J Geom Anal
DOI 10.1007/s12220-015-9595-5

Averaging Operators Over Homogeneous Varieties Over Finite Fields

Doowon Koh · Chun-Yen Shen · Igor Shparlinski

Received: 21 September 2014

Abstract In this paper we study the mapping properties of the averaging operator over a variety given by a system of homogeneous equations over a finite field. We obtain optimal results on the averaging problems over two-dimensional varieties whose elements are common solutions of diagonal homogeneous equations. The proof is based on a careful study of algebraic and geometric properties of such varieties. In particular, we show that they are not contained in any hyperplane and are complete intersections. We also address partial results on averaging problems over arbitrary dimensional homogeneous varieties which are smooth away from the origin.

Keywords Averaging operator · Finite fields · Homogeneous varieties

Mathematics Subject Classification 43A32 · 11T23 · 43A15

D. Koh
Department of Mathematics, Chungbuk National University, Cheongju, Chungbuk-Do 361-763, Korea
e-mail: koh131@chungbuk.ac.kr

C.-Y. Shen (✉)
Department of Mathematics, National Central University, Chungli 32054, Taiwan
e-mail: chunyshen@gmail.com

I. Shparlinski
Department of Pure Mathematics, University of New South Wales, Sydney, NSW 2052, Australia
e-mail: igor.shparlinski@unsw.edu.au

Published online: 24 February 2015

1 Introduction

1.1 Motivation

Analysis in finite fields is a useful subject because it interacts with other mathematical fields. In addition, the finite field case serves as a typical model for the Euclidean case and possesses structural advantages which enable us to relate our problems to other well-studied problems in number theory, arithmetic combinatorics, or algebraic geometry. For these reasons, problems in Euclidean harmonic analysis have been recently reformulated and studied in the finite field setting. For example, see [3–5,9,15,18,23] and references therein. In this paper we investigate $L^p - L^r$ estimates of averaging operators over algebraic varieties given by a system of homogeneous polynomials in finite fields. For Euclidean averaging problems, we refer readers to [10,16]. However, we notice that the settings of finite fields allows us additional flexibility to formulate and treat these problems over rather general algebraic varieties. In particular, there are no Euclidean analogues of our results.

1.2 Main Definitions and Setup

We begin with notation and definitions for averaging problems in finite fields. Let $\mathbb{F}_q^d$ be a d-dimensional vector space over a finite field $\mathbb{F}_q$ with q elements. Throughout this paper, we assume that the characteristic of $\mathbb{F}_q$ is sufficiently large. We denote by dm the counting measure on the space $\mathbb{F}_q^d$. The pair $(\mathbb{F}_q^d, dm)$ is named as a function space. We now consider a frequency space, denoted by the pair $(\mathbb{F}_{q^*}^d, dx)$, where $\mathbb{F}_{q^*}^d$ and dx denote the dual space of $\mathbb{F}_q^d$ and the normalized counting measure on $\mathbb{F}_{q^*}^d$, respectively. Since $\mathbb{F}_q^d$ is isomorphic to $\mathbb{F}_{q^*}^d$ as an abstract group, we identify $\mathbb{F}_q^d$ with $\mathbb{F}_{q*}^d$. For instance, we write $(\mathbb{F}_q^d, dx)$ for $(\mathbb{F}_{q^*}^d, dx)$. This convention helps us to avoid complicated notation appearing in doing some computations. We shorten both $(\mathbb{F}_q^d, dm)$ and $(\mathbb{F}_q^d, dx)$ as just $\mathbb{F}_q^d$ if there is no risk of confusion between the function space $(\mathbb{F}_q^d, dm)$ and the frequency space $(\mathbb{F}_q^d, dx)$. Let V be an algebraic variety in the frequency space $(\mathbb{F}_q^d, dx)$. We endow V with a normalized surface measure, denoted by $d\sigma$, which can be defined by the relation

$$\int f(x)\, d\sigma(x) = \frac{1}{|V|} \sum_{x \in V} f(x),$$

where $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$ and $|V|$ denotes the cardinality of V. Notice that we can replace $d\sigma(x)$ by $q^d |V|^{-1} V(x) dx$, where $V(x)$ indicates the characteristic function on V. Then the convolution function of f and $d\sigma$ is defined on $(\mathbb{F}_q^d, dx)$:

$$f * d\sigma(y) = \int_{\mathbb{F}_q^d} f(y-x)\, d\sigma(x) = \frac{1}{|V|} \sum_{x \in V} f(y-x).$$

In the finite field setting, the averaging problem is to determine $1 \le p, r \le \infty$ such that

$$\|f * d\sigma\|_{L^r(\mathbb{F}_q^d,dx)} \le C\|f\|_{L^p(\mathbb{F}_q^d,dx)} \quad \text{for all} \quad f : \mathbb{F}_q^d \to \mathbb{C}, \tag{1.1}$$

where $C > 0$ is independent of the function f and the size of the underlying finite field.

Definition 1.1 We use $\mathfrak{P}(p, r)$ to indicate that inequality (1.1) holds.

As an analogue of averaging problems in Euclidean space, this problem has first been addressed by Carbery et al. [3]. They mainly investigated the $L^p - L^r$ estimates of the averaging operator over a k-dimensional variety given by a vector-valued polynomial $P_k : \mathbb{F}_q^k \to \mathbb{F}_q^d$. In particular, Carbery et al. [3] consider a variety $\mathcal{V}_k \subseteq \mathbb{F}_q^d$, $1 \le k \le d-1$, which is given by the range of $P_k : \mathbb{F}_q^k \to \mathbb{F}_q^d$ defined by

$$P_k(t) = \left(t_1, t_2, \ldots, t_k, t_1^2 + t_2^2 + \cdots + t_k^2, \ldots, t_1^{d-k+1} + \cdots + t_k^{d-k+1}\right)$$

for

$$t = (t_1, t_2, \ldots, t_k) \in \mathbb{F}_q^k.$$

Observe that the generalized parabolic variety $\mathcal{V}_k$ can be written by

$$\mathcal{V}_k = \left\{x \in \mathbb{F}_q^d : g_1(x) = g_2(x) = \cdots = g_{d-k}(x) = 0\right\}, \tag{1.2}$$

where $g_j(x) = x_1^{j+1} + x_2^{j+1} + \cdots + x_k^{j+1} - x_{k+j}$ for $j = 1, 2, \ldots, d-k$. Namely, the variety $\mathcal{V}_k$ is exactly the collection of the common solutions of the $d-k$ equations: $g_j(x) = 0$ for $j = 1, 2, \ldots, d-k$. It is clear that $|\mathcal{V}_k| = q^k$ for all $k = 1, 2, \ldots, d-1$, because $x_{k+1}, \ldots, x_d \in \mathbb{F}_q$ are uniquely determined whenever we choose $x_1, x_2, \ldots, x_k \in \mathbb{F}_q$. Applying the Weil Theorem [22], the aforementioned authors [3] have obtained the sharp Fourier decay estimates on the variety $\mathcal{V}_k$ and, as a consequence, they give the complete solution of the averaging problem over the variety $\mathcal{V}_k$. Before we present the result of [3], we need to introduce one more notation:

Definition 1.2 For points $P_1, \ldots, P_s \in \mathbb{R}^2$ of the Euclidean plane, we use $\langle P_1, \ldots, P_s\rangle$ to denote their *convex hull*.

We use Definitions 1.1 and 1.2 to formulate our main results, in which $\mathfrak{P}(p, r)$ is related to belonging the point $(1/p, 1/r)$ to certain convex polygon. We also denote

$$P_{0,0} = (0, 0), \qquad P_{0,1} = (0, 1), \qquad P_{1,1} = (1, 1).$$

For example, it is shown in [3] that for the variety $\mathcal{V}_k$ we have

$$\mathfrak{P}(p, r) \iff \left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, \left(\frac{d}{2d-k}, \frac{d-k}{2d-k}\right)\right\rangle. \tag{1.3}$$

1.3 Goals of This Work

Here we show that bounds of character sums along algebraic varieties can be used to study more complicated varieties than $\mathcal{V}_k$. In particular, instead of the variety $\mathcal{V}_k$ we study the homogeneous variety $\mathcal{H}_k$ defined as

$$\mathcal{H}_k = \left\{x \in \mathbb{F}_q^d : h_1(x) = h_2(x) = \cdots = h_{d-k}(x) = 0\right\}, \tag{1.4}$$

where

$$h_j(x) = x_1^{j+1} + x_2^{j+1} + \cdots + x_k^{j+1} - x_{k+j}^{j+1}, \qquad j = 1, 2, \ldots, d-k,$$

for which the averaging problem becomes much harder.

We note that the variety $\mathcal{H}_k$ is more complicated than $\mathcal{V}_k$ as it does not contain any linear variables. On the other hand $\mathcal{H}_k$ is a homogeneous variety, which allows us to use bounds of characters sums over such varieties that are not known for arbitrary varieties; see [2,19]. It is quite possible that several other varieties can be treated by our method. For example, one can introduce some coefficients in the polynomials $h_j(x)$, of consider a variety defined only some of the polynomials $h_j(x)$, $j = 1, 2, \ldots, d-k$. We avoid such generalization as they complicated the exposition without bringing anything substantially new to our arguments. However many of our auxiliary results are given in more general forms that needed for this work and so are fully ready for such extensions.

There are two main reasons why it is difficult to find sharp $L^p - L^r$ averaging estimates over $\mathcal{H}_k$:

- First, it is not immediately clear how to find the size of $\mathcal{H}_k$.
- Second, the computation of the Fourier decay estimate on $\mathcal{H}_k$ is not easy, in part because it cannot be obtained by simply applying the Weil theorem [22]. Moreover, it may be possible that the Fourier decay on $\mathcal{H}_k$ is slower than that on $\mathcal{V}_k$, because the homogeneous variety $\mathcal{H}_k$ contains lots of lines which could be key factors to make $\mathcal{H}_k$ flat.

These reasons suggest that the $L^p - L^r$ averaging estimates over $\mathcal{V}_k$ maybe be much better than those over $\mathcal{H}_k$. In some cases, it is true but is not always true in the finite field setting. Indeed, we show here that if $k = 2$, then $\mathcal{V}_k$ and $\mathcal{H}_k$ yield the same $L^p - L^r$ averaging estimates. In addition, we conjecture that this also happens for even $k \geq 4$.

