Constructions for the Elekes–Szabó and Elekes–Rónyai problems

Mehdi Makhul*
Faculty of Mathematics,
University of Vienna, Austria
mmakhul@risc.jku.at

Oliver Roche-Newton† Audie Warren‡ Frank de Zeeuw
Radon Institute for Computational and Applied Mathematics
Linz, Austria
o.rochenewton@gmail.com, audie.warren@oeaw.ac.at
fdezeeuw@gmail.com

Submitted: Apr 15, 2019; Accepted: Feb 18, 2020; Published: Mar 20, 2020

Abstract

We give a construction of a non-degenerate polynomial $F \in \mathbb{R}[x, y, z]$ and a set A of cardinality n such that $|Z(F) \cap (A \times A \times A)| \gg n^{\frac{3}{2}}$, thus providing a new lower bound construction for the Elekes–Szabó problem. We also give a related construction for the Elekes–Rónyai problem restricted to a subgraph. This consists of a polynomial $f \in \mathbb{R}[x, y]$ that is not additive or multiplicative, a set A of size n, and a subset $P \subset A \times A$ of size $|P| \gg n^{3/2}$ on which f takes only n distinct values.

Mathematics Subject Classifications: 52C10

1 Introduction

Throughout this paper, we write $X \gg Y$ if and only if there exists some absolute constant $c > 0$ such that $X \geqslant cY$. If the constant c depends on another parameter k, we use the shorthand $X \gg_k Y$. Given a polynomial $F(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$, $Z(F) = \{(x_1, \ldots, x_n) : F(x_1, \ldots, x_n) = 0\}$ denotes the zero set of F.

*Supported by the Austrian Science Fund (FWF): W1214-N15, Project DK9 and Project P 30405-N32.
†Supported by the Austrian Science Fund (FWF): Project P 30405-N32
‡Supported by the Austrian Science Fund (FWF): Project P 30405-N32

1.1 The Elekes–Szabó Problem

Elekes and Szabó [6] considered the size of the intersection of the zero set of a polynomial $F(x, y, z) \in \mathbb{R}[x, y, z]$ of degree d with a Cartesian product $A \times B \times C \subset \mathbb{R}^3$, where $|A| = |B| = |C| = n$. By the Schwartz–Zippel Lemma (see for instance [9, Lemma A.4]), we have

$$|Z(F) \cap (A \times B \times C)| \ll_d n^2. \tag{1}$$

This bound cannot be improved in general. For example, if $F(x, y) = x + y + z$, $A = B = \{1, \dots, n\}$, and $C = \{-1, \dots, -n\}$, then $|Z(F) \cap (A \times B \times C)| \gg n^2$. More generally, if the equation $F(x, y, z) = 0$ is in some sense equivalent to an equation of the form $\varphi_1(x) + \varphi_2(y) + \varphi_3(z) = 0$, then we can choose A, B, C so that $|Z(F) \cap (A \times B \times C)| \gg n^2$. The following definition makes this property precise.

Definition 1. A polynomial $F(x, y, z) \in \mathbb{R}[x, y, z]$ is *degenerate* if there are intervals I_1, I_2, I_3, and for each i there is a smooth (infinitely differentiable) function $\varphi_i : I_i \to \mathbb{R}$ which has a smooth inverse, such that for all $(x, y, z) \in I_1 \times I_2 \times I_3$ we have $F(x, y, z) = 0$ if and only if $\varphi_1(x) + \varphi_2(y) + \varphi_3(z) = 0$.

Elekes and Szabó [6] showed that if the polynomial is not degenerate in this sense, then the bound (1) can be improved to $n^{2-\eta}$ for some $\eta > 0$. A quantitative improvement to $\eta = 1/6$ was obtained by Raz, Sharir and de Zeeuw [9], leading to the following statement.

Theorem 2 ([6, 9])**.** *Let $F \in \mathbb{R}[x, y, z]$ be a polynomial of degree d. If F is not degenerate, then for any $A, B, C \subset \mathbb{R}$ of size n we have*

$$|Z(F) \cap (A \times B \times C)| \ll_d n^{2-1/6}.$$

Not much attention has been paid to lower bound constructions for this theorem. Elekes [3] noted that for $F = x^2 + xy + y^2 - z$ and $A = \{1, \dots, n\}$ we have $|Z(F) \cap (A \times A \times A)| \gg n\sqrt{\log n}$ (actually, Elekes formulated this in a different way, which we mention in the next section; see [15] for more discussion). This was the only known lower bound for Theorem 2, and some have suggested that the upper bound could be improved as far as $O(n^{1+\varepsilon})$ for an arbitrarily small $\varepsilon > 0$; for instance, the fourth author wrote this in [15].

