Discrete Comput Geom 19:383–389 (1998)

Discrete & Computational
Geometry

A Combinatorial Problem on Polynomials*

G. Elekes

Department of Computer Science, Eötvös University,
Múzeum krt 6–8, H-1088 Budapest, Hungary
elekes@cs.elte.hu

Communicated by János Pach

Abstract. Problems and results on polynomials of two variables which take few distinct values on finite Cartesian products are considered. The methods we use come from combinatorial geometry.

1. Introduction

Freiman [2] described the structure of subsets $\mathcal{A} \subset \mathbf{R}$ of n elements for which $|\mathcal{A}+\mathcal{A}| \leq Cn$. (Here $\mathcal{A}+\mathcal{A}$ denotes the set of all pairwise sums of elements of $\mathcal{A}$.) He proved there that $\mathcal{A}$ must be contained in a "generalized" arithmetic progression. (See also [8].)

Here we initiate the study of polynomials of two real variables which, from the above point of view, behave like $x+y$, i.e.,those which can take few distinct values while x and y (independently of each other) range over appropriate finite subsets of $\mathbf{R}$.

Definition 1. Let n be a positive integer, $C > 1$, and let $P \in \mathbf{R}[x, y]$ be a polynomial in two real variables.

We say that P is (C, n)-*restricted* if there exist $X, Y \subset \mathbf{R}$ such that

$$|X| = |Y| = n,$$

and

$$|P(X \times Y)| \leq Cn. \tag{1}$$

Moreover, P is *restricted*, if it is (C, n)-restricted for some $C \geq 1$ and for all $n \in \mathbf{N}$.

* This research was partially supported by OTKA Grants I014302, T019367, and T017580.

Two examples of restricted polynomials (with $C = 2$) are $x + y$ and xy, which only take $2n - 1$ distinct values if both x and y are from an arithmetic or geometric (also called "exponential") progression, respectively.

Conjecture 1. *If P is restricted, then there are polynomials $f, g, h \in \mathbf{R}[z]$ such that*

$$\begin{aligned} \textit{either} \quad & P(x, y) = f(g(x) + h(y)), \\ \textit{or} \quad & P(x, y) = f(g(x) \cdot h(y)). \end{aligned}$$

We prove two special cases of Conjecture 1.

Definition 2. $P \in \mathbf{R}[x, y]$ is a *special* restricted polynomial if, in the definition of restrictedness, we can always require Y to be an arithmetic progression, i.e.,$\exists C\ \forall n\ \exists X\ \exists$ arithmetic progression Y which satisfy (1).

Theorem 1. *Every special restricted polynomial P is of the form*

$$P(x, y) = f(y - g(x)),$$

or

$$P(x, y) = g(x),$$

for some polynomials $f, g \in \mathbf{R}[z]$.

We mention without proof that if we assume that the $Y = Y_n$ are all geometric progressions for $n \in \mathbf{N}$, then $P(x, y) = f(y \cdot g(x))$ or just $g(x)$.

Also, Conjecture 1 holds for all restricted polynomials which are *linear* in one variable, say y.

Theorem 2. *A restricted polynomial $P(x, y) = a(x) \cdot y + b(x)$, (where $a(x)$ and $b(x)$ are from $\mathbf{R}[x]$), can only be one of two types*:

$$\begin{aligned} \textit{either} \quad & P(x, y) = a \cdot y + b(x), \\ \textit{or} \quad & P(x, y) = a(x) \cdot (y - u) + v, \end{aligned}$$

for some real constants a, or u and v.

It may be of interest that both proofs use methods from combinatorial geometry.

We cannot resist mentioning one more related problem, where we have been unable even to guess a precise answer.

Question 1. What is the structure of those polynomials $Q(x, y, z)$ which, for all n, vanish on some $0.001n^2$ points of an appropriate $n \times n \times n$ Cartesian product $X_n \times Y_n \times Z_n$? (Or, perhaps, with some arbitrary fixed $c > 0$ in place of 0.001.)

Remark 3. A suitable answer to the above problem may imply an answer to Conjecture 1, if applied to $Q(x, y, z) = z - P(x, y)$.

2. Proof of Theorem 1

In the course of the proof, we shall use a simple consequence (Lemma 6) of a general theorem by Pach and Sharir. To start with, we describe this tool. Then, in the second subsection, we turn our attention to the proof itself.

