SoS Certification for Symmetric Quadratic Functions and Its Connection to Constrained Boolean Hypercube Optimization

Adam Kurpisz ✉
Department of Mathematics, ETH Zürich, Switzerland

Aaron Potechin ✉
Department of Computer Science, University of Chicago, IL, USA

Elias Samuel Wirth ✉
Institute of Mathematics, TU Berlin, Germany

Abstract

We study the rank of the Sum of Squares (SoS) hierarchy over the Boolean hypercube for Symmetric Quadratic Functions (SQFs) in n variables with roots placed in points $k-1$ and k. Functions of this type have played a central role in deepening the understanding of the performance of the SoS method for various unconstrained Boolean hypercube optimization problems, including the Max Cut problem. Recently, Lee, Prakash, de Wolf, and Yuen proved a lower bound on the SoS rank for SQFs of $\Omega(\sqrt{k(n-k)})$ and conjectured the lower bound of $\Omega(n)$ by similarity to a polynomial representation of the n-bit OR function.

Leveraging recent developments on Chebyshev polynomials, we refute the Lee–Prakash–de Wolf–Yuen conjecture and prove that the SoS rank for SQFs is at most $O(\sqrt{nk}\log(n))$.

We connect this result to two constrained Boolean hypercube optimization problems. First, we provide a degree $O(\sqrt{n})$ SoS certificate that matches the known SoS rank lower bound for an instance of Min Knapsack, a problem that was intensively studied in the literature. Second, we study an instance of the Set Cover problem for which Bienstock and Zuckerberg conjectured an SoS rank lower bound of $n/4$. We refute the Bienstock–Zuckerberg conjecture and provide a degree $O(\sqrt{n}\log(n))$ SoS certificate for this problem.

2012 ACM Subject Classification Theory of computation → Semidefinite programming; Theory of computation → Convex optimization

Keywords and phrases symmetric quadratic functions, SoS certificate, hypercube optimization, semidefinite programming

Digital Object Identifier 10.4230/LIPIcs.ICALP.2021.90

Category Track A: Algorithms, Complexity and Games

Funding *Adam Kurpisz*: supported by SNSF project PZ00P2_174117.
Aaron Potechin: supported in part by NSF grant CCF-2008920.

1 Introduction

Semialgebraic proof systems, also called certificates of nonnegativity, are systematic methods to prove nonnegativity of polynomials over semialgebraic sets. One of the most successful approaches for constructing theoretically efficient algorithms for polynomial optimization problems is the Sum of Squares (SoS) certificate [17, 38, 39, 46],

For a wide variety of combinatorial optimization problems, SoS provides the best available algorithms [1, 14, 5, 19, 34]. The strength of this method has also come to light for Max CSP [32] and problems in robust estimation [21], dictionary learning [3, 45], tensor completion and decomposition [4, 20, 41], and problems arising from statistical physics [13].

However, the SoS algorithm also admits certain weaknesses. It is known to struggle with solving certain combinatorial optimization problems, e.g., [7, 10, 18, 26, 49]. In a seminal example, Grigoriev showed that a $\Omega(n)$ degree SoS certificate is needed to detect a simple integrality argument for the Knapsack problem [15], see also [16, 24, 31]. A degree $n^{\Omega(\varepsilon)}$ SoS algorithm was proved to be unable to asymptotically certify an upper bound smaller than 2 times the optimal value for Sherrington-Kirkpatric Hamiltonian [23, 13]. Moreover, the degree $\Omega(\sqrt{n})$ SoS hierarchy was proved to have problems scheduling unit size jobs on a single machine to minimize the number of late jobs, see [27], even though the problem is known to be solvable in polynomial time using the Moore-Hodgson algorithm [36]. Finally, various examples where the SoS hierarchy fares very badly have been shown for the planted clique [2, 35] and Max CSP problems [22, 48].

The discrepancy between the excellent performance of the SoS hierarchy and its severe weaknesses has been studied extensively throughout the last decade. Thus, a natural question arises: what factors determine the difficulty of solving a problem for the SoS method?

