The Sum-of-Squares Method

Amit Rajaraman

Last updated April 12, 2023

Contents

§0. Notation

Given $n \times n$ matrices A, B, denote $\langle A, B \rangle = \mathrm{Tr}(AB) = \sum_{i,j} A_{ij} B_{ij}$.

§1. Fundamentals

1.1. Introduction

Consider the problem of, for a given multivariate polynomial p, determining whether $p(x) \geq 0$ for x in some (subset of) $\mathbb{R}^n$. It is not difficult to see that this can capture a huge spectrum of problems, specifically NP-hard ones such as max-cut – given a graph G on n vertices, consider the polynomial $f : \{-1, 1\}^n \to \mathbb{R}$ defined by

$$f(x) = \sum_{ij \in E} (x_i - x_j)^2.$$

Then, there exists x such that $f(x) \leq k$ – or equivalently, the polynomial $k - f(x)$ is non-negative on $\{-1, 1\}^n$ – iff every cut is of size at most k.
So, this problem of determining non-negativity of a polynomial is NP-hard. What next?

The sum-of-squares technique, at its most basic form, is a a restriction to a certain type of non-negativity. For now, suppose that our "base set" is $\{0, 1\}^n$.
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, the resulting algorithm need not be efficient otherwise).

Definition 1.1 (Sum-of-squares proof)**.** Given a polynomial $f \in \mathbb{R}[x_1, \ldots, x_n]$, 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

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

as polynomials. If f has a degree d sum-of-squares certificate, we write that

$$\vdash_x^d f(x) \geq 0.$$

Let $\mathcal{A}$ be a set of constraints of the form $f_i(x) \geq 0$ for $i \in [m]$. Then, an *degree d SoS proof given $\mathcal{A}$* of $f \geq 0$ is a set $\{p_S\}_{S \subseteq [m]}$ of degree d sum-of-squares polynomial (in the sense that it satisfies Equation (1.1) for some (g_i)), where S ranges over *multi*sets of elements in $[m]$ such that

$$f(x) = \sum_{S \subseteq [m]} p_S(x) \prod_{i \in S} f_i(x)$$

as polynomials. If this is the case, we write

$$\mathcal{A} \vdash_x^d f \geq 0.$$

We always assume that d in this context is even. We often suppress the variable x, and rarely even the degree d, in the above notation if they are clear from context.
Although $\mathcal{A}$ contains only inequalities of polynomials, we can easily also make it contain equalities of polynomials by adding two corresponding constraints – for $p(x) = k$, add $p(x) - k \geq 0$ and $k - p(x) \geq 0$.

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. Other than this, the reader can more or less

ignore the second part of the above definition until Section 5, where we shall use its power in more depth. Also observe 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 αth 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 $x^\top A x \geq 0$ 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,

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

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 ϵ, 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 $\text{poly}(n^d, \log(1/\epsilon))$.

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

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

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 $\text{poly}(n, \text{size}(K)) \log(R/r)$ – 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 $\text{vol}(B(0,r))$.
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 α 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 ϵ 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 $|\langle A, X\rangle - b_i| \le \epsilon$ 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 $\|A\|_F^2 \le \text{Tr}(A)^2 \le \hat{f}(\varnothing)^2$, 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

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

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, $\langle C, X\rangle \ge b^\top y$.

Proof. We have

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

The final inequality requires showing that if $S, X \succeq 0$, then $\langle S, X\rangle \ge 0$ – this is a simple corollary of the Schur Product Theorem we shall see later, using $\mathbf{1}^\top (S \circ X)\mathbf{1} \ge 0$. ■

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 α^*, β^*. Then, $\langle C, \alpha^*\rangle = \langle b, \beta^*\rangle$ if

1. the spectrahedron $\mathcal{S}$ is non-empty and there exists β 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 $\leq d/2$ function $f : \{-1,1\}^n \to \mathbb{R}$ (so $f(x) = \hat{f}^\top v_{d/2}(x)$),

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

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

Given any function that is not non-negative everywhere, there exists some distribution μ 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 $\widetilde{\mathbb{E}}$, $\widetilde{\mathbb{E}}f \geq 0$.

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 μ to make it exactly equal to 1. By Lemma 1.5, we have $L > 0$ such that $\widetilde{\mathbb{E}}(f + L) \geq 0$. 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 $\widetilde{\mathbb{E}}f < \epsilon$.

§2. Degree 2: Quadratic optimization on the hypercube

2.1. 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 $E(S, S^c) = \{\{i, j\} \in E : i \in S, j \in S^c\}$ 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

$$f_G(x) = \frac{1}{4} \sum_{ij \in E} (x_i - x_j)^2 = \frac{1}{2} \sum_{ij \in E} (1 - x_i x_j). \tag{2.1}$$

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

$$f_G(x) = \frac{1}{4} x^\top L_G x. \tag{2.2}$$

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

Theorem 2.1. Set $\alpha_{\mathrm{GW}} \coloneqq \min_{\rho \in [-1,1]} \frac{2 \arccos(\rho)}{\pi(1-\rho)} \approx 0.8786$. Then,

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

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 $\mathsf{opt}_{\mathrm{SOS}_2}(G)$. Clearly, $\mathsf{opt}_{\mathrm{SOS}_2}(G) \geq \mathsf{opt}(G)$. Furthermore, by the previous theorem,

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

By the discussion at the end of the previous subsection, we can find in $\mathrm{poly}(n, 1/\epsilon)$ a degree 2 pseudodistribution μ such that

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

So,

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

Lemma 2.2. Let μ be a degree 2 pseudodistribution on $\{-1, 1\}^n$. Then, there exists a ("real") distribution μ' on $\{-1, 1\}^n$ such that

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

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

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

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

Proof that Lemma 2.2 implies Theorem 2.1. It suffices to show that for all pseudodistributions $\widetilde{\mathbb{E}}_\mu$,

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

Equivalently, we would like to show that

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

Letting μ' be a distribution as in Lemma 2.2,

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

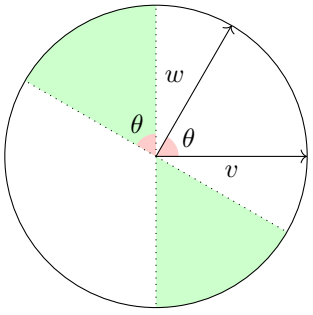
Proof of Lemma 2.2. We may assume wlog that $\widetilde{\mathbb{E}}_\mu x = 0$, by changing $\mu(x)$ to $\frac{\mu(x)+\mu(-x)}{2}$ – note that this procedure does not change $\widetilde{\mathbb{E}}_\mu f_G$ because $f_G(x) = f_G(-x)$. Using Proposition 1.11(b) and recalling that any principal submatrix of a PSD matrix is PSD, $\widetilde{\mathbb{E}}_\mu xx^\top \succeq 0$. So, let ν be a normal distribution on $\mathbb{R}^n$ with mean 0 and covariance matrix $\widetilde{\mathbb{E}}_\mu xx^\top$. Finally, define μ' by the process that samples a vector g according to ν and returns $\hat{x} = \text{sign}(g)$, the vector in $\{-1, 1\}^n$ whose ith coordinate is just the sign ± 1 of g_i – this is well-defined with probability 1. Note that an $(x_i - x_j)^2$ term in f_G contributes to the cut iff $\text{sign}(g_i) \neq \text{sign}(g_j)$. That is,

$$\mathbb{E}_{\mu'} f_G = \sum_{ij \in E} \Pr[\text{sign}(g_i) \neq \text{sign}(g_j)].$$

For distinct i, j, set $\rho_{ij} = \mathbb{E}_\mu[x_i x_j] = \mathbb{E}[g_i g_j]$. Let $h \sim \mathcal{N}(0, \text{Id}_2)$. Then, to analyze the above probability (for a fixed i, j), we can assume that $g_i = \langle h, v \rangle$ and $g_j = \langle h, w \rangle$ for some v, w such that $\langle v, w \rangle = \rho_{ij}$. So, $\text{sign}(g_i) \neq \text{sign}(g_j)$ iff $\langle h, v \rangle$ and $\langle h, w \rangle$ have opposite signs. Because the "direction" $h/\|h\|$ of h is uniformly distributed on $\mathbb{S}^1$, we get that

$$\Pr[\text{sign}(g_i) \neq \text{sign}(g_j)] = \frac{\arccos(\rho_{ij})}{\pi},$$

as seen in the following diagram, where h must lie in the green region for the signs to be different.



The angle between v, w is $\theta = \arccos(\rho_{ij})$.

Using the facts that $\mathbb{E}[g_i^2] = 1$ and $\mathbb{E}[g_i g_j] = \rho_{ij}$, we have that $\mathbb{E}[(g_i - g_j)^2] = 2(1 - \rho_{ij})$ and so

$$\begin{aligned}\mathbb{E}_{\mu'} f_G &= \sum_{ij \in E} \Pr[\text{sign}(g_i) \neq \text{sign}(g_j)] \\ &= \sum_{ij \in E} \frac{\arccos(\rho_{ij})}{2\pi(1-\rho_{ij})} \mathbb{E}[(g_i - g_j)^2] \\ &\geq \frac{\alpha_{\text{GW}}}{4} \cdot \mathbb{E}\left[\sum_{ij \in E} (g_i - g_j)^2\right] = \alpha_{\text{GW}} \widetilde{\mathbb{E}}_{\mu} f_G.\end{aligned}$$

■

Now, we have managed to get roughly an α_{GW}-approximation using degree 2 SoS. Is it possible to do any better using degree 2 SoS? What about with a higher (but constant) degree? It might even be interesting to see if we can get a better approximation with non-constant degree, say $O(\log n)$.
To answer the first question, it turns out that what we have done is indeed the best possible. There is also strong reason to believe that an $(\alpha_{\text{GW}} + \epsilon)$-approximation is NP-hard, assuming the *Unique Games Conjecture*, that we shall study in more detail in Section 3.2.

Let us get back to the Goemans-Williamson algorithm. Instead of looking at the best approximation ratio, can we parametrize the output result in terms of the optimal value?

Proposition 2.3. Let G be a graph with $\text{opt}(G) = (1-\delta)|E|$. For the output distribution μ' of the Goemans-Williamson algorithm, $\mathbb{E}_{\mu'} f_G \geq (1 - \sqrt{\delta})|E|$.

Proof. Let

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

It suffices to show that given a degree 2 pseudodistribution μ such that $\widetilde{\mathbb{E}}_{\mu} h_G = \delta|E|$, there exists a distribution μ' such that $\mathbb{E}_{\mu'} h_G \leq \sqrt{\delta}|E|$. This distribution μ' is defined exactly the same as in the Goemans-Williamson algorithm. We denote g and $\hat{x}$ as we do in the proof. Letting $\rho_{ij} = \mathbb{E} g_i g_j = \widetilde{\mathbb{E}}_{\mu} x_i x_j$, recall from the proof of Lemma 2.2 that $\mathbb{E}\hat{x}_i \hat{x}_j = \frac{2}{\pi} \arcsin \rho_{ij}$. This implies that

$$\mathbb{E}_{\mu'} h_G = \mathbb{E}_{\mu'} \sum_{ij \in E} \frac{1 + \hat{x}_i \hat{x}_j}{2} = \frac{1}{2} \sum_{ij \in E} 1 + \frac{2}{\pi} \arcsin(\rho_{ij}).$$

Also note that

$$\sup_{\rho \in [-1,1]} \frac{\left(1 + (2/\pi)\arcsin(\rho)\right)^2}{1+\rho} = 2. \tag{2.3}$$

Consequently,

$$\begin{aligned}
\left(\mathbb{E}_{\mu'} h_G\right)^2 &= \frac{1}{4}\left(\sum_{ij\in E} 1 + \frac{2}{\pi}\arcsin(\rho_{ij})\right)^2 \\
&\leq \frac{|E|}{4}\sum_{ij\in E}\left(1+\frac{2}{\pi}\arcsin(\rho_{ij})\right)^2 \qquad \text{(Cauchy-Schwarz)} \\
&\overset{(2.3)}{\leq} \frac{|E|}{2}\sum_{ij\in E} 1+\rho_{ij} \\
&= |E|\cdot\mathbb{E}\left[\sum_{ij\in E}\frac{1+g_i g_j}{2}\right] \\
&= |E|\cdot\widetilde{\mathbb{E}}_\mu h_G = \delta|E|^2,
\end{aligned}$$

so $\mathbb{E}_{\mu'} h_G \leq \sqrt{\delta}|E|$, completing the proof. ■

Is this rounding we have done, called "Gaussian rounding", the best possible? It turns out that it is not, and we can in general do better using the "RPR^2" scheme of roundings. We shall soon study this in more detail.

