Multiplicative Energy of Polynomial Images of Intervals Modulo q *†

Kyle Castro and Mei-Chu Chang ‡

October 26, 2016

Abstract

Given a smooth integer q, we use existing upper bounds for character sums to find a lower bound for the size of a multiplicative subgroup of the integers modulo q which contains the image of an interval of consecutive integers $I \subset \mathbb{Z}_q$ under a polynomial $f \in \mathbb{Z}[X]$.

1 Introduction

In this paper we give a result in the spirit of Shparlinski's theorem, [12, Theorem 7], through the application of the Graham-Ringrose Theorem as improved by Chang [2]. In [12] lies an improvement to an earlier result of Shparlinski and Gómez-Pérez, [7, Theorem 7], which discusses the greatest lower bound for the order of a subgroup of a finite field containing the image of an interval of consecutive integers under a rational function. There are various bounds for the number of images of consecutive polynomial values which belong to a given multiplicative subgroup (see [3], [5], and [7]); [12, Theorem 7] shows that the size of the intersection discussed above is dependent on the size of the subgroup of the finite field $\mathbb{F}_p$.

Theorem. (Shparlinski) Let $f(X) \in \mathbb{F}_p[X]$ be a square-free quadratic polynomial. For any interval I of consecutive integers and a subgroup G of $\mathbb{F}_p^*$, we have

$$|f(I) \cap G| \leq (1 + |I|^{3/4} p^{-1/8}) |G|^{1/2} p^{o(1)},$$

as $|I| \to \infty$.

While the previous theorem uses a fact about the arithmetic p-norm (see [12, Lemma 5]) which is found using Minkowski's Second Theorem in [6], we take a different approach to prove our main result. The following theorem uses the convention that $\pi_q(\cdot)$ is an operator with functional arguments which evaluates the function modulo q.

*2010 *Mathematics Subject Classification.* 11L26, 11L40.

†*Key words.* character sums, polynomial images, subgroups of finite fields

‡Research partially financed by the NSF Grant DMS 1301608.

Theorem 1.1. Given an integer m and $\epsilon > 0$, let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree d. For a sufficiently large square-free integer $q > q(\epsilon)$, take $I \subset \mathbb{Z}_q$ to be an interval of consecutive integers with $d < (\log |I|)^{1/8}$ such that

(1) for all $p|q$, $p < q^{\frac{1}{160d^4m^{2d}}}$

(2) $\log\log q > 16d^4m^{2d}$.

If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| \geq \min\{|I|^{m/2}, q^{1-\epsilon}\}$.

Note that for a prime modulus, [12, Theorem 7] is nontrivial if $|I| > p^{1/2}$; however, assuming the modulus is smooth, Theorem 1.1 is nontrivial for smaller intervals as well. Furthermore, we can restate Theorem 1.1 in the form of [12, Theorem 7] as an upper bound for the number of images of consecutive values which belong to a multiplicative subgroup of $\mathbb{Z}_q$. In the following corollary $o(|I|) = \epsilon|I|$ for any $\epsilon > 0$ as $|I|$ approaches infinity.

Corollary 1.2. Given an integer q and a polynomial $f(X) \in \mathbb{Z}[X]$, let G be a multiplicative subgroup of $\mathbb{Z}_q^*$ and take $I \subset \mathbb{Z}_q$ to be an interval of consecutive integers. Then,

$$|f(I) \cap G| \leq \frac{|I|}{\varphi(q)}|G| + o(|I|).$$

These theorems have relevance in polynomial dynamics as well as in the study of Dirichlet characters. More specifically, [12, Theorem 7] can be generalized in the study of the frequency of elements in the orbit of iterations of f which belong to a subfield of the finite field $\mathbb{F}_{q^r}$ (see [10] and [11]). Moreover, the bounds above give nontrivial bounds for the size of a character sum of a polynomial,

$$\left|\sum_{x\in I} \chi(f(x))\right|$$

as discussed in [4]. While incomplete character sums over an interval are being studied thoroughly, the notion of character sums with polynomial arguments can be improved with results such as these.

Before we begin discussing the preparations needed to prove our main result, we list the notation which will be used throughout the paper.

1. $\omega(q)$ is the number of distinct prime divisors of the integer q.

2. $V(J)$ represents the variety, or common zero set, of a set of functions J.

3. $\pi_q(\cdot)$ will be used as an operator with functional arguments which evaluates the function mod q.