To address the above issues, first we establish the absolute irreducibility of $\mathcal{H}_k$. Then we estimate the Fourier decay via bounds of character sums over the homogeneous varieties. Although such bounds are readily available from [2,19], the main difficulty here is to compute the dimension and establish the necessary smoothness condition of $\mathcal{H}_k$ to make sure these bounds apply. These fundamental algebraic-geometric properties of the variety $\mathcal{H}_k$ are established in Propositions 1.9, 1.10 and 1.11.

Besides standard algebraic-geometric methods, we also use several other rather unusual for this area tools such as bound multiplicative character sums with polynomials and a polynomial analogue of the Zsigmondy Theorem of Flatters and Ward [6].

We believe that these results, as well as the methods used in their proofs, are of independent interest and may have several more applications.

As we have mentioned there are no Euclidean analogues of our results. Formulating and solving such averaging problems for Euclidean analogues of the varieties $\mathcal{V}_k, \mathcal{H}_k$ and others, is a very interesting direction of research.

1.4 Conjecture on the Averaging Problem Over $\mathcal{H}_k$

The $L^p - L^r$ averaging estimates over $\mathcal{H}_k$ depend on the maximal dimension of subspaces lying in the variety $\mathcal{H}_k$. Let us denote by $d\sigma_k$ the normalized surface measure on $\mathcal{H}_k$. For a moment, let us assume that $|\mathcal{H}_k| = (1+o(1))q^k$ for $k = 2, 3, \ldots, d-1$, which in fact follows from Proposition 1.10 and Lemma 3.5 below.

We recall that for any real U and V, $U \lesssim V$ or $V \gtrsim U$ means that there exists $C > 0$ independent of q such that $|U| \leq CV$, and $U \asymp V$ is used to indicate that $U \lesssim V$ and $V \lesssim U$. Throughout the paper, the implied constants may depend on degrees and the number of variables of the polynomials defining algebraic varieties under consideration, in particular on the integer parameters d, k, s.

Suppose that the following averaging estimate over $\mathcal{H}_k$ holds true for $1 \leq p, r \leq \infty$:

$$\|f * d\sigma_k\|_{L^r(\mathbb{F}_q^d, dx)} \lesssim \|f\|_{L^p(\mathbb{F}_q^d, dx)} \quad \text{for all} \quad f : \mathbb{F}_q^d \to \mathbb{C}.$$

Testing this inequality with $f = \delta_0$ shows that we must have

$$\frac{d}{p} \leq k + \frac{d-k}{r}.$$

By duality, we conclude that

$$\mathfrak{P}(p, r) \Longrightarrow \left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, \left(\frac{d}{2d-k}, \frac{d-k}{2d-k}\right)\right\rangle, \tag{1.5}$$

where $\delta_0(x) = 1$ if $x = (0, \ldots, 0)$ and $\delta_0(x) = 0$ otherwise. In fact, this necessary condition for $\mathfrak{P}(p, r)$ has been observed by the authors in [3]. In addition, they remarked that if $\mathcal{H}_k$ contains an α-dimensional affine subspace Π_k, then taking f as the characteristic function on Π_k yields a further necessary condition that

$$\frac{1}{r} \geq \frac{1}{p} - \frac{k-\alpha}{d-\alpha}.$$

Notice that this inequality enables us to improve the necessary condition (1.5) only if $\alpha > k/2$. More precisely, if $\alpha \leq k/2$, then the necessary condition for $\mathfrak{P}(p, r)$ can be taken as (1.5). On the other hand, if $\alpha > k/2$, then the necessary condition (1.5) can be improved as

$$\mathfrak{P}(p,r) \Longrightarrow \left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, Q_{d,k,\alpha}, R_{d,k,\alpha}\right\rangle, \tag{1.6}$$

where

$$Q_{d,k,\alpha} = \left(\frac{k^2+\alpha d-2\alpha k}{k(d-\alpha)}, \frac{\alpha(d-k)}{k(d-\alpha)}\right),$$
$$R_{d,k,\alpha} = \left(\frac{d(k-\alpha)}{k(d-\alpha)}, \frac{(d-k)(k-\alpha)}{k(d-\alpha)}\right).$$

Hence, to find a more precise necessary condition for $\mathfrak{P}(p,r)$, we need to observe the maximal dimension α of the affine subspaces Π_k lying in the homogeneous variety $\mathcal{H}_k$. We have the following result.

Lemma 1.3 *Let $\mathcal{H}_k \subseteq \mathbb{F}_q^d$ be defined as in (1.4). Suppose that $k = 2$ or $\max\{d-3, 3\} \leq k \leq d-1$. In addition, assume that $\Pi_k \subseteq \mathcal{H}_k$ is an α-dimensional affine subspace and the characteristic of $\mathbb{F}_q$ is sufficiently large.*

- *If k is even, then $\alpha \leq k/2$.*
- *If k is odd, then $\alpha \leq (k+1)/2$.*

Proof First, we prove that $\alpha \leq k/2$ for even k. By contradiction, let us assume that k is even and $\alpha > k/2$. Since k is even and α is an integer, this implies that $\alpha \geq (k+2)/2$. Without loss of generality, we may assume that $|\Pi_k| = q^\alpha = q^{(k+2)/2}$. Taking $\alpha = (k+2)/2$, it follows from (1.6) that

$$\mathfrak{P}(p,r) \Longrightarrow \left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, Q_{d,k,\alpha}, R_{d,k,\alpha}\right\rangle,$$

where

$$Q_{d,k,\alpha} = \left(\frac{(k+2)d-4k}{k(2d-k-2)}, \frac{(k+2)(d-k)}{k(2d-k-2)}\right),$$
$$R_{d,k,\alpha} = \left(\frac{d(k-2)}{k(2d-k-2)}, \frac{(d-k)(k-2)}{k(2d-k-2)}\right).$$

However, this contradicts Theorem 1.5 for $k = 2$ and Theorem 1.7 for even $k \geq 4$ (see Sect. 1.5 below). To see this, notice that if $k = 2$, then $\mathfrak{P}((2d-2)/d, (2d-2)/(d-2))$ holds by Theorem 1.5 but

$$\left(\frac{d}{2d-2}, \frac{d-2}{2d-2}\right) \notin \left\langle P_{0,0}, P_{0,1}, P_{1,1}, Q_{d,k,\alpha}, R_{d,k,\alpha}\right\rangle.$$

Also observe that if $k \geq 4$, then $\mathfrak{P}((2d-k-1)/(d-1), (2d-k-1)/(d-k))$ follows by Theorem 1.7 but

$$\left(\frac{d-1}{2d-k-1}, \frac{d-k}{2d-k-1}\right) \notin \left\langle P_{0,0}, P_{0,1}, P_{1,1}, Q_{d,k,\alpha}, R_{d,k,\alpha}\right\rangle.$$

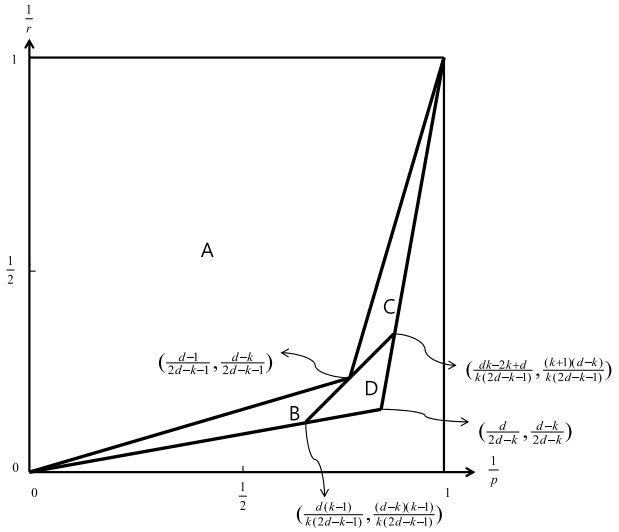

Fig. 1 When $k \geq 2$ is even, $A \cup B \cup C \cup D$ is region of $(1/p, 1/r)$ of Conjecture 1.4. Theorem 1.5 covers the conjectured region for $k = 2$. Furthermore, $A \cup B \cup C$ indicates the conjectured region in the case when $k \geq 3$ is odd and $\mathcal{H}_k$ contains a $(k+1)/2$-dimensional affine subspace. The region A corresponds to the result of Theorem 1.7

By the similar argument, it is not hard to derive that if k is odd, then $\alpha \leq (k+1)/2$. □

Combining Lemma 1.3 with (1.5) and (1.6), we are lead to the following conjecture (see Fig. 1).

Conjecture 1.4 *Let $\mathcal{H}_k \subseteq \mathbb{F}_q^d$ be the homogeneous variety defined as in (1.4). Assume that $k = 2$ or $\max\{d-3, 3\} \leq k \leq d-1$ (we also assume that the characteristic of $\mathbb{F}_q$ is sufficiently large).*

- *If k is even, we have*

$$\mathfrak{P}(p,r) \iff \left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, \left(\frac{d}{2d-k}, \frac{d-k}{2d-k}\right)\right\rangle.$$

- *If k is odd and $\mathcal{H}_k$ contains a $(k+1)/2$-dimensional affine subspace, then*

$$\mathfrak{P}(p,r) \iff \left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, S_{d,k}, T_{d,k}\right\rangle,$$

where

$$S_{d,k} = \left(\frac{dk-2k+d}{k(2d-k-1)}, \frac{(k+1)(d-k)}{k(2d-k-1)}\right),$$
$$T_{d,k} = \left(\frac{d(k-1)}{k(2d-k-1)}, \frac{(d-k)(k-1)}{k(2d-k-1)}\right).$$

When $d \geq 3$ is odd and $k = d-1$, it is observed in [14] that Conjecture 1.4 holds true. In the case when $d \geq 4$ is even and $k = d-1$, Conjecture 1.4 has recently been established in [13]. Namely, the averaging problem over H_{d-1} has been completely solved where $H_{d-1} = \{x \in \mathbb{F}_q^d : x_1^2 + x_2^2 + \cdots + x_{d-1}^2 - x_d^2 = 0\}$ and $-1 \in \mathbb{F}_q$ is a square. However, there are no known results on Conjecture 1.4 for $d - k \geq 2$.

