A QUANTITATIVE RESULT ON DIOPHANTINE APPROXIMATION FOR INTERSECTIVE POLYNOMIALS

Neil Lyall[1]
Department of Mathematics, The University of Georgia, Athens, Georgia
lyall@math.uga.edu

Alex Rice
Department of Mathematics, University of Rochester, Rochester, New York
alex.rice@rochester.edu

Received: 3/1/14, Accepted: 11/30/14, Published: 6/15/15

Abstract

In this short note, we closely follow the approach of Green and Tao to extend the best known bound for recurrence modulo 1 from squares to the largest possible class of polynomials. The paper concludes with a brief discussion of a consequence of this result for polynomial structures in sumsets and limitations of the method.

1. Introduction

We begin by recalling the well-known Kronecker approximation theorem:

Theorem A (Kronecker Approximation Theorem). *Given $\alpha_1, \dots, \alpha_d \in \mathbb{R}$ and $N \in \mathbb{N}$, there exists an integer $1 \leq n \leq N$ such that*

$$\|n\alpha_j\| \ll N^{-1/d} \text{ for all } 1 \leq j \leq d.$$

Remark on Notation: In Theorem A above, and in the rest of this paper, we use the standard notations $\|\alpha\|$ to denote, for a given $\alpha \in \mathbb{R}$, the distance from α to the nearest integer and the Vinogradov symbol $\ll$ to denote "less than a constant times".

Kronecker's theorem is of course an almost immediate consequence of the pigeonhole principle: one simply partitions the torus $(\mathbb{R}/\mathbb{Z})^d$ into N "boxes" of side length at most $2N^{-1/d}$ and considers the orbit of $(n\alpha_1, \dots, n\alpha_d)$. In [3], Green and Tao presented a proof of the following quadratic analogue of the above theorem, due to Schmidt [9].

[1]NL was partially supported by Simons Foundation Collaboration Grant for Mathematicians 245792.

Theorem B (Simultaneous Quadratic Recurrence, Proposition A.2 in [3]). *Given $\alpha_1, \dots, \alpha_d \in \mathbb{R}$ and $N \in \mathbb{N}$, there exists an integer $1 \leq n \leq N$ such that*

$$\|n^2\alpha_j\| \ll dN^{-c/d^2} \quad \textit{for all} \quad 1 \leq j \leq d.$$

The argument presented by Green and Tao in [3] was later extended (in a straightforward manner) by the second author and Magyar in [6] to any system of polynomials without constant term.

Theorem C (Simultaneous Polynomial Recurrence, consequence of Proposition B.2 in [6]). *Given any system of polynomials $h_1, \dots, h_d$ of degree at most k with real coefficients and no constant term and $N \in \mathbb{N}$, there exists an integer $1 \leq n \leq N$ such that*

$$\|h_j(n)\| \ll k^2 dN^{-ck^{-C}/d^2} \quad \textit{for all} \quad 1 \leq j \leq d,$$

where $C, c > 0$ and the implied constant are absolute.

Such a recurrence result does not hold for every polynomial. Specifically, if $h \in \mathbb{Z}[x]$ has no root modulo q for some $q \in \mathbb{N}$, then $\|h(n)/q\| \geq 1/q$ for all $n \in \mathbb{Z}$, a local obstruction which leads to the following definition.

Definition 1. We say that $h \in \mathbb{Z}[x]$ is *intersective* if for every $q \in \mathbb{N}$, there exists $r \in \mathbb{Z}$ with $q \mid h(r)$. Equivalently, h is intersective if it has a root in the p-adic integers for every prime p.

Intersective polynomials include all polynomials with an integer root, but also include certain polynomials without rational roots, such as $(x^3 - 19)(x^2 + x + 1)$.

2. Recurrence for Intersective Polynomials

The purpose of this note is to extend the argument of Green and Tao [3] to establish the following quantitative improvement of a result of Lê and Spencer [4].