4. $E(A_1, \ldots, A_m) = |\{(a_1, a_1', \ldots, a_m, a_m') \in A_1^2 \times \cdots \times A_m^2 : a_1 \cdots a_m = a_1' \cdots a_m'\}|$ is the multiplicative energy of m sets.

5. The logarithmic height of a polynomial is the maximum logarithm of the modulus of the coefficients of the polynomial.

6. δ, ϵ, c, and c' are various constants with δ, $\epsilon > 0$. Furthermore, the constant p will always be considered as prime and the constant q will be a composite integer with any added conditions stated as needed.

7. $A = o(B)$ is equivalent to the statement that $|A| \leq \epsilon|B|$ for any $\epsilon > 0$ as the given parameter tends to infinity.

8. $A \ll B$ is equivalent to the statement $|A| \leq c|B|$ for some constant c.

2 Preparations

We now discuss some preparations needed for the proof of the main theorem. First, we need a sharp arithmetic version of Hilbert's Effective Nullstellensatz Theorem [9, Theorem 1].

Theorem 2.1. (Krick, Pardo, and Sombra) Let $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials of degree at most D and logarithmic height at most H. If $V(P_1, \ldots, P_m) = \emptyset$ in $\mathbb{C}^n$, then there exists a positive integer b and polynomials $Q_1, \ldots, Q_m \in \mathbb{Z}[X_1, \ldots, X_n]$ such that

$$b = \sum_{i=1}^{m} Q_i P_i \tag{2.1}$$

and

$$\log b \leq 4n(n+1)D^n[H + \log m + (n+7)\log(n+1)D]. \tag{2.2}$$

We will also use the following result on the number of factorizations in a generalized arithmetic progression [1, Proposition 3].

Theorem 2.2. (Chang) Given integers $c_0, c_1, \ldots, c_d$ and $J_1, \ldots J_d \geq 1$ a generalized arithmetic progression P is

$$P = \{c_0 + \sum_{i=1}^{d} k_i c_i | k_i \in \mathbb{Z}, 0 \leq k_i \leq J_i\}.$$

Let $r_h(n)$ be the number of representations of the integer n as a product of h elements in P. If $J = \max_i J_i$, then for all $n \in \mathbb{Z}$

$$r_h(n) < e^{C_{d.h} \log J / \log\log J}$$

where $C_{d.h}$ is a constant depending on d and h.

Another tool used in obtaining the lower bound found in this paper will be the improvement to the Graham-Ringrose Theorem for character sums [2, Theorem 3$''$]. To discuss [2, Theorem 3$''$], we need the notion of an admissible pair.

Definition 2.3. (Chang) Given a prime p and a polynomial $f \in \mathbb{Z}[x]$, we say p is a *good* prime (or f is *p-good*) if f mod p has a simple root or a simple pole. Moreover, for $\bar{q}|q_r$ such that $\bar{q} > \sqrt{q_r}$, the pair $(f, \bar{q})$ is *q_r-admissible* if

$$p > \sqrt{\log q_r} \text{ for all } p|\bar{q}$$

and

$$\prod_{\substack{p|\bar{q} \\ \text{p is good}}} p > \frac{\bar{q}}{q_r^\tau}, \text{ where } \tau = \frac{10}{\log\log q_r}.$$

Theorem 2.4. (Chang) Assume $q = q_1 \cdots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$ and q_r square-free. Factor $\chi = \chi_1 \cdots \chi_r$ where $\chi_i \pmod{q_i}$ is arbitrary for $i < r$ and primitive for $i = r$. Let $N < q$ and assume

(a) for all $p|q$, $p < N^{1/10}$;

(b) $\log N > C\frac{\log q}{\log\log q}$.

Let

$$f(x) = \prod_j (x - b_j)^{c_j}, \ c_i \in \{-1, 1\} \text{ for some } i, \ d = \deg f = \sum |c_j|.$$

Suppose that (f, q_r) is admissible. Furthermore, assume that

(c) $d = \deg f < (\log q_r)^{1/8}$.

Then,

$$\left| \sum_{x=1}^{N} \chi(f(x)) \right| \ll N e^{-(\log q_r)^{1-c}/\log\log q_r}.$$

We would like to point out that in the factorization of q in the previous theorem, one can assume that up to reordering $q_i < q_j$ for $i < j$. It is also important to note that the assumptions (a) and (b) are not the assumptions of [2, Theorem 3″] as stated; that is, (a) and (b) are the stronger assumptions of [2, Theorem 3] as discussed in [2, Remark 3.1]. Moreover, we take a moment to discuss how the assumptions of [2, Theorem 3”] can be further weakened.

