# Sum-of-squares

**Amit Rajaraman**

Last updated December 12, 2022

## Contents

# §1. Fundamentals

## 1.1. Introduction

The sum-of-squares technique, at its most basic form, is a way of determining whether for some polynomial $p$ over $\mathbb{R}^n$, $p(x) \geq 0$ for $x$ in some base set. For now, suppose that our "base set" is $\{0,1\}^n$. Elegantly, it manages to convert *disproofs* of such inequalities to *algorithms* to determine a point where $p(x) < 0$.
More concretely, we shall show non-negativity by expressing $p$ as a *sum of squares* of *low degree* polynomials (while low degree is not technically required, it makes the converted algorithm efficient).

**Definition 1.1** (Sum-of-squares proof)**.** Given a polynomial $f$ in variables $x_1, \ldots, x_n$, a *degree* $d$ *sum-of-squares proof* or *degree* $d$ *sum-of-squares certificate* (abbreviated SoS proof or SoS certificate) of $f \geq 0$ is a set $\{g_1, \ldots, g_m\}$ of polynomials of degree at most $d/2$ such that

$$f(x) = \sum_{i=1}^{m} g_i^2(x) \tag{1.1}$$

for all $x$. If $f$ has a degree $d$ sum-of-squares certificate, we write that

$$\vdash_d f(x) \geq 0.$$

Let $\mathcal{A}$ be a set of constraints of the form $A_i(x) = 0$ or $B_j(x) \geq 0$ for $i \in [k], j \in [\ell]$. Then, an *degree* $d$ *SoS proof given* $\mathcal{A}$ of $f \geq 0$ is a set $\{g_1, \ldots, g_m\}$ of polynomials of degree at most $d/2$ such that (1.1) holds for all $x$ satisfying the constraints in $\mathcal{A}$. If such a set exists, we write

$$\mathcal{A} \vdash_d f \geq 0.$$

We always assume that $d$ in this context is even.
Note that simple set restrictions can be captured by the set of constraints. In particular, we can check restrict ourselves to the boolean hypercube $\{-1,1\}^n$ by having $\mathcal{A}$ contain $x_i^2 = 1$ for all $i$. Note that the set of functions with degree $d$ SoS proofs of non-negativity forms a closed convex cone.

**Proposition 1.2.** Any non-negative $f : \{-1,1\}^n \to \mathbb{R}$ has a degree $2n$ sum-of-squares proof.

*Proof.* Recall that any function $h : \{-1,1\}^n \to \mathbb{R}$ can be expressed as a polynomial of degree at most $n$ as

$$h(x) = \sum_{S \subseteq [n]} \hat{f}(S) x_S,$$

where $x_S = \prod_{i \in S} x_i$ with the convention $x_\varnothing = 1$. Knowledgeable readers may recognize this as the *Fourier expansion* of $h$ – we omit the details of why such an expansion exists, but refer the reader to the excellent text by O'Donnell [O'D14] for more details. In particular, $\sqrt{f}$ is a polynomial of degree at most $n$, so squaring both sides we get that $f$ has a degree $2n$ SoS proof. ∎

The above is *not* true in general; not every non-negative polynomial $f : \mathbb{R}^n \to \mathbb{R}$ can be written as a sum of squares.

**Definition 1.3.** Given a vector $y \in \mathbb{R}^n$, the vector $y^{\otimes k} \in \mathbb{R}^{n^d}$ has entries indexed by elements of $[n]^d$, with the $\alpha$th entry being $\prod_{j \in d} y_{\alpha_j}$. Also denote $v_k(x)$ to be the size $\binom{n+k}{k}$ vector with entries equal to all the monomials of $x$ of degree at most $k$.

Note that for $x \coloneqq (x_1, \ldots, x_n) \in \mathbb{R}^n$, any monomial of degree at most $d/2$ appears in the vector $(1,x)^{\otimes d/2}$, where $(1,x) = (1, x_2, \ldots, x_n) \in \mathbb{R}^{n+1}$. Also recall that a matrix $A$ is said to be positive semidefinite, denoted $A \succeq 0$, if $x^\top Ax \geq 0$ for all vectors $x$, which is equivalent to asserting that all eigenvalues of the matrix are non-negative.

