An Exposition of "A PSPACE construction of Hitting Set for the Closure of Small Algebraic Circuits".

Somnath Dake

Under the supervision of

K. V. Subrahmanyam

Saturday 24th October, 2020

Abstract

In this paper authors study the complexity of constructing a hitting set for closure of VP, the class of polynomials that can be infinitesimally approximated by polynomials that are computed by polynomial sized algebraic circuits. Specifically, authors prove that there is a PSPACE algorithm which given n, s, r in unary outputs a set of inputs from $\mathbb{Q}^n$ of size $poly(n, s, r)$, with $poly(n, s, r)$ bit complexity, that hits all n-variate polynomials of degree r which are in the limit of polynomials computed by size s algebraic circuits. We say a set $\mathcal{H}$ consisting of n-tuples of rational numbers hits a polynomial p in n variables, if there is at least one element in $\mathcal{H}$ on which p evaluates to non-zero. It was known that a random set of n-tuples of the same size is a hitting set, but the best deterministic construction known before this work was in EXPSPACE.

Hitting sets can be constructed for VP in PSPACE (Mul17). The authors study this construction carefully to try and see if this can be modified to work for VP closure as well. They identify the main technical difficulty in extending the existing constructions known for VP to the closure of VP. They come up with the notion of a robust hitting set. A set of inputs is said to be a robust hitting set if for every nonzero polynomial that can be computed by a polynomial sized algebraic circuit there is an element of the set on which this polynomial evaluates to a not too small value.

The authors show the existence of such robust hitting sets using anti-concentration results for polynomials and some tools from algebraic geometry. Then using the existential theory of reals they give a PSACE construction.

Contents

1 Introduction

In the paper [FS17] authors study the following problem. What is the complexity of constructing a set that is guaranteed to be a hitting set for $\overline{\text{VP}}$? 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 $v \in \mathcal{H}$ such that $f(\boldsymbol{v}) \neq 0$. $\overline{\text{VP}}$ consist of polynomials that can be infinitesimally approximated by small algebraic circuits.

The question of constructing a hitting set for $\overline{\text{VP}}$ 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 $\overline{\text{VP}}$. For VP, he proved that it can be done in PSPACE using the results in [HS80a], [Raz10] and [Koi96]. In the paper authors solve the problem for $\overline{\text{VP}}$.

1.1 Sketch of proof

First we will study the PSPACE algorithms which construct hitting set for VP. The idea is that one can enumerate over all subsets of search space and for each such subset check whether there exists a circuit that computes a nonzero polynomial that vanishes over the subset. To get a PSPACE algorithm from the idea, first we need to prove the existence of search space which can be enumerated in PSPACE, this is already done in [HS80a], the paper also proves that size of hitting set is polynomially bounded. Second we need a procedure which can check in PSPACE that the subset is hitting set or not, this can be done using universal circuit. The universal circuit $\Psi(\boldsymbol{x}, \boldsymbol{y})$ is a circuit in n essential variables $\boldsymbol{x}$ and $poly(r, s)$ auxiliary variables $\boldsymbol{y}$ such that for any size s and degree r circuit $\phi(\boldsymbol{x})$ there is an assignment $\boldsymbol{a}$, to the auxiliary variables, so that the polynomials computed by $\Psi(\boldsymbol{x}, \boldsymbol{a})$ and $\phi(\boldsymbol{x})$ are the same. Thus, if our subset is $\boldsymbol{v}_1, ..., \boldsymbol{v}_m$, where m is polynomially bounded and if we can check whether there is $\boldsymbol{y}$ such that

$$\forall i\big(\Psi(\boldsymbol{v}_i, \boldsymbol{y}) = 0\big) \; and \; \exists \boldsymbol{u}\big(\psi(\boldsymbol{u}, \boldsymbol{y}) = 1\big).$$

then $\boldsymbol{v}_1, ..., \boldsymbol{v}_m$ is not a hitting set. Above expression can be checked in PSPACE using Hilbert's Nullstellensatz. 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 and it is solvable in PSPACE, see [Koi96].

We would like to use similar approach to construct hitting set for $\overline{\text{VP}}$. The problem is that even if $\mathcal{H}$ is a hitting set for the n-variate circuits of size s and degree r, it may be the case that for a sequence of polynomials $\{f_i\}$, even if $f_i(\boldsymbol{v}) \neq 0$ for all i, the limit polynomial may still vanish at $\boldsymbol{v}$. Thus, it is not clear that $\mathcal{H}$ also hits the closure of n variate circuits of size s and degree r.

To overcome the discrepancy between a hitting set for VP and a hitting set for VP, we would like to find what we call a "robust hitting set", a set of inputs is said to be a η-robust hitting set if for every nonzero polynomial that can be computed by a polynomial sized algebraic circuit there is an element of the set on which this polynomial evaluates to at least $\eta > 0$, after adequate normalization. Thus, if f_i are all normalized and evaluate to at least η on $\boldsymbol{v} \in \mathcal{H}$, then if $\lim f_i = f$ then by continuity f also evaluates to at least η on $\boldsymbol{v}$. Thus, $\mathcal{H}$ hits f as well.

Therefore, the first step in our proof is to prove the existence of poly size robust hitting set and a search space which can be enumerated in PSPACE. We need to move to $\mathbb{C}$ since we want to use few results in algebraic geometry. Then our search space for robust hitting set will be

$$G_\delta^{\mathbb{C}} = \{\boldsymbol{a} + \iota \boldsymbol{b} : \boldsymbol{a}, \boldsymbol{b} \in \{-1, -1 + \delta, -1 + 2\delta, ..., 1 - 2\delta, 1 - \delta\}^n\}.$$

We note that [HS80a] proved the existence of a poly size hitting set for n-variate circuits of size s and degree r, but their proof does not yield robust hitting set. To prove the existence of robust hitting set which is subset of $G_\delta^{\mathbb{C}}$, we think of a polynomials as points represented by coefficient vectors in euclidean space. we use the bounds given by Heintz and Sieveking [HS80b] on the dimension, denoted by d, and degree, denoted by D, of the algebraic variety of efficiently computable polynomials, we denote the algebraic variety by $V(n, s, r)$. Following are the steps to prove existence of robust hitting set:

- Prove existence of ϵ-net E for $V(n, s, r)$ and find the bound on size of E. The proof we give is geometric in nature and bound we will get on $|E|$ is $D \cdot (\frac{N}{\epsilon})^{\mathcal{O}(d)}$ where N is number of n-variate monomials of degree r.
- For some $\eta > 0$, prove existence of poly size η-robust hitting set $\mathcal{H}$ for E. The proof is probabilistic in nature and uses anti-concentration result for polynomials proved in [CW01].
- Prove if $\mathcal{H}$ is η-robust hitting set for E then for some $\eta' > 0$ it is η'-robust hitting set for $V(n, s, r)$. The proof uses few results related to norms of polynomial and find the relation between η and η'.

Now that we know that robust hitting sets exist the PSPACE algorithm works as follows. It enumerates over all subsets of a $G_\delta^{\mathbb{C}}$ of polynomial size. For each such subset it checks whether there exists an normalized algebraic circuit that evaluates to at most η 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 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.

1.2 Notations

We shall use the following notation.

- n is number of variables in circuit.
- s is size of circuit.
- r is degree of circuit.
- $N = \binom{n+r-1}{r}$ is number of n-variate monomials of degree r.
- $\boldsymbol{f}$ is vector of coefficients of polynomial f.
- $G_\delta = \{-1, -1+\delta, -1+2\delta, ..., 1-2\delta, 1-\delta\}^n$ where $0 < \delta < 1$. We call it δ-grid in $\mathbb{R}^n$.
- $G_\delta^{\mathbb{C}} = \{\boldsymbol{a} + \iota\boldsymbol{b} : a, b \in G_\delta\}$. We call it δ-grid in $\mathbb{C}^n$.
- $[-1, 1]_{\mathbb{C}}^N = [-1, 1]^N + \iota \cdot [-1, 1]^N = \{\boldsymbol{a} + \iota\boldsymbol{b} : \boldsymbol{a}, \boldsymbol{b} \in [-1, 1]^N\}$

2 Preliminaries

2.1 Algebraic Circuits

An *Algebraic Circuit* is a directed acyclic graph whose leaves are labeled by either variables $x_1, ..., x_n$ or elements from the field $\mathbb{F}$, 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. A circuit is called *homogeneous* if every gate in it computes a homogeneous polynomial.

We define *complexity* of a polynomial to be the size of a smallest circuit computing it. **VP** consist of sequences of polynomials $\{f_n\}$ such that for each n, complexity of f_n and degree of f_n is polynomially bounded in n, that is there exist polynomial $t : \mathbb{N} \to \mathbb{N}$ such that complexity and degree of f_n is bounded by $t(n)$. For more on Algebraic Circuits see [AB09], [MAH12]

The class of polynomials that can be infinitesimally approximated by polynomial size algebraic circuits is denoted by $\overline{\text{VP}}$. Formal definition over field $\mathbb{C}$ is as follows:

Definition 1 ($\overline{\text{VP}}$)**.** *We say that a polynomial family $\{f_n\}, n \in \mathbb{N}$ is in $\overline{VP}$, if there exists a family of sequences of polynomials $\{f_n^{(i)}\}, n \in \mathbb{N}$ in VP for $i = 1, 2, ...$, such that for every n, the sequence of polynomials $f_n^{(i)}, i = 1, 2, ...$, converges coefficient-wise to f_n, in the usual complex topology.*

Note that if sequence of polynomials converges to a polynomial coefficient-wise then the convergence is also point-wise

Definition 2 (Hitting Set)**.** *A set $\mathcal{H} \subset \mathbb{F}^n$ is a hitting set for a circuit class $\mathcal{C}$ if for every nonzero polynomial $f \in \mathcal{C}$, there exists $\boldsymbol{a} \in \mathcal{H}$ such that $f(\boldsymbol{a}) \neq 0$.*

Next we define universal circuit for homogeneous n-variate polynomials[1] of degree r and computable by circuits of size s, intuitively circuit Ψ is universal for class $\mathcal{C}$ of polynomials if every polynomial $f \in \mathcal{C}$ is a projection of Ψ.

Definition 3 (Universal Circuit)**.** *A homogeneous algebraic circuit Ψ is said to be universal for n-variate homogeneous circuits of size s and degree r if Ψ has n essential-inputs $\boldsymbol{x}$ and m auxiliary-inputs $\boldsymbol{y}$, 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 $\boldsymbol{a}$ to the m auxiliary-variables of Ψ such that the polynomial computed by $\Psi(\boldsymbol{x}, \boldsymbol{a})$ is $f(\boldsymbol{x})$.*

Next theorem states existence of Universal circuit.

