The Multivariate Schwartz-Zippel Lemma

M. Levent Doğan[1], Alperen A. Ergür[2], Jake D. Mundo[3], and Elias Tsigaridas[4]

1 Technische Universität Berlin, Institut für Mathematik, Strasse des 17. Juni 136, 10623, Berlin, Germany
dogan@math.tu-berlin.de

2 Carnegie Mellon University, School of Computer Science, 5000 Forbes Avenue, Pittsburgh, PA, 15213, USA
aergur@cs.cmu.edu

3 Inria Paris and Institut de Mathématiques de Jussieu-Paris Rive Gauche, Sorbonne Université and Paris Université, France
elias.tsigaridas@inria.fr

4 Swarthmore College, Department of Mathematics & Statistics, 500 College Avenue, Swarthmore, PA, 19081, USA
jakedmundo@gmail.com

Abstract

Motivated by applications in combinatorial geometry, we consider the following question: Let $\lambda = (\lambda_1, \dots, \lambda_m)$ be an m-partition of n, let $S_i \subseteq \mathbb{C}^{\lambda_i}$ be finite sets, and let $S := S_1 \times S_2 \times \cdots \times S_m \subseteq \mathbb{C}^n$ be the multi-grid defined by S_i. If p is a degree d polynomial with n variables, how many zeros can p have on S?

We show that, except for a special family of polynomials –that we call λ-reducible– a natural generalization of the Schwartz-Zippel-DeMillo-Lipton Lemma holds. Moreover, we mention a symbolic algorithm to detect λ-reducibility for a special case. Along the way, we also present a multivariate generalization of Combinatorial Nullstellensatz, which might be of independent interest.

We refer the reader to the extended version of work [2] for further details, the missing proofs, and the presentation of the symbolic algorithm [2].

1 Introduction

Counting the number of zeros of a polynomial on a finite grid of points has been a subject of extensive research in combinatorics and theoretical computer science, see, for example, [6], [5]. The Schwartz-Zippel-DeMillo-Lipton Lemma is a well-known result in this line of research [7, 12, 3].

▶ **Theorem 1.1** (The Schwartz-Zippel-DeMillo-Lipton Lemma). *Let $\mathbb{F}$ be a field, let $S \subseteq \mathbb{F}$ be a finite set, and let $p \in \mathbb{F}[x_1, \dots, x_n]$ be a polynomial of degree d. Suppose $|S| > d$ and let $S^n := S \times S \times \cdots \times S$. Then we have*

$$|Z(p) \cap S^n| \leq d|S|^{n-1}$$

where $Z(p) = \{v \in \mathbb{F}^n \mid p(v) = 0\}$ is the zero set of p.

Alon [1] presents a similar statement for polynomials and grids. The result is known as Combinatorial Nullstellensatz:

▶ **Theorem 1.2** (Combinatorial Nullstellensatz). *Let $p \in \mathbb{F}[x_1, \dots, x_n]$ with $\deg(p) = \sum_{i=1}^{n} d_i$ for some positive integers d_i, and assume that the coefficient of $\prod_{i=1}^{n} x_i^{d_i}$ in p is non-zero.*

36th European Workshop on Computational Geometry, Würzburg, Germany, March 16–18, 2020.
This is an extended abstract of a presentation given at EuroCG'20. It has been made public for the benefit of the community and should be considered a preprint rather than a formally reviewed paper. Thus, this work is expected to appear eventually in more final form at a conference with formal proceedings and/or in a journal.

Let $S_i \subseteq \mathbb{F}$ be finite sets with $|S_i| > d_i$ and let $S \subseteq \mathbb{F}^n$ be defined by $S := S_1 \times S_2 \times \cdots \times S_n$. Then there exists $v \in S$ such that

$$p(v) \neq 0.$$

We generalize the Schwartz-Zippel-DeMillo-Lipton Lemma and the Combinatorial Nullstellensatz to *multi-grids.*