1.5 Statement of Main Results

Our first result below says that Conjecture 1.4 is true for any integer $d \geq 3$ and $k = 2$ (see Fig. 1).

For each $k = 2, 3, \ldots, d-1$, let $d\sigma_k$ be the normalized surface measure on the homogeneous variety $\mathcal{H}_k \subseteq \mathbb{F}_q^d$ given in (1.4).

Theorem 1.5 *If $d \geq 3$ is an integer and $k = 2$, then, assuming that the characteristic of $\mathbb{F}_q$ is sufficiently large,*

$$\mathfrak{P}(p,r) \iff \left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0},\, P_{0,1},\, P_{1,1},\, \left(\frac{d}{2d-2}, \frac{d-2}{2d-2}\right)\right\rangle.$$

Remark 1.6 As mentioned before, this statement has only been known in [14] for $d = 3$ and $k = 2$. Notice from Theorem 1.5 that the optimal averaging result for the homogeneous variety $\mathcal{H}_2$ is exactly the same as that in (1.3) for the general parabolic variety $\mathcal{V}_2$ defined in (1.2).

Let $\mathbb{A}^d$ be the affine d-space $\overline{\mathbb{F}}_q^d$, where $\overline{\mathbb{F}}_q$ denotes the algebraic closure of the finite filed $\mathbb{F}_q$ with q elements.

For each $k = 2, 3, \ldots, d-1$, let us consider the algebraic variety

$$\overline{\mathcal{H}}_k = \left\{x \in \mathbb{A}^d : h_1(x) = h_2(x) = \cdots = h_{d-k}(x) = 0\right\},$$

where h_j, $j = 1, \ldots, d-k$, are the homogeneous polynomials defined as in (1.4). One interesting point is that the smoothness of $\overline{\mathcal{H}}_k$ depends on the dimension d of $\mathbb{A}^d$. Indeed, we see from Proposition 1.11 below that the variety $\overline{\mathcal{H}}_k$ is smooth away from the origin if and only if $d - k = 1, 2, 3$. In the case when $\overline{\mathcal{H}}_k$ for $k \geq 3$ is smooth away from the origin, we are able to obtain certain $L^p - L^r$ averaging estimates on $\mathcal{H}_k$ (see Fig. 1).

Next, we state our averaging results over $\mathcal{H}_k$ for $k \geq 3$.

Theorem 1.7 *If $\max\{d-3, 3\} \leq k \leq d-1$, then, assuming that the characteristic of $\mathbb{F}_q$ is sufficiently large,*

$$\left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0},\, P_{0,1},\, P_{1,1},\, \left(\frac{d-1}{2d-k-1}, \frac{d-k}{2d-k-1}\right)\right\rangle \Longrightarrow \mathfrak{P}(p,r).$$

Remark 1.8 The result of Theorem 1.7 is far from the conjectured averaging result, but if $\mathcal{H}_k$ would contain a $(k+1)/2$-dimensional affine subspace, it gives a sharp $L^p - L^r$ estimate for $p = (2d-k-1)/(d-1)$.

Our work has been mainly motivated by the character sum estimates on abstractly given homogeneous varieties due to authors in [19]. To prove our main results, we first derive a useful result about averaging on general homogeneous varieties with abstract algebraic structures. Then our main results follow by applying it to our variety $\mathcal{H}_k$. To do this, we make the following three key observations on $\mathcal{H}_k \subseteq \mathbb{F}_q^d$ for $k = 2, 3, \ldots, d-1$.

Proposition 1.9 *Suppose that the characteristic of $\mathbb{F}_q$ is sufficiently large. Then, for every $k = 2, \ldots, d-1$, the algebraic variety $\overline{\mathcal{H}_k} \subseteq \mathbb{A}^d$ is not contained in any hyperplane in $\mathbb{A}^d$.*

Proposition 1.10 *Suppose that the characteristic of $\mathbb{F}_q$ is sufficiently large. Then for every $k = 2, \ldots, d-1$, the algebraic variety $\overline{\mathcal{H}_k} \subseteq \mathbb{A}^d$ is absolutely irreducible and* $\dim \overline{\mathcal{H}_k} = k$.

That is, Propositions 1.9 and 1.10 assert that $\mathcal{H}_k$ is a complete intersection.

Proposition 1.11 *Suppose that the characteristic of $\mathbb{F}_q$ is sufficiently large. Then for every $k = 2, \ldots, d-1$, the algebraic variety $\overline{\mathcal{H}_k} \subseteq \mathbb{A}^d$ is smooth away from the origin if and only if $d - k = 1, 2, 3$.*

Furthermore, we note that the smoothness condition on $\mathcal{H}_2 \subseteq \mathbb{F}_q^d$ is not necessary in completing the proof of Theorem 1.5. Therefore, the conclusion of Theorem 1.5 holds true for any d and $k = 2$, and Conjecture 1.4 for $k = 2$ is established. On the contrary, we use the smooth condition on $\mathcal{H}_k \subseteq \mathbb{F}_q^d$ for $k \geq 3$ in proving Theorem 1.7. Thus, by Proposition 1.11, the conditions that $d - k = 1, 2, 3$ and $k \geq 3$ are imposed to the statement of Theorem 1.7.

1.6 Overview of this Paper

In the remaining parts of this paper, we concentrate on proving Theorems 1.5 and 1.7 which are our main results. Instead of proving directly main theorems, we derive them by means of working on more general homogeneous varieties with specific geometric structures.

To this end, in Sect. 2 we collect facts about the multiplicative character sums and the existence of a primitive prime divisor of a family of shifted monomials. In particular, we make use of a polynomial analogue of the Zsigmondy theorem which is due to Flatters and Ward [6].

Section 3 is devoted to setting up notation and basic concepts essential in defining abstract varieties in algebraic geometry.

In Sect. 4, we derive a result for averaging problems over general homogeneous varieties, where we adapt the standard analysis technique in [3] together with the results on character sums in [19]; see Lemma 4.2 below. In fact, this result generalizes our main results related to $\mathcal{H}_k$.

In Sect. 5, we show that Lemma 4.2 applies to the variety $\mathcal{H}_k$ and complete the proofs of our main results, that is, Theorems 1.5 and 1.7.

We note that our main tool are bounds of character sums along algebraic varieties, which we interpret as results about the decay of Fourier coefficients.

2 Multiplicative Character Sums and Roots of Some Polynomials

2.1 Root of Shifted Monomials

We need the following simple observation, which immediately follows from the Taylor formula (which applies if the characteristic is large enough).

Lemma 2.1 *For any fixed integer $s \geq 1$, if the characteristic of $\mathbb{F}_q$ is sufficiently large then for any $a \in \mathbb{F}_q^*$, the polynomial $t^s + a \in \mathbb{F}_q[t]$ has no multiple roots.*

Lemma 2.2 *For any fixed integer $s \geq 1$, if the characteristic of $\mathbb{F}_q$ is sufficiently large then the polynomial $t^s + 1 \in \mathbb{F}_q[t]$ has at least one root which is not a root of the polynomials $t^j + 1 \in \mathbb{F}_q[t]$, $j = 1, \ldots, s-1$.*

Proof By a result of Flatters and Ward [6, Theorem 2.6], if the characteristic of $\mathbb{F}_q$ is large enough then $t^{2s} - 1$ has an irreducible factor $q(t) \in \mathbb{F}_q[t]$ that does not divide any of the polynomials $t^j - 1 \in \mathbb{F}_q[t]$, $j = 1, \ldots, 2s-1$. In particular, $q(t)$ is relatively prime with $t^s - 1$ and thus is a divisor of

$$t^s + 1 = \frac{t^{2s} - 1}{t^s - 1}.$$

Furthermore, $q(t)$ is relatively prime to

$$t^j + 1 = \frac{t^{2j} - 1}{t^j - 1}, \qquad j = 1, \ldots, s-1,$$

which concludes the proof. □

2.2 Multiplicative Character Sums with Polynomials

We also need the following result due to Wan [21, Corollary 2.3] that follows almost instantly from the Weil bound in the form given in [11, Theorem 11.23].

Lemma 2.3 *Let $g_1(t), \ldots, g_s(t)$ be s monic pairwise prime polynomials in $\mathbb{F}_q[t]$. Denote by $\chi_1, \ldots, \chi_s$ nontrivial multiplicative characters of $\mathbb{F}_q$ with order $d_1, \ldots, d_s$, respectively. If for some $i = 1, 2, \ldots, s$, the polynomial $g_i(t)$ is not of the form $q(t)^{d_i}$ with $q(t) \in \mathbb{F}_q[t]$, then we have*

$$\left| \sum_{t \in \mathbb{F}_q} \chi_1(g_1(t)) \cdots \chi_s(g_s(t)) \right| \lesssim q^{\frac{1}{2}}.$$

Lemma 2.4 *For any fixed integer $s \geq 1$, if the characteristic of $\mathbb{F}_q$ is sufficiently large, then for any multiplicative characters χ_j, $j = 1, 2, \ldots, s$, among which at least one is nontrivial, we have*

$$\left| \sum_{t \in \mathbb{F}_q} \prod_{j=1}^{s} \chi_j(t^{j+1} + 1) \right| \lesssim q^{\frac{1}{2}}.$$

Proof After ignoring all trivial characters, it suffices to prove that for some positive integer $m \leq s$, we have

$$\left| \sum_{t \in \mathbb{F}_q} \widetilde{\chi}_1(t^{s_1+1}+1) \cdots \widetilde{\chi}_m(t^{s_m+1}+1) \right| \lesssim q^{\frac{1}{2}}, \tag{2.1}$$

where $1 \leq s_1 < s_2 < \cdots < s_m \leq s$ and $\tilde{\chi}_1, \ldots, \tilde{\chi}_m$ denote nontrivial multiplicative characters of $\mathbb{F}_q$. Factoring the polynomials $t^{s_i+1}+1$, $i = 1, \ldots, m$, into irreducible factors over $\mathbb{F}_q$ and using the multiplicativity, we see from Lemma 2.1 that

$$\sum_{t \in \mathbb{F}_q} \widetilde{\chi}_1(t^{s_1+1}+1) \cdots \widetilde{\chi}_m(t^{s_m+1}+1) = \sum_{t \in \mathbb{F}_q} \eta_1(q_1(t)) \cdots \eta_u(q_u(t))$$

for some multiplicative characters η_i and monic pairwise prime polynomials q_i, $i = 1, 2, \ldots, u$.