Let us now return to our earlier statement that it is impossible to do better using degree 2 SoS. That is, for graphs in general, if we can get a degree 2 SoS certificate of non-negativity for

$$\frac{\mathsf{opt}(G)}{c} - f_G(x),$$

how large can c be? We shall show that $c = \alpha_{\mathrm{GW}}$ is optimal, by looking at the cycle C_n for odd n. This serves as a "gap" example. It is easily seen that the max-cut in this graph is $n-1 = \left(1-\frac{1}{n}\right)|E|$. We shall show that there exists a degree 2 pseudodistribution μ such that

$$\widetilde{\mathbb{E}}_\mu f_{C_n} \geq \left(1 - O\left(\frac{1}{n^2}\right)\right)|E|.$$

Due to Proposition 2.3, this shows that the Goemans-Williamson algorithm is tight, at least up to constant factors. We can think of the cycle as something of a discretization of the 2-dimensional sphere. If we instead look at the discretization of a high-dimensional sphere, it can be shown that this is tight even up to constant factors. We refer the reader to [FS02] for details. The sketch of the proof for the cycle is as follows.
Recall eq. (2.2), so we are interested in $\max_{x\in\{-1,1\}^n} x^\top L_G x$. This is at most $\max_{x:\|x\|_2=\sqrt{n}} x^\top L_G x = n\|L_G\|_2$, which can be computed in polynomial time. Now, how do we construct a pseudodistribution $\widetilde{\mathbb{E}}$ for the cycle as mentioned earlier? Note that a given $\widetilde{\mathbb{E}}$ is a well-defined degree 2 pseudodistribution iff $\widetilde{\mathbb{E}}(1,x)(1,x)^\top$ is a PSD matrix with 1s on the diagonal. Now,

$$\begin{aligned}
\widetilde{\mathbb{E}} f_G(x) &= \widetilde{\mathbb{E}} x^\top L_G x \\
&= \widetilde{\mathbb{E}}\langle L_G, xx^\top\rangle \\
&= \left\langle L_G, \widetilde{\mathbb{E}} xx^\top\right\rangle.
\end{aligned}$$

Observe that the top eigenvalue of L_G is indeed $1 - O(1/n^2)$, and this eigenspace is 2-dimensional. It turns out that for an appropriate choice of v_1, v_2 in this eigenspace, we can ensure that $v_1 v_1^\top + v_2 v_2^\top$ does have only 1s on the diagonal (this is essentially a consequence of the fact that $\sin^2\theta + \cos^2\theta = 1$).

2.2. The positive semidefinite case

In the previous subsection, we looked at $\max_{x\in\{-1,1\}^n} x^\top L_G x$, where L_G is the (positive semidefinite) Laplacian of a graph. This is an example of quadratic optimization, where we are more generally interested in

$$\mathsf{opt}(B) \coloneqq \max_{x\in\{-1,1\}^n} x^\top B x$$

for some $n \times n$ matrix B.
In the case where $B \succeq 0$, it turns out that we can do something similar to what we had done in the max-cut algorithm.

Theorem 2.4 (Nesterov)**.** Let B be a positive semidefinite $n \times n$ matrix. Then,

$$\frac{\mathsf{opt}(B)}{c} - x^\top B x$$

has a degree 2 sum-of-squares certificate for $c = 2/\pi \approx 0.63$.

By the discussion in the previous section, this means as a corollary that we have a $\mathrm{poly}(n, 1/\epsilon)$-time $(2/\pi - \epsilon)$-approximation algorithm for any $\epsilon > 0$.

Definition 2.5. Let $M \in \mathbb{R}^{n\times n}$. Given $f : \mathbb{R} \to \mathbb{R}$, define $f[M] \in \mathbb{R}^{n\times n}$ by $f[M]_{ij} = f(M_{ij})$ for all i, j.

Proposition 2.6. Suppose M is a positive semidefinite matrix and f a function whose Taylor series has all positive Taylor coefficients and is uniformly convergent on $[-1, 1]$. Then, $f[M]$ is positive semidefinite.

The above is a corollary of the following simple observation.

Proposition 2.7 (Schur Product Theorem)**.** Let M, M' be positive semidefinite matrices. Denote by $M \circ M'$ the *Hadamard product* of M, M' defined by $(M \circ M')_{ij} = M_{ij}M'_{ij}$. Then, $M \circ M'$ is positive semidefinite.

Proof. Let $M = \sum_i \lambda_i v_i v_i^\top$ and $M' = \sum_j \lambda'_j v'_j v'^\top_j$. Using linearity of the Hadamard product,

$$M \circ M' = \sum_{i,j} \lambda_i\lambda'_j (v_i v_i^\top) \circ (v_j v_j'^\top) = \sum_{i,j} \lambda_i\lambda'_j (v_i \circ v'_j)(v_i \circ v'_j)^\top \succeq 0. \qquad \blacksquare$$

Proof of Proposition 2.6. Denote $[M]^2 = M \circ M$, and $[M]^i = [M]^{i-1} \circ M$ more generally. By the Schur Product Theorem, $[M]^i \succeq 0$ for all i. Therefore, $\sum c_i[M]^i \succeq 0$, that is, $(\sum c_i x^i)[M] \succeq 0$. $\blacksquare$

Proof of Nesterov. As in the previous subsection, let μ be a zero mean degree 2 pseudodistribution on $\{-1, 1\}^n$, g a normal random variable with zero mean and covariance matrix $\widetilde{\mathbb{E}}_\mu xx^\top$, and $\hat{x} \coloneqq \mathrm{sign}(g)$ distributed as μ'. A straightforward byproduct of the final part of the proof of Lemma 2.2 is that

$$\mathbb{E}_{\mu'}[\hat{x}_i\hat{x}_j] = \frac{2}{\pi}\arcsin \mathbb{E}[g_i g_j].$$

Therefore,

$$\begin{aligned}
\mathbb{E}_{\mu'}\hat{x}^\top B\hat{x} &= \sum_{i,j} B_{ij}\mathbb{E}[\hat{x}_i\hat{x}_j] \\
&= \sum_{i,j} B_{ij}\frac{2}{\pi}\arcsin[g_i g_j] \\
&= \frac{2}{\pi}\left\langle B, \arcsin\left[\mathbb{E}gg^\top\right]\right\rangle.
\end{aligned}$$

Recall that if $B, C \succeq 0$, then $\langle B, C \rangle \geq 0$. In particular,

$$\left\langle B, \arcsin\left[\mathbb{E} gg^\top\right] - \mathbb{E} gg^\top \right\rangle \geq 0,$$

so

$$\mathbb{E}_{\mu'} \hat{x}^\top B \hat{x} \geq \frac{2}{\pi} \langle B, \mathbb{E} gg^\top \rangle = \frac{2}{\pi} \widetilde{\mathbb{E}}_\mu x^\top B x.$$

The remainder of the proof is identical to that in the previous subsection. ■

2.3. The most general case

Let us next look at the case where B is any arbitrary matrix. First of all, we may assume that B is symmetric by looking at its symmetrization $(B + B^\top)/2$ instead. We may also assume that all diagonal entries of B are 0, since if we set $B = D + N$ where D is diagonal and N has all diagonal entries zero,

$$\max_{y \in \{-1,1\}^n} y^\top B y = \mathrm{Tr}(B) + \max_{y \in \{-1,1\}^n} y^\top N y.$$

We assume so for the remainder of this subsection.
We shall give an $O(\log n)$-approximation algorithm. First of all, is $\mathsf{opt}(B)$ even non-negative?

Proposition 2.8. Let $y \in [-1,1]^n$. Then, there exists $\hat{y} \in \{-1,1\}^n$ such that $\hat{y}^\top B y \geq y^\top B y$.

In particular, setting $y = 0$ implies that the desired value is non-negative.

Proof. Consider the random variable $\hat{y}$ on $\{-1,1\}^n$ which has $\hat{y}_i = 1$ with probability $(1+y_i)/2$ and 0 with probability $(1 - y_i)/2$, independently for different coordinates i. Note that $\mathbb{E} \hat{y}_i \hat{y}_j = y_i y_j$ for distinct i, j. Consequently,

$$\mathbb{E}_\mu \hat{y}^\top B \hat{y} = y^\top B y,$$

so the desideratum follows. ■

The above result is also true in the more general case where $\mathrm{Tr}(B) \geq 0$, but we do not require it.

We can in fact get a stronger lower bound than just the 0 in the above proposition.

Proposition 2.9.

$$\max_{y \in \{-1,1\}^n} y^\top B y \geq \frac{1}{n} \sum_{i,j} |B_{ij}|.$$

Proof. *** INCOMPLETE *** ■

The sum-of-squares proof we shall give is due to [Meg01, CW04].

Theorem 2.10. For sufficiently large n and $c = O(\log n)$,

$$\frac{\mathsf{opt}(B)}{c} - x^\top B x$$

has a degree 2 sum-of-squares certificate.

While we do not compute the exact constants exactly, the above is true for roughly $n > 60$ and $c = 4 \log n$.

Proof. As in the max-cut and PSD cases, we prove that given any pseudodistribution μ, there exists an (efficiently sampleable) distribution μ' on $\{-1,1\}^n$ such that $\mathbb{E}_{\mu'} \hat{x}^\top B \hat{x} \geq \frac{1}{O(\log n)} \widetilde{\mathbb{E}}_\mu x^\top B x$. By Proposition 2.8, it suffices to show this for a distribution on the continuous hypercube $[-1,1]^n$ instead of $\{-1,1\}^n$.
As before, choose $g \sim \mathcal{N}(0, \mathbb{E}_\mu x x^\top)$, so

$$\mathbb{E}[g^\top B g] = \widetilde{\mathbb{E}}_\mu [x^\top B x].$$

Make the mild assumption that $\mathbb{E}[g^\top B g] \geq 0$; the analysis of the general case is nearly identical. For a suitable constant C, we have that

$$\Pr[\|g\|_\infty > C \log n] \cdot \mathbb{E}[g^\top B g \mid \|g\|_\infty > C \log n] \leq \frac{1}{n^2} \mathbb{E}[g^\top B g], \text{ so}$$
$$\Pr[\|g\|_\infty \leq C \log n] \cdot \mathbb{E}[g^\top B g \mid \|g\|_\infty \leq C \log n] \geq \left(1 - \frac{1}{n^2}\right) \mathbb{E}[g^\top B g] \tag{2.4}$$

Our assumption that $\mathbb{E}[g^\top B g] \geq 0$ also implies that all the quantities above are non-negative. The final random variable $\hat{x}$ on the solid hypercube is defined by

$$\hat{x}_i = \begin{cases} \frac{g_i}{C\sqrt{\log n}}, & |g_i| \leq C\sqrt{\log n}, \\ \frac{g_i}{|g_i|}, & \text{otherwise.} \end{cases}$$

Then,

$$\begin{aligned} \mathbb{E}[\hat{x}^\top B x] &\geq \Pr[\|g\|_\infty \leq C\sqrt{\log n}] \cdot \mathbb{E}[\hat{x}^\top B \hat{x} \mid \|g\|_\infty \leq C\sqrt{\log n}] \\ &\geq \frac{1}{2C^2 \log n} \mathbb{E}[g^\top B g \mid \|g\|_\infty \leq C\sqrt{\log n}] \\ &\overset{(2.4)}{\geq} \frac{1}{O(\log n)} \mathbb{E}[g^\top B g] = \frac{1}{O(\log n)} \widetilde{\mathbb{E}}_\mu [x^\top B x], \end{aligned}$$

completing the proof. ∎

This above rounding is a specific case of the more general RPR^2 scheme of roundings that we mentioned earlier. In this, we "modify" $\widetilde{\mathbb{E}}_\mu x x^\top$ in some way (in the above method of Nesterov, we scale it down), sample a Gaussian with this modified covariance matrix, then do randomized rounding. In the setting of max-cut, we search over all RPR^2 roundings and output whichever returns the maximum cut value.

2.4. The bipartite support case

In this section, we shall look at the specific case where the *support* $\mathrm{supp}(B) \coloneqq \{\{i,j\} : B_{ij} \neq 0\}$ defines a bipartite graph (on vertex set $[n]$). We also assume that B is symmetric by symmetrizing it. The constant-factor approximation we shall describe is due to Alon and Naor [AN04].
Since $\mathrm{supp}(B)$ is bipartite, there exists some bipartition $X \cup Y$ of $[n]$ such that $B_{xx'} = B_{yy'} = 0$ for any $x, x' \in X$ and $y, y' \in Y$. Letting B' be the submatrix of B consisting of the X-rows and Y-columns (note that the submatrix consisting of the Y-rows and X-columns is then $B'^\top$) and splitting a given vector $x \in \mathbb{R}^n$ into two parts (x_X, x_Y), we have that

$$x^\top B x = 2 x_X^\top B' x_Y.$$

Therefore, our optimization problem is equivalent to the following: given an arbitrary $n \times n$ matrix B, determine

$$\max_{x,y \in \{-1,1\}^n} x^\top B y.$$

For simplicity, denote the above maximum by $\mathsf{opt}(B)$.

