# A PSPACE Construction of a Hitting Set for the Closure of Small Algebraic Circuits

Michael A. Forbes*
University of Illinois at Urbana-Champaign
Department of Computer Science
USA
miforbes@illinois.edu

Amir Shpilka†
Tel Aviv University
Department of Computer Science
Tel Aviv, Israel
shpilka@post.tau.ac.il

## ABSTRACT

In this paper we study the complexity of constructing a hitting set for $\overline{\mathsf{VP}}$, the class of polynomials that can be infinitesimally approximated by polynomials that are computed by polynomial sized algebraic circuits, over the real or complex numbers. Specifically, we show that there is a PSPACE algorithm that given $n, s, r$ in unary outputs a set of inputs from $\mathbb{Q}^n$ of size $\mathrm{poly}(n, s, r)$, with $\mathrm{poly}(n, s, r)$ bit complexity, that hits all $n$-variate polynomials of degree $r$ that are the limit of size $s$ algebraic circuits. Previously it was known that a random set of this size is a hitting set, but a construction that is certified to work was only known in EXPSPACE (or EXPH assuming the generalized Riemann hypothesis). As a corollary we get that a host of other algebraic problems such as Noether Normalization Lemma, can also be solved in PSPACE deterministically, where earlier only randomized algorithms and EXPSPACE algorithms (or EXPH assuming the generalized Riemann hypothesis) were known.

The proof relies on the new notion of a *robust hitting set* which is a set of inputs such that any nonzero polynomial that can be computed by a polynomial size algebraic circuit, evaluates to a not too small value on at least one element of the set. Proving the existence of such a robust hitting set is the main technical difficulty in the proof.

Our proof uses anti-concentration results for polynomials, basic tools from algebraic geometry and the existential theory of the reals.

## CCS CONCEPTS

• **Theory of computation → Algebraic complexity theory**; *Pseudorandomness and derandomization*;

## KEYWORDS

Algebraic circuits, Arithmetic Circuits, explicit construction, hitting-set, polynomial identity testing, PSPACE

**ACM Reference Format:**
Michael A. Forbes and Amir Shpilka. 2018. A PSPACE Construction of a Hitting Set for the Closure of Small Algebraic Circuits. In *Proceedings of 50th Annual ACM SIGACT Symposium on the Theory of Computing (STOC'18).* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3188745.3188792

## 1 INTRODUCTION

This paper studies the following question. What is the complexity of constructing a set of points $\mathcal{H} \subset \mathbb{R}^n$, of small bit complexity, that is guaranteed to be a hitting set for polynomials that can be infinitesimally approximated by small algebraic circuits over the real or complex numbers? Recall that $\mathcal{H}$ is a hitting set for a class of polynomials $\mathcal{C}$ if for every $f \in \mathcal{C}$ there is some $\mathbf{v} \in \mathcal{H}$ such that $f(\mathbf{v}) \neq 0$. The class of polynomials that can be infinitesimally approximated by poly-size algebraic circuits is commonly denoted by $\overline{\mathsf{VP}}$. Thus, we ask what is the complexity of constructing a hitting set for $\overline{\mathsf{VP}}$.[1]

Relying on a result of Heintz and Sieveking [HS80b], who proved that the variety of efficiently computed polynomials has polynomial dimension and exponential degree, Heintz and Schnorr [HS80a] showed that there is a poly-size hitting set for $\overline{\mathsf{VP}}$, and that a random set of the appropriate polynomial size is a hitting set with high probability. If we were satisfied with a 99.9% percent guarantee then picking $\mathcal{H}$ at random would work [HS80a]. The main difficulty however is certifying that the set that we constructed is a hitting set.

The problem of explicitly constructing an object whose existence is known by probabilistic arguments has received a lot of attention. The question is usually most difficult when there is no efficiently computable certificate to test whether a candidate construction satisfies the required properties. For example, consider $d$-regular expander graphs that have expansion larger than half the degree. By probabilistic arguments we know that random $d$-regular graphs are such expanders. Yet, we don't know of an efficiently checkable certificate that certifies such large expansion (for expansion less than $d/2$ we can use spectral methods to certify expansion). Another such question arises in construction of Ramsey graphs. We know that when picking a graph at random from $G(n, 1/2)$ (i.e. each edge

[1] One can think of algebraic circuits over the reals, but our results hold for the complex numbers as well. To prove our results it will be convenient to assume that we work over algebraically closed fields, but at the end we output a set $\mathcal{H} \subset \mathbb{Q}^n$ of small bit complexity.

*This work was completed when the first author was at Stanford University, supported by the NSF, including NSF CCF-1617580, and the DARPA Safeware program; and when the author was at the Simons Institute for the Theory of Computing, at the University of California, Berkeley.
†The research leading to these results has received funding from Israel Science Foundation (grant number 552/16) and from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 257575. Part of this work was done while the second author was at NYU.


*STOC'18, June 25–29, 2018, Los Angeles, CA, USA*

ACM ISBN 978-1-4503-5559-9/18/06…$15.00
https://doi.org/10.1145/3188745.3188792

is picked with probability 1/2) with high probability it will not have cliques nor anti-cliques of size larger than, say, $3 \log n$. Despite many recent advances it is not known how to efficiently construct such graphs nor to check whether a given graph has this property. Constructing binary codes that meet the Gilbert-Varshamov bound is yet another such problem and so is the question of constructing a truth table of length $n$ that cannot be computed by boolean circuits (on $\log n$ bits) of size, say, $\sqrt{n}$. A more extreme example is that of constructing strings with large Kolmogorov complexity. A random string of length $n$ will have Kolmogorov complexity of $\Omega(n)$, but the question of deciding the Kolmogorov complexity of a string is undecidable.

We note that even when an object is known to exist via probabilistic arguments it is still not clear that it can be deterministically constructed, even in PSPACE. Indeed, in PSPACE we can go over all choices of random coins for our randomized algorithm and for each construct the potential object, yet when no efficiently checkable certificate is known it is not clear how to verify that the object that we constructed have the required properties. For the questions mentioned above, of constructing expander graphs, Ramsey graphs, codes that meet the Gilbert-Varshamov bound or hard truth tables, it is clear how to check in PSPACE whether they have the required property.

The situation is quite different when we think about hitting sets for $\overline{\mathsf{VP}}$. One such difference is that for hitting sets it is impossible to go over all polynomials in $\overline{\mathsf{VP}}$ as there are infinitely many such polynomials. Furthermore, we do not know an efficient way of representing them as they are limits of polynomials in VP and are not believed to have small circuits themselves: Recall that over the real or complex numbers $\overline{\mathsf{VP}}$ has several equivalent definitions, the easiest may be that a polynomial $f$ is in $\overline{\mathsf{VP}}$ if there exists a sequence of polynomials $\{f_i\}$ such that each $f_i$ can be computed by a size $n^c$ (for some constant $c$) algebraic circuit such that $f_i \to f$ coefficient-wise.[2] The best upper bound on the complexity of polynomials in $\overline{\mathsf{VP}}$ is exponentially larger than the complexity of the approximating polynomials (which is nontrivial as the degrees could be polynomially large). See [LL89, Bür04] for the exponential upper bound and also [GMQ16] for polynomial upper bound if one tweaks the definition of $\overline{\mathsf{VP}}$ by restricting the type of allowed approximations. Thus, there is no guarantee that polynomials in $\overline{\mathsf{VP}}$ have concise representation using algebraic circuits. To get a sense of why the complexity of a limit polynomial may be larger consider the tensor associated with univariate polynomial multiplication modulo $X^2$. That is, $T = x_0y_0z_0 + (x_1y_0 + x_0y_1)z_1$. It is known that the tensor rank of $T$ is 3. However, $T$ can be represented as the limit of rank 2 tensors: For any $\varepsilon \neq 0$ consider the tensor

$$T_\varepsilon = \frac{1}{\varepsilon} \cdot (x_0 + \varepsilon x_1) \cdot (y_0 + \varepsilon y_1) \cdot z_1 + x_0 \cdot y_0 \cdot (z_0 - \frac{1}{\varepsilon} z_1)$$
$$= x_0y_0z_0 + (x_1y_0 + x_0y_1)z_1 + \varepsilon \cdot x_1y_1z_1 \ .$$

It is clear that as $\varepsilon \to 0$ we get $T_\varepsilon \to T$. This example shows that limits of algebraic computations can have smaller complexity than each of the polynomials in the sequence.

[2] One can define the class $\overline{\mathsf{VP}}$ over fields of positive characteristic using notion similar to border rank but we do not need this alternative definition here.

The question of constructing a hitting set for $\overline{\mathsf{VP}}$ that is guaranteed to work was raised by Mulmuley [Mul17]. Specifically, Mulmuley asked what is the complexity of constructing a set that is guaranteed to be a hitting set for VP and $\overline{\mathsf{VP}}$. For VP he observed that a hitting set can be constructed in PSPACE (when the parameters of the circuits are given in unary) and that, assuming the generalized Riemann hypothesis (GRH for short), it can be brought down to PH using a result of Koiran [Koi96]. The idea is to reduce the question of checking whether a given set of points is not a hitting set to a question regarding the satisfiability of a certain set of polynomial equations in poly($n$) variables and polynomial degree. I.e., to an instance of Hilbert's Nullstellensatz problem. However, for $\overline{\mathsf{VP}}$ the situation is more complicated as polynomials in this class are not known (nor believed) to have small algebraic circuits. Thus, it is not clear whether the question of checking whether $\mathcal{H}$ is or is not a hitting set could be reduced to Hilbert's Nullstellensatz problem. Using Gröbner basis, Mulmuley gave an EXPSPACE algorithm[3] for constructing such a hitting set [Mul17].

Mulmuley raised this question due of its applicability to other questions on the borderline of geometry and complexity, mainly the so called Noether Normalization Lemma (NLL) question. He showed that constructing a normalization map could be reduced to constructing a hitting set for $\overline{\mathsf{VP}}$ and thus concluded that it can be solved using randomness with a Monte Carlo algorithm, or deterministically in EXPSPACE.

We note that the problem we consider is that of constructing a (qualitatively) optimal hitting set. This in particular implies a deterministic black-box PIT algorithm for $\overline{\mathsf{VP}}$ which inherits the PSPACE complexity of our construction. However, this latter result is easy to obtain directly, as one can simply evaluate the circuit over the (exponentially large) set $\{0, \ldots, r\}^n$. The correctness follows from polynomial interpolation, and one can iteratively evaluate a circuit on all points of this set in PSPACE.

## 1.1 Our Results

Here we show that the problem of constructing a hitting set for $\overline{\mathsf{VP}}$ is in PSPACE, which bears the same consequences for the results obtained in Mulmuley's paper.

**Theorem 1.1** (Informal statement of main result (Theorem 7.1))**.** *For integers $n, s, r$ there is an algorithm that runs in* poly$(n, s, r)$*-space and constructs a* poly$(n, s, r)$*-size hitting set for all polynomials that can be infinitesimally approximated by $n$-variate homogeneous algebraic circuits of size $s$ and degree $r$.*

From the work of Mulmuley it follows that PSPACE algorithms could also be devised for constructing normalizing maps (as in Noether Normalization Lemma). We refer the readers to [Mul17] for more on Noether Normalization Lemma. As introducing all the relevant definitions and concepts from [Mul17] requires substantial work and this is not the main focus of our work we rely on the notation of [Mul17] in the statement of the next two theorems.

**Theorem 1.2** (NNL for $\Delta[det, m]$ in PSPACE (see Theorem 4.1 of [Mul17]))**.** *The problem of constructing an h.s.o.p. for $\Delta[det, m]$, specified succinctly, belongs to* PSPACE.

[3] Assuming the generalized Riemann hypothesis his algorithm can be modified to yield an EXPH algorithm using [Koi96].

A similar result holds for other explicit varieties.

**Theorem 1.3** (NNL for explicit varieties in PSPACE (see Theorem 5.5 of [Mul17])). *The problem of constructing an h.s.o.p. for an explicit variety $W_n$ belongs to* PSPACE.

Another corollary of our result is that for every $s = \text{poly}(n)$ we can construct in PSPACE the coefficients of an $n$-variate polynomial of constant degree that cannot even be approximated by algebraic circuits of size $s$.