▶ **Definition 1.3** (Algebraic Degree of a Finite Set)**.** Let $\mathbb{F}$ be a field, and let $S \subseteq \mathbb{F}^n$ be a finite set of points. Let $I(S) \subseteq \mathbb{F}[x_1, \dots, x_n]$ be the ideal of polynomials vanishing on S. We define the algebraic degree, $\deg(S)$, of S to be

$$\deg(S) := \min_{0 \neq p \in I(S)} \deg(p).$$

For the univariate case we have $S \subseteq \mathbb{F}$ and so $\deg(S) = |S|$. However, for $n \geq 2$, one can have arbitrarily large sets of degree one. For example, in $\mathbb{F}^n$ we can consider arbitrarily many points sampled from a hyperplane. The only general relation between the size and the degree of a set $S \subseteq \mathbb{F}^n$ seems to be the following inequality that we can prove using basic linear algebra:

$$|S| \geq \binom{\deg(S) - 1 + n}{n}.$$

Notation We call a sequence $\lambda = (\lambda_1, \dots, \lambda_m)$ a partition of n into m parts if $n = \lambda_1 + \lambda_2 + \cdots + \lambda_m$. In this case, we write $\lambda \underset{m}{\vdash} n$. Given a partition $\lambda \underset{m}{\vdash} n$, we introduce the notation $\overline{x_1} = (x_1, x_2, \dots, x_{\lambda_1}), \overline{x_2} = (x_{\lambda_1+1}, \dots, x_{\lambda_1+\lambda_2})$, and so on. Given a polynomial $p \in \mathbb{F}[x_1, x_2, \dots, x_n]$, we denote by $\deg_i(p)$, the degree of p with respect to the variables in $\overline{x_i}$. Given finite sets $S_1 \subseteq \mathbb{F}^{\lambda_1}, S_2 \subseteq \mathbb{F}^{\lambda_2}$ etc. we call the product

$$S_1 \times S_2 \times \cdots \times S_m \subseteq \mathbb{F}^n$$

the multi-grid defined by $S_1, S_2, \dots, S_m$.

Now we can give our first result that forbids polynomials to vanish on multi-grids defined by finite sets of large degree:

▶ **Theorem 1.4.** *Let $\mathbb{F}$ be a field, $\lambda \underset{m}{\vdash} n$ be a partition of n into m parts, and let $p \in \mathbb{F}[x_1, \dots, x_n]$ be a polynomial with $\deg(p) = \sum_{i=1}^{m} d_i$. Furthermore, suppose that there exists a non-zero term x^α in p with $\deg_i(x^\alpha) = d_i$ for all $i \in [m]$. Let $S_i \subseteq \mathbb{F}^{\lambda_i}$ be finite sets, and let the multi-grid $S \subseteq \mathbb{F}^n$ be defined by $S := S_1 \times S_2 \times \cdots \times S_m$. If $\deg(S_i) > d_i$ for all $i \in [m]$, then there exists $v \in S$ such that*

$$p(v) \neq 0.$$

In the case that $\lambda = (1, 1, \dots, 1) \vdash n$, we obtain Alon's Combinatorial Nullstellensatz. In this sense, the above theorem is a generalization of Combinatorial Nullstellensatz. However, for the applications in incidence geometry, we want to obtain quantitative statements. In other words, we want to give bounds in terms of $|S_i|$. The next observation shows that it is not always possible to obtain such bounds:

▶ **Observation 1.5.** *Let $g_1 \in \mathbb{C}[x_1, x_2] \setminus \mathbb{C}$ and $g_2 \in \mathbb{C}[x_3, x_4] \setminus \mathbb{C}$. For any $h_1, h_2 \in \mathbb{C}[x_1, x_2, x_3, x_4]$ and $p = g_1h_1 + g_2h_2$, the zero set $Z(p)$ of p contains $Z(g_1) \times Z(g_2)$ which is a positive dimensional variety. Thus, we can have arbitrarily large finite sets $S_1 \subseteq Z(g_1)$ and $S_2 \subseteq Z(g_2)$ such that*

$$S_1 \times S_2 \subseteq Z(p).$$

As the above observation shows, in order to have a quantitative statement on $|Z(p) \cap S|$, one has to assume certain compatibility conditions between p and S:

▶ **Definition 1.6** (λ-irreducibility)**.** Let $\lambda \underset{m}{\vdash} n$ be a partition of n into m parts, and let $V \subseteq \mathbb{C}^n$ be an algebraic set. We call V λ-reducible if there exist positive dimensional varieties $V_i \subseteq \mathbb{C}^{\lambda_i}$ for $i = 1, \ldots, m$ such that

$$V_1 \times V_2 \times \cdots \times V_m \subseteq V.$$

We call V λ-irreducible otherwise. If V is a hypersurface defined by a polynomial p, then we say p is λ-reducible (resp. λ-irreducible).

