

EXPANDING POLYNOMIALS ON SETS WITH FEW PRODUCTS

COSMIN POHOATA

ABSTRACT. In this note, we prove that if A is a finite set of real numbers such that $|AA| = K|A|$, then for every polynomial $f \in \mathbb{R}[x, y]$ we have that $|f(A, A)| = \Omega_{K, \deg f}(|A|^2)$, unless f is of the form $f(x, y) = g(M(x, y))$ for some monomial M and some univariate polynomial g .

1. INTRODUCTION

Given polynomials $f \in \mathbb{R}[x]$ and $g \in \mathbb{R}[x, y]$, and sets $A, B \subset \mathbb{R}$, we write

$$f(A) = \{f(a) : a \in A\} \quad \text{and} \quad g(A, B) = \{g(a, b) : a \in A, b \in B\}.$$

That is, $g(A, B)$ is the set of distinct values that can be obtained by applying g on the cartesian product $A \times B$. When $g(x, y) = x + y$ or $g(x, y) = xy$, the more convenient notation $g(A, B) = A + B$ or $g(A, B) = AB$ is generally preferred. This paper will be concerned with understanding the growth of sets such as $g(A, B)$ with respect to $|A|$ and $|B|$. We will only focus on polynomials over the reals, so our story begins with the result of Elekes and Rónyai, who in [8] uncovered that $|f(A, B)|$ must be asymptotically larger than $|A|$ or $|B|$, unless the polynomial $f \in \mathbb{R}[x, y]$ has one of the special forms $f = h(g_1(x) + g_2(y))$ and $f = h(g_1(x) \cdot g_2(y))$, for some $h, g_1, g_2 \in \mathbb{R}[x]$. The current best bound for this problem is the following one by Raz, Sharir, and Solymosi [11].

Theorem 1.1. *Let $A, B \subset \mathbb{R}$ be finite sets, and let $f \in \mathbb{R}[x, y]$ be of a constant degree. Then, unless $f = h(g_1(x) + g_2(y))$ or $f = h(g_1(x) \cdot g_2(y))$ for some $h, g_1, g_2 \in \mathbb{R}[x]$, we have*

$$|f(A, B)| = \Omega \left(\min \left\{ |A|^{2/3} |B|^{2/3}, |A|^2, |B|^2 \right\} \right).$$

Theorem 1.1 generalizes many problems from discrete geometry and additive combinatorics, and so has many applications (for example, see [11] or [12]). While we will not aim to give a complete background, it is important to also mention that the analogue problem has been considered over different fields instead of \mathbb{R} , where many interesting results are also available. See for instance [18] for a more complete account. In particular, over finite fields it is worth pointing out the result of Vu from [19], who classified the two variable polynomials $f(x, y) \in \mathbb{F}_q[x, y]$ such that $|f(A, A)|$ is large whenever $|A + A|$ is small.

Theorem 1.2. *Let A be a subset of \mathbb{F}_q and let $f(x, y) \in \mathbb{F}_q[x, y]$ be a polynomial which cannot be written as $g(L(x, y))$ for some linear polynomial L and some univariate polynomial g . Then,*

$$\max\{|A + A|, f(A, A)\} = \Omega\left(\min\{|A|^{2/3}q^{1/3}, |A|^{3/2}q^{-1/4}\}\right).$$

Motivated by Theorem 1.2, Shen then considered the analogue question over the reals and proved in [14] the following very interesting result, which in part preceded Theorem 1.1.

Theorem 1.3. *Let $f \in \mathbb{R}[x, y]$ be a polynomial of a constant degree that is not of the form $g(L(x, y))$ for some linear polynomial L and some univariate polynomial g . If A is a finite set of real numbers, then*

$$|A + A||f(A, A)| = \Omega(|A|^{5/2}).$$

The proof of Theorem 1.3 is in some sense a generalization of Elekes’s argument from [7] (for the particular case when $f(x, y) = xy$), which manages to replace the spectral graph theory from the finite field case [19] with tools from incidence geometry over the reals. In particular, Theorem 1.3 implies that when $A \subset \mathbb{R}$ satisfies $|A + A| = O(|A|)$, we have that $|f(A, A)| = \Omega(|A|^{3/2})$ for every polynomial that is not of the form $g(L(x, y))$ for some linear polynomial L and some univariate polynomial g . Like Theorem 1.1, however, this is not optimal and it is widely believed that the exponent $3/2$ could probably be replaced with $2 - \epsilon$ for every $\epsilon > 0$ in general (as it is the case for $f(x, y) = xy$; see for example [15] for more details).