Theorem 1. *Given $\alpha_1, \dots, \alpha_d \in \mathbb{R}$, an intersective polynomial $h \in \mathbb{Z}[x]$ of degree k, and $N \in \mathbb{N}$, there exists an integer $1 \leq n \leq N$ with $h(n) \neq 0$ and*

$$\|h(n)\alpha_j\| \ll dN^{-c^k/d^2} \textit{ for all } 1 \leq j \leq d,$$

where $c > 0$ is absolute and the the implied constant depends only on h.

In [4], the right hand side is replaced with $N^{-\theta}$ for some $\theta = \theta(k, d) > 0$. Here we follow Green and Tao's [3] refinement of Schmidt's [9] lattice method nearly verbatim, beginning with the following definitions.

Definition 2. Suppose that $\Lambda \subseteq \mathbb{R}^d$ is a full-rank lattice. For any $t > 0$ and $x = (x_1, \dots, x_d) \in \mathbb{R}^d$, we define the *theta function*

$$\Theta_\Lambda(t,x) := \sum_{m\in\Lambda} e^{-\pi t|x-m|^2}.$$

Further, we define

$$A_\Lambda := \Theta_{\Lambda^*}(1,0) = \sum_{\xi\in\Lambda^*} e^{-\pi|\xi|^2} = \det(\Lambda)\sum_{m\in\Lambda} e^{-\pi|m|^2},$$

where $\Lambda^* = \{\xi \in \mathbb{R}^d \ : \xi\cdot m \in \mathbb{Z} \text{ for all } m \in \Lambda\}$ and the last equality follows from the Poisson summation formula. Finally, for a polynomial $h \in \mathbb{Z}[x]$, $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{R}^d$, and $N > 0$, we define

$$F_{h,\Lambda,\alpha}(N) := \det(\Lambda)\mathbb{E}_{1\leq n\leq N}\Theta_\Lambda(1, h(n)\alpha).$$

For the remainder of the discussion, we fix an intersective polynomial $h \in \mathbb{Z}[x]$ of degree k, and we let $K = 2^{10k}$. We use C and c to denote sufficiently large and small absolute constants, respectively, and we allow any implied constants to depend on h. By definition h has a root at every modulus, but we need to fix a particular root at each modulus in a consistent way, which we accomplish below.

Definition 3. For each prime p, we fix p-adic integers z_p with $h(z_p) = 0$. By reducing and applying the Chinese Remainder Theorem, the choices of z_p determine, for each natural number q, a unique integer $r_q \in (-q, 0]$, which consequently satisfies $q \mid h(r_q)$. We define the function λ on $\mathbb{N}$ by letting $\lambda(p) = p^m$ for each prime p, where m is the multiplicity of z_p as a root of h, and then extending it to be completely multiplicative.
For each $q \in \mathbb{N}$, we define the *auxiliary polynomial*, h_q, by

$$h_q(x) = h(r_q + qx)/\lambda(q),$$

noting that each auxiliary polynomial maintains integral coefficients.

As in [3], we make use of the following properties of F, only one of which needs to be tangibly modified due to the presence of a general intersective polynomial.

Lemma 1 (Properties of $F_{h_q,\Lambda,\alpha}$). *If $\Lambda \subseteq \mathbb{R}^d$, $\alpha \in \mathbb{R}^d$, and $q, N \in \mathbb{N}$, then*

(i) (Contraction of N) $F_{h_q,\Lambda,\alpha}(N) \gg cF_{h_q,\Lambda,\alpha}(cN)$ *for any* $c \in (10/N, 1)$.

(ii) (Dilation of α) $F_{h_q,\Lambda,\alpha}(N) \gg \frac{1}{q'}F_{h_{qq'},\Lambda,\lambda(q')\alpha}(N/q')$ *for any* $q' \leq N/10$.