While the B' we looked at above in the bipartite setting need not be square, we can assume it is by appending appropriately many rows/columns filled with zeros.
Given norms $\|\cdot\|$ and $\|\cdot\|$ on $\mathbb{R}^n$, we have an associated *operator norm* on matrices defined by

$$\|A\| = \inf\{c \geq 0 : \|Ax\| \leq \|x\| \text{ for all } x \in \mathbb{R}^n\}.$$

When the first norm is the L^p and the second is the L^q, the operator norm is denoted the $\|\cdot\|_{q\to p}$ norm. That is,

$$\|A\|_{q\to p} \coloneqq \max_{\substack{x\in\mathbb{R}^n \\ x\neq 0}} \frac{\|Ax\|_p}{\|x\|_q}.$$

Now, note that for a given x,

$$\max_{y\in\{-1,1\}^n} x^\top By = \max_{y\in\{-1,1\}^n} \langle Bx, y\rangle = \|Bx\|_1,$$

since we can just choose the sign of y_i opposite to that of $(Bx)_i$. Further,

$$\begin{aligned}\|B\|_{\infty\to 1} &= \max_{\|x\|\le 1} \sum_i \left|\sum_j B_{ij}x_j\right| \\ &= \max_{|x_i|=1} \left|\sum_j B_{ij}x_j\right| \\ &= \max_{x\in\{-1,1\}^n} \|Bx\|_1 = \max_{x,y\in\{-1,1\}^n} x^\top By,\end{aligned}$$

where the second equality is because the summation is a convex function of the (x_i), so it is maximized at a vertex of the cube $[-1,1]^n$, namely at a point in $\{-1,1\}^n$. Therefore, our problem is equivalent to approximating $\|B\|_{\infty\to 1}$ for an arbitrary matrix $B\in\mathbb{R}^{n\times n}$.

Theorem 2.11. There exists a constant K_G such that

$$K_G\mathsf{opt}(B) - x^\top By$$

has a degree 2 sum-of-squares certificate.

Interestingly, the exact value of K_G is an open problem, and the interested reader may look up *Grothendieck's inequality* for more details. It is known that

$$1.57 \approx \frac{\pi}{2} \le K_G \le \frac{\pi}{2\ln(1+\sqrt{2})} \approx 1.78.$$

We shall give a proof due to Krivine in 1977 which yields the bound on the right.

Proof. This proof is slightly different from previous ones in terms of execution. We shall show that given a degree 2 pseudodistribution μ (on $\{-1,1\}^n$), there exists a real distribution μ' such that

$$\mathbb{E}_{\mu'}\hat{x}\hat{y}^\top = \frac{2\ln(1+\sqrt{2})}{\pi}\widetilde{\mathbb{E}}_\mu xy^\top.$$

Given this,

$$\begin{aligned}\mathbb{E}_{\mu'}\hat{x}^\top B\hat{y} &= \left\langle B, \mathbb{E}_{\mu'}\hat{x}\hat{y}^\top\right\rangle \\ &= \frac{2\ln(1+\sqrt{2})}{\pi}\left\langle B, \widetilde{\mathbb{E}}_\mu xy^\top\right\rangle = \frac{2\ln(1+\sqrt{2})}{\pi}\widetilde{\mathbb{E}}_\mu x^\top By,\end{aligned}$$

so we are done by methods similar to previous proofs. We shall first modify the "covariance matrix" of $\widetilde{\mathbb{E}}$ in some manner to get another matrix M' before creating the Gaussian used in rounding. Let $c = \ln(1+\sqrt{2})$. This matrix M' is defined by

$$M' = \begin{pmatrix} \sinh\left[c\widetilde{\mathbb{E}}_\mu xx^\top\right] & \sin\left[c\widetilde{\mathbb{E}}_\mu xy^\top\right] \\ \sin\left[c\widetilde{\mathbb{E}}_\mu yx^\top\right] & \sinh\left[c\widetilde{\mathbb{E}}_\mu yy^\top\right]\end{pmatrix}.$$

We shall explain the reasoning behind this choice in the proof. Then, we choose Gaussians $g,h\sim\mathcal{N}(0,M')$, and we finally define $\hat{x}=\operatorname{sign}(g)$ and $\hat{y}=\operatorname{sign}(h)$. To complete the proof, we need to show three things.

(a) $\mathbb{E}_{g,h}\hat{x}\hat{y}^\top = (2c/\pi)\widetilde{\mathbb{E}}_\mu xy^\top$. Recall that

$$\mathbb{E}\hat{x}\hat{y}^\top = \frac{2}{\pi}\arcsin[\mathbb{E}gh^\top].$$

We want this expression on the left to be some constant times $\widetilde{\mathbb{E}}_\mu xy^\top$. So, it makes sense to choose $\mathbb{E}gh^\top = \sin[c\widetilde{\mathbb{E}}_\mu xy^\top]$. This means that the bottom-left and bottom-right of our modified matrix should look like that of M'. While this might inspire us to choose sins on the diagonal blocks as well, doing so causes problems when it comes to PSD-ness, so we choose $\sinh$ instead. The reason for the precise choice of $\sinh$ is explained when we look at why $M' \succeq 0$.
Recalling the definition of $\mathbb{E}gh^\top$ from M',

$$\mathbb{E}[\hat{x}\hat{y}^\top] = \frac{2}{\pi}\arcsin[\mathbb{E}gh^\top] = \frac{2}{\pi}\arcsin[\sin[c\widetilde{\mathbb{E}}_\mu xy^\top]] = \frac{2\ln(1+\sqrt{2})}{\pi}\widetilde{\mathbb{E}}_\mu xy^\top.$$

(b) $M' \succeq 0$. We saw earlier in the proof of Proposition 2.6 that if M is PSD, so is $[M]^i$. It turns out, in fact, that if

$$M = \begin{pmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{pmatrix}$$

is PSD, so is

$$\begin{pmatrix} [M_{11}]^i & -[M_{12}]^i \\ -[M_{21}]^i & [M_{22}]^i \end{pmatrix}.$$

Indeed,

$$\begin{pmatrix} v \\ w \end{pmatrix}^\top \begin{pmatrix} [M_{11}]^i & -[M_{12}]^i \\ -[M_{21}]^i & [M_{22}]^i \end{pmatrix} \begin{pmatrix} v \\ w \end{pmatrix} = \begin{pmatrix} v \\ -w \end{pmatrix}^\top \begin{pmatrix} [M_{11}]^i & [M_{12}]^i \\ [M_{21}]^i & [M_{22}]^i \end{pmatrix} \begin{pmatrix} v \\ -w \end{pmatrix}$$

and the matrix on the right is PSD. Recalling that the Taylor series expansions of $\sin$ and $\sinh$ are given by

$$\sinh(x) = \sum_{n=0}^{\infty} \frac{1}{(2n+1)!}x^{2n+1} \text{ and}$$
$$\sin(x) = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}x^{2n+1},$$

it follows by a proof very similar to that of Proposition 2.6 that $M' \succeq 0$.

(c) $M'_{ii} = 1$ for each i. The value of c is forced by this requirement, and indeed $\sinh(\ln(1+\sqrt{2})) = 1$. ■

Krivine conjectured in his original paper that K_G is exactly equal to this quantity. Later however, it was shown [BMMN11] that K_G is strictly less than this.

Here, we looked at matrices with bipartite support. More generally, if the support of the matrix is some graph G, [AMMN06] give an $O(\log(\chi(G)))$-approximation algorithm and also show it is impossible to get an $o(\log(\omega(g)))$-approximation algorithm – recall that $\chi(G)$ and $\omega(G)$ are the chromatic number and clique number of a graph G respectively.

§3. Higher degree sum-of-squares

3.1. Approximating conductance

In Section 2.1, we looked at the NP-hard problem of max-cut. Before moving to the rest of this section where we look at conductance, let us look at the far simpler min-cut problem. The reader might know that this problem can be solved in polynomial time using the Ford-Fulkerson max-flow algorithm. Before moving to the main problem of this subsection, let us overkill min-cut by giving a randomized algorithm via SoS.
Min-cut and conductance will be our first example of degree 4 sum-of-squares. The main reason for the degree 4 requirement here is the following.

Theorem 3.1 (Squared Triangle Inequality)**.** For indeterminates $a, b, c \in \{-1, 1\}$,

$$(a-c)^2 \leq (a-b)^2 + (b-c)^2$$

has a degree 4 sum-of-squares certificate.

Proof. We have

$$\begin{aligned}\frac{1}{2}\left((a-b)^2 + (b-c)^2 - (a-c)^2\right) &= b^2 - ab - bc + ac \\ &= (1-bc)(1-ab) \\ &= \frac{1}{4}(b^2+c^2-2bc)(a^2+b^2-2ab) = \left(\frac{(b-c)(a-b)}{2}\right)^2.\end{aligned}$$

■

While we will not use it, we also state the following, which can be proved by considering a Gaussian with the same first two moments (like in Section 2) and using the fact that the L^2 metric (on $\mathbb{R}$) is a metric.

Theorem 3.2. For any degree 2 pseudodistribution μ,

$$\sqrt{\widetilde{\mathbb{E}}_\mu (x_i - x_k)^2} \leq \sqrt{\widetilde{\mathbb{E}}_\mu (x_i - x_j)^2} + \sqrt{\widetilde{\mathbb{E}}_\mu (x_j - x_k)^2}.$$

For the remainder of this subsection, let G be a graph with vertex set $[n]$, and let $\widetilde{\mathbb{E}}$ be any degree 4 pseudodistribution. We continue to denote by f_G the function in eq. (2.1). Our proof strategy for the min-cut problem will be to give a distribution μ' such that $\mathbb{E}_{\mu'} f_G \leq \widetilde{\mathbb{E}}_\mu f_G$. For any $i, j \in [n]$, denote

$$D(i,j) = \widetilde{\mathbb{E}}_\mu \frac{1}{4}(x_i - x_j)^2$$

and for non-empty $A \subseteq [n]$, $D(A,i) = D(i,A) = \min_{j \in A} D(i,j)$. Because μ is a degree 2 pseudodistribution (degree 4 in fact), $D(i,A) \geq 0$ for any i, A and it is bounded from above by 1. Consider the "line embedding" of the vertices $[n]$ on the interval $[0,1]$ defined by $i \mapsto D(i,1)$. μ' is defined by uniformly randomly choosing $t \in [0,1]$, and outputting the cut $\{i \in [n] : D(i,1) \leq t\}$. An edge $\{i,j\}$ is cut with probability

$$|D(j,1) - D(i,1)| = \frac{1}{4}\left|\widetilde{\mathbb{E}}_\mu (x_i - x_1)^2 - \widetilde{\mathbb{E}}_\mu (x_j - x_1)^2\right| \leq \frac{1}{4}\widetilde{\mathbb{E}}_\mu (x_i - x_j)^2 = D(i,j),$$

where we have used the fact that μ is degree 4 for the squared triangle inequality. Summing over all edges,

$$\mathbb{E}_{\mu'} f_G \leq \sum_{ij \in E} D(i,j) = \widetilde{\mathbb{E}}_\mu f_G.$$

Note that this proof works out more generally in the scenario where we have $D(i,A)$ for some set A instead. To ensure non-triviality, we choose $t \in [0, \max_j D(1,j)]$ instead of $t \in [0,1]$.

Let us now get to a more non-trivial problem.

Definition 3.3. Given a d-regular graph $G = (V, E)$ with n vertices and a non-empty subset $S \subsetneq V$, the *conductance* or *normalized cut* of S is

$$\Phi_G(S) = \frac{E(S, V \setminus S)}{(d/n)|S||V \setminus S|}.$$

The denominator can be thought of as the expected number of edges between S and S^c if the graph is a Erdős-Rényi random graph with edge probability d/n.

Definition 3.4. Given a graph $G = (V, E)$ with n vertices, the *conductance* or *expansion* of G is

$$\Phi_G = \min_{\varnothing \neq S \subsetneq V} \Phi_G(S).$$

Conductance is very closely related to the rate of convergence of the standard random walk on the graph – a low conductance implies that there is a "tight bottleneck" somewhere in the graph where the walk can get stuck. Indeed, if we remove the d/n in the denominator, the conductance of a set is just the probability of exiting the set if we start a random walk at a uniformly random point in it.

The problem of determining the conductance of a graph (and possibly a cut that attains it) is called the uniform sparsest cut problem. It is not too difficult to show that this is NP-hard using a reduction from max-cut. In fact, [CKK+06] show that the Unique Games Conjecture implies that any constant-factor approximation for Φ_G is NP-hard! It is quite interesting how min-cut is in P, max-cut is NP-hard but we can get a good constant-factor approximation, but even that is not possible for sparsest-cut (assuming the UGC).
It is quite easy to see that

$$\Phi_G = \min_{x \in \{-1,1\}^n} \frac{f_G(x)}{(d/4n)\sum_{i,j}(x_i - x_j)^2} = \min_{x \in \{-1,1\}^n} \frac{f_G(x)}{(d/n) f_{K_n}(x)}.$$

Minimizing this directly seems impossible using the sum-of-squares method since we are looking at a rational function that is not a polynomial. So, we instead try to get a "large" α such that

$$f_G(x) - \alpha \frac{d}{n} f_{K_n}(x)$$

has a sum-of-squares certificate.