The main purpose of this paper is to show by means of a simple example that this is not the case, and that in fact the bound in Theorem 2 cannot be improved beyond $O(n^{3/2})$. Our main result is the following theorem.

Theorem 3. *There exists a polynomial $F \in \mathbb{R}[x, y, z]$ of degree 2 that is not degenerate, such that for any n there is a set $A \subset \mathbb{R}$ of size n with*

$$|Z(F) \cap (A \times A \times A)| \gg n^{3/2}.$$

In Section 4, we briefly discuss possible extensions of this theorem to polynomials in more variables.

The construction of the polynomial F in the above statement is closely related to a construction of Valtr [14], which first appeared in the context of the Erdős unit distance problem. Other constructions throughout this paper also use similar ideas.

1.2 The Elekes-Rónyai Problem

Before the work of Elekes and Szabó [6], Elekes and Rónyai [5] considered the question of bounding the image of a polynomial $f \in \mathbb{R}[x,y]$ restricted to a Cartesian product, assuming that f does not have a certain special form, which is specified in the following definition.

Definition 4. A polynomial $f(x,y) \in \mathbb{R}[x,y]$ is *additive* if there are polynomials $g,h,k \in \mathbb{R}[t]$ such that $f(x,y) = g(h(x)+k(y))$, and it is *multiplicative* if there are polynomials $g,h,k \in \mathbb{R}[t]$ such that $f(x,y) = g(h(x)\cdot k(y))$.

Elekes and Rónyai [5] proved that if $f \in \mathbb{R}[x,y]$ is not additive or multiplicative, then for every $A,B \subseteq \mathbb{R}$ with $|A| = |B| = n$ the image $|f(A,B)|$ is superlinear in n. The current state of the art for this problem is the following result of Raz, Sharir and Solymosi [8].

Theorem 5 ([5, 8])**.** *Let $f \in \mathbb{R}[x,y]$ be a polynomial of degree d. If f is not additive or multiplicative, then for any $A,B \subset \mathbb{R}$ of size n we have*

$$|f(A,B)| \gg_d n^{4/3}.$$

Elekes [3] noted that if $f(x,y) = x^2+xy+y^2$ and $A = \{1,\dots,n\}$, then $|f(A,A)| \ll n^2/\sqrt{\log n}$. This is the best known upper bound construction for Theorem 5, which suggests that we may have $|f(A,B)| \gg n^{2-\epsilon}$ for all positive ϵ. This conjecture is widely believed, see for instance Elekes [3] or Matoušek [7, Section 4.1]. The construction that we give in the proof of Theorem 3 does not translate into a construction that disproves this conjecture.

Nevertheless, we show that there is a polynomial that takes only a linear number of values on a certain large subset of the pairs in $A \times A$. This approach is partly inspired by work of Alon, Ruzsa and Solymosi [1] concerning constructions for the sum-product problem along graphs. See also [12] for a slightly improved construction.

Let G be a bipartite graph on A and B with edge set $E(G) \subset A \times B$. For a polynomial $f \in \mathbb{R}[x,y]$ we define the image of f along G to be $f_G(A,B) = \{f(a,b) : (a,b) \in E(G)\}$. Our result is the following.

Theorem 6. *There exists a polynomial $f \in \mathbb{R}[x,y]$ of degree 2 that is not additive or multiplicative, a finite set $A \subset \mathbb{R}$ of size n, and a bipartite graph G on $A \times A$, such that*

$$|E(G)| \gg n^{3/2} \qquad \text{and} \qquad |f_G(A,B)| \leqslant n.$$

2 The Elekes–Szabó problem

In this section we prove Theorem 3.