(iii) (Stability) *If* $\tilde{\alpha} \in \mathbb{R}^d$ *with* $|\alpha - \tilde{\alpha}| < \epsilon/\max_{1\leq n\leq N}|h_q(n)|$ *and* $\epsilon \in (0,1)$*, then*

$$F_{h_q,\Lambda,\alpha}(N) \gg F_{h_q,(1+\epsilon)\Lambda,(1+\epsilon)\tilde{\alpha}}(N).$$

Proof. Property (i) follows immediately from the definition of F and the positivity of Θ, and property (iii) is exactly as in Lemma A.5 in [3]. For property (ii), by positivity of Θ, complete multiplicativity of λ, and the fact that $r_q \equiv r_{qq'} \bmod qq'$, we have

$$\begin{aligned} F_{h_q,\Lambda,\alpha}(N) &= \det(\Lambda)\mathbb{E}_{\substack{r_q+q\leq n\leq r_q+qN \\ n\equiv r_q \bmod q}}(1, h(n)\alpha/\lambda(q)) \\ &\geq \det(\Lambda)\mathbb{E}_{\substack{r_q+q\leq n\leq r_q+qN \\ n\equiv r_{qq'} \bmod qq'}}(1, h(n)\alpha/\lambda(q)) \\ &\gg \frac{1}{q'}\det(\Lambda)\mathbb{E}_{1\leq n\leq N/q'}\Theta_\Lambda\Big(1, \frac{h(r_{qq'}+qq'n)}{\lambda(qq')}\lambda(q')\alpha\Big) \\ &= \frac{1}{q'}F_{h_{qq'},\Lambda,\lambda(q')\alpha}(N/q'), \end{aligned}$$

as required. ☐

The key to the argument is the following "alternative lemma."

Lemma 2 (Schmidt's Alternative). *If $\Lambda \subseteq \mathbb{R}^d$ is a full-rank lattice, $\alpha \in \mathbb{R}^d$, and $q \leq N^{1/K}$, then one of the following holds:*

(i) $F_{h_q,\Lambda,\alpha}(N) \geq 1/2$

(ii) *There exists $q' \ll dA_\Lambda^{Ck}$ and a primitive $\xi \in \Lambda^* \setminus \{0\}$ such that*

$$|\xi| \ll \sqrt{d} + \sqrt{\log A_\Lambda}$$

and

$$\|q'\xi\cdot\alpha\| \ll A_\Lambda^{Ck}N^{-k}.$$

The proof of Lemma 2 is identical to that of the corresponding lemma in [3], once armed with the following result, which follows from Weyl's Inequality and observations of Lucier [5] on auxiliary polynomials.

Lemma 3. *If $\delta \in (0,1)$, $q \leq N^{1/K}$, and $|\mathbb{E}_{1\leq n\leq N}\ e^{2\pi i h_q(n)\theta}| \geq \delta$, then there exists $q' \ll \delta^{-k}$ such that $\|q'\theta\| \ll (\delta N)^{-k}$.*

Additionally, a proof of Lemma 3 is contained in Section 6.4 of [7]. Precisely as in [3], the alternative lemma gives the following inductive lower bound on F.

Corollary 1 (Inductive lower bound on $F_{h,\Lambda,\alpha}$). *If $\Lambda \subseteq \mathbb{R}^d$ is a full-rank lattice, $\alpha \in \mathbb{R}^d$, $N > (dA_\Lambda)^{C_0 k}$ for a suitably large absolute constant C_0, and $q < N^{1/K}$, then one of the following holds:*

(i) $F_{h_q,\Lambda,\alpha}(N) \geq 1/2$

(ii) *There exists* $\alpha' \in \mathbb{R}^{d-1}$*, a full-rank lattice* $\Lambda' \subseteq \mathbb{R}^{d-1}$*,* $N' \gg (dA_\Lambda)^{-Ck}N$*, and* $q' \ll (dA_\Lambda)^{Ck}$ *with*

$$A_{\Lambda'} \ll (\sqrt{d} + \sqrt{\log A_\Lambda})A_\Lambda \tag{1}$$

and

$$F_{h_q,\Lambda,\alpha}(N) \gg (dA_\Lambda)^{-Ck} F_{h_{qq'},\Lambda',\alpha'}(N'). \tag{2}$$

Finally, we use Corollary 1 to obtain a lower bound on $F_{h,\Lambda,\alpha}$ that is sufficient to prove Theorem 1.