Theorem 3.5 (Cheeger's Inequality)**.** There is a degree 2 sum-of-squares certificate for

$$f_G(x) - \frac{\Phi_G^2}{2} \cdot \frac{d}{n} f_{K_n}(x).$$

Furthermore, this value of α is tight up to constants for degree 2 SoS – with the example used being the cycle again. We omit the proof of this (standard) inequality; the reader may consult
In [cite Leighton-Rao 88], Leighton-Rao gave an $O(\log n)$-approximation using linear programming. In the setting where $\Phi_G = O(1/\log n)$, this improves on Cheeger's inequality. We shall study the Arora-Rao-Vazirani (ARV) algorithm [cite ARV04], which gives an $O(\sqrt{\log n})$-approximation, based on degree 4 sum-of-squares.
In Section 2, our analysis was completely local in the sense that we analyzed what happens to each $(x_i - x_j)^2$ term completely independent of the others. It might not be too ambitious to hope that some sort of global analysis is

possible, wherein we show that if one term is small, then others must be large, thus forcing the entire summation to be large. Of course, our remarks before Proposition 2.3 make this unlikely, at least in the setting of max-cut.
On the other hand, we shall use global analysis in the ARV algorithm. Even before ARV, it has helped in better approximations to vertex cover, graph coloring, max-cut gain etc.

Theorem 3.6 (ARV)**.** Let G be a d-regular graph with n vertices. There is a degree 4 sum-of-squares certificate for

$$f_G(x) - \frac{\varphi_G}{\Theta(\sqrt{\log n})} \cdot \frac{d}{n} f_{K_n}(x).$$

Furthermore, given any degree 4 pseudodistribution μ on $\{-1,1\}^n$, it is possible to find in polynomial time a set $S \subseteq V$ such that

$$\varphi_G(S) \leq O(\sqrt{\log n}) \cdot \frac{\widetilde{\mathbb{E}}_\mu f_G}{(d/n)\widetilde{\mathbb{E}}_\mu f_{K_n}}.$$

Like in prior proofs, we shall show that given any degree 4 pseudodistribution μ, there exists a distribution μ' such that

$$\frac{\mathbb{E}_{\mu'} f_G}{\mathbb{E}_{\mu'} f_{K_n}} \leq O(\sqrt{\log n}) \cdot \frac{\widetilde{\mathbb{E}}_\mu f_G}{\widetilde{\mathbb{E}}_\mu f_{K_n}}.$$

We have a distribution μ' such that $\mathbb{E}_{\mu'} f_G \leq \widetilde{\mathbb{E}}_\mu f_G$, but we would also like to show that $\mathbb{E}_{\mu'} f_{K_n} \geq C \cdot \widetilde{\mathbb{E}}_\mu f_{K_n}$. Denoting by $\mathbb{1}(\hat{x})$ the set of vertices where $\hat{x} = 1$, we have that $\mathbb{E}_{\mu'} f_{K_n} = |\mathbb{1}(\hat{x})|(n - |\mathbb{1}(\hat{x})|)$.

Definition 3.7. $A, B \subseteq V$ are said to be *large* Δ*-separated sets* if for all $i \in A, j \in B$, $D(i,j) \geq \Delta$ and $|A||B| = \Omega(n^2)$.

If we manage to find large Δ-separated sets, we can do the rounding (similar to the min-cut procedure) using $D(j, A)$, so

$$\mathbb{E}_{\mu'} f_{K_n} = \sum_{i,j} \mathbb{E}_{\mu'} \frac{1}{4}(x_i - x_j)^2 \geq \sum_{i \in A, j \in B} \mathbb{E}_{\mu'} \frac{1}{4} D(j, A) \geq \frac{\Delta}{4}|A||B| = \Omega(\Delta n^2) \geq \Omega(\Delta)\widetilde{\mathbb{E}}_\mu f_{K_n}.$$

Therefore, if we manage to find large Δ-separated sets, we immediately get an $O(1/\Delta)$-approximation algorithm.

Theorem 3.8 (Global Structure Theorem)**.** Let G be a d-regular graph and μ a degree 4 pseudodistribution. Suppose that $\sum_{i,j} D(i,j) = \Omega(n^2)$. Then, there exist A, B that can be found in polynomial time that are $\Omega(1/\sqrt{\log n})$-separated.

Let us first give a proof of the Leighton-Rao $O(\log n)$-approximation algorithm, which proves the above for $\Omega(1/\log n)$-separation instead. Their original Leighton-Rao proof was based on linear programming, but we give one based on the above sum-of-squares idea.

Proof of weaker Global Structure Theorem. Like before, assume wlog that $\widetilde{\mathbb{E}}_\mu x = 0$, and let $g \sim \mathcal{N}(0, \widetilde{\mathbb{E}}_\mu x x^\top)$. Let

$$A^{(0)} = \{i : g_i \leq -1\} \text{ and } B^{(0)} = \{i : g_i \geq 1\}.$$

Because $\mathbb{E} g_i^2 = 1$ and $\mathbb{E} g_i = 0$, these two sets have size $\Omega(n)$ in expectation.
However, this is not enough, because it is possible that the probability that *both* sets are large is small. To fix this, we can show without much difficulty that $\Pr[g_i \leq -1 \text{ and } g_j \geq 1] \geq C D(i,j)$ for some constant C using arguments from

earlier sections. Since $\sum_{i,j} D(i,j) = \Omega(n^2)$, we can use linearity of expectation to conclude that $\mathbb{E}|A^{(0)}||B^{(0)}| = \Omega(n^2)$. Now, while $A^{(0)}$ and $B^{(0)}$ are well-separated for the draw of the Gaussian that is used to define them, we care about the separation in expectation. That is, while $g_j - g_i \geq 2$ for $i \in A^{(0)}, j \in B^{(0)}$, we want that $\mathbb{E}(g_i - g_j)^2 \geq \Delta$ for $i \in A, j \in B$. We would like to show that if some coordinates appear in $A^{(0)}, B^{(0)}$, then with good probability they are "good" pairs in the sense of also being Δ-separated.
If we have for some pair i, j that $\mathbb{E}(g_i - g_j)^2 \leq \Delta$, then standard concentration inequalities show that $\Pr[g_j - g_i \geq 2] \leq e^{-\Omega(1/\Delta)}$. When $\Delta = O(1/\log n)$, we can use a union bound argument to extend this to all pairs i, j. ■

Consider the graph H on vertex set $[n]$ with ij adjacent iff $D(i,j) \leq \Delta$. Our goal is to find $\Omega(n)$-sized sets A, B such that there are no edges between A and B in H. Such pairs are typically called *vertex separators*.
The $A^{(0)}$ and $B^{(0)}$ we have now are random sets such that $(g_j - g_i) \geq 2$ for $i \in A^{(0)}, j \in B^{(0)}$ and $\mathbb{E}|A^{(0)}||B^{(0)}| = \Omega(n^2)$. The issue that might require us to throw away vertices from $A^{(0)}$ and $B^{(0)}$ is when for some two vertices, $\mathbb{E}(g_j - g_i)^2 \leq \Delta$. One cause for this might be if in our draw, there is some vertex j whose value g_j is abnormally large, which results in it contributing to many "bad" edges. To account for this, in the ARV result, we remove such vertices only once using a matching.
Before the algorithm begins, deterministically fix an ordering on the vertices. Greedily find a maximal matching M in $E(H) \cap (A^{(0)} \times B^{(0)})$, and then set $A = A^{(0)} \setminus V(M)$ and $B = B^{(0)} \setminus V(M)$. Note that this A and B are indeed Δ-separated – were they not, we would be able to make the matching larger by adding an edge. For ease of notation, direct all edges in M from $A^{(0)}$ to $B^{(0)}$.
We would like to show that M is small, so not too many vertices are removed from $A^{(0)}$ and $B^{(0)}$ to get A, B. To prove this, we shall show that

Lemma 3.9. It holds that

$$O(\sqrt{\log n}) \geq \mathbb{E} \max_{i,j \in [n]} (g_j - g_i) \geq \frac{\Omega(1)}{\Delta} \cdot \left(\frac{\mathbb{E}|M|}{n}\right)^3.$$

In particular, on setting $\Delta = \Theta(1/\sqrt{\log n})$, $|M|$ is $O(n)$, so $|A||B| = \Omega(n^2)$, completing the proof of the Global Structure Theorem.

Proof. The left-hand-side is proved rather simply, using the fact that if $(Z_1, Z_2, \ldots, Z_t)$ are jointly Gaussian, then

$$\operatorname{Var} \max_{i \leq t} Z_i \leq O(1) \max_{i \leq t} \operatorname{Var} Z_i. \tag{3.1}$$

The variable $\max Z_i$ is actually a subgaussian distribution around its mean, which is around $\sqrt{\log t}$ (this may be proved using a Hoeffding bound argument). In our context, we have n^2 Gaussians $(g_j - g_i)$, and this is around $O(\sqrt{\log n})$ with good probability.

The more difficult part of the inequality is the lower bound. Let $H^k(i)$ be the vertices at most k steps away of i in the graph H, and $\gamma_i^k = \max_{j \in H^k(i)} g_j - g_i$. The idea is that we shall "chain" together edges in the matching, each of which increases the difference $g_j - g_i$ of the terminal edges in the path by 2, such that the final difference is quite large. Let $\phi_k = \sum_i \mathbb{E}\gamma_i^k$. We shall try to show $\phi_\cdot$ becomes quite large. More precisely, we claim that

$$\phi_{k+1} - \phi_k \geq \mathbb{E}|M| - O(n) \max_{\substack{i \in [n] \\ j \in H^{k+1}(i)}} (\mathbb{E}(g_j - g_i)^2)^{1/2}. \tag{3.2}$$

Given this, let us prove the lower bound. Note that for any vertices i, j which are k steps apart in H, we have $\mathbb{E}(g_i - g_j)^2 \leq k\Delta$ by the squared triangle inequality. Consequently, using (3.2),

$$\phi_{k+1} - \phi_k \geq \mathbb{E}|M| - O(n)\sqrt{k\Delta}.$$

Set $k_0 = \frac{c}{\Delta}\left(\frac{\mathbb{E}|M|}{n}\right)^2$, for some constant c to be fixed later. For $k \leq k_0$, we have that

$$\phi_{k+1} - \phi_k \geq 2\mathbb{E}|M| - O(n)\sqrt{\Delta \cdot \frac{c}{\Delta}\left(\frac{\mathbb{E}|M|}{n}\right)^2} \geq \mathbb{E}|M|,$$

where we set c appropriately to get the second inequality. In particular, $\phi_{k_0} \geq k_0 \mathbb{E}|M|$. Noting that $\max_{i,j\in[n]}(g_j - g_i) \geq \phi_{k_0}/n$, we get that

$$\max_{i,j\in[n]}(g_j - g_i) \geq \Omega\left(\frac{k_0}{n}\mathbb{E}|M|\right) = \frac{\Omega(1)}{\Delta}\left(\frac{\mathbb{E}|M|}{n}\right)^3$$

as desired.

Now, to conclude the proof, let us prove eq. (3.2). First off, we have that if $ij \in E(H)$, $H_k(j) \subseteq H_{k+1}(i)$ so

$$\gamma_j^{k+1} \geq \gamma_i^k + (g_j - g_i).$$

In particular, if ij is an edge in the matching M, then by definition, $\gamma_j^{k+1} \geq \gamma_i^k + 2$. Now, for each vertex i, set

$$L_i = \begin{cases} 1, & i \text{ has an outgoing edge in } M, \\ 0, & i \text{ has an incoming edge in } M, \\ 1/2, & i \text{ is unmatched in } M \end{cases}$$

and $R_i = (1 - L_i)$. Because $H^{k+1}(\cdot) \supseteq H^k(\cdot)$, we have that $\gamma_\cdot^{k+1} \geq \gamma_\cdot^k$ and so,

$$\sum_i L_i \gamma_i^{k+1} \geq \sum_i R_i \gamma_i^k + 2|M|$$

and

$$\sum_i \mathbb{E}L_i \gamma_i^{k+1} \geq \sum_i \mathbb{E}R_i \gamma_i^k + 2\mathbb{E}|M|. \tag{3.3}$$