**Theorem 1.4.** *For every constant $c$ there is a constant $c'$ such that there is a* PSPACE *algorithm that outputs the coefficients of an $n$ variate polynomial of degree $c'$ that is not in the closure of algebraic circuits of size $n^c$.*

Sketch of proof. The idea is to find in PSPACE a hitting set for the closure of size $s$ circuits. This hitting set has size $|\mathcal{H}| = \text{poly}(s)$. Then, by solving a system of linear equations one can find a non zero polynomial of degree roughly $\log|\mathcal{H}|/\log n$, that vanishes on the points in $\mathcal{H}$. By the construction of $\mathcal{H}$ this polynomial is not in the closure of size $s$ algebraic circuits. □

We end this part of the introduction by mentioning a natural open problem.

**Open Problem 1.** *Can the problem of constructing a hitting set for* $\overline{\text{VP}}$ *be solved in* PH *(assuming GRH)?*

## 1.2 Sketch of Proof

The first observation is that constructing a hitting set for size $s$ and degree $r$ homogeneous circuits (i.e. for circuits in VP) can be done in PSPACE. The idea is that one can enumerate over all subsets of, say, $[r^2]^n$ of size, say, $(nrs)^{10}$, and for each such subset check whether there exists a circuit that computes a nonzero polynomial that vanishes over the subset. The existence of such a circuit can be checked using the universal circuit. The universal circuit $\Psi(\mathbf{x},\mathbf{y})$ is a circuit in $n$ essential variables $\mathbf{x}$ and $\text{poly}(r,s)$ auxiliary variables $\mathbf{y}$ such that for any size $s$ and degree $r$ circuit $\Phi(\mathbf{x})$ there is an assignment $\mathbf{a}$, to the auxiliary variables, so that the polynomials computed by $\Psi(\mathbf{x},\mathbf{a})$ and $\Phi(\mathbf{x})$ are the same. Thus, if our subset is $\mathbf{v}_1,\ldots,\mathbf{v}_m$ we can check whether there exists a solution to $\Psi(\mathbf{v}_i,\mathbf{a}) = 0$ for all $i \in [m]$ and $\Psi(\mathbf{u},\mathbf{a}) = 1$.[4] The problem of deciding whether a system of polynomial equalities has a complex solution is known as Hilbert's Nullstellensatz problem in the computer science literature. It is solvable in PSPACE and assuming the Generalized Riemann Hypothesis (GRH) it is solvable in PH (the polynomial hierarchy), see [Koi96].

We would like to use the same idea to construct hitting sets for polynomials that can be infinitesimally approximated by size $s$ and degree $r$ circuits. The problem is that even if $\mathcal{H}$ is a hitting set for size $s$ and degree $r$, it may be the case that for a sequence of polynomials $\{f_i\}$, even if $f_i(\mathbf{v}) \neq 0$ for all $i$, the limit polynomial may still vanish at $\mathbf{v}$. Thus, it is not clear that $\mathcal{H}$ also hits the closure of size $s$ and degree $r$. Indeed, consider the example given in Section 1:

$$T = x_0y_0z_0 + (x_1y_0 + x_0y_1)z_1$$

and

$$T_\varepsilon = \frac{1}{\varepsilon}\cdot(x_0+\varepsilon x_1)\cdot(y_0+\varepsilon y_1)\cdot z_1 + x_0\cdot y_0\cdot(z_0-\frac{1}{\varepsilon}z_1)$$
$$= x_0y_0z_0 + (x_1y_0+x_0y_1)z_1 + \varepsilon\cdot x_1y_1z_1\ .$$

In addition to showing that the complexity of $T$ (measured in terms of tensor rank) is larger than that of any of the polynomials approximating it, it also demonstrates that constructing a hitting set for VP may not be sufficient for constructing a hitting set for $\overline{\text{VP}}$. Just to illustrate the difference consider the input $(x_0,x_1) = (y_0,y_1) = (z_0,z_1) = (0,1)$. Each of the tensors in the sequence is nonzero on this input, and indeed $T_\varepsilon((0,1),(0,1),(0,1)) = \varepsilon \neq 0$, but in the limit we get zero, whereas the limit tensor is not the zero tensor. Thus, the input $(x_0,x_1) = (y_0,y_1) = (z_0,z_1) = (0,1)$ "hits" every polynomial in the sequence but the limit polynomial vanishes on it. Thus, a hitting set for a class of polynomials $\mathcal{C}$ does not necessarily extends to the closure of $\mathcal{C}$. However, this does not rule out getting hitting sets for $\bar{\mathcal{C}}$ via hitting sets for a class of polynomials only slightly stronger than $\mathcal{C}$, or by strengthening the notion of a hitting set for $\mathcal{C}$ which is what we do here.

To overcome the discrepancy between a hitting set for VP and a hitting set for $\overline{\text{VP}}$, we would like to find what we call a "robust hitting set". In a nutshell, a robust hitting set $\mathcal{H}$ is such that for every polynomial $f$ that can be computed by a size $s$ and degree $r$ circuit, after an adequate normalization, there will be a point in $\mathcal{H}$ on which $f$ evaluates to at least, say, 1. Thus, if $f_i$ are all normalized and evaluate to at least 1 on $\mathbf{v}$, then if $\lim f_i = f$ then by continuity $f$ also evaluates to at least 1 on $\mathbf{v}$. Thus, $\mathcal{H}$ hits $f$ as well (this idea is captured by Claim 5.2).

Hence, the first step in our proof is to first prove the existence of robust hitting sets. We note that Heintz and Schnorr [HS80a] proved the existence of a small hitting set for size $s$ and degree $r$ circuits, but their proof does not yield robust hitting sets. To prove the existence of such hitting sets we use anti-concentration results for polynomials of Carbery-Wright [CW01]. These results show that for a given polynomial, if we sample enough evaluation points at random, then with high probability the polynomial will evaluate to a large value on at least one of those points. This is not enough though as we cannot use the union bound since there are infinitely many circuits. What we do instead is find an $\varepsilon$-net in the set of all efficiently computable polynomials. For this we use the bounds given by Heintz and Sieveking [HS80b] on the dimension and degree of the algebraic variety of efficiently computable polynomials. We prove that for an algebraic variety in $\mathbb{C}^N$, of dimension $d$ and degree $D$, there exists an $\varepsilon$-net of size roughly $D\cdot(N/\varepsilon)^{O(d)}$. Combining the two results we are able to prove the existence of a polynomially small robust hitting set for the variety of efficiently computable polynomials. Showing the existence of robust hitting sets is the main technical difficulty in the proof.

Now that we know that robust hitting sets exist the PSPACE algorithm works as follows. It enumerates over all subsets of a relevant domain of polynomial size. For each such subset it checks whether there exists an algebraic circuit that has the right normalization (e.g. that evaluates to at least 1 on some input from $[-1,1]^n$) and that evaluates to at most $\varepsilon$ on all points in the subset. If such a solution is found then the subset is not robust and we move to the next subset. To check whether such a solution exists we need

[4] Since $\Psi(\mathbf{x},\mathbf{a})$ is a homogeneous polynomial in $\mathbf{x}$, if it is not identically zero then on some input $\mathbf{u}$ it evaluates to 1.

to express this system of inequalities as a formula in the language of the existential theory of the reals. Then we use the fact that formulas in this language can be decided in PSPACE to conclude that our algorithm works in PSPACE.

### 1.3 Organization

The rest of the paper is organized as follows. Section 2 contains some preliminaries including the notation we use throughout the paper (Section 2.1), the definition of universal algebraic circuit (Section 2.2) and some basic results concerning norms of polynomials and the relation between them (Section 2.3). Section 3 contains results concerning anti-concentration of polynomials. In Section 4 we discuss basic properties of algebraic varieties and state some results concerning the variety of polynomials computed by poly-size algebraic circuits. In Section 4.1 we give an upper bound on the size of $\varepsilon$-net for algebraic varieties of polynomial dimension and exponential degree. Then, in Section 5 we prove the existence of a robust hitting set for algebraic circuits. We discuss the existential theory of the reals in Section 6 and in Section 7 we give the PSPACE algorithm for constructing a hitting set for $\overline{\mathrm{VP}}$.

## 2 PRELIMINARIES

### 2.1 Notation

We shall use the following notation. We do not mention which variety or circuit we study rather just that we shall use this parameters for every circuit or variety.

- $n$ is number of variables in the circuit
- $s$ is size of circuit
- $r$ is degree of circuit
- $d$ is dimension of variety
- $D$ is degree of variety
- $N_{n,r}^{\mathrm{hom}} = \binom{n+r-1}{r}$ is number of homogeneous monomials in $n$ variables of degree $r$
- $\mathbf{v}, \mathbf{u}, \mathbf{e}$ points in $\mathbb{R}^*$
- $\mathbf{x}$ vector of variables
- $f(\mathbf{x})$ is a polynomial and $\mathbf{f}$ is its vector of coefficients
- For $0 < \delta < 1$, $G_\delta = \{-1, -1+\delta, -1+2\delta, \ldots, 1-2\delta, 1-\delta\}^n$ is the grid
- $\iota = \sqrt{-1}$ is the complex imaginary root of $-1$
- $[-1,1]_{\mathbb{C}}^N = [-1,1]^N + \iota \cdot [-1,1]^N = \{\mathbf{a} + \iota \cdot \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in [-1,1]^N\}$.
- For $0 < \delta < 1$, $G_\delta^{\mathbb{C}} = \{a + \iota \cdot b \mid a, b \in \{-1, -1+\delta, -1+2\delta, \ldots, 1-2\delta, 1-\delta\}^n\}$ is the grid in $\mathbb{C}$.
- For $0 < \delta < 1$, $G_{\delta,r} \triangleq \{\mathbf{a} + k \cdot \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in G_\delta \text{ and } 0 \le k \le r\}$.
- $\Psi, \Phi$ denote circuits

### 2.2 Algebraic Circuits

An *algebraic circuit* is a directed acyclic graph whose leaves are labeled by either variables $x_1, \ldots, x_n$ or elements from the field $\mathbb{F}$,[5] and whose internal nodes are labeled by the algebraic operations of addition ($+$) or multiplication ($\times$). Each node in the circuit computes a polynomial in the natural way, and the circuit has one or more *output nodes*, which are nodes of out-degree zero. The *size* of the circuit is defined to be the number of wires, and the *depth* is defined to be the length of a longest path from an input node to the output node. A circuit is called *homogeneous* if every gate in it computes a homogeneous polynomial.

A useful notion is that of a universal algebraic circuit, which is a circuit that "encodes" all circuits of somewhat smaller size.

**Definition 2.1** (Universal circuit). *A homogeneous algebraic circuit $\Psi$ is said to be universal for $n$-variate homogeneous circuits of size $s$ and degree $r$ if $\Psi$ has $n$ essential-inputs $\mathbf{x}$ and $m$ auxiliary-inputs $\mathbf{y}$, such that for every homogeneous $n$-variate polynomial $f$ of degree $r$ that is computed by an homogeneous algebraic circuit of size $s$ there exists an assignment $\mathbf{a}$ to the $m$ auxiliary-variables of $\Psi$ such that the polynomial computed by $\Psi(\mathbf{x}, \mathbf{a})$ is $f(\mathbf{x})$.* ◊

The existence of efficiently computable universal circuits was shown by Raz [Raz10] (see also [SY10]).

**Theorem 2.2** (Universal circuit). *There exist constants $c_1$ and $c_2$ such that the following hold. For any natural numbers $n, s, r$ there exists a homogeneous circuit $\Psi$ such that $\Psi$ has $n$ essential-variables, $c_1 \cdot sr^4$ auxiliary-variables, degree $c_2 \cdot r$ and size $c_1 \cdot sr^4$,[6] and it is universal for $n$-variate homogeneous circuits of size $s$ and degree $r$. Furthermore, for any polynomial $f(\mathbf{x})$ that can be computed by $\Psi$ and any constant $\alpha$, the polynomial $\alpha \cdot f$ can also be computed by $\Psi$.*

### 2.3 Norms of Polynomials

**Definition 2.3** (Norm of a polynomial). *For an $n$-variate polynomial $f(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ we denote*

$$\|f\|_2 := \left( \int_{[-1,1]^n} |f(\mathbf{x})|^2 d\mu(\mathbf{x}) \right)^{1/2} = \left( \mathcal{E}_\mu[f^2] \right)^{1/2},$$

*where $\mu(\mathbf{x})$ is the uniform probability measure on $[-1,1]^n$. We also denote*

$$\|f\|_\infty = \max_{\mathbf{v} \in [-1,1]^n} |f(\mathbf{v})|.$$

◊

**Remark 2.4.** *We shall also need to work with the usual Euclidean norm of vectors. To avoid confusion we shall denote the usual Euclidean norm of a vector $\mathbf{v}$ with $\|\mathbf{v}\|$. I.e., we omit the subscript when dealing with the Euclidean norm.* ◊

We will need some basic results relating the $L_\infty$ norm of a polynomial to its $L_2$ norm. We start by stating a result of Wilhelmsen that generalizes a classical result by Markov for univariate polynomials.