Corollary 2. *If* $\alpha \in \mathbb{R}^d$*,* $\Lambda \subseteq \mathbb{R}^d$ *is a full-rank lattice with* $\det(\Lambda) \geq 1$*, and* $N > (dA_\Lambda)^{C_1 kKd}$ *for a suitably large absolute constant* C_1*, then*

$$F_{h,\Lambda,\alpha}(N) \gg (dA_\Lambda)^{-Ckd}.$$

Proof. Setting $\alpha_0 = \alpha$, $\Lambda_0 = \Lambda$, and $N_0 = N$, we repeatedly apply Corollary 1, obtaining vectors $\alpha_j \in \mathbb{R}^{d-j}$, lattices $\Lambda_j \subseteq \mathbb{R}^{d-j}$, and integers q_j, N_j for $j = 0, 1, \ldots$. Assuming that $N_j > (dA_{\Lambda_j})^{C_0 k}$ and $q_j \leq N_j^{1/K}$ throughout the iteration, which we will show to be the case shortly, we must either pass through case *(i)* of Proposition 1 at some point, or the iteration continues all the way to dimension 0. The worst bounds come from the latter scenario, and we note that $F_{h_{q_d},\Lambda_d,\alpha_d}(N_d) = 1$. Using (1) and the crude inequality $\sqrt{d} + \sqrt{\log X} \ll dX^{1/d}$, we see that $A_{\Lambda_j} \ll A_{\Lambda_0}^C$ throughout the iteration. Since $N_{j+1} \geq (dA_{\Lambda_j})^{-Ck}N_j$ and $q_{j+1} \ll (dA_{\Lambda_j})^{Ck}q_j$, we see that $N_j > (dA_{\Lambda_j})^{C_0 k}$ and $q_j \leq N_j^{1/K}$ throughout, provided $N \geq (dA_\Lambda)^{C_1 kKd}$ for suitably large C_1. From (2), the result follows. □

2.1. Proof of Theorem 1

Fix real numbers $\alpha_1, \ldots, \alpha_d \in \mathbb{R}$ and an intersective polynomial $h \in \mathbb{Z}[x]$ of degree k. Let R be a quantity to be chosen later, and apply Corollary 2 with $\alpha = (R\alpha_1, \ldots, R\alpha_d)$ and $\Lambda = R\mathbb{Z}^d$. By definition we have

$$A_\Lambda = R^d\Big(\sum_{m \in R\mathbb{Z}} e^{-\pi m^2}\Big) \leq (CR)^d,$$

so if $R \geq C_2 d$ and $N > C_2 R^{C_2 kKd^2}$ for suitably large C_2, Corollary 2 implies

$$F_{h,\Lambda,\alpha}(N) \gg R^{-Ckd^2}.$$

Since $\det(\Lambda) = R^d$, it follows from the definition of $F_{h,\Lambda,\alpha}$ that

$$\mathbb{E}_{1\le n\le N} \sum_{m\in R\mathbb{Z}^d} e^{-\pi|h(n)\alpha-m|^2} \gg R^{-Ckd^2}$$