**Proposition 1.4.** Let $f$ be a polynomial. $f$ has a degree $d$ sum-of-squares proof iff there exists $A \succeq 0$ such that

$$f(x) = \langle v_{d/2}(x), A v_{d/2}(x) \rangle. \tag{1.2}$$

*Proof.* For the forward direction, suppose that $f = \sum_{i=1}^m g_i^2$, with $g_i(x) = v_i^\top v_{d/2}(x)$ by writing it out in the monomial basis. Then,

$$\begin{aligned} f(x) &= \sum_{i=1}^m v_{d/2}(x)^\top v_i v_i^\top v_{d/2}(x) \\ &= \left\langle v_{d/2}(x), \underbrace{\sum_{i=1}^m v_i v_i^\top}_{A} v_{d/2}(x) \right\rangle. \end{aligned}$$

The backward direction is straightforward by decomposing $A$ as $\sum \lambda_i v_i v_i^\top$, where each $\lambda_i \geq 0$, and observing that each $v_i^\top v_{d/2}(x)$ is a polynomial of degree at most $d/2$. ■

As a corollary, this implies that if an $f$ has a degree $d$ SoS proof, it has one with at most $\binom{n+d}{d}$ squares. Also note that eq. (1.2) is *linear* in the elements of $A$.
If we bump up a function by enough, we can ensure non-negativity. It turns out that we can do the same to ensure SoS-ness.

**Lemma 1.5.** Let $f : \{-1, 1\}^n \to \mathbb{R}$ be any function of degree at most $d$. For sufficiently large $L$, $L + f$ has a degree $d$ SoS certificate.

*Proof.* Note that for any $S$, $1 + x_S \geq 0$ has a degree $\lceil |S|/2 \rceil$ SoS proof. Indeed, setting $S = T_1 \sqcup T_2$ for $T_1, T_2$ of (almost) equal size, $1 + x_S = \frac{1}{2}(x_{T_1} + x_{T_2})^2$. Similarly, $1 - x_S$ has a degree $|S|$ SoS proof as well. Therefore,

$$\sum_{|S| \leq d} |\hat{f}(S)| + \sum_{|S| \leq d} \hat{f}(S) x_S = \sum_{|S| \leq d} |\hat{f}(S)| (1 + \operatorname{sign}(\hat{f}(S)) x_S)$$

has a degree $d$ SoS certificate, so the statement is true with $L = \sum_{|S| \leq d} \hat{f}(S)$. ■

## 1.2. Semidefinite Programming

The reader is likely familiar with *linear programming*, where we are interested in

$$\min_{x \in \mathcal{P}} c^\top x, \text{ where } \mathcal{P} = \{x \geq 0 : Ax = b\}.$$

Although a linear program may in general have inequalities in the constraints, we may merge these into the $x \geq 0$ condition by introducing slack variables (if we have $\sum_i a_i x_i \geq 0$, we may add a non-negative variable $y$ and make it $\sum_i a_i x_i - y = 0$). In *semidefinite programming*, the setting is mostly the same, albeit with the minor change that we represent the variables by a matrix instead of a vector, and we additionally have that this matrix is positive semidefinite. More concretely, denoting

$$\langle C, X \rangle = \sum_{i,j} C_{ij} X_{ij},$$

we are interested in

$$\min_{X \in \mathcal{S}} \langle C, X \rangle, \text{ where } \mathcal{S} = \{X \succeq 0 : \langle A_i, X \rangle = b_i \text{ for } i \in [m]\}.$$

We interchangeably use $\mathcal{S}$ to denote the set of constraints and the corresponding body. Proposition 1.4 suggests a link between SoS proofs and SDPs. A natural question is: can we solve SDPs efficiently?
Note that the set of all PSD matrices $X$ forms a convex cone. In combination with the linear constraints, the intersection of this cone and the affine subspace form a so-called "spectrahedron", which we would like to minimize our quantity over. Note that any linear program is a semidefinite program, by enforcing that all off-diagonal elements of the matrix are zero. To answer our earlier question, it turns out that we cannot solve SDPs exactly.[1] However, if we enforce certain structural restrictions, we can solve them approximately (up to a small additive error).

