Sum of Squares Lower Bounds from Symmetry and a Good Story

Aaron Potechin

University of Chicago Department of Computer Science, 5730 S. Ellis Avenue,
John Crerar Library, Chicago, IL 60637, United States
potechin@uchicago.edu

Abstract

In this paper, we develop machinery which makes it much easier to prove sum of squares lower bounds when the problem is symmetric under permutations of $[1, n]$ and the unsatisfiability of our problem comes from integrality arguments, i.e. arguments that an expression must be an integer. Roughly speaking, to prove SOS lower bounds with our machinery it is sufficient to verify that the answer to the following three questions is yes:

1. Are there natural pseudo-expectation values for the problem?
2. Are these pseudo-expectation values rational functions of the problem parameters?
3. Are there sufficiently many values of the parameters for which these pseudo-expectation values correspond to the actual expected values over a distribution of solutions which is the uniform distribution over permutations of a single solution?

We demonstrate our machinery on three problems, the knapsack problem analyzed by Grigoriev, the MOD 2 principle (which says that the complete graph K_n has no perfect matching when n is odd), and the following Turan type problem: Minimize the number of triangles in a graph G with a given edge density. For knapsack, we recover Grigoriev's lower bound exactly. For the MOD 2 principle, we tighten Grigoriev's linear degree sum of squares lower bound, making it exact. Finally, for the triangle problem, we prove a sum of squares lower bound for finding the minimum triangle density. This lower bound is completely new and gives a simple example where constant degree sum of squares methods have a constant factor error in estimating graph densities.

2012 ACM Subject Classification Theory of computation → Proof complexity

Keywords and phrases Sum of squares hierarchy, proof complexity, graph theory, lower bounds

Digital Object Identifier 10.4230/LIPIcs.ITCS.2019.61

Related Version A full version of the paper is available at `https://arxiv.org/abs/1711.11469`.

Acknowledgements The author would like to thank Sasha Razborov for suggesting the triangle problem and for helpful conversations. The author would also like to thank Johan Håstad, Fernando Geronimo, Annie Raymond, and anonymous reviewers for helpful comments on the paper. Finally, the author would like to thank Fernando Geronimo for helpful discussions on representation theory. This work was supported by the Simons Collaboration for Algorithms and Geometry, the NSF under agreement No. CCF-1412958, the Knut and Alice Wallenberg Foundation, the European Research Council, and the Swedish Research Council.

1 Introduction

The sum of squares hierarchy (which we call SOS for brevity), a hierarchy of semidefinite programs first indepedently investigated by Shor [33], Nesterov [27], Parrilo [28], Lasserre [22], and Grigoriev [15, 16], is an exciting frontier of algorithm design, complexity theory, and proof complexity. SOS is exciting because it provides a single unified framework which can be applied to give approximation algorithms for a wide variety of combinatorial optimization problems. Moreover, SOS is conjectured to be optimal for many of these problems. In particular, SOS captures the Goemans-Williamson algorithm for MAX-CUT [13], the Goemans-Linial relaxation for sparsest cut (analyzed by Arora, Rao, and Vazirani [2]), and the subexponential time algorithm for unique games found by Arora, Barak, and Steurer [1]. More recently, SOS has been applied directly to give algorithms for several problems including planted sparse vector [5], dictionary learning [6], tensor decomposition [12, 19, 25], tensor completion [8, 29], and quantum separability [7].

That said, there are limits to the power of SOS. As shown by SOS lower bounds for constraint satisfactions problems (CSPs) [16, 32, 3, 20] and gadget reductions [34], SOS requires degree $\Omega(n)$ (and thus exponential time) to solve most NP-hard problems. As shown by SOS lower bounds on planted clique and other planted problems [26, 10, 17, 4, 18], SOS can have difficulty distinguishing between a random input and an input which is random except for a solution which has been planted inside it. Finally, as shown by Grigoriev's SOS lower bound for the knapsack problem [15], SOS has difficulty capturing integrality arguments, i.e. arguments which say that an expression must be an integer.

In this paper, we further explore this last weakness of SOS. In particular, we develop machinery which makes it much easier to prove SOS lower bounds when the problem is symmetric and the unsatisfiability of our problem comes from integrality arguments. The usual process for proving SOS lower bounds involves finding pseudo-expectation values (see subsection 2.3) and then proving that a matrix called the moment matrix is PSD (postive semidefinite), which can be quite difficult. Roughly speaking, to prove SOS lower bounds with our machinery it is sufficient to verify that the answer to the following three questions is yes:

1. Are there natural pseudo-expectation values for the problem?
2. Are these pseudo-expectation values rational functions of the problem parameters?
3. Are there sufficiently many values of the parameters for which these pseudo-expectation values correspond to the actual expected values over a distribution of solutions which is the uniform distribution over permutations of a single solution?

We demonstrate our machinery on three problems, the knapsack problem itself, the MOD 2 principle (which says that the complete graph K_n on n vertices does not have a perfect matching when n is odd), and the following Turan-type problem: Minimize the number of triangles in a graph G with a given edge density.

1.1 Equations and SOS lower bounds for knapsack, the MOD 2 principle, and a triangle problem

To state our SOS lower bounds on knapsack, the MOD 2 principle, and the triangle problem, we must first express these problems as infeasible systems of polynomial equations. We do this because as we will discuss in subsection 2.3, SOS gives a proof system for proving that systems of polynomial equations over $\mathbb{R}$ are infeasible. Our lower bounds show that SOS requires high degree to prove that the systems of equations corresponding to knapsack, the MOD 2 principle, and the triangle problem are infeasible.

For the knapsack problem, we consider the simple case when all of the weights are 1, the knapsack capacity is k, and we are asked whether it is possible to fill the knapsack to its capacty. We can express this problem with equations as follows:

1. $\forall i, x_i^2 - x_i = 0$
2. $\sum_{i=1}^n x_i - k = 0$.

These equations are clearly infeasible whenever $k \notin \mathbb{Z}$. However, as Grigoriev [15] showed, since SOS has difficulty capturing integrality arguments, SOS requires high degree to refute these equations.

▶ **Theorem 1** (Grigoriev's SOS lower bound for knapsack)**.**
Degree $\min\{2\lfloor \min\{k, n-k\}\rfloor + 3, n\}$ *SOS fails to prove that the knapsack equations are infeasile.*

In this paper, we observe that Grigoriev's lower bound (which is tight) follows immediately from our machinery.

For the MOD 2 principle, we are asked whether the complete graph K_n has a perfect matching. To express this problem with equations, we take a variable x_{ij} for each possible edge (i, j) and we want that $x_{ij} = 1$ if the edge (i, j) is in our matching and $x_{ij} = 0$ otherwise. We encode this and the claim that we have a perfect matching as follows:

1. For all $i, j \in [1, n]$ such that $i < j$, $x_{ij}^2 - x_{ij} = 0$
2. For all $i \in [1, n]$, $\sum_{j \in [1,n]: j \neq i} x_{ij} - 1 = 0$ (where we take $x_{ij} = x_{ji}$ whenever $i > j$)

These equations are infeasible whenever n is odd. However, Grigoriev [16] showed that SOS requires high degree to refute these equations. While Grigoriev's lower bound is shown via a reduction from the Tseitin equations and is tight up to a constant factor, in this paper we use our machinery to obtain the following tight SOS lower bound directly.

▶ **Theorem 2** (SOS lower bound for the MOD 2 principle)**.**
Degree $\frac{n-1}{2}$ *SOS fails to prove that the equations for the MOD 2 principle are infeasible.*

For the triangle problem, we want to minimize the number of triangles in a graph with edge density ρ. For this problem, Goodman [14] showed the following lower bound.

▶ **Theorem 3** (Goodman's bound)**.** *The minimal number of triangles in a graph* G *with* n *vertices and edge density* ρ *is at least*

$$t(n, \rho) := \binom{n}{3} - \frac{n(n-1)(1-\rho)}{6}((1+2\rho)n - 2 - 2\rho)$$

As we will discuss in the full version of this paper, this bound is tight if there is an integer k such that

1. $\frac{n}{k} - 1 = (1-\rho)(n-1)$
2. n is divisible by k.

If so, then we can take G to have k independent sets of size $\frac{n}{k}$ and have all of the edges between different independent sets, which minimizes the number of triangles in G and matches Goodman's bound. Otherwise, Goodman's bound cannot be achieved.

To express this problem using equations, we again create a variable x_{ij} for each possible edge (i, j) and we want $x_{ij} = 1$ if the edge (i, j) is in the graph and $x_{ij} = 0$ if the edge (i, j) is not in the graph. We encode this, the requirement the edge density is ρ, and the claim that Goodman's bound can be achieved with the following equations

1. For all $i, j \in [1, n]$ such that $i < j$, $x_{ij}^2 - x_{ij} = 0$
2. $\sum_{i,j \in [1,n]: i<j} x_{ij} - \rho\binom{n}{2} = 0$
3. $\sum_{i,j,k \in [1,n]: i<j<k} x_{ij}x_{ik}x_{jk} - t(n, \rho) = 0$ where $t(n, \rho) = \binom{n}{3} - \frac{n(n-1)(1-\rho)}{6}((1+2\rho)n - 2 - 2\rho)$

Using our machinery, we show the following SOS lower bound which is completely new and was the motivation for developing our machinery.

▶ **Theorem 4** (SOS lower bound for the triangle problem)**.**
Letting k be the number such that $\frac{n}{k} - 1 = (1-\rho)(n-1)$, degree $\lfloor \min\{k, \frac{n}{k}\} \rfloor + 1$ SOS fails to refute the triangle problem equations.