Mojarrad et al. [4] study the same problem for the special case of $\lambda = (2, 2)$. Their observation is that $(2, 2)$-reducible polynomials have a particularly concrete form. Namely, a polynomial $p \in \mathbb{C}[x_1, x_2, x_3, x_4]$ is λ-reducible if and only if there exist polynomials $g_1 \in \mathbb{C}[x_1, x_2] \setminus \mathbb{C}, g_2 \in \mathbb{C}[x_3, x_4] \setminus \mathbb{C}$ and $h_1, h_2 \in \mathbb{C}[x_1, x_2, x_3, x_4]$ such that

$$p = g_1 h_1 + g_2 h_2.$$

Mojarrad et al. ask for an algorithm to check whether a given polynomial $p \in \mathbb{C}[x_1, x_2, x_3, x_4]$ is $(2, 2)$-reducible. In the last section, we mention an algorithm which detects λ-reducibility for partitions of the form $\lambda = (2, 2, \ldots, 2)$. The full details of this algorithm can be found in [2]. For now, we turn our attention back to polynomials and multi-grids.

Now, using the concept of λ-reducibility, we can give a bound on the cardinality of multi-grids on which a λ-irreducible polynomial can vanish:

▶ **Theorem 1.7.** *Let $\lambda \underset{m}{\vdash} n$ be a partition of n into m parts, and let $p \in \mathbb{C}[x_1, \ldots, x_n]$ be a λ-irreducible polynomial such that $\deg_i(p) = d_i$. Let $S_i \subseteq \mathbb{C}^{\lambda_i}$ be finite sets, and set $S := S_1 \times S_2 \times \cdots \times S_m$. If $|S_i| > d_i^{\lambda_i}$, then there exists $v \in S$ such that*

$$p(v) \neq 0.$$

We state our main theorem.

▶ **Theorem 1.8.** *Let $\lambda \underset{m}{\vdash} n$, let $S_i \subseteq \mathbb{C}^{\lambda_i}, i = 1, \ldots, m$ be finite sets, and let $S := S_1 \times S_2 \times \cdots \times S_m$ be the multi-grid defined by S_i. Then for a λ-irreducible polynomial p of degree $d \geq 2$, and for every $\varepsilon > 0$ we have*

$$|Z(p) \cap S| = O_{n,\varepsilon}\left(d^5 \prod_{i=1}^{m} |S_i|^{1-\frac{1}{\lambda_i+1}+\varepsilon} + d^{2n^4} \sum_{i=1}^{m} \prod_{j\neq i} |S_j| \right)$$

where $O_{n,\varepsilon}$ notation only hides constants depending on n and ε.

2 Applications

As our first application, we recover the complex version of Szemerédi-Trotter Theorem [10] on the number of incidences between points and lines in real plane. To our knowledge, this version is first proven by Tóth except for the ε in the exponent [11].

▶ **Corollary 2.1.** *Let P be a set of points and L be a set of lines in the complex plane $\mathbb{C}^2$, and let $\mathcal{I}(P, L)$ denote the set of point-line incidences. Then, for all $\varepsilon > 0$, we have*

$$|\mathcal{I}(P, L)| = O(|P|^{\frac{2}{3}+\varepsilon} |L|^{\frac{2}{3}+\varepsilon} + |P| + |L|).$$

Proof. Let $p = x_1 + x_2x_3 + x_4$. It is straightforward to show that p is $(2,2)$-irreducible. Moreover, for a point $v = (z_1, z_2) \in \mathbb{C}^2$ and a line $l : x + by + c = 0$, we have $p \in l$ if and only if $p(z_1, z_2, b, c) = 0$. Theorem 1.8 yields the result. ◀

As a second application, we consider the following problem: Given a set P of n points in the complex plane $\mathbb{C}^2$, can we bound the number of pairs $((v_1, v_2),(w_1, w_2)) \in P \times P$ such that $(v_1 - w_1)^2 + (v_2 - w_2)^2 = 1$? In the real plane, the problem is known as the unit distance problem and a subquadratic upper bound is given by Spencer, Szemerédi and Trotter [9]. In the complex case, Solymosi and Tao reproduced the same bound except for the ε in the exponent. [8]. We obtain the same bound using Theorem 1.8.