Define

$$F(x,y,z) = (x-y)^2 + x - z.$$

We set $A = \{1, \dots, n\}$ and we consider the intersection of F with $A \times A \times A$. Consider the subset

$$T = \left\{(k, k+\ell, k+\ell^2) : k, \ell \in \mathbb{Z},\ 0 \leqslant k \leqslant n/2,\ 0 \leqslant \ell \leqslant \sqrt{n}/2\right\} \subset A \times A \times A.$$

Each choice of k and ℓ determines a distinct triple in T, and so we have $|T| \gg n^{3/2}$. For each triple in T, we have

$$F(k, k+\ell, k+\ell^2) = (k - (k+\ell))^2 + k - (k+\ell^2) = 0,$$

so $T \subset Z(F)$. Therefore we have

$$|Z(F) \cap (A \times A \times A)| \gg n^{3/2}.$$

It remains to show that F is not degenerate in the sense of Definition 1. We will use an idea introduced by Elekes and Rónyai [5], which is that this type of degeneracy can be verified using the following straightforward derivative test; see for instance [6, Lemma 33] or [15, Lemma 2.2].

Lemma 7. *Let $f : \mathbb{R}^2 \to \mathbb{R}$ be a smooth function on some open set $U \subset \mathbb{R}^2$ with f_x and f_y not identically zero. If there exist smooth functions $\psi, \varphi_1, \varphi_2$ on U such that*

$$f(x, y) = \psi(\varphi_1(x) + \varphi_2(y)),$$

then

$$\frac{\partial^2 \left(\log |f_x/f_y|\right)}{\partial x \partial y} \tag{2}$$

is identically zero on U.

Suppose that $F(x, y, z) = (x-y)^2 + x - z$ is degenerate, so in some neighborhood $I_1 \times I_2 \times I_3$ we have $F(x, y, z) = 0$ if and only if $\varphi_1(x) + \varphi_2(y) + \varphi_3(z) = 0$. Then, since φ_3 has a smooth inverse on I_3, we can write $\psi(t) = \varphi_3^{-1}(-t)$, so that $F(x, y, z) = 0$ is equivalent to $z = \psi(\varphi_1(x) + \varphi_2(y))$. At the same time, $F(x, y, z) = 0$ rewrites to $z = (x-y)^2 + x$, so on $I_1 \times I_2 \times I_3$ we have

$$\psi(\varphi_1(x) + \varphi_2(y)) = (x-y)^2 + x.$$

We now check if the expression (2) is identically zero on $I_1 \times I_2 \times I_3$. We have

$$\log |f_x/f_y| = \log \left| \frac{2(x-y)+1}{-2(x-y)} \right| = \log |2x - 2y + 1| - \log |2x - 2y|,$$

so

$$\frac{\partial^2 \left(\log |f_x/f_y|\right)}{\partial x \partial y} = \frac{\partial}{\partial x}\left(\frac{-1}{x-y+1/2} + \frac{1}{x-y}\right) = \frac{1}{(x-y+1/2)^2} - \frac{1}{(x-y)^2}.$$

This expression equals zero only when $y - x = 1/4$, so it does not vanish on any nontrivial open set. Thus (2) is not identically zero, and by Lemma 7 this contradicts our assumption that F is degenerate.

3 The Elekes–Rónyai problem along a graph

We now prove Theorem 6, concerning the image of a polynomial along a subset of a Cartesian product.

Define the polynomial

$$f(x,y) = (x-y)^2 + x.$$

Set $A = \{1, \dots, n\}$ and let G be the bipartite graph on $A \times A$ with the edge set

$$E(G) = \left\{(k, k+\ell) : k, \ell \in \mathbb{Z},\ 0 \leqslant k \leqslant n/2,\ 0 \leqslant \ell \leqslant \sqrt{n}/2\right\} \subset A \times A.$$

We have $|E(G)| \gg n^{3/2}$. Applying f along any edge gives a non-negative integer

$$(k-(k+\ell))^2 + k < n.$$

This shows that

$$|f_G(A \times A)| \leqslant n.$$

It remains to prove that f is not additive or multiplicative. We could again do this using Lemma 7, but here we can use a more elementary approach. We treat the two cases separately.