1.2 Relation to previous work on symmetry and SOS

There is a considerable body of prior research on symmetry and SOS. Several works built on the difficulty on knapsack and/or further investigated symmetric polynomials on the variables $\{x_1, \ldots, x_n\}$. Laurent [23] used the difficulty of knapsack to show that degree $\lceil \frac{n}{2} \rceil$ SOS is required to capture the CUT polytope of the complete graph. Bleckherman, Gouveia, and Pfeiffer [9] used the difficulty of knapsack to construct degree 4 polynomials which are non-negative but cannot be written as a sum of squares of low degree *rational* functions. Lee, Prakash, Wolf, and Yuen [24] showed that there are symmetric non-negative polynomials on the variables $\{x_1, \ldots, x_n\}$ which cannot be approximated with low degree sums of squares. Kurpisz, Leppänen, and Mastrolilli [21] gave a general criterion for determining if a symmetric polynomial on $\{x_1, \ldots, x_n\}$ is a sum of squares or not.

While these prior works give more precise results for symmetric problems on the variables $\{x_1, \ldots, x_n\}$, they do not show how to handle problems which are symmetric under permutations of $[1, n]$ but have variables such as $\{x_{ij} : i < j\}$ which depend on 2 or more indices. Thus, these prior works are incomparable with this work.

Another line of research on symmetry and SOS which is more closely connected to this work uses symmetry to reduce the algorithmic complexity of implementing SOS. Gatermann and Parrilo [11] showed how representation theory can be used to greatly reduce the search space for pseudo-expectation values, allowing SOS to be run more efficiently on symmetric problems. Recently, Raymond et. al. [30] combined the analysis of Gatermann and Parrilo with Razborov's flag algebras [31] to show that in the case of k-subset hypercubes, the resulting semidefinite program has size which is independent of n. These results are quite general and apply to all of the problems we are considering. That said, these results do not tell us how to find or verify pseudo-expectation values by hand, which is generally what is needed for SOS lower bounds.

In this paper, we show how the representation theory which allows Gatermann and Parrilo [11] and Raymond et. al. [30] to dramatically reduce the size of the semidefinite programs for SOS on symmetric problems can also be used to help prove theoretical SOS lower bounds on symmetric problems. In particular, Theorem 21, which is a crucial part of our machinery, essentially follows from Corollary 2.6 of Raymond et. al. [30]. We obtain our lower bounds by combining this theorem with the additional assumption that the unsatisfiability of the problem we are analyzing comes from integrality arguments.

1.3 Paper outline

The remainder of the paper is organized as follows. In Section 2, we give some preliminaries. In Section 3 we describe how we can find candidate pseudo-expectation values from stories. In Section 4 we highlight how symmetry is useful for proving SOS lower bounds even without additional assumptions. In Section 5, we rigorously define what stories and good stories are and show that good stories imply SOS lower bounds. Finally, in Section 6, we show a method for verifying that stories are good stories.

2 Preliminaries

Before we can describe our machinery, we must first give some preliminaries. We begin by describing the class of symmetric problems which our machinery can be applied to. We then define the sum of squares hierarchy and discuss some notation for the paper.

2.1 Symmetric problems

▶ **Definition 5.** We make the following assumptions about the problem P we are analyzing:

1. We assume that P is a problem about hypergraphs G with vertices $V(G) = [1, n]$ and a set of possible hyperedges E_P. We view the hyperedges $e \in E_P$ as subsets of $[1, n]$ which may be unordered or ordered depending on P. If all of these subsets have the same size $t \geq 1$ then we say that the problem P has arity t.
2. We assume that P has variables $\{x_e : e \in E_P\}$ and P is a YES/NO question which is described by a set of problem equations $\{s_i(\{x_e : e \in E_P\}) = 0\}$. The answer to P is YES if all of these equations can be satisfied simultaneously and NO otherwise.
3. We assume that the set E_P of possible hyperedges and the set $\{s_i(\{x_e : e \in E_P\}) = 0\}$ of problem equations are both symmetric under permutations of $[1, n]$.

If a problem P satisfies all of these assumptions then we say that P is a symmetric hypergraph problem. Since we only consider problems of this type, for brevity we will just say symmetric problem rather than symmetric hypergraph problem.

▶ **Example 6.** Symmetric problems P of arity 1 are YES/NO questions on the variables $\{x_1, \ldots, x_n\}$ which are symmetric under permutations of $[1, n]$.

▶ **Example 7.** For symmetric problems P of arity 2, E_P is the set of subsets of $[1, n]$ of size 2. If the subsets in E_P are unordered then G is an undirected graph and we have variables $\{x_{ij} : i, j \in [1, n], i \neq j\}$ where we take $x_{ji} = x_{ij}$. If the subsets in E_P are ordered then G is a directed graph and we have distinct variables $\{x_{ij} : i, j \in [1, n], i \neq j\}$.

▶ Remark. While our machinery can handle symmetric problems of any arity, the examples we focus on all have arity 1 or 2. Knapsack with unit weights has arity 1 while the MOD 2 principle and the triangle problem have arity 2 and are about undirected graphs.

▶ Remark. Since our machinery is based on polynomial interpolation, it is important that the symmetric problem P does not have inequalities as well as equalities. If P has inequalities then our machinery does not immediately give an SOS lower bound and more analysis is needed.

2.2 Index degree

For our results, rather than considering the degree of a polynomial f, it is more natural to consider the largest number of indices mentioned in any one monomial of f. We call this the index degree of f.

▶ **Definition 8** (Index degree)**.**

1. Given a monomial $p = \prod_{e \in E_p} x_e$, we define $I(p) = \{i : \exists e \in E_p : i \in e\}$ and we define the index degree of p to be

$$indexdeg(p) = indexdeg_{[1,n]}(p) = |I(p)|$$

   In other words, $indexdeg(p)$ is the number of indices which p depends on.
2. Given a polynomial f, if $f = \sum_j c_j p_j$ is the decomposition of f into monomials then we define the index degree of f to be $indexdeg(f) = \max_j \{indexdeg(p_j)\}$

▶ **Example 9.** If p is the monomial $p = x_{12}x_{34}$ then p has degree 2 and index degree 4.

▶ **Example 10.** If $f = x_{12}x_{13} + x_{24}^4$ then f has degree 4 and index degree 3.
We will also need an analagous definition where we only consider the indices outside of a subset $I \subseteq [1, n]$.

▶ **Definition 11** (Index degree outside of I)**.** Let $I \subseteq [1, n]$ be a subset of indices.
1. Given a monomial $p = \prod_{e \in E_p} x_e$, we define the index degree of p on $[1, n] \setminus I$ to be

   $$indexdeg_{[1,n]\setminus I}(p) = |I(p) \setminus I|$$

   In other words, $indexdeg_{[1,n]\setminus I}(p)$ is the number of indices in $[1, n] \setminus I$ which p depends on.
2. Given a polynomial f, if $f = \sum_j c_j p_j$ is the decomposition of f into monomials then we define the index degree of f on $[1, n] \setminus I$ to be $indexdeg_{[1,n]\setminus I}(f) = \max_j \{indexdeg_{[1,n]\setminus I}(p_j)\}$

2.3 SOS and pseudo-expectation values

We now define SOS and pseudo-expectation values, which are used to prove SOS lower bounds. One way to describe SOS is through SOS/Positivstellensatz proofs, which are defined as follows:

▶ **Definition 12.** Given a system of polynomial equations $\{s_i = 0\}$ over $\mathbb{R}$, an index degree d SOS/Positivstellensatz proof of infeasibility is an equality of the form

$$-1 = \sum_i f_i s_i + \sum_j g_j^2$$

where
1. $\forall i, indexdeg(f_i) + indexdeg(s_i) \leq d$
2. $\forall j, indexdeg(g_j) \leq \frac{d}{2}$

▶ Remark. This is a proof of infeasibility because the terms $f_i s_i$ should all be 0 by the problem equations and the terms g_j^2 must all be non-negative, so they can't possibly sum to -1 if all of the problem equations are satisfied.

▶ **Definition 13.** Index degree d SOS gives the following feasibility test for whether a system of polynomial equations over $\mathbb{R}$ is feasible or not. If there is an index degree d Positivstellensatz proof of infeasibiblity then index degree d SOS says NO. Otherwise, index degree d SOS says YES.

▶ Remark. Index degree d SOS may give false positives by failing to say NO on systems of equations which are infeasible but will never give a false negative.
In this paper, we show SOS lower bounds for the infeasible systems of equations described in subsection 2.1 by showing that for small d there is no index degree d Positivstellensatz proof of infeasibility for our system of equations. This can be done with index degree d pseudo-expectation values, which are defined as follows:

▶ **Definition 14.** Given a system of polynomial equations $\{s_i = 0\}$ over $\mathbb{R}$, index degree d pseudo-expectation values are a linear mapping $\tilde{E}$ from polynomials of index degree $\leq d$ to $\mathbb{R}$ which satisfies the following conditions:
1. $\tilde{E}[1] = 1$
2. $\forall i, f, \tilde{E}[f s_i] = 0$ whenever $indexdeg(f) + indexdeg(s_i) \leq d$
3. $\forall g, \tilde{E}[g^2] \geq 0$ whenever $indexdeg(g) \leq \frac{d}{2}$

▶ **Proposition 15.** *If there are index degree d pseudo-expectation values $\tilde{E}$ for a system of polynomial equations $s_1 = 0$, $s_2 = 0$, etc. over $\mathbb{R}$, then there is no index degree d Positivstellensatz proof of infeasibility for these equations.*

Proof. Assume that we have both index degree d pseudo-expectation values and an index degree d Positivstellensatz proof of infeasibility. Applying the pseudo-expectation values to the Positivstellensatz proof, we get the following contradiction:

$$-1 = \tilde{E}[-1] = \sum_i \tilde{E}[f_i s_i] + \sum_j \tilde{E}[g_j^2] \geq 0$$ ◀

▶ Remark. Condition 3 of definition 14 is equivalent to the statement that the moment matrix M is PSD (positive semidefinite) where M is indexed by monomials p, q of index degree $\leq \frac{d}{2}$ and has entries $M_{pq} = \tilde{E}[pq]$. Proving SOS lower bounds usually involves proving that $M \succeq 0$, which can be quite difficult. In this paper we can instead analyze $\tilde{E}[g^2]$ more directly.