In this paper, we address the “dual” problem of classifying the two variable polynomials $f(x, y) \in \mathbb{R}[x, y]$ such that $|f(A, A)|$ is large whenever $|AA|$ is small. As above, it is easy to check that there are some polynomials for which this fails. For instance, consider $A = \{2, 2^2, \dots, 2^N\}$ for which $|AA| = 2N - 1$. If we let f be a single monomial such as $f(x, y) = x^2y^3$, then it is easy to check that $f(A, A) = 5N - 4$. More generally, if we choose g to be a polynomial in one variable and $M(x, y)$ to be a single monomial, the $f(A, A)$ will also be usually small for $f(x, y) = g(M(x, y))$. Indeed, consider say $f(x, y) = xy + x^2y^2$; then we also have that $f(A, A) = 2N - 1$. Our main result shows that $g(M(x, y))$ is the *only* real enemy, in the following strong sense.

Theorem 1.4. *Let $f \in \mathbb{R}[x, y]$ be a polynomial of a constant degree that is not of the form $g(M(x, y))$ for some single monomial M and some univariate polynomial g . If A is a finite set of real numbers such that $|AA| = K|A|$, then*

$$|f(A, A)| = \Omega_K(|A|^2).$$

This is also optimal up to the dependence on K . We prove Theorem 1.4 in Section 3, after introducing the required ingredients in the upcoming Section 2.

2. PRELIMINARIES

The proof of Theorem 1.4 is in some sense in spirit with the proofs of Theorem 1.1 and Theorem 1.3, but it does not rely on any incidence geometry. The main new ingredient is a quantitative version of the celebrated Schmidt subspace theorem [13] due to Amoroso and Viada [1].

Theorem 2.1. *Let $a_1, \dots, a_n \in K$ be nonzero elements of an algebraically closed field K , and let Γ be a subgroup of K of finite rank r . Then, the number of solutions of the equation*

$$a_1 z_1 + \dots + a_n z_n = 1$$

with $z_i \in \Gamma$ and no subsum on the left hand side vanishing is at most

$$C(n, r) := (8n)^{4n^4(n+nr+1)}.$$

Schmidt's subspace theorem (together with its different variants) represents a powerful result in number theory, particularly famous for its many applications in diophantine approximation and complexity of algebraic numbers. We will not remind them here, since many excellent surveys have been written about it, so we refer the reader for instance to [3] and [16]. In fact, Theorem 2.1 has already manifested itself in additive combinatorics as well in [4], where Chang noticed that one can use it to prove that $|AA| = O(|A|)$ implies $|A + A| = \Omega(|A|^2)$. Theorem 1.4 can therefore also be seen as a generalization of this phenomenon.

The next ingredient is a multiplicative version of a somewhat more unusual version of Freiman's theorem from additive combinatorics, which is essentially a combination of [5] and Freiman's Lemma [9]. See [10] for more details.

Theorem 2.2. *Let $t \geq 1$ be an integer, let $\epsilon > 0$, and let A be a finite set of real numbers with $|AA| = K|A|$ and $|A| \geq CK^2/\epsilon$ for some absolute constant $C > 0$. Then, A is a subset of a set G , which is of the form¹*

$$G := g_1^{[H_1]} \cdot \dots \cdot g_r^{[H_r]} = \left\{ \prod_{i=1}^r g_i^{\mu_i} : \mu_i \in \mathbb{Z}, \mu_i \in [H_i] \right\},$$

where $r \leq \lfloor K - 1 + \epsilon \rfloor$, all the products in

$$G^{(t)} := \left\{ \prod_{i=1}^r g_i^{\mu_i} : \mu_i \in \mathbb{Z}, \mu_i \in [tH_i] \right\}$$

are pairwise distinct, and

$$|G| = H_1 \cdot \dots \cdot H_r \leq t^K \exp(CK^2 \log^3 K) |B|.$$

¹If n is a positive integer, $[n]$ denotes the set $\{0, 1, \dots, n-1\}$.