Theorem 4 (Existence of Universal Circuit[Raz08])**.** *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 Ψ such that Ψ has n essential-variables, $c_1 \cdot sr^4$ auxiliary-variables, degree $c_2 \cdot r$ and size $c_1 \cdot sr^4$ and it is universal for n-variate homogeneous circuits of size s and degree r. Furthermore, for any polynomial $f(\boldsymbol{x})$ that can be computed by Ψ and any constant α, the polynomial $\alpha \cdot f$ can also be computed by Ψ.*

[1] Polynomial is homogeneous if all monomials in polynomial with nonzero coefficient have same degree.

2.2 Markov Inequality

Let f be a n-variate polynomial of degree at most r, T be a convex compact in $\mathbb{R}^n$, ∂T be the boundry of T and for every $\boldsymbol{v} \in T,\ |f(\boldsymbol{v})| \leq 1$. Let $\boldsymbol{v}^* \in T$ such that for all $\boldsymbol{v} \in T,\ \|(\nabla f)(\boldsymbol{v}^*)\|_2 \geq \|(\nabla f)(\boldsymbol{v})\|_2$.

For any $\boldsymbol{v}_0 \in \partial T$, let $\boldsymbol{u} \in \mathbb{R}^n$ be unit vector such that for any $\boldsymbol{v} \in T, \langle \boldsymbol{v} - \boldsymbol{v}_0, u\rangle \leq 0$. We call such $\boldsymbol{u}$ an outer normal of T at $\boldsymbol{v}_0$ (Note that for any $\boldsymbol{v}_0$ such u exist but need not be unique, also for any $\boldsymbol{u}$ there is $\boldsymbol{v}_0$ such that $\boldsymbol{u}$ is outer normal of T at $\boldsymbol{v}_0$ again need not be unique). For any outer normal $\boldsymbol{u}$ of T at $\boldsymbol{v}_0$, let $H_u = \{\boldsymbol{w} : \langle \boldsymbol{w} - \boldsymbol{v}_0, \boldsymbol{u}\rangle = 0\}$. We call H_u the support hyperplane of T at $\boldsymbol{v}_0$. Let $\omega_u = |\langle \boldsymbol{w}_1 - \boldsymbol{w}_2, \boldsymbol{u}\rangle|$ for any $\boldsymbol{w}_1 \in H_u, \boldsymbol{w}_2 \in H_{-u}$, the distance between H_u and H_{-u}. We denote $\lambda = inf\{\omega_u : \boldsymbol{u} \in \mathbb{R}^n, \|u\|_2 = 1,\ \omega_u \text{ is distance between } H_u \text{ and } H_{-u}\}$

Theorem 5. *For all $\boldsymbol{v} \in T,\ \|(\nabla f)(\boldsymbol{v})\|_2 < \frac{4r^2}{\lambda}$.*

If f is constant function then result is trivial, hence we assume f is not constant. We will use following result while proving the theorem:

Theorem 6. *If $p : [-1, 1] \to [-1, 1]$ be a polynomial of degree r then for all $v,\ |p'(v)| \leq r^2$*

Corollary 7. *If $p : [a, b] \to [-1, 1]$ be a polynomial of degree r then for all $v,\ |p'(v)| \leq \frac{2r^2}{b-a}$.*

Proof. This can be easily proved by applying scaling and translation on polynomial and using theorem 2. □

We will use following lemma as one of the case.

Lemma 8. *If $|f(\boldsymbol{v}^*)| = 1$ then $\|(\nabla f)(\boldsymbol{v}^*)\|_2 \leq \frac{2r^2}{\lambda}$*

Proof. $\boldsymbol{v}^* \in \partial T$ since otherwise we can find a point $\boldsymbol{v}_0 \in T$ such that $|f(\boldsymbol{v}_0)| > 1$ using $\|(\nabla f)(\boldsymbol{v}*)\|_2 \neq 0$ and $|f(\boldsymbol{v}^*)| = 1$ (which contradict $|f(\boldsymbol{v})| \leq 1$ for all $\boldsymbol{v} \in T$). Let $f(\boldsymbol{v}^*) = 1$ (the case for $f(\boldsymbol{v}^*) = -1$ is similar) and $\boldsymbol{u} = (\nabla f)(\boldsymbol{v}^*)/\|(\nabla f)(\boldsymbol{v}^*)\|_2$, the unit vector in the direction of gradient at $\boldsymbol{v}^*$. We claim that $\boldsymbol{u}$ is the outer normal of T at $\boldsymbol{v}^*$. If not, there is $\boldsymbol{v}_0 \in T$ such that $\langle \boldsymbol{v}_0 - \boldsymbol{v}^*, \boldsymbol{u}\rangle > 0$ which implies f is strictly increasing in the direction $\boldsymbol{v}_0 - \boldsymbol{v}^*$ at $\boldsymbol{v}^*$. Since T is convex, there is $\boldsymbol{v}_1 \in T$ on line segment joining $\boldsymbol{v}_0$ and $\boldsymbol{v}^*$ such that $f(\boldsymbol{v}_1) > 1$ since $f(\boldsymbol{v}^*) = 1$, which contradicts for every $\boldsymbol{v} \in T,\ |f(\boldsymbol{v})| \leq 1$.

Let H_u and H_{-u} be the support hyperplanes of T at $\boldsymbol{v}^*$ and $\boldsymbol{v}_1$ respectively and ω_u is the distance between them. Since T is convex, line segment $[\boldsymbol{v}^*, \boldsymbol{v}_1] \in T$. $f|_{[\boldsymbol{v}^*, \boldsymbol{v}_1]}$ is univariate polynomial of degree at most r given by $f|_{[\boldsymbol{v}^*, \boldsymbol{v}_1]}(t) = f(\boldsymbol{v}^* + t\boldsymbol{w})$ where $t \in [0, \|v_1 - v^*\|_2]$ and $\boldsymbol{w} = (\boldsymbol{v}_1 - \boldsymbol{v}^*)/\|\boldsymbol{v}_1 - \boldsymbol{v}^*\|_2$. By Corollary 1, we have

$$\frac{2r^2}{\|\boldsymbol{v}_1 - \boldsymbol{v}^*\|_2} \geq |f|'_{[\boldsymbol{v}^*, \boldsymbol{v}_1]}(t)|$$

In perticular for $t = 0$

$$\begin{aligned}
\frac{2r^2}{\|\boldsymbol{v}_1 - \boldsymbol{v}^*\|_2} &\geq |f|'_{[\boldsymbol{v}^*, \boldsymbol{v}_1]}(0)| = |\langle (\nabla f)(\boldsymbol{v}^*), \boldsymbol{w}\rangle| \\
&= \|(\nabla f)(\boldsymbol{v}^*)\|_2 \cdot \frac{\omega_u}{\|\boldsymbol{v}_1 - \boldsymbol{v}^*\|_2} \\
&\geq \frac{\lambda \cdot \|(\nabla f)(\boldsymbol{v}^*)\|_2}{\|\boldsymbol{v}_1 - \boldsymbol{v}^*\|_2}
\end{aligned}$$

$$\frac{2r^2}{\lambda} \geq \|(\nabla f)(\boldsymbol{v}*)\|_2$$

□

Proof of Theorem 1. Since $\|(\nabla f)(\boldsymbol{v}^*)\|_2 \geq \|(\nabla f)(\boldsymbol{v})\|_2 \; \forall \boldsymbol{v} \in T$, it suffices to prove that $\|(\nabla f)(\boldsymbol{v}^*)\|_2 < \frac{4r^2}{\lambda}$. the case for $|f(\boldsymbol{v}^*)| = 1$ is proved in lemma above, hence we can assume $|f(\boldsymbol{v}^*)| < 1$. Let $\boldsymbol{u} = (\nabla f)(\boldsymbol{v}^*)/\|(\nabla f)(\boldsymbol{v}^*)\|_2$, H_u and H_{-u} be the support hyperplanes of T at $\boldsymbol{v}_0$ and $\boldsymbol{v}_1$ respectively. Assume distance[2] between $\boldsymbol{v}^*$ and H_u is $\geq \omega_u/2$. (Proof of the case $d(H_{-u}, t^*) \geq \omega_u/2$ is simillar). Since $|f(\boldsymbol{v}^*)| < 1$, we can find $\boldsymbol{v}_\delta$ in the direction of $\boldsymbol{v}^* - \boldsymbol{v}_0$ such that $|f(\boldsymbol{v})| \leq 1$ for any $\boldsymbol{v}$ on segment $[\boldsymbol{v}_0, \boldsymbol{v}_\delta]$ and $d(H_u, \boldsymbol{v}_\delta) > \omega_u/2 \geq \lambda/2$. By applying Corollary 1 to univariate polynomial $f|_{[\boldsymbol{v}_0, \boldsymbol{v}_\delta]}(t) = f(\boldsymbol{v}_0 + t\boldsymbol{w})$, $t \in [0, \|\boldsymbol{v}_\delta - \boldsymbol{v}_0\|_2]$, $\boldsymbol{w} = (v_\delta - v_0)/\|v_\delta - v_0\|_2$ and degree $\leq r$, we get

$$\frac{2r^2}{\|v_\delta - \boldsymbol{v}_0\|_2} \geq |f|'_{[\boldsymbol{v}_0, v_\delta]}(t)|$$

In perticular for $t = \|\boldsymbol{v}^* - \boldsymbol{v}_0\|_2$

$$\begin{aligned}
\frac{2r^2}{\|\boldsymbol{v}_\delta - \boldsymbol{v}_0\|_2}| &\geq |f|'_{[\boldsymbol{v}_0, v_\delta]}(\|\boldsymbol{v}^* - \boldsymbol{v}_0\|_2)| \\
&= |\langle (\nabla f)(\boldsymbol{v}*), \boldsymbol{w} \rangle| \\
&= \|(\nabla f)(\boldsymbol{v}^*)\|_2 \cdot \frac{d(H_u, v_\delta)}{\|v_\delta - \boldsymbol{v}_0\|_2} \\
&> \frac{\lambda \|(\nabla f)(\boldsymbol{v}^*)\|_2}{2\|v_\delta - \boldsymbol{v}_0\|_2} \\
\frac{4r^2}{\lambda} &> \|(\nabla f)(\boldsymbol{v}^*)\|_2
\end{aligned}$$

□

2.3 Norms

Definition 9 (Inner Product)**.** *Let $\mathbb{F}$ be the field of real or complex numbers, and V a vector space over $\mathbb{F}$. An inner product on V is a function which assigns to each ordered pair of vectors $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ a scalar denoted by $\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$ in $\mathbb{F}$ in such a way that for all $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3 \in V$ and all scalars $c \in \mathbb{F}$*

1. $\langle \boldsymbol{v}_1 + \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle = \langle \boldsymbol{v}_1, \boldsymbol{v}_3 \rangle + \langle \boldsymbol{v}_2, \boldsymbol{v}_3 \rangle$.
2. $\langle c\boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = c\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle$.
3. $\langle \boldsymbol{v}_1, \boldsymbol{v}_2 \rangle = \overline{\langle \boldsymbol{v}_2, \boldsymbol{v}_1 \rangle}$.
4. $\langle \boldsymbol{v}_1, \boldsymbol{v}_1 \rangle > 0$ *if* $\boldsymbol{v}_1 \neq 0$.