▶ Remark. The idea behind pseudo-expectation values is that they should mimic actual expected values over a distribution of solutions. In particular, as shown by the following proposition, if $\tilde{E}$ comes from a distribution over actual solutions then it automatically gives pseudo-expectation values. This fact is crucial for our results.

▶ **Proposition 16.** *If the equations $\{s_i = 0\}$ are feasible over $\mathbb{R}$ and Ω is a probability distribution over actual solutions then the linear mapping $\tilde{E}[p] = E_\Omega[p]$ gives index degree d pseudo-expectation values for these equations for all d.*

Proof. Observe that:

1. For any $x \sim \Omega$, $1 = 1$. Thus, $\tilde{E}[1] = E_\Omega[1] = 1$.
2. For any $x \sim \Omega$, for all i, f, $f(x)s_i(x) = 0$. Thus, for all i, f, $\tilde{E}[fs_i] = E_\Omega[fs_i] = 0$.
3. For any $x \sim \Omega$, for all g, $g(x)^2 \geq 0$. Thus, for all g, $\tilde{E}[g^2] = E_\Omega[g^2] \geq 0$. ◀

2.4 Sequences of distinct indices

We will need the following definitions about sequences of distinct indices in $[1, n]$.

▶ **Definition 17** (Operations on sequences)**.**

1. Given a sequence of distinct indices $A = (i_1, \ldots, i_m)$, we define the set I_A to be $I_A = \{i_1, \ldots, i_m\}$. In other words, I_A is just A without the ordering.
2. Given two sequences of distinct indices $A = (i_1, \ldots, i_{m_1})$ and $B = (i'_1, \ldots, i'_{m_2})$, we say that $A \subseteq B$ if $m_1 \leq m_2$ and $\forall j \in [1, m_1], i'_j = i_j$.
3. Given two sequences of distinct indices $A = (i_1, \ldots, i_{m_1})$ and $B = (i'_1, \ldots, i'_{m_2})$ such that $I_A \cap I_B = \emptyset$, we define $A \cup B$ to be the sequence $A \cup B = (i_1, \ldots, i_{m_1}, i'_1, \ldots, i'_{m_2})$

In this paper, we will never consider sequences of indices which are not distinct, so we assume without stating it explicitly that all of our sequences contain distinct indices.

3 Finding pseudo-expectation values: Stories and a verifier/adversary game for SOS

In this section, we describe a verifier/adversary game which we use to find pseudo-expectation values and deduce SOS lower bounds. We then describe how the adversary can play this game using stories and describe the resulting pseudo-expectation values for knapsack, the MOD 2 principle, and the triangle problem.

The verifier/adversary game is as follows. The verifier queries sequences of indices $\{A_i\}$. For each sequence of indices $A = (i_1, \dots, i_m)$ the verifier queries, for each $j \in [1, m]$ and every possibility for what happens with the previous indices $(i_1, \dots, i_{j-1})$, the adversary must provide a probability distribution for what happens with the index i_j. Taken together, these answers give a probability distribution for all of the possibilities for what happens with the indices in A. From these probability distributions, we can obtain pseudo-expectation values.

The verifier wins if he/she detects one of the following flaws in the adversary's answers

1. The adversary gives a probability for some event which is either negative or undefined.
2. The adversary's answers do not result in well-defined pseudo-expectation values because they are inconsistent. More precisely, there exist two sequences of indices $A = (i_1, \dots, i_m)$ and $A' = (i'_1, \dots, i'_m)$ such that A' and A are equal as sets (i.e. $\{i'_1, \dots, i'_m\}$ is a permutation of $\{i_1, \dots, i_m\}$) and the resulting probability distributions for what happens with the indices $\{i_1, \dots, i_m\}$ do not match.
3. The adversary's answers result in pseudo-expectation values such that some problem equation $s_i = 0$ is violated i.e. $\tilde{E}[fs_i] \neq 0$ for some polynomial f.

If the verifier is unable to find such a flaw then the adversary wins.

▶ Remark. Roughly speaking, when we say that the adversary specifies what happens with a set of indices I we mean that the adversary assigns values to all variables x_e such that the indices of e are contained in I. We make this more precise in Section 5.

The adversary often has a strategy for this game based on a story for what happens with the indices. For the problems we are analyzing, the adversary's stories are as follows:

1. Knapsack: We set k out of the n x_i to be 1 and set the rest to 0.
2. The MOD 2 principle: For each vertex i, the perfect matching contains precisely one of the edges which are incident to i.
3. The triangle problem: We have k independent sets of size $\frac{n}{k}$.

▶ Remark. The adversary's stories are not convicing to us, as we can understand integrality arguments. However, the adversary just has to fool SOS, which is poor at capturing integrality arguments.

We now demonstrate how these stories naturally give probability distributions for what happens with the indices and thus give pseudo-expectation values.

▶ **Example 18** (Knapsack)**.** For knapsack, if the verifier first queries vertex i, the adversary says that $x_i = 1$ with probability $\frac{k}{n}$ and $x_i = 0$ with probability $\frac{n-k}{n}$. Thus, according to the adversary the expected value of x_i is $\frac{k}{n}$ so we take $\tilde{E}[x_i] = \frac{k}{n}$

If the verifier then queries x_j, if we have $x_i = 1$ then the adversary says that $x_j = 1$ with probability $\frac{k-1}{n-1}$ and $x_j = 0$ with probability $\frac{n-k}{n-1}$ as the adversary wants to set $k-1$ of the remaining $n-1$ variables to 1. If we have $x_i = 0$ then the adversary instead says that $x_j = 1$ with probability $\frac{k}{n-1}$ and $x_j = 0$ with probability $\frac{n-k-1}{n-1}$ as the adversary wants to set k of the remaining $n-1$ variables to 1. Thus, according to the adversary the expected value of $x_i x_j$ is $\frac{k(k-1)}{n(n-1)}$ so we take $\tilde{E}[x_i x_j] = \frac{k(k-1)}{n(n-1)}$.

Following similar logic, for all $I \subseteq [1, n]$ such that $|I| \leq d$, $\tilde{E}[\prod_{i \in I} x_i] = \frac{\binom{k}{|I|}}{\binom{n}{|I|}}$

▶ **Example 19** (MOD 2 principle)**.** For the MOD 2 principle, if the verifier first queries i, the adversary gives no information because there is nothing distinguishing i from other vertices. If the verifier then queries j, the adversary says that $x_{ij} = 1$ with probability $\frac{1}{n-1}$ and $x_{ij} = 0$ with probability $\frac{n-2}{n-1}$ because the adversary wants to match 1 out of the remaining $n-1$ vertices with i. Thus, we take $\tilde{E}[x_{ij}] = \frac{1}{n-1}$

We now consider $\tilde{E}[x_{ij}x_{kl}]$ where i,j,k,l are all distinct. $x_{ij}x_{kl} = 0$ unless $x_{ij} = 1$ so we can focus on the case when $x_{ij} = 1$, which according to the adversasry happens with probability $\frac{1}{n-1}$. In this case, if the verifier queries k, the adversary gives no additional information because there is nothing distinguishing k from other vertices in $[1,n] \setminus (i,j)$. If the verifier then queries l, the adversary says that $x_{kl} = 1$ with probabililty $\frac{1}{n-3}$ and $x_{kl} = 0$ with probabililty $\frac{n-4}{n-3}$ because the adversary wants to match 1 of the $n-3$ remaining vertices with k. Thus, we take $\tilde{E}[x_{ij}x_{kl}] = \frac{1}{(n-1)(n-3)}$

Following similar logic, we obtain that for all $E \subseteq \{(i,j) : i,j \in [1,n], i < j\}$ such that $|E| \leq d$, $\tilde{E}[\prod_{(i,j)\in E} x_{ij}] = \frac{1}{\prod_{j=1}^{|E|}(n-2j+1)}$ if E is a partial matching and $\tilde{E}[\prod_{(i,j)\in E} x_{ij}] = 0$ otherwise.

▶ **Example 20** (Triangle Problem)**.** For the triangle problem, if the verifier first queries i, the adversary gives no information because there is nothing distinguishing i from other vertices. If the verifier then queries j, the adversary says that j is in the same independent set as i with probability $\frac{\frac{n}{k}-1}{n-1}$ and is in a different independent set with probability $\frac{n-\frac{n}{k}}{n-1}$.

