in the fibre for every \( x \in X \). Since \( X \) is non-singular we have \( \nabla F(x) \neq 0 \) for every \( x \in X \), therefore we have the condition
\[
\text{rank} \left( \frac{z}{\nabla F(x)} \right) = 1,
\]
i.e. each minor in the matrix equals 0. It is easy to see that this implies that any other \( z \in \mathbb{F}^{n-1} \) in the same fibre is such that \( z \) is proportional to \( \nabla F(x) \), i.e. \( [z] = [\nabla F(x)] \). This means that the fibre consists of a single point. Hence \( I \) is irreducible and by the theorem on the dimension of fibres we get
\[
\dim(I) = \dim(\pi_2^{-1}(x)) + \dim(X) = 0 + n - 2 = n - 2.
\]
Let \( U \) be an irreducible component of \( T_s \) and consider the projection
\[
\pi_1 : I \to U.
\]
Then
\[
n - 2 = \dim(I) \geq s + \dim(U),
\]
which yields \( \dim(T_s) \leq n - 2 - s \).

We will also need the following estimate of the dimensions of \( G_{F,j} \).

**Lemma 2.2.** For any homogeneous and non-singular polynomial \( F \) and \( j \geq 0 \) we have
\[
\dim(G_{F,j}(\mathbb{A}_{\mathbb{F}_p}^n)) \leq n - j.
\]

**Proof.** When we regard \( X \) and \( H_z \) over \( \mathbb{A}_{\mathbb{F}_p}^n \) as affine varieties, and respectively the affine singular locus of their intersection \( \text{sing}(X \cap H_z)(\mathbb{A}_{\mathbb{F}_p}^n) = V_2(\mathbb{A}_{\mathbb{F}_p}^n) \), we have \( \dim(V_2(\mathbb{A}_{\mathbb{F}_p}^n)) = \dim(V_2) + 1 \). Thus if \( [z] \in T_s \) for \( s \geq -1 \), we have \( \dim(V_2) \geq s \) and respectively \( \dim(W_{F,z}(\mathbb{A}_{\mathbb{F}_p}^n)) \geq s + 1 \), so any of the corresponding \( z \in \mathbb{F}_p^n \) satisfies \( z \in G_{F,s+1} \). As \( \dim(T_s) \leq n - 2 - s \) and \( T_s \) is exactly \( G_{F,s+1}(\mathbb{F}_p^{n-1}) \), we have \( \dim(G_{F,s+1}) \leq (n - 2 - s) + 1 = n - (s + 1) \). We conclude that for \( j \geq 0 \) we have \( \dim(G_{F,j}(\mathbb{A}_{\mathbb{F}_p}^n)) \leq n - j \).

This completes the proof of Theorem 1.1.

**Acknowledgements.** We are grateful to Prof. Tim Browning for helping with Lemma 2.1. K. Lapkova is supported by a Hertha Firnberg grant [T846-N35] of the Austrian Science Fund (FWF).

**References**

[1] L. Devin, *On the congruence class modulo prime numbers of the number of rational points of a variety*, Int. Math. Res. Not. (14) (2018), 4450–4479

[2] E. Fouvry, *Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums*, Israel J. Math. 120 (2000), part A, 81–96

[3] E. Fouvry, N. Katz, *A general stratification theorem for exponential sums, and applications*, J. reine angew. Math 540 (2001), 115-166.

[4] D. R. Heath-Brown, *A multiple exponential sum to modulus \( p^2 \)*, Canad. Math. Bull. (4) 28 (1985), 394–396.

[5] D. R. Heath-Brown, *The density of rational points on nonsingular hypersurfaces*, Proc. Indian Acad. Sci. Math. Sci. (1) 104 (1994), 1329.
[6] C. Hooley, *On the power free values of polynomials*, Mathematika 14 (1967), 21-26.
[7] C. Hooley, *On the power-free values of polynomials in two variables*, Analytic Number Theory: Essays in Honour of Klaus Roth (2009).
[8] C. Hooley, *On the power-free values of polynomials in two variables II*, Journal of Number Theory 129 (2009), 1443-1455.
[9] K. Lapkova, S. Y. Xiao, *Density of power-free values of polynomials*, Mathematika (4) 65 (2019), 1038-1050.
[10] K. Lapkova, S. Y. Xiao, *Density of power-free values of polynomials II*, Preprint.
[11] P. Michel, review of “A general stratification theorem for exponential sums, and applications” (in J. reine angew. Math 540 (2001), 115-166, by E. Fouvry, N. Katz), Mathematical Reviews/MathSciNet MR1868601.
[12] S. A. Stepanov, *Rational trigonometric sums on “algebraic varieties”*, Mat. Zametki (2) 39 (1986), 161–174, 301.
[13] S. Y. Xiao, *Square-free values of decomposable forms*, Canadian J. of. Math 70 (2018), 1390-1415.
[14] J. Xu, *Stratification for Multiplicative Character Sums*, Int. Math. Res. Not. IMRN, 05 2018.rny096.

**Institute of Analysis and Number Theory, Graz University of Technology, Kopernikusgasse 24/II, 8010 Graz, Austria**

**E-mail address:** lapkova@math.tugraz.at

**Department of Mathematics, University of Toronto, Bahen Centre, 40 St. George St., Room 6290, Toronto, Ontario, Canada M5S 2E4**

**E-mail address:** stanley.xiao@math.toronto.edu