Abstract. We introduce a new approach and obtain new results for the problem of studying polynomial images of affine subspaces of finite fields. We improve and generalise several previously known results, and also extend the range of such results to polynomials of degrees higher than the characteristic of the field. Our approach is based on estimates for a certain new type of exponential sums. The results we obtain have a wide scope of applications similar to those associated with their counterparts studying consecutive intervals over prime fields instead of affine subspaces. Here we give only two immediate consequences: to bounding the size of the intersection of orbits of polynomial dynamical systems with affine subspaces and to the Waring problem over affine subspaces.

1 Introduction

Motivation. Given a polynomial $f$ over a field $F$ and two “interesting” finite sets $A, B \subseteq F$, it is natural to ask about the size of the intersection

$$f(A) \cap B = \{ f(a) : a \in A \text{ and } f(a) \in B \}$$

and possible improvements of the trivial bound $\min\{\#A, \#B\}$ on the size of this intersection. In particular, for the case of prime finite fields $F_p$ of $p$ elements with $A, B$ chosen as intervals of consecutive elements (in a natural ordering of elements of $F_p$), a series of such results have been obtained in $[7, 8, 9]$, where also a broad variety of applications have been given. For example, one motivating application for these results comes from the study of the number of points in polynomial orbits that fall in a given interval; see $[5, 6, 9, 18]$.

Here we mostly concentrate on the case of finite fields that are high degree extensions of prime fields. Furthermore, our sets $A, B$ are affine subspaces, which are the natural analogues of intervals in these settings.

More precisely, for a prime power $q$ and an integer $r > 1$ we denote by $K = F_q$ and $L = F_{q^r}$ the finite fields of $q$ and $q^r$ elements, respectively, and consider
affine subspaces of $\mathbb{L}$ over $\mathbb{K}$. We are especially interested in the case when the dimension $s$ of these spaces is small compared to $r$ and thus standard approaches via algebraic geometry methods (such as the Weil bound) do not apply.

We note that a similar point of view has recently been adopted by Cilleruelo and Shparlinski [10] and by Roche-Newton and Shparlinski [22], who obtained several results in this direction. In fact, the results and method of [10] apply only to a very special class of affine spaces, while [22] uses methods of additive combinatorics to address the case of arbitrary affine spaces. Here, using a different approach, we improve some of the results of [22] and also obtain a series of other results. In particular, we obtain some nontrivial results for a class of polynomials of degree $d \geq p$, where $p$ is the characteristic of $\mathbb{L}$, while for the inductive method of [22] the condition $d < p$ seems to be unavoidable.

Our approach appeals to the recent bounds of Bourgain and Glibichuk [4] of multilinear exponential sums in arbitrary finite fields, which we couple with the classical van der Corput differencing. We use this combination to estimate exponential sums with polynomials of degree $d$ along affine spaces.

We remark that under some natural conditions the dimension $s$ of these spaces can be as low as $r/d$ by the order of magnitude. This corresponds exactly to the lowest possible length of intervals over $\mathbb{F}_p$ for which one can estimate nontrivially the corresponding exponential sums via Vinogradov’s method; see the recent striking results of Wooley [26, 27, 28].

As in the previous works in this direction, we also give some applications of our results. Namely, we study the intersection of orbits of polynomial dynamical systems and affine spaces and improve and complement some results of Roche-Newton and Shparlinski [22]; both are analogues of those of [5, 6, 9, 18]. We also recall that this question was introduced by Silverman and Viray [23] in characteristic zero and then studied using a very different technique. Finally, we also give estimates for certain exponential sums over consecutive integers and consider the Waring problem in subspaces.

We now outline in more detail our main results, which are given in Theorems 9, 15, 19 and 21 below.

**Exponential sums over affine subspaces and polynomial values in affine subspaces.** Our first motivation is to estimate the number of elements $u$ in an affine subspace $\mathcal{A}$ of $\mathbb{L}$, that is, a translate of a linear subspace of $\mathbb{L}$, such that $f(u)$ falls also in an affine subspace $\mathcal{B}$ of $\mathbb{L}$. We denote this number by $I_f(\mathcal{A}, \mathcal{B})$, that is, for a nonlinear polynomial $f \in \mathbb{L}[X]$,

$$I_f(\mathcal{A}, \mathcal{B}) = \#\{u \in \mathcal{A} \mid f(u) \in \mathcal{B}\}. \quad (1)$$
Our basic tool in obtaining estimates for \( J_f(A, B) \) is a recent estimate of Bourgain and Glibichuk [4, Theorem 4] on multilinear exponential sums over subsets of \( \mathbb{L} \); see Lemma 7 below. To enable an application of this result, we apply the classical van der Corput differencing method for our exponential sum to reduce the degree of the polynomial \( f \); see also [3, Theorem C]. However, this method was applied so far only with polynomials of degree less than \( p \).

Let \( \psi \) be an additive character of \( \mathbb{L} \) and \( \chi : \mathbb{L} \to \mathbb{C} \) a function satisfying \( \chi(x + y) = \chi(x)\chi(y) \), \( x, y \in \mathbb{L} \). The first main result of this paper is obtaining, under certain conditions, estimates for exponential sums over affine subspaces \( A \) of \( \mathbb{L} \) of the type

\[
\sum_{x \in A} \chi(x)\psi(f(x)).
\]

What is new about this result is that it applies to several classes of polynomials of degree larger than \( p \) (see Theorem 9), in contrast to previous results that apply only to polynomials of degree less than \( p \).

To estimate \( J_f(A, B) \), we first use the classical Weil bound to estimate exponential sums, but the bound we obtain is nontrivial only for \( s > r(1/2 + \varepsilon) \), for some \( \varepsilon > 0 \), and it also applies only for polynomials of degree coprime to \( p \). However, applying Theorem 9 we obtain nontrivial estimates for any \( s \geq \varepsilon r \), and moreover for more general polynomials of degree larger than or equal to \( p \); see Theorem 15.

The bound of Theorem 15 improves the very recent estimate (19) obtained in [22] for \( s < 2.5(\tfrac{5}{4})^d \varepsilon r \). Moreover, Theorem 15 generalises the result of [22], which holds only for polynomials of degree \( d < p \).

We also conclude from Theorem 15 that, under certain conditions, \( f(A) \) is not included in any proper affine subspace \( B \) of \( \mathbb{L} \); see Corollary 16.

**Polynomial orbits in affine subspaces.** Given a polynomial \( f \in \mathbb{L}[X] \) and an element \( u \in \mathbb{L} \), we define the orbit

\[
(2) \quad \text{Orb}_f(u) = \{ f^{(n)}(u) : n = 0, 1, \ldots \},
\]

where \( f^{(n)} \) is the \( n \)th iterate of \( f \), that is,

\[
f^{(0)} = X, \quad f^{(n)} = f(f^{(n-1)}), \quad n \geq 1.
\]

As the orbit (2) is a subset of \( \mathbb{L} \), and thus a finite set, we denote by \( T_{f,u} = \# \text{Orb}_f(u) \) the size of the orbit.

Here we study the frequency of orbit elements that fall in an affine subspace of \( \mathbb{L} \) considered as a linear vector space over \( \mathbb{K} \). This question is motivated by a recent work of Silverman and Viray [23] (in characteristic zero and using a very
different technique). Recently, several results have been obtained in [22] using additive combinatorics. Here we improve on several results of [22] and we also extend the class of polynomials to which these results apply; see Corollary 17.

We also note that the argument of the proof of [22, Theorem 6] can give information about the frequency of (not necessarily consecutive) iterates falling in a subspace. We present such a result in Theorem 19, as well as apply it to obtain information about intersection of orbits of linearised polynomials in Corollary 20.

**Exponential sums over consecutive integers and the Waring problem.**

For a positive integer $n \leq p^r - 1$, we consider the $p$-adic representation
\[ n = n_0 + n_1 p + \cdots + n_{s-1} p^{s-1} \]
for some $s \leq r$. Let $q = p$, $1 \leq N \leq p^r - 1$ and let $f \in \mathbb{L}[X]$ be a polynomial of degree $d$. Furthermore, let $\psi$ be an additive character of $\mathbb{L}$ and let $\chi : \mathbb{N} \to \mathbb{C}$ be a $p$-multiplicative function; see Section 6 for a definition.

Using Theorem 9 under certain conditions, we give a bound on the twisted exponential sums of the form
\[ S(N) = \sum_{n \leq N} \chi(n) \psi(f(\xi_n)), \]
where $\omega_0, \ldots, \omega_{r-1}$ is a basis of $\mathbb{L}$ over $\mathbb{F}_p$ and
\[ \xi_n = \sum_{i=0}^{s-1} n_i \omega_i, \]
which we hope to be of independent interest. We present such a result in Theorem 21 using the class of $p$-multiplicative functions
\[ \chi(n) = \exp \left( 2\pi i \sum_{j=0}^{s-1} \alpha_j n_j \right), \]
where $\alpha_j$, $j = 0, 1, \ldots$, is a fixed infinite sequence of real numbers.

Let $f \in \mathbb{L}[X]$ be a polynomial of degree $d$. As another direct consequence of Theorem 9 we prove the existence of a positive integer $k$ such that for any $y \in \mathbb{L}$, the equation
\[ f(\xi_{n_1}) + \cdots + f(\xi_{n_k}) = y \]
is solvable in positive integers $n_1, \ldots, n_k \leq N$. We do this first for the case $N = p^r - 1$ in Theorem 23 and conclude then Corollary 24 for the case $p^{s-1} \leq N < p^s$. 

Recently, quite substantial progress has been achieved in the classical Waring problem in finite fields; see [11, 12, 13, 25].

We conclude the paper with some remarks and possible extensions of our results, as well as some connections to constructing affine dispersers.

2 Consecutive differences of polynomials

For our main results we need a few auxiliary results regarding consecutive differences of polynomials. For a polynomial \( f \in \mathbb{L}[X] \) of degree \( d \geq 1 \) with leading coefficient \( a_d \in \mathbb{L}^* \), we define recursively a sequence of polynomials \( D_{k,f} \in \mathbb{L}[X_1, \ldots, X_k] \) in the following way: \( D_{1,f}(X_1) = f(X_1) \) and 
\[
D_{2,f}(X_1, X_2) = f(X_1 + X_2) - f(X_2) = X_1 F_2(X_1, X_2),
\]
for some polynomial \( F_2 \in \mathbb{L}[X_1, X_2] \) of degree
\[
\deg_{X_2} F_2 \leq d - 1
\]
with leading coefficient \( d a_d \). Recursively, we define
\[
D_{k,f}(X_1, \ldots, X_k) = F_{k-1}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k) - F_{k-1}(X_1, \ldots, X_{k-2}, X_k)
= X_k F_k(X_1, \ldots, X_k),
\]
for some polynomial \( F_k \in \mathbb{L}[X_1, \ldots, X_k] \) of degree
\[
\deg_{X_k} F_k \leq d - (k - 1).
\]
If \( d < p \), then the above bounds on the degrees become equalities, and the leading coefficient of \( F_k \) with respect to \( X_k \) is \( d(d - 1) \cdots (d - (k - 2)) a_d \).