Furthermore, by Lemma 2.2 we have $\eta_{i_0} = \widetilde{\chi}_{i_0}$ for at least one $i_0 \in \{1, \ldots, u\}$, and thus η_{i_0} is a nontrivial character. Now using Lemma 2.3 we complete the proof. □

3 Algebraic Properties of General Homogeneous Varieties

3.1 Preliminaries

In this section, we review known facts on general varieties generated by a system of $s-$homogeneous polynomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_d]$. We begin by setting up notation.

Let $2 \leq s \leq d-1$ be an integer. Assume we are given $s-$homogeneous polynomials in d variables over $\mathbb{F}_q$ of degree at least two each, which we write as

$$f_j(x) \in \mathbb{F}_q[x_1, x_2, \ldots, x_d], \quad \deg f_j \geq 2, \qquad j = 1, \ldots, s,$$

where $x = (x_1, x_2, \ldots, x_d)$. Now, define the closed algebraic set

$$\overline{H}_{\mathbb{A}} = \left\{ x \in \mathbb{A}^d \ : \ f_1(x) = f_2(x) = \cdots = f_s(x) = 0 \right\}. \tag{3.1}$$

Let $H_{\mathbb{A}}$ be the collection of points in $\overline{H}_{\mathbb{A}}$ with coordinates in $\mathbb{F}_q$:

$$H_{\mathbb{A}} = \left\{ x \in \mathbb{F}_q^d \ : \ f_1(x) = f_2(x) = \cdots = f_s(x) = 0 \right\}. \tag{3.2}$$

We also use the standard notation $\mathbb{P}^{d-1}$ for the $(d-1)$-dimensional projective space over $\overline{\mathbb{F}}_q$, which can be considered as the collection of all one-dimensional subspaces of the vector space $\mathbb{A}^d$. For $P = [a_1 : a_2 : \cdots : a_d] \in \mathbb{P}^{d-1}$ and a polynomial $f \in \overline{\mathbb{F}}_q[x_1, \ldots, x_d]$, recall that $f(P) = 0$ means that $f(\lambda a_1, \ldots, \lambda a_d) = 0$ for all $\lambda \neq 0$. Like the algebraic subset $\overline{H}_{\mathbb{A}}$ of the affine space $\mathbb{A}^d$, we define the projective algebraic set

$$\overline{H}_{\mathbb{P}} = \{P \in \mathbb{P}^{d-1} \ : \ f_1(P) = f_2(P) = \cdots = f_s(P) = 0\}.$$

Let us recall an affine cone over a projective subset in $\mathbb{P}^{d-1}$. Denote by $\pi : \mathbb{A}^d \backslash \{(0, \ldots, 0)\} \to \mathbb{P}^{d-1}$ the projection map defined by

$$\pi(x_1, \ldots, x_d) = [x_1 : \cdots : x_d].$$

Then the affine cone over $Y \subseteq \mathbb{P}^{d-1}$ is defined by

$$C(Y) = \pi^{-1}(Y) \cup \{(0, \ldots, 0)\} \subseteq \mathbb{A}^d.$$

Notice that $\overline{H}_{\mathbb{A}}$ is the affine cone over the projective variety $\overline{H}_{\mathbb{P}}$.

Definition 3.1 We say that a homogeneous variety $H_{\mathbb{A}} \subseteq \mathbb{F}_q^d$ defined as in (3.2) is a **complete intersection** if the following two conditions hold:

- $\overline{H}_{\mathbb{A}} \subseteq \mathbb{A}^d$ is an affine cone over a projective variety $\overline{H}_{\mathbb{P}}$ which is not contained in a hyperplane,
- $\overline{H}_{\mathbb{A}}$ is an absolutely irreducible variety of dimension $d-s$ (or $\dim \overline{H}_{\mathbb{P}} = d-1-s$).

Definition 3.2 We say that a homogeneous variety $H_{\mathbb{A}} \subseteq \mathbb{F}_q^d$ defined as in (3.2) is **smooth** if $\overline{H}_{\mathbb{A}}$ is smooth away from the origin.

3.2 Character Sums and Fourier Coefficients

It has been observed in [19] that if $H_{\mathbb{A}}$ is a smooth homogeneous variety, which is a complete intersection, then $\overline{H}_{\mathbb{A}} \cap \overline{\Pi}(m)$ can have at most isolated singularities in $\mathbb{P}^{d-1}$ where

$$\overline{\Pi}(m) = \left\{x \in \mathbb{A}^d : m \cdot x = 0\right\}$$

for $m \neq (0, \ldots, 0)$, where $m \cdot x$ denotes the inner products of the vectors m and x.

In turn, based on this observation, the following bound of character sum over $H_{\mathbb{A}}$ in given in [19, Theorem 1].

Lemma 3.3 *Let $H_{\mathbb{A}} \subseteq \mathbb{F}_q^d$ be defined as in (3.2). Suppose that $H_{\mathbb{A}}$ is a* **smooth** *homogeneous variety, which is a complete intersection, and the characteristic of $\mathbb{F}_q$ is sufficiently large. Then we have for all $m \in \mathbb{F}_q^d \backslash \{(0, \ldots, 0)\}$*

$$\left| \sum_{x \in H_{\mathbb{A}}} \psi(m \cdot x) \right| \lesssim \begin{cases} q^{(d-s+1)/2} & \text{if } d-s \geq 3, \\ q & \text{if } d-s = 2, \end{cases}$$

where ψ denotes a nontrivial additive character of $\mathbb{F}_q$.

Here, we point out that the proof of Lemma 3.3 for $d-s = 2$ is given in [19] without using the smoothness assumption on $H_{\mathbb{A}}$. Therefore, the smoothness condition on $H_{\mathbb{A}}$ can be relaxed for $d - s = 2$. Indeed, the following bound follows immediately from a result of Cochrane [2, Theorem 4.3.5].

Lemma 3.4 *If $H_{\mathbb{A}} \subseteq \mathbb{F}_q^d$ is a homogeneous variety which is a complete intersection given by (3.2) of dimension* $\dim \overline{H}_{\mathbb{A}} = d - s$, *where $\overline{H}_{\mathbb{A}}$ is given by (3.1), then*

$$\left| \sum_{x \in H_{\mathbb{A}}} \psi(m \cdot x) \right| \lesssim q^{d-s-1}$$

for all $m \in \mathbb{F}_q^d \backslash \{(0, \ldots, 0)\}$.

The following estimate on the cardinality of $H_{\mathbb{A}}$ due to Chatzidakis, van den Dries and Macintyre [1, Proposition 3.3] gives an extension of the result of Lang and Weil [17].

Lemma 3.5 *Suppose that $\overline{V} \subseteq \mathbb{A}^d$ is an algebraic variety with v absolutely irreducible components and of dimension e defined by polynomials over $\mathbb{F}_q$ and let $V = \{x \in \overline{V} \cap \mathbb{F}_q^d\}$. Then*

$$|V| - vq^e \lesssim q^{e-1/2}.$$

It is clear from Lemma 3.5 that $|H_{\mathbb{A}}| = (1 + o(1))q^{d-s}$ if $H_{\mathbb{A}}$ is a homogeneous variety, given by (3.2) which is a complete intersection in $\mathbb{F}_q^d$.

Now, we endow a homogeneous variety $H_{\mathbb{A}}$ with the normalized surface measure $d\sigma_H$. Recall that if $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$, then

$$\int f(x)\, d\sigma_H(x) = \frac{1}{|H_{\mathbb{A}}|} \sum_{x \in H_{\mathbb{A}}} f(x).$$

The following decay estimates of the Fourier coefficients

$$(d\sigma_H)^\vee(m) = \frac{1}{|H_{\mathbb{A}}|} \sum_{x \in H_{\mathbb{A}}} \psi(m \cdot x), \qquad m \in \mathbb{F}_q^d,$$

on $H_{\mathbb{A}}$ follow immediately from Lemmas 3.4 and 3.3.

Lemma 3.6 *Let $d\sigma_H$ be the normalized surface measure on the homogeneous variety $H_{\mathbb{A}} \subseteq \mathbb{F}_q^d$ given by (3.2), which is a complete intersection. If the characteristic of $\mathbb{F}_q$ is sufficiently large, then:*

(i) *If $d - s = 2$, then we have*

$$|(d\sigma_H)^\vee(m)| \lesssim q^{-1}$$

for all $m \in \mathbb{F}_q^d \backslash \{(0, \ldots, 0)\}$.

(ii) *If $H_{\mathbb{A}}$ is smooth and $d - s \geq 3$, then*

$$|(d\sigma_H)^\vee(m)| \lesssim q^{-(d-s-1)/2}$$

for all $m \in \mathbb{F}_q^d \backslash \{(0, \ldots, 0)\}$.

4 Fourier Coefficients and $L^p - L^r$ Averaging Estimates over $H_{\mathbb{A}}$

4.1 Estimates for Varieties with Given Rate of Decay of Fourier Coefficients

First we need the following general result which can be obtained by adapting the arguments in [3]. For the sake of completeness, we provide the proof in full detail.

Lemma 4.1 *Let $d\sigma_H$ be the normalized surface measure on an affine homogeneous variety $H_{\mathbb{A}} \subseteq \mathbb{F}_q^d$ given by (3.2), which is a complete intersection. If $(d\sigma)^\vee(m) \lesssim q^{-\vartheta/2}$ for all $m \in \mathbb{F}_q^d \backslash \{(0, \dots, 0)\}$ and for some fixed $\vartheta > 0$, then $\mathfrak{P}(p, r)$ holds with*

$$p = \frac{2s + \vartheta}{s + \vartheta} \quad \text{and} \quad r = \frac{2s + \vartheta}{s}.$$

Proof We must show that

$$\|f * d\sigma_H\|_{L^r(\mathbb{F}_q^d, dx)} \lesssim \|f\|_{L^p(\mathbb{F}_q^d, dx)}$$

for all function $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$ with the above values of p and r.