Note that for a specific draw g of the gaussians, the matching $M(g)$ has all the edges in $M(-g)$ but reversed (due to the greedy nature when defining M). Therefore, the probability that a vertex has an incoming edge in M is the same as the probability that a vertex has an outgoing edge in the perfect matching. This implies that $\mathbb{E}L_i = \mathbb{E}R_i = (1/2)$. We are almost done, barring the issue that the expectation of the product above is not equal to the product of the expectation. The difference between the two is bounded using Cauchy-Schwarz without too much difficulty as

$$\begin{aligned}
\left|\mathbb{E}L_i\gamma_i^{k+1} - \mathbb{E}L_i\mathbb{E}\gamma_i^{k+1}\right| &= \left|\mathbb{E}(L_i - \mathbb{E}L_i)(\gamma_i^{k+1} - \mathbb{E}\gamma_i^{k+1})\right| \\
&\leq \sqrt{\mathbb{E}(L_i - \mathbb{E}L_i)^2}\sqrt{\mathbb{E}(\gamma_i^{k+1} - \mathbb{E}\gamma_i^{k+1})^2} \\
&\leq \sqrt{\operatorname{Var}\gamma_i^{k+1}} \\
&\overset{(3.1)}{\leq} O(1)\sqrt{\max_{j\in H^{k+1}(i)}\mathbb{E}(g_j - g_i)^2},
\end{aligned}$$

with a similar inequality for R_i instead of L_i. Substituting this back in Equation (3.3), we get that

$$\begin{aligned}
\phi^{k+1} &= \sum_i \mathbb{E}\gamma_i^{k+1} \\
&= 2\sum_i \mathbb{E}L_i\mathbb{E}\gamma_i^{k+1} \\
&\geq 2\sum_i \mathbb{E}L_i\gamma_i^{k+1} - O(1)\sum_i \sqrt{\max_{j\in H^{k+1}(i)}\mathbb{E}(g_j - g_i)^2} \\
&\geq 2\sum_i \mathbb{E}R_i\gamma_i^k + 2\mathbb{E}|M| - O(1)\sum_i \max_{j\in H^{k+1}(i)}\sqrt{\mathbb{E}(g_j - g_i)^2} \\
&\geq 2\sum_i \mathbb{E}R_i\mathbb{E}\gamma_i^k + 2\mathbb{E}|M| - O(1)\sum_i \max_{j\in H^{k+1}(i)}\sqrt{\mathbb{E}(g_j - g_i)^2} \\
&\geq \phi^k + 2\mathbb{E}|M| - O(n)\max_{\substack{i\in[n] \\ j\in H^{k+1}(i)}}\sqrt{\mathbb{E}(g_j - g_i)^2}.
\end{aligned}$$

■

3.2. The Unique Games Conjecture

3.2.1. Introduction

Definition 3.10 (2-Constraint Satisfaction Problem)**.** In a 2-*CSP*, we have n variables $(x_i)_{i=1}^n$, which take values in a finite alphabet $[q]$ and m constraints $((C_i, S_i))_{i=1}^m$, where each C_i is a pair of variables (x_{i_1}, x_{i_2}), and $S_i \subseteq [q]^2$. A certain constraint (C_i, S_i) is said to be *satisfied* by a certain assignment of the variables if the corresponding pair is contained in S_i. The algorithmic goal of a 2-CSP is to find an assignment that maximizes the number of satisfied assignments.

In our setting, q is typically a constant. An example of a (boolean) 2-CSP is the max-cut problem, where for each edge ij in the graph, we have the constraint $(x_i, x_j) \in \{(0,1),(1,0)\}$. An example of a non-boolean 2-CSP is max 3-coloring, where we try to find a coloring of the vertices that maximizes the number of "good" edges which have end-vertices of different colours – try to encode this as a CSP!

Definition 3.11 (Promise Problem)**.** For $0 \leq s \leq c \leq 1$, the (c, s) promise problem takes as input a 2-CSP instance, and the goal is to decide whether

1. there exists an assignment that satisfies a $\geq c$ fraction of constraints, or
2. every assignment satisfies a $\leq s$ fraction of the constraints.

The quantities c and s are typically referred to as *completeness* and *soundness.*

When the input is a general 2-CSP, we refer to this problem as (c, s)-2CSP. We use similar notation throughout, for example in restricted classes of 2-CSPs.
It is clear that if we have a (s/c)-approximation algorithm for a CSP, then the (c, s)-version of this problem is easy.

For example, a $(1, 1 - 1/m)$-2CSP could be used to check the satisfiability of a CNF. For $q \geq 3$, $(1, 1 - 1/m)$-2CSP is NP-hard.

Definition 3.12 (Unique 2-CSP)**.** A q-sized alphabet 2-variable constraint (C, S) is said to be *unique* if for every possible assignment to one of the two variables, there is exactly one satisfying assignment to the other variable. A 2-CSP is said to be a *unique* 2-*CSP* or *unique game* if all its constraints are unique.

A unique constraint is essentially just a permutation π of $[q]$, where the set S is just $\{(i, \pi(i)) : i \in [q]\}$.
Max-Cut is an example of a boolean unique game, while MAX2SAT is not. A non-boolean unique game is MAX2LIN, where q is a prime and the constraints are linear equations like $x_i \pm x_j \equiv a_{ij} \pmod q$.

Given that $(1, 1 - 1/m)$-2CSP is NP-hard for $q \geq 3$, the following may be slightly surprising.

Theorem 3.13 (Propagation)**.** There is a polynomial time algorithm for $(1, 1 - 1/m)$-UG.

Proof. Let G be the graph of all pairs that appear in constraints. Assume wlog that G is connected; if it is not, we can apply the following argument separately on connected components. Start an arbitrary vertex u, and give it the

assignment 1. Due to uniqueness, this single assignment propagates to an assignment on all vertices in u. If we get conflicting assignments at some point, then there is no satisfying assignment which assigns 1 to u. We can then repeat this by varying the assignment for u to determine if there is a satisfying assignment. ■

Given the previous, the following may be very surprising.

Conjecture (Unique Games Conjecture)**.** For any $\epsilon > 0$, for sufficiently large q_ϵ, $(1-\epsilon, \epsilon)$-UG is NP-hard.

The conjecture was born when trying to show "hardness of approximation" results, which claim that even getting a good approximation of certain quantities is NP-hard. For example, recall how in Section 2.1, we had said that the Unique Games Conjecture would imply that getting a $(\alpha_{\text{GW}} + \epsilon)$-approximation of the max-cut is NP-hard. The real advent of these results was with the PCP Theorem, an implication of which is the following.

Theorem 3.14. For some constant $c > 0$, $(1, 1-c)$-3SAT is NP-hard.

In the original proof of the above, the constant c was incredibly tiny. Later, this was improved by Ran Raz [Raz98] in the parallel repetition theorem. Finally, Håstad [Hå01] proved the best possible result, showing that for any $\epsilon > 0$, $(1, 7/8+\epsilon)$-3SAT is NP-hard; there is a simple (but clever) $7/8$-approximation algorithm. In the same paper, Håstad also proved that $(1, 1/2+\epsilon)$-3LIN is NP-hard; we shall return to this later in Section 4.
This provided a more general system for proving hardness of approximation results, including many other CSPs. However, questions regarding the hardness of approximating problems like MAX-CUT and MAX2LIN remained elusive. Recall that for the former, Proposition 2.3 implies that $(1-\epsilon, 1-\sqrt{\epsilon})$-CUT is in P. VERTEX-COVER was another problem that seemed difficult to approximate – a simple algorithm gives a 2-approximation, but we were unable to do better on the algorithmic or hardness fronts.

3.2.2. A brief history of unique games

The Unique Games Conjecture was proposed by Subhash Khot [Kho02] in 2002, and connected it to one of the three problems mentioned above.

Theorem 3.15 (Khot)**.** If the Unique Games Conjecture is true, for all $\epsilon > 0, 1 \geq t \geq (1/2)$, $(1-\epsilon, 1-\epsilon^t)$-2LIN is NP-hard.

In 2003, Khot-Regev [KR08] connected it to VERTEX-COVER.

Theorem 3.16 (Khot-Regev)**.** If the Unique Games Conjecture is true, for all $\epsilon > 0$, $(2-\epsilon)$-VERTEXCOVER is NP-hard.

An alternate way of phrasing this is as follows. Supposing the Unique Games Conjecture is true and someone manages to synthesize a $(2-\epsilon)$-approximation algorithm for VERTEX-COVER, then P = NP, so we can in fact solve VERTEX-COVER exactly!
In 2004, Khot-Kindler-Mossell-O'Donnell [KKMO07] connected it to MAX-CUT, as we mentioned in Section 2.1.

Theorem 3.17 (Khot-Kindler-Mossell-O'Donnell)**.** For $\epsilon > 0$, $(1-\rho_{\text{GW}}, \alpha_{\text{GW}} + \epsilon)$-CUT is NP-hard.

This paper gave some very surprising connections between Gaussian rounding of CSPs and 2-CSPs! A bit later, O'Donnell-Wu gave a strengthening of this, to the analogue of Proposition 2.3, showing we cannot do better than RPR^2 rounding either! Finally, in 2008, the following was showed by Raghavendra [Rag08].

Theorem 3.18 (Raghavendra)**.** For every CSP, there exists a natural SDP (the analogue of degree 2 sum-of-squares) and a natural rounding (the analogue of RPR^2) that, assuming the Unique Games Conjecture, is optimal.

Now, setting implications aside, is the Unique Games Conjecture true?

In Khot's original paper [Kho02], an $(1/q)$-approximation algorithm was given. More precisely, they showed that $(1-\epsilon, 1-O(q^2\epsilon^{1/5}\sqrt{\log 1/\epsilon}))$-UG is solvable in polynomial time; this is very good in the small ϵ regime. There is a long line of work improving on this, and today, the best known algorithm is due to Charikar-Makarychev-Makarychev in 2007 [CMM06], where they gave an optimal polynomial time algorithm for $(1-\epsilon, 1-O(\sqrt{\epsilon \log q}))$-UG. This algorithm is optimal in the sense that if the Unique Games Conjecture is true, we cannot do any better! More concretely, [KKMO07] also showed that if the Unique Games Conjecture is true, then for any $\epsilon > 0$, $(1-\epsilon, 1-\sqrt{\frac{2}{\pi}}\sqrt{\epsilon \log q} + \epsilon)$-UG is NP-hard! Improving the [CMM06] algorithm just a little bit would disprove the Unique Games Conjecture. All the above results are algorithms using degree 2 sum-of-squares (or rather, an analogue of what we have seen so far in a non-boolean setting).

On the other hand, a proof of the Unique Games Conjecture also seems within reach! In 2010, Arora-Barak-Steurer [ABS15] showed that for all q, ϵ, there exists a $2^{q^2 n^{O(\epsilon^{1/3})}}$-time algorithm to find a $(1/2)$-satisfying assignment for any $(1-\epsilon)$-satisfiable instance of UG. That is, $(1-\epsilon, 1/2)$-UG has a $2^{q^2 n^{O(\epsilon^{1/3})}}$-time algorithm. This is better than the naïve exponential time $2^{O(n)}$ algorithm.
Consider the following, proposed by Impagliazzo-Kabanets-Wigderson [IKW02] in 2002. This can be thought of as a stronger version of P $\neq$ NP.

Conjecture (Exponential Time Hypothesis)**.** 3-SAT does not have a $2^{o(n)}$-algorithm.

The ETH is easily seen to imply that 3-coloring doesn't have a $2^{O(n)}$ algorithm. If it was able to get a $2^{n^{o(1)}}$ algorithm for $(1-\epsilon, 1/2)$-UG, assuming the ETH would imply that the UGC is false. Indeed, if the UGC were true instead, there is a $\mathrm{poly}(n)$ algorithm that reduces a 3SAT instance to an instance of UG. Using the $2^{n^{o(1)}}$ algorithm on top of this yields a $2^{n^{o(1)}}$ algorithm for 3SAT, contradicting ETH.
We also have that assuming the ETH and the UGC, the Arora-Barak-Steurer algorithm shows that no reduction from 3SAT to UGC can have an instance size blow-up of less than $O(n^{\epsilon^{-1/3}})$.
Recently in 2018, Dinur-Khot-Kindler-Minzer-Safra [DKK+18] settled the 2-to-2 Games Conjecture, which is a weaker version of the Unique Games Conjecture, wherein instead of "unique" constraints where fixing a variable leaves precisely *one* choice for the other variable, there are now *two* possibilities. A consequence of this is that $(1/2-\epsilon, \epsilon)$-UG is NP-hard.

3.3. Global correlation rounding

We have extensively looked at Gaussian rounding, which works for degree 2 pseudodistributions. Later, we combined this with the squared triangle inequality to get something for degree 4 pseudodistributions. In this section, we shall study a more general scheme called global correlation rounding that works for higher degree pseudodistributions. This is also the idea behind the Arora-Barak-Steurer algorithm mentioned in the previous section.
Our running example over this section will be the max-cut problem over a certain restricted class of graphs.

Recall the normalized adjacency matrix (random walk matrix) A of a d-regular graph G on $[n]$. Let $1 = \lambda_1 \geq \cdots \geq \lambda_n \geq -1$ be the eigenvalues of A. Recall that G is said to be a combinatorial expander if the conductance $\Phi_G \geq \delta$ for some constant δ, and a spectral expander if $\lambda_2 \leq 1-\delta$. A direct consequence of Cheeger's Inequality is that these two notions are equivalent, with $\Phi_G \geq \delta$ implying that $\lambda_2 \leq 1 - O(\delta^2)$.
An example of an expander is a random d-regular graph. We also have more explicit examples such as *configuration models*, where $\lambda_2 = \frac{2\sqrt{d-1}}{d} + o(1)$ (this is interesting because of the Alon-Boppana bound in extremal graph theory).

Definition 3.19. Let G be a d-regular graph with eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. The *$\rho$-threshold rank* of G $\mathrm{rank}_\rho(G)$ is the number of eigenvalues that are at least ρ.

In particular, on expanders, $\mathrm{rank}_{1-\epsilon}(G) = 1$ for sufficiently small ϵ. The threshold rank ends up being related to some notion of graph expansion, but we shall not study this.