Definition 10 (Norm)**.** *Let $\mathbb{F}$ be the field of real or complex numbers, and V a vector space over $\mathbb{F}$. A norm on V is a function which assigns each vector $\boldsymbol{v} \in V$ a scalar denoted by $\|\boldsymbol{v}\|$ in $[0, +\infty)$ such that for all $\boldsymbol{v}_1, \boldsymbol{v}_2 \in V$ and scalar $c \in \mathbb{F}$*

1. $\|\boldsymbol{v}_1 + \boldsymbol{v}_2\| \leq \|\boldsymbol{v}_1\| + \|\boldsymbol{v}_2\|$
2. $\|c\boldsymbol{v}_1\| = |c| \cdot \|\boldsymbol{v}_1\|$

[2]The distance is defined as $d(H_u, \boldsymbol{v}^*) = |\langle \boldsymbol{v} - \boldsymbol{v}^*, \boldsymbol{u} \rangle|$ for any $\boldsymbol{v} \in H_u$.

3. If $\|\boldsymbol{v}_1\| = 0$ then $\boldsymbol{v}_1 = 0$

Lemma 11 (Inner Product in $\mathbb{R}[\boldsymbol{x}]$)**.** *Let $f, g \in \mathbb{R}[\boldsymbol{x}]$. Prove that the formula*

$$\langle f, g\rangle = \int_{[-1,1]^n} f(\boldsymbol{x})g(\boldsymbol{x})d\mu(\boldsymbol{x})$$

defines inner product on the space $\mathbb{R}[\boldsymbol{x}]$.

Lemma 12 (L_2 Norm on $\mathbb{R}[\boldsymbol{x}]$)**.** *Let $f \in \mathbb{R}[\boldsymbol{x}]$. Prove that the formula*

$$\|f\|_2 = \left(\int_{[-1,1]^n} f(\boldsymbol{x})^2 d\mu(\boldsymbol{x})\right)^{\frac{1}{2}}$$

defines norm over $\mathbb{R}[\boldsymbol{x}]$. We call this norm the L_2 norm over $\mathbb{R}[\boldsymbol{x}]$.

Lemma 13 (L_2 Norm on $\mathbb{C}[\boldsymbol{x}]$)**.** *Let $f \in \mathbb{C}[\boldsymbol{x}]$. Prove that the formula*

$$\|f\|_2 = \|\Re(f)\|_2 + \|\Im(f)\|_2$$

defines norm over $\mathbb{C}[\boldsymbol{x}]$. Where $\|\Re(f)\|_2$ and $\|\Im(f)\|_2$ are L_2 norm defined in above lemma over $\mathbb{R}[\boldsymbol{x}]$[3]. We call this norm the L_2 norm over $\mathbb{C}[\boldsymbol{x}]$.

Lemma 14 (Supremum Norm on $\mathbb{C}[\boldsymbol{x}]$)**.** *Let $f \in \mathbb{C}[\boldsymbol{x}]$. Prove that the formula*

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

defines norm over $\mathbb{C}[\boldsymbol{x}]$. We call this norm the supremum norm.

Proofs of Lemma 3, 4, 5 and 6 are very easy and left as exercise. We will use these lemmas as definitions of respective terms.

We denote n-dimensional ball of radius α centered at $\boldsymbol{u}$ by $B(n, \alpha, \boldsymbol{u})$ and its Lebesgue measure by $vol(n, \alpha)$.

Theorem 15. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be a homogeneous polynomial of degree r, then*

$$\|f\|_2 \geq \frac{1}{2^{n+1}}\|f\|_\infty \Big(vol(n, \frac{1}{4r^2})\Big)^{1/2}.$$

Proof. Let $g = \frac{1}{\|f\|_\infty} f$, hence $\|g\|_\infty = 1$. Let $\boldsymbol{u} \in [-1,1]^n$ such that $|g(\boldsymbol{u})| = 1$, Assume $g(\boldsymbol{u}) = 1$ (The case for $g(\boldsymbol{u}) = -1$ is simillar). Define set $A = B(n, \frac{1}{4r^2}, \boldsymbol{u}) \cap [-1,1]^n$. Since $\boldsymbol{u} \in [-1,1]^n$, at least 2^{-n} part of $B(n, \frac{1}{4r^2}, \boldsymbol{u})$ is inside of $[-1,1]^n$, also μ on $[-1,1]^n$ scale down the Lebesgue measure by 2^{-n}, we have $\mu(A) \geq \frac{1}{4^n} vol(n, \frac{1}{4r^2})$.

We claim that for any $\boldsymbol{v} \in A$, $g(\boldsymbol{v}) \geq \frac{1}{2}$. Since gradient is bounded by $2r^2$ on $[-1,1]^n$ and $\|\boldsymbol{v} - \boldsymbol{u}\|_2 = \frac{1}{4r^2}$, maximum fall in the direction of $\boldsymbol{v} - \boldsymbol{u}$ is bounded by $\frac{1}{2}$, hence $g(\boldsymbol{v}) \geq \frac{1}{2}$, hence we have

$$\|g\|_2 = \left(\int_{[-1,1]^n} g^2(x)d\mu(x)\right)^{1/2} \geq \left(\int_A \frac{1}{4}d\mu(x)\right)^{1/2} \geq \Big(\frac{1}{4}\mu(A)\Big)^{1/2} \geq \frac{1}{2^{n+1}}\Big(Vol(n, \frac{1}{4r^2})\Big)^{1/2}.$$

Claim is now trivial. □

[3]Note the difference between $\boldsymbol{x}$ in $\mathbb{R}[\boldsymbol{x}]$ and $\mathbb{C}[\boldsymbol{x}]$.

Next we prove the result stating relation between L_2-norm of polynomial and largest coefficient of monomials in polynomial.

Theorem 16. *Let f be a n-variate homogeneous polynomial of degree r and one of the coefficients in f is at least α. Then $\|f\|_2 \geq \alpha 2^{n/2} e^{-r}$.*

To prove this theorem, first we construct orthrogonal basis for space of n-variate polynomials. We start with natural basis of $\mathbb{R}[x]$ i.e. $\{1, x, x^2, x^3, ...\}$ and construct orthrogonal basis by Gram-Schmidt w.r.t. following inner product

$$f \cdot g = \int_{-1}^{1} f(x)g(x)d\mu(x)$$

Each basis polynomial obtained is called Legendre polynomial. We take this as given without going into the actual construction[4]. We denote by L_k the k^{th} Legendre polynomial. We will use the following properties of Legendre polynomials.

1. Leading coefficient(coefficient of degree term) of L_k is $\frac{1}{2^k}\binom{2k}{k}$
2. $\int_{-1}^{1} L_k(x)L_m(x)\,\mathrm{d}x = \delta_{km}\frac{2}{2k+1}$. Where δ_{km} is Kronecker delta.
3. Degree of L_k is k

For any $\boldsymbol{e} = (e_1, e_2, ..., e_n) \in \mathbb{N}^n$, define $L_{\boldsymbol{e}} = \prod_{i=1}^{n} L_{e_i}$. It is easy to see that coefficient of term $\boldsymbol{x}^{\boldsymbol{e}}$ in[5] $L_{\boldsymbol{e}}$ is $\prod_{i=1}^{n} \frac{1}{2^{e_i}}\binom{2e_i}{e_i}$.

Lemma 17. *$\{L_{\boldsymbol{e}} : \forall \boldsymbol{e} \in \mathbb{N}^n\}$ is orthrogonal family of polynomials in $\mathbb{R}[\boldsymbol{x}]$ w.r.t inner product.*

$$f \cdot g = \int_{[-1,1]^n} f(\boldsymbol{x})g(\boldsymbol{x})d\mu(\boldsymbol{x})$$

Proof.

$$\begin{aligned}
L_{\boldsymbol{e}_1} \cdot L_{\boldsymbol{e}_2} &= \int_{[-1,1]^n} \prod_{i=1}^{n} L_{e_{1i}}(x_i) \prod_{j=1}^{n} L_{e_{2j}}(x_j)d\mu(\boldsymbol{x}) \\
&= \int_{-1}^{1}\int_{-1}^{1} ... \int_{-1}^{1} \prod_{i=1}^{n} (L_{e_{1i}}(x_i)L_{e_{2i}}(x_i))d\mu(x_1)d\mu(x_2)...d\mu(x_n) \\
&= \prod_{i=1}^{n} \int_{-1}^{1} L_{e_{1i}}(x_i)L_{e_{2i}}(x_i)d\mu(x_i) \\
&= \prod_{i=1}^{n} \frac{2}{2e_i+1} && (e_1 = e_2 = e) \\
&= 0 && (e_1 \neq e_2)
\end{aligned}$$

□

[4]Refer http://web.mit.edu/18.06/www/Spring09/legendre.pdf for actual construction.
[5]$\boldsymbol{x}^{\boldsymbol{e}} = \prod_{i=1}^{n} x_i^{e_i}$

Lemma 18. *Let f be a n-variate homogeneous polynomial of degree r. Then for any exponent vector $\boldsymbol{e}' = (e'_1, e'_2, ..., e'_n)$ such that $\sum_{i=1}^n e'_i = r$ we have*

$$l_{\boldsymbol{e}'} = c_{\boldsymbol{e}'} \prod_{i=1}^n 2^{e'_i} \frac{1}{\binom{2e'_i}{e'_i}}$$

Where $c_{\boldsymbol{e}'}$ is coefficient of $\boldsymbol{x}^{\boldsymbol{e}'}$ in f and $l_{\boldsymbol{e}'}$ is coefficient of $L_{\boldsymbol{e}'}$ in Legendre expansion of f.