Define a function K on $(\mathbb{F}_q^d, dm)$ by $K = (d\sigma_H)^\vee - \delta_0$. Observe that $d\sigma_H(x) = \widehat{K}(x) + \widehat{\delta_0}(x) = \widehat{K}(x) + 1$ for $x \in (\mathbb{F}_q^d, dx)$, where for a function F on $(\mathbb{F}_q^d, dm)$ we define

$$\widehat{F}(x) = \sum_{m \in \mathbb{F}_q^d} F(m)\psi(-m \cdot x).$$

and, as before, $m \cdot x$ denotes the inner products of m and x. Since $\vartheta > 0$ and dx is the normalized counting measure on $\mathbb{F}_q^d$, it follows from Young's inequality (see [8,12]) that

$$\|f * 1\|_{L^r(\mathbb{F}_q^d, dx)} \lesssim \|f\|_{L^p(\mathbb{F}_q^d, dx)}.$$

Thus, it suffices to prove that

$$\|f * \widehat{K}\|_{L^r(\mathbb{F}_q^d, dx)} \lesssim \|f\|_{L^p(\mathbb{F}_q^d, dx)} \tag{4.1}$$

for all functions $f : (\mathbb{F}_q^d, dx) \to \mathbb{C}$.

Notice that (4.1) can be obtained by interpolating

$$\|f * \widehat{K}\|_{L^2(\mathbb{F}_q^d, dx)} \lesssim q^{-\vartheta/2}\|f\|_{L^2(\mathbb{F}_q^d, dx)} \tag{4.2}$$

and

$$\|f * \widehat{K}\|_{L^\infty(\mathbb{F}_q^d, dx)} \lesssim q^s\|f\|_{L^1(\mathbb{F}_q^d, dx)}. \tag{4.3}$$

It remains to prove (4.2) and (4.3). By the definition of K and the assumption that $(d\sigma_H)^\vee(m) \lesssim q^{-\vartheta/2}$ for $m \neq (0, \dots, 0)$, we see that

$$\max_{m\in\mathbb{F}_q^d} |K(m)| \lesssim q^{-\vartheta/2}.$$

Therefore, (4.2) follows by applying the Plancherel theorem (see [8,12]):

$$\begin{aligned}\|f * \widehat{K}\|_{L^2(\mathbb{F}_q^d,dx)} &= \|f^\vee K\|_{L^2(\mathbb{F}_q^d,dm)}\\ &\lesssim q^{-\vartheta/2}\|f^\vee\|_{L^2(\mathbb{F}_q^d,dm)} = q^{-\vartheta/2}\|f\|_{L^2(\mathbb{F}_q^d,dx)}.\end{aligned}$$

To prove (4.3), notice that $|H_{\mathbb{A}}| = (1+o(1))q^{d-s}$, because $H_{\mathbb{A}}$ is a complete intersection. From Young's inequality and the observation that $\|\widehat{K}\|_{L^\infty(\mathbb{F}_q^d,dx)} \lesssim q^s$, we obtain (4.3):

$$\|f * \widehat{K}\|_{L^\infty(\mathbb{F}_q^d,dx)} \le \|\widehat{K}\|_{L^\infty(\mathbb{F}_q^d,dx)}\|f\|_{L^1(\mathbb{F}_q^d,dx)} \lesssim q^s\|f\|_{L^1(\mathbb{F}_q^d,dx)}.$$

Thus, the proof of Lemma 4.1 is complete. □

4.2 Main Estimates

As a direct application of the Fourier decay estimates in Lemma 3.6, we can now derive averaging results related to general homogeneous variety $H_{\mathbb{A}}$, which is a complete intersection. Applying Lemma 4.1 with Lemma 3.6 yields the result below.

Lemma 4.2 *Let $d\sigma_H$ be the normalized surface measure on a homogeneous variety $H_{\mathbb{A}} \subseteq \mathbb{F}_q^d$, given by (3.2), which is a complete intersection. If the characteristic of $\mathbb{F}_q$ is sufficiently large, then:*

(i) *If $d-s=2$, then*

$$\mathfrak{P}(p,r) \iff \left(\frac{1}{p},\frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, \left(\frac{d}{2d-2},\frac{d-2}{2d-2}\right)\right\rangle.$$

(ii) *If $H_{\mathbb{A}}$ is a smooth and $d-s\ge 3$, then*

$$\left(\frac{1}{p},\frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, \left(\frac{d-1}{d+s-1},\frac{s}{d+s-1}\right)\right\rangle \Longrightarrow \mathfrak{P}(p,r).$$

Proof To prove (i), let us assume that $d-s=2$. Then $|H_{\mathbb{A}}| = (1+o(1))q^{d-s} = q^2$, because $H_{\mathbb{A}}$ is a complete intersection. Now, suppose that $\mathfrak{P}(p,r)$. In particular, we see that

$$q^{-(d+2r-2)/r} \asymp \|\delta_0 * d\sigma_H\|_{L^r(\mathbb{F}_q^d,dx)} \lesssim \|\delta_0\|_{L^p(\mathbb{F}_q^d,dx)} = q^{-d/p}.$$

It therefore follows that

$$\frac{-d-2r+2}{r} \le \frac{-d}{p}.$$

By duality, we also have

$$\frac{-d-2p^*+2}{p^*} \leq \frac{-d}{r^*},$$

where

$$p^* = \frac{p}{p-1} \quad \text{and} \quad r^* = \frac{r}{r-1}$$

denote the Hölder conjugates of p and r, respectively. In conclusion,

$$\left(\frac{1}{p}, \frac{1}{r}\right) \in \left\langle P_{0,0}, P_{0,1}, P_{1,1}, \left(\frac{d}{2d-2}, \frac{d-2}{2d-2}\right)\right\rangle. \tag{4.4}$$

Conversely, we now assume that the inclusion (4.4) holds. If $1 \leq r \leq p \leq \infty$, then it is clear that $\mathfrak{P}(p,r)$, because both $d\sigma_H$ and $(\mathbb{F}_q^d, dx)$ have total mass 1. By the interpolation theorem, it therefore suffices to prove that

$$\mathfrak{P}\left(\frac{2d-2}{d}, \frac{2d-2}{d-2}\right)$$

holds. Since $d - s = 2$, applying Lemma 4.1 with Lemma 3.6 (i) yields the above property, and the proof of Lemma 4.2 (i) is complete.

In order to prove (ii), it is enough to show that

$$\mathfrak{P}\left(\frac{d+s-1}{d-1}, \frac{d+s-1}{s}\right)$$

holds. However, this follows immediately by using Lemma 4.1 together with Lemma 3.6 (ii). □

Remark 4.3 Even if Lemma 4.2 provides us of powerful averaging results on general homogeneous varieties, applying it in practice may not be simple, because it contains certain abstract hypotheses.

5 Proofs of Main Results

5.1 Preliminaries

In this section, we complete the proofs of Theorems 1.5 and 1.7 which are considered as main theorems in this paper. We complete the proofs by showing that Lemma 4.2 is a general version of both Theorems 1.5 and 1.7. To do this, we begin by recalling from (1.4) that for each $k = 2, 3, \ldots, d-1$, our homogeneous variety $\mathcal{H}_k$ is exactly the common solutions in $\mathbb{F}_q^d$ of a system of the $(d-k)$ equations

$$\begin{aligned} h_1(x) &= x_1^2 + x_2^2 + \cdots + x_k^2 - x_{k+1}^2 = 0, \\ &\vdots \\ h_j(x) &= x_1^{j+1} + x_2^{j+1} + \cdots + x_k^{j+1} - x_{k+j}^{j+1} = 0, \\ &\vdots \\ h_{d-k}(x) &= x_1^{d-k+1} + x_2^{d-k+1} + \cdots + x_k^{d-k+1} - x_d^{d-k+1} = 0, \end{aligned} \quad , \tag{5.1}$$

where $j = 1, 2, \ldots, (d-k)$. Let $s = d - k$ which is the number of homogeneous equations h_j defining $\mathcal{H}_k$. Then it is clear that $\overline{\mathcal{H}_k}$ is an affine cone over its corresponding projective variety determined by s-homogeneous polynomials h_j. Thus, if we are able to show that the conclusions of Propositions 1.9 and 1.10 hold for $k = 2$ then Theorem 1.5 follows from Lemma 4.2 (i). Furthermore, if all Propositions 1.9–1.11 hold true for $k \geq 3$, then Theorem 1.7 follows from Lemma 4.2 (ii) where the smoothness condition on $\overline{\mathcal{H}_k}$ is essential. In summary, to prove both Theorems 1.5 and 1.7, it suffices to justify Propositions 1.9–1.11. In the following subsections, we give the complete proofs of Propositions 1.9–1.11.

5.2 Proof of Proposition 1.9

Since any hyperplane in $\mathbb{A}^d$ is a subspace with dimension $d-1$, it suffices to prove that there exists d linearly independent points $\{P_1, P_2, \ldots, P_d\} \subseteq \overline{\mathcal{H}_k}$. Now fix $k = 2, 3, \ldots, (d-1)$. For each $j = 1, 2, \ldots, d-k$, choose a $\beta_{k+j} \in \mathbb{A}$ such that $\beta_{k+j}^{j+1} = 1$ and $\beta_{k+j} \neq 1$. Since $\mathbb{A}$ is an algebraic closure and the characteristic of $\mathbb{F}_q$ is sufficiently large, the β_{k+j} always exists. Denote by $I_{k\times k}$ the $k \times k$ identity matrix. We also define $1_{k\times(d-k)}$ as the $k \times (d-k)$ matrix whose all entries are 1. Also define the following $(d-k) \times k$ matrix $C_{(d-k)\times k}$ and the $(d-k) \times (d-k)$ matrix $D_{(d-k)\times(d-k)}$:

$$C_{(d-k)\times k} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix},$$

$$D_{(d-k)\times(d-k)} = \begin{bmatrix} \beta_{k+1} & 1 & \cdots & 1 & 1 \\ 1 & \beta_{k+2} & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \cdots & 1 & \beta_{d-1} & 1 \\ 1 & 1 & \cdots & 1 & \beta_d \end{bmatrix}.$$

Now consider the $d \times d$ matrix $M_{d\times d}$ defined by

$$M_{d\times d} = \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_d \end{bmatrix} = \begin{bmatrix} I_{k\times k} & 1_{k\times(d-k)} \\ C_{(d-k)\times k} & D_{(d-k)\times(d-k)} \end{bmatrix}.$$

Note that all $P_1, P_2, \ldots, P_d$ are solutions of a system of equations (5.1). Hence, it follows that $\{P_1, P_2, \ldots, P_d\} \subseteq \overline{\mathcal{H}}_k$ for any $k = 2, 3, \ldots, (d-1)$. Moreover, since $\beta_{k+j} - 1 \neq 0$ for all $j = 1, 2, \ldots, d-k$, it follows from simple Gauss elimination that the rank of the matrix $M_{d\times d}$ is exactly d, which completes the proof of Proposition 1.9.