For \( k \geq 3 \) we also have the following recurrence relation:
\[
D_{k,f}(X_1, \ldots, X_k) = \frac{1}{X_{k-2}}(D_{k-1,f}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k) - D_{k-1,f}(X_1, \ldots, X_{k-2}, X_k)).
\]

We now give more details in the following straightforward statement which is well-known but is not readily available in the literature.

**Lemma 1.** Let \( f \in \mathbb{L}[X] \) be a polynomial of degree \( d < p \) and leading coefficient \( a_d \in \mathbb{L}^* \). Then
\[
D_{k,f}(X_1, \ldots, X_k) = X_{k-1} F_k(X_1, \ldots, X_k)
\]
where
\[
F_k(X_1, \ldots, X_k) = d(d - 1) \cdots (d - k + 2)a_d X_k^{d-k+1} + \bar{F}_k(X_1, \ldots, X_k),
\]
for some polynomial \( \bar{F}_k \in \mathbb{L}[X_1, \ldots, X_k] \) of degrees
\[
\deg_{X_i} \bar{F}_k \leq d - k + 1, \quad i = 1, \ldots, k - 1, \quad \deg_{X_k} \bar{F}_k \leq d - k.
\]

**Proof.** The result follows by induction over \( k \). Easy computations prove the statement for \( k = 2 \). We assume it is true for \( k - 1 \) and we prove the statement for \( k \). Using the induction hypothesis, we have
\[
D_{k,f}(X_1, \ldots, X_k)
= F_{k-1}(X_1, \ldots, X_k) - F_{k-1}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k)
= d(d - 1) \cdots (d - k + 3)a_d(X_{k-1} + X_k)^{d-k+2} + \bar{F}_{k-1}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k) - d(d - 1) \cdots (d - k + 3)a_d X_k^{d-k+2} - \bar{F}_{k-1}(X_1, \ldots, X_{k-2}, X_k),
\]
where \( \bar{F}_{k-1}(X_1, \ldots, X_{k-2}, Y) \in \mathbb{L}[X_1, \ldots, X_{k-2}, Y] \) is a polynomial of degrees
\[
\deg_{X_i} \bar{F}_{k-1} \leq d - k + 2, \quad i = 1, \ldots, k - 2, \quad \deg_Y \bar{F}_{k-1} \leq d - k + 1.
\]
We write
\[
\bar{F}_{k-1}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k) = X_{k-1} H_k(X_1, \ldots, X_k) + \bar{F}_{k-1}(X_1, \ldots, X_{k-2}, X_k),
\]
where \( H_k \in \mathbb{L}[X_1, \ldots, X_k] \), and taking into account the degrees above, we obtain
\[
\deg_{X_i} H_k \leq d - k + 1, \quad i = 1, \ldots, k - 2,
\]
and
\[
\deg_{X_i} H_k \leq d - k, \quad i = k - 1, k.
\]
Taking into account (6) and (7), and using the binomial expansion of
\[
(X_{k-1} + X_k)^{d-k+2},
\]
we obtain
\[
D_{k,f}(X_1, \ldots, X_k)
= X_{k-1}(d(d - 1) \cdots (d - k + 3)(d - k + 2)a_d X_k^{d-k+1} + \bar{F}_k(X_1, \ldots, X_k)),
\]
where \( \tilde{F}_k \in \mathbb{L}[X_1, \ldots, X_k] \) is defined by

\[
\tilde{F}_k(X_1, \ldots, X_k) = H_k(X_1, \ldots, X_k) + d(d - 1) \cdots (d - k + 3) a_d \\
\times \frac{(X_{k-1} + X_k)^{d-k+2} - X_k^{d-k+2} - (d - k + 2) X_{k-1} X_k^{d-k+1}}{X_{k-1}},
\]

and thus satisfy the conditions

\[
\deg_{X_i} \tilde{F}_k \leq d - k + 1, \quad i = 1, \ldots, k - 1, \quad \deg_{X_k} \tilde{F}_k \leq d - k.
\]

We thus conclude the inductive step. \( \square \)

If we take \( k = d \) in Lemma 1, and then two more consecutive differences, that is, \( k = d + 1 \) and \( k = d + 2 \), we obtain the following consequence.

**Corollary 2.** We have

\[
D_{d,f}(X_1, \ldots, X_d) = X_{d-1}(d! a_d X_d + \tilde{F}_d(X_1, \ldots, X_{d-1})),
\]

where \( \tilde{F}_d \in \mathbb{L}[X_1, \ldots, X_{d-1}] \) is of degrees

\[
\deg_{X_i} \tilde{F}_d \leq 1, \quad i = 1, \ldots, d - 1,
\]

and thus

\[
D_{d+1,f}(X_1, \ldots, X_{d+1}) = d! a_d X_d, \quad D_{d+2,f}(X_1, \ldots, X_{d+2}) = 0.
\]

**Lemma 3.** Let \( \nu \) be a positive integer and \( f = X^\nu g \in \mathbb{L}[X] \), where \( g \in \mathbb{L}[X] \) is of degree \( d < p \). Then

\[
D_{d+3,f}(X_1, \ldots, X_{d+3}) = 0.
\]

**Proof.** We prove by induction over \( k \geq 2 \) that

\[
D_{k,f}(X_1, \ldots, X_k)
= X_{k-1} \left( \sum_{j=1}^{k} X_j^{\nu^{j-1}} \right) G_k(X_1, \ldots, X_k)
+ X_{k-1} \sum_{j=1}^{k-1} X_j^{\nu^{j-1}} G_{k-1}(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_{k-1}, X_k),
\]

where \( G_{k-1} \) and \( G_k \) are defined by (3) and (5) applied to the polynomial \( g \).

The case \( k = 2 \) follows by simple computations, and thus we prove only the induction step from \( k - 1 \) to \( k, k \geq 3 \). Using (4) and the induction step, for \( k \geq 3 \),
we have

\[ D_{k,f}(X_1, \ldots, X_k) = \frac{1}{X_{k-2}} (D_{k-1,f}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k) \]

\[ - D_{k-1,f}(X_1, \ldots, X_{k-2}, X_k)) \]

\[ = \left( \sum_{j=1}^{k-1} X_j^{p^\nu} + X_k^{p^\nu} \right) G_{k-1}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k) \]

\[ + \sum_{j=1}^{k-2} X_j^{p^\nu-1} G_{k-2}(X_1, \ldots, X_{j-1}, \ldots, X_{k-2}) \]

\[ - \left( \sum_{j=1}^{k-2} X_j^{p^\nu} + X_k^{p^\nu} \right) G_{k-1}(X_1, \ldots, X_{k-2}) \]

\[ - \sum_{j=1}^{k-2} X_j^{p^\nu-1} G_{k-2}(X_1, \ldots, X_{j-1}, \ldots, X_{k-1}, X_k) \].

By the definition (3), we have

\[ G_{k-2}(Y_1, \ldots, Y_{k-3}, Y_{k-2} + Y_{k-1}) \]

\[ = G_{k-2}(Y_1, \ldots, Y_{k-3}, Y_{k-1}) + Y_{k-2} G_{k-1}(Y_1, \ldots, Y_{k-1}) , \]

which is applied in (9) with \((Y_1, \ldots, Y_{k-3}) = (X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_{k-2})\), \(Y_{k-2} = X_{k-1}\) and \(Y_{k-1} = X_k\). Similarly, by (3), we have

\[ G_{k-1}(X_1, \ldots, X_{k-2}, X_{k-1} + X_k) \]

\[ = G_{k-1}(X_1, \ldots, X_{k-2}, X_k) + X_{k-1} G_{k}(X_1, \ldots, X_k) . \]

Going now back in (9), and making simple computations, we get the equation (8). In fact, using Lemma 1 and the fact that, by (3) we have

\[ D_{k,g}(X_1, \ldots, X_k) = X_{k-1} G_{k}(X_1, \ldots, X_k) \]

and for \(1 \leq j \leq k - 2\) one has

\[ D_{k-1,g}(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_{k-1}, X_k) \]

\[ = X_{k-1} G_{k-1}(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_{k-1}, X_k) , \]

one can rewrite the equation (8) as follows:

\[ D_{k,f}(X_1, \ldots, X_k) = D_{k,g}(X_1, \ldots, X_k) \left( \sum_{j=1}^{k} X_j^{p^\nu} \right) \]

\[ + \sum_{j=1}^{k-2} X_j^{p^\nu-1} D_{k-1,g}(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_{k-1}, X_k) \]

\[ + X_{k-1}^{p^\nu} G_{k-1}(X_1, \ldots, X_{k-2}, X_k) . \]
By Corollary 2 we have

\[ D_{d+2,g}(X_1, \ldots, X_{d+1}, X_{d+2}) = 0, \]
\[ D_{d+2,g}(X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_{d+2}, X_{d+3}) = 0, \]

and similarly \( D_{d+2,g}(X_1, \ldots, X_{d+1}, X_{d+3}) = 0 \) from where we get

\[ G_{d+2}(X_1, \ldots, X_{d+1}, X_{d+3}) = 0, \]

and thus we conclude the proof.

As a direct application of Lemma 3, we obtain the following more general result.

**Corollary 4.** Let \( \nu \) be a positive integer and

\[ f = X^{p^\nu} g_{\nu} + \cdots + X^p g_1 + g_0, \quad g_i \in \mathbb{L}[X], \quad i = 0, \ldots, \nu, \]

with

\[ \deg g_i + 3 \leq \deg g_0 = d < p, \quad i = 1, \ldots, \nu, \]

and with \( g_0 \) having leading coefficient \( a_d \). Then

\[ D_{d,f}(X_1, \ldots, X_d) = X_{d-1}(d!a_d X_d + \tilde{F}_d(X_1, \ldots, X_{d-1})), \]

where \( \tilde{F}_d \in \mathbb{L}[X_1, \ldots, X_{d-1}] \) is of degrees

\[ \deg_{X_i} \tilde{F}_d \leq 1, \quad i = 1, \ldots, d - 1. \]

**Proof.** The proof follows directly from Lemma 3. Indeed, we have

\[ D_{k,f}(X_1, \ldots, X_k) = \sum_{i=1}^{\nu} D_{k,X^{p^\nu} g_{i}}(X_1, \ldots, X_k) + D_{k,g_0}(X_1, \ldots, X_k). \]

As \( d \geq \deg g_i + 3 \), from Lemma 3 we obtain

\[ D_{d,X^{p^\nu} g_{i}}(X_1, \ldots, X_d) = 0, \]

and thus

\[ D_{d,f}(X_1, \ldots, X_d) = D_{d,g_0}(X_1, \ldots, X_d). \]

Applying now Corollary 2 we conclude the proof.