Remark 2.5. In Definition 2.3, the function is required to have a simple root or pole to ensure that $f \pmod{p}$ is not an k^{th} power of a polynomial; this assumption allows for the use of Weil's estimate on the complete character sum $\left|\sum_{x=1}^{q} \chi(f(x))\right|$ where χ is a multiplicative character of order $k > 1$. It is possible to change the definition of a good prime as follows.

Definition 2.6. Given a prime p and a polynomial $f \in \mathbb{Z}[x]$, we say p is *good* if $f \pmod{p}$ is not an k^{th} power of a polynomial.

Using Definition 2.6 we can remove the assumption that $c_i \in \{-1, 1\}$ for some i in Theorem 2.4 since its primary purpose is to ensure $f(x)$ is not an k^{th} power of a polynomial. Now since

$$|\{\chi : \chi \text{ is a multiplicative character of order } k\}| = C(d)$$

(where $C(d)$ is a constant depending d), we can consider any polynomial in $\mathbb{Z}[X]$ and omit those characters of order k so that the conclusion of [2, Theorem 3″] still holds.

The following lemmas will be also useful; the first is a result on the multiplicative energy of several sets which follows from the Cauchy–Schwarz inequality.

Lemma 2.7. Given subsets $A_1, \ldots, A_m$ of a multiplicative group,

$$|A_1 \cdots A_m| \geq \frac{|A_1|^2 \ldots |A_m|^2}{E(A_1, \ldots, A_m)}.$$

Proof. Notice

$$\sum_{x \in A_1 \cdots A_m} \big|\{(x_1, \ldots, x_m) \in A_1 \times A_2 \times \cdots \times A_m : x_1 x_2 \cdots x_m = x\}\big| \geq |A_1||A_2| \cdots |A_m|.$$

However by the Cauchy-Schwarz inequality

$$\left(\sum_{x \in A_1 \cdots A_m} \big|\{(x_1, \ldots, x_m) \in A_1 \times A_2 \times \cdots \times A_m : x_1 x_2 \cdots x_m = x\}\big| \right)^2$$

$$\leq |A_1 \cdots A_m| \sum_{x \in A_1 \cdots A_m} |\{(x_1, \ldots, x_m) \in A_1 \times A_2 \times \cdots \times A_m : x_1 x_2 \cdots x_m = x\}|^2.$$

However

$$\sum_{x \in A_1 \cdots A_m} |\{(x_1, \ldots, x_m) \in A_1 \times A_2 \times \cdots \times A_m : x_1 x_2 \cdots x_m = x\}|^2$$

$$\leq \sum_{x \in A_1 \cdots A_m} |\{(x_1, x_1', \ldots, x_m, x_m') \in A_1^2 \times \cdots \times A_m^2 : x_1 \cdots x_m = x = x_1' \cdots x_m'\}|$$

so that

$$|A_1 \cdots A_m| \geq \frac{|A_1|^2 \ldots |A_m|^2}{E(A_1, \ldots, A_m)}.$$

□

Finally, we give a lower bound on the size of the image of an interval under a polynomial $f \pmod{q}$.

Lemma 2.8. Given a square-free integer q, an interval of consecutive integers $I \subset \mathbb{Z}_q$, and a monic polynomial f of degree d

$$|\pi_q f(I)| \geq \frac{|I|}{d^{\omega(q)}}. \tag{2.3}$$

Proof. For each $y \in \mathbb{Z}_q$, consider

$$|\{x \in I : f(x) \equiv y \pmod{q}\}| = \prod_{p|q} |\{x \in I : f(x) \equiv y \pmod{p}\}| \leq d^{\omega(q)}.$$

Since $|\pi_q f(I)| \geq \frac{|I|}{\max\limits_{y \in \mathbb{Z}_q} |\{x \in I : f(x) \equiv y \pmod{q}\}|}$, we have

$$|\pi_q f(I)| \geq \frac{|I|}{d^{\omega(q)}}$$

as desired. □

3 Proofs

We will prove Theorem 1.1 using two propositions.

Proposition 3.1. Given an integer m, let $f(X) = X^d + C_{d-1}X^{d-1} + \ldots + C_1X + C_0 \in \mathbb{Z}[X]$ be a monic polynomial of degree d. For a square-free integer q and an interval $I \subset \mathbb{Z}_q$ of consecutive integers such that

(i) $d < (\log |I|)^{1/8}$

(ii) $|I| < q^{1/16d^4m^{2d}}$.