A prominent example that was studied through the lens of this question is the Max Cut problem, which not only lies at the center of SoS research but was also one of the first problems for which lower bounds of the SoS rank were studied. Grigoriev proved that SoS needs at least degree $\lfloor \frac{n}{2} \rfloor$ to certify the size of the maximum cut in an odd clique of n vertices [15], for alternative proofs see also [16, 24, 31]. In a breakthrough paper nearly two decades later, Parrilo showed that the Grigoriev lower bound is tight by proving that every n-variate polynomial of degree 2, nonnegative over Boolean hypercube has an SoS certificate of degree at most $\lceil \frac{n}{2} \rceil$, see [12]. Subsequently, the analog of the results by Grigoriev and Parrilo for higher degree symmetric functions recently appeared in [25, 44], respectively.

Many of the problem instances with large lower bounds of the SoS rank target known limitations of the SoS method such as an issue with dealing with integrality constraints. Indeed, certifying the size of the maximum cut in a clique can be transformed into the problem of proving nonnegativity of the *Symmetric Quadratic Function* (SQF) of the form $q_{\lceil \frac{n}{2} \rceil}(\mathbf{x})$ over the Boolean hypercube, where, throughout this paper, $q_k : \{0,1\}^n \to \mathbb{R}$ is a multivariate polynomial of the form

$$q_k(\mathbf{x}) := (|\mathbf{x}| - k)(|\mathbf{x}| - k + 1). \tag{1.1}$$

The optimization of degree 2 polynomials over the Boolean hypercube plays a central role in Theoretical Computer Science. This claim is supported by the fact that high degree optimization problems attracted limited attention, especially since solving an NP-complete problem can be reduced in polynomial time to proving nonnegativity of a degree-4 even form [37]. Moreover, if an SQF has a complex root with a corresponding conjugate root, the polynomial is globally nonnegative and admits an SoS certificate of degree 2. Similarly, there exists an SoS certificate of nonnegativity of degree 2 for SQFs over the Boolean hypercube if the roots are real and placed outside the interval $[0, n]$. Hence, the only interesting case is when the roots are real and located within some interval $[k-1, k]$ for $k \in \{1, \ldots, n\}$.

Finding an SoS representation of the symmetric function q_k has gained significant attention in the SoS community. However, up to this day, the exact SoS rank for q_k is not known. The most recent result towards a characterization of the SoS rank of q_k provides a lower and upper bound of the SoS degree that approximates the function q_k with SoS polynomials in l_1 and l_∞ norm [33]. However, since finding an exact SoS certificate is at least as difficult as providing an approximate SoS representation, the result implies that for $k \geqslant 2$, q_k does not admit an SoS certificate of degree smaller than $\Omega\left(\sqrt{k(n-k)}\right)$. Moreover, in [33], Lee, Prakash, de Wolf, and Yuen conjectured that the lower bound of the SoS approximate representation with error at most ε in the l_∞ norm is expected to be $\Omega\left(\sqrt{k(n-k)}+\sqrt{n\log(1/\varepsilon)}\right)$. They support the conjecture by arguing about similarity with approximating n-bit OR functions [40, 50]. This conjecture, if true, would imply a lower bound on the exact SoS certificate for SQFs of $\Omega(n)$, even for small, constant values of k. Proving this conjecture is left as an open question in [33]. In this paper, we refute the Lee–Prakash–de Wolf–Yuen (LPdWY) conjecture. We show that certifying SQFs is easier than representing n-bit OR functions. More specifically, we prove the following theorem.