The last two ingredients are more algebraic in nature. First, recall that a polynomial $f \in \mathbb{R}[x, y]$ is said to be *reducible* if there exist polynomials $f_1, f_2 \in \mathbb{R}[x, y]$ of positive degrees such that $f(x, y) = f_1(x, y) \cdot f_2(x, y)$. A polynomial that is not reducible is said to be *irreducible*. Furthermore, we say that a polynomial $p \in \mathbb{R}[x, y]$ is *decomposable* if there exists a univariate polynomial p_1 of degree at least two and $p_2 \in \mathbb{R}[x, y]$ such that $p(x, y) = p_1(p_2(x, y))$. Similarly, a polynomial that is not decomposable is said to be *indecomposable*.

We will need a consequence of a theorem of Stein [17], which follows from the main result of [2]. See [11] for more details.

Theorem 2.3. *If $f \in \mathbb{R}[x, y]$ is indecomposable, then the polynomial $f(x, y) - \lambda$ is reducible for at most $\deg f$ values of $\lambda \in \mathbb{R}$.*

Last but not least, we will also need the classical Bézout theorem [6], which again we only state for real polynomials, as these are the main objects of our paper.

Theorem 2.4. *Let f and g be two polynomials in $\mathbb{R}[x, y]$. If f and g vanish simultaneously on more than $(\deg f)(\deg g)$ points of \mathbb{R}^2 , then f and g have a common non-trivial factor.*

3. PROOF OF THEOREM 1.4

Let $f \in \mathbb{R}[x, y]$ be a polynomial that is not of the form $g(M(x, y))$ for some single monomial M and some univariate polynomial g , and let d be the degree of f . We will prove that

$$|f(A, A)| = \Omega_{d,K}(|A|^2)$$

whenever $A \subset \mathbb{R}$ satisfies $|AA| = K|A|$. The dependence on d and K is going to be explicit, but since it is not a priority from time to time we will reserve the right to hide certain expressions under the asymptotic notation whenever it is more convenient.

First, recall that if f is decomposable, then there exist a univariate f_1 of degree at least two and $f_2 \in \mathbb{R}[x, y]$ such that $f(x, y) = f_1(f_2(x, y))$. Let (f_1, f_2) be a pair of such polynomials that minimizes the degree of f_2 . In particular, this implies that f_2 is indecomposable. Since f is of degree at most d , so are f_1 and f_2 . Since f_1 is univariate, for every $a \in \mathbb{R}$ there exist at most d numbers $b \in \mathbb{R}$ such that $f_1(b) = a$. Thus, if $|f_2(A, A)| \geq T$ holds for some positive quantity T , then $|f(A, A)| \geq T/d$. It then remains to derive the lower bound for the indecomposable f_2 , which we also know it is not a single monomial $M(x, y)$ from the hypothesis. Abusing of notation, we will refer to f_2 as f from now on, and therefore assume without loss of generality that f is indecomposable and not a single monomial as well.

Next, we naturally define the following polynomial energy of A by

$$E_f(A) := \left| \{(x, y, x', y') \in A^4 : f(x, y) = f(x', y')\} \right|.$$

For each $\alpha \in f(A, A)$, we also let $m_A(\alpha)$ denote the number of pairs $(x, y) \in A \times A$ such that $f(x, y) = \alpha$. In particular,

$$m_A(\alpha)^2 = \left| \{(x, y, x', y') \in A^4 : f(x, y) = f(x', y') = \alpha\} \right|,$$

so by Cauchy-Schwarz,

$$E_f(A) = \sum_{\alpha \in f(A, A)} m_A(\alpha)^2 \geq \frac{1}{|f(A, A)|} \cdot \left(\sum_{\alpha \in f(A, A)} m_A(\alpha) \right)^2 = \frac{|A|^4}{|f(A, A)|}.$$

In order to prove that $|f(A, A)| = \Omega_{d, K}(|A|^2)$, it thus suffices to show that $E_f(A) = O_{d, K}(|A|^2)$ instead. To achieve this, we will show that for most values of $\alpha \in f(A, A)$, the number of solutions in $A \times A$ to the equation $f(x, y) = \alpha$ is at most a constant which depends solely on d and K . More precisely, we claim that

$$\left| \left\{ \alpha \in f(A, A) : m_A(\alpha) > C \left(\binom{d+2}{2}, K \right) + d^2 2^{\binom{d+2}{2}} \right\} \right| = O_d(1), \quad (3.1)$$

where $C \left(\binom{d+2}{2}, K \right)$ is the explicit constant from Theorem 2.1.