If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| > |I|^{m/2}$.

Proof. First take $q_1|q$ so that $q_1 \geq |I|$ (and hence $|I| = |\pi_{q_1}(I)|$), but $\frac{q_1}{p} < |I|$ for some prime $p|q_1$. For each ordered $2m$-tuple, $\vec{h} = (h_1, \ldots, h_{2m}) \in I^{2m}$, define the polynomial $P_{\vec{h}}(\vec{a}) \in \mathbb{Z}[\vec{a}]$ with indeterminates $\vec{a} = (a_0, \ldots, a_{d-1})$ by

$$P_{\vec{h}}(\vec{a}) := \prod_{i=1}^{m} g(h_i) - \prod_{j=m+1}^{2m} g(h_j)$$

where $g(h_k) = h_k^d + a_{d-1}h_k^{d-1} + \ldots + a_0$ for $1 \leq k \leq 2m$. Let $\vec{C} = (C_0, C_1, \ldots, C_{d-1}) \in \mathbb{Z}^d$, then define $E = \{\vec{h} \in I^{2m} : P_{\vec{h}}(\vec{C}) \equiv 0 \pmod q\}$ and let J be the ideal generated by $P_{\vec{h}}$ for $\vec{h} \in E$. Then by Lemma 2.7,

$$|G| \geq \left| \prod_{i=1}^{m} \pi_q f(I) \right| \geq \frac{|\pi_q f(I)|^{2m}}{|E|}. \tag{3.1}$$

Notice that Lemma 2.8 gives, $|\pi_{q_1} f(I)| \geq \frac{|I|}{d^{\omega(q_1)}}$; however since q_1 is square-free and $\frac{q_1}{p} < |I|$, for q_1 sufficiently large

$$\omega(q_1) = \omega(\frac{q_1}{p}) + 1 \leq \big(1 + o(1)\big)\frac{\log(\frac{q_1}{p})}{\log\log(\frac{q_1}{p})} + 1 \leq \frac{\log |I|}{\log\log |I|} + 1$$

so that

$$|\pi_{q_1} f(I)| \geq \frac{1}{d}|I|^{1-\frac{\log d}{\log\log |I|}}.$$

Now assume $|G| \leq |I|^{m/2}$. Then (3.1) gives that

$$|E| \geq \frac{|\pi_{q_1} f(I)|^{2m}}{|G|} \geq d^{-2m}|I|^{\frac{3m}{2} - \frac{2m\log d}{\log\log |I|}} > \frac{|I|^{\frac{5m}{4}}}{\log |I|^{\frac{m}{4}}} \tag{3.2}$$

where the last inequality follows from the fact that (i) gives that $d^{-2m} > \log |I|^{-\frac{m}{4}}$ and $\frac{2m \log d}{\log\log |I|} < \frac{m}{4}$. However, using Theorem 2.2, for any $\vec{z} = (z_0, \ldots, z_{d-1}) \in \mathbb{C}^d$ we have

$$|\{\vec{h} \in I^{2m} : P_{\vec{h}}(\vec{z}) = 0\}| < |I|^{m+\epsilon_{d,m}} \tag{3.3}$$

for q sufficiently large. So, (3.2) and (3.3) together give that for each $\vec{z} \in \mathbb{C}^d$ there exists $\vec{h} \in E$ such that $P_{\vec{h}}(\vec{C}) \equiv 0 \pmod{q}$, but $P_{\vec{h}}(\vec{z}) \neq 0$. Therefore, $V(J) = \emptyset$. Thus, by Theorem 2.1 there exists an integer b with

$$0 < \log b < 4d(d+1)m^d(\log |I|^d + \log |E| + (d+7)\log(d+1)m) \tag{3.4}$$

and polynomials $Q_{\vec{h}} \in \mathbb{Z}[\vec{a}]$ for all $\vec{h} \in E$ such that

$$b = \sum_{\vec{h} \in E} Q_{\vec{h}} P_{\vec{h}}. \tag{3.5}$$

Note $(d+7)\log(d+1)m < d(d+1)m \log |I|$ and $|E| < |I|^{2m}$, so that (3.4) is bounded by $16d^4m^{2d} \log |I|$ giving $0 < b < |I|^{16d^4m^{2d}}$. Evaluating the sum in (3.5) at $\vec{C}$ gives that $b \equiv 0 \pmod{q}$ so that

$$q \leq b < |I|^{16d^4m^{2d}} \tag{3.6}$$

which contradicts (ii). □

Remark 3.2. Note that by assuming $\pi_{q_1} f(I) \subset G$ for G a subgroup of $\mathbb{Z}_{q_1}^*$ where q_1 is as above, Proposition 3.1 holds for wider range of moduli than the smooth q of Theorem 1.1.