Theorem 3.20. Let G be a d-regular graph on $[n]$ and set $r = \mathrm{rank}_\delta(G)/\delta^4$. Given a degree $r+2$ pseudodistribution μ, we can find in polynomial time a distribution μ' such that

$$\mathbb{E}_{\mu'} f_G \geq \widetilde{\mathbb{E}}_\mu f_G - m \cdot O(\sqrt{\delta}).$$

The "restricted class of graphs" we mentioned is that of graphs with bounded threshold rank. This gives us a $n^{O(r)}$ time algorithm to compute an additive $O(\sqrt{\delta})$-approximation of the max-cut. Alternatively, this gives us an algorithm to find an $1 - O(\sqrt{\delta})$ multiplicative approximation of the max-cut – this is a consequence of the fact that the max-cut is at least $m/2$. In particular, this gives us a polynomial time algorithm for max-cut on expanders.

Definition 3.21 (Marginal pseudodistribution)**.** Let μ be a pseudodistribution on $\{-1,1\}^n$. For any $S \subseteq [n]$, the marginal pseudodistribution $\mu|_S : \{-1,1\}^S \to \mathbb{R}$ is defined by

$$\mu|_S(y) = \sum_{x \colon x|_S = y} \mu(x).$$

The following observations near-immediately follow from the definition.

Proposition 3.22. Let μ be a degree r pseudodistribution on $\{-1,1\}^n$. Then,

(a) For any $U \subseteq S$, $\widetilde{\mathbb{E}}_\mu x_U = \widetilde{\mathbb{E}}_{\mu|_S} x_U$.

(b) For any function f of degree r that depends only on variables in S, $\widetilde{\mathbb{E}}_\mu f = \widetilde{\mathbb{E}}_{\mu|_S} f$.

(c) Let μ be a degree r pseudodistribution on $\{-1,1\}^n$. Let $S \subseteq [n]$ with $|S| \leq r/2$. Then, $\mu|_S$ is an actual probability distribution. For such S, we call this distribution the *local distribution* of μ on S.

(c) above is essentially a consequence of Proposition 1.2.

Definition 3.23 (Reweighting)**.** Let μ be a degree r pseudodistribution. Suppose p is polynomial of degree $r' \leq r$ that has a sum-of-squares certificate, such that $\widetilde{\mathbb{E}}_\mu p > 0$ (without this assumption, we only have non-negativity). Then, μ', the *reweighting* of μ by p, is defined by

$$\mu'(x) = \frac{\mu(x)p(x)}{\widetilde{\mathbb{E}}_\mu p}.$$

Defining μ' as above, we have for any other polynomial f that

$$\widetilde{\mathbb{E}}_{\mu'} f = \frac{\widetilde{\mathbb{E}}_\mu pf}{\widetilde{\mathbb{E}}_\mu p}.$$

Proposition 3.24. Let μ be a degree r pseudodistribution and p a sum-of-squares polynomial of degree at most r' with $\widetilde{\mathbb{E}}_\mu p > 0$. Then, μ', the reweighting of μ by p, is a degree $(r - r')$ pseudodistribution.

Proof. We clearly have $\widetilde{\mathbb{E}}_{\mu'} 1 = 1$. For any function f of degree $\leq (r - r')/2$,

$$\widetilde{\mathbb{E}}_{\mu'} f^2 = \frac{\widetilde{\mathbb{E}}_\mu pf^2}{\widetilde{\mathbb{E}}_\mu p} \geq 0$$

since pf^2 is an SoS polynomial of degree at most r. ■

We can also more generally condition on events.

Definition 3.25 (Conditioning)**.** Let μ be a pseudodistribution of degree r, and let $S \subseteq [n]$ with $|S| \leq r/2$. Let $\alpha \in \{-1, 1\}^S$. Then, $\mu|_{x_S = \alpha}$ is the reweighting of μ by the polynomial f_α^2, where

$$f_\alpha(x) = \begin{cases} 1, & x|_S = \alpha, \\ 0, & \text{otherwise.} \end{cases}$$

How do we round high-degree pseudodistributions?

Definition 3.26 (Independent rounding)**.** Let μ be a pseudodistribution. The independent rounding of μ is the distribution of the random variable x' which independently sets

$$x'_i = \begin{cases} 1, & \text{with probability } 1/2 + (1/2)\widetilde{\mathbb{E}}_\mu x_i \\ -1, & \text{with probability } 1/2 - (1/2)\widetilde{\mathbb{E}}_\mu x_i. \end{cases}$$

That is, the different coordinates are independent and $\mathbb{E} x'_i = \widetilde{\mathbb{E}}_\mu x'_i$.

Proposition 3.27. Let μ be a pseudodistribution (of degree ≥ 2) and x' the independent rounding of x as defined above. Then,

$$\mathbb{E} f_G(x') = \widetilde{\mathbb{E}}_\mu f_G(x) + \sum_{ij \in E} \frac{1}{2} \widetilde{\mathrm{Cov}}_\mu(x_i, x_j),$$

where $\widetilde{\mathrm{Cov}}_\mu(x_i, x_j) \coloneqq \widetilde{\mathbb{E}}_\mu (x_i - \widetilde{\mathbb{E}}_\mu x_i)(x_j - \widetilde{\mathbb{E}}_\mu x_j)$.

We do not incur any loss when distinct coordinates are independent (according to μ); loss is introduced only in the presence of negative correlation. This makes sense in the context of cuts, since here a negative correlation between two adjacent vertices corresponds to the two vertices being likely to be on opposite sides of the cut; when we make it independent, this information is lost.

Proof. Due to linearity of expectation, we can look at a single edge $ij \in E$. On the left, independence implies that

$$\mathbb{E}(x'_i - x'_j)^2 = \mathbb{E}x'^2_i + \mathbb{E}x'^2_j - 2\mathbb{E}x'_i\mathbb{E}x'_j = 2 - 2\widetilde{\mathbb{E}}_\mu x_i \widetilde{\mathbb{E}}_\mu x_j.$$

and

$$\widetilde{\mathbb{E}}_\mu (x_i - x_j)^2 = 2 - 2\widetilde{\mathbb{E}}_\mu x_i x_j.$$

The desideratum follows on subtracting the two, since $\widetilde{\mathrm{Cov}}_\mu(x_i, x_j) = \widetilde{\mathbb{E}}_\mu x_i x_j - \widetilde{\mathbb{E}}_\mu x_i \widetilde{\mathbb{E}}_\mu x_j$. ■

The main insight of global correlation rounding is the following. We start with a high-degree pseudodistribution μ, and produce a low average covariance pseudodistribution μ_1 by conditioning it, while ensuring that $\widetilde{\mathbb{E}} f_G$ does not change by much. Following this, we just independently round μ_1 to μ' and are done.

Definition 3.28 (Local correlation)**.** Let μ be a pseudodistribution on $\{-1,1\}^n$ and G a graph on $[n]$. The *local correlation* of μ under G is

$$\mathrm{LC}_G(\mu) = \mathbb{E}_{ij\in E} \left|\widetilde{\mathrm{Cov}}(x_i, x_j).\right|$$

We drop the G subscript if it is clear from context.
If the local correlation were less than δ (i.e., it is used to represent the "low average covariance" condition we described in the previous paragraph), we get that

$$\mathbb{E} f_G(x') \geq \widetilde{\mathbb{E}}_{\mu_1} f_G - m\delta \approx \widetilde{\mathbb{E}}_\mu f_G - m\delta.$$

If independent rounding fails to give an additive δ approximation, then we must have that the local correlation is at least 2δ.
Unfortunately, we cannot expect to find a pseudodistribution of low local correlation for arbitrary G, since we cannot approximate max-cut to an arbitrarily small error.

Recall that the *entropy* of a random variable X on $[q]$ is defined by

$$H(X) \coloneqq \sum_{i\in[q]} \Pr[X = i] \log \Pr[X = i].$$

Also recall the *mutual information* between a pair of random variables, which is a measure of how independent the two are, defined by

$$\mathbb{I}(X;Y) \coloneqq \sum_{i,j\in[q]} \Pr[X = i, Y = j] \log \frac{\Pr[X = i, Y = j]}{\Pr[X = i]\Pr[Y = j]}.$$

In particular, the mutual information of two independent random variables is 0. A consequence of these definitions is that defining the conditional entropy of two random variables by

$$H(X \mid Y) = \sum_{i\in[q]} \Pr[Y = i] H(X \mid Y = i),$$

we have

$$\mathbb{I}(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X).$$

Proposition 3.29. Let X, Y be $[q]$-valued random variables. Then,

$$|\operatorname{Cov}(X,Y)| = O(\sqrt{\mathbb{I}(X;Y)}).$$

Definition 3.30 (Global correlation)**.** Let μ be a pseudodistribution of degree at least 4. The *global correlation* of μ is defined by

$$\mathrm{GC}(\mu) = \mathbb{E}_{i,j\in[n]}\mathbb{I}(X_i; X_j).$$

Note here that we are using $\mathbb{I}$ despite μ being a pseudodistribution because Proposition 3.22(c) implies that the marginal $\mu|_{\{i,j\}}$ is indeed a distribution (this uses that the degree of μ is at least 4).
Unlike local correlation, we can always find a pseudodistribution with low global correlation.

Lemma 3.31. Let μ be a pseudodistribution on $\{-1,1\}^n$ of degree $\ell + 2/\eta$. Then, there is a reweighting μ' (of degree at least ℓ) of μ by a degree $2/\eta$ sum-of-squares polynomial such that $\mathrm{GC}(\mu') \le \eta$.

Proof. We shall build a sequence of reweightings $\mu = \mu_0, \mu_1, \ldots, \mu_{t-1}, \ldots$, with each μ_t being a degree 2 reweighting of μ_{t-1}. We shall do this η times, then show that one of these η reweightings must satisfy the required.
Sample a uniformly random $1/\eta$-tuple of variables from $[n]$, say $i_1, \ldots, i_{1/\eta}$. For $1 \le t \le 1/\eta$, sample α_t from $\mu_{t-1}|_{i_t}$. Finally, get μ_t from μ_{t-1} by conditioning on $x_{i_t} = \alpha_t$.
We are obtaining μ_t from μ_{t-1} by reweighting with $\mathbb{1}_{x_{i_t}=\alpha_t}$, which is a degree 1 polynomial, so μ_t has degree 2 less than μ_{t-1}. Now, how do we show that one of the μ_is work?

Now, suppose instead that for all $t \le 1/\eta$, $\mathbb{E}_{i,j\in[n]}\mathbb{I}_{\mu_t}(x_i; x_j) > \eta$. So, for some i, $\mathbb{E}_j\mathbb{I}_{\mu_t}(x_i, x_j) > \eta$. Conditioning on $x_i = \alpha_i$ for some such i,

$$\mathbb{E}_j H_{\mu_{t-1}}(x_j) - H_{\mu_t}(x_j) = \mathbb{E}_j H_{\mu_{t-1}}(x_j) - H_{\mu_{t-1}}(x_j \mid x_i) = \mathbb{E}_j\mathbb{I}_{\mu_{t-1}}(x_i; x_j)$$

is large. Considering the potential function $\mathbb{E}_i H_{\mu_t}(x_i)$, this means that if the chosen i is a typical i, the potential increases by η at each step. However, this potential function cannot go over 1, so we are done since we have $1/\eta$ pseudodistributions.
This gives us an $n^{O(1/\eta)}$ algorithm to also find this reweighting, by brute-forcing over all possible $i_1, \ldots, i_{1/\eta}$ – this algorithm also uses the fact that global correlations can easily be computed for a given pseudodistribution. ■

Now, we would like to connect global correlation and local correlation. This is where our assumption of bounded threshold rank enters the picture.

Lemma 3.32. Let G be a graph on $[n]$ and μ a pseudodistribution on $\{-1,1\}^n$. If $\mathrm{LC}_G(\mu) \ge \delta$, then for any ρ,

$$\mathrm{GC}(\mu) \ge \left(\frac{\delta - \rho}{\mathrm{rank}_\rho(G)}\right)^2.$$

In particular,

$$\mathrm{GC}(\mu) \ge \left(\frac{\delta}{2\,\mathrm{rank}_{\delta/2}(G)}\right)^2.$$

If $\mathrm{GC}(\mu) < \eta$, then we have that $\mathrm{LC}_G(\mu) < \delta$ for any δ such that

$$\delta^2 \le 4\,\mathrm{rank}_{\delta/2}(G)^2\eta.$$

This tells us that we should choose some η that is much less than $1/\,\mathrm{rank}_{\delta/2}(G)^2$, that is, we should start with a degree $\Omega(\mathrm{rank}_{\delta/2}(G)^2)$ pseudodistribution.

Proof. The following claim implies the desideratum. If M is an $n \times n$ PSD matrix such that $\mathrm{Tr}(M) \leq n$ and $|M_{ij}| \leq 1$ for all i, j, then if $\mathbb{E}_{ij \in E} M_{ij} \geq \delta$, then $\mathbb{E}_{i,j \in [n]} M_{ij}^2 \geq \left(\frac{\delta - \rho}{\mathrm{rank}_\rho(G)}\right)^2$.