**Theorem 2.5** (Multivariate Markov's theorem [Wil74]). *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a homogeneous polynomial of degree $r$, that for every $\mathbf{v} \in [-1,1]^n$ satisfies $|f(\mathbf{v})| \le 1$. Then, for every $\|\mathbf{v}\| \le 1$ it holds that $\|\nabla(f)(\mathbf{v})\| \le 2r^2$.*

Denote with $B(n, \alpha, \mathbf{u})$ the $n$-dimensional ball of radius $\alpha$ around $\mathbf{u}$ and with $\mathrm{Vol}(n, \alpha)$ its volume.

**Corollary 2.6.** *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a homogeneous polynomial of degree $r$. Then,*

$$\|f\|_2 \ge \frac{1}{2^{2n+2}} \|f\|_\infty \cdot \mathrm{Vol}(n, \frac{1}{4r^2}) .$$

[5] In this paper we only consider fields of characteristic zero.

[6] We can assume without loss of generality that the number of auxiliary variables is the same as the size of the circuit as we can ignore some of the variables.

Proof. By normalizing $f$ it is enough to prove the result for the case $\|f\|_\infty = 1$.

Let $\mathbf{u} \in [-1,1]^n$ be such that $1 = \|f\|_\infty = |f(\mathbf{u})|$. Assume further, w.l.o.g. that $f(\mathbf{u}) = 1$. Consider the intersection $A = B(n, \frac{1}{4r^2}, \mathbf{u}) \cap [-1,1]^n$. We have that $\mu(A) \geq \frac{1}{4^n} \cdot \mathrm{Vol}(n, \frac{1}{4r^2})$, where $\mu(\mathbf{x})$ is the uniform measure on $[-1,1]^n$. Indeed, $\mu$ scales down by a factor of $2^n$ the usual measure of $A$, and it is immediate that $A$ contains at least a fraction $2^{-n}$ of $\mathrm{Vol}(B(n, \frac{1}{4r^2}, \mathbf{u}))$.

Theorem 2.5 implies that for any $\mathbf{v} \in A$, it holds that $f(\mathbf{v}) \geq \frac{1}{2}$. Indeed, this follows immediately from the bound on the gradient of $f$, the assumption that $f(\mathbf{u}) = 1$ and the fact that $\|\mathbf{u} - \mathbf{v}\| \leq \frac{1}{4r^2}$. Thus, we get that

$$\|f\|_2 = \int |f(\mathbf{x})|^2 d\mu(\mathbf{x}) \geq \frac{1}{4}\mu(A) \geq \frac{1}{2^{2n+2}} \cdot \mathrm{Vol}(n, \frac{1}{4r^2}) .$$

□

We shall also need the following lower bound on the norm of $f$ when it has at least one not too small coefficient.

**Lemma 2.7.** *Let $f$ be an $n$-variate homogeneous of degree $r$. Assume that one of the coefficients in $f$ is at least $\alpha$ in absolute value. Then $\|f\|_2 \geq \alpha \cdot 2^{n/2} \cdot e^{-r}$.*

The proof will use Legendre polynomials as a basis for the space of polynomials. Recall that Legendre polynomials $\{L_k(x)\}$ are univariate polynomials such that $\deg(L_k) = k$ and

$$\int_{-1}^{1} L_k(x) \cdot L_m(x) d\mu(\mathbf{x}) = \delta_{k=m} \cdot \frac{2}{2k+1}.$$

For an exponent vector $\bar{e} = (e_1, \ldots, e_n)$ we will denote $L_{\bar{e}}(\mathbf{x}) := \prod_{i=1}^n L_{e_i}(x_i)$. It is again easy to see that when we run over all $\bar{e}$ we get an orthogonal family of polynomials. For a polynomial we denote with $f = \sum_{\bar{e}} c_{\bar{e}} \cdot \prod_{i=1}^n x_i^{e_i}$ its usual monomial expansion and with $f = \sum_{\bar{e}} \ell_{\bar{e}} \cdot L_{\bar{e}}$ its expansion with respect to the Legendre basis. We shall also need the fact that the coefficient of $x^k$ in $L_k(x)$ is $\frac{1}{2^k} \cdot \binom{2k}{k}$. For more on Legendre polynomials see e.g. [San91].

**Claim 2.8.** *Let $f(\mathbf{x})$ be a homogeneous polynomial of degree $r$. Then for any exponent vector $\bar{e^0} = (e_1^0, \ldots, e_n^0)$ such that $\sum_i e_i^0 = r$ we have that*

$$\ell_{\bar{e^0}} = c_{\bar{e^0}} \cdot \prod_{i=1}^n 2^{e_i^0} \cdot \frac{1}{\binom{2e_i^0}{e_i^0}}.$$

*In particular $\ell_{\bar{e^0}} \geq c_{\bar{e^0}}$.*

Proof. From the properties above it is not hard to see that

$$\ell_{\bar{e^0}} = \prod_{i=1}^n \frac{2e_i^0+1}{2} \int_{[-1,1)^n} f \cdot L_{\bar{e^0}} d\mu(\mathbf{x})$$
$$= \prod_{i=1}^n \frac{2e_i^0+1}{2} \sum_{\bar{e}} \int_{[-1,1)^n} c_{\bar{e}} \cdot \prod_{i=1}^n x_i^{e_i} \cdot L_{\bar{e^0}} d\mu(\mathbf{x})$$

Since $f$ is homogeneous, any exponent vector $\bar{e} \neq \bar{e^0}$ appearing in the equation has a coordinate $i$ with $e_i < e_i^0$. As $L_{e_i^0}(x_i)$ is perpendicular to all lower degree polynomials we get that

$$= \prod_{i=1}^n \frac{2e_i^0+1}{2} \int_{[-1,1)^n} c_{\bar{e^0}} \cdot \prod_{i=1}^n x_i^{e_i^0} \cdot L_{\bar{e^0}} d\mu(\mathbf{x}).$$

By the same reasoning can add lower degree terms to $\prod_{i=1}^n x_i^{e_i^0}$ to get the polynomial $b \cdot L_{\bar{e^0}}$ where $b$ is the inverse of the product of the leading coefficients of the $L_{e_i^0}$. That is, $b = \prod_{i=1}^n 2^{e_i^0} \cdot \frac{1}{\binom{2e_i^0}{e_i^0}}$.

Hence

$$= \prod_{i=1}^n \frac{2e_i^0+1}{2} \cdot c_{\bar{e^0}} \cdot \prod_{i=1}^n 2^{e_i^0} \cdot \frac{1}{\binom{2e_i^0}{e_i^0}} \cdot \int_{[-1,1)^n} L_{\bar{e^0}}^2 d\mu(\mathbf{x})$$
$$= c_{\bar{e^0}} \cdot \prod_{i=1}^n 2^{e_i^0} \cdot \frac{1}{\binom{2e_i^0}{e_i^0}}.$$

□

We now prove Lemma 2.7.

Proof of Lemma 2.7. Let $f = \sum_{\bar{e}} \ell_{\bar{e}} \cdot L_{\bar{e}}$ be the expansion of $f$ in the Legendre basis. From orthogonality we get that

$$\mathcal{E}_\mu[f^2] = \sum_{\bar{e}} \mathcal{E}_\mu[\ell_{\bar{e}}^2 \cdot L_{\bar{e}}^2] = \sum_{\bar{e}} \ell_{\bar{e}}^2 \cdot \prod_{i=1}^n \frac{2}{2e_i+1}$$
$$\geq \alpha^2 \cdot \frac{2^n}{(2r/n+1)^n} \geq \alpha^2 \cdot 2^n \cdot e^{-2r}.$$

□

Finally, we will need the following simple result connecting the usual Euclidean norm of the vector of coefficients of a polynomial and its $\|\|_2$ norm.

**Lemma 2.9.** *Let $f(\mathbf{x})$ be an $n$-variate polynomial with $S$ monomials. Let $\mathbf{f} \in \mathbb{R}^S$ be its vector of coefficients. Then,*

$$\|f\|_2 \leq \|f\|_\infty \leq \|\mathbf{f}\| \cdot \sqrt{S}.$$

Proof. Let $f = \sum_M c_M \cdot M$ be the representation of $f$ as sum of monomials. We have that for all $\mathbf{v} \in [-1,1]^n$

$$|f(\mathbf{v})| = |\sum_M c_m M(\mathbf{v})| \leq \sum_M |c_M|$$
$$\leq \left(\sum_M |c_M|^2\right)^{1/2} \cdot \sqrt{S} = \|\mathbf{f}\| \cdot \sqrt{S} .$$

□

## 3 ANTI-CONCENTRATION RESULTS FOR POLYNOMIALS

We will rely on the following theorem of Carbery-Wright (see Theorem 8 in [CW01]).

**Theorem 3.1** (Carbery-Wright). *There exists an absolute constant $C$ such that if $f : \mathbb{R}^n \to \mathbb{R}$ is a polynomial of degree at most $r$, $0 < q < \infty$, and $\mu$ is a log-concave probability measure on $\mathbb{R}^n$, then, for $\alpha > 0$, it holds that*

$$\left(\int |f(x)|^{q/r} d\mu(\mathbf{x})\right)^{1/q} \cdot \mu\{\mathbf{v} \in \mathbb{R}^n \mid |f(\mathbf{v})| \leq \alpha\} \leq C \cdot q \cdot \alpha^{1/r}.$$

We give a version specialized to our purposes.

**Theorem 3.2** (Carbery-Wright). *There exists an absolute constant $C_{CW}$ such that if $f : \mathbb{R}^n \to \mathbb{R}$ is a polynomial of degree at most $r$, and $\|f\|_2 = 1$ then, for $\alpha > 0$, it holds that*

$$\Pr_{\mathbf{v} \in_U [-1,1)^n} [|f(\mathbf{v})| \leq \alpha] \leq C_{CW} \cdot r \cdot \alpha^{1/r}.$$

Proof. Apply Theorem 3.1 for $\mu$ the uniform measure on $[-1,1)^n$ and $q = 2\deg(f)$. Observe that

$$\int_{[-1,1)^n} |f(x)|^{q/r} d\mu(\mathbf{x}) = \int_{[-1,1)^n} |f|^2 d\mu(\mathbf{x}) = \|f\|_2^2 = 1.$$

□

We need a discrete version of this theorem which we state below. Let $\delta > 0$ be such that $1/\delta$ is an integer. Recall that $G_\delta = \{-1, -1+\delta, -1+2\delta, \ldots, 1-2\delta, 1-\delta\}^n$.

**Theorem 3.3** (Discrete Carbery-Wright). *Let $C_{CW}$ be the constant guaranteed in Theorem 3.2. Let $\delta > 0$ be such that $1/\delta$ is an integer. If $f : \mathbb{R}^n \to \mathbb{R}$ is a homogeneous polynomial of degree at most $r$ with $\|f\|_2 = 1$ then, for $\alpha > 0$, it holds that*

$$\Pr_{\mathbf{v} \in_U G_\delta} \left[|f(\mathbf{v})| \leq \alpha - \delta \cdot (8nr^2)^{n+1}\right] \leq C_{CW} \cdot r \cdot \alpha^{1/r}.$$

For the proof of the theorem it will be helpful to think of the uniform distribution on $G_\delta$ as generated in the following way: we first sample a point $\mathbf{v} \in [-1,1)^n$ uniformly at random and then round each coordinate $v_i$ to $m_i\delta$ for some integer $m_i$ such that $m_i\delta \leq v_i < (m_i+1)\delta$.

To prove the theorem we need the following simple result regarding polynomials.