▶ **Corollary 2.2.** *Let $P \subseteq \mathbb{C}^2$ be a finite set of points in the complex plane. Set $S = \{((v_1, v_2),(w_1, w_2)) \in P \times P \mid (v_1 - w_1)^2 + (v_2 - w_2)^2 = 1\}$. Then, for all $\varepsilon > 0$, we have*

$$|S| = O(|P|^{4/3+\varepsilon}).$$

Proof. Let $p = (x_1 - y_1)^2 + (x_2 - y_2)^2 - 1 \in \mathbb{C}[x_1, x_2, y_1, y_2]$. We claim that no 3×3 multi-grid is contained in $Z(p)$. Given three distinct points $u = (u_1, u_2), v = (v_1, v_2), w = (w_1, w_2) \in \mathbb{C}^2$, the system

$$\begin{aligned} p(u_1, u_2, y_1, y_2) &= 0 \\ p(v_1, v_2, y_1, y_2) &= 0 \\ p(w_1, w_2, y_1, y_2) &= 0 \end{aligned}$$

has at most one solution: If u, v, w are on an affine (complex) line, a direct computation shows that the above system has no solution. If they are not on an affine (complex) line then taking differences between pairs of polynomials in the above system, we see that

$$\begin{bmatrix} y_1 & y_2 \end{bmatrix} \cdot \begin{bmatrix} v_1 - u_1 & w_1 - u_1 & w_1 - v_1 \\ v_2 - u_2 & w_2 - u_2 & w_2 - v_2 \end{bmatrix} = 0$$

and as u, v, w are affinely independent, we obtain $y = 0$. We deduce that p is $(2,2)$-irreducible and applying Theorem 1.8 to $\varepsilon/2$ yields the result. ◀

▶ **Theorem 2.3** (The Sparse Hypersurface-Point Incidence Theorem). *Let $A = \{a_1, a_2, \ldots, a_k\}$ be a set of lattice points in $\mathbb{Z}^n_{\geq 0}$ with $\sum_{j=1}^n a_{ij} \leq d$ for all $1 \leq i \leq k$. We say a polynomial f is supported in A if*

$$f = \sum_{j=1}^{k} c_j x^{a_j}$$

where $c_j \in \mathbb{C}$ and $x^{a_j} = x_1^{a_{j1}} x_2^{a_{j2}} \ldots x_n^{a_{jn}}$. Let P be a set of points in $\mathbb{C}^n$, L be a set of polynomials supported in A, and let $\mathcal{I}(P, L)$ denote the set of incidences between P and L. We assume for any sets $U_1 \subseteq P$ with $|U_1| > d^n$ and $U_2 \subseteq L$ with $|U_2| > d^k$, the product $U_1 \times U_2$ is not included in $\mathcal{I}(P, L)$. Then, for all $\varepsilon > 0$, we have

$$|\mathcal{I}(P, L)| = O_{n,k,\varepsilon}(d^3 |P|^{1-\frac{1}{n+1}+\varepsilon} |L|^{1-\frac{1}{k+1}+\varepsilon} + d^{(n+k)^4}(|P| + |L|)).$$

3 Algorithms

In [2], Section 3, we give an algorithm for the following problem:

Problem: Consider the partition $\lambda = (n, n, \ldots, n)$ of $n(m+1)$ into $m+1$ parts. Given a polynomial $p \in \mathbb{Q}[\overline{x_1}, \overline{x_2}, \ldots, \overline{x_{m+1}}]$, are there polynomials $g_i \in \mathbb{Q}[\overline{x_i}] \setminus \mathbb{Q}$ and $h_i \in \mathbb{Q}[\overline{x_1}, \overline{x_2}, \ldots, \overline{x_{m+1}}]$ such that

$$p = \sum_{i=1}^{m+1} g_i h_i \quad ? \tag{1}$$

Equivalently, are there hypersurfaces $\mathcal{V}_i \subseteq \mathbb{C}^n$ such that

$$\mathcal{V}_1 \times \mathcal{V}_2 \times \cdots \times \mathcal{V}_{m+1} \subseteq V(p) \subseteq \mathbb{C}^{n(m+1)},$$

where $\mathcal{V}_i = V(g_i)$ are the zero sets of the polynomials g_i for $i \in [m+1]$?