Let us first check that this claim implies that $E_f(A) = O_{d, K}(|A|^2)$. For convenience, let

$$\Upsilon(A) := \left\{ \alpha \in f(A, A) : m_A(\alpha) > C \left(\binom{d+2}{2}, K \right) + d^2 2^{\binom{d+2}{2}} \right\},$$

and write

$$E_f(A) = \sum_{\alpha \in \Upsilon(A)} m_A(\alpha)^2 + \sum_{\alpha \in f(A, A) \setminus \Upsilon(A)} m_A(\alpha)^2. \quad (3.2)$$

For every $\alpha \in f(A, A)$, it is easy to see that $m_A(\alpha)^2 = O_d(|A|^2)$. Indeed, recall that this quantity is the number of solutions in A^4 to $f(x, y) = f(x', y') = \alpha$, so once x and x' are chosen in A , there are at most d value for each y and y' that can satisfy the equality. In particular, if $|\Upsilon(A)| = O_d(1)$, this implies that the first term in (3.2) satisfies

$$\sum_{\alpha \in \Upsilon(A)} m_A(\alpha)^2 = O_d(|A|^2).$$

For the second term, note that if $\alpha \notin \Upsilon(A)$ then

$$M := \max_{\alpha \in f(A, A) \setminus \Upsilon(A)} m_A(\alpha) \leq C \left(\binom{d+2}{2}, K \right) + d^2 2^{\binom{d+2}{2}} = O_{d, K}(1),$$

therefore

$$\sum_{\alpha \in f(A, A) \setminus \Upsilon(A)} m_A(\alpha)^2 \leq M \sum_{\alpha \in f(A, A) \setminus \Upsilon(A)} m_A(\alpha) \leq M|A|^2 = O_{d, K}(|A|^2).$$

Putting these two estimates together, we indeed get that $E_f(A) = O_{d, K}(|A|^2)$. We are now left to prove (3.1), which will require the tools from Section 2.

Recall that A satisfies $|AA| = K|A|$. If the size of A is upper bounded by a constant in terms of K , then there is nothing to prove since $|f(A, A)| =$

$\Omega_{d,K}(|A|^2)$ is trivially true, so we can safely apply Theorem 2.2 with $\epsilon = 1$ and $t = d$. This implies that A is a subset of a set G , which is of the form

$$G := g_1^{[H_1]} \cdot \dots \cdot g_r^{[H_r]} = \left\{ \prod_{i=1}^r g_i^{\mu_i} : \mu_i \in \mathbb{Z}, \mu_i \in [H_i] \right\},$$

where $r \leq \lfloor K \rfloor \leq K$ and all the products all the products in

$$G^{(d)} := \left\{ \prod_{i=1}^r g_i^{\mu_i} : \mu_i \in \mathbb{Z}, \mu_i \in [dH_i] \right\}$$

are pairwise distinct. We also have a quantitative estimate for $|G|$, but it is not required.

For each $\alpha \in f(A, A)$, we now analyze the number of solutions in $A \times A$ to $f(x, y) = \alpha$. Write f explicitly as

$$f(x, y) := \sum_{(i,j) \in S} a_{i,j} x^i y^j,$$

where S is some subset of the set of pairs $\{(i, j) : i, j \geq 0, i + j \leq d\}$ and $a_{i,j}$ is a real coefficient for each $(i, j) \in S$.

We begin with a first key lemma.

Lemma 3.1. *For every $\alpha \in f(A, A)$, the number of solutions in $A \times A$ to*

$$\sum_{(i,j) \in S} a_{i,j} x^i y^j = \alpha$$

with no subsum on the left hand side vanishing is at most $C\left(\binom{d+2}{2}, K\right)$.

Proof. Let Γ be the multiplicative subgroup of \mathbb{C}^* generated by g_1, \dots, g_r , which has rank $r \leq K$ and contains G (and thus also A). The number of solutions to

$$\sum_{(i,j) \in S} a_{i,j} z_{i,j} = \alpha \tag{3.3}$$

with $z_{i,j} \in G^{(d)}$ for each $(i, j) \in S$ and no subsum on the left hand side vanishing is at most the number of solutions to (3.3) with the $z_{i,j}$ in Γ and no subsum on the left hand side vanishing, so by Theorem 2.1 it is at most $C\left(\binom{d+2}{2}, K\right)$. If we also can argue that for each such solution $(z_{i,j})_{(i,j) \in S}$ to (3.3), there is at most one solution $(x, y) \in G \times G$ (and thus in $A \times A$) to the system of equations

$$x^i y^j = z_{i,j} \quad \text{for each } (i, j) \in S, \tag{3.4}$$

then the claim follows.