**Lemma 3.4.** *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a homogeneous polynomial of degree at most $r$. Let $\delta > 0$ be such that $1/\delta$ is an integer. Let $\mathbf{v} \in [-1,1)^n$ and $\mathbf{u}$ be obtained from $\mathbf{v}$ by the rounding process described above (i.e. rounding each coordinate $v_i$ to the largest integer multiple of $\delta$ that is smaller than or equal to $v_i$). Then $|f(\mathbf{v}) - f(\mathbf{u})| \leq \delta \cdot (8nr^2)^{n+1} \cdot \|f\|_2$.*

Proof. By the mean value theorem there exists a point $\mathbf{w}$ on the line segment connecting $\mathbf{u}$ and $\mathbf{v}$ such that $|f(\mathbf{v}) - f(\mathbf{u})| = \|\mathbf{u}-\mathbf{v}\| \cdot |f'(\mathbf{w})|$, where $f'(\mathbf{w})$ is the derivative of $f$ in direction $\mathbf{u}-\mathbf{v}$ evaluated at $\mathbf{w}$. From Theorem 2.5 it follows that $|f'(\mathbf{w})| \leq 2 \cdot \|f\|_\infty \cdot r^2$. Corollary 2.6 implies that

$$\begin{aligned}|f(\mathbf{v}) - f(\mathbf{u})| = \|\mathbf{u}-\mathbf{v}\| \cdot |f'(\mathbf{w})| &\leq 2 \cdot \|\mathbf{u}-\mathbf{v}\| \cdot \|f\|_\infty \cdot r^2 \\ &\leq 2 \cdot \|\mathbf{u}-\mathbf{v}\| \cdot r^2 \cdot \|f\|_2 \cdot 2^{2n+2} \cdot \frac{1}{\mathrm{Vol}(n, \frac{1}{2r^2})}.\end{aligned}$$

As $\|\mathbf{u}-\mathbf{v}\| \leq \delta \cdot \sqrt{n}$ and $\mathrm{Vol}(n, \frac{1}{2r^2}) \geq \left(\frac{1}{2nr^2}\right)^n$ we get that

$$\begin{aligned}|f(\mathbf{v}) - f(\mathbf{u})| &\leq \delta \cdot \sqrt{n} \cdot r^2 \cdot \|f\|_2 \cdot 2^{2n+3} \cdot (2nr^2)^n \\ &\leq \delta \cdot (8nr^2)^{n+1} \cdot \|f\|_2.\end{aligned}$$

□

**Corollary 3.5.** *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a polynomial of degree at most $r$ with $\|f\|_2 = 1$. Let $\delta > 0$ be such that $1/\delta$ is an integer. Assume that for some $\mathbf{v} \in [-1,1]^n$, $|f(\mathbf{v})| > \alpha$ and that $\mathbf{u}$ is obtained from $\mathbf{v}$ by the rounding process described above. Then $|f(\mathbf{u})| > \alpha - \delta \cdot (8nr^2)^{n+1}$.*

We now give the proof of Theorem 3.3.

Proof of Theorem 3.3. We use the sampling procedure given above to sample a point $\mathbf{u} \in G_\delta$. That is, we first pick $\mathbf{v} \in [-1,1)^n$ at random and then round it to $\mathbf{u}$. By Theorem 3.2 with probability at least $1 - C_{CW} \cdot r \cdot \alpha^{1/r}$, $\mathbf{v}$ is such that $|f(\mathbf{v})| > \alpha$. By Corollary 3.5, for any such $\mathbf{v}$ we have that $|f(\mathbf{u})| > \alpha - \delta \cdot (8nr^2)^{n+1}$. Thus, the probability that we sample $\mathbf{u}$ with $|f(\mathbf{u})| \leq \alpha - \delta \cdot (8nr^2)^{n+1}$ is at most $C_{CW} \cdot r \cdot \alpha^{1/r}$. □

We will be working over the complex numbers and so we need to slightly adjust the results above. Let $f : \mathbb{C}^n \to \mathbb{C}$ be a homogeneous polynomial of degree $r$. Consider the real and imaginary parts of $f$, $\Re(f)$ and $\Im(f)$, respectively. We can view both as polynomials $\Re(f), \Im(f) : \mathbb{R}^{2n} \to \mathbb{R}$. That is, for every $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$, $f(\mathbf{a} + \imath\mathbf{b}) = \Re(f)(\mathbf{a},\mathbf{b}) + \imath \cdot \Im(f)(\mathbf{a},\mathbf{b})$. It is clear that both $\Re(f)$ and $\Im(f)$ are homogeneous polynomials of degree $r$ as well. We define $\|f\|_2 \triangleq \|\Re(f)\|_2 + \|\Im(f)\|_2$. As we work over the complex numbers we will refer to the set $G_\delta^{\mathbb{C}} = \{\mathbf{a} + \imath \cdot \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in G_\delta\}$.

**Theorem 3.6** (Discrete Carbery-Wright over $\mathbb{C}$). *Let $C_{CW}$ be the constant guaranteed in Theorem 3.2. If $f : \mathbb{C}^n \to \mathbb{C}$ is a homogeneous polynomial of degree at most $r$ with $\|f\|_2 = 1$ then, for $\alpha > 0$, it holds that*

$$\Pr_{\mathbf{v} \in_U G_\delta^{\mathbb{C}}} \left[|(f)(\mathbf{v})| \leq \alpha - \frac{1}{2}\delta \cdot (16nr^2)^{2n+1}\right] \leq C_{CW} \cdot r \cdot (2\alpha)^{1/r}.$$

Proof. As $\|f\|_2 = 1$ either $\|\Re(f)\|_2 \geq 1/2$ or $\|\Im(f)\|_2 \geq 1/2$. Assume without loss of generality the former happens. Note also that if $|\Re(f)(\mathbf{a},\mathbf{b})| > \gamma$ then $|f(\mathbf{a} + \imath \cdot \mathbf{b})| > \gamma$. Theorem 3.3 implies that the probability that we sample $\mathbf{a}, \mathbf{b} \in G_\delta$ with $|\Re(f)(\mathbf{a},\mathbf{b})| \leq 2\alpha - \delta \cdot (16nr^2)^{2n+1} \cdot \|\Re(f)\|_2$ is at most $C_{CW} \cdot r \cdot (2\alpha)^{1/r}$. Thus, with probability at least $1 - C_{CW} \cdot r \cdot (2\alpha)^{1/r}$ we get that $(\mathbf{a} + \imath\mathbf{b})$ is such that

$$\begin{aligned}|f(\mathbf{a} + \imath \cdot \mathbf{b})| &> 2\alpha - \delta \cdot (16nr^2)^{2n+1} \cdot \|\Re(f)\|_2 \\ &\geq \frac{1}{2}(2\alpha - \delta \cdot (16nr^2)^{2n+1}).\end{aligned}$$

□

## 4 THE ALGEBRAIC VARIETY OF SMALL ALGEBRAIC CIRCUITS

We start by providing some basic definitions from algebraic geometry. For more on algebraic geometry see [CLO06]. We follow essentially the same treatment given in [HS80a, HS80b].

**Definition 4.1** (Basic AG definitions). *A subset $V \subseteq \mathbb{C}^n$ is called (Zariski-)closed[7] if there exists a set of polynomials $\mathcal{F} \subseteq \mathbb{C}[\mathbf{x}]$ such that $V = \{\mathbf{v} \in \mathbb{C}^n \mid \forall f \in \mathcal{F},\ f(\mathbf{v}) = 0\}$. The closed sets define the Zariski topology of $\mathbb{C}^n$. The closure of a set $V \subseteq \mathbb{C}^n$ is the intersection of all closed sets containing $V$. A closed set $V$ is called irreducible if for any two closed sets $V_1, V_2$ such that $V_1 \cup V_2 = V$ it holds that either $V_1 = V$ or $V_2 = V$.* ◊

Closed sets are also called varieties. Irreducible closed sets are irreducible varieties.

[7] Over $\mathbb{C}$ if a set is closed in the Zariski topology then it is also closed in the usual Euclidean topology.

**Definition 4.2** (Dimension). *The dimension of an irreducible variety $V$, denoted* $\dim(V)$ *is the maximal integer $m$ such that there exist $m$ irreducible varieties $\{V_i\}$ satisfying $\emptyset \subsetneq V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_m \subsetneq V$. The dimension of a reducible variety is the maximal dimension of its irreducible components.* ◊

We now give some basic facts.

**Fact 4.3.** (1) *Each variety $V$ can be represented uniquely as a minimal finite union of irreducible varieties. Each irreducible set in this representation is called a component of $V$.*
(2) *The dimension of every variety $\emptyset \neq V$ is finite.*
(3) *If $U, V$ are varieties, where $U$ is irreducible and $U \nsubseteq V$ then* $\dim(U \cap V) < \dim(U)$.

It is a basic fact that any irreducible variety over $\mathbb{C}$ is connected (as a complex manifold).

**Theorem 4.4** (Irreducible varieties are connected). *Every irreducible variety $V \subseteq \mathbb{C}^N$ is connected as a topological space (in the usual Euclidean topology).*

Proof. The claim follows immediately from Theorem 1 in Chapter VII section 2.2 of [Sha88], noting that in our variety every point is closed (thus, $X(\mathbb{C})$ in the statement of Theorem 1 there is our irreducible variety). □

Another important definition is that of a *degree* of a variety.

**Definition 4.5** (Degree). *The degree of an irreducible variety $V \subseteq \mathbb{C}^n$, denoted* $\deg(V)$, *is the maximal cardinality of a finite intersection of $V$ with an affine linear space. That is,*

$$\deg(V) = \max\left\{|V \cap A| \mid A \subset \mathbb{C}^n \text{ is an affine linear space, and } |V \cap A| < \infty\right\} .$$

*When $V$ is not irreducible, let $V = \cup_i V_i$, where $V_i$ are the irreducible components of $V$. We define* $\deg(V)$ *as*

$$\deg(V) = \sum_i \deg(V_i) .$$

◊

We will rely on the following estimates of Heintz and Sieveking.

**Theorem 4.6** (Variety of easy polynomials [HS80b]). *For every natural numbers $n, s, r$ there exists a set $W(n,s,r) \subseteq \mathbb{C}^{N^{hom}_{n,r}}$ such that $W(n,s,r)$ contains the coefficient vectors of all $n$-variate homogeneous polynomials, $f \in \mathbb{C}[\mathbf{x}]$, of degree $r$, that can be computed by homogeneous algebraic circuits of size at most $s$. Furthermore,*

$$\dim(W(n,s,r)) \leq (s+1+n)^2$$

*and*

$$\deg(W(n,s,r)) \leq (2sr)^{(s+1+n)^2} .$$

**Remark 4.7.** *We note that the result above holds not only for homogeneous polynomials and can be slightly improved if we restrict our attention to the homogeneous case as we do here, but this is not crucial for our purposes.* ◊

**Remark 4.8.** *We note that the main message behind Theorem 4.6 is that the dimension of the ambient space, $N^{hom}_{n,r}$, does not appear in the upper bounds on* $\dim(W(n,s,r))$ *and* $\deg(W(n,s,r))$. ◊

To prove our main result it will be convenient to consider the universal circuit. As the universal circuit for $n$-variate homogeneous circuits of size $s$ and degree $r$ has size $O(sr^4)$ we obtain the following immediate corollary. Note that when speaking of the polynomials that can be computed by the universal circuit we think of the set of polynomials that is obtained by running over all assignments to the auxiliary variables. Indeed, for any such assignment the circuit that is obtained is homogeneous in its essential variables and of size $O(sr^4)$.

**Theorem 4.9** (Variety of projection of the universal circuit). *For all natural numbers $n, r, s$ there exists a set $V(n,s,r) \subseteq \mathbb{C}^{N^{hom}_{n,r}}$ such that $V(n,s,r)$ contains the coefficient vectors of all homogeneous polynomials of degree $r$ that can be computed by the universal circuit for $n$-variate homogeneous circuits of size $s$ and degree $r$. Furthermore, there exists a constant $c$ such that*

$$\dim(V(n,s,r)) \leq c \cdot (sr^4 + 1 + n)^2$$

*and*

$$\deg(V(n,s,r)) \leq (csr^5)^{c\cdot(sr^4+1+n)^2} .$$

To ease notations we shall use the following corollary.

**Corollary 4.10.** *Let $V(n,s,r)$ be as in Theorem 4.9. Then, there exists a constant $c_{4.10}$ such that*

$$\dim(V(n,s,r)) \leq (srn)^{c_{4.10}}$$

*and*

$$\deg(V(n,s,r)) \leq 2^{(srn)^{c_{4.10}}} .$$

Theorem 4.9 speaks about a variety containing coefficient vectors of easy polynomials. As varieties are closed, the same variety also contains all coefficient vectors of polynomials that are limits of easy polynomials.