**Remark 5.** We note that when \( g_i, i = 1, \ldots, \nu, \) are constant polynomials in Corollary 4 we are in the case

\[ f = c_\nu X^{p^\nu} + \cdots + c_1 X^p + g_0, \quad g_0 \in \mathbb{L}[X], \quad c_i \in \mathbb{L}, \quad i = 1, \ldots, \nu, \]
with
\[ 3 \leq \deg g_0 = d < p. \]

Then, we need to take only two differences to eliminate the power of \( p \) monomials, that is, we have

\[ D_{3,f}(X_1, X_2, X_3) = D_{3,g_0}(X_1, X_2, X_3) = X_2G_3(X_1, X_2, X_3), \]

where \( G_3 \in \mathbb{L}[X_1, X_2, X_3] \) is defined by (3) (applied with \( g_0 \)) with \( \deg_{X_3} G_3 = d - 2 \).

**Lemma 6.** Let \( f = g(l(x)) \in \mathbb{L}[X] \), where \( g \in \mathbb{L}[X] \) is a polynomial of degree \( d < p \) with leading coefficient \( a_d \), \( \nu \) is a positive integer and

\[ l = \sum_{i=0}^{\nu} b_i X^{p^i} \in \mathbb{L}[X], \quad p^\nu < q^\nu, \]

is a \( p \)-polynomial. Then

\[ D_{d,f}(X_1, \ldots, X_d) = l(X_{d-1})(d!a_d l(X_d) + \widetilde{F}_d(l(X_1), \ldots, l(X_{d-1}))), \]

where \( \widetilde{F}_d \in \mathbb{L}[X_1, \ldots, X_{d-1}] \) is of degrees

\[ \deg_{X_i} \widetilde{F}_d \leq 1, \quad i = 1, \ldots, d - 1. \]

**Proof.** As the polynomial \( l \) is additive, that is \( l(X_1 + X_2) = l(X_1) + l(X_2) \), then the proof follows exactly as in the proof of Lemma 1. \( \square \)

3 Exponential sums over subspaces

First we introduce the following:

**Definition 1.** For \( 0 < \eta \leq 1 \), we define a subset \( A \subseteq \mathbb{L} \) to be \( \eta \)-good if

\[ \#(A \cap b\mathbb{F}) \leq (\#A)^{1-\eta} \]

for any element \( b \) and a proper subfield \( \mathbb{F} \) of \( \mathbb{L} \).

The main result of this section is based on the following estimate due to Bourgain and Glibichuk [4, Theorem 4] which applies to \( \eta \)-good sets.

For \( 0 < \eta \leq 1 \), we define

\[ \gamma_\eta = \min \left( \frac{1}{156450}, \frac{\eta}{120} \right). \]

Also, throughout the paper \( \psi \) represents an additive character of \( \mathbb{L} \).
**Lemma 7.** Let $3 \leq n \leq 0.9 \log_2 \log_2 q^\varepsilon$ and $A_1, A_2, \ldots, A_n \subseteq \mathbb{L}^*$. Let $0 < \eta \leq 1$ and $\gamma_\eta$ be defined by (11). Suppose $\#A_i \geq 3$, $i = 1, 2, \ldots, n$, and that for every $j = 3, 4, \ldots, n$ the sets $A_j$ are $\eta$-good. Assume further that

$$\#A_1 \#A_2 (\#A_3 \cdots \#A_n)^\gamma_\eta > q^{r(1+\varepsilon)}$$

for some $\varepsilon > 0$. Then, for sufficiently large $q^\varepsilon$, we have the estimate

$$\left| \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_n \in A_n} \psi(a_1a_2 \ldots a_n) \right| < 100 \#A_1 \#A_2 \cdots \#A_n q^{-0.45r/2^\eta}.$$  

For our results we need an estimate for slightly different (and possibly larger) sums

$$\sum_{a_2 \in A_2} \cdots \sum_{a_n \in A_n} \left| \sum_{a_1 \in A_1} \psi(a_1a_2 \ldots a_n) \right|,$$

which we derive directly from Lemma 7. We record this estimate for more general weighted sums, which may be of independent interest for some future applications.

**Corollary 8.** Let $4 \leq n \leq 0.9 \log_2 \log_2 q^\varepsilon + 1$ and $A_1, A_2, \ldots, A_n \subseteq \mathbb{L}^*$. Let $0 < \eta \leq 1$ and $\gamma_\eta$ be defined by (11). Suppose $\#A_i \geq 3$, $i = 2, \ldots, n$, and that for every $j = 4, \ldots, n$ the sets $A_j$ are $\eta$-good. Assume further that

$$\#A_2 \#A_3 (\#A_4 \cdots \#A_n)^\gamma_\eta > q^{r(1+\varepsilon)}$$

for some $\varepsilon > 0$. Let the weights $w_i : \mathbb{L} \to \mathbb{C}$, $i = 1, \ldots, n$, be such that

$$\sum_{a_i \in A_i} |w_i(a_i)|^2 \leq W_i, \quad i = 1, \ldots, n.$$  

Then, for sufficiently large $q^\varepsilon$, for the sum

$$J = \sum_{a_2 \in A_2} \cdots \sum_{a_n \in A_n} w_2(a_2) \cdots w_n(a_n) \left| \sum_{a_1 \in A_1} w_1(a_1) \psi(a_1a_2 \cdots a_n) \right|,$$

we have the estimate

$$|J| < \prod_{i=1}^{n} (W_i \#A_i)^{1/2} ((\#A_1)^{-1/2} + 10q^{-0.45r/2^\eta}).$$

**Proof.** Squaring and applying the Cauchy-Schwarz inequality, we get

$$|J|^2 \leq \sum_{a_2 \in A_2} \cdots \sum_{a_n \in A_n} |w_2(a_2)|^2 \cdots |w_n(a_n)|^2$$ \n
$$\times \sum_{a_2 \in A_2} \cdots \sum_{a_n \in A_n} \left| \sum_{a_1 \in A_1} w_1(a_1) \psi(a_1a_2 \cdots a_n) \right|^2$$ \n
$$= \prod_{i=2}^{n} \left( \sum_{a_i \in A_i} |w_i(a_i)|^2 \right) \sum_{a_1, b_1 \in A_1} w_1(a_1) \overline{w_1(b_1)} \sum_{a_2 \in A_2} \cdots \sum_{a_n \in A_n} \psi(a_2 \cdots a_n(a_1 - b_1)).$$
Applying (13) and Lemma 7 (for the sum over \(A_2, \ldots, A_n\)), we obtain
\[
|\mathcal{J}| \leq \prod_{i=2}^{n} W_i^{1/2} \left( W_1^{1/2} \prod_{i=2}^{n} (\#A_i)^{1/2} \right) + 10 \prod_{i=2}^{n} (\#A_i)^{1/2} q^{-0.45 r_1/2^n} \left( \sum_{a_1, b_1 \in A_1} w_1(a_1) \overline{w_1(b_1)} \right)^{1/2},
\]
where the first summand comes from the case \(a_1 = b_1\). Taking into account that
\[
\sum_{a_1, b_1 \in A_1} w_1(a_1) \overline{w_1(b_1)} = \left| \sum_{a \in A_1} w_1(a) \right|^2 \leq \#A_1 \sum_{a \in A_1} |w_1(a)|^2,
\]
and using again (13), we conclude the proof. \(\square\)

Throughout the paper, we slightly abuse this notion of \(\eta\)-good sets and in the case of affine spaces introduce the following:

**Definition 2.** We say that an affine subspace \(A \subseteq \mathbb{L}\) is \(\eta\)-good if \(A = \mathcal{L} + a\) for some \(a \in \mathbb{L}\) and linear subspace \(\mathcal{L} \subseteq \mathbb{L}\) which is \(\eta\)-good as in Definition 1.

Using Lemma 7 we prove the following estimate of additive character sums with polynomial argument over an affine subspace of \(\mathbb{L}\), which can be seen as an explicit version of [3, Theorem C]. However, we notice that all previous such estimates are known for polynomials of degree less than \(p\). Here we obtain results for more general polynomials.

For \(0 < \varepsilon, \eta \leq 1\), we define
\[
(14) \quad \delta(\varepsilon, \eta) = \max(4, \gamma_\eta^{-1}(\varepsilon^{-1} - 1) + 3),
\]
where \(\gamma_\eta\) is defined by (11).

We prove the next result under a rather technical condition on the weight \(\chi\) of the sum, however, this condition is satisfied in a much stronger form in all interesting examples; see Remark 10.

**Theorem 9.** Let \(0 < \varepsilon, \eta \leq 1\) be arbitrary numbers, \(\gamma_\eta\) and \(\delta(\varepsilon, \eta)\) be defined by (11) and (14), respectively. Let \(A \subseteq \mathbb{L}\) be an \(\eta\)-good affine subspace of dimension \(s\) over \(\mathbb{K}\) with \(s \geq \varepsilon r\).

Let \(d\) be an integer satisfying the inequalities
\[
(15) \quad \delta(\varepsilon, \eta) < d \leq \min(p - 2, 0.9 \log_2 \log_2 q^\nu) + 1,
\]
\(\nu \geq 1\) and \(f\) any polynomial of one of the following forms:
(i) \( f = X^0 g_v + \cdots + X^0 g_1 + g_0 \), where \( g_i \in \mathbb{L}[X] \), \( i = 0 \ldots, v \), are such that 
\[
\deg g_0 = d \geq \deg g_i + 3, \quad i = 1 \ldots, v;
\]
(ii) \( f = g(l(X)) \in \mathbb{L}[X] \), where \( g \in \mathbb{L}[X] \) with \( \deg g = d \) and \( l \in \mathbb{L}[X] \) is a permutation \( p \)-polynomial of the form (10) such that \( l(L) \) is \( \eta \)-good.

Let \( \chi : \mathbb{L} \to \mathbb{C} \) be a function satisfying \( \chi(x + y) = \chi(x)\chi(y) \), \( x, y \in \mathbb{L} \), and such that 
\[
\frac{1}{q^d} \max \left\{ \sum_{x \in A} |\chi(x)|^{2^d}, \sum_{x \in L} |\chi(x)|^{2^d} \right\} \leq \Xi,
\]
where \( L \) is the \( \mathbb{K} \)-linear space underlying \( A \). Then, for sufficiently large \( q^d \), we have 
\[
\left| \sum_{x \in A} \chi(x)\psi(f(x)) \right| \leq 2\Xi^{(d+1)/2^{d+1}} q^{\frac{d-\vartheta}{d}},
\]
where \( \vartheta = \frac{0.9\varepsilon}{2^{2d}} \).

**Proof.** Write \( A = a + L, a \in \mathbb{L} \), where \( L \) is a \( \mathbb{K} \)-linear space of dim_{\mathbb{K}}(L) = s. Making the linear transformation \( x \in L \to a + x \), we reduce the problem to estimating the character sum over a linear subspace, 
\[
S = \sum_{x \in L} \chi(x + a)\psi(f_a(x)), \quad f_a(X) = f(X + a).
\]

We use the method in [24]. For this we square the sum and after changing the order of summation and substituting \( x_1 \to x_1 + x_2 \) and using the fact that 
\[
\chi(x_1 + x_2 + a) = \chi(x_1)\chi(x_2 + a),
\]
we get 
\[
|S|^2 = \sum_{x_1, x_2 \in L} \chi(x_1 + a)\overline{\chi(x_2 + a)}\psi(f_a(x_1) - f_a(x_2))
\]
\[
= \sum_{x_1, x_2 \in L} \chi(x_1 + x_2 + a)\overline{\chi(x_2 + a)}\psi(f_a(x_1 + x_2) - f_a(x_2))
\]
\[
= \sum_{x_1 \in L} \chi(x_1) \sum_{x_2 \in L} |\chi(x_2 + a)|^2 \psi(D_{2, f_a}(x_1, x_2)),
\]
where the polynomial \( D_{2, f_a} \) is defined by (3).