5.3 Proof of Proposition 1.10

Recall from (5.1) that $\overline{\mathcal{H}}_k \subseteq \mathbb{A}^d$ is given by a system of $(d-k)$ homogeneous equations. For each $j = 1, 2, \ldots, d-k$, define an algebraic set

$$\overline{\mathcal{H}}_k^j = \left\{x \in \mathbb{A}^d \ : \ h_j(x) = 0\right\},$$

where h_j is defined by (5.1). By the definition of $\overline{\mathcal{H}}_k$, it follows that

$$\overline{\mathcal{H}}_k = \bigcap_{j=1}^{d-k} \overline{\mathcal{H}}_k^j. \tag{5.2}$$

We need the following claim.

Lemma 5.1 *For each $n \in \{1, 2, \ldots, (d-k-1)\}$, we have*

$$\left(\bigcap_{j=1}^{n} \overline{\mathcal{H}}_k^j\right) \bigcap \overline{\mathcal{H}}_k^{n+1} \neq \emptyset$$

and there exists $\alpha \in \mathbb{A}^d$ such that

$$\alpha \in \bigcap_{j=1}^{n} \overline{\mathcal{H}}_k^j \quad \text{and} \quad \alpha \notin \overline{\mathcal{H}}_k^{n+1}.$$

Proof The first part is trivial. For the second part of this claim, fix $n \in \{1, 2, \ldots, (d-k-1)\}$ and let $l \in \overline{\mathbb{F}}_q$ with $l^{n+2} \neq 1$. Now, choose an $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathbb{A}^d$ whose coordinates satisfy that

$$\alpha_j = \begin{cases} 0 & \text{if } \ j = 2, 3, \ldots, k, \\ l & \text{if } \ j = k+n+1, \\ 1 & \text{otherwise.} \end{cases}$$

Then it is straightforward to check that $\alpha \in \bigcap_{j=1}^{n} \overline{\mathcal{H}}_k^j$ and $\alpha \notin \overline{\mathcal{H}}_k^{n+1}$ and the result follows. □

To compute the dimension of $\overline{\mathcal{H}}_k$, we apply the following result; see [7, p. 55] for a proof.

Lemma 5.2 *Let $\overline{V} \subseteq \mathbb{A}^d$ be an irreducible algebraic set, and let $f \in \overline{\mathbb{F}}_q[x_1, x_2, \ldots, x_d]$ be a nonconstant polynomial which does not vanish identically on $\overline{V}$. In addition, let us define $\mathbb{Z}(f) = \{x \in \mathbb{A}^d \ : \ f(x) = 0\}$. If $\overline{V} \cap \mathbb{Z}(f) \neq \emptyset$, then we have*

$$\dim(\overline{V} \cap \mathbb{Z}(f)) = \dim \overline{V} - 1.$$

We are ready to prove Proposition 1.10. It is not hard to see that $\overline{\mathcal{H}}_k^1$, $k = 2, 3, \ldots, d-1$, is absolutely irreducible, because it is the same as the absolute irreducibility of the polynomial

$$F(x_1, x_2, \ldots, x_{k+1}) = x_1^2 + x_2^2 + \cdots + x_k^2 - x_{k+1}^2.$$

Assume $F = RH$. Clearly, we see $deg_{x_1} R = deg_{x_1} H = 1$. Write

$$R = \big(x_1 + g(x_2, \ldots, x_{k+1})\big)\big(x_1 + h(x_2, \ldots, x_{k+1})\big).$$

We see that we should have $g = -h$ and so $x_2^2 + \cdots + x_k^2 - x_{k+1}^2 = -g^2$, which is easy to rule out for $k \geq 2$ (for example, by specializing $x_3 = \cdots = x_k = 0, x_{k+1} = 1$).

Since $\overline{\mathcal{H}}_k^1$, $k = 2, 3, \ldots, d-1$, is absolutely irreducible, it follows from the Affine Jacobian criterion that $\dim \overline{\mathcal{H}}_k^1 = d - 1$ (see Lemma 5.4 below). Notice that this completes the proof of Proposition 1.10 in the case when $k = d-1$ with $k \geq 2$. Thus, we may assume that $d - k \geq 2$. Observe by induction that Proposition 1.10 is a direct result from the following statement.

Lemma 5.3 *Assume that the characteristic of $\mathbb{F}_q$ is sufficiently large. Let $n \in \{1, 2, \ldots, (d-k-1)\}$ with $k = 2, 3, \ldots, d-2$. Suppose that $\bigcap_{j=1}^{n} \overline{\mathcal{H}}_k^j$ is absolutely irreducible with dimension $d - n$. Then $\bigcap_{j=1}^{n+1} \overline{\mathcal{H}}_k^j$ is also absolutely irreducible with dimension $d - n - 1$.*

Proof From Lemmas 5.1 and 5.2, it is clear that

$$\dim \bigcap_{j=1}^{n+1} \overline{\mathcal{H}}_k^j = d - n - 1. \tag{5.3}$$

Thus, it remains to prove that $\bigcap_{j=1}^{n+1} \overline{\mathcal{H}}_k^j$ is absolutely irreducible. Assume that $\bigcap_{j=1}^{n+1} \overline{\mathcal{H}}_k^j$ has ν absolutely irreducible components in $\overline{\mathbb{F}}_q$. By (5.3) and Lemma 3.5 to show that $\nu = 1$, it is enough to prove that

$$N(k, n) = \left| \bigcap_{j=1}^{n+1} \mathcal{H}_k^j \right| = (1 + o(1))q^{d-n-1}, \tag{5.4}$$

where $\mathcal{H}_k^j = \left\{x \in \mathbb{F}_q^d : x_1^{j+1} + \cdots + x_k^{j+1} - x_{k+j}^{j+1} = 0\right\}$. Notice that $N(k,n)$ is the number of common solutions in $\mathbb{F}_q^d$ of the following equations

$$\begin{aligned} x_1^2 + x_2^2 + \cdots + x_k^2 - x_{k+1}^2 &= 0, \\ &\vdots \\ x_1^{j+1} + x_2^{j+1} + \cdots + x_k^{j+1} - x_{k+j}^{j+1} &= 0, \\ &\vdots \\ x_1^{n+2} + x_2^{n+2} + \cdots + x_k^{n+2} - x_{k+n+1}^{n+2} &= 0. \end{aligned}$$

For each $j = 1, 2, \ldots, n+1$, define

$$N_j(x_1, x_2, \ldots, x_k) = \left|\left\{x_{k+j} \in \mathbb{F}_q : x_{k+j}^{j+1} = x_1^{j+1} + \cdots + x_k^{j+1}\right\}\right|.$$

Since $x_{k+n+2}, \ldots, x_d \in \mathbb{F}_q$ are free variables and $x_{k+1}, \ldots, x_{k+n+1} \in \mathbb{F}_q$ depend only on $x_1, \ldots, x_k$, we can write

$$N(k,n) = \sum_{x_1,\ldots,x_k \in \mathbb{F}_q} \left(\prod_{j=1}^{n+1} N_j(x_1, \ldots, x_k)\right) q^{d-k-n-1}.$$

In order to prove (5.4), it therefore suffices to show that

$$\sum_{x_1,\ldots,x_k \in \mathbb{F}_q} \left(\prod_{j=1}^{n+1} N_j(x_1, \ldots, x_k)\right) = (1 + o(1))q^k. \tag{5.5}$$

For each $j = 1, 2, \ldots, n+1$, let $d_j = \gcd(j+1, q-1)$ and denote by χ_j the multiplicative character of order d_j. Then, from the orthogonality of multiplicative characters it follows that

$$N_j(x_1, \ldots, x_k) = \sum_{i_j=0}^{d_j-1} \chi_j^{i_j}\left(x_1^{j+1} + \cdots + x_k^{j+1}\right);$$

see [11, Sect. 3.1]. Hence, the left hand side of (5.5) is written by

$$\begin{aligned} &\sum_{x_1,\ldots,x_k \in \mathbb{F}_q} \left(\prod_{j=1}^{n+1} N_j(x_1, \ldots, x_k)\right) \\ &\quad = \sum_{i_1=0}^{d_1-1} \cdots \sum_{i_{n+1}=0}^{d_{n+1}-1} \sum_{x_1,\ldots,x_k \in \mathbb{F}_q} \prod_{j=1}^{n+1} \chi_j^{i_j}\left(x_1^{j+1} + \cdots + x_k^{j+1}\right). \end{aligned}$$

When $(i_1, \dots i_{n+1}) = (0, \dots, 0)$, the sum over $x_1, \dots, x_k$ is q^k, where we use the usual convention that $\chi_0(0) = 1$ for the trivial multiplicative character χ_0. Thus, to establish (5.5), it is enough to prove that for each $(i_1, \dots, i_{n+1}) \neq (0, \dots, 0)$ with $i_j = 0, 1, \dots, d_j - 1$,

$$\sum_{x_2,\dots,x_k \in \mathbb{F}_q} \left| \sum_{x_1 \in \mathbb{F}_q} \chi_1^{i_1}\left(x_1^2 + \cdots + x_k^2\right) \cdots \chi_{n+1}^{i_{n+1}}\left(x_1^{n+2} + \cdots + x_k^{n+2}\right) \right| = o(q^k).$$

Now, we define the sets $B, G \subseteq \mathbb{F}_q^{k-1}$ (of "bad" and "good" vectors $(x_2, \dots, x_k) \in \mathbb{F}_q^{k-1}$) by

$$B = \Big\{ (x_2, \dots, x_k) \in \mathbb{F}_q^{k-1} \ : \\ x_2^{j+1} + \cdots + x_k^{j+1} = 0 \quad \text{for some} \quad j = 1, 2, \dots, n+1 \Big\},$$

and

$$G = \mathbb{F}_q^{k-1} \backslash B.$$

For each fixed $\overline{x} = (x_2, \dots, x_k) \in G$, define

$$A_j(\overline{x}) = x_2^{j+1} + \cdots + x_k^{j+1} \quad \text{for} \quad j = 1, 2, \dots, n+1.$$

Note that $A_j(\overline{x}) \neq 0$ for $\overline{x} \in G$ and all $j = 1, 2, \dots, n+1$.

