# Sum of Squares: Part 1

Apoorv Vikram Singh

February 2, 2021

# Introduction

Reason two basic problems about polynomial inequalities

1. Feasibility of polynomial system.

$$\begin{aligned} p_1(\boldsymbol{x}) &\geq 0 \\ &\vdots \\ p_m(\boldsymbol{x}) &\geq 0 \end{aligned} \tag{1}$$

   Is there an $\boldsymbol{x}$ such that (1) is satisfied?

2. Checking non-negativity: Is $q(\boldsymbol{x}) \geq 0$, $\forall \boldsymbol{x}$ satisfying (1) ?

# Justification: Feasibility

Feasibility checking is highly expressive.

- Example: MaxCut.
  - Input: $G = (V, E)$, $|V| = n$.
  - Goal: Find $S \subseteq V$ such that $\left|E(S, \overline{S})\right|$ is maximized.
  - Polynomial Feasibility: For some $\beta \in \mathbb{Z}^+$,

$$\frac{1}{4} \sum_{(i,j) \in E} (\boldsymbol{x}_i - \boldsymbol{x}_j)^2 = \beta \, |E|$$

$$\boldsymbol{x}_i^2 = 1, \qquad \forall 1 \leq i \leq n.$$

  - $n + 1$ degree-2 polynomials. Enumerate over polynomial number of values of $\beta$ and solve MaxCut.

Other examples: MaxClique, Max 3-SAT, Knapsack. Therefore, polynomial feasibility checking problem is *NP*-Hard.

# Goal

- Analyze a relaxation for the feasibility problem, and try to find interesting situations where one can get a poly-time algorithms.

# Justification: Non-Negativity

- Checking positivity: Given $f : \{-1, 1\}^n \to \mathbb{R}$ with rational coefficients, decide if:
  - $f \geq 0$, $\forall \boldsymbol{x} \in \{-1, 1\}^n$, or,
  - find an $\boldsymbol{x} \in \{-1, 1\}^n$ such that $f(\boldsymbol{x}) \leq 0$.
- Example MaxCut: Decide if MaxCut $\leq c$.
  - Let $f_G(\boldsymbol{x}) \stackrel{\text{def}}{=} \frac{1}{4} \sum_{(i,j) \in E} (\boldsymbol{x}_i - \boldsymbol{x}_j)^2$.
  - Decide if $c - f_G(\boldsymbol{x}) \geq 0$, $\forall \boldsymbol{x} \in \{-1, 1\}^n$.

# Certifying Non-Negativity

Given $f : \{-1, 1\}^n \to \mathbb{R}$, find an "efficiently verifiable" certificate of non-negativity.

# SoS Certificates

### Definition (SoS cert of non-neg (or) SoS proof of non-neg)

A degree-$d$ SoS certificate of non-negativity of $f : \{-1, 1\}^n \to \mathbb{R}$ is a list of polynomials $g_1, \ldots, g_r : \{-1, 1\}^n \to \mathbb{R}$, such such that

- $\deg(g_i) \leq d/2$, and
- $f(\boldsymbol{x}) = \sum_{i \leq r} g_i^2(\boldsymbol{x})$, $\forall \boldsymbol{x} \in \{-1, 1\}^n$.

# Efficiently Verifiable (?)

Polynomials $f, g_1, \ldots, g_r$ are represented as a vector of coefficients.

1. How large if $r$? ($\leq n^d$, see later)
2. How large are coefficients of $g_i$?

# Efficiently Verifiable

### Proposition (Efficiently Verifiable)

*Suppose $r \leq n^d$, all coefficients of $g_i$ are bounded in magnitude by $2^{\mathrm{poly}(n^d)}$. Then the identity $f = \sum_{i \leq r} g_i^2$ over all $\boldsymbol{x} \in \{-1, 1\}^n$ can be checked in poly$(n^d)$ time.*

### Proof.

- Given $g_i$, can compute $g_i^2$, and $\sum_{i \leq r} g_i^2$ in polynomial time.
- Check if $(f - \sum_{i \leq r} g_i^2)(\boldsymbol{x}) = 0$, $\forall \boldsymbol{x} \in \{-1, 1\}^n$.
- Using the fact that coefficient vector representation is unique, just check if $f - \sum_{i \leq r} g_i^2 = \mathbf{0}$

$\square$

## Fact (Unique Representation)

*$\forall f : \{-1,1\}^n \to \mathbb{R}$, there exists a unique representation of $f$: The multi-linear representation of $f$*

$$f = \sum_{S \subseteq [n]} \hat{f}(S) \prod_{i \in S} \boldsymbol{x}_i \, .$$

*(this representation is its Fourier transform)*

$\implies$ coefficient vector representation is unique.
(multilinear representation exists because $\boldsymbol{x}_i^2 = 1$)

# Are non-negative functions always certifiable?

### Proposition (Certifiablity of non-negative functions)

*Let* $f : \{-1, 1\}^n \to \mathbb{R}$ *be non-negative over* $\{-1, 1\}^n$*. Then, there exists a* $\deg(2n)$*-SoS certificate of non-negativity.*

### Proof.

- Consider $g : \{-1, 1\}^n \to \mathbb{R}$, and $g(\boldsymbol{x}) = \sqrt{f(\boldsymbol{x})}$.
- Every function on $\{-1, 1\}^n$ is a polynomial of deg $\leq n$.
- $f = g^2 \implies \deg(2n)$-SoS Certificate.