2.1. *The Curve Lemma*

Following Pach and Sharir [6] and [7] (see also [5]), we define regular classes of curves—in purely combinatorial terms. (Actually, they allow slightly more general curves than we do; however, the following will be sufficient for our purposes.)

Definition 4. A class Ω of simple—open or closed—continuous real plane curves (where "simple" means that a curve does not intersect itself) is a *regular class of curves of k degrees of freedom* if, for any k points of the plane, at most one curve of Ω passes through all of them.

Proposition 5 (Pach–Sharir Theorem). *For every positive integer k and every regular class Ω of curves of k degrees of freedom, there is a constant $C = C_\Omega$ with the following property*:

If $\Gamma \subset \Omega$ and $\mathcal{A} \subset \mathbf{R}^2$ is an arbitrary point set (both finite), then, for the number I of incidences between Γ and $\mathcal{A}$,

$$I(\mathcal{A}, \Gamma) \leq C \max\{|\mathcal{A}|^{k/(2k-1)} \cdot |\Gamma|^{(2k-2)/(2k-1)}\ ;\ |\mathcal{A}|;\ |\Gamma|\}.$$

Note that the class of all irreducible real algebraic curves of degree not exceeding d does not satisfy the above definition, since it contains curves which intersect themselves—though, by Bézout's theorem [3], any two of its members intersect in not more than d^2 points. A curve from this family has at most $\binom{d-1}{2}$ singular points (see [4, p. 265]). By deleting these, every such curve can be decomposed into at most $1 + \binom{d-1}{2}$ disjoint simple components. Such portions of the curves of the above type already form a regular class with $d^2 + 1$ degrees of freedom.

Also note that if an original curve contains, say, cN points of a given point set, then at least one of its simple pieces will contain $cN/(d^2)$ of them, provided that $N > n_0(c, d)$.

This and the Pach–Sharir theorem immediately imply the following observation.

Lemma 6 (Curve Lemma). *For every $c > 0$ and positive integer d, there is a $C' = C'(c, d)$ with the following property*:

Let $\mathcal{A} \subset \mathbf{R}^2$ with $|\mathcal{A}| \leq N^2$ and assume that a set Γ of irreducible real algebraic curves of degree not exceeding d has the property that every $\gamma \in \Gamma$ intersects $\mathcal{A}$ in at least

$$|\gamma \cap \mathcal{A}| \geq cN$$

points. Then $|\Gamma| \leq C'N$, provided that $N > n_0(c, d)$.

It is worth noting that the order of magnitude of the bound imposed on $|\Gamma|$ is always linear, whatever d is; only the coefficient C' depends on d.

2.2. *The Proof*

Let $P \in \mathbf{R}[x, y]$ be a special restricted polynomial and let $n \in \mathbf{N}$ be sufficiently large (to be specified later). Moreover, assume that (1) holds for an $X = X_n \subset \mathbf{R}$ and an arithmetic progression $Y = Y_n \subset \mathbf{R}$.

If P does not depend on y, then there is nothing to prove. Thus, without loss of generality, we may assume that this is not the case.

1. Put $Z = Z_n = P(X_n \times Y_n)$. Now our assumption is equivalent to the following: *At most Cn real algebraic curves of type*

$$\gamma_i: \quad P(x, y) = z_i \qquad (z_i \in Z) \tag{2}$$

cover $X \times Y$.

2. Denote the degree of P by d. Then every curve γ_i can be decomposed into not more than d *irreducible* ones. From each such decomposition, pick a factor with a maximum number of points of $X \times Y$, and denote it by $\hat{\gamma}_i$. Thus we get at most Cn curves which, together, cover n^2/d or more points. Note that since we assumed that P does depend on y, therefore at most d of the $\hat{\gamma}_i$ are vertical lines. Deleting them, the rest will still cover $n^2/d - dn > \hat{c}n^2$ points. Also, using Bézout's theorem (see, e.g.,[3]) for such a $\hat{\gamma}_i$ and $\prod_{x_i \in X}(x - x_i)$, we infer that none of the $\hat{\gamma}_i$ covers more than dn.