Proof.

$$\begin{aligned} l_{\boldsymbol{e}'} &= \frac{f \cdot L_{\boldsymbol{e}'}}{\|L_{\boldsymbol{e}'}\|_2^2} = \frac{1}{\|L_{\boldsymbol{e}'}\|_2^2} \cdot \int_{[-1,1]^n} f \cdot L_{\boldsymbol{e}'} d\mu(\boldsymbol{x}) \\ &= \frac{1}{\|L_{\boldsymbol{e}'}\|_2^2} \cdot \sum_{\boldsymbol{e}} \int_{[-1,1]^n} c_{\boldsymbol{e}} \boldsymbol{x}^{\boldsymbol{e}} L_{\boldsymbol{e}'} d\mu(\boldsymbol{x}) \\ &= \frac{1}{\|L_{\boldsymbol{e}'}\|_2^2} \cdot \sum_{\boldsymbol{e}} c_{\boldsymbol{e}} \prod_{i=1}^n \int_{-1}^1 x_i^{e_i} L_{e'_i} d\mu(x_i) \end{aligned}$$

f is homogeneous $\Rightarrow \forall \boldsymbol{e}\ \exists i (e_i < e'_i) \Rightarrow$ by consrtuction of univariate Legendre basis $\int_{-1}^1 x_i^{e_i} L_{e'_i} d\mu(x_i) = 0 \Rightarrow$ if $\boldsymbol{e} \neq \boldsymbol{e}'$ then $\int_{[-1,1]^n} \boldsymbol{x}^{\boldsymbol{e}} L_{\boldsymbol{e}'} d\mu(\boldsymbol{x}) = 0$, thus we have

$$\begin{aligned} l_{\boldsymbol{e}'} &= \frac{c_{\boldsymbol{e}'}}{\|L_{\boldsymbol{e}'}\|_2^2} \cdot \prod_{i=0}^n \int_{-1}^1 x_i^{e'_i} L_{e'_i} d\mu(x_i) = \frac{c_{\boldsymbol{e}'}}{\|L_{\boldsymbol{e}'}\|_2^2} \cdot \int_{[-1,1]^n} \boldsymbol{x}^{\boldsymbol{e}'} L_{\boldsymbol{e}'} d\mu(\boldsymbol{x}) \\ &= \frac{c_{\boldsymbol{e}'}}{\|L_{\boldsymbol{e}'}\|_2^2} \cdot \int_{[-1,1]^n} \left[\prod_{i=1}^n \frac{2^{e'_i}}{\binom{2e'_i}{e'_i}} (L_{\boldsymbol{e}'} - \textit{lower degree terms in } L_{\boldsymbol{e}'}) \right] L_{\boldsymbol{e}'} d\mu(\boldsymbol{x}) \\ &= c_{\boldsymbol{e}'} \prod_{i=0}^n \frac{2^{e'_i}}{\binom{2e'_i}{e'_i}} \cdot \frac{1}{\|L_{\boldsymbol{e}'}\|_2^2} \int_{[-1,1]^n} L_{\boldsymbol{e}'}^2 d\mu(\boldsymbol{x}) \\ &\qquad\qquad (\textstyle\int_{[-1,1]^n} (\textit{lower degree terms in } L_{\boldsymbol{e}'}) L_{\boldsymbol{e}'} d\mu(\boldsymbol{x}) = 0) \end{aligned}$$

□

No we will give the proof of theorem 1

Proof of Theorem 1. Let $f = \sum_{\boldsymbol{e}} l_{\boldsymbol{e}} L_{\boldsymbol{e}}$ be the Legendre expansion of f

$$\begin{aligned} \|f\|_2^2 &= \int_{[-1,1]^n} \sum_{\boldsymbol{e}_1, \boldsymbol{e}_2} l_{\boldsymbol{e}_1} l_{\boldsymbol{e}_2} (L_{\boldsymbol{e}_1} \cdot L_{\boldsymbol{e}_2}) d\mu(\boldsymbol{x}) = \sum_{\boldsymbol{e}} \int_{[-1,1]^n} l_{\boldsymbol{e}}^2 L_{\boldsymbol{e}}^2 d\mu(\boldsymbol{x}) \\ &\geq \alpha^2 \prod_{i=0}^n \frac{2}{2e_i + 1} \geq \alpha^2 \frac{2^n}{2r/n + 1} \geq \alpha^2 2^n e^{2r} \end{aligned}$$

□

We will prove one more result about relation between Euclidean norm of coeffocoent vector of polynomial and L_2 norm of polynomial.

Lemma 19. *Let f be a n-variate polynomial with S monomials. Let $\boldsymbol{f} \in \mathbb{R}^S$ be the coefficient vector of f. Then we have $\|f\|_2 \leq \|f\|_\infty \geq \sqrt{S} \|\boldsymbol{f}\|_2$*

Proof. $\|f\|_2 \le \|f\|_\infty$ is easy. We will prove second inequality. Let $f = \sum_M c_M M$ where M is a monomial in f, for any $v \in [-1,1]^n$

$$|f(v)| = \Big|\sum_M c_M M\Big| \le \sum_M |c_M| \le \sqrt{S}\Big(\sum_M c_M^2\Big)^{1/2} \le \sqrt{S}\|\boldsymbol{f}\|_2$$

□

Our aim in this section is to prove following theorem:

Theorem 20. *There exist absolute constant C_{CW} such that if $f : \mathbb{C}^n \to \mathbb{C}$ is homogeneous polynomial of degree r, $\|f\|_2 = 1$ and $\delta > 0$ be such that $1/\delta$ is an integer then for any $\alpha > 0$,*

$$\Pr_{\boldsymbol{v} \in G_\delta^{\mathbb{C}}}\Big[|f(\boldsymbol{v})| \le \alpha - \frac{1}{2}\delta(16nr^2)^{2n+1}\Big] \le C_{CW} \cdot r \cdot (2\alpha)^{1/r}.$$

In that direction, we first prove continuous version[6] of the theorem on reals, then we prove discrete version on reals using already proved continuous version and finaly we give the proof of above theorem. Before starting we state few defination and facts required in this section.

Definition 21 (log-concave probability measure)**.** *Probability measure[7] μ on probability space $(\mathbb{R}^n, \mathcal{B}, \mu)$ is log-concave if function $(\log \circ \mu)$ is concave. That is,*

$$\mu(\lambda A + (1-\lambda)B) \ge \mu(A)^\lambda \mu(B)^{1-\lambda}$$

where $\mathcal{B}$ is σ-algebra[8] generated by usual topology on $\mathbb{R}^n$; $A, B \in \mathcal{B}$ and $\lambda \in (0,1)$.

Fact 22. *Uniform probability measure over convex set is log concave.*

Proof. □

We use following result [CW01] without proving it here.

Theorem 23 ([CW01])**.** *There exist an absolute constant C such that if $f : \mathbb{R}^n \to \mathbb{R}$ is a polynomial of degree at most r, $0 < q < \infty$, μ is log-concave probability measure on $\mathbb{R}^n$ then*

$$\left(\int |f(v)|^{q/r} d\mu(x)\right)^{1/q} \cdot \mu(\{v : |f(v)| \le \alpha\}) \le C \cdot q \cdot \alpha^{1/r}$$

for any $\alpha \ge 0$.

Following is the continuous version of Theorem 1 on reals.

Corollary 24. *There exist an absolute constant C_{CW} such that if $f : \mathbb{R}^n \to \mathbb{R}$ is a polynomial of degree r and $\|f\|_2 = 1$, then for any $\alpha > 0$*

$$\Pr\Big[|f(v)| \le \alpha\Big] \le C_{CW} \cdot r \cdot \alpha^{1/r}$$

[6] You will understand why we call it "continuous version".

[7] Probability measure is just usual measure with $\mu(\Omega) = 1$.

[8] σ-Algebra $\mathcal{B} \subset \mathcal{P}(\mathbb{R}^n)$ is set which is closed under complementation, countable union and $\emptyset \in \mathcal{B}$.

Proof. Apply Theorem (..) for uniform measure on $[-1,1]^n$ and $q = 2r$,

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

Now the claim is trivial. □

Let $\delta > 0$ such that $1/\delta$ is an integer and $G_\delta = \{-1, -1+\delta, -1+2\delta, ..., 1-2\delta, 1-\delta\}^n \subset [-1,1)^n$. For $v \in [-1,1)^n$ we define $\underline{v}$ as $\underline{v}_i = m_i\delta$ where m_i is an integer such that $m_i\delta \leq v_i < (m_i+1)\delta$.

Lemma 25. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be the polynomial function such that $\|f\|_2 = 1$, $\delta > 0$ such that $1/\delta$ is an integer then $|f(\boldsymbol{v}) - f(\underline{\boldsymbol{v}})| \leq \delta \cdot (8nr^2)^{n+1}$.*

Proof. By mean value theorem there exist point $\mathbf{w}$ on line segment joining $\mathbf{v}$ and $\underline{\mathbf{v}}$ and if $f'(\mathbf{w})$ denote derivative of f at $\mathbf{w}$ in the direction of $v - \underline{v}$ then

$$\begin{aligned}
|f(\mathbf{v}) - f(\underline{\mathbf{v}})| &= \|\mathbf{v} - \underline{\mathbf{v}}\| \cdot f'(\mathbf{w}) \\
&\leq \|\mathbf{v} - \underline{\mathbf{v}}\| \cdot 2r^2 \cdot \|f\|_\infty && \text{(By Multivariate Markov Inequality.)} \\
&\leq \|\mathbf{v} - \underline{\mathbf{v}}\| \cdot 2r^2 \cdot \|f\|_2 \cdot 2^{n+1} \cdot \frac{1}{\left(vol(n, \frac{1}{4r^2})\right)^{1/2}} && \text{(By Lemma (..))}
\end{aligned}$$

We have that $\|\mathbf{v} - \underline{\mathbf{v}}\| \leq \delta\sqrt{n}$ and since cube of side $\sqrt{2}R$ can be inscribed in ball of radius R $vol(n, \frac{1}{4r^2}) \geq \left(\frac{1}{2\sqrt{2}r^2}\right)^n \geq \left(\frac{1}{2\sqrt{2}nr^2}\right)^n$.

$$|f(\mathbf{v}) - f(\underline{\mathbf{v}})| \leq \delta\sqrt{n} \cdot 2r^2 \cdot \|f\|_2 \cdot 2^{n+1} \cdot (2\sqrt{2}nr^2)^{n/2} \leq \delta \cdot (8nr^2)^{n+1} \cdot \|f\|_2.$$

□

Corollary 26. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be such that $\|f\|_2 = 1$, $\delta > 0$ such that $1/\delta$ is an integer and $\boldsymbol{v} \in [-1,1]^n$ such that $|f(\boldsymbol{v})| > \alpha$ for some $\alpha > 0$. Then $|f(\underline{\boldsymbol{v}})| > \alpha - \delta \cdot (8nr^2)^{n+1}$.*

Proof.

$$\alpha < |f(\mathbf{v})| \leq |f(\mathbf{v}) - f(\underline{\mathbf{v}})| + |f(\underline{\mathbf{v}})| \leq \delta \cdot (8nr^2)^{n+1} + |f(\underline{\mathbf{v}})|$$

□

Theorem 27. *Let $f : \mathbb{R}^n \to \mathbb{R}$ be the polynomial function such that $\|f\|_2 = 1$, $\delta > 0$ such that $1/\delta$ is an integer then for any $\alpha > 0$*

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

Where C_{CW} is the constant guaranteed in Corollary 5.