If the verifier then queries k, if i,j are in the same independent set then the adversary says that k is in the same independent set as i,j with probability $\frac{\frac{n}{k}-2}{n-2}$ and is in a different independent set with probability $\frac{n-\frac{n}{k}}{n-2}$. If i,j are in different independent sets then the adversary says that k is in the same independent set as i with probability $\frac{\frac{n}{k}-1}{n-2}$, k is in the same independent set as j with probability $\frac{\frac{n}{k}-1}{n-2}$, and k is in a different independent set with probability $\frac{n-2\frac{n}{k}}{n-2}$. Thus, the adversary gives the following probabilities for what happens with i,j,k:

1. The probability that i,j,k are all in the same independent set is $\frac{(\frac{n}{k}-1)(\frac{n}{k}-2)}{(n-1)(n-2)}$
2. The probability that i,j are in the same independent set and k is in a different independent set is $\frac{(\frac{n}{k}-1)(n-\frac{n}{k})}{(n-1)(n-2)}$. This is also the probability that i,k are in the same independent set and j is in a different independent set and the probability that j,k are in the same independent set and i is in a different independent set.
3. The probability that i,j,k are all in different independent sets is $\frac{(n-\frac{n}{k})(n-2\frac{n}{k})}{(n-1)(n-2)}$

This gives the following pseudo-expectation values:

1. $\tilde{E}[x_{ij}] = \frac{n-\frac{n}{k}}{n-1}$
2. $\tilde{E}[x_{ij}x_{ik}] = \tilde{E}[x_{ij}x_{jk}] = \tilde{E}[x_{ik}x_{jk}] = \frac{(\frac{n}{k}-1)(n-\frac{n}{k})}{(n-1)(n-2)} + \frac{(n-\frac{n}{k})(n-2\frac{n}{k})}{(n-1)(n-2)} = \frac{(n-\frac{n}{k})(n-\frac{n}{k}-1)}{(n-1)(n-2)}$
3. $\tilde{E}[x_{ij}x_{ik}x_{jk}] = \frac{(n-\frac{n}{k})(n-2\frac{n}{k})}{(n-1)(n-2)}$

▶ Remark. For the triangle problem, it is difficult to write down the general expression for $\tilde{E}$ explicitly. Fortunately, as we will show, we can verify the conditions of Definition 14 based on the story for $\tilde{E}$

4 Symmetry and SOS lower bounds

In this section, we highlight how symmetry can help prove SOS lower bounds even without additional assumptions. In particular, we have the following theorem which essentially follows from Corollary 2.6 of [30].

▶ **Theorem 21.** *If $\tilde{E}$ is a linear map from polynomials to $\mathbb{R}$ which is symmetric with respect to permutations of $[1,n]$ then for any polynomial g, we can write*

$$\tilde{E}[g^2] = \sum_{I\subseteq[1,n],j:|I|\leq indexdeg(g)} \tilde{E}[g_{Ij}^2]$$

where for all I,j,

1. g_{Ij} *is symmetric with respect to permutations of* $[1,n] \setminus I$.
2. $indexdeg(g_{Ij}) \leq indexdeg(g)$
3. $\forall i \in I, \sum_{\sigma \in S_{[1,n]\setminus(I\setminus\{i\})}} \sigma(g_{Ij}) = 0$

Theorem 21 is very useful for proving SOS lower bounds on symmetric problems because it implies that instead of checking that $\tilde{E}[g^2] \geq 0$ for all polynomials of index degree $\leq \frac{d}{2}$, it is sufficient to check polynomials which are symmetric under permutations of all but $\frac{d}{2}$ indices. However, despite its simplicity, Theorem 21 is quite deep. To prove Theorem 21, we must carefully decompose g and then use symmetry to analyze all of the non-square terms of g^2 and either eliminate them or reduce them to square terms. Fortunately, this has already been done by Corollary 2.6 of [30] using representation theory. We now sketch how Theorem 21 follows from Corollary 2.6 of [30].

Proof sketch of Theorem 21 using Corollary 2.6 of [30].

▶ **Definition 22** (Definition 2.1 of [30]). If $\oplus_\lambda V_\lambda$ is the isotypic decomposition of the vector space of polynomials of degree $\leq d$ and τ_λ is a tableau of shape λ, define

$$W_{\tau_\lambda} := V_\lambda^{\mathcal{R}_{\tau_\lambda}}$$

to be the subspace of the isotypic V_λ fixed by the action of the row group $\mathcal{R}_{\tau_\lambda}$ (which keeps each row of τ_λ fixed but may permute the elements within each row of τ_λ)

Corollary 2.6 of [30] (rephrased slightly) says the following:

▶ **Corollary 23** (Corollary 2.6 of [30]). *Suppose p is a polynomial on the variables $\{x_{ij} : i,j \in [1,n], i<j\}$ such that p is symmetric under permutations of $[1,n]$ and p can be written as a sum of squares of polynomials of degree $\leq d$. For each partition $\lambda \vdash n$, fix a tableau τ_λ of shape λ and choose a vector space basis $\{b_1^{\tau_\lambda}, \ldots, b_{m_\lambda}^{\tau_\lambda}\}$ for W_{τ_λ}. Then for each partition $\lambda \in \Lambda$, there exists an $m_\lambda \times m_\lambda$ PSD matrix Q_λ such that*

$$p = \sum_{\lambda \in \Lambda} tr(Q_\lambda Y^{\tau_\lambda})$$

where $\Lambda := \{\lambda \vdash n : \lambda \geq_{lex} (n-2d, 1^{2d})\}$ and $Y_{ij}^{\tau_\lambda} := sym(b_i^{\tau_\lambda} b_j^{\tau_\lambda})$

Using Corollary 2.6 of [30], we can prove Theorem 21 as follows. Since $\tilde{E}$ is symmetric, $\tilde{E}[g^2] = \tilde{E}[sym(g^2)]$ where $sym(g^2) = \frac{1}{n!}\sum_{\sigma \in S_n} (\sigma(g))^2$. Since $sym(g^2)$ is symmetric and a sum of squares, by Corollary 2.6 of [30], there exist PSD matrices Q_λ such that

$$\tilde{E}[g^2] = \sum_{\lambda \in \Lambda} \tilde{E}[tr(Q_\lambda Y^{\tau_\lambda})]$$

Since $\tilde{E}$ is symmetric, this implies that

$$\tilde{E}[g^2] = \sum_{\lambda \in \Lambda} \tilde{E}[tr(Q_\lambda Y'^{\tau_\lambda})]$$

where $Y'^{\tau_\lambda}_{ij} := b_i^{\tau_\lambda} b_j^{\tau_\lambda}$. Now consider each $\lambda \in \Lambda$ separately and observe that since $Q_\lambda \succeq 0$, we can write $Q_\lambda = \sum_j q^j q^{jT}$ for some vectors $\{q^1, \ldots, q^{m_\lambda}\}$. Thus,

$$tr(Q_\lambda Y^{\tau_\lambda}) = tr(\sum_j q^j q^{jT} b^{\tau_\lambda} b^{\tau_\lambda T}) = \sum_j q^{jT} b^{\tau_\lambda} b^{\tau_\lambda T} q^j = \sum_j \left(\sum_{i \in m_\lambda} q_i^j b_i^{\tau_\lambda} \right)^2$$

which means we can reexpress $sym(g^2)$ as a sum of squares, each of which has the form $(\sum_{i=1}^{m_\lambda} c_i b_i^{\tau_\lambda})^2$ for some partition $\lambda \vdash n$, tableau τ_λ of shape λ, and coefficients $\{c_i\}$

For each square $(\sum_{i=1}^{m_\lambda} c_i b_i^{\tau_\lambda})^2$, let I be the set of indices which are not in the top row of τ_λ. To show the first statement of Theorem 21, observe that permuting the indices of $[1,n] \setminus I$ is just permuting the top row of τ_λ. By definition, the elements of W_{τ_λ} are all invariant under such permutations, so $\sum_{i=1}^{m_\lambda} c_i b_i^{\tau_\lambda}$ is invariant under permutations of $[1,n] \setminus I$, as needed.

▶ Remark. In the setting of Corollary 2.6 of [30] the variables are $\{x_{ij} : i,j \in [1,n], i<j\}$ so if g has degree d, g can have index degree $2d$ which matches the fact that $\Lambda := \{\lambda \vdash n : \lambda \geq_{lex} (n-2d, 1^{2d})\}$. To prove Thorem 21 as stated using Corollary 2.6 of [30], Corollary 2.6 of [30] must be restated in terms of index degree and the proof adjusted accordingly.

The second statement of Theorem 21 is trivial as all of the $b_i^{\tau_\lambda}$ are in the vector space of polynomials of degree $\leq d$ and thus index degree $\leq 2d$.

To show the third statement of Theorem 21, we need to prove the following lemma

▶ **Lemma 24.** *For any τ_λ, letting I be the set of indices which are not in the top row of τ_λ, for any $i \in I$ and any $p \in W_{\tau_\lambda}$,*

$$\sum_{\sigma \in S_{([1,n]\setminus I)\cup\{i\}}} \sigma(p) = 0$$

Proof sketch. This lemma follows from the following claim:

▶ **Definition 25.** Define $U_r = span\{p : \exists I \subseteq [1,n] : |I| = r, \forall \sigma \in S_{[1,n]\setminus I}, \sigma(p) = p\}$ and define

$$V_r = U_r/U_{r-1} = span\{p : \exists I \subseteq [1,n] : |I| = r, \forall \sigma \in S_{[1,n]\setminus I}, \sigma(p) = p, \forall J \subseteq [1,n] : |J| \leq r-1, \sum_{\sigma \in S_{[1,n]\setminus J}} \sigma(p) = 0\}$$

▶ **Claim 26.** $V_r = \oplus_{\lambda : \text{The top row of } \lambda \text{ has length } n-r} V_\lambda$

Assuming this claim, for any τ_λ, letting I be the set of indices which are not in the top row of τ_λ, for any $p \in W_{\tau_\lambda} \subseteq V_\lambda$ and any J such that $|J| < |I|$, $\sum_{\sigma \in S_{[1,n]\setminus J}} \sigma(p) = 0\}$. Taking $J = I \setminus \{i\}$, the result follows.