▶ **Theorem 1.** *For any $k \in \{2,\dots,\lceil\frac{n}{2}\rceil\}$, there exists a degree $O(\sqrt{nk}\log(n))$ SoS certificate of nonnegativity for the Boolean function q_k as in* (1.1)*.*

We motivate the research on the SoS degree of the SQFs q_k by connecting it to two combinatorial optimization problems. We first consider the instance of the Min Knapsack (MK) problem. For $P \geqslant 2$, the problem is defined as:

$$\text{MK:} \qquad \min\sum_{i\in[n]} x_i \qquad \text{s.t.} \quad \sum_{i\in[n]} x_i \geqslant \frac{1}{P}, \qquad \mathbf{x}\in\{0,1\}^n. \tag{1.2}$$

For $P = 2$, the problem was previously considered by Cook and Dash [11]. They proved that the Lovasz-Schrijver hierarchy rank is n. For the Sherali-Adams hierarchy, Laurent proved that the rank is also equal to n and raised the open question to find the rank for the SoS hierarchy [30]. For $n = 2$, they also proved that the SoS rank is 2, but the discussion of general n was left as an open question. Currently, it is known that the SoS rank of the MK problem falls within $\Omega(\sqrt{n})$ and $\lceil\frac{n+4\lceil\sqrt{n}\rceil}{2}\rceil$, see [28]. In this paper, we prove an upper bound on the SoS rank for the MK problem.

▶ **Theorem 2.** *The SoS rank for the MK problem is $\Omega(\sqrt{n}\log(P))$.*

The existing lower bound for general P (see Lemma 14 of [28]) is $\Omega(\sqrt{n\log(P)})$, so this is tight when P is constant, though for larger P there is a gap of $O(\sqrt{\log(P)})$.

We also consider the following instance of the Set Cover (SC) problem:

$$\text{SC:} \qquad \min\sum_{i\in[n]} x_i \qquad \text{s.t.} \quad \sum_{i\in[n]\setminus\{j\}} x_i \geqslant 1 \quad \forall j\in[n], \qquad \mathbf{x}\in\{0,1\}^n. \tag{1.3}$$

This instance was considered in [8] and it is known that the SoS hierarchy cannot solve this problem with a degree smaller than $\Omega(\sqrt{n})$ [28]. In [8], Bienstock and Zuckerberg raised the question of what the actual SoS rank of this polytope is, conjecturing that, based on numerical experiments, the SoS rank is at least $\frac{n}{4}$. In this paper, using the SoS certificate for SQFs in Theorem 1, we refute the Bienstock–Zuckerberg conjecture and provide a nearly tight SoS rank for the SC problem:

▶ **Theorem 3.** *The SoS rank for the SC problem is at most $O(\sqrt{n}\log(n))$.*

2 Preliminaries

For $n \in \mathbb{N}$, let $[n] = \{1,\dots,n\}$. For $\mathbf{x}\in\mathbb{R}^n$, let $\mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1,\dots,x_n]$ be the ring of *n-variate real polynomials*. For a set of polynomials $\mathcal{G} \subseteq \mathbb{R}[x]$, the corresponding *semialgebraic set* is

$$\mathcal{G}_+ \;:=\; \{\mathbf{x}\in\mathbb{R}^n \mid g(\mathbf{x}) \geqslant 0 \text{ for all } g\in\mathcal{G}\} \subseteq \mathbb{R}^n.$$

Throughout this paper, we consider optimization problems on the Boolean hypercube $\{0,1\}^n$ and therefore, for $\mathcal{H} := \{\pm(x_1^2 - x_1),\dots,\pm(x_n^2-x_n)\}$, we assume that $\mathcal{G}$ is of the form

$$\mathcal{G} \;:=\; \mathcal{H}\cup\{g_1,\dots,g_m :\; g_i\in\mathbb{R}[\mathbf{x}] \text{ for all } \; i\in[m]\},$$

where $m \in \mathbb{N}_{>0}$. This implies that $\mathcal{G}_+ \subseteq \{0,1\}^n$. Moreover, define the *cone of nonnegative polynomials with respect to a given semialgebraic set,* $\mathcal{G}_+$, as

$$\mathcal{K}(\mathcal{G}_+) \ := \ \{f \in \mathbb{R}[\mathbf{x}] \mid f(\mathbf{x}) \geqslant 0 \text{ for all } \mathbf{x} \in \mathcal{G}_+\}.$$