**Definition 1.6** (Separation Oracle)**.** For a convex body $K \subseteq \mathbb{R}^n$, a (*strong*) *separation oracle* for $K$ does the following given as input any $x \in K$.

1. if $x \in K$, it returns yes.
2. if $x \notin K$, it returns no, and in addition a vector $a$ and real $b$ such that $\langle a, y\rangle \geq b$ for all $y \in K$ and $\langle a, x\rangle < b$ – this is a so-called "separating hyperplane" that separates $x$ and $K$.

More generally, we can efficiently minimize an inner product over a convex (bounded) body up to an additive error of $\epsilon$, given an efficient weak separation oracle.

**Theorem 1.7.** Let $f : \{-1, 1\}^n \to \mathbb{R}$ have a degree $d$ sum-of-squares proof of non-negativity. Then, for $\epsilon > 0$, there exists an algorithm that finds a sum-of-squares proof of $f + \epsilon$ in $\mathrm{poly}(n^d, \log(1/\epsilon))$.

The high-level idea of the algorithm is as follows.
We first solve the "feasibility problem" of finding a point in a body $K$, given that $B(c, r) \subseteq K \subseteq B(0, R)$. We begin by setting $\mathcal{E}^{(0)} = B(0, R)$. Given the ellipsoid $\mathcal{E}^{(i)}$, if its center returns yes, we return the point itself. Otherwise, we use the separating hyperplane to get a halfspace $H$ in which $K$ is contained, and set $\mathcal{E}^{(i+1)}$ to be the smallest ellipsoid containing $\mathcal{E}^{(i)} \cap H$. This algorithm runs in $\mathrm{poly}(n, \mathrm{size}(K)) \log(R/r)$ – the proof amounts to showing that the volume of the ellipsoid decreases by a factor of at least $\exp(1/2(n+1))$ at each stage, and we have a lower bound on the volume of $K$ by $\mathrm{vol}(B(0, r))$.
We can slightly modify this algorithm to one that approximately solves the optimization version of maximizing $c^\top x$ as well. Once we get a point $\alpha$ in the body, we begin looking at $K \cap \{x : c^\top x > c^\top \alpha\}$ and repeat the feasibility algorithm. This is repeatedly done until we can guarantee that we are within $\epsilon$ of the optimum. The only non-trivial part of this algorithm is showing that we can use the oracle to construct an oracle for the new body $K \cap \{x : c^\top x > c^\top \alpha\}$.
To complete the connection to SDPs, we require that the SDP constraints $\mathcal{S}$ admits an efficient weak separation oracle; we omit the details of this. Next, we require that the body $\mathcal{S}$ contains a ball and is contained in a ball. The former is not true in general because the constraints typically make our body lower-dimensional (a subspace). To get around this, we introduce an additive error in each the contraints, so the new constraints are $|\langle A, X\rangle - b_i| \leq \epsilon$ for each $i$. In this case, there is a ball of radius $O((\epsilon/\|A\|_F)^n)$ contained in the body, where $\|A\|_F^2 = \sum_{i,j,k}(A_i)_{jk}^2$.
In our context of finding $X$ such that $f(x) = v_{d/2}(x)^\top X v_{d/2}(x)$, we know that $\|A\|_F^2 \leq \mathrm{Tr}(A)^2 \leq \hat{f}(\varnothing)^2$, so the body is bounded as well.

Like how LPs have duals, so do SDPs. If we have the primal

$$\min_{X \in \mathcal{S}} \langle C, X\rangle, \text{ where } \mathcal{S} = \left\{X \succeq 0 : \langle A_i, X\rangle = b_i \text{ for } i \in [m]\right\},$$

its dual is

$$\max_{y \in \mathcal{S}^D} b^\top y, \text{ where } \mathcal{S}^D = \left\{S \succeq 0 : C - \sum_{i=1}^m y_i A_i = S\right\}.$$

[1] It is not even known if this is in NP! It is known that it is in PSPACE however.

The PSDness condition in the dual just says that $C \succeq \sum_{i=1}^m y_i A_i$.