We defer the proof of this claim to the full version. ◀

◀

However, Corollary 2.6 of [30] does not give us an explicit expression for $\tilde{E}[g^2]$, so we can ask whether we can obtain an explicit expression for $\tilde{E}[g^2]$. It turns out that there is such an expression but it is quite complicated. For an alternative proof of Theorem 21 which is explicit and combinatorial but technical, see the full version of this paper.

5 Sum of squares lower bounds from symmetry and a good story

In this section, we show how strategies for the verifier/adversary game described in section 3 with certain properties, which we call good stories, imply SOS lower bounds.

5.1 Stories

In this subsection, we rigorously define what we mean by stories. Once the definition is understood, stories are generally recognizable on sight.

▶ **Definition 27.** Given a subset I of $[1, n]$, we define $\mathcal{P}_I$ to be the set of all polynomials which only depend on the variables $\{x_e : e \subseteq I\}$

▶ **Definition 28** (Stories)**.** Let P be the problem we are anaylzing and let $A = (i_1, \ldots, i_m)$ be a sequence of indices. We say that a strategy S for adversary is a level n' story for (P, A), describing what will happen with the remaining indices after we have already queried A, if the following is true:

1. $n' \leq n - |I_A|$
2. S specifies what happened with the indices in A. More precisely, there is a linear map $\tilde{E}_{S,A} : \mathcal{P}_{I_A} \to \mathbb{R}$ corresponding to S
3. For all $i \in [1, n] \setminus I_A$, S gives values $\{p_{ij}\}$ for the probabilities of level $n' - 1$ stories S_{ij} for $(P, A \cup (i))$.
4. We have that for all $i \in [1, n] \setminus I_A$, $\sum_j p_{ij} = 1$ and $\forall f \in \mathcal{P}_{I_A}, \forall j, \tilde{E}_{S,A}[f] = \tilde{E}_{S_{ij},(A\cup(i))}[f]$

Given a level n' story S for (P, A), for all sequences B such that $A \subseteq B$, letting i be the next element in B after A, we define $\tilde{E}_{S,B} = \sum_j p_{ij} \tilde{E}_{S_{ij},B}$

▶ Remark. Note that we do not require the values p_{ij} to be non-negative in this definition.

▶ Remark. For all of our examples we will have that $n' = n - |I_A|$ but we do not force this to be the case in the definition.

5.2 Useful story properties part 1

We now define several properties our stories may have which are useful for proving SOS lower bounds. In Section 6 we will describe a method for verifying these properties.

The first property we want is that our story S gives the same linear map $\tilde{E}_S$ regardless of the order we query the indices.

▶ **Definition 29.** We say that a level n' story S for (P, A) is self-consistent if whenever B, B' are sequences such that $A \subseteq B, A \subseteq B', |I_B \setminus I_A| \leq n', |I_B \setminus I_A| \leq n'$,

$$\forall p \in \mathcal{P}_{I_B \cap I_{B'}}, \tilde{E}_{S,B}[p] = \tilde{E}_{S,B'}[p]$$

If S is self-consistent then we define $\tilde{E}_S : \{f : indexdeg_{[1,n]\setminus I_A}(f) \leq n'\} \to \mathbb{R}$ to be the linear map such that for all monomials p such that $indexdeg_{[1,n]\setminus I_A}(p) \leq n'$, for any sequence B of length at most n' such that $I_B \cap I_A = \emptyset$ and B contains all indices in variables of p which are not in I_A, $\tilde{E}_S[p] = \tilde{E}_{S,(A\cup B)}[p]$

A second property we want is that our story sounds like we are taking the expected values over the uniform distribution of permutations of a single input graph G_0. To make this precise, we note a useful property such expected values have. We then define single-graph mimics to be stories/pseudo-expectation values which also have this property.

▶ **Proposition 30.** *If Ω is the trivial distribution consisting of a single graph G_0 then for any polynomials f and g, $E_\Omega[fg] = E_\Omega[f]E_\Omega[g]$*

Proof. $E_\Omega[fg] = f(G_0)g(G_0) = E_\Omega[f]E_\Omega[g]$ ◀

▶ **Proposition 31.** *If Ω is the uniform distribution over all permutations of a single graph G_0 then for all symmetric polynomials f and g, $E_\Omega[fg] = E_\Omega[f]E_\Omega[g]$.*

Proof. For any symmetric polynomial h and any permutation σ, $h(\sigma(G_0)) = h(G_0)$ which implies that $E_\Omega[h] = h(G_0)$. Thus, we again have that $E_\Omega[fg] = f(G_0)g(G_0) = E_\Omega[f]E_\Omega[g]$, as needed. ◀

▶ Remark. The property that $E[fg] = E[f]E[g]$ for all symmetric polynomials f, g is useful because it immediately implies that for all symmetric polynomials g, $E[g^2] = (E[g])^2 \geq 0$.

We now define single graph mimics.

▶ **Definition 32.** Let P be a symmetric problem with equations $\{s_i = 0\}$ and let I be a subset of $[1, n]$. We say that $\tilde{E}$ is a level n' single graph mimic for P on $[1, n] \setminus I$ if the following conditions hold:

1. $\tilde{E} : \{p : indexdeg_{[1,n]\setminus I}(p) \leq n'\} \to \mathbb{R}$ is a linear map which is symmetric under permutations of $[1, n] \setminus I$
2. For all i and all polynomials f such that $indexdeg_{[1,n]\setminus I}(f) + indexdeg_{[1,n]\setminus I}(s_i) \leq n'$, $\tilde{E}[fs_i] = 0$
3. For all polynomials f, g which are symmetric under permutations of $[1, n] \setminus I$ such that $indexdeg_{[1,n]\setminus I}(f) + indexdeg_{[1,n]\setminus I}(g) \leq n'$, $\tilde{E}[fg] = \tilde{E}[f]\tilde{E}[g]$.

We say that S is a level n' single-graph mimic for (P, A) if S is a self-consistent level n' story for (P, A) and $\tilde{E}_S$ is a level n' single-graph mimic for P on $[1, n] \setminus I_A$.

A third property we want is that is that our story assigns non-negative probabilities to its substories as long as we don't query too many indices. If our story and all of its substories satisfy these three properties then we call it a good story.

▶ **Definition 33.** We say that S is a level (r, n') good story for (P, A) if the following conditions hold:

1. S is a level n' single graph mimic for (P, A).
2. If $r > 0$ then for any $i \in [1, n] \setminus I_A$, the values p_{ij} are non-negative and the stories $\{S_{ij}\}$ are all level $(r - 1, n' - 1)$ good stories for $(P, A \cup (i))$.

5.3 SOS lower bounds from good stories

We now prove that good stories imply SOS lower bounds.

▶ **Theorem 34.** *Let P be a symmetric problem with equations $\{s_i = 0\}$. If we have a level (r, n') good story for P then index degree $d = \min\{2r, n'\}$ SOS fails to refute the equations for P.*

Proof. We need two components to prove this theorem. The first component is the following theorem which shows that if we have a good story then we satisfy all of the linear constraints on $\tilde{E}$ and we have that $\tilde{E}[g^2] \geq 0$ whenever g is symmetric under permutations of all but a few indices.

▶ **Theorem 35.** *Let P be a symmetric graph problem with constraints $\{s_i = 0\}$ (where the $\{s_i\}$ are polynomials in the input variables). If we have a level (r, n') good story S for P then the corresponding linear map $\tilde{E}_S : \{f : indexdeg(f) \leq n'\} \to \mathbb{R}$ satisfies the following properties*

1. *$\tilde{E}_S$ is symmetric under permutations of $[1, n]$*
2. *If $I \subseteq [1, n]$ is a subset of indices of size at most r and g is a polynomial which is symmetric under permutations of $[1, n] \setminus I$ such that $indexdeg_{[1,n]\setminus I}(g) \leq \frac{n'-|I|}{2}$ then $\tilde{E}_S[g^2] \geq 0$*
3. *For all i and all f such that $indexdeg(f) + indexdeg(s_i) \leq n'$, $\tilde{E}_S[fs_i] = 0$.*

Proof. Since S is a single graph mimic and single graph mimics are symmetric with respect to permutations of $[1,n]$, the first statement follows. Similarly, the third statement follows directly from condition 2 of Definition 32

For the second statement, by conditions 1 and 2 of Definition 33, we can express $\tilde{E}_S$ as a probability distribution Ω over level $n-|I|$ single graph mimics $\tilde{E}_j$ for P on $[1,n]\setminus I$. Since g is symmetric under permutations of $[1,n]\setminus I$, for all of the $\tilde{E}_j$, $\tilde{E}_j[g^2] = \tilde{E}_j[g]\tilde{E}_j[g] \geq 0$. We now have that $\tilde{E}_S[g^2] = E_{E_j\sim\Omega}\left[\tilde{E}_j[g^2]\right] \geq 0$, as needed. ◀

The second component we need is Theorem 21, which shows that it is sufficient to verify that $\tilde{E}_S[g^2] \geq 0$ whenever g is symmetric with respect to permutations of all but a few indices. which is exactly what is shown by Theorem 35.