3. We claim that there are at least $\hat{c}n/(2d)$ of the $\hat{\gamma}_i$, which cover $\hat{c}n/(2C)$ or more points each. (Indeed, otherwise those with less than this many points, would together cover less than $Cn \cdot \hat{c}n/(2C) = \hat{c}n^2/2$, as well as the rest which could cover less than $dn \cdot \hat{c}n/(2d) = \hat{c}n^2/2$, making a total less than $\hat{c}n^2$, a contradiction.)

4. We define an equivalence relation.

Definition 7. We say that two of the curves, say $\hat{\gamma}_i$ and $\hat{\gamma}_j$ are *equivalent*, if they are shifted copies of each other in the y-direction, i.e.,if there is a Δ, for which (using the notation of (2)),

$$P(x, y - \Delta) = z_j \qquad \text{whenever} \quad (x, y) \in \hat{\gamma}_i.$$

Lemma 8. *Among those $\hat{\gamma}_i$, which cover $\hat{c}n/(2C)$ or more points, the number of the equivalence classes cannot exceed a constant $C^* = C^*(C, d)$.*

Proof. Let e be the number of these equivalence classes. From each such class, pick a curve and shift it in the y-direction, by $1, 2, \ldots, n$ steps, each step the difference of the arithmetic progression Y. (Note that the points in Y move to points of another arithmetic progression of double length, which we denote by $2Y$.) Put $N = 2n$. Thus we get en distinct, irreducible curves, each covering $\hat{c}N/(4C)$ or more points of $(X \times 2Y) \subset (2X \times 2Y)$, where the latter has N^2 elements.

By Lemma 6,

$$en \le \hat{C}N = 2\hat{C}n,$$

whence, indeed, $e \le 2\hat{C} \stackrel{\text{def}}{=} C^*$. □

Corollary 9. *At least $\hat{c}n/(2C^*d)$ of the $\hat{\gamma}_i$ are equivalent.*

5. So far we have not specified how large n should be. In what follows, let $n > 2C^*d^2/\hat{c}$. For such a value, the above corollary implies the existence of $d+1$ equivalent $\hat{\gamma}_i$, say $\hat{\gamma}_0, \hat{\gamma}_1, \ldots, \hat{\gamma}_d$. Recall that all of these are non-vertical irreducible factors of distinct curves of type (2).

Let Δ_i be the length of the vertical shift which moves $\hat{\gamma}_0$ to $\hat{\gamma}_i$, i.e.,

$$P(x, y + \Delta_i) = z_i, \qquad \text{whenever} \quad (x, y) \in \hat{\gamma}_0. \tag{3}$$

6. Pick an arbitrary, nonsingular point (x_0, y_0) of $\hat{\gamma}_0$, with the additional requirements that the tangent line of $\hat{\gamma}_0$ is nonvertical there (which is possible because at most $d-1$ tangent lines can be vertical) and that $P(x_0, y)$ is not a constant (which is also possible since P can be a constant on at most d vertical lines).

Without loss of generality, assume that $x_0 = y_0 = 0$ and $\hat{\gamma}_0$ corresponds to $P(x, y) = 0$ (otherwise apply a linear transform on P). In an ε-neighborhood of 0, the curve $\hat{\gamma}_0$ is described by an analytic function $y = g(x)$; i.e.,$|x| < \varepsilon$ implies $P(x, g(x)) = 0$.

7. Put

$$f(y) \stackrel{\text{def}}{=} P(0, y).$$

We show that

$$P(x, y) = f(y - g(x)), \tag{4}$$

for all $(x, y) \in \mathbf{R}^2$.

First we claim that it holds for all $|x| < \varepsilon$ and $y \in \mathbf{R}$. To show this, recall that $(x, g(x)) \in \hat{\gamma}_0$ which, together with (3), implies

$$P(x, g(x) + \Delta_i) = z_i = P(0, \Delta_i) = f(\Delta_i),$$

for each $x \in (-\varepsilon, \varepsilon)$ and $d+1$ distinct values $y = \Delta_i$. Hence $P(x, g(x)+y) = f(y)$ as polynomials of y, for every fixed x with $|x| < \varepsilon$. Now, in order to prove (4), it suffices to observe that there are analytic functions on both sides and they coincide on a rectangle (actually on an infinite stripe). Therefore (4) is, indeed, an identity.