We prove now by induction, squaring and applying the Cauchy-Schwarz inequality \( k \) times, that we get 
\[
|S|^{2^k} \leq q^{e_k} \sum_{x_1, x_2, x_3, \ldots, x_{2^k} \in L} |\chi(x_1)|^{2^{k-1}} |\chi(x_2)|^{2^{k-1}} \cdots |\chi(x_{2^k})|^{2^{k-1}}
\]
\[
\times \left| \sum_{x_{k+1} \in L} |\chi(x_{k+1} + a)|^{2^k} \psi(x_1 x_2 \cdots x_{k-1} D_{k+1, f_a}(x_1, \ldots, x_{k+1})) \right|,
\]
where 
\[
e_k = s(2^k - k - 1), \quad k \geq 1.
\]
From the above we see that the case $k = 1$ holds (where we use the convention that the empty product always equals 1 and thus the argument of $\psi$ is $D_{2,f_0}(x_1, x_2)$). We assume the inequality true for $k$ and we prove it for $k+1$. Squaring and applying the Cauchy-Schwarz inequality to $|S|^{2^k}$, we get

$$|S|^{2^{k+1}} \leq q^{2^{k+1} + k} \sum_{x_1, x_2, \ldots, x_k \in \mathcal{L}} |\chi(x_1)|^{2^k} |\chi(x_2)|^{2^k} \cdots |\chi(x_k)|^{2^k}$$

$$\times \left| \sum_{x_{k+1} \in \mathcal{L}} |\chi(x_{k+1} + a)|^{2^k} \psi(x_1 x_2 \cdots x_{k-1} D_{k+1,f_0}(x_1, \ldots, x_k)) \right|^2$$

$$= q^{2^{k+1}} \sum_{x_1, x_2, \ldots, x_k \in \mathcal{L}} |\chi(x_1)|^{2^k} |\chi(x_2)|^{2^k} \cdots |\chi(x_k)|^{2^k}$$

$$\times \sum_{x_{k+1}, x_{k+2} \in \mathcal{L}} |\chi(x_{k+1} + a)|^{2^k} |\chi(x_{k+2} + a)|^{2^k}$$

$$\times \psi(x_1 x_2 \cdots x_k)$$

$$\times (D_{k+1,f_0}(x_1, \ldots, x_k, x_{k+1}) - D_{k+1,f_0}(x_1, \ldots, x_k, x_{k+2})).$$

Substituting $x_{k+1} \rightarrow x_{k+1} + x_{k+2}$, and using again the property

$$\chi(x_{k+1} + x_{k+2} + a) = \chi(x_{k+1}) \chi(x_{k+2} + a)$$

and (4), we get

$$|S|^{2^{k+1}} \leq q^{2^{k+1}} \sum_{x_1, x_2, \ldots, x_{k+1} \in \mathcal{L}} |\chi(x_1)|^{2^k} |\chi(x_2)|^{2^k} \cdots |\chi(x_{k+1})|^{2^k}$$

$$\times \sum_{x_{k+2} \in \mathcal{L}} |\chi(x_{k+2} + a)|^{2^{k+1}} \psi(x_1 x_2 \cdots x_k D_{k+2,f_0}(x_1, \ldots, x_k)),$$

which proves the induction step.

Applying (17) with $k = d - 1$ and using Corollary 4 for the polynomial $f_0(X) = f(X + a)$ with $f$ corresponding to (i), we get to the exponential sum

$$|S|^{2^{d-1}} \leq q^{2^{(d-1) - d}} \sum_{x_1, x_2, \ldots, x_{d-1} \in \mathcal{L}} |\chi(x_1)|^{2^{d-2}} |\chi(x_2)|^{2^{d-2}} \cdots |\chi(x_{d-1})|^{2^{d-2}}$$

$$\times \left| \sum_{x_d \in \mathcal{L}} |\chi(x_d + a)|^{2^{d-1}} \psi(d! a_d x_1 x_2 \cdots x_d) \right|$$

$$= q^{2^{(d-1) - d}} \sum_{x_1, x_2, \ldots, x_{d-1} \in \mathcal{L}} |\chi(x_1)|^{2^{d-2}} |\chi(x_2)|^{2^{d-2}} \cdots |\chi(x_{d-1})|^{2^{d-2}}$$

$$\times \left| \sum_{x_d \in \mathcal{A}} |\chi(x_d)|^{2^{d-1}} \psi(d! a_d x_1 x_2 \cdots x_d) \right|.$$

We apply now Corollary 8 with

$$4 \leq n = d \leq 0.9 \log_2 q^r + 1.$$
and $A_2 = \ldots = A_n = \mathcal{L}$ and $A_1 = \mathcal{A}$. We note that the condition (15) implies that
\[ s(2 + (d - 3)\gamma \eta) > r(\varepsilon + 1), \]
and thus the condition (12) in Corollary 8 is also satisfied. Moreover, we have
\[ \left( \sum_{x \in \mathcal{L}} |\chi(x)|^{2d-1} \right)^2 \leq q^s \sum_{x \in \mathcal{L}} |\chi(x)|^{2d} \leq \Xi q^{2s} \]
and thus
\[ \sum_{x \in \mathcal{L}} |\chi(x)|^{2d-1} \leq \Xi^{1/2} q^s. \]

We get
\[ |S|^{2d-1} \leq 11 \Xi^{(d+1)/4} q^{2d-1 - 0.45\varepsilon/2^d}, \]
which immediately implies the result.

For the case (ii), proceeding the same but applying Lemma 6 and taking into account that $l$ is a permutation polynomial, we get to the exponential sum
\[ |S|^{2d-1} \leq q^{(2d-1-d)} \sum_{x_1, x_2, \ldots, x_{d-1} \in \mathcal{L}} |\chi(x_1)|^{2d-2} |\chi(x_2)|^{2d-2} \cdots |\chi(x_{d-1})|^{2d-2} \]
\[ \times \left| \sum_{x_d \in \mathcal{A}} |\chi(x_d)|^{2d-1} \psi(d!a_d l(x_1)l(x_2) \cdots l(x_d)) \right| \]
\[ = q^{(2d-1-d)} \sum_{x_1, x_2, \ldots, x_{d-1} \in \mathcal{L}} |\chi(l(x_1))|^{2d-2} |\chi(l(x_2))|^{2d-2} \cdots \]
\[ \times \left| \chi(l(x_{d-1})) |^{2d-2} \sum_{x_d \in l(\mathcal{A})} |\chi(l(x_d))|^{2d-1} \psi(d!a_dx_1x_2 \cdots x_d) \right|, \]
where $l(\mathcal{L})$ and $l(\mathcal{A})$ are subsets of $\mathbb{L}$ of cardinality $q^s$ (we note that if $l$ is a $q$-polynomial, then $l(\mathcal{L})$ is actually a $\mathbb{K}$-linear subspace of $\mathbb{L}$) and the compositional inverse map $\bar{l}$ of $l$ is again a linearised polynomial of the form (10), see [29, Theorem 4.8]. Thus, we have that
\[ \chi(l(x + y)) = \chi(l(x)l(y)) = \chi(l(x))\chi(l(y)) \]
and
\[ \sum_{x \in l(\mathcal{L})} |\chi(l(x))|^{2d} = \sum_{x \in \mathcal{L}} |\chi(x)|^{2d} \leq \Xi q^s \]
As we also assume that $l(\mathcal{L})$ is $\eta$-good, the estimate follows the same by applying Corollary 8 \qed
Remark 10. In the most interesting cases we always have $|\chi(x)| \leq 1$, $x \in \mathbb{L}$. In this case the condition of Theorem 9 on the power moments of $\chi$ is satisfied with $\Xi = 1$.

Probably the most natural example of the function $\chi$ in Theorem 9 is given by exponential functions such as

$$\chi(x) = \exp \left(2\pi i \sum_{j=1}^{m} \zeta_j \text{Tr}_{\mathbb{F}_p}(\tau_j x)\right)$$

for some $\zeta_j \in \mathbb{R}$ and $\tau_j \in \mathbb{L}$. See also Section 6 for more examples.

Remark 11. We note that, by [21, Theorem 7.9], a $p$-polynomial $l \in \mathbb{L}[X]$ as defined by (10) is a permutation polynomial if and only if its only root in $\mathbb{L}$ is 0.

Remark 12. We now give some examples of $l$ and $\mathcal{L}$ for which the set $l(\mathcal{L})$ is $\eta$-good and thus satisfy the conditions of Theorem 9, (ii). We note that when $l(X) = X^p$, then the inverse map of $l$ is given by the polynomial $l(X) = X^{p-r} + \mathbb{F}$, for any subfield $\mathbb{F}$ of $\mathbb{L}$ and any element $b$ not in $\mathbb{F}$, and thus $l(\mathcal{L})$ is $\eta$-good (because $\#(l(\mathcal{L}) \cap b\mathbb{F}) = \#(\mathcal{L} \cap l(b\mathbb{F})) = \#(\mathcal{L} \cap b^{p-r} \mathbb{F})$ since $l$ is a permutation and $\mathcal{L}$ is $\eta$-good).

Another immediate example can be given for a prime $q = p$ and also a prime $r$. Since the only proper subfield $\mathbb{F}$ of $\mathbb{L}$ is $\mathbb{F}_p$, if $s \geq 2$, that is, $\#\mathcal{L} \geq p^2$, then

$$\#(l(\mathcal{L}) \cap b\mathbb{F}) \leq p \leq \#l(\mathcal{L})^{1/2}.$$

4 Values of polynomials in subspaces

In this section we give upper bounds for $I_f(A, B)$ defined by (1), that is, the cardinality of $f(A) \cap B$, for a polynomial $f \in \mathbb{L}[X]$ and affine subspaces $A, B$ of $\mathbb{L}$ over $\mathbb{K}$.

For our first result we use the Weil bound (see [21, Theorem 5.38]) in a standard way. We recall it for the sake of completeness and use it as a benchmark for further improvements.

Lemma 13. Let $f \in \mathbb{L}[X]$ be of degree $d \geq 1$ with $(d, p) = 1$, and let $\psi$ be a nontrivial additive character of $\mathbb{L}$. Then

$$\left| \sum_{c \in \mathbb{L}} \psi(f(c)) \right| \leq (d-1)q^{d/2}.$$

Theorem 14. Let $f \in \mathbb{L}[X]$ be a polynomial of degree $d \geq 2$, $(d, p) = 1$, $A \subseteq \mathbb{L}$ and $B \subseteq \mathbb{L}$ affine subspaces of dimension $s$ and $m$, respectively, over $\mathbb{K}$. Then, we have

$$I_f(A, B) = q^{s+m-r} + O(dq^{r/2}).$$
Proof. As in Theorem 9, we can reduce the problem to estimating $I_f(L_1, L_2)$, where $L_1, L_2$ are linear spaces.