Additive case: Suppose $f(x,y) = g(h(x) + k(y))$. Note that g, h and k must have degree at most 2. We cannot have $\deg(g) = 1$, since then $f(x,y)$ would not have any cross term xy. If $\deg(g) = 2$, then $\deg(h) = \deg(k) = 1$. We can write

$$g(t) = a_2t^2 + a_1t + a_0, \quad h(x) = b_1x + b_0, \quad k(y) = c_1y + c_0,$$

with b_1 and c_1 non-zero. Then we have

$$f(x,y) = (x-y)^2 + x = a_2(b_1x + b_0 + c_1y + c_0)^2 + a_1(b_1x + b_0 + c_1y + c_0) + a_0. \tag{3}$$

Calculating the coefficient for the y term on the right hand side and comparing with the left hand side, it follows that

$$2a_2(b_0 + c_0) + a_1 = 0. \tag{4}$$

On the other hand, calculating the coefficient for the x term on the right hand side of (3) and comparing with the left hand side, it follows that

$$b_1(2a_2(b_0 + c_0) + a_1) = 1.$$

Since $b_1 \neq 0$, this contradicts (4).

Multiplicative case: Suppose $f(x,y) = g(h(x) \cdot k(y))$. We cannot have $\deg(g) = 2$, since then h or k would have to be constant, and $f(x,y)$ would not depend on both variables. Therefore we have $\deg(g) = 1$. In this case, we must have $\deg(h) = \deg(k) = 1$. We can write

$$g(t) = a_1t + a_0, \quad h(x) = b_1x + b_0, \quad k(y) = c_1y + c_0$$

and

$$(x-y)^2 + x = f(x,y) = a_1((b_1x + b_0)(c_1y + c_0)) + a_0.$$

This is a contradiction, since there is no x^2 or y^2 term on the right hand side.

This completes our proof that f is not additive or multiplicative, which completes our proof of Theorem 5.

4 Extensions to more variables

4.1 Four variables

One can consider the same problems for polynomials in more variables. Raz, Sharir and de Zeeuw [10] proved that for $F \in \mathbb{R}[x, y, s, t]$ of degree d and $A, B, C, D \subset \mathbb{R}$ of size n, we have

$$|Z(F) \cap (A \times B \times C \times D)| \ll_d n^{8/3}, \tag{5}$$

unless $F(x, y, s, t) = 0$ is in a local sense (similar to Definition 1) equivalent to an equation of the form $\varphi_1(x) + \varphi_2(y) + \varphi_3(s) + \varphi_4(t) = 0$.

A construction of Valtr [14] (see also [13, Section 5.3]) essentially shows that for

$$V(x, y, s, t) = (x - y)^2 + s - t$$

one can set $A = B = \{1, \dots, n^{2/3}\}$ and $C = D = \{1, \dots, n^{4/3}\}$, so that

$$|Z(V) \cap (A \times B \times C \times D)| \gg n^{8/3}.$$

This would show that (5) is tight, if it weren't for the fact that A, B and C, D have different sizes. (A similar, older, construction of Elekes [4, Example 1.16] achieves the same with the polynomial $xy + s - t$, but is less relevant to us here.)

If we require that A, B, C, D have the same size (and then we may as well assume that they all equal $A \cup B \cup C \cup D$), then we can take Valtr's polynomial $V(x, y, s, t)$ together with the set $A = \{1, \dots, n\}$. Similarly to in our proof of Theorem 3, considering quadruples of the form $(k, k + \ell, m, m + \ell^2)$ with $1 \leqslant k, m \leqslant n/2$ and $1 \leqslant \ell \leqslant \sqrt{n}/2$, we get

$$|Z(V) \cap (A \times A \times A \times A)| \gg n^{5/2}.$$

It is not hard to verify (as in our proof of Theorem 3) that $V(x, y, s, t)$ is not degenerate in the sense of [10], so this gives a lower bound construction for (5), which is the best known.

Note that the polynomial $F(x, y, z)$ in our proof of Theorem 3 can be obtained from Valtr's polynomial $V(x, y, s, t)$ by setting $s = x$ and $t = z$.

4.2 More than four variables

For more than four variables, we do not have a statement that is entirely analogous to Theorem 2 or (5). Bays and Breuillard [2] proved a similar statement for any number of variables, but without an explicit exponent, and with a different description of the exceptional form. Also, Raz and Tov [11] extended Theorem 5 to any number of variables, with an explicit exponent.