Proof. Let $\mathbf{v} \in_u [-1,1]^n$, by Corollary 5,

$$\Pr\left[|f(\mathbf{v})| > \alpha \right] > 1 - C_{CW} \cdot r \cdot \alpha^{1/r}.$$

By corollary 7,

$$\Pr\left[|f(\underline{\mathbf{v}})| > \alpha - \delta(8nr^2)^{n+1} \textit{ given } |f(\mathbf{v})| > \alpha \right] = 1.$$

Thus we have,

$$\Pr\left[|f(\underline{\mathbf{v}})| > \alpha - \delta(8nr^2)^{n+1} \right] = 1 - C_{CW} \cdot r \cdot \alpha^{1/r}.$$

.

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

□

Next we give proof of Theorem 1. Let $f : \mathbb{C}^n \to \mathbb{C}$ be a polynomial of degree r. $\Re(f), \Im(f) : \mathbb{R}^{2n} \to \mathbb{R}$ be the real and imaginary parts of f, that is $f(\mathbf{a} + \iota\mathbf{b}) = \Re(f)(\mathbf{a}, \mathbf{b}) + \iota\Im(f)(\mathbf{a}, \mathbf{b})$. Note that $\Re(f)$ and $\Im(f)$ are polynomials of degree r. We define $\|f\|_2 := \|\Re(f)\|_2 + \|\Im(f)\|_2$.

Proof of Theorem 1. Since $\|f\|_2 = 1$, either $\|\Re(f)\|_2 \geq 1/2$ or $\|\Im(f)\|_2 \geq 1/2$. Assume w.l.o.g $\|\Re(f)\| \geq 1/2$. By applying Theorem 8 to $\Re(f)$ and α',

$$\Pr \left[|\Re(f)(\mathbf{a}, \mathbf{b})| > \left(\alpha' - \delta \cdot (8(2n)r^2)^{2n+1}\right) \cdot \|\Re(f)\|_2 \right] > 1 - C_{CW} \cdot r \cdot (\alpha')^{1/r}.$$

Note that, for any γ, $|\Re(f)(\mathbf{a}, \mathbf{b})| > \gamma$ then $|f(\mathbf{a} + \iota\mathbf{b})| > \gamma$. Using $\|\Re(f)\|_2 \geq 1/2$ and $\alpha' = 2\alpha$ we have,

$$\Pr \left[|f(\mathbf{a} + \iota\mathbf{b})| > \left(2\alpha - \delta \cdot (16nr^2)^{2n+1}\right) \cdot \frac{1}{2} \right] > 1 - C_{CW} \cdot r \cdot (2\alpha)^{1/r}.$$

$$\therefore \Pr \left[|f(\mathbf{a} + \iota\mathbf{b})| \leq \left(\alpha - \frac{1}{2} \cdot \delta \cdot (16nr^2)^{2n+1}\right) \right] \leq C_{CW} \cdot r \cdot \alpha^{1/r}.$$

□

3 Algebraic Geometry

In this section we will give basic definitions from geometry.

Definition 28 (Variety, Irreducible Variety)**.** *A subset $V \subset \mathbb{C}^n$ is called Variety, if there exists a set of polynomials $\mathcal{F} \subset \mathbb{C}[\boldsymbol{x}]$ such that $V = \{\boldsymbol{v} \in \mathbb{C}^n : \forall f \in \mathcal{F}, f(\boldsymbol{v}) = 0\}$. Varieties are closed sets and define zariski topology over $\mathbb{C}^n$. The closure of set $V \subset \mathbb{C}^n$ is intersection of all closed sets containing V. Variety 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 $V_2 = V$.*

Definition 29 (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 $\emptyset \subset V_1 \subset V_2 ... \subset V_m \subset V$. The dimension of a reducible variety is the maximal dimension of its irreducible components.*

Definition 30 (Degree)**.** *Let $A \subset \mathbb{C}^n$ is an affine linear space. The degree of an irreducible variety $V \subset \mathbb{C}^n$ is*

$$deg(V) = \max_A \{|V \cap A| : |V \cap A| < \infty\}.$$

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 use following result proved in [HS80b].

Theorem 31 (Variety of easy polynomials)**.** *For every natural number n, s, r there exists a set $W(n,s,r) \subset \mathbb{C}^N$ which contains the coefficient vectors of all n-variate homogeneous polynomials $f \in \mathbb{C}[\boldsymbol{x}]$ of degree r that can be computed by n-variate homogeneous circuits of size s and degree r. Further,*

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

and

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

.

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 $\mathcal{O}(sr^4)$ 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[9].

Corollary 32 (Variety of projections of universal circuit)**.** *For every natural number n, s, r there exists a set $V(n,s,r) \subset \mathbb{C}^N$ which contains the coefficient vectors of all n-variate homogeneous polynomials of degree r that can be computed by universal circuit for n-variate homogeneous circuits of size s and degree r. Further there exist constant c such that,*

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

and

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

.

As varieties are closed, the same variety also contains all coefficient vectors of polynomials that are limits of easy polynomials.

Definition 33 (Closure of easy polynomials)**.** *A homogeneous polynomial $f \in \mathbb{C}[\boldsymbol{x}]$ is in the closure of size s and degree r algebraic circuits if there exists a sequence of n-variate, degree r, homogeneous polynomials $\{f_i(\boldsymbol{x})\}$, 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.*

Next we define notion that will be helpful in upcoming proofs.

Definition 34 (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*

$$dim(V \cap A) \leq dim(V) - codim(A).$$

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.

[9] This can be seen from the proof of existence of universal circuits.

Lemma 35. *Let V is axis-parallel random then for every axis-parallel affine subspace A, $V \cap A$ is also axis-parallel random.*

Proof. Proof is very easy from definition. □

Next result state 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 36. *Let $\delta > 0$ 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_{ij} is chosen independently uniformly at random from $[0, \delta]$. Let $V \subset \mathbb{C}^N$ be a variety of dimension d. Then $T(V)$ with probability 1 $T(V)$ is axis-parallel random.*

3.1 ϵ-Net for Variety

Definition 37 (ϵ-Net)**.** *Let $V \subset \mathbb{C}^N$. A set $E \subset V$ is an ϵ-net for V if for every $\boldsymbol{v} \in V$ there exists $\boldsymbol{e} \in E$ such that $\|\boldsymbol{e} - \boldsymbol{v}\| \leq \epsilon$.*

Theorem 38 (ϵ-Net for Axis-parllel Random Varieties)**.** *Let $N \geq 2$ and $V \subset \mathbb{C}^N$ be a d-dimentional axis-parallel random variety of degree D and $d < \sqrt{N}$. Denote $\hat{V} \subset V \cap [-1, 1]^N_{\mathbb{C}}$. Then, for $\epsilon > 0$, there exist ϵ-net $E \subset \hat{V}$ such that $|E| \leq D(1750N^3/\epsilon^2)^{d+1}$*

Proof. We prove claim by induction on dimension of variety. If $d = 0$ then $|\hat{V}| \leq D$ and claim is trivial since for any $\epsilon > 0$ we take $E := \hat{V}$.

For $d > 0$, idea of proof is following: For some $\eta > 0$, we construct η grid[10] in $[-1, 1]^N_{\mathbb{C}}$. We need $1/\eta$ to be an integer[11] so that we get all cuboids of side η. Next, for some $\delta > 0$ and for each hyperplane contributing to the grid, we apply induction hypothesis to get δ-net[12] for the part of variety in the hyperplane. Union of all such δ-nets produced will be our almost ϵ-net for some particular values of δ and η. Finally we calculate the values of δ and η and prove the bound on size of ϵ-net.

Assume $d > 0$. Let $\alpha \in \mathbb{C}$, $1 \leq i \leq N$, define

$$H_i(\alpha) := \{\boldsymbol{v} \in \mathbb{C}^N : v_i = \alpha\}.$$
$$\hat{V}_i(\alpha) := H_i(\alpha) \cap \hat{V}.$$

$H_i(\alpha)$ is hyperplane obtained by fixing i^{th} coordinate and $\hat{V}_i(\alpha)$ is part of $\hat{V}$ which is in $H_i(\alpha)$. Note that since V is axis-parallel random, for any $\alpha \in \mathbb{C}$, dimention of $\hat{V}_i(\alpha)$ is $d - 1$, degree at most D and is axis-parallel random[13]. By induction hypothesis there is a δ-net $E_i(\alpha) \subset \hat{V}_i(\alpha)$ such that $|E_i(\alpha)| \leq D(1750N^3/\delta^2)^d$ for $\delta > 0$. Let η be the constant such that $1/\eta$ is integer. Let

$$E' = \bigcup_{i \in [N], a, b \in \{-1, -1+\eta, \ldots, 1-\eta, 1\}} E_i(a + \iota b)$$

Using induction hypothesis and fact that we are working in $\mathbb{C}^N$, we get

$$|E'| \leq N \cdot (2/\eta + 1)^2 \cdot D(1750N^3/\delta^2)^d$$

[10] Here we mean η-grid in $[-1, 1]^{2N}_{\mathbb{R}}$

[11] Strictly speaking this is not required to prove the claim but this will make out life little easier.

[12] Ideally we would like to use ϵ-net but calculations doesent allow it.

[13] This needs proof

Let

$$H = \bigcup_{i\in[N],a,b\in\{-1,-1+\eta,\ldots,1-\eta,1\}} H_i(a+\iota b)$$

Consider set $[-1,1]^N\backslash H$. This set is unoin of open -walls are removed- cuboids of side lenght η. Any irreducible component of $\hat{V}$ will either completely inside of a cuboid or intersect the wall of it or disjoint from it. Consider the set of components, each one of which is completely inside of one cuboid[14], we pick any one point from each of them. Let B be the set of such points. Since there are at most D components[15], we can have at most D such points, thus $|B| \leq D$. Define $E := E' \cup B$. We claim that for

$$\delta = \epsilon\Big(1 - \frac{1}{\sqrt{2N}}\Big), \quad \eta = \frac{1}{\lceil\frac{2N}{\epsilon}\rceil}$$

E is ϵ-net of $\hat{V}$. For any $\boldsymbol{v} \in \hat{V}$, if the component containing $\boldsymbol{v}$ intersects wall of some cuboid and let $\boldsymbol{u}$ be the point in intersection, then there is $\boldsymbol{e} \in E'$ such that $\|\boldsymbol{e}-\boldsymbol{u}\| \leq \delta$ and hence $\|\boldsymbol{e}-\boldsymbol{v}\| \leq \delta + \sqrt{2N}\eta \leq \epsilon$. If component containing $\boldsymbol{v}$ is completely contained in one of the cuboid then there is $\boldsymbol{e} \in B$ such that $\|\boldsymbol{e}-\boldsymbol{v}\| \leq \sqrt{2N}\eta \leq \epsilon$. Hence E is ϵ-net for $\hat{V}$.