Let $\beta_1, \ldots, \beta_{r-s}$ be the basis for the complementary space of $L_1$ and $\omega_1, \ldots, \omega_{r-m}$ be the basis for the complementary space of $L_2$, that is, $u \in L_1$ and $v \in L_2$ if and only if

$$\text{Tr}_{L_1|K}(\beta_i u) = 0, \quad i = 1, \ldots, r-s, \quad \text{Tr}_{L_2|K}(\omega_i v) = 0, \quad i = 1, \ldots, r-m.$$  \hfill (18)

We use the relations (18) to give an upper bound for $I_f(A, B) = I_f(L_1, L_2)$.

Indeed, let $\psi$ be a nontrivial additive character of $L$. Using additive character sums to count the elements $u \in L_1$ such that the elements of $f(u)$ satisfy (18), we have

$$I_f(L_1, L_2) = \frac{1}{q^{r-s-m}} \sum_{x \in L} \sum_{c_i, d_j \in K} \psi \left( \sum_{i=1}^{r-s} c_i \beta_i x + \sum_{j=1}^{r-m} d_j \omega_j f(x) \right),$$

where the first term is given by $c_i = d_j = 0, \quad i = 1, \ldots, r-s, \quad j = 1, \ldots, r-m,$ and $\sum^*$ means that at least one element $c_i, d_j \neq 0$.

We notice that since $\deg f = d \geq 2$, nontrivial linear combinations

$$\sum_{i=1}^{r-s} c_i \beta_i x + \sum_{j=1}^{r-m} d_j \omega_j f(x), \quad c_i, d_j \in K, \quad i = 1, \ldots, r-s, \quad j = 1, \ldots, r-m,$$

that appear in the inner sum are all nonconstant polynomials. Indeed, assume that this is not the case, and without loss of generality we can also assume that $d_i \neq 0$ for at least one $i = 1, \ldots, r-m$. Then, the vanishing of the leading coefficients (of the monomial $X^d$)

$$\sum_{i=1}^{r-m} d_i \omega_i X^d = 0$$

implies that the elements $\omega_1, \ldots, \omega_{r-m}$ are linearly dependent as elements of $L$ seen as a vector space over $K$, which contradicts the hypothesis.

We can apply now the Weil bound given by Lemma 13 to the sum over $x \in L$ and conclude the proof. \hfill $\Box$

We note that the bound of Theorem 14 is nontrivial whenever $dq^{r/2} < q^s$, and thus only for $s > r(1/2 + \epsilon)$, for some $\epsilon > 0$.

In the rest of this section we obtain a bound that depends on both parameters $s$ and $m$. We recall first a similar result that was recently obtained in [22, Theorem 7] for the case $A = B$ and only for polynomials of degree smaller than $p$. 

For $d \geq 2$, define the sequences
\[
\eta_d = \frac{4}{277 \cdot 5^{d-2} - 1}, \quad \kappa_d = \frac{4}{277 \cdot 5^{d-2} + 3},
\]
and also for $d \geq 3$,
\[
\vartheta_d = \eta_d + \vartheta_{d-1} - \eta_d \vartheta_{d-1}, \quad \rho_d = \eta_d + \vartheta_d - \eta_d \vartheta_d,
\]
where $\eta_2 = \vartheta_2 = 1/69$.

Let $f \in \mathbb{L}[X]$ be of degree $d = \deg f$ with $p > d \geq 2$ and let $\mathcal{A} \subseteq \mathbb{L}$ be an affine subspace of dimension $s$ over $\mathbb{K}$ such that for any subfield $\mathbb{F} \subseteq \mathbb{L}$ and any $b \in \mathbb{L}$ we have
\[
\#(\mathcal{L} \cap b\mathbb{F}) \leq \max \left\{ \left(\#\mathbb{L}\right)^{1/2}, \frac{q^{r(1-\rho_d)}}{8} \right\},
\]
where $\mathcal{A} = a + \mathcal{L}$ for some $a \in \mathbb{F}$ and a linear subspace $\mathcal{L} \subseteq \mathbb{L}$. Then the following estimate is obtained in \cite[Theorem 7]{22}:
\[
(19) \quad \mathcal{I}_f(\mathcal{A}, \mathcal{A}) \ll q^{s(1-\kappa_d)}.
\]

We prove now one of our main results using Theorem \cite{9}.

**Theorem 15.** Let $0 < \varepsilon, \eta \leq 1$ be arbitrary numbers and let $\gamma_\eta$ and $\delta(\varepsilon, \eta)$ be defined by (11) and (14), respectively. Let $\mathcal{A} \subseteq \mathbb{L}$ be an $\eta$-good affine subspace of dimension $s$ over $\mathbb{K}$ with
\[
s \geq \varepsilon r,
\]
and $\mathcal{B} \subseteq \mathbb{L}$ another affine subspace of dimension $m$ over $\mathbb{K}$. Let $d$ and $f$ be as in Theorem \cite{9} Then, for sufficiently large $q^r$,
\[
|\mathcal{I}_f(\mathcal{A}, \mathcal{B}) - q^{s+m-r}| \leq 2q^{s-r\vartheta},
\]
where $\vartheta$ is defined by (16).

**Proof.** As in the proof of Theorem \cite{14} (where we take the sum over $\mathcal{L}_1$, not all the field $\mathbb{L}$), we have
\[
\mathcal{I}_f(\mathcal{A}, \mathcal{B}) = \frac{1}{q^{r-m}} \sum_{i=1,\ldots,r-m} \sum_{x \in \mathcal{L}_1} \psi \left( \sum_{i=1}^{r-m} c_i \alpha_i f(x) \right),
\]
\[
= q^{s+m-r} + \frac{1}{q^{r-m}} \sum_{i=1,\ldots,r-m} \sum_{x \in \mathcal{L}_1} * \psi \left( \sum_{i=1}^{r-m} c_i \alpha_i f(x) \right),
\]
where the first term corresponds to \( c_i = 0 \) for all \( i = 1, \ldots, r - m \) and \( \sum^* \) means that at least one \( c_i \neq 0 \). We denote

\[
T = \sum_{x \in \mathcal{L}_1} \psi \left( \sum_{i=1}^{r-m} c_i \omega_i f(x) \right).
\]

We apply Theorem 9 (with \( \chi(x) = 1, x \in \mathbb{L} \), and \( \Xi = 1 \)) for the sum \( T \) with the polynomial

\[
F = \sum_{i=1}^{r-m} c_i \omega_i f(X) \in \mathbb{L}[X],
\]

which is of degree \( d \) as at least one \( c_i \neq 0 \). We get

\[
|T| \leq 2q^{s-r \rho},
\]

and thus we conclude the proof.

We note that \( I_f(A, B) > 0 \) in Theorem 15 if \( m > r(1 - \vartheta) \). Furthermore, for any fixed \( \rho > 1 - \vartheta \) and \( m \geq r \rho \), Theorem 15 gives an asymptotic formula for \( I_f(A, B) \) as \( q^r \to \infty \).

When \( A = B \) in Theorem 15 we get the estimate

\[
I_f(A, A) \leq q^{2s-r} + 2q^{s-r \rho}.
\]

This bound improves the estimate (19) obtained in [22] for

\[
s < 2.5 \left( \frac{5}{4} \right)^d r \varepsilon.
\]

In particular, if \( \varepsilon = s/r \), it always improves (19) whenever \( d \) satisfies the condition (15). Moreover, Theorem 15 generalises (19) as this estimate was obtained in [22] only for polynomials of degree \( d < p \).

Note also that the result of Roche-Newton and Shparlinski [22] always requires \( \eta \geq 1/2 \) (but also applies to polynomials of lower degree).

**Corollary 16.** For sufficiently large \( q^r \), if under the conditions of Theorem 15 we have \( f(A) \subseteq B \), then \( B = \mathbb{L} \).

**Proof.** Indeed, if \( f(A) \subseteq B \), then from Theorem 15 we derive

\[
q^s = I_f(A, B) \leq q^{s+m-r} + 2q^{s-r \rho},
\]

which is possible only if \( m = r \).
Theorem 15 has also direct consequences on the image and kernel subspaces of \( q \)-polynomials defined by

\[
I = \sum_{i=0}^{v} b_i X^{q^i} \in \mathbb{L}[X], \quad v < r.
\]

Then, for an affine subspace \( B \) of \( \mathbb{L} \) of dimension \( m \leq r \), the image set \( I(B) = \{ I(x) \mid x \in B \} \) is a \( \mathbb{K} \)-affine subspace of dimension at most \( m \).

Moreover, we denote by \( \text{Ker}(I) \) the set of zeroes of the polynomial \( I \). By [21, Theorem 3.50], \( \text{Ker}(I) \) is a \( \mathbb{K} \)-linear subspace of \( \mathbb{F}_{q^r} \), where \( \mathbb{F}_{q^r} \) is the field extension of \( \mathbb{L} \) containing all the roots of \( I \). Taking now the trace over \( \mathbb{L} \), we have that \( \text{Tr}_{\mathbb{F}_{q^r}|\mathbb{L}}(\text{Ker}(I)) \) is a \( \mathbb{K} \)-linear subspace of \( \mathbb{L} \).

Under the conditions of Theorem 15 for any \( q \)-polynomial \( I \in \mathbb{L}[X] \) defined by (20), we have

\[
|J_f(A, I(B)) - q^{r+m-r}| \leq 2q^{r-r_{\psi}},
\]

where \( \psi \) is defined by (16). The same estimate holds for

\[
J_f(A, \text{Tr}_{\mathbb{F}_{q^r}|\mathbb{L}}(\text{Ker}(I)))
\]

with \( m \) replaced by \( \text{dim}_{\mathbb{K}} \text{Tr}_{\mathbb{F}_{q^r}|\mathbb{L}}(\text{Ker}(I)) \).

Moreover, as in Corollary 16, we see that \( f(A) \) is not included in \( I(B) \) for any proper subspace \( B \subseteq \mathbb{L} \) or in \( \text{Tr}_{\mathbb{F}_{q^r}|\mathbb{L}}(\text{Ker}(I)) \).

It would be certainly interesting to find upper bounds for the intersection of image sets of polynomials on affine subspaces. That is, given \( f, g \in \mathbb{L}[X] \), find estimates for the size of \( f(A) \cap g(A) \) for a given proper affine subspace \( A \subseteq \mathbb{L} \). For prime fields, Chang shows in [17] that the intersection of the images of two polynomials on a given interval is sparse. In the case of arbitrary finite fields, several such estimates are given in [10] for very special classes of polynomials and affine spaces.