8. We are left to show that g is a polynomial. Denote the degree of f by $k > 0$ and assume that $f(y) = \lambda_k y^k + \lambda_{k-1} y^{k-1} + \cdots + \lambda_0$. Then, in (4), the coefficient of y^{k-1} is

$$\lambda_k \cdot k \cdot g(x) + \lambda_{k-1}$$

on the right-hand side while it is a polynomial of x on the left. Moreover, the coefficient of $g(x)$ in the above formula is nonzero. Therefore, $g \in \mathbf{R}[x]$.

This finishes the proof of Theorem 1. □

3. The Proof of Theorem 2

The following was proven in [1] as part (ii) of the Lattice Lemma there.

Proposition 10. *For every $C > 1$ and $c > 0$, there is a $c^* = c^*(C, c)$ with the following property*:

Let $Y, Z \subset \mathbf{R}$ with $n \le |Y|, |Z| \le Cn$. If some cn straight lines contain n or more points of $Y \times Z$ each, then at least c^*n of these lines are parallel or concurrent.

Now the proof of Theorem 2 goes as follows:

1. By our assumption, there is a $C > 1$ such that, for all $n \in \mathbf{N}$, there are $X = X_n$, $Y = Y_n$ with $|X| = |Y| = n$, and $P(X \times Y) \le Cn$. Put

$$Z_n \stackrel{\text{def}}{=} P(X \times Y).$$

Of course, $|Z_n| \le Cn$ here.

2. For all $x_i \in X$, consider the linear functions (of y):

$$p_i(y) \stackrel{\text{def}}{=} P(x_i, y) = a(x_i) \cdot y + b(x_i),$$

where a (resp., b) is the leading coefficient (resp., the constant) in P as a *linear* polynomial of just y.

Every such p_i maps Y_n to a subset of Z_n, whence their graphs must all contain $|Y_n| = n$ points of $Y_n \times Z_n$.

3. Put $d = \max\{\deg(a),\ \deg(b)\}$. We show that the graphs of at least $d + 1$ of the p_i are parallel or concurrent, provided that n is large enough.

If $d + 1$ or more of the p_i are identical, we are done. Otherwise, at least n/d of the p_i are distinct. In this case, use Proposition 10 for $c = 1/d$ and the original C to get a $c^* = c^*(C, c)$. Now if

$$n > \frac{d}{c^*},$$

then, again, we get $d + 1$ parallel or concurrent graphs.

4. We distinguish two cases:

(a) If we have $d + 1$ parallel p_i, then $a(x)$ takes identical values for this many of the x_i. Hence it is a constant a.

(b) If there are $d+1$ concurrent p_i through a point, say (u, v), then $a(x)u+b(x) = v$ for this many of the x_i. Therefore, $b(x) = -a(x)u + v$ is an identity, whence $P(x, y) = a(x)(y - u) + v$. □

Acknowledgments

The author is deeply indebted to L. Rónyai for his comments on an earlier version of the manuscript and also to an anonymous referee for his very careful work.

References

1. G. Elekes. On linear combinatorics, III. *Combinatorica*. To appear.
2. G. A. Freiman. *Foundations of a Structural Theory of Set Addition*. Translation of Mathematical Monographs, vol. 37. American Mathematical Society, Providence, RI, 1973.
3. W. Fulton. *Algebraic Curves*. W. A. Benjamin, New York, 1969.
4. J. Harris. *Algebraic Geometry*. Springer-Verlag, Berlin, 1992.
5. J. Pach and P. K. Agarwal. *Combinatorial Geometry*. Wiley, New York, 1995.
6. J. Pach and M. Sharir. Repeated angles in the plane and related problems. *J. Combin. Theory, Ser. A*, **59**:12–22, 1990.
7. J. Pach and M. Sharir. On the number of incidences between points and curves. *Combinatorics, Probability and Computing*. To appear.
8. I. Z. Ruzsa. Generalized arithmetic progressions and sum sets. *Acta Math. Sci. Hungar.*, **65**:379–388, 1994.

Received January 6, 1997, *and in revised form June* 13, 1997.

Note added in proof. L. Ronyai and the author have settled Conjecture 1 in the affirmative; see the forthcoming paper "A Combinatorial Problem on Polynomials and Rational Functions" (submitted to *J. Combin. Theory*).