With these components in hand, we now prove Theorem 34. We need to check the following:

1. Whenever $indexdeg(f) + indexdeg(s_i) \leq d = \min\{2r, n'\}$, $\tilde{E}_S[fs_i] = 0$.
2. Whenever $indexdeg(g) \leq \frac{d}{2} = \min\{r, \frac{n'}{2}\}$, $\tilde{E}_S[g^2] \geq 0$

For the first statement, note that $indexdeg(f) + indexdeg(s_i) \leq n'$, so by Theorem 35, $\tilde{E}_S[fs_i] = 0$. For the second statement, given a polynomial g of index degree at most $\frac{d}{2}$, by Theorem 21 we can write

$$\tilde{E}_S[g^2] = \sum_{I\subseteq[1,n],j:|I|\leq indexdeg(g)} \tilde{E}_S[g_{Ij}^2]$$

where for all I, j,

$$\forall i \in I, \sum_{\sigma\in S_{[1,n]\setminus(I\setminus\{i\})}} \sigma(g_{Ij}) = 0$$

We now use the following lemma to upper bound $indexdeg_{[1,n]\setminus I}(g_{Ij})$:

▶ **Lemma 36.** *If g_{Ij} is symmetric with respect to permutations of $[1,n]\setminus I$ and*

$$\forall i \in I, \sum_{\sigma\in S_{[1,n]\setminus(I\setminus\{i\})}} \sigma(g_{Ij}) = 0$$

then all monomials in g_{Ij} depend on all of the indices in I

Proof. Assume that there is an $i \in I$ and some monomial p which does not depend on i which has a nonzero coefficient in g_{Ij}. By symmetry, for all permutations σ of $[1,n]\setminus I$, the coefficient of $\sigma(p)$ is the same as the coefficient of p. However, these are also the coefficients of $\sigma_2(p)$ for permutations σ_2 of $[1,n]\setminus(I\setminus\{i\})$. Since $\forall i \in I, \sum_{\sigma\in S_{[1,n]\setminus(I\setminus\{i\})}} \sigma(g_{Ij}) = 0$, all of these coefficients must be 0, which is a contradiction. ◀

This lemma implies that for all of the g_{Ij}, $indexdeg_{[1,n]\setminus I}(g_{Ij}) \leq \frac{n'}{2} - |I| \leq \frac{n'-|I|}{2}$. Thus, by Theorem 35, $\tilde{E}_S[g_{Ij}^2] \geq 0$. Since this holds for all I, j, $\tilde{E}_S[g^2] \geq 0$, as needed. ◀

6 Verifying good stories

In this section, we describe a method to verify that a story S is a good story. For this method, we make the following assumption.

▶ **Definition 37.** We assume that the problem equations and S depend on a set of parameters and we take $\alpha_1, \ldots, \alpha_m$ to be these parameters.

▶ Remark. For knapsack and the triangle problem, we have two parameters n and k. For the MOD 2 principle we only have the parameter n.

6.1 Useful story properties part 2

We now describe two additional properties our stories may have which are useful for verifying that they are good stories. Once the definitions are understood, these properties are generally recognizable on sight.

One property S usually has is that the linear maps $\tilde{E}_{S,B}$ assign values to monomials which are rational functions of the parameters $\alpha_1, \dots, \alpha_m$.

▶ **Definition 38.** We say that a level n' story S for (P, A) is rational if the following conditions hold

1. For all B such that $A \subseteq B$ and $|I_B \setminus I_A| \leq n'$, for all monomials p such that $I(p) \subseteq I_B$, $\tilde{E}_{S,B}[p]$ is a rational function of the parameters $\alpha_1, \dots, \alpha_m$.
2. The rational functions $\{\tilde{E}_{S,B}[p] : A \subseteq B, |I_B \setminus I_A| \leq n', I(p) \subseteq I_B\}$ have a common denominator $q_S(\alpha_1, \dots, \alpha_m)$ and the degree of the numerator is bounded by a function of n' and $indexdeg(p)$.

A second property our stories may have is that there are many settings of the parameters $\alpha_1, \dots, \alpha_m$ for which S and $\tilde{E}_S$ actually correspond to probabilities and expected values of the uniform distribution over permutations of a single input G_0.

▶ **Definition 39.** Let S be a story for (P, A)

1. We say that S is honest for $(\alpha_1, \dots, \alpha_m)$ if S corresponds to what happens if we take the uniform distribution for all permutations of an actual input graph G_0 over $[1, n] \setminus I_A$ and G_0 satisfies the equations for P. Note that if this is the case then S is automatically a single graph mimic for (P, A) for the parameter values $(\alpha_1, \dots, \alpha_m)$ and $\tilde{E}_S[p] = E_{\sigma \in S_{[1,n] \setminus I_A}}[p(\sigma(G_0))]$
2. We say that S is z-honest for $(\alpha_1, \dots, \alpha_{m-1})$ if there are at least z values of α_m such that S is honest for $(\alpha_1, \dots, \alpha_m)$.
3. For all $j \in [1, m-2]$, we say that S is z-honest for $(\alpha_1, \dots, \alpha_j)$ if there are at least z values of α_{j+1} such that S is z-honest for $(\alpha_1, \dots, \alpha_{j+1})$.
4. We say that S is z-honest if there are at least z values of α_1 such that S is z-honest for (α_1).

The intution is that it is difficult for SOS to determine whether the parameters take one of these values for which we actually have a solution or we are in between these values.

The following lemma is very useful

▶ **Lemma 40.** *Let S be a story which is z-honest. If $p(\alpha_1, \dots, \alpha_m)$ is a polynomial such that $deg(p) < z$ and $p(\alpha_1, \dots, \alpha_m) = 0$ whenever S is honest for $(\alpha_1, \dots, \alpha_m)$ then $p(\alpha_1, \dots, \alpha_m) = 0$*

Proof. We prove this lemma by induction. Assume that $p(\alpha_1, \dots, \alpha_m) = 0$ whenever S is z-honest for $\alpha_1, \dots, \alpha_j$.

Consider p as a polynomial in the variables $\alpha_{j+1}, \dots, \alpha_m$. Each monomial has a coefficient which is a polynomial $c(\alpha_1, \dots, \alpha_j)$ and we must have that $c(\alpha_1, \dots, \alpha_j) = 0$ whenever S is z-honest for $\alpha_1, \dots, \alpha_j$. We now show that all of these coefficients $c(\alpha_1, \dots, \alpha_j)$ must be 0 whenever S is z-honest for $\alpha_1, \dots, \alpha_{j-1}$. To see this, consider such a polynomial $c(\alpha_1, \dots, \alpha_j)$ and assume that we have $\alpha_1, \dots, \alpha_{j-1}$ such that S is z-honest for $\alpha_1, \dots, \alpha_{j-1}$. Considering c as a polynomial in α_j, $c(\alpha_j) = 0$ whenever S is z-honest for $\alpha_1, \dots, \alpha_j$, which by definition happens for at least z values of α_j. Since $deg(c) < z$, we must have that $c(\alpha_1, \dots, \alpha_j) = c(\alpha_j) = 0$. Thus, $p(\alpha_1, \dots, \alpha_m) = 0$ whenever S is z-honest for $\alpha_1, \dots, \alpha_{j-1}$, as needed. ◀

6.2 Sufficient conditions for single graph mimics

With these definitions, we can now give sufficient conditions for showing that a story S is a single graph mimic.

▶ **Lemma 41.** *Let S be a level n' story for (P, A). If S and the parameter values $\alpha_1, \ldots, \alpha_m$ satisfy the following conditions*

1. *S is rational and symmetric with respect to permutations of $[1, n] \setminus I_A$.*
2. *For all $z > 0$, S is z-honest.*
3. *Letting $q_S(\alpha_1, \ldots, \alpha_m)$ be the common denominator for $\{\tilde{E}_{S,B}[p] : A \subseteq B, |I_B \setminus I_A| \leq n', I(p) \subseteq I_B\}$, $q_S(\alpha_1, \ldots, \alpha_m) \neq 0$*

then for the parameter values $\alpha_1, \ldots, \alpha_m$, S is a level n' single graph mimic for (P, A).

Proof. We need to verify the following for the given values of $\alpha_1, \ldots, \alpha_m$:

1. S is self-consistent.
2. For all i and all polynomials f such that $indexdeg_{[1,n]\setminus I_A}(f) + indexdeg_{[1,n]\setminus I_A}(s_i) \leq n'$, $\tilde{E}_S[fs_i] = 0$
3. For any polynomials f, g such that f, g are symmetric under permutations of $[1, n] \setminus I_A$ and $indexdeg_{[1,n]\setminus I_A}(f) + indexdeg_{[1,n]\setminus I_A}(g) \leq n'$, $\tilde{E}_S[fg] = \tilde{E}_S[f]\tilde{E}_S[g]$.

We first verify that S is self-consistent for the given values of $\alpha_1, \ldots, \alpha_m$. Let p be a monomial and let B, B' be sequences of indices such that $A \subseteq B$, $A \subseteq B'$, and $I(p) \subseteq I_B \cap I_{B'}$. Since S is rational, $\tilde{E}_{S,B}[p] = \frac{p_1(\alpha_1,\ldots,\alpha_m)}{q(\alpha_1,\ldots,\alpha_m)}$ and $\tilde{E}_{S,B'}[p] = \frac{p_2(\alpha_1,\ldots,\alpha_m)}{q(\alpha_1,\ldots,\alpha_m)}$ are rational functions of the parameters $\alpha_1, \ldots, \alpha_m$. Now note that whenever S is honest for $(\alpha_1, \ldots, \alpha_m)$, $\tilde{E}_{S,B'}[p] = \tilde{E}_{S,B}[p]$ which implies that

$$p_1(\alpha_1, \ldots, \alpha_m)q_S(\alpha_1, \ldots, \alpha_m) = p_2(\alpha_1, \ldots, \alpha_m)q_S(\alpha_1, \ldots, \alpha_m)$$

Since S is z-honest for all $z > 0$, by Lemma 40 we have that $p_1 q_S = p_2 q_S$ as polynomials in $\alpha_1, \ldots, \alpha_m$. Plugging in our actual values of $\alpha_1, \ldots, \alpha_m$, $q_S(\alpha_1, \ldots, \alpha_m) \neq 0$ so $p_1(\alpha_1, \ldots, \alpha_m) = p_2(\alpha_1, \ldots, \alpha_m)$ and thus $\tilde{E}_{S,B'}[p] = \tilde{E}_{S,B}[p]$, as needed.