Let us see why this gives the required. For ease of notation, denote $\overline{x}_i = x_i - \widetilde{\mathbb{E}}_\mu x_i$. The local correlation condition says that $\mathbb{E}_{ij \in E} |\widetilde{\mathbb{E}}_\mu \overline{x}_i \overline{x}_j| \geq \delta$. Set $M_{ij} = \widetilde{\mathbb{E}}_\mu \overline{x}_i \overline{x}_j$. $M = \widetilde{\mathbb{E}}_\mu \overline{x}\, \overline{x}^\top$ is clearly PSD, and the above condition gives that $\sum_{ij \in E} M_{ij} \geq \delta$. Using the claim, we get that

$$\mathbb{E}_{i,j \in [n]} \widetilde{\mathrm{Cov}}_\mu(x_i, x_j)^2 \geq \left(\frac{\delta - \rho}{\mathrm{rank}_\rho(G)}\right)^2.$$

Proposition 3.29 then yields that

$$\mathrm{GC}(\mu) = \mathbb{E}_{i,j \in [n]} \mathbb{I}(X_i; X_j) \geq \Omega\left(\left(\frac{\delta - \rho}{\mathrm{rank}_\rho(G)}\right)^2\right)$$

as desired.

Let us now prove the claim. Let A be the transition matrix of G, with eigenvalues λ_i and corresponding eigenvectors v_i. Using the PSDness of M with the fact that the largest eigenvalue of A is 1, we have

$$\begin{aligned}
\delta &\leq \mathbb{E}_{ij \in E} M_{ij} \\
&= \frac{1}{n} \sum_{i,j \in [n]} A_{ij} M_{ij} \\
&= \frac{1}{n} \sum_i \lambda_i v_i^\top M v_i \\
&\leq \frac{1}{n} \left(\sum_{i : \lambda_i \geq \rho} \lambda_i v_i^\top M v_i + \rho \sum_i v_i^\top M v_i \right) \\
&\leq \frac{1}{n} \left(\sum_{i : \lambda_i \geq \rho} v_i^\top M v_i + \rho\, \mathrm{Tr}(M) \right) \\
(\delta - \rho) &\leq \frac{1}{n} \sum_{i : \lambda_i \geq \rho} v_i^\top M v_i.
\end{aligned}$$

It follows that for some v_i,

$$\frac{1}{n} v_i^\top M v_i \geq \frac{\delta - \rho}{\mathrm{rank}_\rho(G)}.$$

That is,

$$\frac{\delta - \rho}{\mathrm{rank}_\rho(G)} \leq \frac{1}{n} \|M_2\| \leq \frac{1}{n} \|M\|_F = \sqrt{\mathbb{E}_{i,j \in [n]} M_{ij}^2},$$

completing the proof. ∎

§4. Lower bounds through sum-of-squares

Back towards the ending of Section 2.1, we showed a "lower bound" using a cycle graph that our analysis of degree 2 sum-of-squares is essentially the best. However, this specific example can be "broken" by degree 4 sum-of-squares, as a consequence of the squared triangle inequality.

4.1. k-XOR is hard using sum-of-squares

How do we establish convincing lower bounds more generally? Our running example in this section will be k-LIN over $\mathbb{F}_2$, alternatively called k-XOR. While we initiate our discussion by looking at *worst-case* lower bounds, we shall soon realize that we are instead proving *average-case* lower bounds, which are lower-bounds on certain random instances.

Definition 4.1. An instance of k-sparse linear equations over $\mathbb{F}_2$ is given by a collection of equations

$$z_1 \oplus \cdots \oplus z_k = 1 \text{ or } 0,$$

that is, an instance of k-LIN over $\mathbb{F}_2$ where each equation has exactly k variables. The goal is to maximize the number of satisfied constraints.

Instead looking at $\mathbb{F}_2$ as $\{-1, 1\}$ with multiplication, with 0 mapping to 1 and 1 mapping to -1, each equation is of the form

$$x_1 x_2 \cdots x_k = \pm 1.$$

where each $x_i \in \{-1, 1\}$.
An instance of k-XOR is given by m subsets $(C_i)_{i=1}^m$ of $[n]$ of size k, denoting the XORed variables in the ith constraint, and m numbers $(b_i)_{i=1}^m$, each of which is ± 1. That is, the pair (C_i, b_i) denotes the constraint

$$b_i \prod_{j \in C_i} x_j = 1.$$

We denote the collection $(C_i, b_i)_{i=1}^m$ by $\mathcal{I}$.
This can be pictured as a bipartite graph $G(A, B)$, where $A = [n]$ denotes the set of variables and $B = [m]$ denotes the set of constraints. Each $v \in B$ is labeled b_v, and there is an edge from $u \in A$ to $v \in B$ if $u \in C_v$. Finally, define

$$\mathcal{I}(x) = \frac{1}{m} \sum_{i=1}^{m} b_i \prod_{j \in C_i} x_j.$$

This is a degree k polynomial over the reals, which takes as input boolean assignments in $\{-1, 1\}^n$. For $x \in \{-1, 1\}^n$,

$$\mathrm{Val}_{\mathcal{I}}(x) := \frac{\mathcal{I}(x) + 1}{2}$$

is the fraction of constraints satisfied by x. In particular, $\mathcal{I}(x) = 1$ if all constraints are satisfied by x and -1 if no constraint is satisfied by x. Finally, set $\mathsf{opt}(\mathcal{I}) = \max_{x \in \{-1,1\}^n} \mathrm{Val}_{\mathcal{I}}(x)$. Our goal is to approximate $\mathsf{opt}(\mathcal{I})$.
In the situation where $\mathsf{opt}(\mathcal{I}) = 1$, we can easily find an x achieving this using Gaussian elimination since we just have a set of linear equations.
For any $\mathcal{I}$, a random assignment satisfies half the constraints, so we have a $1/2$-approximation algorithm. The same phenomenon occurs in the trivial $1/2$-approximation algorithm for max-cut – it is just 2-XOR in the case where all the b_i are -1. In max-cut, we were able to beat $1/2$ by a lot using the Goemans-Williamson algorithm. However, there turns out to be a marked difference between $k = 2$ and $k > 2$ here!
In a seminal Gödel prize winning paper, Håstad [Hå01] proved the following.

Theorem 4.2 (Håstad)**.** For $\epsilon > 0$ and $k \geq 3$, it is NP-hard to decide whether an instance of k-XOR is $\geq (1-\epsilon)$-satisfiable or $\leq (1/2+\epsilon)$-satisfiable.

$\geq (1-\epsilon)$-satisfiability means that $\mathcal{I}(x) \geq 1-2\epsilon$ for some x, and $\leq (1/2+\epsilon)$-satisfiability means that $\mathcal{I}(x) \leq 2\epsilon$ for all x.
So, if P $\neq$ NP, there is no polynomial time algorithm to find a $1/2+2\epsilon$-satisfying assignment for a $(1-\epsilon)$-satisfiable instance.
As a result, in k-XOR for $k > 2$, the random assignment algorithm is essentially optimal. If we restrict our view to just sum-of-squares algorithms, we can establish an analogous result unconditionally.

Theorem 4.3. Let $k \geq 3$, $c < 2$. Then, there is a constant $c'(k,\epsilon)$ and a family of k-XOR instances $(\mathcal{I}_n)_{n\geq 1}$ such that

$$c \cdot \mathsf{opt}(\mathcal{I}_n) - \mathrm{Val}_{\mathcal{I}_n}(x)$$

does not have a degree $c'n$ certificate of non-negativity for large enough n.

That is, if we want a degree r sum-of-squares certificate for

$$c \cdot \mathsf{opt}(\mathcal{I}) - \mathrm{Val}_{\mathcal{I}}(x),$$

the existence of which would immediately yield a $\mathrm{poly}(n^r)$ algorithm for a $(1/c)$-approximation of $\mathsf{opt}(\mathcal{I})$, we require $r = \Omega(n)$ (!) if $1/c > 1/2$.
This result was originally proved by Grigoriev [Gri01], and later independently by Schoenebeck [Sch08]. We shall look at Grigoriev's proof.
Over the rest of this subsection, we prove Theorem 4.3.
Each k-tuple is taken to be in $\mathcal{I}_n$ with probability $\Delta/\binom{n}{k}$, so $\mathcal{I}_n$ has around Δn random constraints, where we shall set Δ later. For each such tuple, we sample the corresponding b_i uniformly and randomly from $\{-1,1\}$.
We would like to prove that $c \cdot \mathsf{opt}(\mathcal{I}_n) - \mathrm{Val}_{\mathcal{I}_n}(x)$ does not have a degree $c'n$ certificate. Equivalently, we would like to show that there is a pseudodistribution μ of degree $c'n$ such that

$$\widetilde{\mathbb{E}}_\mu \left(c \cdot \mathsf{opt}(\mathcal{I}_n) - \mathrm{Val}_{\mathcal{I}_n}(x)\right) < 0,$$

that is,

$$\widetilde{\mathbb{E}}_\mu \mathrm{Val}_{\mathcal{I}_n}(x) > c \cdot \mathsf{opt}(\mathcal{I}_n). \tag{4.1}$$

We shall give a pseudodistribution μ such that $\widetilde{\mathbb{E}}_\mu \mathrm{Val}_{\mathcal{I}} = 1$, or equivalently, $\widetilde{\mathbb{E}}_\mu \mathcal{I}(x) = 1$. That is, it pretends like *all* constraints are satisfiable! Framed more offensively, this says that sum-of-squares cannot even solve linear equations.
Such a pseudodistribution satisfies Equation (4.1) with high probability because of the following proposition.

Proposition 4.4. For some constant D, if $\Delta \geq D/\epsilon^2$, $\Pr[\mathsf{opt}(\mathcal{I}_n) \leq 1/2+\epsilon] \geq 0.99$.

Proof. Fix any assignment $y \in \{-1,1\}^n$, and a random draw of the set (C_i) of constraints. The ith constraint is satisfied by y with probability $1/2$, depending on the value of b_i. Furthermore, this is independent for different constraints, so an application of the Chernoff bound, followed by a union bound over y, completes the proof – this requires $m \gg n/\epsilon^2$ to work out. ∎

To describe this μ, it suffices to describe $\widetilde{\mathbb{E}}_\mu x_S$ for all $|S| \leq c'n$. To have $\widetilde{\mathbb{E}}_\mu \mathcal{I}(x) = 1$, we *must* give $\widetilde{\mathbb{E}}_\mu x_{C_i} = b_i$ for each i. Indeed, recalling Proposition 3.22(c), μ restricts to an actual distribution on the coordinates C_i since its degree is *far* greater than $2k$, so we have $\left|\widetilde{\mathbb{E}}_\mu x_{C_i}\right| \leq 1$. Similarly, $\widetilde{\mathbb{E}}_\mu x_{C_i} x_{C_j} = b_i b_j$.
Consider the output Der_d of the following process.

1. In step i, for i in 1 through m, add $x_{C_i} = b_i$ to Der_d.
2. Traverse all monomials in some fixed order graded by degree $\leq d$. For each x_U in this traversal, if $x_S = b_S$ and $x_T = b_T$ are included in Der_d for some S_1, S_2 such that $S_1 \oplus S_2 = U$, we then add $x_U = b_U \coloneqq b_{S_1} b_{S_2}$ to Der_d.

Finally, for any $x_S = b_S$ constraint in Der_d, set $\widetilde{\mathbb{E}}_\mu x_S = b_S$.
However, what do we do if there are two choices for the S_1, S_2, which lead to conflicting values for $\widetilde{\mathbb{E}}_\mu x_S$? We shall show that with high probability (over $\mathcal{I}_n$), this does not happen.

Definition 4.5 (Hypergraph expansion)**.** A k-uniform hypergraph on $[n]$ is said to be (t, β)-*expanding* if for every subset $\mathcal{C}$ of at most t hyperedges,

$$\left| \bigcup_{e \in \mathcal{C}} e \right| \geq \beta |\mathcal{C}|.$$

This is a direct generalization of the notion of combinatorial expansion on ordinary (2-uniform hyper)graphs.
We call an instance $\mathcal{I}$ expanding if the corresponding hypergraph is expanding.

Proposition 4.6. Let $\mathcal{I}_n$ be a random instance with m constraints. Then, for all $\delta > 0$, there exists $\eta = \eta(\Delta, \delta)$, such that with high probability, the hypergraph with edges $C_1, \ldots, C_m$ is $(\eta n, k - 1 - \delta)$-expanding.

We shall prove this proposition later, and first show how this leads to the existence of the desired pseudodistribution.

Lemma 4.7. Suppose that $\{C_1, \ldots, C_m\}$ is $(\eta n, \alpha)$-expanding, where $k/2 + 0.1 < \alpha < k - 1$. Then, for $d < \eta n/100$, there do not exist constraints S_1, S_2, T_1, T_2 in Der_d such that $S_1 \oplus S_2 = T_1 \oplus T_2$.

Note that this says something slightly stronger than what we want, since we are fine if there is such a pair S_1, T_1, S_2, T_2 as long as $b_{S_1} b_{T_1} = b_{S_2} b_{T_2}$.