For given $f \in \mathbb{R}[\mathbf{x}]$ and $\mathcal{G} \subseteq \mathbb{R}[\mathbf{x}]$, define the corresponding *Constrained Polynomial Optimization Problem* (CPOP) as

$$f^* \ := \ \min\{f(\mathbf{x}) \mid \mathbf{x} \in \mathcal{G}_+\} \ = \ \max\{\lambda \in \mathbb{R} \mid f - \lambda \in \mathcal{K}(\mathcal{G}_+)\}.$$

Generally, since CPOP is NP-hard, it is desirable to find a proper subset that is a good inner approximation of $\mathcal{K}(\mathcal{G}_+)$ such that the corresponding program is computationally *tractable*.

The *SoS method* approximates the cone $\mathcal{K}(\mathcal{G}_+)$ by using the set of *sum of square polynomials*. We define the set of finite sum of squares polynomials as $\Sigma := \{s \mid s = \sum_{i=1}^k s_i^2, s_i \in \mathbb{R}[\mathbf{x}] \ \forall i \in [k], k \in \mathbb{N}_{>0}\}$ and let $\Sigma_{n,d} := \{s \mid s = \sum_{i=1}^k s_i^2, s_i \in \mathbb{R}[\mathbf{x}] \wedge \deg(s_i) \leqslant d \ \forall i \in [k], k \in \mathbb{N}_{>0}\}$ denote the polynomials which are sums of squares of polynomials of degree at most d. We define the *hierarchy of certificates of nonnegativity depending on* $d, n \in \mathbb{N}$ as

$$\Sigma_{n,d}^{\mathcal{G}} := \left\{ s_0 + \sum_{i=1}^{m} s_i g_i \mid s_i \in \Sigma_{n,d},\ g_i \in \mathcal{G} \ \forall i \in [m] \text{ and } s_0 \in \Sigma_{n,2\left\lceil \frac{2d+\deg(\mathcal{G})}{2} \right\rceil} \right\},$$

where $\deg(\mathcal{G}) = \max\{\deg(g) \mid g \in \mathcal{G}\}$. The *degree d SoS certificate* for f being nonnegative over $\mathcal{G}_+$ is $f \in \Sigma_{n,d}^{\mathcal{G}}$. Moreover, throughout the paper we say that a multivariate polynomial f is *a degree d SoS modulo Boolean axioms* if $f \in \Sigma_{n,d}^{\mathcal{H}}$. The *degree d SoS program* for CPOP is

$$f_\Sigma^d \ := \quad \max\{\lambda \in \mathbb{R} \mid f - \lambda \in \Sigma_{n,d}^{\mathcal{G}}\} \tag{2.1}$$

and is called *exact* if $f_\Sigma^d = f^*$. The smallest degree d such that the degree d SoS program is exact is called the *SoS rank*. Over the Boolean hypercube, the degree d SoS program can be solved via a *semidefinite program* (SDP) of size $O(m \sum_{k=0}^d \binom{n}{k})$. Moreover, the degree n SoS program is exact, see, e.g., [6, 29, 30].

Throughout this paper, we often encounter the following type of multivariate polynomials.

▶ **Definition 4.** *A polynomial $f : \ \{0,1\}^n \to \mathbb{R}$ is* symmetric *if there exists a univariate polynomial $\tilde{f} \ : \mathbb{R} \to \mathbb{R}$ such that $f(\mathbf{x}) = \tilde{f}\left(\sum_{i=1}^n x_i\right)$ for all $\mathbf{x} \in \{0,1\}^n$.*

With this in mind, let $|\mathbf{x}| := \sum_{i=1}^n x_i$ for any $\mathbf{x} \in \{0,1\}^n$. To prove SoS rank upper bounds, we consider symmetric multivariate polynomials over $\{0,1\}^n$ as univariate polynomials over $[0,n]$ and apply one of the many results on SoS certificates for univariate polynomials.