Moreover, Proposition 3.1 is a generalization of [8, Lemma 6] with explicit constants and a square-free modulus; that is, assuming $|I| < p^{(c/m)^{2d+1}}$ for some absolute constant c, [8, Lemma 6] gives that $|G| > |I|^m e^{-c(d,m)\frac{\log |I|}{\sqrt{\log\log |I|}}}$.

Proposition 3.3. *Given a sufficiently large square-free integer $q = q_1 \dots q_r$, take $f(X) \in \mathbb{Z}[X]$ to be a monic and q_r-admissible polynomial of degree d. Let $I \subset \mathbb{Z}_q$ be an interval of consecutive integers such that*
(i) $\log |I| > \log q / \log\log q$
(ii) for all $p|q$, $p < |I|^{1/10}$.
If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| \geq q^{1-\epsilon}$ provided $q > q(d, \epsilon)$.

Proof. Let $S = \{\chi : \chi$ is a multiplicative character modulo q and $\chi(a) = 1$ for all $a \in G\}$. Then,

$$|S| = \frac{\varphi(q)}{|G|}. \tag{3.7}$$

Moreover, since $\pi_q f(I) \subset G$, we have that $\chi(f(h)) = 1$ for all $h \in I$. Thus,

$$\sum_{h \in I} \chi(f(h)) = |I|. \tag{3.8}$$

Notice that for any $\chi \in S$ there exists a $q'|q$ such that χ is a primitive character mod q'. Therefore if $|I| \leq q'$, (3.8) is impossible unless assumption (c) of Theorem 2.4 is violated; that is $q_r < c(d)$. Again, up to re-indexing $q_r > q_i$ for all i; this gives a bound for q in terms of d so that $|S| < c'(d)$. Thus (3.7) gives $|G| > \dfrac{\varphi(q)}{c'(d)}$ which gives $|G| > q^{1-\epsilon}$ provided $q > q(d, \epsilon)$.

On the other hand, if $|I| > q'$, we can separate the character sum in (3.8) as follows; let $I' \subset I$ be a complete residue system mod q' so that using [2, Weil's Theorem'] we have

$$\left|\sum_{h\in I}\chi(f(h))\right| = \left|\sum_{x\in I'}\chi(f(x)) + \sum_{x\in I\setminus I'}\chi(f(x))\right| < d^{\omega(q')}\sqrt{q'} + (N - q')$$

which contradicts (3.8) unless $\sqrt{q'} \leq d^{\omega(q')}$. Thus, the characters $\chi \in S$ which are primitive for a small q' can be omitted. That is, if the characters discussed in this case were a significant portion of the set S, then $|S| < c''(d)$ giving a bound on $|G|$ as before. □

Moreover, we can state Proposition 3.3 without the mention of an admissible pair.

Proposition 3.4. Given $f(X) \in \mathbb{Z}[X]$ a monic polynomial of degree d, let q be a squarefree integer and $I \subset \mathbb{Z}_q$ be an interval of consecutive integers such that
(i′) $\log|I| > \log q/\log\log q$
(ii′) for all $p|q$, $p < |I|^{1/10}$
If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| \geq q^{1-\epsilon}$ provided $q > q(d,\epsilon)$.

Remark 3.5. Proposition 3.4 need not mention $f(x)$ being q_r-admissible as is assumed in Proposition 3.3. Since

$$\prod_{\substack{p|q\\ p<\sqrt{\log q}}} p < q^{1/10}$$

as discussed in [2, Remark 3.1], we can omit the assumption that $p > \sqrt{\log q}$. Thus, after the omission of the characters of order r where d is a multiple of r (as discussed in Remark 2.5), we have that $f(x)$ is q-admissible.

Proof of Theorem 1.1. We have two cases. If $|I| < q^{1/16d^4m^{2d}}$, we can apply Proposition 3.1. If $|I| \geq q^{1/16d^4m^{2d}}$, then the assumptions (1) and (2) of Theorem 1.1 give (i′) and (ii′) of Proposition 3.4 which proves Theorem 1.1. □

We conclude with the proof of Corollary 1.2 as stated in the introduction.

