Canad. Math. Bull. Vol. 58 (4), 2015 pp. 774–786
http://dx.doi.org/10.4153/CMB-2015-036-2

Character Sums Over Bohr Sets

Brandon Hanson

Abstract. We prove character sum estimates for additive Bohr subsets modulo a prime. These estimates are analogous to the classical character sum bounds of Pólya–Vinogradov and Burgess. These estimates are applied to obtain results on recurrence mod p by special elements.

1 Introduction

Let p be a prime number and let $\mathbb{F}_p$ be the finite field with p elements. A non-trivial multiplicative character modulo p is a homomorphism $\chi\colon \mathbb{F}_p^\times \to \mathbb{C}^\times$ which is non-constant. We may abuse notation and view χ as a function on the integers defined by $n \mapsto \chi(n \bmod p)$ and $\chi(n) = 0$ when $p \mid n$. Given a subset $A \subset \mathbb{F}_p$, we are interested in the sum

$$S(\chi) = \sum_{a \in A} \chi(a).$$

Since χ takes values on the unit circle, it is always true that $|S(\chi)| \leq |A|$ and when A is a subgroup of $\mathbb{F}_p^\times$ this bound is best possible. However, for the typical set A we expect that $|S(\chi)|$ is about $\sqrt{|A|}$. So, to some extent, the size of $S(\chi)$ is a measure of multiplicative structure of A. For instance, the number of solutions to $ab = cd$ with all variables in A is given by $\frac{1}{p-1}\sum_\chi |S(\chi)|^4$.

There are classical estimates for $S(\chi)$ when A is an interval. The first result in this direction is due independently to Pólya and Vinogradov. Before stating it, we recall Vinogradov's asymptotic notation. For sequences X_n and Y_n, we take $X_n \ll Y_n$ to mean that $X_n/Y_n \leq c$ for some positive constant c (we shall also write $X_n = O(Y_n)$ to mean the same thing). For sequences X_n and Y_n, we take $X_n = o(Y_n)$ to mean that $X_n/Y_n \to 0$. The following results should be thought of as $p \to \infty$.

Theorem (Pólya-Vinogradov) *Let χ be a non-trivial multiplicative character modulo p. Then*

$$\Big|\sum_{M \leq n \leq M+N} \chi(n)\Big| \ll \sqrt{p}\log p.$$

This estimate is better than the trivial estimate provided $N \gg \sqrt{p}\log p$ and is simple to prove. In [P], Paley proved that the bound is, in fact, nearly sharp. One needs to work harder to get non-trivial estimates for shorter intervals. The best result in this direction is due to Burgess.

Received by the editors October 14, 2014; revised January 21, 2015.
Published electronically July 24, 2015.
AMS subject classification: **11L40**, 11T24, 11T23.
Keywords: character sums, Bohr sets, finite fields.

Theorem (Burgess) *Let χ be a non-trivial multiplicative character modulo p. Then for any positive integer k and $\varepsilon > 0$, we have*

$$\Big|\sum_{M\le n\le M+N}\chi(n)\Big| \ll_{k,\varepsilon} N^{1-1/k}p^{(k+1)/4k^2+\varepsilon}.$$

This result is better than trivial provided $N \gg p^{1/4+\delta}$, which can be seen by taking the parameter k to be sufficiently large. Obtaining estimates for even shorter intervals remains a major open problem in analytic number theory. The interested reader is referred to [IK, Chapter 12].

It is invariance under small translations that allows one to prove such theorems. Similar theorems are proved for arithmetic progressions using the same methods. In this paper we prove analogous theorems for sets exhibiting strong additive structure, namely additive Bohr sets.

2 Statement of Results and Applications

2.1 Main Results

Given a subset $\Gamma \subset \mathbb{F}_p$ and a parameter $\varepsilon > 0$, we define the Bohr set

$$B = B(\Gamma,\varepsilon) = \Big\{x \in \mathbb{F}_p : \Big\|\frac{xr}{p}\Big\| \le \varepsilon \text{ for each } r \in \Gamma\Big\}.$$

Here $\|\cdot\|$ denotes the distance to the nearest integer. Elements $x \in B(\Gamma,\varepsilon)$ dilate Γ into a short interval, and the additive structure of this interval carries over to B. Bohr sets will be discussed further in Section 2.

In Section 3 we obtain the following analog of the Pólya–Vinogradov estimate; it is non-trivial for large Bohr sets.

Theorem 2.1 (Pólya–Vinogradov for Bohr sets) *Let $B = B(\Gamma,\varepsilon)$ be a Bohr set with $|\Gamma| = d$. Then for any non-trivial multiplicative character χ,*

$$\Big|\sum_{x\in B}\chi(x)\Big| \ll_d \sqrt{p}(\log p)^d.$$

This result is comparable to [Sh] in which a Pólya–Vingradov estimate is established for generalized arithmetic progressions of rank d. For non-trivial estimates when the Bohr set is on the order of $\sqrt{p}$ or smaller, we appeal to Burgess' method. We are able to prove non-trivial results provided the Bohr set satisfies a certain niceness condition known as *regularity*; see Definition 3.5.