Because for the Elekes–Szabó problem in more than four variables we do not have explicit exponents, and also because the appropriate definition of degeneracy is not clear, we only briefly touch on constructions for more variables here.

There are various ways of extending our constructions to more variables; one can for instance take the polynomial

$$F(x_1, \dots, x_m) = (x_1 + \cdots + x_{m-1})^2 + x_1 - x_m$$

and the grid A^m, where $A = [-n, 2n]$. Consider the set

$$T = \left\{(k_1, k_2 - k_1, \dots, k_{m-2} - k_{m-3}, \ell - k_{m-2}, k_1 + \ell^2) : 0 \leqslant k_i \leqslant n,\ 0 \leqslant \ell \leqslant \sqrt{n}\right\}.$$

Then we have $T \subset Z(F) \cap A^m$, which implies

$$\left|Z(F) \cap A^m\right| \gg n^{m-\frac{3}{2}}.$$

This should be compared with the Schwartz–Zippel bound $|Z(F) \cap A^m| \ll n^{m-1}$. A potential Elekes–Szabó theorem in m variables, i.e. an explicit version of the result of Bays and Breuillard, would give a bound of the form $|Z(F) \cap A^m| \ll n^{m-1-\eta_m}$ for some $\eta_m > 0$, under the condition that F is not degenerate in some sense. Presuming that our polynomial F is not of this form, it would show that we must have $\eta_m \leqslant 1/2$.

Acknowledgements

We are very grateful to Niels Lubbes, for a particularly interesting conversation which resulted in us attempting to find non-trivial constructions for the Elekes–Szabó problem. Thanks to József Solymosi for pointing out some helpful and relevant references. Thanks also to the anonymous referee for helpful corrections and suggestions.

References

[1] N. Alon, I. Ruzsa and J. Solymosi, *Sums, products and ratios along the edges of a graph*, Publ. Mat. **64**, no. 1, 143-155, 2020.

[2] M. Bays and E. Breuillard, *Projective geometries arising from Elekes–Szabó problems*, `arXiv:1806.03422`, 2018.

[3] G. Elekes, *A note on the number of distinct distances*, Period. Math. Hungar. **38**, 173–177, 1999.

[4] G. Elekes, *SUMS versus PRODUCTS in Number Theory, Algebra and Erdős Geometry*, Paul Erdős and his Mathematics II, Bolyai Society Mathematical Studies **11**, 241–290, 2002.

[5] G. Elekes and L. Rónyai, *A combinatorial problem on polynomials and rational functions*, J. Combin. Theory Ser. A **89**, 1–20, 2000.

[6] G. Elekes and E. Szabó, *How to find groups? (And how to use them in Erdős geometry?)*, Combinatorica **32**, 537–571, 2012.

[7] J. Matoušek, *Lectures on Discrete Geometry*, Springer, 2002.

[8] O.E. Raz, M. Sharir and J. Solymosi, *Polynomials vanishing on grids: The Elekes–Rónyai problem revisited*, Amer. J. Math. **138**, 1029–1065, 2016.

[9] O.E. Raz, M. Sharir and F. de Zeeuw, *Polynomials vanishing on Cartesian products: The Elekes–Szabó Theorem revisited*, Duke Math. J. **165**, 3517–1566, 2016.

[10] O.E. Raz, M. Sharir and F. de Zeeuw, *The Elekes–Szabó Theorem in four dimensions*, Israel J. Math. **227**, 663–690, 2018.

[11] O.E. Raz and Z.S. Tov, *Expanding polynomials: A generalization of the Elekes–Rónyai theorem to d variables*, arXiv:1807.02238, 2018.

[12] O. Roche-Newton and A. Warren, *Improved bounds for pencils of lines*, To appear in Proc. Amer. Math. Soc., preprint arXiv:1805.09188, 2018.

[13] R. Schwartz, J. Solymosi and F. de Zeeuw, *Extensions of a result of Elekes and Rónyai*, J. Combin. Theory Ser. A **120**, 1695–1713, 2013.

[14] P. Valtr, *Strictly convex norms allowing many unit distances and related touching questions*, manuscript, Charles University, Prague, 2005.

[15] F. de Zeeuw, *A survey of Elekes–Rónyai-type problems*, New Trends in Intuitive Geometry, 95–124, Springer, 2018.