We can use similar ideas to prove the second and third statements but there is a subtle point we must be careful of. A problem equations s_i may be a polynomial which is symmetric in $n \setminus I_A$ rather than being a fixed polynomial. In this case, $\tilde{E}_S[s_i]$ and $\tilde{E}_S[fs_i]$ will still be rational functions in the parameters $\alpha_1, \ldots, \alpha_m$. However, the equality $\tilde{E}_S[fs_i] = \frac{p_{fs_i}(\alpha_1,\ldots,\alpha_m)}{q_S(\alpha_1,\ldots,\alpha_m)}$ may break down if

$$indexdeg_{[1,n]\setminus I_A}(f) + indexdeg_{[1,n]\setminus I_A}(s_i) > n'$$

▶ **Example 42.** If $f = x_1x_2$ and $s_i = \sum_{i=1}^{n} x_i - k$ then

$$fs_i = x_1^2x_2 + x_1x_2^2 + x_1x_2 \sum_{i\in[1,n]\setminus\{1,2\}} x_i - kx_1x_2$$

and by symmetry

$$\tilde{E}_S[fs_i] = \tilde{E}_S[x_1^2x_2] + \tilde{E}_S[x_1x_2^2] + (n-2)\tilde{E}_S[x_1x_2x_3] - k\tilde{E}_S[x_1x_2]$$

Thus, fs_i generally has index degree 3 and $\tilde{E}_S[fs_i] = \frac{p_{fs_i}(\alpha_1,\ldots,\alpha_m)}{q_S(\alpha_1,\ldots,\alpha_m)}$ is a rational function of the parameters $\alpha_1, \ldots, \alpha_m$. However, if $n' = n = 2$ then we are missing the term $x_1x_2\sum_{i\in[1,n]\setminus\{1,2\}} x_i$ from fs_i which may break the equality $\tilde{E}_S[fs_i] = \frac{p_{fs_i}(\alpha_1,\ldots,\alpha_m)}{q_S(\alpha_1,\ldots,\alpha_m)}$. Note that this problem will not occur as long as

$$indexdeg_{[1,n]\setminus I_A}(f) + indexdeg_{[1,n]\setminus I_A}(s_i) \leq n'$$

With this point in mind, for the second statement, note that since S is rational and $indexdeg(f) + indexdeg(s_i) \leq n'$, we can write $\tilde{E}_S[fs_i] = \frac{p_{fs_i}(\alpha_1,\dots,\alpha_m)}{q(\alpha_1,\dots,\alpha_m)}$. Now observe that $\tilde{E}[fs_i] = 0$ whenever $\tilde{E}$ is honest for $(\alpha_1,\dots,\alpha_m)$ and thus $p_{fs_i}(\alpha_1,\dots,\alpha_m) = 0$ whenever S is honest for $(\alpha_1,\dots,\alpha_m)$. Since S is z-honest for all $z > 0$, by Lemma 40, $p_{fs_i}(\alpha_1,\dots,\alpha_m) = 0$ as a polynomial. Plugging in the given values of $\alpha_1,\dots,\alpha_m$, $q(\alpha_1,\dots,\alpha_m) \neq 0$ so $\tilde{E}_S[fs_i] = \frac{p_{fs_i}(\alpha_1,\dots,\alpha_m)}{q(\alpha_1,\dots,\alpha_m)} = 0$, as needed.

Similarly, for the third statement we want to view f, g, and fg as polynomials which depend on n rather than being fixed polynomials. Still, since S is rational and $indexdeg(f) + indexdeg(g) \leq n'$, we can write $\tilde{E}_S[f] = \frac{p_f(\alpha_1,\dots,\alpha_m)}{q(\alpha_1,\dots,\alpha_m)}$, $\tilde{E}_S[g] = \frac{p_g(\alpha_1,\dots,\alpha_m)}{q(\alpha_1,\dots,\alpha_m)}$, and $\tilde{E}_S[fg] = \frac{p_{fg}(\alpha_1,\dots,\alpha_m)}{q(\alpha_1,\dots,\alpha_m)}$. Now observe that $\tilde{E}_S[fg] = \tilde{E}_S[f]\tilde{E}_S[g]$ whenever S is honest for $(\alpha_1,\dots,\alpha_m)$ and thus

$$p_f(\alpha_1,\dots,\alpha_m)p_g(\alpha_1,\dots,\alpha_m) - q(\alpha_1,\dots,\alpha_m)p_{fg}(\alpha_1,\dots,\alpha_m) = 0$$

whenever S is honest for $(\alpha_1,\dots,\alpha_m)$. Since S is z-honest for all z, by Lemma 40, $p_f p_g - qp_{fg} = 0$ as a polynomial. Plugging in the given parameters $\alpha_1,\dots,\alpha_m$, $q(\alpha_1,\dots,\alpha_m) \neq 0$ so

$$\tilde{E}_S[fg] = \frac{p_{fg}(\alpha_1,\dots,\alpha_m)}{q(\alpha_1,\dots,\alpha_m)} = \frac{p_f(\alpha_1,\dots,\alpha_m)p_g(\alpha_1,\dots,\alpha_m)}{(q(\alpha_1,\dots,\alpha_m))^2} = \tilde{E}_S[f]\tilde{E}_S[g]$$ ◀

6.3 Verifying good stories

We are now ready to give sufficient conditions for a story to be a good story.

▶ **Theorem 43.** *If S is a story for (P, A) such that*

1. *S is symmetric with respect to permutations of $[1, n] \setminus I_A$*
2. *S is rational*
3. *For all $z > 0$, S is z-honest.*

then for a given choice of parameters $\alpha_1,\dots,\alpha_m$, if n' and r are numbers such that $n' \leq n - |I_A|$ and

1. *If we consider up to r further indices, the probabilities p_{ij} are always non-negative.*
2. *If we consider up to n' further indices, we may get negative values for some p_{ij} but these values are always well-defined (i.e. the denominator is nonzero).*

then S is a level (n', r) good story for (P, A).

Proof. Since we can consider up to n' further indices and get well-defined values for the p_{ij}, S is a level n' story for (P, A). Now by Lemma 41, S is a level n' single graph mimic for (P, A).

We now prove the theorem by induction on r. The base case $r = 0$ is trivial. If $r > 0$ then for all $i \in [1, n] \setminus I_A$, S gives non-negative values $\{p_{ij}\}$ for the probabilities of level $n' - 1$ stories S_{ij} for $(P, A \cup (i))$. Now note that for each of these S_{ij}, the values of subsequent p_{ij} will always be non-negative if we consider up to $r - 1$ further indices and will be well-defined if we consider up to $n' - 1$ further indices. Moreover, S_{ij} is symmetric with respect to permutations of $[1, n] \setminus (I_A \cup \{i\})$, rational, and is z-honest because S_{ij} is honest for $(\alpha_1,\dots,\alpha_m)$ whenever S is honest for $(\alpha_1,\dots,\alpha_m)$. Thus, by the inductive hypothesis, each S_{ij} is a level $(r - 1, n' - 1)$ good story for $(P, A \cup (i))$ so S is a level (r, n') good story for (P, A), as needed. ◀

6.4 Good stories for knapsack, the MOD 2 principle, and the triangle problem

In this subsection, we apply Theorem 43 to verify that our stories for knapsack, the MOD 2 principle, and the triangle problem are good stories.

▶ **Theorem 44.**

1. *Saying that we take k out n elements is a level $(\lfloor \min\{k, n-k\} \rfloor + 1, n)$ good story for the knapsack problem.*
2. *Saying that we every vertex is incident with precisely one edge is a level $(\lfloor \frac{n}{2} \rfloor + 1, n)$ good story for the MOD 2 principle.*
3. *Saying that we have k independent sets of size $\frac{n}{k}$ is a level $(\lfloor \min\{k, \frac{n}{k}\} \rfloor + 1, n)$ good story for the triangle problem.*

Proof. For knapsack and the triangle problem, we take $\alpha_1 = n$ and $\alpha_2 = k$. For the MOD 2 principle, we just take $\alpha_1 = n$.

Our stories are clearly rational and symmetric with respect to permutations of $[1, n]$. We now check that they are z-honest for all z.

For knapsack, note that our story is honest for (n, k) whenever k is an integer between 0 and n. Thus, whenever $n \geq z$ there are at least z values of k such that our story is honest for (n, k), which implies that our story is z-honest for (n) whenever $n \geq z$. For all z there are infinitely many valules of n such that $n \geq z$ so our story is z-honest for all z, as needed.

For the MOD 2 principle, note that our story is honest for (n) whenever n is an even integer. There are infinitely many even integers so our story is z-honest for all z, as needed.

For the triangle problem, note that ourstory is honest for (n, k) whenever k is an integer and n is divisible by k. Thus, whenever $n = a!$ and $a \geq z$ then there are at least z values of k such that our description is honest for (n, k), which implies that our story is z-honest for (n) whenever $n = a!$ and $a \geq z$. For all z there are infinitely many valules of n such that $n = a!$ where $a \geq z$ so our story is z-honest for all z, as needed.