Theorem 2.2 (Burgess for Bohr sets) *Let $B = B(\Gamma,\varepsilon)$ be a regular Bohr set with $|\Gamma| = d$. Let $k \ge 1$ be an integer and let χ be non-trivial multiplicative character. When $|B| \ge \sqrt{p}$, we have the estimate*

$$\Big|\sum_{x\in B}\chi(x)\Big| \ll_{k,d} |B|\cdot p^{5d/16k^2+o(1)}\Big(\frac{|B|}{\varepsilon^d p}\Big)^{5/16k}\Big(\frac{p}{|B|}\Big)^{-1/8k}.$$

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

When $|B| < \sqrt{p}$, we have the estimate

$$\Big|\sum_{x\in B}\chi(x)\Big| \ll_{k,d} |B|\cdot p^{5d/16k^2+o(1)}\Big(\frac{|B|}{\varepsilon^d p}\Big)^{5/16k}\Big(\frac{|B|^5}{p^2}\Big)^{-1/8k}.$$

The statement appears complicated, but usually one has $|B| \approx \varepsilon^d p$, so the middle factor in the estimate is harmless. If the rank d is bounded, one can take k much larger than d and obtain a non-trivial estimate in the range $|B| \gg p^{2/5+\delta}$ for some positive δ. This is comparable to character sum estimates of M.-C. Chang for generalized arithmetic progressions of comparable rank proved in [C]. As in her proof, we make use of sum-product phenomena in $\mathbb{F}_p$.

2.2 Applications

Recall that Dirichlet's approximation theorem states that for real numbers $\alpha_1,\dots,\alpha_d$ there is an integer $n \le Q$ so that $\max_k\{\|n\alpha_k\|\} \le Q^{-1/d}$. Schmidt proved in [Sch] that, at the cost of weakening the approximation, we can take n to be a perfect square. Specifically, he proved the following theorem.

Theorem *Given real numbers $\alpha_1,\dots,\alpha_d$ and Q a positive integer, there is an integer $1 \le n \le Q$ and a positive absolute constant c such that*

$$\max_{1\le k\le d}\{\|n^2\alpha_k\|\} \ll dQ^{-c/d^2}.$$

This result was also proved by Green and Tao in [GT] and extended to different systems of polynomials in [LM]. An elementary proof of a slightly weaker estimate was also given in [CLR].

When Γ is a subset of $\mathbb{F}_p$ and $\varepsilon > 0$, then the elements of $B(\Gamma,\varepsilon)$ are precisely the elements guaranteed by Dirichlet's approximation theorem. Here we are replacing approximation in the continuous torus $\mathbb{R}/\mathbb{Z}$ with approximation in the discrete torus $\mathbb{F}_p$. We will prove the following $\mathbb{F}_p$ analog of Schmidt's theorem.

Theorem 2.3 (Recurrence of k-th powers) *Let Γ be a set of d integers and let p be a prime. There is an integer $x \le p$ for which*

$$\max_{r\in\Gamma}\Big\{\Big\|x^k\frac{r}{p}\Big\|\Big\} \ll_d p^{-1/2d}\log p\cdot k^{1/d}.$$

In a similar fashion, we can prove a result about recurrence of primitive roots.

Theorem 2.4 (Recurrence of primitive roots) *Let Γ be a set of d integers and let p be a prime. There is an integer $1 < x < p$ that generates $\mathbb{F}_p^\times$ and such that*

$$\max_{r\in\Gamma}\Big\{\Big\|x\frac{r}{p}\Big\|\Big\} \ll_d \frac{p^{1/2d}\log p}{\phi(p-1)^{1/d}}.$$

The remainder of this article is structured as follows. In the next section we recall necessary facts from Fourier analysis in $\mathbb{F}_p$, character sums, Bohr sets and their

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

properties, and sum-product theory. In Section 3 we give the proof of Theorem 2.1 and in Section 4 the proof of Theorem 2.2. In Section 5 we present the applications to recurrence.

3 Preliminaries

In this section we describe necessary results from discrete Fourier analysis, character sums, the theory of Bohr sets, and sum-product theory in $\mathbb{F}_p$.

3.1 Discrete Fourier Analysis

The results in this section are standard. The interested reader is referred to [TV, Chapter 4]. We define $e_p(a) = e^{2\pi ia/p}$, which is p-periodic as a function on $\mathbb{Z}$ and so well-defined on $\mathbb{F}_p$. For $f: \mathbb{F}_p \to \mathbb{C}$ and $q \geq 1$ we have the L^q norm

$$\|f\|_q = \Big(\frac{1}{p}\sum_{x\in\mathbb{F}_p} |f(x)|^q\Big)^{1/q}.$$

The Fourier transform of a function f at $t \in \mathbb{F}_p$ is defined as

$$\widehat{f}(t) = \sum_{x\in\mathbb{F}_p} f(x)e_p(-tx).$$

Lemma 3.1 (Properties of the Fourier Transform) *Let $f, g: \mathbb{F}_p \to \mathbb{C}$; then we have*

(i) *Fourier inversion:* $f(x) = \frac{1}{p}\sum_{t\in\mathbb{F}_p} \widehat{f}(t)e_p(tx)$.

(ii) *Parseval's identity:* $\sum_{x\in G} f(x)\overline{g(x)} = \frac{1}{p}\sum_{t\in\mathbb{F}_p} \widehat{f}(t)\overline{\widehat{g}(t)}$.