**Definition 4.11** (Closure of easy polynomials). *A homogeneous polynomial $f \in \mathbb{C}[\mathbf{x}]$ is in the closure of size $s$ and degree $r$ algebraic circuits if there exists a sequence of $n$-variate, degree $r$, homogeneous polynomials $\{f_i(\mathbf{x})\}$, such that each $f_i$ can be computed by a homogeneous circuit of size $s$ and degree $r$, and $\lim_{i\to\infty} f_i = f$. In other words, there exists a sequence of homogeneous algebraic circuits of degree $r$ and size $s$ such that the coefficients vector of the polynomials they compute converge to the coefficient vector of $f$.* ◊

**Remark 4.12.** *At first sight it may seem, thanks to the definition of the universal circuit $\Psi(\mathbf{x},\mathbf{y})$, that if $f \in \overline{\mathsf{VP}}$ that $f$ also has a small circuit. Indeed, if $f_i \to f$ and $f_i = \Psi(\mathbf{x}, \mathbf{a}_i)$ then it seems that $f = \Psi(\mathbf{x}, \lim_{i\to\infty} \mathbf{a}_i)$. The problem with this argument however is that $\{\mathbf{a}_i\}$ may not converge. An example for this phenomenon may be seen in the the difference between the border rank of a tensor and its rank. It may be the case that a tensor has border rank $r$ yet it's rank may be larger. See e.g. Section 1 in this paper and Section 6 in [Blä13].* ◊

**Corollary 4.13.** *The variety $V(n,s,r)$ defined in Theorem 4.9 contains all coefficient vectors of homogeneous polynomials that are in the closure of size $s$ and degree $r$ algebraic circuits.*

Finally, we define a notion that will be useful in the upcoming proofs.

**Definition 4.14** (Axis-parallel random variety)**.** *We say that a variety $V$ is axis-parallel random if for any axis-parallel affine subspace $A$ (i.e. a subspace defined by setting some coordinates to constants) it holds that* $\dim(V \cap A) \leq \dim(V) - \operatorname{codim}(A)$. ♢

One way to think of this definition is that a variety is axis-parallel-random if by restricting a variable to a constant we move to a strictly smaller subvariety.

It is clear that if $V$ is axis-parallel random then for every axis-parallel affine subspace $A$, $V \cap A$ is also axis-parallel random. Next we show that by slightly perturbing a variety makes it an axis-parallel random one. That is, we will show that for a linear transformation $T$, the variety $T(V)$ is axis-parallel random.

**Theorem 4.15** (A random perturbation makes a variety axis-parallel random)**.** *Let $0 < \delta$ and let $T = I_N + A$, where $I_N$ is the $N \times N$ identity matrix and $A$ is a random matrix where each $a_{i,j}$ is chosen independently uniformly at random from $[0, \delta]$. Let $V \subseteq \mathbb{C}^N$ be a variety of dimension $d$. Then $T(V)$ with probability 1 $T(V)$ is axis-parallel random.*

To prove the theorem we will need the following theorem that characterizes the dimension of a variety in terms of the algebraic rank of the polynomials defining that variety. See e.g. Theorem 2 in Chapter 9, §5 of [CLO06].

**Theorem 4.16** (Characterization of dimension via algebraic dependence)**.** *Let $V \subseteq \mathbb{C}^N$ be a variety and let $I = I(V)$ be the ideal of all polynomials vanishing on $V$. Let the coordinate ring of $V$ be $\mathbb{C}[V] \triangleq \mathbb{C}[\mathbf{x}]/I$. Then the dimension of $V$ equals the maximal number of elements of $\mathbb{C}[V]$ that are algebraically independent.*

Proof of Theorem 4.15. To prove the theorem we first show that with high probability no variable (or actually no linear function of the form $x_i = c$) will be in the ideal $I(V)$. Then we prove that restricting any variable to a constant reduces the algebraic rank of $\mathbb{C}[V]$.

**Lemma 4.17.** *Let $L \subset I(T(V))$ be the linear space of all linear functions in $I(T(V))$. If $\dim(V) = d$ then for any $d$ variables $x_{i_1}, \ldots, x_{i_d}$ the probability that there exists a non zero linear combination $\sum_{j=1}^{d} \alpha_j \cdot x_{i_j} + \alpha_0 \in I(T(V))$ is 0.*[8]

Proof. First observe that $d \leq N - \dim(L)$, or $\dim(L) \leq N - d$. Further, observe that the effect of applying $T$ to $V$ on $L$ is essentially applying $T^{-1}$ to the linear functions in $L$. Thus, the event that we are considering checks whether a random subspace of dimension at most $N - d$ intersects a given $d$ dimensional affine space. This probability is 0 over the reals. This holds even for a $T$ chosen as in the theorem. For example, this can be seen by noting that the two subspaces intersect iff a certain determinant is zero: the rows of the determinant will compose of the basis for the two subspaces. It is easy to see that the determinant is a nonzero polynomial in the $A$ variables and thus it is nonzero with probability 1. □

Next we wish to show that setting any $k \leq \dim(V)$ variables to constant reduces the algebraic rank of $\mathbb{C}[V]$ by $k$ with probability 1. We prove this property for irreducible varieties and then conclude it to arbitrary varieties. A property that will be useful is that if $V$ is an irreducible variety then $I(V)$ is a prime ideal (see e.g., [CLO06]).

**Lemma 4.18.** *Let $f_1, \ldots, f_d$ be algebraically independent polynomials in $\mathbb{C}[T(V)]$. Let $x_{i_1}, \ldots, x_{i_k}$ be any $k \leq d$ different variables. Then for any $k$ field elements $\alpha_1, \ldots, \alpha_k$ restricting $x_i = \alpha_i$ reduces the algebraic rank of $\{f_i\}$ by $k$ with probability 1 (over the choice of $T$).*

Proof. We will prove the claim by induction on $k$. For $k = 1$ note that since the $f_i$ are maximally algebraically independent in $\mathbb{C}[T(V)]$ then for any other nonzero polynomial $g$ in $C[T(V)]$ there exists a nonzero polynomial $F_g(z_1, \ldots, z_{d+1})$ such that we have the identity $F_g(f_1, \ldots, f_d, g) \equiv 0$, where by that we mean that $F_g(f_1, \ldots, f_d, g)$ is the zero element in $\mathbb{C}[T(V)]$, that is, we have that $F_g(f_1, \ldots, f_d, g) \in I(T(V))$. Observe further that since $I(T(V))$ is a prime ideal (applying an invertible linear transformation does not affects the irreducibility of the variety) if $g \cdot h \in I(T(V))$ then $h \in I(T(V))$. Hence, we can assume without loss of generality that $z_{d+1}$ does not divide $F_g$.

From Lemma 4.17 we know that for any $\alpha$, $g = x_{i_1} - \alpha$ is not the zero polynomial in $\mathbb{C}[T(V)]$. Thus, there is such polynomial $F_g$. As $z_{d_1}$ does not divide $F_g$ we can express it as $F_g = z_{d+1} \cdot F_1(z_1, \ldots, z_{d+1}) + F_0(z_1, \ldots, z_d)$, where $F_0 \neq 0$. Thus the polynomial $g \cdot F_1(f_1, \ldots, f_d, g) + F_0(f_1, \ldots, f_d)$ is in $I(T(V))$. Now, adding the linear polynomial $g$ to $I(T(V))$ to get $I^{(1)} = (I(T(V)), g)$ (the ideal generated by $I(T(V))$ and $g$), it follows that $F_0(f_1, \ldots, f_d) \in I^{(1)}$. Thus, the $\{f_i\}$ become algebraic dependent when setting $g = 0$, i.e. when restricting $x_{i_1} = \alpha$.

To prove the case of general $k$ we just notice that the same argument will work thanks to Lemma 4.17, where at the $k$th step we consider any algebraically independent set $f'_1, \ldots, f'_{d-k+1}$ in $\mathbb{C}[I^{(k-1)}]$. □

The proof of Theorem 4.15 now follows since the probability of a bad event is 0 and each variety it the union of a finite number of irreducible components.

□

## 4.1 $\varepsilon$-nets for Algebraic Varieties

In this section we construct $\varepsilon$-nets for varieties. We shall use the Euclidean norm for this and to avoid confusion we shall denote the Euclidean norm of a vector $a$ with it with $\|a\|$. That is, there is no subscript 2 when using the Euclidean norm.

**Definition 4.19** ($\varepsilon$-net)**.** *Let $V \subseteq \mathbb{C}^N$. A set $E \subseteq V$ is an $\varepsilon$-net for $V$ if for every $\mathbf{v} \in V$ there exists $\mathbf{e} \in E$ such that $\|\mathbf{e} - \mathbf{v}\| \leq \varepsilon$.* ♢

Recall the notation $[-1, 1]^N_{\mathbb{C}} = [-1, 1]^N + \iota \cdot [-1, 1]^N = \{\mathbf{a} + \iota \cdot \mathbf{b} \mid \mathbf{a}, \mathbf{b} \in [-1, 1]^N\}$.

**Theorem 4.20** ($\varepsilon$-net for varieties)**.** *Let $N, d, D$ be integers such that $d < \sqrt{N}$, and $\varepsilon > 0$. Let $V \subseteq \mathbb{C}^N$ be a $d$-dimensional variety of degree $D$ which is axis-parallel random. Denote $\hat{V} = V \cap [-1, 1]^N_{\mathbb{C}}$. There exists an $\varepsilon$-net $E \subseteq \hat{V}$ of size smaller or equal to $D \cdot (75N^2/\varepsilon^2)^{d+1}$.*

Proof. The proof is by induction on the dimension of $V$. If $\dim(V) = 0$ then $|V| = D$ and the claim is trivial. Furthermore, it is

[8] That is, this can fail only for a set of matrices of measure zero

a $\delta$-net for any $\delta > 0$. Assume $d > 0$. For $\alpha \in \mathbb{C}$ and $i \in [N]$ let

$$H_i(\alpha) = \{\mathbf{v} \in \mathbb{C}^N \mid \mathbf{v}_i = \alpha\}.$$

That is, $H_i(\alpha)$ is the hyperplane obtained by fixing the $i$'th coordinate to $\alpha$. Let $V_i(\alpha) = V \cap H_i(\alpha)$ and $\hat{V}_i(\alpha) = V_i(\alpha) \cap [-1,1]^N_{\mathbb{C}}$. As $V$ is axis-parallel random, $V_i(\alpha)$ is a variety of dimension $d-1$ and degree at most $D$, which is also axis-parallel random. Let $\eta, \delta > 0$ be constants to be determined later, such that $1/\eta$ is an integer. By the induction hypothesis, there is a subset $E_i(\alpha) \subseteq \hat{V}_i(\alpha)$ which is a $\delta$-net for $V_i(\alpha) \cap [-1,1]^N_{\mathbb{C}}$ of size $D \cdot (75N^2/\delta)^{(d-1)+1}$. Let

$$E' = \bigcup_{i \in [N], \alpha, \beta \in \{-1, -1+\eta, \ldots, 1-\eta, 1\}} E_i(\alpha + \iota \cdot \beta).$$

It is clear that

$$|E'| \leq N \cdot (2/\eta + 1)^2 \cdot D \cdot (75N^2/\delta^2)^d.$$

The set $E'$ is almost our $\varepsilon$-net. All that is left to do is to cover points of $V$ that are not close to any intersection point of $V$ with any of the hyperplanes we considered.