Proof of Corollary 1.2. Define $I' = \{x \in I : f(x) \in G\}$ and let $S = \{\chi : \chi$ is a character on $\mathbb{Z}_q^*$ and $\chi(a) = 1$ for all $a \in G\}$. Consider

$$\left|\sum_{x\in I'}\sum_{\chi\in S}\chi(f(x))\right| = |I'||S|. \tag{3.9}$$

On the other hand, using $I'(\cdot)$ as the indicator function for the set I' we have

$$\left|\sum_{x\in I'}\sum_{\chi\in S}\chi(f(x))\right| = \left|\sum_{x\in I}\sum_{\chi\in S}I'(x)\chi(f(x))\right|.$$

Then the Cauchy–Schwarz inequality gives

$$\begin{aligned}\left|\sum_{x\in I}\sum_{\chi\in S} I'(x)\chi(f(x))\right| &\le |I'|^{1/2}\left(\sum_{x\in I}\left|\sum_{\chi\in S}\chi(f(x))\right|^2\right)^{1/2}\\ &= |I'|^{1/2}\sum_{x\in I}\sum_{\chi\in S}\sum_{\chi'\in S}\chi(f(x))\overline{\chi'}(f(x))\\ &= |I'|^{1/2}\left(\sum_{x\in I}\sum_{\chi=\chi'\in S}\chi(f(x))\overline{\chi'}(f(x))+\sum_{x\in I}\sum_{\substack{\chi,\chi'\in S\\ \chi\neq\chi'}}\chi(f(x))\overline{\chi'}(f(x))\right)\\ &\le |I'|^{1/2}[|I||S|+(|S|^2-|S|)o(|I|)]^{1/2}.\end{aligned}$$

So after a substitution of (3.9), we have

$$|I'||S|^2 \le |I||S| + (|S|^2-|S|)o(|I|)$$

which gives

$$|I'| \le \frac{|I|}{|S|} + o(|I|) = \frac{|I|}{\varphi(q)}|G| + o(|I|) \text{ by (3.7).}$$

□

References

[1] M-C. Chang, *Factorization in Generalized Arithmetic Progressions and Application to the Erdős-Szemerédi Sum-Product Problems*, Geom. Funct. Anal., 13 (2003), pp. 720–736.

[2] M-C. Chang, *Short Character Sums for Composite Moduli*, Journal d'Analyse Mathematique 123, 1–33 (2014).

[3] 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. Vol. 63 (2014), 503-534.

[4] M.-C. Chang and I. E. Shparlinski, *Double Character Sums over Subgroups and Intervals*, Bull. Aust. Math. Soc. Vol 90: 3, 376-390 (2014).

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

[6] D. Gómez-Pérez and J. Gutierrez, *On the Linear Complexity and Lattice Test of Nonlinear Pseudorandom Number Generators*, Applied Algebra and Number Theory, Cambridge Univ. Press, Cambridge, (2014), 91–101.

[7] D. Gómez-Pérez and I. E. Shparlinski, *Subgroups Generated by Rational Functions in Finite Fields*, Monatsh. Math., (2015), v.176, 241-253.

[8] G. Ivanyos, M. Karpinski, M. Santha, N. Saxena, and I. E. Shparlinski, *Polynomial Interpolation and Identity Testing From High Powers Over Finite Fields*, Preprint (2015).

[9] T. Krick, L. M. Pardo, and M. Sombra, *Sharp Arithmetic Nullstellensatz*, Duke Math. J. 109 (2001), no. 3, 521–598.

[10] A. Ostafe, *Polynomial Values in Affine Subspaces Over Finite Fields*, Preprint, (2014), available from arXiv:1410.1252.

[11] O. Roche-Newton and I. E. Shparlinski, *Polynomial Values in Subfields and Affine Subspaces of Finite Fields*, Quart. J. Math., (2015), v.66, 693-706.

[12] I. E. Shparlinski, *Polynomial Values in Small Subgroups of Finite Fields*, Revista Matem. Iberoamer., (to appear).

[13] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge: Cambridge UP, 2006.

K. Castro (Corresponding author), Department of Mathematics, University of California, Riverside, CA 92521

E-mail address, kcastro@math.ucr.edu

M-C. Chang, Department of Mathematics, University of California, Riverside, CA 92521

E-mail address, mcc@math.ucr.edu