(iii) *Plancherel's identity:* $\sum_{x\in G} |f(x)|^2 = \frac{1}{p}\sum_{t\in\mathbb{F}_p} |\widehat{f}(t)|^2$.

3.2 Character Sums

Here we recall well-known facts concerning complete character sums over finite fields. For details, we refer the reader to [IK, Chapter 11]. Suppose χ is a non-trivial multiplicative character. For $x \in \mathbb{F}_p$ the Fourier transform of χ at x is

$$\tau(\chi, -x) = \sum_{y\in\mathbb{F}_p} \chi(y)e_p(-xy),$$

which is known as the Gauss sum. By expanding the square modulus, it is not hard to prove the following lemma.

Lemma 3.2 *For non-zero $x \in \mathbb{F}_p$ we have $|\tau(\chi, -x)| = \sqrt{p}$ and $\tau(\chi, 0) = 0$.*

In the proof of Theorem 2.2 we shall need Weil's estimate for character sums with polynomial arguments.

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

Theorem (Weil) *Let $f \in \mathbb{F}_p[x]$ be a polynomial with r distinct roots over $\overline{\mathbb{F}_p}$. Then if χ has order l and provided f is not an l-th power over $\overline{\mathbb{F}_p}[x]$, we have*

$$\Big|\sum_{x\in\mathbb{F}_p} \chi(f(x))\Big| \le r\sqrt{p}.$$

3.3 Bohr Sets

The material here can be found in [TV, Section 4.4]. Suppose $\Gamma \subset \mathbb{F}_p$ and $\varepsilon > 0$ is a parameter; then the Bohr set $B(\Gamma, \varepsilon)$ is defined as

$$B(\Gamma,\varepsilon) = \left\{ x \in \mathbb{F}_p : \left\| \frac{xr}{p} \right\| \le \varepsilon \text{ for each } r \in \Gamma \right\}.$$

Here $\|\cdot\|$ is the distance to the nearest integer, which in this case will be a rational number with denominator p. There are a few ways to view Bohr sets. If we let I be the integer interval $[-\varepsilon p, \varepsilon p] \cap \mathbb{Z}$ (thought of as a subset of $\mathbb{F}_p$), then $B(\Gamma, \varepsilon)$ consists of those elements $x \in \mathbb{F}_p$ such that $x\Gamma = \{xr : r \in \Gamma\} \subset I$. Since $\|\theta\| \approx |e^{2\pi i\theta} - 1|$, another way to view $B(\Gamma, \varepsilon)$ is as the set of $x \in \mathbb{F}_p$ such that $|e_p(xr) - 1| \ll \varepsilon$ for $r \in \Gamma$. In this way, $B(\Gamma, \varepsilon)$ is approximately the kernel of the homomorphism $T\colon \mathbb{F}_p \to \mathbb{T}^d$ given by $T(x) = (e_p(rx))_{r\in\Gamma}$. Since $\mathbb{F}_p$ has no non-trivial additive subgroups, Bohr sets are often used as a close approximation.

We have the following estimates on the size of a Bohr set.

Lemma 3.3 *Let $\Gamma \subset \mathbb{F}_p$ with $|\Gamma| = d$ and $\varepsilon > 0$. Then*

$$|B(\Gamma,\varepsilon)| \ge \varepsilon^d p \quad \text{and} \quad |B(\Gamma, 2\varepsilon)| \le 4^d |B(\Gamma,\varepsilon)|.$$

Since $B(\Gamma, \varepsilon) + B(\Gamma, \varepsilon) \subset B(\Gamma, 2\varepsilon)$ by the triangle inequality, we can immediately deduce the following bound.

Corollary 3.4 *Let $\Gamma \subset \mathbb{F}_p$ with $|\Gamma| = d$ and $\varepsilon > 0$. Then*

$$|B(\Gamma,\varepsilon) + B(\Gamma,\varepsilon)| \le 4^d |B(\Gamma,\varepsilon)|.$$

Given $\Gamma \subset \mathbb{F}_p$, there are certain values of ε for which $|B(\Gamma, \varepsilon + \kappa)|$ varies nicely for small values κ. More precisely, we define a regular Bohr set as follows.

Definition 3.5 Suppose $\Gamma \subset \mathbb{F}_p$ is a set of size d; we say ε is a *regular value* for Γ if whenever $|\kappa| < \frac{1}{100d}$ we have

$$1 - 100d|\kappa| \le \frac{|B(\Gamma, (1+\kappa)\varepsilon)|}{|B(\Gamma,\varepsilon)|} \le 1 + 100d|\kappa|.$$

We say the Bohr set $B(\Gamma, \varepsilon)$ is regular.

The natural first question to ask is if a given Γ has any regular values. In fact, a result due to Bourgain ([B]) shows that one can always find a regular value close to any desired radius.

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

Lemma 3.6 (Bourgain) *Let Γ be a set of size d and let $\delta \in (0,1)$. There is an $\varepsilon \in (\delta, 2\delta)$ that is regular for Γ.*

The crucial property of regular Bohr sets is that they are almost invariant under translation by Bohr sets of small radius. This allows us to replace a character sum over a Bohr set by something "smoother".