Let

$$H = \bigcup_{i \in [N], \alpha, \beta \in \{-1, -1+\eta, \ldots, 1-\eta, 1\}} H_i(\alpha + \iota \cdot \beta).$$

Consider the set $[-1,1]^N_{\mathbb{C}} \setminus H$. It is a union of disjoint "cells" whose "walls" have been removed (the walls being the hyperplanes). Recall that by Theorem 4.4 we have that an irreducible variety is connected. Thus, when considering the irreducible components of $V$, we see that each component either intersects a "wall" of a cell or is completely contained in it (or completely disjoint from it). Thus, as $V$ is of degree $D$, it has at most $D$ irreducible components and in particular, at most $D$ of $V$'s irreducible components are contained in cells. From each connected component that is contained in such a cell pick any point. Let $B$ be the set of points thus chosen. It follows that, $|B| \leq D$. Finally, let $E = E' \cup B$. We claim that for

$$\eta = \frac{1}{\lceil \frac{2N}{\varepsilon} \rceil} \quad \text{and} \quad \delta = \left(1 - \frac{1}{\sqrt{2N}}\right) \cdot \varepsilon\,,$$

the set $E$ is an $\varepsilon$-net for $\hat{V}$. Indeed, let $\mathbf{v} \in \hat{V}$ be arbitrary. Consider the connected component to which $\mathbf{v}$ belongs. If this component is contained in one of the cells, then there is some $\mathbf{e} \in B \subseteq E$ in the same cell as $\mathbf{v}$. As each cell is contained in a cube whose diameter is $\sqrt{2N}\eta$, it holds that $\|\mathbf{v} - \mathbf{e}\| \leq \sqrt{2N}\eta \leq \varepsilon$. On the other hand, if the connected component containing $\mathbf{v}$ is not contained in any of the cells, then it must intersect the closure of the cell containing $\mathbf{v}$. Let $\mathbf{u}$ be this intersection point. By the construction of $E'$, there is some point $\mathbf{e}$ such that $\|\mathbf{e} - \mathbf{u}\| \leq \delta$. As $\|\mathbf{v} - \mathbf{u}\| \leq \sqrt{2N}\eta$ we get by the triangle inequality that $\|\mathbf{e} - \mathbf{v}\| \leq \sqrt{2N}\eta + \delta \leq \varepsilon$. To conclude the proof we note that

$$\begin{aligned}
|E| &\leq N \cdot (2/\eta + 1)^2 \cdot D \cdot (75N^2/\delta^2)^d + D \\
&\leq N \cdot (5N/\varepsilon)^2 \cdot D \cdot \left(75\left(1 + \frac{1}{\sqrt{N}}\right)N^2/\varepsilon^2\right)^d + D \\
&\leq (70N^2/\varepsilon^2) \cdot D \cdot \left(75N^2/\varepsilon^2\right)^d + D \\
&\leq D \cdot (75N^2/\varepsilon^2) \cdot \left(75N^2/\varepsilon^2\right)^d \\
&= D \cdot \left(75N^2/\varepsilon^2\right)^{d+1},
\end{aligned}$$

where we have used the fact that for $N \geq 2$ and $d < \sqrt{N}$ it holds that $(1 + 1/\sqrt{N})^d < 2.8$. □

We would like to apply the result of Theorem 4.20 for $V(n,s,r)$. A small technical issue is that $V(n,s,r)$ is not axis-parallel random. Nevertheless, Theorem 4.15 guarantees that for a random transformation $T$ the set $T(\mathcal{H})$ is an $(\eta/2)$-robust hitting set for $V(n,s,r)$.

Let $T$ be as guaranteed by Theorem 4.15 for $V = V(n,s,r)$. Note that if $V = V(\mathcal{F})$ and we define $V' = V(\mathcal{F} \circ T)$ then $V = T(V')$. Indeed, $v \in V'$ iff $(f \circ T)(\mathbf{v}) = 0$ for all $f \in \mathcal{F}$ which is equivalent to $T\mathbf{v} \in V$ or $\mathbf{v} \in T^{-1}V$.

**Lemma 4.21.** *Let $V' = T^{-1}(V) \subseteq \mathbb{C}^N$ be an axis-parallel random variety where $T = I + A$ such that each entry of $A$ lies in $[0, 1/N^{2d}]$.*[9] *Let $E' \subseteq V'$ be an $\varepsilon$-net for $V' \cap [-1,1]^N_{\mathbb{C}}$. Then $E := T(E') \subset V$ is an $(1 + 1/N) \cdot \varepsilon$-net for $V \cap [-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N_{\mathbb{C}}$.*

Proof. Note that by construction of $T$ we have that $T^{-1} = I + \sum_{k=1}^{\infty}(-A)^k$ and that each entry of $T^{-1} - I$ is bounded in absolute value by, say, $\frac{1}{N^d}$. In particular,

$$T^{-1}\left([-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N_{\mathbb{C}}\right) \subseteq [-1,1]^N_{\mathbb{C}}\,,$$

where, as before, we have $[-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N_{\mathbb{C}} = [-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N + \iota[-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N$.[10]

Let $\mathbf{v} \in V \cap [-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N_{\mathbb{C}}$. We have that

$$\begin{aligned}
T^{-1}(\mathbf{v}) \in T^{-1}(V) \cap T^{-1}&\left([-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N_{\mathbb{C}}\right) \\
&\subseteq T^{-1}(V) \cap [-1,1]^N_{\mathbb{C}} = V' \cap [-1,1]^N_{\mathbb{C}}\,.
\end{aligned}$$

Let $\mathbf{e} \in E'$ be such that $\|\mathbf{e}' - T^{-1}(\mathbf{v})\| \leq \varepsilon$. We thus have that $\|T(\mathbf{e}) - \mathbf{v}\| \leq \|T\| \cdot \|\mathbf{e} - T^{-1}\mathbf{v}\| \leq^{(*)} (1 + 1/N)\varepsilon$, where inequality $(*)$ follows easily from the construction of $T$ (and $\|T\|$ is the operator norm of $T$). □

As corollary we get the same parameters for varieties that are not necessarily axis-parallel random.

**Corollary 4.22** ($\varepsilon$-net for varieties). *Let $N, d, D$ be integers such that $d < \sqrt{N}$, and $\varepsilon > 0$. Let $V \subseteq \mathbb{C}^N$ be a $d$-dimensional variety of degree $D$. Denote $\hat{V} = V \cap [-(1 - \frac{1}{N}), 1 - \frac{1}{N}]^N_{\mathbb{C}}$. There exists an $\varepsilon$-net $E \subseteq \hat{V}$ of size smaller or equal to $D \cdot (76N^2/\varepsilon^2)^{d+1}$.*

[9] Observe that the conclusion of Theorem 4.15 holds for any choice of $0 < \delta$, in particular for $\delta = N^{-2d}$.

[10] Notice that as $T$ is real it operates on the real part and the imaginary part of each vector separately.

Proof. This follows from Theorem 4.20 and Lemma 4.21 by plugging $\varepsilon' = \varepsilon/(1+\frac{1}{N})$ to the bounds there. □

## 5 ROBUST HITTING SETS

In this section we define the notion of a robust hitting set and prove its existence.

**Definition 5.1** ($\varepsilon$-Robust hitting set). *A subset $\mathcal{H} \subseteq \mathbb{C}^n$ is an $\varepsilon$-robust hitting set for a set of polynomials $V \subseteq \mathbb{F}[\mathbf{x}]$ if for every $f \in V$ there is some $\mathbf{v} \in \mathcal{H}$ such that $|f(\mathbf{v})| \geq \varepsilon \cdot \|f\|_2$.*

*Let $n, r, s$ be integers. We say that $\mathcal{H}$ is an $\varepsilon$-robust hitting set for size $s$ and degree $r$ if it is an $\varepsilon$-robust hitting set for the set of $n$-variate polynomials that can be computed by size $s$ and degree $r$ homogeneous algebraic circuits.* ◊

The next claim shows that a robust hitting set for size $s$ algebraic circuits is also a robust hitting set for the closure of such circuits, that is for $V(n,s,r)$.

**Claim 5.2.** *If a finite $\mathcal{H} \subseteq \mathbb{R}^n$ is an $\varepsilon(n)$-robust hitting set for size $s$ and degree $r$ then for any $f \in V(n,s,r)$ there is $\mathbf{v} \in \mathcal{H}$ such that $|f(\mathbf{v})| \geq \varepsilon(n) \cdot \|f\|_2$.*

Proof. Let $f \in V(n,s,r)$. For $i \in \mathbb{N}$ let $f_i \in V(n,s,r)$ be such that $\lim_{i\to\infty} f_i = f$ and each $f_i$ is computed by a homogeneous circuit of size $s$ and degree $r$. Clearly, it also holds that $\lim_{i\to\infty} \|f_i\|_2 = \|f\|_2$. As $\mathcal{H}$ is finite there is $\mathbf{v} \in \mathcal{H}$ at which infinitely many $f_i$ evaluate (in absolute value) to at least $\varepsilon(n) \cdot \|f_i\|_2$. Thus, there is a subsequence $f_{i_j}$ satisfying $\lim_{j\to\infty} f_{i_j} = f$ and $|f_{i_j}(\mathbf{v})| \geq \varepsilon(n) \cdot \|f_{i_j}\|_2$. By continuity it holds that $|f(\mathbf{v})| \geq \varepsilon(n) \cdot \|f\|_2$ as well. □

In the next lemma we think of each point $\mathbf{f} \in \mathbb{C}^{N^{\hom}_{n,r}}$ as being the coefficient vector of some homogeneous $n$ variate polynomial $f$ of degree $r$. That is $f(\mathbf{x}) = \sum_{\deg(M)\leq r} f_M \cdot M(\mathbf{x})$, and we index coordinates of $\mathbb{C}^{N^{\hom}_{n,r}}$ with degree $r$ monomials. The lemma shows that in order to construct a robust hitting set for a set of polynomials it is enough to construct a good enough robust hitting set for an $\varepsilon$-net in the variety.

**Lemma 5.3.** *Let $V \subseteq [-1,1]^{N^{hom}_{n,r}}_{\mathbb{C}}$ be such that if $\mathbf{f} \in V$ and $\alpha\mathbf{f} \in [-1,1]^{N^{hom}_{n,r}}_{\mathbb{C}}$ then $\alpha\mathbf{f} \in V$.[11] Let $E \subseteq V$ an $\varepsilon$-net for $V$. Assume that $\mathcal{H} \subseteq [-1,1]^n_{\mathbb{C}}$ is such that for every $\mathbf{g} \in E$ there exists $\mathbf{v} \in \mathcal{H}$ such that $g(\mathbf{v}) \geq \eta \cdot \|g\|_2$, for some $\eta < 1$. Assume further that $\eta, \varepsilon, N^{hom}_{n,r}$ and $r$ satisfy that*

$$10 \cdot \varepsilon \cdot \sqrt{N^{hom}_{n,r}} < \frac{1}{8}\eta \cdot 2^{n/2} \cdot e^{-r} < \frac{1}{4}.$$

*Then, for every $\mathbf{f} \in V$ there exists $\mathbf{v} \in \mathcal{H}$ such that $|f(\mathbf{v})| \geq \frac{1}{4}\eta\|f\|_2$.*

Proof. Let $\mathbf{f} \in V$. Assume w.l.o.g. that the maximal coefficient of $f$ is $1/2$. This can be easily obtained by multiplying $\mathbf{f}$ by a field element. Let $\mathbf{g} \in E$ be such that $\|\mathbf{f}-\mathbf{g}\| \leq \varepsilon$. Observe that $\|f\|_2 \leq \|g\|_2 + \|f-g\|_2$ and that by Lemma 2.9

$$\|\Im(f) - \Im(g)\|_\infty \,,\ \|\Re(f) - \Re(g)\|_\infty \leq \|\mathbf{f}-\mathbf{g}\| \cdot \sqrt{N^{\hom}_{n,r}} = \varepsilon \cdot \sqrt{N^{\hom}_{n,r}}\,.$$

Thus

$$\|f-g\|_\infty \leq \sqrt{2} \cdot \varepsilon \cdot \sqrt{N^{\hom}_{n,r}}.$$

Since $\Re(f)$ has a large coefficient and $\|\mathbf{f}-\mathbf{g}\| \leq \varepsilon < 1/10$ it follows that some coefficient in $\mathbb{R}(g)$ is at least $1/4$. Let $\mathbf{v} \in \mathcal{H}$ be such that $|g(\mathbf{v})| \geq \eta \cdot \|g\|_2$. Then,

$$\begin{aligned}
|f(\mathbf{v})| &\geq |g(\mathbf{v})| - |(f-g)(\mathbf{v})| \\
&\geq \eta \cdot \|g\|_2 - \sqrt{2} \cdot \varepsilon \cdot \sqrt{N^{\hom}_{n,r}} \\
&\geq \eta \cdot \|g\|_2 - \frac{1}{8}\eta \cdot 2^{n/2} \cdot e^{-r} && (5.4)\\
&\geq \frac{1}{2}\eta \cdot \|g\|_2 && (5.5)\\
&\geq \frac{1}{4}\eta \cdot \|f\|_2 && (5.6)
\end{aligned}$$

where Equation 5.4 holds because of the assumption in the lemma, Equation 5.5 follows from Lemma 2.7 using the fact that some coefficient in $g$ is at least $1/4$. Indeed, Lemma 2.7 implies that $\|g\|_2 \geq \frac{1}{4}2^{n/2} \cdot e^{-r}$. Finally, Equation 5.6 holds since

$$\begin{aligned}
\|f\|_2 &\leq \|g\|_2 + \|f-g\|_2 \\
&= \|g\|_2 + \|\Re(f-g)\|_2 + \|\Im(f-g)\|_2 \\
&\leq \|g\|_2 + \|\Re(f-g)\|_\infty + \|\Im(f-g)\|_\infty \\
&\leq \|g\|_2 + 2\varepsilon \cdot \sqrt{N^{\hom}_{n,r}} \leq 2\|g\|_2.
\end{aligned}$$

□

### 5.1 Robust Hitting Sets for Polynomial Varieties

In this section we prove that for any variety of $n$-variate degree $r$ polynomials of polynomial dimension and exponential degree there exists an $\exp(-\mathrm{poly}(nr))$ robust hitting set of polynomials size.