$\square$

# Tensor Notation

- Suppose vector $\boldsymbol{v} \in \mathbb{R}^n$.
- $\boldsymbol{v}^{\otimes 2} \in \mathbb{R}^{n^2}$, where $\boldsymbol{v}(i,j) = \boldsymbol{v}_i \boldsymbol{v}_j$.
- $\boldsymbol{v}^{\otimes k} \in \mathbb{R}^{n^k}$.

# Proving Efficient Verifiability

## Theorem (PSD Matrices and SoS Certificates)

*$f : \{-1,1\}^n \to \mathbb{R}$ has a $\deg(d)$-SoS certificate of non-negativity iff there exists a matrix $A$ such that $A \succcurlyeq 0$, and*

$$f(\boldsymbol{x}) = \left\langle (1,\boldsymbol{x})^{\otimes \frac{d}{2}}, A \cdot (1,\boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle .$$

- Parsing Notation:
  - $(1,\boldsymbol{x}) \in \mathbb{R}^{(n+1)}$.
  - $(1,\boldsymbol{x})^{\otimes \frac{d}{2}}$: populate in a vector all possible monomials in the variable $\boldsymbol{x}$ of degree at most $d/2$.
  - $A \in \mathbb{R}^{(n+1)^{d/2} \times (n+1)^{d/2}}$.

## Proof

- If Part:

$$\begin{aligned} f(\boldsymbol{x}) &= \left\langle (1,\boldsymbol{x})^{\otimes \frac{d}{2}}, A \cdot (1,\boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle \\ &= \left\langle (1,\boldsymbol{x})^{\otimes \frac{d}{2}}, (B^\top B) \cdot (1,\boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle \\ &= \left\langle B \cdot (1,\boldsymbol{x})^{\otimes \frac{d}{2}}, B \cdot (1,\boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle \\ &= \left\| B \cdot (1,\boldsymbol{x})^{\otimes \frac{d}{2}} \right\|^2 . \end{aligned} \tag{2}$$

  - Let $g_i(\boldsymbol{x}) = \left\langle e_i, B \cdot (1,\boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle$, i.e., $i$-th entry of the vector.
  - $B$ is a matrix of constants, applied to monomials of degree at most $d/2$, therefore, $deg(g_i) \leq d/2$.
  - Therefore,

$$f(\boldsymbol{x}) = \sum_{i=1}^{(n+1)^{\otimes d/2}} g_i^2(\boldsymbol{x}) .$$

## Proof Cont...

- Only if Part: Suppose $f$ has a degree-$d$ SoS certificate.

$$f = \sum_{i \leq r} g_i^2 \,, \text{ and } \underbrace{g_i(\boldsymbol{x})}_{\deg \leq d/2} = \left\langle \boldsymbol{v}_i, (1, \boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle .$$

$$\begin{aligned} f(\boldsymbol{x}) &= \sum_{i \leq r} \left\langle \boldsymbol{v}_i, (1, \boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle^2 \\ &= \left\langle (1, \boldsymbol{x})^{\otimes \frac{d}{2}}, \underbrace{\left( \sum_{i \leq r} \boldsymbol{v}_i \boldsymbol{v}_i^\top \right)}_{\succcurlyeq 0} \cdot (1, \boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle . \end{aligned}$$

$\square$

# Efficient Verifiability

### Corollary (Bound on $r$)

*If $f : \{-1,1\}^n \to \mathbb{R}$ has a degree-d SoS certificate, then it has a certificate with $r \le (n+1)^{d/2}$.*

### Proof.

Follows from (2):

$$f(\boldsymbol{x}) = \left\| B \cdot (1, \boldsymbol{x})^{\otimes \frac{d}{2}} \right\|^2 .$$

$\square$

# Efficient Verifiability

**Lemma (Bit-complexity of SoS proofs)**

*Suppose $f$ has a degree-$d$ certificate over $\{-1,1\}^n$. Then, $f$ has a degree-$d$ SoS certificate with bit complexity $\mathrm{poly}(n^d)$.*

- $\{-1,1\}^n$ is important, and doesn't necessarily hold for other domains.

Proof.

Since we are given $f$, we know that it can be efficiently represented. Therefore, we try to bound the entries of $A$ in terms of $f$.

- $f(\boldsymbol{x}) = \left\langle (1, \boldsymbol{x})^{\otimes \frac{d}{2}}, A \cdot (1, \boldsymbol{x})^{\otimes \frac{d}{2}} \right\rangle$, for some $A$.
- $f = \sum_u \hat{f}_u \boldsymbol{x}_u$, where $\boldsymbol{x}_u = \prod_{i \in u} \boldsymbol{x}_i$.
- Expanding the inner product, we see $\hat{f}_u = \sum_{S,T} A_{S,T}$, such that $S \Delta T = u$, and $|S|, |T| \leq d/2$.
- $\hat{f}_\emptyset = \sum_S A_{S,S} = \mathrm{tr}(A) = \sum_i \underbrace{\lambda_i(A)}_{\geq 0}$.
- $\|A\|_F^2 = \sum_{S,T} A_{S,T}^2 = \sum_i \lambda_i^2(A) \leq \hat{f}_\phi^2$.

$\square$

# References I


Moitra, A. (2015).
Super-resolution, extremal functions and the condition number of vandermonde matrices.
In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '15, page 821–830, New York, NY, USA. Association for Computing Machinery.