▶ Remark 5. Throughout this paper, we make frequent use of the fact that SoS certificates for polynomials over $[0,n]$ translate to SoS certificates for symmetric polynomials over $\{0,1\}^n$. More formally, if a univariate polynomial $\tilde{f} \ : \mathbb{R} \to \mathbb{R}$ has an univariate SoS certificate of degree d on $[0,n]$, then the multivariate polynomial $f \ : \{0,1\}^n \to \mathbb{R}$ such that $f(\mathbf{x}) := \tilde{f}(|\mathbf{x}|)$ has a degree d SoS certificate of nonnegativity over the Boolean hypercube.

In this paper, we use the following theorem to prove the SoS rank for univariate polynomials.

▶ **Theorem 6** ([9, Theorem 3.72])**.** *Let $a < b$. Then the univariate polynomial $p(x)$ is nonnegative on $[a,b]$ if and only if it can be written as*

$$\begin{cases} p(x) = s(x) + (x-a)(b-x)\cdot t(x) & \textit{if } \deg(p) \textit{ is even,} \\ p(x) = (x-a)\cdot s(x) + (b-x)\cdot t(x) & \textit{if } \deg(p) \textit{ is odd,} \end{cases}$$

where s, t are sum of squares. In the first case, we have $\deg(p) = 2d$, $\deg(s) \leqslant 2d$, and $\deg(t) \leqslant 2d-2$. In the second, $\deg(p) = 2d+1$, $\deg(s) \leqslant 2d$, and $\deg(t) \leqslant 2d-2$.

Finally, throughout the paper we use degree-d Chebyshev polynomials of the first type, which were used is several applications for bounds of sum of squares ranks, i.e., [28, 47, 42]. We frequently use the following lemma.

▶ **Lemma 7.** *Let $n, d \in \mathbb{N}$ such that $d \leqslant n$. Then,*

1. *For all $c \in [0, n]$, $T_d^2\left(-1-\frac{c}{n}\right) \geqslant \frac{1}{4}\left(-1-\sqrt{\frac{2c}{n}}\right)^{2d}$ and $T_d^2\left(-1-\frac{c}{n}\right) \leqslant \left(-1-2\sqrt{\frac{2c}{n}}\right)^{2d}$.*

   Moreover, for constant c and n big enough, $T_d^2\left(-1-\frac{c}{n}\right) \leqslant \left(-1-\sqrt{\frac{2c+1}{n}}\right)^{2d}$.
2. *For all $c \in (n, \infty)$, $T_d^2\left(-1-\frac{c}{n}\right) \leqslant \left(-1-3\frac{c}{n}\right)^{2d}$.*

Proof. It holds that:

1. Consider the characterization of Chebyshev polynomials given in [43, Equation 1.12]: $T_d(x) = \frac{1}{2}\left(\left(x-\sqrt{x^2-1}\right)^d + \left(\sqrt{x^2-1}+x\right)^d\right)$. For $x = -1-\frac{c}{n}$ and $c \in [0, n]$, we have $T_d^2\left(-1-\frac{c}{n}\right) \geqslant \frac{1}{4}\left(\left(-1-\frac{c}{n}\right)-\sqrt{\left(-1-\frac{c}{n}\right)^2-1}\right)^{2d} \geqslant \frac{1}{4}\left(-1-\sqrt{\frac{2c}{n}}\right)^{2d}$ and
$$\begin{aligned} T_d^2\left(-1-\frac{c}{n}\right) &\leqslant \left(\left(-1-\frac{c}{n}\right)-\sqrt{\left(-1-\frac{c}{n}\right)^2-1}\right)^{2d} \\ &\leqslant \left(\left(-1-\frac{c}{n}\right)-\sqrt{\frac{2c}{n}+\frac{c^2}{n^2}}\right)^{2d} \\ &\leqslant \left(-1-\sqrt{\frac{c}{n}}-\sqrt{\frac{2c}{n}+\frac{c}{n}}\right)^{2d} \leqslant \left(-1-2\sqrt{\frac{2c}{n}}\right)^{2d}. \end{aligned} \tag{2.2}$$
   Moreover, we have $T_d^2\left(-1-\frac{c}{n}\right) \leqslant \left(\left(-1-\frac{c}{n}\right)-\sqrt{\left(-1-\frac{c}{n}\right)^2-1}\right)^{2d} \leqslant \left(-1-\sqrt{\frac{2c+1}{n}}\right)^{2d}$, where the last inequality holds for n large compared to c.
2. For $x = -1-\frac{c}{n}$ and $c \in (n, \infty)$, we have
$$\begin{aligned} T_d^2\left(-1-\frac{c}{n}\right) &\leqslant \left(\left(-1-\frac{c}{n}\right)-\sqrt{\left(-1-\frac{c}{n}\right)^2-1}\right)^{2d} \\ &\leqslant \left(\left(-1-\frac{c}{n}\right)-\sqrt{\frac{2c}{n}+\frac{c^2}{n^2}}\right)^{2d} \\ &\leqslant \left(-1-\frac{c}{n}-\sqrt{\frac{2c^2}{n^2}+\frac{c^2}{n^2}}\right)^{2d} \leqslant \left(-1-3\frac{c}{n}\right)^{2d}. \end{aligned} \tag{2.3}$$