We now prove that size of E is as expected.

$$\begin{aligned}
|E| &\leq N\Big(\frac{2}{\eta}+1\Big)^2 D\Big(\frac{1750N^3}{\delta^2}\Big)^d + D \\
&= N\Big(2\Big\lceil\frac{2N}{\epsilon}\Big\rceil+1\Big)^2 D\Big(\frac{1750N^3}{\epsilon^2}\big(1-\frac{1}{\sqrt{2N}}\big)^{-2}\Big)^d + D \\
&\leq N\Big(\frac{5N}{\epsilon}\Big)^2 D\Big(\frac{1750N^3}{\epsilon^2}\Big)^d \cdot \Big(1+\frac{3\sqrt{2}}{\sqrt{N}}\Big)^d + D && (\because N \geq 2) \\
&\leq \left(\Big(\frac{25N^3}{\epsilon^2}\Big)\Big(\frac{1750N^3}{\epsilon^2}\Big)^d \cdot e^{3\sqrt{2}} + 1\right) D && (\because d < \sqrt{N}) \\
&\leq D\Big(\frac{1750N^3}{\epsilon^2}\Big)^{d+1}
\end{aligned}$$

Here we used the fact that $(1+3\sqrt{2}/\sqrt{N})^d < 69.6$ and $N \geq 2$. □

We will now prove that if $V' = T(V)$ be the axis-parallel random variety, where $T = I + A$ and $A_{ij} \in [0,\delta]$ for some $\delta > 0$, for any $\epsilon > 0$ there is $\epsilon' > 0$ such that if E' is ϵ'-net for V' then we can get an ϵ-net for V. Before starting the proof of claim, we will state definitions and useful lemmas required in it.

Definition 39 (Operator Norm)**.** *Operator norm of linear operator A over normed space V is defined as*

$$\|A\|_{op} := \sup_{\boldsymbol{x}\in V} \frac{\|A\boldsymbol{x}\|}{\|\boldsymbol{x}\|}$$

.

Lemma 40. *Let A be the linear operator on $\mathbb{C}^n$ such that for $1 \leq i,j \leq n$, we have that $A_{ij} \in [0,\delta]$ for some $\delta > 0$. Then operator norm of A is at most $n\delta$.*

[14]Note that these are the components which are not covered by E'.

[15]this needs a proof

Proof. Let $\boldsymbol{x} \in \mathbb{C}^n$,

$$\|A\boldsymbol{x}\| = \sqrt{\sum_{i=1}^{n}\left(\Big|\sum_{j=1}^{n} A_{ij}x_j\Big|\right)^2} \leq \sqrt{\sum_{i=1}^{n}\left(\sum_{j=1}^{n}|A_{ij}||x_j|\right)^2} \leq \sqrt{\sum_{i=1}^{n}\left(\sum_{j=1}^{n}\delta|x_j|\right)^2}$$
$$\leq \delta\sqrt{n}\sum_{j=1}^{n}|x_j| \leq n\delta \cdot \|\boldsymbol{x}\|$$

□

Lemma 41 (Geometric Series of Matrices)**.** *Let A be a $n \times n$ matrix such that $\lim_{k\to\infty} A^k = 0$ and $I - A$ is invertible. Then*

$$\sum_{k=0}^{\infty} A^k = (I - A)^{-1}.$$

Using that show that if $T = I + B$ is an invertible transformation where B is the $n \times n$ matrix such that $B_{ij} \in [0, \delta]$ for $1 \leq i, j \leq n$ and $\delta \leq n^{-2}$, then

$$T^{-1} = I + \sum_{k=1}^{\infty}(-B)^k$$

.

Proof. Let $S_m = \sum_{k=0}^{m} A^k$ be the sequence of partial sums then note that $S_m - AS_m = I - A^{m+1}$ which implies $\lim_{m\to\infty}(S_m - AS_m) = I$ since $\lim_{k\to\infty} A^k = 0$. Thus S_m converges to $(I - A)^{-1}$.

For the second part note that

$$-\frac{1}{n^{k+1}} = -\frac{n^{k-1}}{n^{2k}} \leq -\delta^k n^{k-1} \leq (-B)^k_{ij} \leq \delta^k n^{k-1} \leq \frac{n^{k-1}}{n^{2k}} = \frac{1}{n^{k+1}}$$

Since sequences $1/n^{k+1}$ and $-1/n^{k+1}$ converges to 0 for $n \geq 2$, we have that $\lim_{k\to\infty}(-B)^k_{ij} = 0$. Hence $\lim_{k\to\infty}(-B)^k = 0$. Therefore

$$T^{-1} = (I - (-B))^{-1} = \sum_{k=0}^{\infty}(-B)^k = I + \sum_{k=1}^{\infty}(-B)^k$$

. □

Now we are ready to prove Theorem 1 even if variety is not axis-parallel random. Note that if $V = V(\mathcal{F})$ for $\mathcal{F} \subset \mathbb{C}[\boldsymbol{x}]$, then $V' = V(\mathcal{F} \circ T^{-1})$. Since $\boldsymbol{v}' \in V'$ iff for all $f \in \mathcal{F}, f \circ T^{-1}(\boldsymbol{v}') = 0$.

Theorem 42 (ϵ-Net for Varieties)**.** *Let $N \geq 2$ and $V' = T(V) \subset \mathbb{C}^N$ be the variety of dimension $d \geq 1$, where $T = I + A$ and $A_{ij} \in [0, N^{-2d}]$ for $1 \leq i, j \leq N$. If E' is an ϵ'-net of $V' \cap [-1, 1]^N_{\mathbb{C}}$ then $E = T^{-1}(E')$ is ϵ-net for $V \cap [-(1 - N^{-1}), (1 - N^{-1})]$ where $\epsilon = (1 + N^{-1})\epsilon'$.*

Proof. The operator norm of A is $\|A\|_{op} \leq N^{1-2d} \leq 1/N < 1$, since $N \geq 2$ and $A_{ij} \in [0, N^{-2d}]$. This implies,

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

Where $[-(1-\frac{1}{N}),(1-\frac{1}{N})]^N_{\mathbb{C}} = [-(1-\frac{1}{N}),(1-\frac{1}{N})]^N + i[-(1-\frac{1}{N}),(1-\frac{1}{N})]^N$. Above containment holds because, for any $\boldsymbol{v} \in [-(1-1/N),(1-1/N)]^N_{\mathbb{C}}$ which is in the direction of basis vector, $\|T(\boldsymbol{v})\| \le \|\boldsymbol{v}\| + \|A\|_{op}\|\boldsymbol{v}\| \le 1$. Hence it hold for any vector in that box.

Let $T^{-1} = I + B$ then $B = \sum_{k=1}^{\infty}(-A)^k$. If k is even $(-A)^k_{ij} \le N^{k-1}/N^{2dk}$, and if k is odd $(-A)^k_{ij} \le 0$, thus we have,

$$|B_{ij}| = \Big|\sum_{k=1}^{\infty}(-A)^k_{ij}\Big| \le \Big|\sum_{k=1}^{\infty}\frac{N^{2k-1}}{N^{4dk}}\Big| = \frac{N}{N^{4d}-N^2}$$

Thus $\|B\|_{op} \le 1/(N^{4d-2}-1) \le 1/N$.

Let $\boldsymbol{u} \in V \cap [-(1-\frac{1}{N}),(1-\frac{1}{N})]^N_{\mathbb{C}}$, then

$$T(\boldsymbol{u}) \in T(V) \cap T\left(\Big[-(1-\frac{1}{N}),(1-\frac{1}{N})\Big]^N_{\mathbb{C}}\right) \subset V' \cap [-1,1]^N_{\mathbb{C}}$$

Therefore there is $\boldsymbol{e}' \in E'$ such that $\|\boldsymbol{e}' - T(\boldsymbol{u})\| \le \epsilon'$. Hence we have

$$\|T^{-1}(\boldsymbol{e}') - \boldsymbol{u}\| = \|T^{-1}(\boldsymbol{e}' - T(\boldsymbol{u}))\| \le \|T^{-1}\|_{op} \cdot \|\boldsymbol{e}' - T(\boldsymbol{u})\| \le (1+1/N)\epsilon'.$$

□

Theorem 43 (ϵ-Net for Varieties)**.** *Let $V \subset \mathbb{C}^N$ be the variety of dimension d, $\hat{V} = V \cap [-(1-\frac{1}{N}),(1-\frac{1}{N})]$. Then for any $\epsilon > 0$, there exist ϵ-net $E \subset \hat{V}$ such that $|E| \le D(15750N^6/\epsilon^2)^{d+1}$.*

Proof. Since $d < \sqrt{N^2+1} \le \sqrt{2N^2}$, we work in space $\mathbb{C}^{2N^2}$ and think of our space $\mathbb{C}^N$ as subspace of $\mathbb{C}^{2N^2}$. Now we apply T to make our variety axis-parallel random and we invoke Theorem 1 above to get ϵ'-net E' for $T(V) \cap [-1,1]^{2N^2}_{\mathbb{C}}$. We have that $|E'| \le D(14000N^6/\epsilon'^2)^{d+1}$. By above theorem, we have that $E = T^{-1}(E')$ is $\epsilon'\Big(1+\frac{1}{2N^2}\Big)$-net for

$$V \cap \Big[-(1-\frac{1}{2N^2}),(1-\frac{1}{2N^2})\Big]^{2N^2}_{\mathbb{C}} \supset V \cap \Big[-(1-\frac{1}{N}),(1-\frac{1}{N})\Big]^{2N^2}_{\mathbb{C}} = V \cap \Big[-(1-\frac{1}{N}),(1-\frac{1}{N})\Big]^{N}_{\mathbb{C}}$$

Substituting $\epsilon' = \epsilon \cdot (1+\frac{1}{2N^2})^{-1}$, we get ϵ-net E of size $|E| \le D(15750N^6/\epsilon^2)^{d+1}$ for $N \ge 2$. □