In the case that $\lambda = (2, 2, \ldots, 2)$, we can check λ-reducibility using the previous algorithm: If p is $(2, 2, \ldots, 2)$-reducible, then it contains a product

$$\mathcal{V}_1 \times \mathcal{V}_2 \times \cdots \times \mathcal{V}_m \subseteq Z(p)$$

where each $\mathcal{V}_i$ is an algebraic curve in $\mathbb{C}^2$. As $\mathcal{V}_i$ are hypersurfaces, they can be written as $\mathcal{V}_i = Z(g_i)$ for some polynomials $g_i \in \mathbb{C}[x_{2i}, x_{2i+1}] \setminus \mathbb{C}$ and thus p is contained in the ideal generated by $g_1, \ldots, g_m$. Conversely, if p is contained in the ideal generated by $(g_1, \ldots, g_m)$, then p contains the product $\mathcal{V}_1 \times \mathcal{V}_2 \times \cdots \times \mathcal{V}_m$ in its zero set. We deduce that a polynomial $p \in \mathbb{C}[x_1, x_2, \ldots, x_{2n}]$ is $(2, 2, \ldots, 2)$-reducible if and only if it is of the form

$$p(x_1, \ldots, x_{2n}) = \sum_{i=1}^{n} g_i(x_{2i}, x_{2i+1}) h_i(x_1, \ldots, x_{2n}),$$

for some $g_i \in \mathbb{C}[x_{2i}, x_{2i+1}] \setminus \mathbb{C}$ and $h_i \in \mathbb{C}[x_1, \ldots, x_{2n}]$. We can detect this property using our algorithm.

We leave the existence of an algorithm that detects λ-reducibility for general λ as an open problem.

Acknowledgements

ET is partially supported by ANR JCJC GALOP (ANR-17-CE40-0009), a public grant as part of the Investissement d'avenir project reference ANR-11-LABX-0056-LMH LabEx LMH (PGMO ALMA), and the PHC GRAPE.

References

1 N. M. Alon. Combinatorial Nullstellensatz. *Combinatorics Probability and Computing*, 8(1-2):7–29, 1 1999. doi:10.1017/S0963548398003411.

2 M. L. Doğan, A. A. Ergür, J. D. Mundo, and E. Tsigaridas. The multivariate schwartz-zippel lemma, 2019. arXiv:1910.01095.

3 R. J. Lipton. The curious history of the Schwartz-Zippel lemma. https://rjlipton.wordpress.com/2009/11/30/the-curious-history-of-the-schwartz-zippel-lemma/.

4 H. N. Mojarrad, T. Pham, C. Valculescu, and F. de Zeeuw. Schwartz-Zippel bounds for two-dimensional products. *Discrete Analysis*, 2018. URL: http://dx.doi.org/10.19086/da.2750, doi:10.19086/da.2750.

5 Orit E. Raz, Micha Sharir, and József Solymosi. Polynomials vanishing on grids: The Elekes-Rónyai problem revisited, 2014. arXiv:1401.7419.

6 N. Saxena. Progress on Polynomial Identity Testing - II, 2014. arXiv:1401.0976.

7 J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, October 1980. URL: https://doi.org/10.1145/322217.322225, doi:10.1145/322217.322225.

8 József Solymosi and Terence Tao. An incidence theorem in higher dimensions. *Discrete & Computational Geometry*, 48(2):255–280, 2012. URL: https://doi.org/10.1007/s00454-012-9420-x, doi:10.1007/s00454-012-9420-x.

9 J. Spencer, E. Szemerédi, and W.T. Trotter. *Unit distances in the Euclidean plane*, pages 294–304. Academic Press, 1984.

10 E. Szemerédi and W. T. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3(3):381–392, 1983. URL: https://doi.org/10.1007/BF02579194, doi:10.1007/BF02579194.

11 C. D. Tóth. The Szemerédi-Trotter theorem in the complex plane. *Combinatorica*, 35(1), Feb 2015. URL: http://dx.doi.org/10.1007/s00493-014-2686-2, doi:10.1007/s00493-014-2686-2.

12 R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and Algebraic Computation*, pages 216–226, Berlin, Heidelberg, 1979. Springer Berlin Heidelberg.