The contribution from all n with $h(n) = 0$ is $\ll (CR)^d/N$, which is negligible if $N > C_2 R^{C_2 kKd^2}$. In this case we conclude that there exists $n \in \{1, \dots, N\}$ with $h(n) \neq 0$ and

$$\sum_{m\in R\mathbb{Z}^d} e^{-\pi|h(n)\alpha-m|^2} \gg R^{-Ckd^2} \tag{3}$$

Fixing such an n, if we had $|h(n)\alpha - m| > \sqrt{R}$ for all $m \in R\mathbb{Z}^d$, then we would have

$$e^{-\pi|h(n)\alpha-m|^2} \le e^{-\pi R^2/2} e^{-\pi|h(n)\alpha-m|^2/2} \tag{4}$$

for all $m \in R\mathbb{Z}^d$. By the Poisson summation formula, we have the identity

$$\sum_{m\in\Lambda} e^{-\pi t|h(n)\alpha-m|^2} = \frac{1}{t^{d/2}\det(\Lambda)} \sum_{\xi\in\Lambda^*} e^{-\pi|\xi|^2/t} e^{2\pi i\xi\cdot h(n)\alpha}. \tag{5}$$

Applying (4) and (5), we conclude that

$$\sum_{m\in R\mathbb{Z}^d} e^{-\pi|h(n)\alpha-m|^2} \le e^{-\pi R^2/2} \frac{2^{d/2}}{\det(\Lambda)} \sum_{\xi\in\Lambda^*} e^{-2\pi|\xi|^2} e^{2\pi i\xi\cdot h(n)\alpha} \le e^{-\pi R^2/2} 2^{d/2} \frac{A_\Lambda}{\det(\Lambda)},$$

which is $\ll e^{-\pi R^2/2}(CR)^d$, which contradicts (3) if $R > C_2 d$. Therefore, under this assumption on R, it must be the case that there exists $m \in R\mathbb{Z}^d$ with $|h(n)\alpha - m| \le \sqrt{R}$, which clearly implies that $\|h(n)\alpha_i\| \le 1/\sqrt{R}$ for all $1 \le j \le d$.
If $N \ge C_3 d^{C_3 kKd^2}$ for suitably large C_3, then the theorem follows by choosing $R = d^{-1} N^{c/d^2 kK}$ for a sufficiently small absolute constant $c > 0$. If instead $N < C_3 d^{C_3 kKd^2}$, then the theorem is trivial. □

3. Consequences and Limitations

3.1. Consequences for Sumsets Following Croot-Łaba-Sisask

Croot, Laba, and Sisask [1] displayed, using machinery from [2] and [8], that for sets $A, B \subseteq \mathbb{Z}$ of small doubling, there exists a low rank, large radius Bohr set T with the property that a shift of any (not too large) subset of T is contained in the sumset $A + B = \{a + b : a \in A, b \in B\}$. The theorems discussed in this paper imply the existence of particular polynomial configurations in Bohr sets, and hence can be incorporated with the techniques found in [1] to establish corresponding sumset results. Specifically, by replacing the Kronecker Approximation Theorem with Theorem 1 and C, respectively, in the proof of Theorem 1.4 in [1], one obtains the following results.

Theorem 2. *Suppose $h \in \mathbb{Z}[x]$ is an intersective polynomial of degree k, and $A, B \in \mathbb{Z}$ with*

$$|A+B| \leq K_A|A|, K_B|B|.$$

Then $A+B$ contains an arithmetic progression

$$\{x + h(n)\ell : 1 \leq \ell \leq L\}$$

with $x, \in \mathbb{Z}$, $n \in \mathbb{N}$, $h(n) \neq 0$ and

$$L \gg \exp\Big(c^k\Big(\frac{\log|A+B|}{K_B^2(\log 2K_A)^6}\Big)^{1/3} - C\log(K_A \log|A|)\Big),$$

where $C, c > 0$ are absolute constants, and the implied constant depends only on h.

Theorem 3. *Suppose $h_1, \ldots, h_m \in \mathbb{Z}[x]$ with $h_i(0) = 0$ and $\deg(h_i) \leq k$ for $1 \leq i \leq \ell$, and $A, B \in \mathbb{Z}$ with*

$$|A+B| \leq K_A|A|, K_B|B|.$$

Then $A+B$ contains a configuration of the form

$$\{x + h_i(n)\ell : 1 \leq i \leq m,\ 1 \leq \ell \leq L\}$$

with $x \in \mathbb{Z}$, $n \in \mathbb{N}$, $h_i(n) \neq 0$ for $1 \leq i \leq m$, and

$$L \gg \exp\Big(ck^{-C}\Big(\frac{\log|A+B|}{m^2K_B^2(\log 2K_A)^6}\Big)^{1/3} - C\log(mkK_A \log|A|)\Big),$$

where $C, c > 0$ and the implied constant are absolute.