**Proposition 1.8** (Weak Duality)**.** Let $X$ and $y$ be solutions to the primal and dual SDPs respectively. Then, $\langle C, X\rangle \geq b^\top y$.

*Proof.* We have

$$\begin{aligned} \langle C, X\rangle &= \left\langle \sum_{i=1}^m y_i A_i + S, X \right\rangle \\ &= \sum_{i=1}^m y_i \langle A_i, X\rangle + \langle S, X\rangle \\ &= b^\top y + \langle S, X\rangle \geq b^\top y. \end{aligned}$$

The final inequality requires showing that if $S, X \succeq 0$, then $\langle S, X\rangle \geq 0$; we omit the details of the proof. ■

In linear programming, we have strong duality which asserts that the two optima are in fact *equal*. However, in SDPs, some mild conditions are required for this to be true.

**Theorem 1.9** (Strong duality)**.** Let $\mathcal{S}$ be the set of constraints of a primal SDP and $\mathcal{S}^D$ the set of constraints in its dual, such that the two have optima $\alpha^*, \beta^*$. Then, $\langle C, \alpha^*\rangle = \langle b, \beta^*\rangle$ if

1. the spectrahedron $\mathcal{S}$ is non-empty and there exists $\beta$ such that $\sum_{i\in[m]} \beta_i A_i - C \succ 0$, or
2. the spectrahedron $\mathcal{S}^D$ is non-empty and there exists $\alpha \succ 0$ such that $\langle A, \alpha\rangle = b_i$ for all $i \in [m]$.

As a corollary, one may show that $\langle C, \alpha^*\rangle = \langle b, \beta^*\rangle$ if the set of optimal solutions of either of the two SDPs is non-empty and bounded.

We omit the (rather involved) proof of the above.

## 1.3. Pseudoexpectations

Let us again restrict ourselves to $\{-1,1\}^n$ for a while. We have established one link between SoS proofs and SDPs, and now we shall establish another link between them and the following.

**Definition 1.10** (Pseudodistribution)**.** A *degree $d$ pseudodistribution* is a function $\mu : \{-1,1\}^n \to \mathbb{R}$ such that the expectation operator $\widetilde{\mathbb{E}}_\mu$ defined by $\widetilde{\mathbb{E}}_\mu f = \sum_{x\in\{-1,1\}^n} f(x)\mu(x)$ satisfies

(a) $\widetilde{\mathbb{E}}_\mu 1 = 1$, and

(b) for all $f$ of degree at most $d/2$, $\widetilde{\mathbb{E}}_\mu f^2 \geq 0$.

In this case, $\widetilde{\mathbb{E}}_\mu$ is called a *pseudoexpectation*.

Analogous to Proposition 1.2, we get that any degree $\geq 2n$ pseudodistribution is an actual distribution, in the sense that $\mu \geq 0$. Analogous to Proposition 1.4, we get the following.

**Proposition 1.11.** $\widetilde{\mathbb{E}}$ is a degree $d$ pseudoexpectation iff

(a) $\widetilde{\mathbb{E}}1 = 1$, and

(b) $\widetilde{\mathbb{E}} v_{d/2}(x) v_{d/2}(x)^\top \succeq 0$.

*Proof.* Note that for any vector $(\hat{f})$ of Fourier coefficients of a degree $\le d/2$ function $f : \{-1,1\}^n \to \mathbb{R}$ (so $f(x) = \hat{f}^\top v_{d/2}(x)$),

$$\begin{aligned}\widetilde{\mathbb{E}} f^2 &= \widetilde{\mathbb{E}} \left( \sum_{|S| \le d} \hat{f}(S) x_S \right)^2 \\ &= \widetilde{\mathbb{E}} \hat{f}^\top v_{d/2}(x) v_{d/2}(x)^\top \hat{f} \\ &= \hat{f}^\top \left( \widetilde{\mathbb{E}} v_{d/2}(x) v_{d/2}(x)^\top \right) \hat{f}.\end{aligned}$$

To conclude, note that $\widetilde{\mathbb{E}} v_{d/2}(x) v_{d/2}(x) \succeq 0$ iff $\hat{f}^\top \left( \widetilde{\mathbb{E}} v_{d/2}(x) v_{d/2}(x)^\top \right) \hat{f} \ge 0$ for all vectors $\hat{f}$. ■

Given any function that is not non-negative everywhere, there exists some distribution $\mu$ such that $\mathbb{E}_\mu f < 0$. Ideally, we would like a similar result in order to distinguish between functions that have SoS certificates of degree $d$ and those that don't.