As before we think of every point $\mathbf{f} \in \mathbb{C}^{N^{\hom}_{n,r}}$ as vector of coefficients of a homogeneous $n$-variate, degree $r$ polynomial $f(\mathbf{x})$.

**Theorem 5.7** (Robust hitting sets for varieties). *Let $V \subset \mathbb{C}^{N^{hom}_{n,r}}$ be a variety of dimension $d$ and degree $D$ satisfying the assumption of Lemma 5.3. Let $\eta = 2^{-n} \cdot \frac{1}{2\cdot(C_{CW}\cdot n\cdot r)^r}$ and $\delta = \frac{\eta}{(16nr^2)^{2n+1}}$. There exists an $(\eta/4)$-robust hitting set $\mathcal{H}$ for $V$ satisfying $\mathcal{H} \subset G^{\mathbb{C}}_\delta$ of size*

$$|\mathcal{H}| = \max\{2\log D, 12r(n+r)\cdot d\}.$$

Proof. Let $k$ be given by $k = \max\{2\log D, 18(n+r)\cdot d\}$. Sample $k$ points $\mathbf{v}_1, \ldots, \mathbf{v}_k \in G^{\mathbb{C}}_\delta$ uniformly and independently at random. Set $\mathcal{H} = \{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$.

Let $\varepsilon = \left(\frac{1}{N^{\hom}_{n,r}}\right)^r$ and $E \subset V(n,s,r) \cap [-(1-\frac{1}{N}), 1-\frac{1}{N}]^N_{\mathbb{C}}$ be the $\varepsilon$-net guaranteed by Corollary 4.22. From Theorem 3.6 (by taking $\alpha = \eta \cdot \|g\|_2$) it follows by the union bound that the probability that there exists $\mathbf{g} \in E$ such that for every $i$,

$$|g(\mathbf{v}_i)| \leq \left(\eta - \frac{1}{2}\cdot\delta\cdot(16nr^2)^{2n+1}\right)\cdot\|g\|_2 = \eta/2\cdot\|g\|_2,$$

[11] Notice that this property holds for $V(n,s,r) \cap [-1,1]^{N^{\hom}_{n,r}}_{\mathbb{C}}$.

is at most

$$\begin{aligned}
&\left(C_{CW}\cdot r\cdot\ (2\eta)^{1/r}\right)^k\cdot|E|\\
&\quad\le\left(C_{CW}\cdot r\cdot(2\eta)^{1/r}\right)^k\cdot D\cdot(75N_{n,r}^{\hom 2}/\varepsilon^2)^{d+1}\\
&\quad<2^{-nk/r}\cdot\left(\frac{1}{n}\right)^k\cdot D\cdot N_{n,r}^{\hom 12rd}\\
&\quad<2^{-nk/r}\cdot\left(\frac{1}{n}\right)^k\cdot D\cdot 2^{12rd(n+r)}\\
&\quad\le 1,
\end{aligned}$$

where the last inequality follows from the definition of $k$. Notice that our choice of $\eta$ and $\varepsilon$ satisfy the condition in Lemma 5.3, that is,

$$10\cdot\varepsilon\cdot\sqrt{N_{n,r}^{\hom}}<\frac{1}{8}\eta\cdot 2^{n/2}\cdot e^{-r}<\frac{1}{4}.$$

The claim of the theorem now follows from Lemma 5.3. □

**Corollary 5.8** (Robust hitting sets for $V(n,s,r)$). *There exists a constant $c$ such that for every integers $n,s,r$, for $\eta=2^{-n}\cdot\frac{1}{2\cdot(C_{CW}\cdot nr)^r}$ and $\delta=\frac{\eta}{(16nr^2)^{2n+1}}$, there is an $\eta/4$-robust hitting set $\mathcal{H}\subset G_\delta^{\mathbb{C}}$, for $V(n,s,r)$, of size*

$$|\mathcal{H}|\le(nsr)^c.$$

Proof. The proof follows immediately from applying Theorem 5.7 to $V(n,s,r)$, and then using the estimates given in Corollary 4.10. □

We note that the proof above gives a robust hitting set $\mathcal{H}$ for $V(n,s,r)$ whose points come from $\mathbb{C}^n$. We obtain a hitting set for $V(n,s,r)$ over $\mathbb{R}$ by using a simple trick.

**Theorem 5.9** (Robust-hitting sets for $V(n,s,r)$ over $\mathbb{R}$). *Let $\mathcal{H}$ be an $\varepsilon$-robust hitting set for $V(n,s,r)$. For each $\mathbf{v}=\mathbf{a}+\iota\cdot\mathbf{b}\in\mathcal{H}$ and an integer $k$ let $\mathbf{v}_k=\mathbf{a}+k\cdot\mathbf{b}$. Set $\mathcal{H}_{\mathbb{R}}\triangleq\{\mathbf{v}_k\mid\mathbf{v}\in\mathcal{H}\text{ and }k\in\{0,\ldots,r\}\}$. It holds that $\mathcal{H}_{\mathbb{R}}$ is an $\frac{\varepsilon}{(r+2)!}$-robust hitting set for $V(n,s,r)$.*

Proof. The fact that $\mathcal{H}_{\mathbb{R}}$ hits $V(n,s,r)$ is simple. Let $z$ be a new variable. For each $\mathbf{v}=\mathbf{a}+\iota\cdot\mathbf{b}\in\mathcal{H}$ and $f\in V(n,s,r)$ consider a new univariate polynomial $F_{\mathbf{v}}(z)=f(\mathbf{a}+z\cdot\mathbf{b})$. Clearly, there is some $\mathbf{v}\in\mathcal{H}$ for which $F_{\mathbf{v}}(z)\not\equiv 0$ as setting $z=\iota$ gives $F_{\mathbf{v}}(\iota)=f(\mathbf{v})$.

Let $c_k$, for $k\in\{0,\ldots,r\}$, be constants satisfying that for every degree $r$ polynomial $g$ it holds that $g(\iota)=\sum_{k=0}^r c_k\cdot g(k)$. Such constants exist by simple interpolation. Furthermore, we have that $|c_k|\le(r+1)!$. Indeed, note that $c_k$ is the $k$'th entry in the result of the following matrix-vector product: The vector has length $(r+1)$ and its $k$'th entry is $\iota^k$. That is, denoting the vector with $\mathbf{w}$ we have that $w_k=\iota^k$. The matrix is the inverse matrix of the Vandermonde matrix $A$ whose $(k,\ell)$-entry, for $k,\ell\in\{0,\ldots,r\}$, is $k^\ell$, where $0^0=1$. To get the bound on $|c_k|$ we observe that the $\ell$'th column of the inverse matrix is given by the coefficient vector of the polynomial $\frac{\prod_{k\neq\ell}(x-k)}{\prod_{k\neq\ell}(\ell-k)}$. The (very) crude bound we gave on $|c_k|$ follows easily.

To see that $\mathcal{H}_{\mathbb{R}}$ is a robust hitting set we note that for $\mathbf{v}\in\mathcal{H}$ for which $|f(\mathbf{v})|\ge\varepsilon\cdot\|f\|_2$ we have that

$$\begin{aligned}
\varepsilon\cdot\|f\|_2\le|f(\mathbf{v})|=|F_{\mathbf{v}}(\iota)| &= \left|\sum_{k=0}^r c_kF_{\mathbf{v}}(k)\right|\\
&= \left|\sum_{k=0}^r c_kf(\mathbf{v}_k)\right|\\
&\le (r+1)\cdot\max_k|c_k|\cdot\max_k|f(\mathbf{v}_k)|\\
&\le (r+2)!\cdot\max_k|f(\mathbf{v}_k)|\ .
\end{aligned}$$

□

We now state the consequence for the robust hitting set constructed in Corollary 5.8. We denote $G_{\delta,r}\triangleq\{\mathbf{a}+k\cdot\mathbf{b}\mid\mathbf{a},\mathbf{b}\in G_\delta\text{ and }0\le k\le r\}$.

**Corollary 5.10** (Robust-hitting sets for $V(n,s,r)$ over $\mathbb{R}$). *There exists a constant $c$ such that for every integers $n,s,r$, for $\eta=2^{-n}\cdot\frac{1}{20\cdot(C_{CW}\cdot nr^2)^r}$ and $\delta=\frac{\eta}{(16nr^2)^{2n+1}}$, there is an $\eta/4$-robust hitting set $\mathcal{H}\subset G_{\delta,r}$, for $V(n,s,r)$, of size*

$$|\mathcal{H}|\le(nsr)^c.$$

Proof. The proof follows immediately from combining Corollary 5.8 with Theorem 5.9 and observing that $(r+2)!<10r^r$. □

## 6 EXISTENTIAL THEORY OF THE REALS

We will need the following theorem regarding the decidability of existential formulas over the reals. To keep this manuscript at a reasonable length we will not give a formal definition of sentences and formulas over the reals. The interested reader is referred to [BPR06]. Intuitively, formulas are constructed as follows. The atoms are polynomial equalities "$f(\mathbf{x})=0$" or inequalities "$f(\mathbf{x})\ge 0$". From them we build formulas in a similar fashion to the way we build formulas in first order logic using the connectives $\neg,\vee,\wedge$ and the quantifiers $\exists,\forall$ (however, in the existential theory we only allow existential quantifiers). For a set of polynomials $\mathcal{F}\subset\mathbb{R}[\mathbf{x}]$, an $\mathcal{F}$-formula is a formula in which all the polynomials appearing in the atoms are from $\mathcal{F}$.

**Theorem 6.1** (Existential theory of the reals in PSPACE [Can88]). *Let $\mathcal{F}\subset\mathbb{R}[\mathbf{x}]$ be a set of* poly$(n)$ *polynomials each of degree at most $r=$ poly$(n)$. Consider the formula $\exists x_1\exists x_2\ldots\exists x_nF(x_1,\ldots,x_n)$, where $F(\mathbf{x})$ is a quantifier free $\mathcal{F}$-formula. There is a* PSPACE *algorithm for deciding the truth of the sentence, where the size of the input to the algorithm is the bit complexity of the formula $F$.*

### 6.1 Formulas Capturing Computations by Algebraic Circuits

**Lemma 6.2** (Computation by the universal circuit). *Let $n,s,r$ be natural numbers and $\varepsilon$ be a rational number with* poly$(n)$ *bit complexity. For real vectors $\mathbf{v},\mathbf{a}$ over the reals there exists an existential sentence over the reals, $\phi(\mathbf{v},\mathbf{a},\varepsilon)$, such that $\phi(\mathbf{a},\mathbf{v},\varepsilon)$ is true iff the polynomial computed by the universal circuit for size $s$ and degree $r$, whose auxiliary variables are set to $\mathbf{a}$, evaluates on input $\mathbf{v}$, in absolute value, to at least $\varepsilon$. That is, for $\Psi(\mathbf{x},\mathbf{y})$ as in Theorem 2.2, $|\Psi(\mathbf{v},\mathbf{a})|\ge\varepsilon$.*

Proof. Let $\Psi(\mathbf{x},\mathbf{y})$ be the universal circuit for size $s$ and degree $r$ (and $n$ variables), where $\mathbf{y}$ are the auxiliary variables. For each gate $u$ of $\Psi$ let $\Psi_u(\mathbf{x},\mathbf{y})$ be the polynomial computed at $u$. For each gate $u$ of $\Psi$ let $z_u$ be a new variable and denote with $z_o$ be the variable corresponding to the output gate.