Noting that if $A, B \subseteq [1, N]$ with $|A| = \alpha N$ and $|B| = \beta N$, then one can take $K_A = 2\alpha^{-1}$ and $K_B = 2\beta^{-1}$, yielding special cases of Theorems 2 and 3 phrased in terms of densities.

3.2. Limitations Toward Simultaneous Recurrence

Upon inspection of Theorems C and 1, and correspondingly Theorems 2 and 3, the natural question arises of the possibility of common refinements. Specifically, if $\alpha_1, \ldots, \alpha_d \in \mathbb{R}$ and $h_1, \cdots, h_m \in \mathbb{Z}[x]$ is a *jointly intersective* collection of polynomials, meaning the polynomials share a common root at each modulus, can one simultaneously control $\|h_i(n)\alpha_j\|$ for $1 \leq i \leq m$ and $1 \leq j \leq d$? In a qualitative sense, Lê and Spencer [4] answered this question in the affirmative, but in this context obstructions arise to the application of the methods found in [6] to establish a bound such as that found in Theorem 1.

For example, suppose $h_1(x) = b_0 + b_1x + b_2x^2$ and $h_2(x) = c_0 + c_1x + c_3x^3$. This system of polynomials is a "nice" system as defined in [4], but to apply the methods of [6] it is necessary to firmly control Gauss sums of the form

$$\sum_{n=1}^{N} e^{2\pi i(h_1(n)a_1+h_2(n)a_2)/q} = \sum_{n=1}^{N} e^{2\pi i\left(b_0a_1+c_0a_2+(b_1a_1+c_1a_2)n+b_2a_1n^2+c_3a_2n^3\right)/q}.$$

Control of this sum is lost if $b_1a_1 + c_2a_2$, b_2a_1, c_3a_2, and q all share a large common factor. While the argument allows us to control (b_1, b_2), (c_1, c_3), and (a_1, a_2, q), this does not prohibit the aforementioned fatal scenario. While it is likely that an analog of Theorem C holds for a jointly intersective collection of polynomials, it appears that new insight is required.

References

[1] E. Croot, I. Laba, O. Sisask, *Arithmetic progressions in sumsets and L^p almost periodicity*, Combinatorics, Probability, and Computing 22 (2013), 351-365.

[2] E. Croot, O. Sisask, *A probabilistic technique for finding almost-periods of convolutions*, Geom. Funct. Anal. 20 (2010), 1367-1396.

[3] B. Green, T. Tao, *New bounds for Szemerédi's theorem II. A new bound for $r_4(N)$*, Analytic number theory, 180-204, Cambridge Univ. Press, 2009.

[4] T. H. Lê, C. Spencer, *Intersective polynomials and Diophantine approximation*, Int. Math. Res. Notices (2012) doi:10.1093/imrn/rns242.

[5] J. Lucier, *Intersective Sets Given by a Polynomial*, Acta Arith. 123 (2006), 57-95.

[6] N. Lyall, À. Magyar, *Simultaneous polynomial recurrence*, Bull. Lond. Math. Soc. 43 (2011), no. 4, 765-785.

[7] A. Rice, *Improvements and extensions of two theorems of Sárközy*, Ph. D. thesis, University of Georgia, 2012. http://alexricemath.com/wp-content/uploads/2013/06/AlexThesis.pdf.

[8] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE 5 (2012), no. 3, 627-655.

[9] W. M. Schmidt, *Small fractional parts of polynomials*, CBMS Regional Conference Series in Math., **32**, Amer. Math. Soc., 1977.

[10] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge University Press, Second Edition, 1997.