### 5 Polynomial orbits in subspaces

As in [22], one can obtain immediately from Theorem 15 the following consequence about the number of consecutive iterates falling in a subspace. Moreover, since whenever \( s > r(1 - \psi) \) we obtain an asymptotic bound in Theorem 15 (with \( s = m \)), in this section, for typographical simplicity, we consider the more interesting case of small dimension

\[
s \leq r(1 - \psi),
\]
where \( \vartheta \) is defined by (16). In this case, the bound in Theorem 15 (with \( \mathcal{A} = \mathcal{B} \)) becomes

\[
I_f(\mathcal{A}, \mathcal{A}) \leq 3q^{s - r \vartheta}.
\]

We recall that for a polynomial \( f \in \mathbb{L}[X] \) and an element \( u \in \mathbb{L} \), we define \( T_{f,u} = \#\text{Orb}_f(u) \) as defined by (2).

**Corollary 17.** Let \( 0 < \varepsilon, \eta \leq 1 \) be arbitrary numbers and let \( \gamma_\eta \) and \( \delta(\varepsilon, \eta) \) be defined by (11) and (14), respectively. Let \( \mathcal{A} \subseteq \mathbb{L} \) be an \( \eta \)-good affine subspace of dimension \( s \) over \( \mathbb{K} \) with

\[
\varepsilon r \leq s \leq r(1 - \vartheta),
\]

where \( \vartheta \) is defined by (16). Let \( d \) and \( f \) be as in Theorem 9. If for some \( u \in \mathbb{L} \) and an integer \( N \) with \( 2 \leq N \leq T_{f,u} \) we have

\[
f^{(n)}(u) \in \mathcal{A}, \quad n = 0, \ldots, N - 1,
\]

then, for sufficiently large \( q^s \),

\[
q^s \geq \frac{1}{3} N q^{r \vartheta}.
\]

**Proof.** The result follows directly from Theorem 15 as

\[
N \leq I_f(\mathcal{A}, \mathcal{A}) \leq 3q^{s - r \vartheta}.
\]

\( \square \)

**Remark 18.** Similarly to Corollary 17 (replacing \( \mathcal{A} \) with the image space of a linearised polynomial \( l \)), based on the discussion after Corollary 16 one can obtain estimates for the number of consecutive elements in the orbit of a polynomial of the form defined in Theorem 9 that fall in the orbit of \( l \) in any point of \( \mathbb{L} \).

We also note that the proof of [22, Theorem 6], using Theorem 15, can give information about the number of arbitrary (not necessarily consecutive) iterates falling in a subspace. For the sake of completeness we repeat the argument of [22, Theorem 6] for the case of subspaces instead of subfields for which this result has been obtained.

We present our bounds in terms of the parameter \( \rho \) which is the frequency of iterates of \( f \in \mathbb{L}[X] \) in an affine space, that is, \( \rho = M/N \), where \( M \) is the number of positive integers \( n \leq N \) with \( f^{(n)}(u) \in \mathcal{A} \). Again, we obtain a power improvement over the trivial bound \( q^s \geq \rho N \) (where \( s = \dim \mathcal{A} \)).
Theorem 19. Let $0 < \varepsilon, \eta \leq 1$ and let $\gamma_\eta$ and $\delta(\varepsilon, \eta)$ be defined by (11) and (14), respectively. Let $A \subseteq \mathbb{L}$ be an $\eta$-good affine subspace of dimension

$$\varepsilon r \leq s \leq r(1 - \vartheta_\rho)$$

over $\mathbb{K}$, where

$$\vartheta_\rho = \frac{0.9\varepsilon}{2d^{2/\rho}}.$$ 

Let $f \in \mathbb{L}[X]$ be a polynomial of degree $d$ such that for $N \leq T_{f,u}$ we have $f^{(n)}(u) \in A$ for $\rho N \geq 2$ values of $n = 1, \ldots, N$. If

$$\delta(\varepsilon, \eta) < d^{2/\rho - 1} \leq \min(p - 2, 0.9 \log_2 \log_2 q^\prime) + 1,$$

then, for sufficiently large $q^\prime$,

$$q^\prime \geq \frac{\rho^2 N}{24} q^{\rho_\vartheta}.$$ 

Proof. We follow exactly the same proof as in [22, Theorem 6]. Let $M = \rho N$ and $1 \leq n_1 < \cdots < n_M \leq N$ be all the values such that $f^{(n_i)}(u) \in A$, $i = 1, \ldots, M$. We denote by $A(h)$ the number of $i = 1, \ldots, M - 1$ with $n_{i+1} - n_i = h$. Clearly

$$\sum_{h=1}^{N} A(h) = M - 1 \quad \text{and} \quad \sum_{h=1}^{N} A(h)h = n_M - n_1 \leq N.$$

Thus, for any integer $1 \leq H \leq N$ we have

$$\sum_{h=1}^{H} A(h) = M - 1 - \sum_{h=H+1}^{N} A(h) \geq M - 1 - (H + 1)^{-1} \sum_{h=H+1}^{N} A(h)h \geq M - 1 - (H + 1)^{-1} N.$$

Hence there exists $k \in \{1, \ldots, H\}$ with

$$A(k) \geq H^{-1}(M - 1 - (H + 1)^{-1} N).$$

Let $H = \lceil 2\rho^{-1} \rceil \geq 1$, and thus $H \leq 2N/M$. Then

$$H^{-1}(M - 1 - (H + 1)^{-1} N) \geq \frac{M - 1}{2H} \geq \frac{M(M - 1)}{4N}$$

and we derive from (22) that

$$A(k) \geq \frac{M(M - 1)}{4N} = \frac{\rho^2 N}{4} \left(1 - \frac{1}{M}\right) \geq \frac{\rho^2 N}{8}.$$
Let \( J \) be the set of \( j \in \{1, \ldots, M - 1\} \) with \( n_{j+1} - n_j = k \). Then we have

\[
f^{(n_j)}(u) \in A \quad \text{and} \quad f^{(n_{j+1})}(u) = f^{(k)}(f^{(n_j)}(u)) \in A,
\]

that is

\[
(f^{(n_j)}(u), f^{(k)}(f^{(n_j)}(u))) \in A \cap f^{(k)}(A).
\]

Therefore, \( A(k) \leq J_{f^{(k)}}(A, A) \), and from (23) and Theorem 15 we get

\[
\frac{\rho^2 N}{8} \leq 3q^{s - r\vartheta_{\rho}},
\]

where \( \vartheta_{\rho} \) is defined by (21). We thus conclude the proof. \( \Box \)

One can also obtain information on the intersection of orbits of a polynomial \( f \) of degree \( d < p \) with orbits of a \( q \)-polynomial \( l \) (see also the discussion after Corollary 16).

**Corollary 20.** Let \( 0 < \varepsilon, \eta \leq 1 \) and let \( \gamma_\eta \) and \( \delta(\varepsilon, \eta) \) be defined by (11) and (14), respectively. Let \( f \in \mathbb{L}[X] \) be a polynomial of degree \( d \) and \( l \in \mathbb{L}[X] \) a linearised polynomial of the form (20) such that \( l(\mathbb{L}) \) is an \( \eta \)-good linear subspace of dimension \( s \geq \varepsilon r \) over \( \mathbb{K} \). Let

\[
M = \#(\text{Orb}_f(u) \cap \text{Orb}_l(v)),
\]

and \( \rho = M/\min(T_{f,u}, T_{l,v}) \) the frequency of intersection of the orbits. If

\[
\delta(\varepsilon, \eta) < d^{2^\rho - 1} \leq \min(p - 2, 0.9 \log_2 \log_2 q^r) + 1,
\]

then, for sufficiently large \( q^r \),

\[
q^r \geq \frac{\rho^2 \min(T_{f,u}, T_{l,v})}{24} q^{r\vartheta_{\rho}},
\]

where \( \vartheta_{\rho} \) is defined by (21).

**Proof.** As \( \text{Orb}_l(v) \subseteq l(\mathbb{L}) \), the proof follows exactly as the proof of Theorem 19 but with \( A \) replaced with \( l(\mathbb{L}) \) and \( N \) replaced with \( \min(T_{f,u}, T_{l,v}) \). \( \Box \)

### 6 Exponential sums over consecutive integers

In this section we consider \( q = p \). For a positive integer \( n \leq p^r - 1 \), we consider the \( p \)-adic representation

\[
n = n_0 + n_1 p + \cdots + n_{s-1} p^{s-1}, \quad 0 \leq n_{j} < p, \quad j = 0, \ldots, s - 1,
\]

for some \( s \leq r \).
In this section we fix a basis $\omega_0, \ldots, \omega_{r-1}$ of $\mathbb{L}$ over $\mathbb{F}_p$ and define

$$\zeta_n = \sum_{j=0}^{s-1} n_j \omega_j.$$  

(25)

Let $1 \leq N \leq p^r - 1$, $f \in \mathbb{L}[X]$ be a polynomial of degree $d$ and $\psi$ an additive character of $\mathbb{L}$. In this section we estimate the exponential sum

$$S(N) = \sum_{n \leq N} \chi(n) \psi(f(\zeta_n)),$$

where $\chi : \mathbb{N} \to \mathbb{C}$ is a $p$-multiplicative function, that is, it satisfies the condition

$$\chi(m + tp^k) = \chi(m)\chi(tp^k)$$

for all $k \geq 0$, $t \geq 0$ and $0 \leq m < p^k$. This class of functions, as well as the closely related class of $p$-additive functions have been studied in classical works of Gelfond [16] and Delange [14], see also [15, 17, 20] and references therein for more recent developments.

A large family of such functions can be obtained as

$$\chi(n) = \exp \left(2\pi i \sum_{j=0}^{s-1} \alpha_j n_j\right),$$

(26)

where $\alpha_j$, $j = 0, 1, \ldots$, is a fixed infinite sequence of real numbers and $n$ is given by the $p$-adic representation as in (24); see also [19] for a more general class. In particular, taking $\alpha_j = \alpha p^j$ and $\alpha_j = \alpha$ for a real $\alpha$, we obtain the following two natural examples,

$$\chi(n) = \exp(2\pi i \alpha n) \quad \text{and} \quad \chi(n) = \exp(2\pi i \sigma_p(n)),$$

respectively, where $\sigma_p(n)$ is the sum of $p$-ary digits of $n$.

**Theorem 21.** Let $0 < \varepsilon, \eta \leq 1$ be arbitrary numbers and let $\gamma_\varepsilon$ and $\delta(\varepsilon, \eta)$ be defined by (11) and (14), respectively. Let $p^{s-1} \leq N \leq p^s - 1$ for some $s \leq r$ satisfying

$$s \geq \varepsilon r,$$

and assume the linear subspace $\mathcal{L}_s \subseteq \mathbb{L}$ spanned by $\omega_0, \ldots, \omega_{s-1}$ is $\eta$-good. Let $f \in \mathbb{L}[X]$ be a polynomial of the form (i) or (ii) as defined in Theorem 9 with $d$ satisfying the condition

$$\delta(\varepsilon/2, \eta/2) + 1 < d \leq \min(p - 2, 0.9 \log_2 \log_2 p^r) + 2,$$

(27)
and ψ an additive character of \( \mathbb{L} \). Let \( \chi : \mathbb{N} \to \mathbb{C} \) be a \( p \)-multiplicative function defined by (26). Then, for sufficiently large \( p' \),

\[
|S(N)| \leq (Np)^{1-\eta/4} + p(Np)^{1-\eta/2} + 2Np^{-\vartheta \eta/2},
\]

where

\[
\vartheta = \frac{0.9 \varepsilon (1 - \eta/2)}{2^{d-2}}.
\]

**Proof.** Let \( K = \lceil s(1 - \eta/2) \rceil \) and \( M = p^K \lfloor N/p^K \rfloor - 1 \). Our sum becomes

\[
|S(N)| \leq |S(M)| + p^K \leq |S(M)| + p(Np)^{1-\eta/2}.
\]

From the definition of \( M \), we have that

\[
M = \sum_{i=0}^{K-1} (p - 1)p^i + Tp^K,
\]

for some \( T \leq p'^{r-K-1} - 1 \leq Np^{-K} - 1 \).