All that we have to do now is to determine n' and r.

For knapsack, when we consider polynomials of index degree at most n', the common denominator will be $n(n-1)\dots(n-n'+1)$ as we are choosing n' elements one by one from $[1, n]$. This is well-defined as long as $n' \leq n$ so we may take $n' = n$. The probabilities will be non-negative up to the $(\lfloor \min\{k, n-k\} \rfloor + 1)$-th index we consider, so we may take $r = \lfloor \min\{k, n-k\} \rfloor + 1$.

For the MOD 2 principle, when we consider polynomials of index degree at most n', the common denominator will be $n(n-1)\dots(n-n'+1)$ as we are choosing n' elements one by one from $[1, n]$. This is well-defined as long as $n' \leq n$ so we may take $n' = n$. The probabilities will be non-negative up to the $(\lfloor \frac{n}{2} \rfloor + 1)$-th index we consider, so we may take $r = \lfloor \frac{n}{2} \rfloor + 1$.

For the triangle problem, when we consider polynomials of index degree at most n', the common denominator will be $k^{n'} n(n-1)\dots(n-n'+1)$. The additional $k^{n'}$ factor appears because there are $\frac{n}{k}$ choices for the first element in an independent set of size $\frac{n}{k}$, $\frac{n-k}{k}$ choices for the second element, etc. Again, this is well-defined as long as $n' \leq n$ so we may take $n' = n$. The probabilities will be non-negative up to the $(\lfloor \min\{k, \frac{n}{k}\} \rfloor + 1)$-th index we consider, so we may take $r = \lfloor \min\{k, \frac{n}{k}\} \rfloor + 1$ ◀

▶ **Corollary 45.**

1. *For all positive integers n and all non-integer $k \in [0, n]$, index degree $\min\{2\lfloor \min\{k, n-k\} \rfloor + 3, n\}$ SOS fails to refute the knapsack equations.*

2. *For all odd n, index degree n SOS fails to refute the equations for the MOD 2 principle.*
3. *For all $n \geq 6$, and all $k \in [1, n]$ such that $k \notin \mathbb{Z}$ or $\frac{n}{k} \notin \mathbb{Z}$, index degree $2\lfloor \min\{k, \frac{n}{k}\} \rfloor + 2$ SOS fails to refute the claim that Goodman's bound can be achieved for the triangle problem.*

References

1 Sanjeev Arora, Boaz Barak, and David Steurer. Subexponential Algorithms for Unique Games and Related Problems. *J. ACM*, 62(5):42:1–42:25, 2015.

2 Sanjeev Arora, Satish Rao, and Umesh Vazirani. Expander Flows, Geometric Embeddings and Graph Partitioning. *J. ACM*, 56(2):5:1–5:37, April 2009.

3 Boaz Barak, Siu On Chan, and Pravesh Kothari. Sum of Squares Lower Bounds from Pairwise Independence. In *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, STOC '15, pages 97–106, 2015.

4 Boaz Barak, Samuel Hopkins, Jonathan Kelner, Pravesh Kothari, Ankur Moitra, and Aaron Potechin. A Nearly Tight Sum-of-Squares Lower Bound for the Planted Clique Problem. In *IEEE 57th Annual Symposium on Foundations of Computer Science, FOCS 2016, 9-11 October 2016, Hyatt Regency, New Brunswick, New Jersey, USA*, pages 428–437, 2016.

5 Boaz Barak, Jonathan A. Kelner, and David Steurer. Rounding Sum-of-squares Relaxations. In *Proceedings of the Forty-sixth Annual ACM Symposium on Theory of Computing*, STOC '14, pages 31–40, 2014.

6 Boaz Barak, Jonathan A. Kelner, and David Steurer. Dictionary Learning and Tensor Decomposition via the Sum-of-Squares Method. In *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, STOC '15, pages 143–151, 2015.

7 Boaz Barak, Pravesh K. Kothari, and David Steurer. Quantum Entanglement, Sum of Squares, and the Log Rank Conjecture. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 975–988, 2017.

8 Boaz Barak and Ankur Moitra. Noisy Tensor Completion via the Sum-of-Squares Hierarchy. In *Proceedings of the 29th Conference on Learning Theory, COLT 2016, New York, USA, June 23-26, 2016*, pages 417–445, 2016.

9 Grigoriy Blekherman, João Gouveia, and James Pfeiffer. Sum of Squares on the hypercube. *Mathematische Zeitschrift*, 284(1-2):41–54, 2016.

10 Yash Deshpande and Andrea Montanari. Improved Sum-of-Squares Lower Bounds for Hidden Clique and Hidden Submatrix Problems. In *COLT*, volume 40 of *JMLR Workshop and Conference Proceedings*, pages 523–562. JMLR.org, 2015.

11 Karin Gatermann and Pablo Parrilo. Symmetry groups, semidefinite programs, and sums of squares. *Journal of Pure and Applied Algebra*, 192(1-3):95–128, 2004.

12 Rong Ge and Tengyu Ma. Decomposing Overcomplete 3rd Order Tensors using Sum-of-Squares Algorithms. In *APPROX-RANDOM*, volume 40 of *LIPIcs*, pages 829–849. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2015.

13 Michel X. Goemans and David P. Williamson. Improved Approximation Algorithms for Maximum Cut and Satisfiability Problems Using Semidefinite Programming. *J. ACM*, 42(6):1115–1145, November 1995.

14 A. Goodman. On sets of acquaintances and strangers at any party. *The American Mathematical Monthly*, 66(9):778–783, 1959.

15 Dima Grigoriev. Complexity of Positivstellensatz proofs for the knapsack. *Computational Complexity*, 10(2):139–154, 2001.

16 Dima Grigoriev. Linear lower bound on degrees of Positivstellensatz calculus proofs for the parity. *Theor. Comput. Sci.*, 259(1-2):613–622, 2001.

17 Samuel B. Hopkins, Pravesh Kothari, Aaron Henry Potechin, Prasad Raghavendra, and Tselil Schramm. On the Integrality Gap of Degree-4 Sum of Squares for Planted Clique. *ACM Trans. Algorithms*, 14(3):28:1–28:31, June 2018.

18 Samuel B. Hopkins, Pravesh K. Kothari, Aaron Potechin, Prasad Raghavendra, Tselil Schramm, and David Steurer. The power of sum-of-squares for detecting hidden structures. *CoRR*, abs/1710.05017, 2017.

19 Samuel B. Hopkins, Tselil Schramm, Jonathan Shi, and David Steurer. Fast spectral algorithms from sum-of-squares proofs: tensor decomposition and planted sparse vectors. In *STOC*, pages 178–191, 2016.

20 Pravesh K. Kothari, Ryuhei Mori, Ryan O'Donnell, and David Witmer. Sum of Squares Lower Bounds for Refuting Any CSP. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 132–145, 2017.

21 Adam Kurpisz, Samuli Leppänen, and Monaldo Mastrolilli. Sum-of-Squares Hierarchy Lower Bounds for Symmetric Formulations. In *IPCO*, volume 9682 of *Lecture Notes in Computer Science*, pages 362–374. Springer, 2016.

22 Jean B. Lasserre. Global Optimization with Polynomials and the Problem of Moments. *SIAM J. on Optimization*, 11(3):796–817, March 2000.

23 Monique Laurent. Lower Bound for the Number of Iterations in Semidefinite Hierarchies for the Cut Polytope. *Math. Oper. Res.*, 28(4):871–883, 2003.

24 Troy Lee, Anupam Prakash, Ronald de Wolf, and Henry Yuen. On the Sum-of-squares Degree of Symmetric Quadratic Functions. In *Proceedings of the 31st Conference on Computational Complexity*, CCC '16, pages 17:1–17:31, 2016.

25 Tengyu Ma, Jonathan Shi, and David Steurer. Polynomial-Time Tensor Decompositions with Sum-of-Squares. In *FOCS*, pages 438–446. IEEE Computer Society, 2016.

26 Raghu Meka, Aaron Potechin, and Avi Wigderson. Sum-of-squares Lower Bounds for Planted Clique. In *Proceedings of the Forty-seventh Annual ACM Symposium on Theory of Computing*, STOC '15, pages 87–96, 2015.

27 Yuri Nesterov. Squared functional systems and optimization problems. *High Performance Optimization*, pages 405–440, 2000.

28 Pablo Parrilo. *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization.* PhD thesis, California Institute of Technology, 2000.

29 Aaron Potechin and David Steurer. Exact tensor completion with sum-of-squares. In *Proceedings of the 30th Conference on Learning Theory, COLT 2017, Amsterdam, The Netherlands, 7-10 July 2017*, pages 1619–1673, 2017.

30 Annie Raymond, James Saunderson, Mohit Singh, and Rekha R. Thomas. Symmetric sums of squares over k-subset hypercubes. *Math. Program.*, 167(2):315–354, 2018.

31 Alexander A. Razborov. Flag algebras. *J. Symb. Log.*, 72(4):1239–1282, 2007.

32 Grant Schoenebeck. Linear Level Lasserre Lower Bounds for Certain k-CSPs. In *FOCS*, pages 593–602. IEEE Computer Society, 2008.

33 N. Shor. An approach to obtaining global extremums in polynomial mathematical programming problems. *Cybernetics and Systems Analysis*, 23(5):695–700, 1987.

34 Madhur Tulsiani. CSP gaps and reductions in the lasserre hierarchy. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 303–312, 2009.