For x and y in G , write

$$x = g_1^{x_1} \cdot \dots \cdot g_r^{x_r} \quad \text{and} \quad y = g_1^{y_1} \cdot \dots \cdot g_r^{y_r},$$

where $x_k, y_k \in [H_k]$ for each $k \in \{1, \dots, r\}$. Similarly, for $z_{i,j} \in G^{(d)}$, let

$$z_{i,j} = g_1^{z_{i,j,1}} \cdot \dots \cdot g_r^{z_{i,j,r}},$$

where $z_{i,j,k} \in [dH_k]$ for each $k \in \{1, \dots, r\}$. Plugging these expressions into (3.4), we get

$$g_1^{ix_1+jy_1} \cdot \dots \cdot g_r^{ix_r+jy_r} = g_1^{z_{i,j,1}} \cdot \dots \cdot g_r^{z_{i,j,r}} \quad \text{for each } (i, j) \in S.$$

Furthermore, since $i + j \leq d$, we also have that $ix_k + jy_k \in [dH_k]$ for each k , so by the fact that $G^{(d)}$ has all its products pairwise distinct, it follows that (3.4) translates into the following system of equalities, call it $\mathcal{S}_{i,j}$, satisfied by the exponents above for each $(i, j) \in S$:

$$ix_k + jy_k = z_{i,j,k} \quad \text{for all } k \in \{1, \dots, r\}.$$

At this point, recall that f is indecomposable by our assumption and is also not a single monomial, so it must contain at least two monomials, say $x^i y^j$ and $x^{i'} y^{j'}$, for which the two-dimensional vectors (i, j) and (i', j') are not a (rational) scalar multiple of each other. In particular, if a pair $(x, y) \in A \times A \subset G \times G$ exists to satisfy both $\mathcal{S}_{i,j}$ and $\mathcal{S}_{i',j'}$, then each pair (x_k, y_k) is uniquely determined in terms of i, j, i', j' and $z_{i,j,k}, z_{i',j',k}$ for each $k \in \{1, \dots, r\}$, which implies that (x, y) is then uniquely determined. This proves the claim. \square

We now analyze what happens if there are vanishing subsums on the left hand side of $f(x, y) = \alpha$. In this sense, we prove the following second key lemma.

Lemma 3.2. *For all but possibly at most $d + 1$ values of $\alpha \in f(A, A)$, the number of pairs $(x, y) \in A \times A$ satisfying $f(x, y) = \alpha$ with some vanishing subsum on the left hand side is at most $d^2 2^{\binom{d+2}{2}}$.*

Proof. Recall $f(x, y) := \sum_{(i,j) \in S} a_{i,j} x^i y^j$ with $|S| \geq 2$, and now suppose that

$$\sum_{(i,j) \in S} a_{i,j} x^i y^j = 0$$

for some nontrivial subset $S' \subset S$. Let $N_{S'}(\alpha)$ be number of common solutions in $A \times A$ to

$$f(x, y) - \alpha = 0 \quad \text{and} \quad g_{S'}(x, y) = 0, \quad (3.5)$$

where $g_{S'} \in \mathbb{R}[x, y]$ is the polynomial defined by

$$g_{S'}(x, y) := \sum_{(i,j) \in S'} a_{i,j} x^i y^j$$

for a nontrivial subset S' of S . By a union bound, it suffices to prove that

$$\sum_{S' \subset S} N_{S'}(\alpha) \leq d^2 2^{\binom{d+2}{2}}$$

holds for all but possibly at most $d + 1$ values of $\alpha \in f(A, A)$.

For each $S' \subset S$, note that $g_{S'}$ has degree at most d , since $\deg f = d$. By Theorem 2.3 there are at most d values of α for which $f(x, y) - \alpha$ is reducible, and at most one value for which $f(x, y) - \alpha$ may be identical to $g_{S'}(x, y)$, for some $S' \subset S$ (α may be equal to the free term in f). For each of the other

$\alpha \in f(A, A)$, we have that $N_{S'}(\alpha) \leq d^2$ for every proper $S' \subset S$. Indeed, if α is such that the polynomial $f(x, y) - \alpha$ is irreducible in $\mathbb{R}[x, y]$ and does not coincide with $g_{S'}(x, y)$, then this simply follows from Theorem 2.4, since (3.5) must have at most d^2 solutions if there is no common factor. Therefore,

$$\sum_{S' \subset S} N_{S'}(\alpha) \leq d^2 2^{|S|} \leq d^2 2^{\binom{d+2}{2}}$$

is indeed satisfied by all $\alpha \in f(A, A)$, except for perhaps at most $d + 1$ values. This completes the proof of Lemma 3.2. \square