Since $|B| \leq (n+1)(n+2)q^{k-2}$, it suffices to prove that for each $(i_1, \dots, i_{n+1}) \neq (0, \dots, 0)$ with $i_j = 0, 1, \dots, d_j - 1$,

$$\sum_{\overline{x}=(x_2,\dots,x_k)\in G} \left| \sum_{x_1 \in \mathbb{F}_q} \prod_{j=1}^{n+1} \chi_j^{i_j}\left(x_1^{j+1} + A_j(\overline{x})\right) \right| \\ = \sum_{\overline{x}=(x_2,\dots,x_k)\in G} \left| \sum_{t \in \mathbb{F}_q} \prod_{j=1}^{n+1} \chi_j^{i_j}\left(t^{j+1} + A_j(\overline{x})\right) \right| = o(q^k). \tag{5.6}$$

From the definition of χ_j and the fact that $(i_1, \dots, i_{n+1}) \neq (0, \dots, 0)$, notice that $\chi_j^{i_j}$ is a nontrivial character for some $j = 1, \dots, n+1$. If $\chi_j^{i_j}$ is a trivial character, then the term $\chi_j^{i_j}\left(t^{j+1} + A_j(\overline{x})\right)$ can be replaced by 1. Thus, it suffices to prove (5.6) under the assumption that all $\chi_j^{i_j}$ are not-trivial characters.

We now consider the cases $k = 2$ and $k \geq 3$ separately.

- If $k = 2$, we must show that

$$\sum_{a\in G}\left|\sum_{t\in\mathbb{F}_q}\prod_{j=1}^{n+1}\chi_j^{i_j}(t^{j+1}+a^{j+1})\right| = o(q^2),$$

for all $(i_1,\dots,i_{n+1}) \neq (0,\dots,0)$ with $i_j = 0, 1, \dots, d_j - 1$. Recall that if $a \in G$, then $a \neq 0$, thus

$$\left|\sum_{t\in\mathbb{F}_q}\prod_{j=1}^{n+1}\chi_j^{i_j}(t^{j+1}+a^{j+1})\right| = \left|\sum_{t\in\mathbb{F}_q}\prod_{j=1}^{n+1}\chi_j^{i_j}(t^{j+1}+1)\right|$$

and recalling Lemma 2.4 we obtain the desired estimate.

- If $k \geq 3$, then it is easy to show that if the characteristic of $\mathbb{F}_q$ is sufficiently large, then for all but $O(q^{k-2})$ choices of $\overline{x} = (x_2,\dots,x_k) \in G$, the polynomials

$$t^{j+1} + A_j(\overline{x}) \in \mathbb{F}_q[t], \qquad j = 1,\dots,n+1$$

have no pairwise common roots. Indeed, assume $k \geq 3$. Let $i_1, i_2 \in \{2, 3, \dots, n+2\}$ with $i_1 \neq i_2$. Notice that if $t^{i_1} - A$ and $t^{i_2} - B$ have a common root then $A^{i_2} = B^{i_1}$. For our expressions for A and B in $x_2,\dots,x_k$ (assuming that $k \geq 3$) one can easily show that this leads to a nontrivial equation and thus has $O(q^{k-2})$ solutions. For such $(x_2,\dots,x_k) \in G$, the inner sum over $t \in \mathbb{F}_q$ in (5.6) is trivially estimated as q, and for the remaining choices of $(x_2,\dots,x_k) \in G$, we apply Lemmas 2.1 and 2.3 to estimate the inner sum over $t \in \mathbb{F}_q$ in (5.6). In conclusion, the left hand side of (5.6) is bounded by $O(q^{k-1/2})$.

This establishes (5.6) for every $k \geq 2$ and concludes the proof. □

As we have mentioned, Lemma 5.3 implies Proposition 1.10.

5.4 Proof of Proposition 1.11

The proof is based on the Affine Jacobian criterion below (see [7, Prop. 4.4.8]).

Lemma 5.4 *Let $\overline{V} \subseteq \mathbb{A}^d$ be an irreducible algebraic set given by a system of s-polynomial equations $g_j(x) = 0$, $j = 1, 2, \dots, s$. Suppose that $v \in \overline{V}$. Then $\overline{V}$ is smooth at v if and only if the rank of the $s \times d$ Jacobian matrix satisfies*

$$\operatorname{rank}\left[\frac{\partial g_j}{\partial x_i}(v)\right]_{s\times d} \geq d - \dim \overline{V}.$$

Now, since $d - k$ is the number of the polynomials h_j in (5.1) defining $\overline{\mathcal{H}}_k$ which is absolutely irreducible with dimension k by Proposition 1.10, we see from Lemma 5.4

that $\overline{\mathcal{H}}_k$ is smooth away from the origin if and only if

$$\operatorname{rank}\left[\frac{\partial h_j}{\partial x_i}(x)\right]_{(d-k)\times d} = d-k$$

for all $x \in \overline{\mathcal{H}}_k \backslash \{(0,\dots,0)\}$. Since we have assumed that the characteristic of $\mathbb{F}_q$ is sufficiently large, it is clear from the Gauss elimination that

$$\operatorname{rank}\left[\frac{\partial h_j}{\partial x_i}(x)\right]_{(d-k)\times d} = \operatorname{rank} J_{k,d}(x),$$

where $J_{k,d}(x)$ denotes the $(d-k)\times d$ matrix given by the concatenation

$$J_{k,d}(x) = [W_{k,d}(x) \,\|\, D_{k,d}(x)]$$

of the Wandermonde

$$W_{k,d}(x) = \left[x_i^j\right]_{(d-k)\times k},$$

and the diagonal matrix

$$D_{k,d}(x) = \begin{bmatrix} -x_{k+1} & 0 & 0\cdots & 0 \\ 0 & -x_{k+2}^2 & 0\cdots & 0 \\ \vdots & \vdots & \vdots\ \vdots & \vdots \\ 0 & 0 & 0\ \ 0 & -x_d^{d-k} \end{bmatrix}.$$

In order to complete the proof of Proposition 1.11, it therefore suffices to prove the following two statements:

(A1) if $d-k \geq 4$ and $k \geq 2$, then there exists $x \in \overline{\mathcal{H}}_k \backslash \{(0,\dots,0)\}$ with $\operatorname{rank} J_{k,d}(x) < d-k$;
(A2) if $d-k = 1,2,3$ and $k \geq 2$, then $\operatorname{rank} J_{k,d}(x) = d-k$ for all $x \in \overline{\mathcal{H}}_k \backslash \{(0,\dots,0)\}$.

First, let us prove (A1). Suppose that $k \geq 2$ is an even integer. For each $l = 1,2,\dots,d-k$, choose an $\alpha_l \in \overline{\mathbb{F}}_q$ with $\alpha_l^{l+1} = k \cdot 1$, and define

$$x_{k+l} = \begin{cases} 0 & \text{for } l \geq 2 \text{ even}, \\ \alpha_l & \text{for } l \geq 1 \text{ odd}. \end{cases}$$

Letting $x = (1,-1,\dots,1,-1,x_{k+1},\dots,x_d)$, it is easy to check that $x \in \overline{\mathcal{H}}_k \backslash \{(0,\dots,0)\}$. Since $d-k \geq 4$, the matrix $J_{k,d}(x)$ has at least four rows, and its second row and fourth row are exactly same. Thus, the rank of $J_{k,d}(x)$ must be less

than $d-k$. Next, assume that $k \geq 3$ is an odd integer. For each $l = 1, 2, \ldots, d-k$, select a $\beta_l \in \overline{\mathbb{F}}_q$ with $\beta_l^{l+1} = (k-1) \cdot 1$, and define

$$x_{k+l} = \begin{cases} 0 & \text{for } l \geq 0 \text{ even}, \\ \beta_l & \text{for } l \geq 1 \text{ odd}. \end{cases}$$

Taking $x = (1, -1, \ldots, 1, -1, 0, x_{k+1}, \ldots, x_d)$, we also see that $x \in \overline{\mathcal{H}}_k \backslash \{(0, \ldots, 0)\}$, and the second row and the fourth row of $J_{k,d}(x)$ are same. Thus, the rank of $J_{k,d}(x)$ is less than $d-k$, which completes the proof of the statement (A1).

Now, we prove the statement (A2). If $d-k=1$ and $k \geq 2$, then (A2) is clearly true, because

$$J_{k,d}(x) = \begin{bmatrix} x_1 & x_2 & \cdots & x_{d-1} & -x_d \end{bmatrix} \neq \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

for $x \neq (0, \ldots, 0)$. Assume that $d-k=2$ and $k \geq 2$. We must show that

$$\operatorname{rank} J_{k,d}(x) = \operatorname{rank} \begin{bmatrix} x_1 & x_2 & \cdots & x_{d-2} & -x_{d-1} & 0 \\ x_1^2 & x_2^2 & \cdots & x_{d-2}^2 & 0 & -x_d^2 \end{bmatrix} = 2$$

for all $x \in \overline{\mathcal{H}}_k \backslash \{(0, \ldots, 0)\}$, where

$$\overline{\mathcal{H}}_k = \left\{ x \in \mathbb{A}^d \ : \ x_1^2 + \cdots + x_{d-2}^2 - x_{d-1}^2 = x_1^3 + \cdots + x_{d-2}^3 - x_d^3 = 0 \right\}.$$

Notice that if $x = (x_1, \ldots, x_d) \in \overline{\mathcal{H}}_k \backslash \{(0, \ldots, 0)\}$, then $x_j \neq 0$ for some $j = 1, 2, \ldots, d-2$. Without loss of generality, we therefore assume that $x_1 \neq 0$. Letting $u_j = x_j / x_1$ for $j = 2, 3, \ldots, d$, it is enough to show that

$$\operatorname{rank} \begin{bmatrix} 1 & u_2 & \cdots & u_{d-2} & -u_{d-1} & 0 \\ 1 & u_2^2 & \cdots & u_{d-2}^2 & 0 & -u_d^2 \end{bmatrix} = 2, \tag{5.7}$$

where $(u_2, u_3, \ldots, u_d) \in \mathbb{A}^{d-1}$ satisfies

$$\begin{cases} 1 + u_2^2 + \cdots + u_{d-2}^2 - u_{d-1}^2 = 0 \\ 1 + u_2^3 + \cdots + u_{d-2}^3 - u_d^3 = 0 \end{cases}. \tag{5.8}$$