**Theorem 1.12.** $f$ has a degree $d$ sum-of-squares proof iff for all degree $d$ pseudoexpectations $\widetilde{\mathbb{E}}$, $\widetilde{\mathbb{E}} f \ge 0$.

Equivalently, $f$ does not have a degree $d$ sum-of-squares proof iff there exists a degree $d$ pseudoexpectation $\widetilde{\mathbb{E}}$ such that $\widetilde{\mathbb{E}} f < 0$.

*Proof.* The forward direction is straightforward by Definition 1.10(b). For the backward direction, suppose instead that $f$ does not have a degree $d$ SoS proof. Then, there exists a separating hyperplane between $f$ and this set, that is, some degree $d$ pseudoexpectation $\widetilde{\mathbb{E}}$ such that $\widetilde{\mathbb{E}} f < 0$. If we manage to show that $\widetilde{\mathbb{E}} 1 > 0$, we are done since we can then rescale $\mu$ to make it exactly equal to $1$. By Lemma 1.5, we have $L > 0$ such that $\widetilde{\mathbb{E}}(f + L) \ge 0$. Since $\widetilde{\mathbb{E}} f < 0$, this means that $\widetilde{\mathbb{E}} L = L \cdot \widetilde{\mathbb{E}} 1 > 0$, completing the proof. ■

Using our earlier discussion, given a function $f$ without a degree $d$ SoS certificate of positivity, we may find in $\mathrm{poly}(n^d, 1/\epsilon, \mathrm{size}(f))$ time a pseudoexpectation $\widetilde{\mathbb{E}}$ such that $\widetilde{\mathbb{E}} f < \epsilon$.

## 1.4. Application: Max-cut

In this subsection, let us describe how the content of the previous three subsections interact through an example, and give an approximation algorithm for the max-cut problem.

**Question.** Given a graph $G = (V, E)$, find $S \subseteq V$ such that the size of the cut $E(S, S^c) = \left\{ \{i, j\} \in E : i \in S, j \in S^c \right\}$ is maximized.

Unlike min-cut, which may be solved in polynomial time using flow, the above is NP-complete.
One basic approximation algorithm was proposed by Erdős, which merely returns a random cut. With constant probability, the returned cut is a $1/2$-approximation of the max-cut. We shall in this algorithm study an algorithm due to Goemans and Williamson [GW00].

Assume wlog that $V = [n]$, and identify any $S \subseteq V$ with the vector in $\{-1, 1\}^n$ with a $1$ at precisely those vertices in $S$. Note that the function defined by

$$f_G(x) = \frac{1}{4}\sum_{ij \in E}(x_i - x_j)^2 = \frac{1}{2}\sum_{ij \in E}(1 - x_i x_j).$$

on input $S$ returns precisely the size of the cut corresponding to $S$. Equivalently, considering the *graph Laplacian* $L_G \coloneqq D_G - A_G$, where $D_G$ is the diagonal matrix of degrees and $A_G$ is the adjacency matrix, we have

$$f_G(x) = \frac{1}{4}x^\top L_G x = \frac{1}{4}\langle L_G, xx^\top\rangle.$$

We are interested in $\max_{x \in \{-1,1\}^n} f_G(x) =: \mathsf{opt}(G)$.

**Theorem 1.13.** Set $\alpha_{\mathsf{GW}} \coloneqq \min_{\rho \in [-1,1]} \frac{2\arccos(\rho)}{\pi(1-\rho)} \approx 0.8786$. Then,

$$\frac{\mathsf{opt}(G)}{\alpha_{\mathsf{GW}}} - f_G(x) \geq 0$$

has a degree $2$ sum-of-squares certificate.