We have

\[
|S(M)| = \left| \sum_{m < p^K} \chi(m) \sum_{t \leq T} \chi(tp^K) \psi(f(\xi_m + tp^K)) \right|
\]

\[
\leq \sum_{m < p^K} \left| \sum_{t \leq T} \chi(tp^K) \psi(f(\xi_m + tp^K)) \right|
\]

and thus, squaring and applying the Cauchy-Schwarz inequality and using the fact that \( |\chi(tp^K)| = 1 \), we get

\[
|S(M)|^2 \leq p^K \sum_{m < p^K} \left| \sum_{t \leq T} \chi(tp^K) \psi(f(\xi_m + tp^K)) \right|^2
\]

\[
\leq p^K \sum_{t_1, t_2 \leq T} \left| \sum_{m < p^K} \psi(f(\xi_{m+t_1p^K}) - f(\xi_{m+t_2p^K})) \right|.
\]

The set of integers \( n \leq M \) is of the form

\[
\left\{ \sum_{i=0}^{K-1} n_ip^i + tp^K \mid 0 \leq n_0, \ldots, n_{K-1} \leq p - 1, 0 \leq t \leq T \right\},
\]

and thus we now see from (25) that

\[
\xi_{m+t, p^K} = \xi_m + \zeta_i, \quad \xi_m \in \mathcal{L}_K, \quad i = 1, 2,
\]
where $\mathcal{L}_K$ is the $K$-dimensional linear subspace defined by the basis elements $\omega_0,\ldots,\omega_{K-1}$ of $\mathbb{L}$ over $\mathbb{F}_p$, and with some $\xi_{t_i} \in \mathbb{L}$, $0 \leq t_i \leq T$, $i = 1, 2$. As $m$ runs over the interval $[0, p^K - 1]$, $\xi_m$ runs over all the elements of $\mathcal{L}_K$, and moreover, $\xi_{t_1} \neq \xi_{t_2}$ for $t_1 \neq t_2$.

Our sum becomes

$$|S(M)|^2 \leq p^K \sum_{t_1,t_2 \leq T} \left| \sum_{x \in \mathcal{L}_K} \psi(f(x + \xi_{t_1}) - f(x + \xi_{t_2})) \right| \leq Np^K + p^K \sum_{t_1,t_2 \leq T, t_1 \neq t_2} \left| \sum_{x \in \mathcal{L}_K} \psi(F_{t_1,t_2}(x)) \right|,$$

where $F_{t_1,t_2}(X) = f(X + \xi_{t_1}) - f(X + \xi_{t_2}) \in \mathbb{L}[X]$.

We note that, as $f \in \mathbb{L}[X]$ is a polynomial of the form (i) or (ii) as defined in Theorem 9 then $F_{t_1,t_2}$ is a nonconstant polynomial of the same form as $f$. When $f$ is of the form (i), we have

$$f = X^{p^r} g_0 + \cdots + X^p g_1 + g_0,$$

where $g_i \in \mathbb{L}[X]$, $i = 0, \ldots, \nu$, are such that $\deg g_0 = d \geq \deg g_i + 3$, $i = 1 \ldots, \nu$. Then we get

$$F_{t_1,t_2}(X) = X^{p^r}(g_0(X + \xi_{t_1}) - g_0(X + \xi_{t_2})) + \cdots + X^p(g_1(X + \xi_{t_1}) - g_1(X + \xi_{t_2})) + F_{0,t_1,t_2}(X),$$

where

$$F_{0,t_1,t_2}(X) = g_0(X + \xi_{t_1}) - g_0(X + \xi_{t_2}) + \sum_{i=1}^{\nu} (g_{p^r}^p g_i(X + \xi_{t_1}) - g_{p^r}^p g_i(X + \xi_{t_2})).$$

For $t_1 \neq t_2$, we note that $g_i(X + \xi_{t_1}) - g_i(X + \xi_{t_2})$, $i = 0, \ldots, \nu$, is a nonconstant polynomial of degree equal to $\deg g_i - 1$, and

$$d - 1 = \deg F_{0,t_1,t_2} \geq \deg(g_i(X + \xi_{t_1}) - g_i(X + \xi_{t_2})) + 3.$$

Thus, $F_{t_1,t_2}$ is of the same form and satisfies the same conditions as $f$.

If $f$ is of the form (ii) of Theorem 9 that is, $f = g(l(x))$ with $\deg g = d$ and some permutation $p$-polynomial $l \in \mathbb{L}[X]$, then

$$F_{t_1,t_2}(X) = g(l(X) + l(\xi_{t_1})) - g(l(X) + l(\xi_{t_2})) = G_{t_1,t_2}(l(X)),$$

where $G_{t_1,t_2}(X) = g(X + l(\xi_{t_1})) - g(X + l(\xi_{t_2})) \in \mathbb{L}[X]$ is of degree $d - 1$.

As $s \geq \varepsilon r$, then $K \geq s(1 - \eta/2) \geq \varepsilon r$, where $\varepsilon = \varepsilon(1 - \eta/2)$ by the hypothesis. Since

$$K \geq s(1 - \eta/2) > s \frac{1 - \eta}{1 - \eta/2}.$$
we also have, for any proper subfield $F$ of $L$,
\[ \#(\mathcal{L}_K \cap bF) \leq \#(\mathcal{L}_L \cap bF) \leq p^{n(1-\eta)} < p^{K(1-\eta/2)}. \]
Moreover, from condition (27), we have $d - 1 > \delta(\varepsilon/2, \eta/2) \geq \delta(\varepsilon, \eta/2)$ as defined by (14). Therefore, the conditions of Theorem 9 are satisfied (with $d$ replaced by $d - 1$, $\varepsilon$ replaced by $\varepsilon\eta$, $\eta$ replaced by $\eta/2$ and $\Xi = 1$), and we obtain
\[ |S(M)|^2 \leq Np^K + 2p^K T^2 p^{K-r^\eta} \leq Np^{s(1-\eta/2)+1} + 2N^2 p^{-r^\eta} \]
\[ \leq (Np)^{2-\eta/2} + 2N^2 p^{-r^\eta}, \]
where $\vartheta_\eta$ is given by (28) and thus, recalling (29), we conclude the proof. □

We also note that we have not put any effort in optimising the condition (27) in Theorem 21. For example, if one imposes the condition $\delta(\varepsilon(1-0.9\eta), 0.1\eta) + 1 < d \leq \min(p - 2, 0.9 \log_2 \log_2 p') + 2$, then one obtains the slightly better bound
\[ |S(N)| \leq (Np)^{1-0.45\eta} + p(Np)^{1-0.9\eta} + 2Np^{-r^\eta/2}, \]
where
\[ \vartheta_\eta = \frac{0.9\varepsilon(1-0.9\eta)}{2^{d-2}}. \]

**Remark 22.** We note that similarly to the proof of Theorem 21, we can derive directly from Theorem 9 a bound for the exponential sum
\[ R(N) = \sum_{n \leq N} \chi(\xi_n) \psi(f(\xi_n)), \]
where $f \in \mathbb{L}[X]$ is of the form (i) or (ii) as defined in Theorem 9 with $d$ satisfying the condition
\[ \delta(\varepsilon/2, \eta/2) < d \leq \min(p - 2, 0.9 \log_2 \log_2 p') + 1. \]
Let $\chi : \mathbb{L} \to \mathbb{C}$ satisfy the conditions $\chi(x + y) = \chi(x)\chi(y), x, y \in \mathbb{L}$, and
\[ |\chi(x)| \leq 1, \quad x \in \mathbb{L}. \]
Then, for sufficiently large $p'$, one obtains
\[ |R(N)| \leq 2Np^{s\eta/2 - r^\eta} + p(Np)^{1-\eta/2} \max_{n \leq N} |\chi(\xi_n)|, \]
where
\[ \vartheta_\eta = \frac{0.9\varepsilon(1-\eta/2)}{2^{d-2}}. \]
Indeed, as in the proof of Theorem 21 we reduce the problem to estimating $|R(M)|$, where $M = p^K \lfloor N/p^K \rfloor - 1$ and $K = \lceil s(1 - \eta/2) \rceil$. As in the proof of Theorem 21 the set of integers $n \leq M$ is of the form (30), and thus we now see from (25) that the set of $\xi_n$ is partitioned into the union of $T + 1$ affine spaces of the shape $A(t) = \mathcal{L}_K + \zeta_t$, where $\mathcal{L}_K$ is the $K$-dimensional linear subspace defined by the basis elements $\omega_0, \ldots, \omega_{K-1}$ of $\mathbb{L}$ over $\mathbb{F}_p$, and with some $\zeta_t \in \mathbb{L}$, $0 \leq t \leq T < N/p^K$.

As there are at most $N/p^K$ elements $\xi_t \in \mathbb{L}$ corresponding to $t \leq T$ as discussed above and in Theorem 21, our sum becomes

$$|R(M)| \leq Np^{-K} \left| \sum_{x \in A(t)} \chi(x) \psi(f(x)) \right|,$$

where $A(t) = \mathcal{L}_K + \zeta_t$ for some $\zeta_t \in \mathbb{L}$, $0 \leq t \leq T$. Now, the estimate follows applying Theorem 9 to the sum $R(M)$.

Moreover, if $N = p^s - 1$, for some $s \leq r$, the set of elements $\xi_n$ corresponding to $n \leq N$ given by (25) defines an affine subspace $A$ of $\mathbb{L}$ of dimension $s$. This case is exactly Theorem 9 and thus

$$|R(N)| \leq 2p^{s-r\vartheta},$$

where $\vartheta$ is defined by (16).

7 Waring problem in intervals and subspaces

Let $f \in \mathbb{L}[X]$ be a polynomial of degree $d$. In this section we consider first the Waring problem over an affine subspace $A$ of $\mathbb{L}$ of dimension $s$, that is, the question of the existence and estimation of a positive integer $k$ such that, for any $y \in \mathbb{L}$, the equation

$$(31) \quad f(x_1) + \cdots + f(x_k) = y,$$

is solvable in $x_1, \ldots, x_k \in A$.

In particular, we denote by $g(f, q, s)$ the smallest possible value of $k$ in (31) and put $g(f, q, s) = \infty$ if such $k$ does not exist.

We obtain the following direct consequence of Theorem 9.