Claim (3.1) now follows by combining Lemma 3.1 and Lemma 3.2. Indeed, together these two imply that for all but possibly at most $d + 1$ values of $\alpha \in f(A, A)$, the number of pairs $(x, y) \in A \times A$ with $f(x, y) = \alpha$ is at most $C\left(\binom{d+2}{2}, K\right) + d^2 2^{\binom{d+2}{2}}$. In other words, $|\Upsilon(A)| \leq d + 1$, where

$$\Upsilon(A) := \left\{ \alpha \in f(A, A) : m_A(\alpha) > C\left(\binom{d+2}{2}, K\right) + d^2 2^{\binom{d+2}{2}} \right\}.$$

This completes the proof of Theorem 1.4.

Acknowledgements. I would like to thank Vlad Matei, Adam Sheffer and Dmitrii Zhelezov for useful discussions.

REFERENCES

- [1] F. Amoroso and E. Viada, Small points on subvarieties of a torus, *Duke Mathematical Journal*, **150**(3):407-442, 2009.
- [2] M. Ayad, Sur les polynômes $f(X, Y)$ tels que $K[f]$ est int egralement ferm e dans $K[X, Y]$, *Acta Arith.* **105** (2002), 9–28.
- [3] Y. Bilu. The Many Faces of the Subspace Theorem (after Adamczewski, Bugeaud, Corvaja, Zannier...). S eminaire Bourbaki, Expos e 967, 59 eme ann ee (2006-2007), *Ast erisque* 317 (2008), 1-38, May 2007.
- [4] M.-C. Chang, Sum and product of different sets, *Contributions to Discrete Mathematics*, **1** (1), 2006.
- [5] M.-C. Chang, Generalized arithmetical progressions and sumsets, *Acta Math. Hungar.*, **65** (1994), no. 4, 379-388.
- [6] D. A. Cox, J. Little and D. O’Shea, *Using Algebraic Geometry*, Springer-Verlag, 2nd Edition, Heidelberg 2005.
- [7] G. Elekes, On the number of sums and products, *Acta Arith.*, **81** (1997) 365-367.
- [8] G. Elekes, L. R onyai, A combinatorial problem on polynomials and rational functions, *J. Combin. Theory Ser. A* **89** (2000), 1-20.
- [9] G.A. Freiman, *Foundations of a Structural Theory of Set Addition*, Kazan Gos. Ped. Inst., Kazan, 1966 (Russian). English translation in Translations of Mathematical Monographs **37**, Amer. Math. Soc., Providence, RI, USA, 1973.
- [10] B. Green, T. Tao, Compressions, Convex Geometry and the Freiman-Bilu Theorem, *Q. J. Math.*, **57** (4) (2006), 495-504.
- [11] O. E. Raz, M. Sharir, and J. Solymosi, Polynomials vanishing on grids: The Elekes-R onyai problem revisited, *Amer. J. Math.* **138** (2016), 1029-1065.
- [12] O. E. Raz, M. Sharir, and F. de Zeeuw, Polynomials vanishing on Cartesian products: The Elekes-Szabo Theorem revisited, *Duke Math. J.*, **165** (2016), 3517-3566.

- [13] W. M. Schmidt, Norm form equations, *Annals of Mathematics*, **96**(3): 526-551, 1972.
- [14] C. Shen, Algebraic methods in sum-product phenomena, *Israel J. Math.* **188** (2012), 123-130.
- [15] J. Solymosi, Bounding multiplicative energy by the sumset, *Adv. Math.*, **222** (2009), pp. 402-408.
- [16] R. Schwarz, J. Solymosi, *Combinatorial Applications of the Subspace Theorem*, Geometry, Structure and Randomness in Combinatorics. Scuola Normale Superiore (2014), 123-140.
- [17] Y. Stein, The total reducibility order of a polynomial in two variables, *Israel J. Math.* **68** (1989), 109-122.
- [18] T. Tao, Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets, *Contributions to Discrete Mathematics* **10** (2015), 22-98.
- [19] V. Vu, Sum-product estimates via directed expanders, *Math. Res. Lett.*, **15** (2008), 375-388.

CALIFORNIA INSTITUTE OF TECHNOLOGY, PASADENA, CA, USA

E-mail address: apohoata@caltech.edu