Notice that if $u_{d-1}, u_d \neq 0$, then (5.7) holds, because

$$\operatorname{rank} \begin{bmatrix} -u_{d-1} & 0 \\ 0 & -u_d^2 \end{bmatrix} = 2.$$

If $u_j = 0$ or 1 for all $j = 2, 3, \ldots, d-2$, then we see from (5.8) that $u_{d-1}, u_d \neq 0$ and so there is nothing to prove. On the other hand, if $u_j \neq 0, 1$ for some $j = 2, 3, \ldots, (d-2)$ then

$$\det \begin{bmatrix} 1 & u_j \\ 1 & u_j^2 \end{bmatrix} = u_j(u_j - 1) \neq 0 \quad \text{or} \quad \operatorname{rank} \begin{bmatrix} 1 & u_j \\ 1 & u_j^2 \end{bmatrix} = 2.$$

Thus (5.7) is also true and we completes the proof of the statement (A2) in the case when $d-k=2$ and $k\geq 2$. Finally let us prove the statement (A2) when $d-k=3$ and $k\geq 2$. Following the previous arguments, our task is to show that

$$\operatorname{rank}\begin{bmatrix} 1 & u_2 & \cdots & u_{d-3} & -u_{d-2} & 0 & 0 \\ 1 & u_2^2 & \cdots & u_{d-3}^2 & 0 & -u_{d-1}^2 & 0 \\ 1 & u_2^3 & \cdots & u_{d-3}^3 & 0 & 0 & -u_d^3 \end{bmatrix} = 3, \tag{5.9}$$

where $(u_2, u_3, \ldots, u_d) \in \mathbb{A}^{d-1}$ satisfies

$$\begin{cases} 1+u_2^2+\cdots+u_{d-3}^2-u_{d-2}^2=0, \\ 1+u_2^3+\cdots+u_{d-3}^3-u_{d-1}^3=0, \\ 1+u_2^4+\cdots+u_{d-3}^4-u_d^4=0. \end{cases} \tag{5.10}$$

Case 1: Suppose that $u_j = 0$ or 1 for all $j = 2, 3, \ldots, d-3$. Then it follows from (5.10) that $u_{d-2}, u_{d-1}, u_d \neq 0$, which implies that

$$\det\begin{bmatrix} -u_{d-2} & 0 & 0 \\ 0 & -u_{d-1}^2 & 0 \\ 0 & 0 & -u_d^3 \end{bmatrix} \neq 0$$

hence

$$\operatorname{rank}\begin{bmatrix} -u_{d-2} & 0 & 0 \\ 0 & u_{d-1}^2 & 0 \\ 0 & 0 & -u_d^3 \end{bmatrix} = 3.$$

Thus (5.9) also follows.

Case 2: Suppose that $u_i, u_j \neq 0, 1$ with $u_i \neq u_j$ for some $i, j = 2, 3, \ldots, d-3$. Then it follows that

$$\det\begin{bmatrix} 1 & u_i & u_j \\ 1 & u_i^2 & u_j^2 \\ 1 & u_i^3 & u_j^3 \end{bmatrix} = u_i u_j (u_i-1)(u_j-1)(u_j-u_i) \neq 0.$$

Thus

$$\operatorname{rank}\begin{bmatrix} 1 & u_i & u_j \\ 1 & u_i^2 & u_j^2 \\ 1 & u_i^3 & u_j^3 \end{bmatrix} = 3,$$

which implies (5.9).

Case 3: Suppose that $u_j \neq 0, 1$ for some $j = 2, 3, \ldots, d-3$, and $u_i = u_j$ if $u_i \neq 0, 1$ for $i = 2, 3, \ldots, d-3$. Let

$$a = |\{l \in \{2, 3, \ldots, d-3\} \ : \ u_l = 1\}|,$$
$$b = |\{l \in \{2, 3, \ldots, d-3\} \ : \ u_l \neq 0, 1\}|.$$

Then $a \geq 0$ and $b \geq 1$ are integers. Thus (5.10) is same as

$$\begin{aligned} (1+a)1 + bu_j^2 - u_{d-2}^2 &= 0, \\ (1+a)1 + bu_j^3 - u_{d-1}^3 &= 0, \\ (1+a)1 + bu_j^4 - u_d^4 \quad &= 0, \end{aligned} \tag{5.11}$$

where $(1+a) \in \mathbb{N}$.

We now claim that either $u_{d-2} \neq 0$ or $u_d \neq 0$. To see this, assume that $u_{d-2}, u_d = 0$. Then from (5.11) we see that $(1+a)1 + bu_j^2 = 0 = (1+a)1 + bu_j^4$. This implies that $bu_j^2(u_j - 1)(u_j + 1) = 0$. Thus we conclude that $u_j = -1$, because $u_j \neq 0, 1$ and $b \in \{1, \ldots, d-4\}$ (assuming that the characteristic of $\mathbb{F}_q$ is sufficiently large). However, since $(1+a)1 + b(-1)^2 = (1+a+b)1 \neq 0$, it is impossible that $u_j = -1$ (again assuming that the characteristic of $\mathbb{F}_q$ is sufficiently large) and the claim is justified.

If $u_{d-2} \neq 0$, then (5.9) follows by the observation that

$$\det \begin{bmatrix} 1 & u_j & -u_{d-2} \\ 1 & u_j^2 & 0 \\ 1 & u_j^3 & 0 \end{bmatrix} = -u_{d-2}u_j^2(u_j - 1) \neq 0.$$

On the other hand, if $u_d \neq 0$, then (5.9) also follows by the observation that

$$\det \begin{bmatrix} 1 & u_j & 0 \\ 1 & u_j^2 & 0 \\ 1 & u_j^3 & -u_d^3 \end{bmatrix} = -u_d^3 u_j(u_j - 1) \neq 0.$$

By Case 1, Case 2 and Case 3, we establish the statement (A2) in the case when $d - k = 3$ and $k \geq 2$. This concludes the proof of Proposition 1.11.

Acknowledgments The authors are grateful to Anthony Flatters and Tom Ward for useful discussions and in particular for the idea of the proof of Lemma 2.2. Doowon Koh was supported by the Research Grant of Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (2012R1A1A1001510). Chun-Yen Shen was supported by the NSC, through Grant NSC102-2115-M-008-015-MY2. Igor Shparlinski was supported by the Research Grant of the Australian Research Council (DP130100237).

References

1. Chatzidakis, Z., van den Dries, L., Macintyre, A.: Definable sets over finite fields. J. Reine Angew. Math. **427**, 107–135 (1992)

2. Cochrane, T.: Exponential Sums and the Distribution of Solutions of Congruences. Institute of Mathematics, Academia Sinica, Taipei (1994)
3. Carbery, A., Stones, B., Wright, J.: Averages in vector spaces over finite fields. Math. Proc. Camb. Philos. Soc. **144**, 13–27 (2008)
4. Dvir, Z.: On the size of Kakeya sets in finite fields. J. Am. Math. Soc. **22**, 1093–1097 (2009)
5. Ellenberg, J.S., Oberlin, R., Tao, T.: The Kakeya set and maximal conjectures for algebraic varieties over finite fields. Mathematika **56**, 1–25 (2012)
6. Flatters, A., Ward, T.: A polynomial Zsigmondy theorem. J. Algebra **343**, 138–142 (2011)
7. Gathmann, A.: Algebraic Geometry. Lecture Notes, University of Kaiserslautern, 2002/2003, available at http://www.mathematik.uni-kl.de/~gathmann/class/alggeom-2002/main
8. Green, B.J.: Restriction and Kakeya phenomena. Lecture Notes, University of Cambridge (2003), available at https://www.dpmms.cam.ac.uk/~bjg23/rkp.html
9. Iosevich, A., Koh, D.: Extension theorems for paraboloids in the finite field setting. Math. Z. **266**, 471–487 (2010)
10. Iosevich, A., Sawyer, E.: Sharp $L^p - L^r$ estimates for a class of averaging operators. Ann. Inst. Fourier Grenoble **46**, 1359–1384 (1996)
11. Iwaniec, H., Kowalski, E.: Analytic Number Theory, vol. 53. Colloquium Publications, Providence (2004)
12. Jones, F.: Lebesgue Integration on Euclidean Space, Revise Ed. Jones and Bartlett, Sudbury (2001)
13. Koh, D.: Averaging operators over nondegenerate quadratic surfaces in finite fields. Forum Math., to appear
14. Koh, D., Shen, C.: Extension and averaging operators for finite fields. Proc. Edinb. Math. Soc. **56**, 599–614 (2013)
15. Lewko, A., Lewko, M.: Endpoint restriction estimates for the paraboloid over finite fields. Proc. Am. Math. Soc. **140**, 2013–2028 (2012)
16. Littman, W.: $L^p - L^q$ estimates for singular integral operators. Proc. Symp. Pure Math. **23**, 479–481 (1973)
17. Lang, S., Weil, A.: Number of points on varieties in finite fields. Am. J. Math. **76**, 819–827 (1954)
18. Mockenhaupt, G., Tao, T.: Restriction and Kakeya phenomena for finite fields. Duke Math. J. **121**, 35–74 (2004)
19. Shparlinski, I.E., Skorobogatov, A.N.: Exponential sums and rational points on complete intersections. Mathematika **37**, 201–208 (1990)
20. Stein, E.M.: Harmonic Analysis. Princeton University Press, Princeton (1993)
21. Wan, D.: Generators and irreducible polynomials over finite fields. Math. Comput. **66**, 1195–1212 (1997)
22. Weil, A.: On some exponential sums. Proc. Natl. Acad. Sci. USA **34**, 204–207 (1948)
23. Wolff, T.: Recent work connected with the Kakeya problem, Prospects in Mathematics (Princeton, NJ, 1996), pp. 129–162. American Mathematical Society, Providence (1999)