**Theorem 23.** Let $0 < \varepsilon, \eta \leq 1$ be arbitrary numbers and let $\gamma_\eta$ and $\delta(\varepsilon, \eta)$ be defined by (11) and (14), respectively. Let $A \subseteq \mathbb{L}$ be an $\eta$-good affine subspace of dimension $s$ over $\mathbb{K}$ with

$$s \geq \varepsilon r.$$
If \( f \in \mathbb{L}[X] \) is a polynomial of the form (i) or (ii) as defined in Theorem\(^9\) then, for sufficiently large \( q' \), for \( k \geq 3 \) with
\[
\left( \frac{q'^\vartheta}{2} \right)^{k-2} > Dq'^{-s},
\]
where \( \vartheta \) is defined by (16) and \( D = \deg f \) in the case (i) and \( D = \deg g \) in the case (ii), we have
\[
g(f, q, s) \leq k.
\]

**Proof.** We use again exponential sums to count the number of solutions \( N_k \) of the equation (31), that is,
\[
N_k = \frac{1}{q'} \sum_{u \in \mathbb{L}} \sum_{x_1, \ldots, x_k \in \mathbb{A}} \psi\left( u\left( \sum_{i=1}^{k} f(x_i) - y \right) \right)
\]
and thus
\[
|N_k - q^{k-r}| \leq \frac{1}{q'} \sum_{u \in \mathbb{L}^*} |S_u|^k = \frac{1}{q'} \sum_{u \in \mathbb{L}^*} |S_u|^{k-2} |S_u|^2
\]
\[
\leq \frac{1}{q'} \sum_{u \in \mathbb{L}^*} |S_u|^{k-2} \sum_{x_1, x_2 \in \mathbb{A}} \psi(u(f(x_1) - f(x_2))),
\]
where
\[
S_u = \sum_{x \in \mathbb{A}} \psi uf(x).
\]
Using Theorem\(^9\) for the sum \( S_u \) and the estimate \( Dq^r \) (for fixed \( x_1 \in \mathbb{A} \), there are at most \( D \) zeros of \( f(x_1) - f(X) \)) for the inner sum, we obtain
\[
|N_k - q^{k-r}| \leq 2^{k-2} Dq^{(k-1)-r(k-2)},
\]
where \( \vartheta \) is defined by (16). Imposing now \( N_k > 0 \), we conclude the proof.

The statement for polynomials of the type (ii) in Theorem\(^9\) follows as \( l \) is a permutation \( p \)-polynomial as defined in Theorem\(^9\). \( \square \)

If \( D \) is fixed in Theorem\(^23\) then for
\[
k > \frac{r-s}{r} \vartheta^{-1} + 2
\]
and sufficiently large \( q' \) we have \( g(f, q, s) < k \).

Next we consider \( q = p \), and, for an integer \( n \leq N \), we have \( \xi_n \) defined by (25). We also study the question of the existence of a positive integer \( k \) such that for any \( y \in \mathbb{L}_n \), the equation
\[
f(\xi_{n_1}) + \cdots + f(\xi_{n_k}) = y
\]
is solvable in positive integers \( n_1, \ldots, n_k \leq N \). As above, we denote by \( G(f, p, N) \) the smallest such value of \( k \) and put \( G(f, p, N) = \infty \) if such \( k \) does not exist.
Corollary 24. Let \( f \in \mathbb{L}[X] \) be a polynomial of the form (i) or (ii) as defined in Theorem 9 and \( p^s - 1 \leq N < p^s \) for some \( s \leq r \) satisfying
\[
s \geq \varepsilon r,
\]
and assume the linear subspace \( \mathcal{L}_s \subseteq \mathbb{L} \) spanned by \( \omega_0, \ldots, \omega_{s-1} \) is \( \eta \)-good. Then, for sufficiently large \( p' \), for \( k \geq 3 \) with
\[
\left( \frac{p'^{r \vartheta}}{2} \right)^{k-2} > D p'^{-s+1},
\]
where \( \vartheta \) is defined by (16) and \( D = \deg f \) in the case (i) and \( D = \deg g \) in the case (ii), we have
\[
G(f, p, N) \leq k.
\]

Proof. As \( N \geq p^s - 1 \), we have that \( G(f, p, N) \leq g(f, p, s - 1) \), and thus we can apply directly Theorem 23 with \( s \) replaced with \( s - 1 \), and with \( q \) replaced by \( p \).

We note that Corollary 24 follows also by applying directly Theorem 21, however the estimate obtained would be slightly weaker.

8 Remarks and open questions

We note that we have been able to prove Theorem 19 only for polynomials of degree less than \( p \). The reason behind this is that when one iterates the polynomial \( f \) of the form (i) or (ii), the shape changes and thus we cannot apply anymore Theorem 9. It would be interesting to extend such a result for more general polynomials.

Theorem 15 can also be translated into the language of affine dispersers; see [1]. We consider \( q = p \) prime and \( \mathbb{L} = \mathbb{F}_{p^r} \), where \( r \) is prime.

Definition 3. A function \( f : \mathbb{L} \to \mathbb{F}_p \) is an \( \mathbb{F}_p \)-affine disperser for dimension \( s \) if for every affine subspace \( A \) of \( \mathbb{L} \) of dimension at least \( s \), we have \( \# f(A) > 1 \).

As a direct consequence of Theorem 15, we obtain the following result.

Corollary 25. Let \( 0 < \varepsilon, \eta \leq 1 \) and let \( f \in \mathbb{L}[X] \) be a polynomial as defined in (i) or (ii) of Theorem 9. Then \( \pi(f) \), where \( \pi : \mathbb{L} \to \mathbb{F}_p \) is a nontrivial \( \mathbb{F}_p \)-linear map, is an affine disperser for dimension greater than \( \varepsilon r \).

We note that condition (15) shows that the larger \( \varepsilon \) is, the smaller the degree \( d \) is, where \( d \) is defined as in Theorem 15. For example, if
\[
\varepsilon = \frac{1}{2} \quad \text{and} \quad \eta \leq \frac{4}{5215},
\]
then one has $d > \delta(1/2, \eta) = \gamma_{\eta}^{-1} + 3 = 156453$. Furthermore, if

$$\epsilon = \frac{1}{3} \quad \text{and} \quad \eta \leq \frac{4}{5215}$$

then $d > \delta(1/3, \eta) = 2\gamma_{\eta}^{-1} + 3 = 312903$.

As mentioned in [22], obtaining analogues of Theorem 9 and thus of the rest of the results of this paper, for rational functions, is an important open direction. For this one has to obtain estimates for the exponential sum

$$S = \sum_{x \in \mathcal{L}} \psi(h(x)),$$

where $h \in \mathbb{L}(X)$ is a rational function and $\psi$ a nontrivial additive character. Even the case $h(X) = X^{-1}$ is still open.

Also of interest is obtaining estimates for

$$S = \sum_{x \in \mathcal{G}} \psi(h(x)),$$

where $\mathcal{G}$ is a multiplicative subgroup of $\mathbb{L}^*$. We note that for the prime field case, such a result would follow from [2, Theorem 1].

Of interest is also a multivariate analogue of Theorem 15, that is, given $F \in \mathbb{L}[X_1, \ldots, X_n]$ and $A_1, \ldots, A_n, B$ affine subspaces of $\mathbb{L}$, estimate the size of $F(A_1, \ldots, A_n) \cap B$.

Acknowledgements. The author would like to thank Igor Shparlinski for suggesting some extensions of initial results, and for his important comments on earlier versions of the paper. The author is also grateful to the Max Planck Institute for Mathematics for hosting the author for two months during the program “Dynamics and Numbers” when important progress on this paper was made. Finally, the author is grateful to the anonymous referee for helpful comments which improved the exposition.

During the preparation of this paper the author was supported by the UNSW Vice Chancellor’s Fellowship.

REFERENCES

[1] E. Ben-Sasson and S. Kopparty, Affine dispersers from subspace polynomials, SIAM J. Comput. 41 (2012), 880–914.

[2] J. Bourgain, Mordell’s exponential sum estimate revisited, J. Amer. Math. Soc. 18 (2005), 477–499.
[3] J. Bourgain, *On exponential sums in finite fields*, in *An Irregular Mind*, János Bolyai Mathematical Society, Budapest, 2010, pp. 219–242.

[4] J. Bourgain and A. Glibichuk, *Exponential sum estimates over a subgroup in an arbitrary finite field*, J. Anal. Math. **115** (2011), 51–70.

[5] M.-C. Chang, *Polynomial iteration in characteristic p*, J. Funct. Anal. **263** (2012), 3412–3421.

[6] M.-C. Chang, *Expansions of quadratic maps in prime fields*, Proc. Amer. Math. Soc. **142** (2014), 85–92.

[7] M.-C. Chang, *Sparsity of the intersection of polynomial images of an interval*, Acta Arith. **165** (2014), 243–249.

[8] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, *Points on curves in small boxes and applications*, Michigan Math. J. **63** (2014), 503–534.

[9] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, *On the concentration of points of polynomial maps and applications*, Math. Z. **272** (2012), 825–837.

[10] J. Cilleruelo and I. E. Shparlinski, *Concentration of points on curves in finite fields*, Monatsh. Math. **171** (2013), 315–327.

[11] J. Cipra, *Waring’s number in a finite field*, Integers **9** (2009), 435–440.

[12] J. Cipra, T. Cochrane and C. G. Pinner, *Heilbronn’s Conjecture on Waring’s number mod p*, J. Number Theory **125** (2007), 289–297.

[13] T. Cochrane and C. Pinner, *Sum-product estimates applied to Waring’s problem mod p*, Integers **8** (2008), A46, 1–18.

[14] H. Delange, *Sur les fonctions q-additives ou q-multiplicatives*, Acta Arith. **21** (1972), 285–298.

[15] M. Drmota, *The joint distribution of q-additive functions*, Acta Arith. **100** (2001), 17–39.

[16] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. **13** (1967/1968), 259–265.

[17] J. H. Silverman and B. Viray, *On a uniform bound for the number of exceptional linear subvarieties in the dynamical Mordell-Lang conjecture*, Math. Res. Letters. **20** (2013), 547–566.

[18] H. Weyl, *Über die Gleichverteilung von Zahlen mod Eins*, Math. Ann. **77** (1916), 313–352.
[27] T. D. Wooley, *Translation invariance, exponential sums, and Waring’s problem*, in *Proceedings of the International Congress of Mathematicians, Vol. II*, Kyung Moon Sa, Seoul, 2014, pp. 505–529.

[28] T. D. Wooley, *Multigrade efficient congruencing and Vinogradov’s mean value theorem*, Proc. London Math. Soc. (3) 111 (2015), 519–560.

[29] B. Wu and Z. Liu, *Linearized polynomials over finite fields revisited*, Finite Fields Appl. 22 (2013), 79–100.

*Alina Ostafe*

**SCHOOL OF MATHEMATICS AND STATISTICS**
**UNIVERSITY OF NEW SOUTH WALES**
**SYDNEY, NSW 2052, AUSTRALIA**
email: alina.ostafe@unsw.edu.au

(Received November 1, 2015)