4 Robust Hitting Set

Definition 44 (η-Robust Hitting Set)**.** *A subset $\mathcal{H} \subset \mathbb{C}^n$ is an η-robust hitting set of $\mathcal{F} \subset \mathbb{C}[\boldsymbol{x}]$, if for every $f \in \mathcal{F}$, there is $\boldsymbol{v} \in \mathcal{H}$ such that $f(\boldsymbol{v}) \ge \eta \cdot \|f\|_2$.*

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

Theorem 45. *If finite $\mathcal{H}$ is η-robust hitting set for $\mathcal{F} \subset \mathbb{C}[\boldsymbol{x}]$ then it is η-robust hitting set for closure*[16] *of $\mathcal{F}$.*

[16] In Euclidean topology

Proof. Let f is in closure of $\mathcal{F}$. If f is not a limit point of $\mathcal{F}$ then $f \in \mathcal{F}$ and claim hold. If f is limit point of $\mathcal{F}$ then there is sequence $\{f_n\}$ in $\mathcal{F}$ such that $\lim_{n\to\infty} f_n = f$. Since $\mathcal{H}$ is finite and for every f_n there is $\boldsymbol{v} \in \mathcal{H}$ such that $|f_n(\boldsymbol{v})| \geq \eta \cdot \|f_n\|_2$ for all n, there is a subsequence f_{n_i} such that there is $\boldsymbol{v}_0 \in \mathcal{H}$ for all f_{n_i} such that $|f_{n_i}(\boldsymbol{v}_0)| \geq \eta \cdot \|f_{n_i}\|_2$ and converges to f. Using $\lim_{i\to\infty} \|f_{n_i}\|_2 = \|f\|_2$[17] and $\lim_{i\to\infty} |f_{n_i}(\boldsymbol{v}_0)| = |f(\boldsymbol{v}_0)|$ we get $|f(\boldsymbol{v}_0)| \geq \eta \cdot \|f\|_2$. Thus $\boldsymbol{v}_0 \in \mathcal{H}$ hits f. □

Corollary 46. *If $\mathcal{H} \subset \mathbb{C}^n$ is η-robust hitting set for size s and degree r then it is η-robust hitting set for $V(n, s, r)$.*

Proof. $V(n, s, r)$ is closure of a set which contain coefficient vectors of all n-variate polynomials of degree r that can be computed by size s circuits. Claim is trivial using above theorem. □

Next we prove if we have hitting set for ϵ-net of a variety then we can get hitting set for the complete variety.

Lemma 47. *Let $E \subset V \subset [-1, 1]_{\mathbb{C}}^{N_{n,r}^{hom}}$ is an ϵ-net for variety V and $\mathcal{H}$ is η-robust hitting set for the polynomials whose coefficient vectors in E and $\eta < 1$. Also V is such that, if $\boldsymbol{f} \in V$ then $\alpha \boldsymbol{f} \in V$, for all α. Further $\eta, \epsilon, N_{n,r}^{hom}$ and r satisfy*

$$\epsilon \cdot \sqrt{2N_{2n,r}^{hom}} < \frac{1}{8}\eta \cdot 2^n \cdot e^{-r} \tag{A1}$$

then $\mathcal{H}$ is $\eta/4$-robust hitting set for V.

Proof. Let $\boldsymbol{f} \in V$. Assume w.l.o.g maximal coefficient of f is[18] 1/2. Let $\boldsymbol{g} \in E$ such that $\|\boldsymbol{f} - \boldsymbol{g}\|_2 \leq \epsilon$. By Lemma 2.9,

$$\|\Re(f) - \Re(g)\|_\infty, \|\Im(f) - \Im(g)\|_\infty \leq \|\boldsymbol{f} - \boldsymbol{g}\|_2 \cdot \sqrt{N_{2n,r}^{hom}}$$

Thus

$$\begin{aligned}\|f - g\|_\infty &= \max_{\boldsymbol{v}\in[-1,1]^n} |(f - g)(\boldsymbol{v})| = \max_{\boldsymbol{v}\in[-1,1]^n} |(\Re(f) - \Re(g))(\boldsymbol{v}) + \iota(\Im(f) - \Im(g))(\boldsymbol{v})| \\ &\leq \sqrt{2} \cdot \|\boldsymbol{f} - \boldsymbol{g}\|_2 \cdot \sqrt{N_{2n,r}^{hom}} \leq \sqrt{2} \cdot \epsilon \cdot \sqrt{N_{2n,r}^{hom}}\end{aligned}$$

Since maximal coefficient of f is $1/2$ and $\|\boldsymbol{f} - \boldsymbol{g}\|_2 \leq \epsilon$ one of the coefficient of g is at least $\frac{1}{2} - \epsilon$. Hence for $\epsilon < \frac{1}{10}$, one of the coefficient of g, and hence[19] $\Re(g)$, is at least $\frac{2}{5} \geq \frac{1}{4}$.

$$\begin{aligned}|f(\boldsymbol{v})| &\geq |g(\boldsymbol{v})| - |(f - g)(\boldsymbol{v})| \geq |g(\boldsymbol{v})| - \|f - g\|_\infty \geq \eta \cdot \|g\|_2 - \sqrt{2N_{2n,r}^{hom}} \cdot \epsilon \\ &\geq \eta \cdot \|g\|_2 - \frac{1}{8} \cdot \eta \cdot 2^n \cdot e^{-r} && \text{(From A1 in Theorem statement)} \\ &\geq \frac{1}{2}\eta \cdot \|g\|_2 && \text{(By Lemma 2.7, } \|g\|_2 \geq \|\Re(g)\|_2 \geq \tfrac{1}{4} \cdot 2^n \cdot e^{-r}\text{)} \\ &\geq \frac{1}{4}\eta \cdot \|f\|_2\end{aligned}$$

[17] Prove if sequence of functions converges then sequence of their norm converges.
[18] This can be easily obtained by multiplying f by a field element
[19] This needs proof

Last inequality follows since[20],

$$\begin{aligned}\|f\|_2 &\le \|g\|_2 + \|f-g\|_2 = \|g\|_2 + \|\Re(f-g)\|_2 + \|\Im(f-g)\|_2 \\ &\le \|g\|_2 + \|\Re(f-g)\|_\infty + \|\Im(f-g)\|_\infty \\ &\le \|g\|_2 + 2\epsilon \cdot \sqrt{N^{hom}_{2n,r}} \le \|g\|_2 + \sqrt{2}\cdot\frac{1}{8}\eta\cdot 2^n \cdot e^{-r} \\ &\le \|g\|_2 + \frac{\eta}{\sqrt{2}}\cdot\|g\|_2 \le 2\cdot\|g\|_2\end{aligned}$$

□

Next we prove that, for our variety there is η-robust hitting set.

Theorem 48. *Let $V \subset [-1,1]^N_{\mathbb{C}}$ be a variety of degree D and dimension d and satisfy assumptions in above theorem. Let $\eta = 2^{-n}\cdot\frac{1}{2\cdot(C_{CW}\cdot r\cdot n)^r}$ and $\delta = \frac{\eta}{(16nr^2)^{n+1}}$. There exist $\eta/4$-robust hitting set $\mathcal{H} \subset G^{\mathbb{C}}_\delta$ for V of size*

$$|\mathcal{H}| = \max\{2r\log D, 76r^2d(n+r)\}$$

Proof. Let k = , Sample k points $\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, ...\boldsymbol{v}_k$ from $G^{\mathbb{C}}_\delta$ uniformly and independently at random. Let $\mathcal{H} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, ...\boldsymbol{v}_k\}$.
Let $\epsilon = (\frac{1}{N})^r$ and $E \subset V \cap [-(1-\frac{1}{N}),(1-\frac{1}{N})]^N_{\mathbb{C}}$ be the ϵ-net gauranteed by theorem (..). For $\alpha = \eta\cdot\|g\|_2$, it follows from Theorem 3.6 and union bound that the probability that there exist g such that for all $1 \le i \le k$,

$$\frac{g(\boldsymbol{v}_i)}{\|g\|_2} \le \eta - \frac{1}{2}\delta\cdot(16nr^2)^{2n+1} = \frac{\eta}{2}$$

is at most

$$\begin{aligned}(C_{CW}\cdot r\cdot(2\eta)^{1/r})^k\cdot|E| &\le (C_{CW}\cdot r\cdot(2\eta)^{1/r})^k\cdot D\cdot\Big(\frac{15750N^3}{\epsilon^2}\Big)^{d+1} \\ &< 2^{-nk/r}\cdot n^{-k}\cdot D\cdot(N^{14}\cdot N^3\cdot N^{2r})^{d+1} \\ &= 2^{-nk/r}\cdot n^{-k}\cdot D\cdot N^{38rd} \\ &= 2^{-nk/r}\cdot n^{-k}\cdot D\cdot\binom{n+r-1}{r}^{38rd} \\ &< 2^{-nk/r}\cdot n^{-k}\cdot D\cdot 2^{38rd(n+r)}\end{aligned}$$

If $2r\log D \ge 76r^2d(n+r)$ then $k = 2r\log D$, hence above inequality will be,

$$= \frac{D\cdot 2^{38rd(n+r)}}{2^{2n\log D}\cdot n^{2r\log D}} = \frac{D}{D^{2n-1}}\cdot\frac{2^{38rd(n+r)}}{2^{\log D}}\cdot\frac{1}{n^{2r\log D}} \le 1.$$

Otherwise $k = 76r^2d(n+r)$, hence above inequality will be,

$$= \frac{D\cdot 2^{38rd(n+r)}}{2^{76nrd(n+r)}\cdot n^{76r^2d(n+r)}} = \frac{D}{2^{38(2n-1)rd(n+r)}}\cdot\frac{1}{n^{76r^2d(n+r)}} \le 1.$$

□

Corollary 49. *There exist a constant c such that for every integer n, s, r for $\eta = 2^{-n}\cdot\frac{1}{2\cdot(C_{CW}\cdot n\cdot r)^r}$ and $\delta = \frac{\eta}{(16nr^2)^{2n+1}}$, there is $\eta/4$-robust hitting set $\mathcal{H} \subset G^{\mathbb{C}}_\delta$ for $V(n,s,r)$ of size $|\mathcal{H}| \le (nsr)^c$.*

[20] Minkowski Inequality needs proof

Proof. Proof is immediate from the above theorem and the fact that degree of $V(n,s,r)$ is bounded by $2^{(nsr)^{c_1}}$ for some c_1. □

Note that we have proved existence of robust hitting set in $\mathbb{C}^n$, next we will prove existence in $\mathbb{R}^n$.