For each internal gate we assign a polynomial equation as follows: If $u$ is an addition gate with children $w_1$ and $w_2$ then we assign the equation $z_u - (z_{w_1} + z_{w_2}) = 0$ to $u$. If it is a multiplication gate with children $w_1, w_2$ then we assign the equation $z_u - z_{w_1} \cdot z_{w_2} = 0$ to $u$. In addition we assign the inequality $z_o^2 \geq \varepsilon^2$ to the output gate. For an input gate $u$ corresponding to a variable $x_i$ consider the equation $z_u - v_i = 0$. For an input gate corresponding to $y_i$ we have the equation $z_u - a_i = 0$.

Let $\mathcal{F}$ be the set of all equalities and inequalities constructed above. Consider the sentence

$$\phi(\mathbf{v},\mathbf{a},\varepsilon) \triangleq \exists \mathbf{z} \bigwedge_{g\in\mathcal{F}} g(\mathbf{z}) \,,$$

where $\exists \mathbf{z}$ is a short hand for writing $\exists z_u$ for all gates $u$ in $\Psi$. It is not hard to see that the exists an assignment to the $z_u$ satisfying this sentence iff $|\Psi(\mathbf{v},\mathbf{a})| \geq \varepsilon$. □

The next lemma shows that deciding whether a polynomial computed by the universal circuit evaluates to at least 1 on some input from $[-1,1]^n$ can be done in PSPACE.

**Lemma 6.3.** *Let $\Psi(\mathbf{x},\mathbf{y})$ be the universal circuit for size $s$ and degree $r$ (and $n$ variables). Let $f(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ be computed by $\Psi(\mathbf{x},\mathbf{y})$ when assigning $\mathbf{a}$ to the auxiliary variables. That is, $f(\mathbf{x}) = \Psi(\mathbf{x},\mathbf{a})$. Given $n, s, r$ in unary encoding there is a* PSPACE *algorithm for deciding whether there exists $\mathbf{v} \in [-1,1]^n$ on which $|f(\mathbf{v})| \geq 1$.*

Proof. Let $\mathcal{F}$ be the set of polynomials in the definition of $\phi(\mathbf{v},\mathbf{a},1)$ in Lemma 6.2. Define

$$\psi(\mathbf{a},1) \triangleq \exists \mathbf{v} \exists \mathbf{z} \left( \bigwedge_{g\in\mathcal{F}} g(\mathbf{z}) \right) \bigwedge \left( \bigwedge_i \left( (1 - v_i^2) \geq 0 \right) \right) .$$

It is not hard to see that $\psi(\mathbf{a},1)$ is true iff there exists $\mathbf{v} \in [-1,1]^n$ such that $|f(\mathbf{v})| = |\Psi(\mathbf{v},\mathbf{a})| \geq 1$. □

## 7 CONSTRUCTION OF A HITTING SET FOR $\overline{\text{VP}}$ IN PSPACE

**Algorithm 1** : Finding a robust hitting set

**Input:** Parameters $n, s, r$

1: Let $\eta, \delta$ be as in Corollary 5.10.
2: Set $\varepsilon = \frac{1}{4} \cdot \eta \cdot \left(\frac{1}{32\cdot n\cdot r^2}\right)^n$.
3: Let $m = (nsr)^c$ (as in Corollary 5.10).
4: Let $\mathbf{v}_1, \ldots, \mathbf{v}_m \in G_{\delta,r}$ so that $(\mathbf{v}_1, \ldots, \mathbf{v}_m)$ is the lexicographically first string in $G_{\delta,r}^m$.
5: **while** Robust set not found yet **do**
6: Check whether there is $\mathbf{a}$ for which $\psi(\mathbf{a},1)$ (of Lemma 6.3) is true and for all $i \in [m]$, $\phi(\mathbf{v}_i,\mathbf{a},\varepsilon)$ (of Lemma 6.2) is false.
7: If no solution $\mathbf{a}$ is found then halt and return $\mathcal{H} = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$.
8: Otherwise, move to the next $\mathbf{v}_1, \ldots, \mathbf{v}_m \in G_{\delta,r}$

**Theorem 7.1** (Main theorem). *Let $c$ be a constant as in Corollary 5.10). Algorithm 1 returns an $\varepsilon = \frac{1}{4} \cdot \left(\frac{1}{C_{CW}\cdot n\cdot r}\right)^r \cdot \left(\frac{1}{32\cdot n\cdot r^2}\right)^n$ robust hitting set of size $(nsr)^c$ for $V(n,s,r)$ and can be executed in* PSPACE*, given $n, s, r$ in unary encoding.*

Proof. We first prove that the algorithm always returns some $\mathcal{H}$ and then prove that any $\mathcal{H}$ returned by the algorithm is an $\varepsilon$ robust hitting set.

*The algorithm always outputs some set:* Corollary 5.10 guarantees that for $m = (nsr)^c$ there exist $\mathbf{v}_1, \ldots, \mathbf{v}_m \in G_{\delta,r}^m$ so that $\mathcal{H} = \{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ is an $\frac{1}{4} \cdot \frac{2^{-n}}{20\cdot(C_{CW}\cdot n\cdot r^2)^r}$ robust hitting set for $V(n,s,r)$. Assume that our while loop reached that set $\mathbf{v}_1, \ldots, \mathbf{v}_m$ (that is, the algorithm did not output any set so far).

Let $\mathbf{a}$ be any assignment for the auxiliary variables of the universal circuit and let $f = \Psi(\mathbf{x},\mathbf{a})$. If $\psi(\mathbf{a},1)$ (of Lemma 6.3) is true then for some $\mathbf{u} \in [-1,1]^n$, $|f(\mathbf{u})| \geq 1$. As $\|f\|_\infty \geq 1$, Corollary 2.6 implies that

$$\|f\|_2 \geq \frac{1}{2^{2n+2}} \cdot V(n, \frac{1}{4r^2}) \geq \left(\frac{1}{32\cdot n\cdot r^2}\right)^n .$$

As $\mathcal{H}$ is an $\frac{\eta}{4} = \frac{1}{4} \cdot \frac{2^{-n}}{20\cdot(C_{CW}\cdot n\cdot r^2)^r}$ robust hitting set for $V(n,s,r)$, for some $i$,

$$\begin{aligned} |f(\mathbf{v}_i)| &\geq \frac{1}{4} \cdot \frac{2^{-n}}{20\cdot\left(C_{CW}\cdot n\cdot r^2\right)^r} \cdot \|f\|_2 \\ &\geq \frac{1}{4} \cdot \frac{2^{-n}}{20\cdot\left(C_{CW}\cdot n\cdot r^2\right)^r} \cdot \left(\frac{1}{32\cdot n\cdot r^2}\right)^n = \varepsilon \,. \end{aligned}$$

Thus, $\phi(\mathbf{v}_i,\mathbf{a},\varepsilon)$ will return true. In particular, no solution $\mathbf{a}$ will be found and so the algorithm will return $\mathcal{H}$ if it did not halt before reaching this particular $\mathcal{H}$. Finally, note that there are polynomials $f$ for which $\psi(\mathbf{a},1)$ is true. Indeed, if $f \not\equiv 0$ then there is some multiple of it that at some point in $[-1,1]^n$ will get value at least 1. By Theorem 2.2 this multiple of $f$ is also computed by the universal circuit.

*Every output is a robust hitting set:* Assume that the algorithm returned some set $\mathcal{H} = \{\mathbf{u}_1, \ldots, \mathbf{u}_m\}$. Let $f$ be a nonzero polynomial computed by a homogeneous algebraic circuit of size $s$ and degree $r$ and assume further that $\|f(\mathbf{u})\|_\infty = 1$.[12] In particular there is some assignment $\mathbf{a}$ to the auxiliary variables of the universal circuit $\Psi$ so that $\Psi(\mathbf{x},\mathbf{a}) = f(\mathbf{x})$. Clearly, for this $\mathbf{a}$, $\psi(\mathbf{a},1)$ is true. As $\mathcal{H}$ was returned it means that for some $i$, $|f(\mathbf{u}_i)| \geq \varepsilon$. As $\|f\|_2 \leq \|f\|_\infty = 1$ we get that

$$|f(\mathbf{u}_i)| \geq \varepsilon \geq \varepsilon \cdot \|f\|_2 \,.$$

As both size of the equation scale the same way when we multiply $f$ by a field element, this equation holds regardless of $\|f\|_\infty$. In other words, $\mathcal{H}$ is an $\varepsilon$-robust hitting set for all polynomials that can be computed by size $s$ and degree $r$ homogeneous circuits and hence it is an $\varepsilon$-robust hitting set for $V(n,s,r)$.

*Complexity:* The fact that the algorithm can be run in PSPACE follows from the fact that all the vectors that are considered (and also $\varepsilon$) have polynomial bit length and from Lemma 6.2 and Lemma 6.3. □

[12] We can restrict our attention to such $f$'s as for any constant $\alpha$ the universal circuit also computes $\alpha \cdot f$. See Theorem 2.2.

## REFERENCES


[Blä13] Markus Bläser. Fast Matrix Multiplication. *Theory of Computing, Graduate Surveys*, 5:1–60, 2013.

[BPR06] Saugata Basu, Richard Pollack, and Marie-Françoise Roy. *Algorithms in Real Algebraic Geometry*. Springer-Verlag, 2006.

[Bür04] Peter Bürgisser. The Complexity of Factors of Multivariate Polynomials. *Foundations of Computational Mathematics*, 4(4):369–396, 2004.

[Can88] John F. Canny. Some Algebraic and Geometric Computations in PSPACE. In Janos Simon, editor, *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 460–467. ACM, 1988.

[CLO06] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2006.

[CW01] Anthony Carbery and James Wright. Distributional and L^q norm inequalities for polynomials over convex bodies in R^n. *Mathematical Research Letters*, 8(3):233–248, 2001.

[GMQ16] Joshua A. Grochow, Ketan D. Mulmuley, and Youming Qiao. Boundaries of VP and VNP. In Ioannis Chatzigiannakis, Michael Mitzenmacher, Yuval Rabani, and Davide Sangiorgi, editors, *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, volume 55 of *LIPIcs*, pages 34:1–34:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016.

[HS80a] Joos Heintz and Claus-Peter Schnorr. Testing Polynomials which Are Easy to Compute (Extended Abstract). In Raymond E. Miller, Seymour Ginsburg, Walter A. Burkhard, and Richard J. Lipton, editors, *Proceedings of the 12th Annual ACM Symposium on Theory of Computing, April 28-30, 1980, Los Angeles, California, USA*, pages 262–272. ACM, 1980.

[HS80b] Joos Heintz and Malte Sieveking. Lower bounds for polynomials with algebraic coefficients. *Theoretical Computer Science*, 11(3):321–330, 1980.

[Koi96] Pascal Koiran. Hilbert's Nullstellensatz Is in the Polynomial Hierarchy. *J. Complexity*, 12(4):273–286, 1996.

[LL89] Thomas Lehmkuhl and Thomas Lickteig. On the Order of Approximation in Approximative Triadic Decompositions of Tensors. *Theor. Comput. Sci.*, 66(1):1–14, 1989.

[Mul17] Ketan D. Mulmuley. Geometric complexity theory V: Efficient algorithms for Noether normalization. *J. Amer. Math. Soc.*, 30(1):225âĂŞ309, 2017.

[Raz10] Ran Raz. Elusive Functions and Lower Bounds for Arithmetic Circuits. *Theory of Computing*, 6(1):135–177, 2010.

[San91] Giovanni Sansone. *Orthogonal Functions*. Dover Books on Advanced Mathematics. Dover Publications, revised edition, 1991.

[Sha88] Igor R. Shafarevich. *Basic Algebraic Geometry 2*. Springer-Verlag, 1988.

[SY10] Amir Shpilka and Amir Yehudayoff. Arithmetic Circuits: A survey of recent results and open questions. *Foundations and Trends in Theoretical Computer Science*, 5(3-4):207–388, 2010.

[Wil74] Don R. Wilhelmsen. A Markov inequality in several dimensions. *Journal of Approximation Theory*, 11(3):216–220, 1974.