Corollary 3.7 *Let $B(\Gamma,\varepsilon)$ be a regular Bohr set with $|\Gamma| = d$. If $\eta \le \delta\varepsilon/200d$ for some $0 < \delta < 1$, then for any natural number $n \ge 1$ and $y_1, \dots, y_n \in B(\Gamma,\eta)$ and we have*

$$\sum_{x\in\mathbb{F}_p} |\mathbf{1}_{B(\Gamma,\varepsilon)}(x + y_1 + \cdots + y_n) - \mathbf{1}_{B(\Gamma,\varepsilon)}(x)| \le n\delta|B(\Gamma,\varepsilon)|.$$

Proof By the triangle inequality it suffices to prove the result for $n = 1$. For $y = y_1$, the value of $|\mathbf{1}_{B(\Gamma,\varepsilon)}(x + y) - \mathbf{1}_{B(\Gamma,\varepsilon)}(x)|$ is 0 unless exactly one of x and $x + y$ lies in $B(\Gamma,\varepsilon)$ in which case there is a contribution of 1. However, if the latter happens, then $x \in B(\Gamma, \varepsilon+\eta) \setminus B(\Gamma,\varepsilon-\eta)$. Owing to the regularity of $B(\Gamma,\varepsilon)$, for any $y \in B(\Gamma,\eta)$, there is a contribution of at most

$$\left|B\Big(\Gamma,\varepsilon\Big(1+\frac{\delta}{200d}\Big)\Big)\right| - \left|B\Big(\Gamma,\varepsilon\Big(1-\frac{\delta}{200d}\Big)\Big)\right| \le \delta\big|B(\Gamma,\varepsilon)\big|. \qquad \blacksquare$$

3.4 A Sum-product Estimate

In order to execute a Burgess type argument for character sums, we shall need estimates on what is known as multiplicative energy. For two sets $A, B \subset \mathbb{F}_p$ we call

$$E_\times(A,B) = \big|\big\{(a_1,a_2,b_1,b_2) \in A\times A\times B\times B : a_1b_1 = a_2b_2\big\}\big|$$

the multiplicative energy between A and B. We observe that if

$$r_\times(x) = \big|\{(a,b) \in A\times B : ab = x\}\big|,$$

then

$$E_\times(A,B) = \sum_{x\in\mathbb{F}_p} r_\times(x)^2.$$

These quantities appear regularly in additive combinatorics and are closely related to $|A\cdot B|$. Specifically, we shall need to bound the multiplicative energy between two Bohr sets. To achieve this, make use of the following estimate from [R].[1] The estimate presented here is not explicitly mentioned, but it is proved on the way to proving Theorem 1 of that article.

Theorem 3.8 (Rudnev) *Let $A \subset \mathbb{F}_p$ satisfy $|A| < \sqrt{p}$. Then*

$$E_\times(A) \ll |A||A+A|^{7/4}\log|A|.$$

[1]Recently, Rudnev's sum-product estimate was improved in [RNRS]. Turning this bound into an energy estimate may give a small improvement on Theorem 2.2. However, sum-product estimates are still far from optimal, and an approach incorporating the structure of Bohr sets would likely be more effective.

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

4 The Pólya–Vinogradov Argument

The Pólya–Vinogradov argument is an effective way of obtaining good character sum estimates over sets whose Fourier transform has a small L^1 norm. Indeed, suppose $A \subset \mathbb{F}_p$; then by Parseval's identity and the Gauss sum estimate we have

$$\Big|\sum_{a\in A}\chi(a)\Big| = \Big|\frac{1}{p}\sum_{x\in\mathbb{F}_p}\widehat{\mathbf{1}_A}(x)\tau(\chi,-x)\Big| \le \sqrt{p}\|\widehat{\mathbf{1}_A}\|_1.$$

One can get a fairly strong estimate on this L^1 norm of Bohr sets. We do so now and establish Theorem 2.1.

Proof of Theorem 2.1 Write $\Gamma = \{r_1,\dots,r_d\}$ and $\boldsymbol{r} = (r_1,\dots,r_d)$. Since $x \in B$ if and only if $rx \in [-\varepsilon p, \varepsilon p] = I$, for each $r \in \Gamma$, we have

$$\begin{aligned}\widehat{\mathbf{1}_B}(y) &= \sum_{x\in B} e_p(-yx) = \sum_{x\in\mathbb{F}_p}\prod_{k=1}^{d}\mathbf{1}_I(xr_k)e_p(-yx)\\ &= \frac{1}{p^d}\sum_{x\in\mathbb{F}_p}\prod_{k=1}^{d}\sum_{v_k\in\mathbb{F}_p}\widehat{\mathbf{1}_I}(v_k)e_p(v_kr_kx)e_p(-yx)\\ &= \frac{1}{p^d}\sum_{\boldsymbol{v}\in\mathbb{F}_p^d}\widehat{\mathbf{1}_{I^d}}(\boldsymbol{v})\sum_{x\in\mathbb{F}_p}e_p(x(\boldsymbol{v}\cdot\boldsymbol{r}-y)) = \frac{1}{p^{d-1}}\sum_{\substack{\boldsymbol{v}\in\mathbb{F}_p^d\\ \boldsymbol{v}\cdot\boldsymbol{r}=y}}\widehat{\mathbf{1}_{I^d}}(\boldsymbol{v}).\end{aligned}$$