Proof. Suppose instead that there are such constraints S_1, S_2, T_1, T_2 such that $S_1 \oplus S_2 = T_1 \oplus T_2$. Each of these four constraints is associated with a XOR of C_i constraints. For $S = S_1, S_2, T_1, T_2$, we have $U_S \subseteq \{C_i : i \in [m]\}$ (where $C_i \subseteq [n]$) and

$$S = \bigoplus_{C \in U_S} C.$$

Now, consider the set

$$U = U_{S_1} \oplus U_{S_2} \oplus U_{T_1} \oplus U_{T_2}.$$

of constraints. Because $S_1 \oplus S_2 = T_1 \oplus T_2$, each variable occurs an even number of times across the constraints in U. In particular, since each constraint contributes k variables, the number of distinct variables in U is at most $(k/2)|U|$. Framed more suggestively,

$$\left| \bigcup_{C \in U} C \right| \leq (k/2)|U|.$$

To get a contradiction, we shall use the expansion of U to get a lower bound on the quantity on the left. We claim that $|U| \leq 40d < \eta n$. Given this, we have due to $(\eta n, \alpha)$-expansion that

$$\left| \bigcup_{C \in U} C \right| \geq \alpha |U| > (k/2)|U|.$$

To complete the proof, we shall show that for any constraint S in Der_d corresponding to the set U_S of (C_i) constraints, $|U_S| \leq 10d$. This immediately implies that $|U| \leq 40d$ since $|U| \leq |U_{S_1}| + |U_{S_2}| + |U_{T_1}| + |U_{T_2}|$.
Let $U_1, \ldots, U_r$ be the subsets of base constraints that are derived in Der_d, and suppose instead that i is the smallest index such that $|U_i| > 10d$. Because $U_i = U_{j_1} \oplus U_{j_2}$ for some $j_1, j_2 < i$ and $|U_{j_1}|, |U_{j_2}| \leq 10d$, we have $|U_i| \leq 20d < \eta n$. Therefore, expansion implies that

$$\left| \bigcup_{C \in U_i} C \right| \geq \alpha |U_i|.$$

On the other hand, the total number of variables that occur at least twice in the clauses in U_i is at most $(k/2)|U_i|$, so the number of variables that occur q exactly once is at least

$$\alpha |U_i| - (k/2)|U_i| \geq (\alpha - k/2) \cdot 10d > d.$$

Thus, the number of variables in $\bigoplus_{C \in U_i} C$ is at least the number of variables that occurs exactly once in the above union, which is greater than d. However, all constraints in Der_d have at most d variables, leading to a contradiction and completing the proof. ■

The above argument describes what $\widetilde{\mathbb{E}}_\mu x_S$ is for S in Der_d. For any $S \notin \mathrm{Der}_d$, we set $\widetilde{\mathbb{E}}_\mu x_S = 0$, which can be thought of as the "least informative option".

In the following proposition, we use the $\widetilde{\mathbb{E}}_\mu$ notation although μ is not known prima facie to be a pseudodistribution.

Proposition 4.8. Let μ be a function on $\{-1,1\}^n$ such that $\widetilde{\mathbb{E}}_\mu x_S = b$ for any constraint (S, b) in Der_d, $\widetilde{\mathbb{E}}_\mu 1 = 1$, and $\widetilde{\mathbb{E}}_\mu x_S = 0$ if S is not a constraint in Der_d. Then, μ is a degree d pseudodistribution such that $\widetilde{\mathbb{E}}_\mu \mathrm{Val}_{\mathcal{I}}(x) = 1$.

Proof. It is obvious from the construction that $\widetilde{\mathbb{E}}_\mu \mathrm{Val}_{\mathcal{I}}(x) = 1$. Let p be a polynomial of degree $\leq (d/2)$ – we shall show that $\widetilde{\mathbb{E}}_\mu p^2 \geq 0$. Consider the relation $\sim$ on $\{S \subseteq [n] : |S| \leq (d/2)\}$ where $S \sim T$ if $\widetilde{\mathbb{E}}_\mu x_S x_T \neq 0$. We claim that this is an equivalence relation. Reflexivity is immediate since $\widetilde{\mathbb{E}}_\mu x_S x_S = \widetilde{\mathbb{E}}_\mu 1 = 1$, and so is symmetry since $\widetilde{\mathbb{E}}_\mu x_S x_T = \widetilde{\mathbb{E}}_\mu x_T x_S$. For transitivity, if $S \sim S'$ and $S' \sim S''$, we have

$$\widetilde{\mathbb{E}}_\mu x_S x_{S''} = \widetilde{\mathbb{E}}_\mu x_S x_{S'} x_{S'} x_{S''} = \left(\widetilde{\mathbb{E}}_\mu x_S x_{S'}\right)\left(\widetilde{\mathbb{E}}_\mu x_{S'} x_{S''}\right) \neq 0,$$

where the second equality follows by the definition of Der_d.
Let the equivalence classes of this relation be $Q_1, \ldots, Q_r$.Now, decompose p as

$$p(x) = \sum_{i \in [r]} \sum_{S \in Q_i} p_S x_S = \sum_{i \in [r]} p_i,$$

where each p_S is a constant and $p_i = \sum_{S \in Q_i} p_S x_S$. Then,

$$\begin{aligned} \widetilde{\mathbb{E}}_\mu p^2 &= \sum_{i \in [r]} \widetilde{\mathbb{E}}_\mu p_i^2 + \sum_{\substack{i,j \in [r] \\ i \neq j}} \widetilde{\mathbb{E}}_\mu p_i p_j \\ &= \sum_{i \in [r]} \widetilde{\mathbb{E}}_\mu p_i^2. \qquad (\widetilde{\mathbb{E}}_\mu x_S x_{S'} = 0 \text{ if } S \in Q_i, S' \in Q_j \text{ for } i \neq j) \end{aligned}$$

Fix some $t \in [r]$, and $S_t \in Q_t$. Then,

$$\begin{aligned}
\widetilde{\mathbb{E}}_\mu p_t^2 &= \widetilde{\mathbb{E}}_\mu \left(\sum_{S \in Q_t} p_S x_S \right)^2 \\
&= \sum_{S,T \in Q_t} p_S p_T \widetilde{\mathbb{E}}_\mu [x_S x_T] \\
&= \sum_{S,T \in Q_t} p_S p_T \widetilde{\mathbb{E}}_\mu [x_S x_{S_t}] \widetilde{\mathbb{E}}_\mu [x_{S_t} x_T] \\
&= \left(\sum_{S \in Q_t} p_S \widetilde{\mathbb{E}}_\mu [x_S x_{S_t}] \right)^2 \geq 0,
\end{aligned}$$

completing the proof. ■

Now that we have completed the proof, let us remark again that although we set out to prove a worst-case hardness result, we ended up proving an *average-case* hardness result. This is very different from the max-cut setting, where we can approximate the optimum very well on random graphs (which are expanders).

In fact, it turns out that we can exactly characterize the predicates P for which a random CSP corresponding to the predicate P is maximally hard, and those for which the worst-case CSP corresponding to P is maximally hard.

§5. Constrained sum-of-squares

Recall the second part of Definition 1.1, which we have not really used after defining SoS certificates on the boolean hypercube. We restate the definition here for convenience

Definition 5.1 (Constrained sum-of-squares proofs)**.** Let $\mathcal{A}$ be a set of constraints of the form $f_i(x) \geq 0$ for $i \in [m]$. Then, an *degree d SoS proof given $\mathcal{A}$* of $f \geq 0$ is a set $\{p_S\}_{S \subseteq [m]}$ of degree d sum-of-squares polynomial (in the sense that it satisfies Equation (1.1) for some (g_i)), where S ranges over *multi*sets of elements in $[m]$ such that

$$f(x) = \sum_{S \subseteq [m]} p_S(x) \prod_{i \in S} f_i(x)$$

as polynomials. If this is the case, we write

$$\mathcal{A} \vdash_x^d \{f \geq 0\}$$

and say that "$\mathcal{A}$ derives $g \geq 0$ in degree d".

Again, we remark that although $\mathcal{A}$ contains only inequalities of polynomials, we can easily also make it contain equalities of polynomials by adding two corresponding constraints – for $p(x) = k$, add $p(x) - k \geq 0$ and $k - p(x) \geq 0$. We often interchangeably use $\mathcal{A}$ to denote the subset $S \subseteq \mathbb{R}^n$ of all x satisfying the constraints in $\mathcal{A}$. Such sets are called *semialgebraic sets*. Let $\mathcal{A}$ be some semialgebraic set. Now, similar to how in the first section we motivated SoS by considering the problem of figuring out whether a polynomial is non-negative everywhere, consider the following.

1. Given $g \in \mathbb{R}[x]$, determine if $g \geq 0$ subject to $\mathcal{A}$.
2. Decide if $\mathcal{A}$ is empty.

Note that the second problem above is a generalization of the first, since the first is true iff $\mathcal{A} \cup \{g < 0\}$ is not empty. In fact, it turns out to be a *strict* generalization, as we shall see soon. Let us now state an analogue of Proposition 1.2.

Lemma 5.2 (Positivstellensatz)**.** Let $\mathcal{A}$ be a semialgebraic set. Then, either $\mathcal{A}$ is non-empty, or there exists a sum-of-squares proof that $\mathcal{A} \vdash^d \{-1 \geq 0\}$ for some integer d.

The above was originally proved by Krivine [Kri64] in 1964 and later independently by Stengle [Ste74] in 1974.

References

[ABS15] Sanjeev Arora, Boaz Barak, and David Steurer. Subexponential algorithms for unique games and related problems. *J. ACM*, 62(5), nov 2015.

[AMMN06] Noga Alon, Konstantin Makarychev, Yury Makarychev, and Assaf Naor. Quadratic forms on graphs. *Inventiones mathematicae*, 163(3):499–522, Mar 2006.

[AN04] Noga Alon and Assaf Naor. Approximating the cut-norm via Grothendieck's inequality. In *Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '04, page 72–80, New York, NY, USA, 2004. Association for Computing Machinery.

[BMMN11] Mark Braverman, Konstantin Makarychev, Yury Makarychev, and Assaf Naor. The Grothendieck constant is strictly smaller than Krivine's bound. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science*, pages 453–462, 2011.

[CKK+06] Shuchi Chawla, Robert Krauthgamer, Ravi Kumar, Yuval Rabani, and D. Sivakumar. On the hardness of approximating multicut and sparsest-cut. *Computational Complexity*, 1506:94–114, 06 2006.

[CMM06] Moses Charikar, Konstantin Makarychev, and Yury Makarychev. Near-optimal algorithms for unique games. In *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '06, page 205–214, New York, NY, USA, 2006. Association for Computing Machinery.

[CW04] M. Charikar and A. Wirth. Maximizing quadratic programs: extending Grothendieck's inequality. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 54–60, 2004.

[DKK+18] Irit Dinur, Subhash Khot, Guy Kindler, Dor Minzer, and Muli Safra. Towards a proof of the 2-to-1 games conjecture? STOC 2018, page 376–389, New York, NY, USA, 2018. Association for Computing Machinery.

[FS02] Uriel Feige and Gideon Schechtman. On the optimality of the random hyperplane rounding technique for MAX CUT. *Random Structures & Algorithms*, 20, 2002.

[Gri01] D. Grigoriev. Complexity of positivstellensatz proofs for the knapsack. *computational complexity*, 10(2):139–154, Dec 2001.

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

[Hå01] Johan Håstad. Some optimal inapproximability results. *J. ACM*, 48(4):798–859, jul 2001.

[IKW02] Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. In search of an easy witness: exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002. Special Issue on Complexity 2001.

[Kho02] Subhash Khot. On the power of unique 2-prover 1-round games. In *Proceedings of the Thiry-Fourth Annual ACM Symposium on Theory of Computing*, STOC '02, page 767–775, New York, NY, USA, 2002. Association for Computing Machinery.

[KKMO07] Subhash Khot, Guy Kindler, Elchanan Mossel, and Ryan O'Donnell. Optimal inapproximability results for MAX-CUT and other 2-variable CSPs? *SIAM Journal on Computing*, 37(1):319–357, 2007.

[KR08] Subhash Khot and Oded Regev. Vertex cover might be hard to approximate to within $2-\epsilon$. *Journal of Computer and System Sciences*, 74(3):335–349, 2008. Computational Complexity 2003.

[Kri64] J. L. Krivine. Anneaux préordonnés. *Journal d'Analyse Mathématique*, 12(1):307–326, Dec 1964.

[Meg01] Alexandre Megretski. Relaxations of quadratic programs in operator theory and system analysis. In Alexander A. Borichev and Nikolai K. Nikolski, editors, *Systems, Approximation, Singular Integral Operators, and Related Topics*. Birkhäuser Basel, 2001.

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

[Rag08] Prasad Raghavendra. Optimal algorithms and inapproximability results for every csp? In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 245–254, New York, NY, USA, 2008. Association for Computing Machinery.

[Raz98] Ran Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[Sch08] Grant Schoenebeck. Linear level lasserre lower bounds for certain k-csps. In *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 593–602, 2008.

[Ste74] Gilbert Stengle. A nullstellensatz and a positivstellensatz in semialgebraic geometry. *Mathematische Annalen*, 207:87–97, 1974.