Let $\widetilde{\mathbb{E}}_{\mathsf{opt}}$ be a pseudoexpectation that maximizes $\widetilde{\mathbb{E}}_{\mathsf{opt}} f_G$ as $\mathsf{opt}_{\mathsf{SOS}_2}(G)$. Clearly, $\mathsf{opt}_{\mathsf{SOS}_2}(G) \geq \mathsf{opt}(G)$. Furthermore, by the previous theorem,

$$\mathsf{opt}(G) \leq \mathsf{opt}_{\mathsf{SOS}_2}(G) \leq \frac{1}{\alpha_{\mathsf{GW}}}\mathsf{opt}(G).$$

By the discussion at the end of the previous subsection, we can find in $\mathrm{poly}(n, 1/\epsilon)$ a pseudodistribution $\mu$ such that

$$\widetilde{\mathbb{E}}_\mu f_G \geq \mathsf{opt}_{\mathsf{SOS}_2}(G) - \epsilon.$$

So,

$$\frac{1}{\alpha_{\mathsf{GW}}}\mathsf{opt}(G) \geq \widetilde{\mathbb{E}}_\mu f_G \geq \mathsf{opt}(G) - \epsilon.$$

**Lemma 1.14.** Let $\mu$ be a degree $2$ pseudodistribution on $\{-1, 1\}^n$. Then, there exists a ("real") distribution $\mu'$ on $\{-1, 1\}^n$ such that

$$\mathbb{E}_{\mu'} f_G \geq \alpha_{\mathsf{GW}} \cdot \widetilde{\mathbb{E}}_\mu f_G.$$

Further, it is possible to efficiently sample from $\mu'$ given $\mu$. Plugging this back into our previous sequence of equations,

$$\mathbb{E}_{\mu'} f_G \geq \alpha_{\mathsf{GW}}(\mathsf{opt}(G) - \epsilon) \geq (\alpha_{\mathsf{GW}} - \epsilon)\mathsf{opt}(G),$$

and efficient sampling implies that we can in $\mathrm{poly}(n, 1/\epsilon)$ time sample a random cut $S$ such that with good probability, the size of the cut of $S$ is a $(\alpha_{\mathsf{GW}} - \epsilon)$-approximation of the max-cut.
Let us now get to the proofs of the above results.

*Proof that Lemma 1.14 implies Theorem 1.13.* It suffices to show that for all pseudodistributions $\widetilde{\mathbb{E}}_\mu$,

$$\widetilde{\mathbb{E}}_\mu\left[\frac{\mathsf{opt}(G)}{\alpha_{\mathsf{GW}}} - f_G\right] \geq 0.$$

Equivalently, we would like to show that

$$\widetilde{\mathbb{E}}_\mu f_G \leq \frac{\mathsf{opt}(G)}{\alpha_{\mathsf{GW}}}.$$

Letting $\mu'$ be a distribution as in Lemma 1.14,

$$\widetilde{\mathbb{E}}_\mu f_G \leq \frac{1}{\alpha_{\text{GW}}} \mathbb{E}_{\mu'} f_G \leq \frac{1}{\alpha_{\text{GW}}} \mathsf{opt}(G). \qquad \blacksquare$$

*Proof of Lemma 1.14.* We may assume wlog that $\widetilde{\mathbb{E}}_\mu x = 0$, by changing $\mu(x)$ to $\frac{\mu(x)+\mu(-x)}{2}$ – note that this procedure does not change $\widetilde{\mathbb{E}}_\mu f_G$ because $f_G(x) = f_G(-x)$. Using Proposition 1.11(b) and recalling that any principal submatrix of a PSD matrix is PSD, $\widetilde{\mathbb{E}}_\mu x x^\top \succeq 0$. So, let $\nu$ be a normal distribution on $\mathbb{R}^n$ with mean $0$ and covariance matrix $\widetilde{\mathbb{E}}_\mu x x^\top$. Finally, define $\mu'$ by the process that samples a vector $v$ according to $\nu$, and returning $\operatorname{sign}(\nu)$ – this is well-defined with probability $1$. $\blacksquare$

# References

[GW00] Michel Goemans and David Williamson. 0.878 approximation algorithms for max cut and max 2-sat. *Journal of the ACM*, 42, 07 2000.

[O'D14] Ryan O'Donnell. *Analysis of Boolean Functions*. Cambridge University Press, 2014.