Here we have set $I^d = I \times^{\times d} \cdots \times I$ and

$$\widehat{\mathbf{1}_{I^d}}((v_1,\dots,v_d)) = \widehat{\mathbf{1}_I}(v_1)\cdots\widehat{\mathbf{1}_I}(v_d).$$

Plugging this in, we obtain

$$\|\widehat{\mathbf{1}_B}\|_1 \le \frac{1}{p^d}\sum_{y\in\mathbb{F}_p}\sum_{\substack{\boldsymbol{v}\in\mathbb{F}_p^d\\ \boldsymbol{v}\cdot\boldsymbol{r}=y}}|\widehat{\mathbf{1}_{I^d}}(\boldsymbol{v})| = \frac{1}{p^d}\sum_{\boldsymbol{v}\in\mathbb{F}_p^d}|\widehat{\mathbf{1}_{I^d}}(\boldsymbol{v})| = \|\widehat{\mathbf{1}_I}\|_1^d.$$

As in the classical proof of the Pólya–Vinogradov inequality,

$$|\widehat{\mathbf{1}_I}(v)| = \Big|\sum_{k=-N}^{N}e_p(-kv)\Big| = \Big|\sum_{k=0}^{2N+1}e_p(-kv)\Big| = \Big|\frac{e_p(v(2N+2)-1}{e_p(v)-1}\Big| \ll \frac{p}{v}.$$

It follows that $\|\widehat{\mathbf{1}_I}\|_1 \ll \log p$, and the theorem is proved. ∎

Remark If one takes $\Gamma = \{1\}$ and $\varepsilon = N/p$ for some positive integer N, then $B(\Gamma,\varepsilon) = [-N,N]$, thought of as a subset of $\mathbb{F}_p$. This recovers the classical Pólya–Vinogradov estimate

$$\sum_{|n|\le N}\chi(n) \ll \sqrt{p}\log p.$$

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

5 The Burgess Argument

In this section we prove Theorem 2.2. The method is the same as in the proof of Burgess' estimate for character sums over an interval, which can be found in [IK, Chapter 12]. The main difference lies in estimating the multiplicative energy between two Bohr sets and for this we use the sum-product result quoted in Section 2. Sum-product estimates were used for the same purpose in [C] with methods taken from [KS]. It is likely that the argument presented here is not efficient. Indeed, Bohr sets are highly structured, and the current sum-product estimates are expected to be sub-optimal. For example, one of the energy estimates proved in [C] was improved in [K] using the geometry of numbers. We were unable to adapt that argument to the present situation.

First, we establish a general version of Burgess' argument, which is an application of Hölder's inequality and Weil's bound.

Lemma 5.1 *Let $A, B, C \subset \mathbb{F}_p$ and suppose χ is a non-trivial multiplicative character. Define*

$$r(x) = \big|\{(a,b) \in A \times B : ab = x\}\big|.$$

Then for any positive integer k, we have the estimate

$$\sum_{x\in\mathbb{F}_p} r(x)\Big|\sum_{c\in C}\chi(x+c)\Big| \le (|A||B|)^{1-1/k}E_\times(A,A)^{1/4k}E_\times(B,B)^{1/4k} \times \big(|C|^{2k}2k\sqrt{p} + (2k|C|)^k p\big)^{1/2k}.$$

Proof Call the left-hand side above S. Applying Hölder's inequality,

$$|S| \le \Big(\sum_{x\in\mathbb{F}_p} r(x)\Big)^{1-1/k}\Big(\sum_{x\in\mathbb{F}_p} r(x)^2\Big)^{1/2k}\Big(\sum_{x\in\mathbb{F}_p}\Big|\sum_{c\in C}\chi(x+c)\Big|^{2k}\Big)^{1/2k} = T_1^{1-1/k}T_2^{1/2k}T_3^{1/2k}.$$

Now T_1 is precisely $|A||B|$, and T_2 is the multiplicative energy $E_\times(A,B)$. By the Cauchy–Schwarz inequality, we have

$$E_\times(A,B) \le \sqrt{E_\times(A,A)E_\times(B,B)}.$$

Expanding T_3 and using that $\overline{\chi}(y) = \chi(y^{p-2})$, we have

$$T_3 = \sum_{c_1,\dots,c_{2k}\in C}\sum_x \chi\big((x-c_1)\cdots(x-c_k)(x-c_{k+1})^{p-2}\cdots(x-c_{2k})^{p-2}\big) = \sum_{c\in C^{2k}}\sum_x \chi\big(f_c(x)\big).$$

Here $f_c(t)$ is the polynomial

$$f_c(t) = (t-c_1)\cdots(t-c_k)(t-c_{k+1})^{p-2}\cdots(t-c_{2k})^{p-2}.$$

By Weil's theorem, $\sum_x \chi(f_c(x)) \le 2k\sqrt{p}$ unless f_c is an l-th power, where l is the order of χ. If any of the roots c_i of f_c is distinct, it occurs with multiplicity 1 or $p-2$, both of which are prime to l since l divides $p-1$. Hence f_c is an l-th power, provided all of its roots can be grouped into pairs. So, for all but at most $(2k)!/2^k k! \le (2k|C|)^k$