Theorem 50. *Let $\mathcal{H} \subset \mathbb{C}^n$ be the η-robust hitting set for $V(n,s,r)$. Prove that there exist $\mathcal{H}_{\mathbb{R}} \subset \mathbb{R}^n$, such that $\mathcal{H}_{\mathbb{R}}$ is a $\frac{\eta}{(r+2)!}$-robust hitting set for $V(n,s,r)$. Also prove that $|\mathcal{H}_{\mathbb{R}}| = r \cdot |\mathcal{H}|$.*

Proof. Define set $\mathcal{H}_{\mathbb{R}}$ as,

$$\mathcal{H}_{\mathbb{R}} = \{\boldsymbol{x} + k\boldsymbol{y} : k \in \{0,1,2,...,r\} \text{ and } \boldsymbol{x} + \iota\boldsymbol{y} \in \mathcal{H}\}.$$

Note that $|\mathcal{H}_{\mathbb{R}}| = r \cdot |\mathcal{H}|$. To prove $\mathcal{H}_{\mathbb{R}}$ is an $\frac{\eta}{(r+2)!}$-robust hitting set, we first prove it is hitting set and then we prove it is robust hitting set for $V(n,s,r)$.

The fact that $\mathcal{H}_{\mathbb{R}}$ hits each polynomial in $V(n,s,r)$ is easy. Let $f \in V(n,s,r)$ and $\boldsymbol{v} = \boldsymbol{a} + \iota\boldsymbol{b} \in \mathcal{H}$ be such that $f(\boldsymbol{v}) \neq 0$. Let $f_v(z) = \boldsymbol{a} + z\boldsymbol{b}$ be the univariate restriction of f to one dimensional complex affine space defined by $\boldsymbol{a} + z\boldsymbol{b}$. f_v is not identical to zero polynomial since $f_v(\iota) = f(\boldsymbol{a} + \iota\boldsymbol{b}) \neq 0$ and hence by fundamental theorem of algebra f_v can have at most r roots. Which implies at least at one point in $\{\boldsymbol{a} + k\boldsymbol{b} : k \in \{0,1,2,...,r\}\}$ f_v evaluates nonzero. Hence $\mathcal{H}_{\mathbb{R}}$ hits f at that point.

By using interpolation formula,

$$f_v(\iota) = \sum_{k=0}^{r} c_k \cdot f_v(k)$$

Where

$$c_k = \prod_{l=0, l\neq k}^{r} \frac{(\iota - l)}{(k - l)}$$

Hence $|c_k| \leq (r+1)!$. Since $|f(\boldsymbol{v})| \geq \eta \cdot \|f\|_2$, we have that

$$\begin{aligned}
\eta \cdot \|f\|_2 \leq |f(\boldsymbol{v})| = |f_v(\iota)| &= \Big| \sum_{k=0}^{r} c_k \cdot f_v(k) \Big| \\
&= \Big| \sum_{k=0}^{r} f(\boldsymbol{a} + k\boldsymbol{b}) \Big| \\
&\leq (r+1) \cdot \max_k |c_k| \cdot \max_k |f(\boldsymbol{a} + k\boldsymbol{b})| \\
&\leq (r+2)! \cdot \max_k |f(\boldsymbol{a} + k\boldsymbol{b})|
\end{aligned}$$

□

We denote $G_{\delta,r} := \{\boldsymbol{x} + k\boldsymbol{y} : 0 \leq k \leq r, \boldsymbol{x} + \iota\boldsymbol{y} \in G_{\delta}^{\mathbb{C}}\}$

Corollary 51. *There exist a constant c such that for every integer n, s, r for $\eta = 2^{-n} \cdot \frac{1}{20 \cdot (C_{CW} \cdot n \cdot r^2)^r}$ and $\delta = \frac{\eta}{(16nr^2)^{2n+1}}$, there is $\eta/4$-robust hitting set $\mathcal{H} \subset G_{\delta,r}$ for $V(n,s,r)$ of size $|\mathcal{H}| \leq (nsr)^c$.*

Proof. Observe that $(r+2)! < 10r^r$, claim is trivial from theorem (..) and theorem (..) □

5 Existential Theory of Reals

We will need the following theorem regarding the decidability of existential formulas over the reals. Formulas are constructed as follows. The atoms are polynomial equalities "$f(\boldsymbol{x}) = 0$" or inequalities "$f(\boldsymbol{x}) \geq 0$". 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 $\exists$. For a set of polynomials $\mathcal{F} \subset \mathbb{R}[\boldsymbol{x}]$, an $\mathcal{F}$-formula is a formula in which all the polynomials appearing in the atoms are from $\mathcal{F}$.

Theorem 52 (Existential theory of reals is in PSPACE)**.** *Let $\mathcal{F} \subset \mathbb{R}[\boldsymbol{x}]$ be a set of poly(n) polynomials each of degree at most $r =$ poly(n) and let $\exists \boldsymbol{x} F(\boldsymbol{x})$ be a sentence where $F(\boldsymbol{x})$ 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.*

We denote by Ψ the universal circuit for n-variate homogeneous circuits of size s and degree r.

Let $m = |\mathcal{H}|$. Let $\mathcal{H} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, ..., \boldsymbol{v}_m\} \subset G_{\delta,r}$ be the potential candidate. $\mathcal{H}$ is η-robust hitting set iff

$$\forall \boldsymbol{a} \left[\psi(\boldsymbol{a}, 1) \implies \phi(\boldsymbol{a}, \eta c) \right]$$

or in other words $\mathcal{H}$ is not η-robust hitting set if

$$\exists \boldsymbol{a} \left[\psi(\boldsymbol{a}, 1) \ \wedge \ \neg \phi(\boldsymbol{a}, \eta c) \right]$$

Where c is constant for given n, s, r and

$$\phi(\boldsymbol{a}, \epsilon) = \exists i \in [m] \left[|\Psi(\boldsymbol{v}_i, \boldsymbol{a})| \geq \epsilon \right]$$

$$\psi(\boldsymbol{a}, 1) = \exists \boldsymbol{v} \in [-1, 1]^n \left[|\Psi(\boldsymbol{v}, \boldsymbol{a})| \geq 1 \right]$$

We will find the value of c. Next lemma shows existence of formula ϕ.

Lemma 53. *Let n, s, r be natural numbers and $\epsilon > 0$ be a rational number with poly(n) bit complexity. For real vectors $\boldsymbol{v}, \boldsymbol{a}$ there exists an existential sentence over the reals, $\varphi(\boldsymbol{v}, \boldsymbol{a}, \epsilon)$, such that $\varphi(\boldsymbol{a}, \boldsymbol{v}, \epsilon)$ is true iff the polynomial computed by the universal circuit for size s and degree r, whose auxiliary variables are set to $\boldsymbol{a}$, evaluates on input $\boldsymbol{v}$, in absolute value, to at least ϵ. That is, $|\Psi(\boldsymbol{v}, \boldsymbol{a})| \geq \epsilon$.*

Proof. For each gate u of Ψ let $\Psi_u(\boldsymbol{x}, \boldsymbol{y})$ be the polynomial computed at u. For each gate u of Ψ 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 $z_o^2 \geq \epsilon^2$ 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

$$\varphi(\boldsymbol{v}, \boldsymbol{a}, \epsilon) = \exists \boldsymbol{z} \bigwedge_{g \in \mathcal{F}} g(\boldsymbol{z})$$

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

Corollary 54. *Let $\mathcal{H} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, ..., \boldsymbol{v}_m\} \subset G_{\delta,r}$ and $|\mathcal{H}| = m$. Then there exist a sentence $\phi(\boldsymbol{a}, \epsilon)$ such that $\phi(\boldsymbol{a}, \epsilon)$ is true iff there is $\boldsymbol{v}_i \in \mathcal{H}$ such that $\varphi(\boldsymbol{v}_i, \boldsymbol{a}, \epsilon)$ is true.*

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.

Next we show existence of formula ψ.

Lemma 55. *Let $f(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]$ and $f(\boldsymbol{x}) = \Psi(\boldsymbol{x}, \boldsymbol{a})$. Given n, s, r in unary, there is a PSPACE algorithm for deciding whether there exists $\boldsymbol{v} \in [-1, 1]^n$ on which $|f(\boldsymbol{v})| \geq 1$.*

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

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

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

6 Algorithm

Input: n,s,r
$\eta = 2^{-n} \cdot \frac{1}{160 \cdot (C_{CW} \cdot n \cdot r^2)^r}$.

$c = \frac{1}{2^{n+1}} \left(vol(n, \frac{1}{4r^2}) \right)^{\frac{1}{2}}$.

$m = (nsr)^{c_2}$.

$\delta = \frac{\eta}{(16nr^2)^{2n+1}}$.

while *Robust set not found yet* **do**
  Let $\{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, ..., \boldsymbol{v}_m\} \in G_{\delta,r}$ so that $(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, ..., \boldsymbol{v}_m)$ is the lexicographically next string in $G_{\delta,r}$.
  Check whether there is $\boldsymbol{a}$ for which $\psi(\boldsymbol{a}, 1)$ is true and $\phi(\boldsymbol{a}, \eta c)$ is false.
  if *no solution $\boldsymbol{a}$ is found* **then**
    return $\mathcal{H} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3, ..., \boldsymbol{v}_m\}$.
  end
end

Correctness. Algorithm always output some set and terminate since we proved that there is $(nsr)^{c_2}$ sized hitting set.

Let $\boldsymbol{v}_1, ...\boldsymbol{v}_m$ be the current set to check. Let $\boldsymbol{a}$ be any assignment for the auxiliary variables of the universal circuit and let $f = \Psi(\boldsymbol{x}, \boldsymbol{a})$. If $\psi(\boldsymbol{a}, 1)$ is true then for some $u \in [-1, 1]^n, |f(\boldsymbol{u})| \geq 1$. As $\|f\|_\infty \geq 1$, Corollary 2.6 implies that

$$\|f\|_2 \geq \frac{1}{2^{n+1}} \cdot \Big(vol(n, \frac{1}{4r^2})\Big)^{\frac{1}{2}}$$

As $\mathcal{H}$ is η-robust hitting set for $v(n, s, r)$, for some i

$$|f(\boldsymbol{v}_i)| \geq \eta \cdot \|f\|_2 \geq \eta c$$

Thus, $\phi(\boldsymbol{a}, \epsilon)$ will return true. In particular, no solution 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 $\psi(\boldsymbol{a}, 1)$ is true. Indeed, if $f \neq 0$ then there is some multiple of it that at some point in $[-1, 1]^n$ will get value at least 1. This multiple of f is also computed by the universal circuit. □

References

[Bal13] Markus Bälser. *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.*

[Bur04] 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 $\mathbb{R}^n$.* Mathematical Research Letters. *8(3):233–248, 2001.*

[FS17] Michael A. Forbes and Amir Shpilka. *A PSPACE Construction of a Hitting Set for the Closure of Small Algebraic Circuits. . .*

[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):225309, 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*.