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

vectors $\boldsymbol{c}$, we have the estimate $2k\sqrt{p}$ for the inner sum. For the remaining $\boldsymbol{c}$ we bound the sum trivially by p. Hence,

$$T_3 \le |C|^{2k} 2k\sqrt{p} + (2k|C|)^k p. \qquad \blacksquare$$

Proof of Theorem 2.2 Suppose $\Gamma \subset \mathbb{F}_p$ has size d, and ε is a regular value for Γ. We may as well assume that $\Gamma \neq 0$, for otherwise $B = \mathbb{F}_p$ and the result is trivial. Write $B = B(\Gamma, \varepsilon)$ and let χ be a non-trivial character of $\mathbb{F}_p^\times$. Then we wish to estimate

$$S(\chi) = \sum_{x \in B} \chi(x).$$

We begin by first using Corollary 3.7. Let $\eta = p^{-1/k}\varepsilon/(200d)$ and let $y \in B(\Gamma, \eta)$. For any natural number $n \le p^{1/2k}$, we have

$$\begin{aligned} S(\chi) &= \sum_{x \in \mathbb{F}_p} \mathbf{1}_B(x)\chi(x) = \sum_{x \in \mathbb{F}_p} \mathbf{1}_B(x+ny)\chi(x) + O\big(n|B|p^{-1/k}\big) \\ &= \sum_{x \in B} \chi(x-ny) + O\big(n|B|p^{-1/k}\big). \end{aligned}$$

Averaging this over all values $1 \le n \le p^{1/2k}$ and all values $y \in B' = B(\Gamma, \eta) \setminus \{0\}$, we obtain

$$S(\chi) \ll \frac{1}{p^{1/2k}|B'|} \sum_{x \in B} \sum_{y \in B'} \sum_{1 \le n \le p^{1/2k}} \chi(x-ny) + O\big(|B|p^{-1/2k}\big).$$

It remains to estimate

$$T(\chi) \ll \frac{1}{p^{1/2k}|B'|} \sum_{x \in B} \sum_{y \in B'} \sum_{1 \le n \le p^{1/2k}} \chi(x-ny).$$

We begin by assuming that $|B| < \sqrt{p}$. Then, applying Lemma 5.1 (where $r(x)$ is now the number of ways of writing x as ab with $a \in B$ and $b \in (B')^{-1}$), we have

$$\begin{aligned} |T(\chi)| &\ll \frac{1}{p^{1/2k}|B'|} \sum_{x \in \mathbb{F}_p} r(x) \Big| \sum_{1 \le n \le p^{1/2k}} \chi(x-n) \Big| \\ &\le \frac{(|B||B'|)^{1-1/k} E_\times(B,B)^{1/4k} E_\times(B',B')^{1/4k}}{p^{1/2k}|B'|} \\ &\qquad \times \left(2kp^{3/2} + (2k)^k p^{3/2}\right)^{1/2k} \\ &\le |B|(|B||B'|)^{-3/4k} (|B+B||B'+B'|)^{7/16k} (\log p)^{1/2k} \sqrt{k} p^{1/4k} \end{aligned}$$

after applying Theorem 3.8. Applying Corollary 3.4, we get the bound

$$|T(\chi)| \ll |B|(|B||B'|)^{-5/16k} 4^{7d/8k} (\log p)^{1/2k} \sqrt{k} p^{1/4k}.$$

Using Lemma 3.3,

$$|B'| \ge \eta^d p = \left(\frac{\varepsilon}{p^{1/k} 200d}\right)^d p$$

so that

$$|T(\chi)| \ll_{d,k} |B| \cdot p^{5d/16k^2 + o(1)} \left(\frac{|B|}{\varepsilon^d p}\right)^{5/16k} \left(\frac{|B|^{5/2}}{p}\right)^{-1/4k}.$$

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

Now if $|B| \geq \sqrt{p}$, first split B into disjoint sets B_i with $\sqrt{p} \ll |B_i| < \sqrt{p}$. Then

$$|T(\chi)| \ll \frac{|B|}{\sqrt{p}} \cdot \frac{1}{p^{1/2k}|B'|} \max_i \sum_{x \in B_i} \sum_{y \in B'} \Big| \sum_{1 \leq n \leq p^{1/2k}} \chi(x - ny) \Big|.$$

Proceeding as before, this time bounding $|B_i| < \sqrt{p}$ and $|B_i + B_i| \leq |B + B|$, we obtain

$$\begin{aligned} |T(\chi)| &\ll |B|(\sqrt{p}|B'|)^{-3/4k}(|B+B||B'+B'|)^{7/16k}(\log p)^{1/2k}\sqrt{k}p^{1/4k} \\ &= \Big(\frac{|B|}{\sqrt{p}}\Big)^{3/4k}\Big(|B|\big(|B||B'|\big)^{-3/4k}\big(|B+B||B'+B'|\big)^{7/16k}\Big) \\ &\quad \times \Big((\log p)^{1/2k}\sqrt{k}p^{1/4k}\Big) \\ &\ll_{d,k} |B| \cdot p^{5d/16k^2+o(1)}\Big(\frac{|B|}{\varepsilon^d p}\Big)^{5/16k}\Big(\frac{p}{|B|}\Big)^{-1/8k}. \end{aligned}$$

■

It is worth remarking that the Burgess estimate just proved gives a genuine improvement over the Pólya–Vinogradov estimate in some cases. To see this, we need a Bohr set whose size is $|B| \approx \varepsilon^d p \approx p^\gamma$ with $2/5 < \gamma < 1/2$. To find such a set, we need only note that the bound in Lemma 3.3 is sharp on average. Averaging over all subsets of $\mathbb{F}_p$ of size d, we have (where I is the interval $[-\varepsilon p, \varepsilon p]$)

$$\begin{aligned} \frac{1}{\binom{p}{d}} \sum_{|A|=d} |B(A,\varepsilon)| &= \frac{1}{\binom{p}{d}} \sum_{|A|=d} \sum_{x \in \mathbb{F}_p} \prod_{a \in A} \mathbf{1}_I(ax) \\ &= \frac{1}{\binom{p}{d}} \sum_{|A|=d} \sum_{x \in \mathbb{F}_p^\times} \prod_{a \in A} \mathbf{1}_{x^{-1}I}(a) + O(1) \\ &= \frac{1}{\binom{p}{d}} \sum_{x \in \mathbb{F}_p^\times} \sum_{|A|=d} \prod_{a \in A} \mathbf{1}_{x^{-1}I}(a) + O(1). \end{aligned}$$

The inner sum vanishes unless $A \subset x^{-1}I$ in which case it contributes $\binom{|I|}{d}$. Thus the total sum is roughly $\binom{|I|}{d}\binom{p}{d}^{-1} p \asymp \varepsilon^d p$. It follows that for the typical choice of A of size d and appropriate choice of ε, which we can take to be regular by Lemma 3.6, we find a regular Bohr set with size in the desired range.

6 Application to Polynomial Recurrence

We are now going to prove Theorem 2.3 and Theorem 2.4. Their proofs will follow the standard method of counting with characters. First we prove an analog of Schmidt's theorem for squares. This proof is quite simple and does not need character sums, but it will give a good idea of what to aim for when we move to higher powers.

Let $\Gamma \subset \mathbb{F}_p$ be a set of size d and let $\varepsilon > 0$ be a parameter. Then $B = B(\Gamma, \varepsilon)$ contains a non-zero square provided $\varepsilon^{2d} p > 1$. To see this, observe that Bohr sets have the dilation property $xB = B(x^{-1}\Gamma, \varepsilon)$, which follows immediately from the definition of a Bohr set. If the non-zero elements of B are all non-squares, then for any non-square element x, $xB(\Gamma,\varepsilon) \cap B(\Gamma,\varepsilon) = \{0\}$. But this intersection contains $B(\Gamma \cup x^{-1}\Gamma, \varepsilon)$ which has size at least $\varepsilon^{2d} p$ by Lemma 3.3, yielding a contradiction. It follows that

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

there is a non-zero integer $1 \le a < p$ such that

$$\max_{r\in\Gamma}\left\{ \left\| a^2 \frac{r}{p} \right\| \right\} \ll p^{-1/2d}.$$

The above argument does not immediately generalize to higher powers, because there is no dichotomy; an element can be in any of the k cosets of the set of k-th powers. Instead, we will use Theorem 2.1 to find higher powers and primitive roots in Bohr sets.

Proof of Theorem 2.3 Write B for $B(\Gamma, \varepsilon)$. Observe that when $(k, p-1) = l$ then the k-th powers are the same as the l-th powers. So we suppose $k|(p-1)$ and K is the subgroup of $\mathbb{F}_p^\times$ consisting of the k-th powers. This group has index k. The problem is then showing that $B(\Gamma, \varepsilon) \cap K$ is non-empty. Let $K^\perp$ be the group of multiplicative characters that restrict to the trivial character on K. This group has size $|K^\perp| = k$. The Poisson Summation Formula, which can be found in [TV, Chapter 4], states that

$$\mathbf{1}_K(x) = \frac{1}{k} \sum_{\chi\in K^\perp} \chi(x).$$

Thus,

$$|K \cap B| = \frac{1}{k} \sum_{\chi\in K^\perp} \sum_{b\in B} \chi(b).$$

After extracting the contribution from the trivial character χ_0, we have

$$\left| |K \cap B| - \frac{|B|}{k} \right| \le \max_{\chi} |S(\chi)|,$$

where $S(\chi) = \sum_{b\in B} \chi(b)$ and the maximum is taken over all non-trivial characters $\chi \in K^\perp$. Thus if we can show that the maximum value of $|S(\chi)|$ is at most $\frac{|B|}{k}$, then B must contain an element of K. By Theorem 2.1, B contains a k-th powers provided $|B| \gg_d kp^{1/2}(\log p)^d$, which is certainly the case when $\varepsilon^d \gg_d kp^{-1/2}(\log p)^d$ in view of Lemma 3.3. Thus,

$$\max_{r\in\Gamma}\left\{ \left\| x^k \frac{r}{p} \right\| \right\} \ll_d p^{-1/2d} \log p \cdot k^{1/d}. \qquad \blacksquare$$

We now turn to primitive roots.

Proof of Theorem 2.4 We can also find primitive roots in a Bohr set. Recall that the group $\mathbb{F}_p^\times$ is cyclic and a primitive element of $\mathbb{F}_p$ is a generator of this group. Denote the primitive roots of $\mathbb{F}_p$ by $\mathcal{P}$. The characteristic function of $\mathcal{P}$ has a nice expansion in terms of characters, due to Vinogradov (see [LN, Exercise 5.14]):

$$\mathbf{1}_{\mathcal{P}}(x) = \frac{\phi(p-1)}{p-1} \sum_{d|(p-1)} \frac{\mu(d)}{\phi(d)} \sum_{\chi_d} \chi(x),$$

where ϕ is Euler's totient function and $\sum_{\chi_d}$ is the sum over all characters with order exactly d. Summing over the elements of a Bohr set B and extracting the contribution from the trivial character, we obtain

$$\left| |B \cap \mathcal{P}| - |B| \frac{\phi(p-1)}{p-1} \right| \ll_d \sqrt{p}(\log p)^d.$$

https://doi.org/10.4153/CMB-2015-036-2 Published online by Cambridge University Press

We deduce that B will contain a primitive root whenever

$$\varepsilon \gg \frac{p^{1/2d}}{\phi(p-1)^{1/d}} \cdot \log p 0.$$

Thus there is a primitive root $1 < x < p$ with

$$\max_{r\in\Gamma}\left\{ \left\| x\frac{r}{p} \right\| \right\} \ll_d \frac{p^{1/2d}\log p}{\phi(p-1)^{1/d}}. \qquad \blacksquare$$

We close by mentioning that use of Theorem 2.2 would allow for smaller choices of ε but for the factor $(|B|/\varepsilon^d p)^k$ appearing in the estimate. As we mentioned in the preceding section, this factor is usually harmless, but we wanted uniform results for all sets Γ, which comes more easily by way of Theorem 2.1.

Acknowledgments The author would like to thank John Friedlander for helpful discussion. He would also like to thank the anonymous referee for helpful comments and suggestions. Part of this research was performed while the author was visiting the Institute for Pure and Applied Mathematics (IPAM), which is funded by the National Science Foundation.

References

[B] J. Bourgain, *On triples in arithmetic progression*. Geom. Funct. Anal. **9**(1999), 968–984. http://dx.doi.org/10.1007/s000390050105

[BGK] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*. J. London Math. Soc. (2) **73**(2006), no. 2, 380–398. http://dx.doi.org/10.1112/S0024610706022721

[BKT] J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*. Geom. Funct. Anal. **14**(2004), no. 1, 27–57. http://dx.doi.org/10.1007/s00039-004-0451-1

[C] M.-C. Chang, *On a question of Davenport and Lewis and new character sum bounds in finite fields*. Duke Math. J. **145**(2008), no. 3, 409–442. http://dx.doi.org/10.1215/00127094-2008-056

[CLR] E. Croot, N. Lyall, and A. Rice, *A purely combinatorial approach to simultaneous polynomial recurrence modulo 1*. arxiv:1307.0779

[G] M. Z. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$. Int. Math. Res. Not. IMRN **2007**, no. 11, Art. ID rnm035.

[GT] B. Green and T. Tao, *New bounds for Szemerédi's theorem. II. A new bound for* $r_4(N)$. In: Analytic number theory, Cambridge University Press, Cambridge, 2009, pp. 180–204.

[IK] H. Iwaniec and E. Kowalski, *Analytic number theory*. American Mathematical Society Colloquium Publications, 53, American Mathematical Society, Providence, RI, 2004.

[KS] N. H. Katz and C.-Y. Shen, *A slight improvement to Garaev's sum product estimate*. Proc. Amer. Math. Soc. **136**(2008), no. 7, 2499–2504. http://dx.doi.org/10.1090/S0002-9939-08-09385-4

[K] S. V. Konyagin, *Estimates for character sums in finite fields*. (Russian) Mat. Zametki **88**(2010), no. 4, 529–542; translation in Math. Notes **88**(2010), no. 3–4, 503–515. http://dx.doi.org/10.4213/mzm8852

[LN] R. Lidl and H. Neiderreiter, *Finite fields*. Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997.

[LM] N. Lyall and A. Magyar, *Simultaneous polynomial recurrence*. Bull. Lond. Math. Soc. **43**(2011), no. 4, 765–785. http://dx.doi.org/10.1112/blms/bdr011

[P] R. E. A. C. Paley, *A theorem on characters*. J. Lond. Math. Soc. **S1-7**(1932), no. 1, 28. http://dx.doi.org/10.1112/jlms/s1-7.1.28

[RNRS] O. Roche-Newton, M. Rudnev, and I. Shkredov, *New sum-product type estimates over finite fields*. arxiv:1408.0542v1

[R] M. Rudnev, *An improved sum-product inequality in fields of prime order*. Int. Math. Res. Not. IMRN **2012**, no. 16, 3693–3705.

[Sch] W. M. Schmidt, *Small fractional parts of polynomials*. Regional Conference Series in Mathematics, 32, American Mathematical Society, 1977.
[Sh] X. Shao, *On character sums and exponential sums over generalized arithmetic progressions*. Bull. Lond. Math. Soc. **45**(2013), no. 3, 541–550. http://dx.doi.org/10.1112/blms/bds115
[TV] T. Tao and V. Vu, *Additive combinatorics*. Cambridge Studies in Advanced Mathematics, 105, Cambridge University Press, Cambridge, 2006. http://dx.doi.org/10.1017/CBO9780511755149

University of Toronto, Toronto, ON M5S 2E4
e-mail: bhanson@math.toronto.edu