◀

3 SoS rank for SQFs

In this section, we refute the LPdWY conjecture stated in [33] by proving Theorem 1. To prove Theorem 1, it is sufficient to prove the following theorem.

▶ **Theorem 8.** *For all $n \in \mathbb{N}$ and all $k \in [n]$, there exists a polynomial $s(x)$ of degree $O(\sqrt{kn}\log(n))$ such that*

1. *$s\left(\sum_{i=1}^n x_i\right)$ is a sum of squares (modulo the Boolean axioms).*
2. *For all $x \in [0, n]$, $(x-k+1)(x-k) - s(x) \geqslant 0$.*

Indeed, by Theorem 8 and Theorem 6, there exist sum of squares polynomials s, s_1 and s_2 of degree $O(\sqrt{kn}\log(n))$ s.t.

$$(x-k+1)(x-k) = s(x) + s_1(x) + s_2(x)x(n-x).$$

We now make the following observations:

1. By Theorem 8, $s(\sum_{i=1}^n x_i)$ is a sum of squares polynomial modulo the Boolean axioms.
2. $s_1(\sum_{i=1}^n x_i)$, $s_2(\sum_{i=1}^n x_i)$ are sum of squares polynomials.
3. $\sum_{i=1}^n x_i = \sum_{i=1}^n x_i^2 - \sum_{i=1}^n \left(x_i^2 - x_i\right)$ is a sum of squares polynomial modulo the Boolean axioms.
4. $n - \sum_{i=1}^n x_i = \sum_{i=1}^n (1-x_i) = \sum_{i=1}^n \left((x_i-1)^2 - \left(x_i^2 - x_i\right)\right)$ is a sum of squares polynomial modulo the Boolean axioms.

Putting everything together, the multivariate polynomial $q_k(\mathbf{x})$ has an $O(\sqrt{kn}\log(n))$ SoS certificate modulo the Boolean axioms of the form

$$q_k(\mathbf{x}) = s\left(\sum_{i=1}^n x_i\right) + s_1\left(\sum_{i=1}^n x_i\right) + s_2\left(\sum_{i=1}^n x_i\right)\left(\sum_{i=1}^n x_i\right)\left(n - \sum_{i=1}^n x_i\right).$$

Before we prove Theorem 8, we make the following observation which shows that our upper bound for $q_k(x)$ applies for any symmetric quadratic function with roots in $[k-1,k]$.

▶ **Corollary 9.** *For any $k \in \{1,\ldots,\lceil n/2\rceil\}$ and any $a \leqslant b \in [k-1,k]$, a polynomial $f_k := (x-a)(x-b)$ admits an SoS certificate over the Boolean hypercube of degree at most the degree of an SoS certificate over the Boolean hypercube for polynomial q_k.*

Proof. We have $f_k(x) \geqslant \big((k-a)(b-k+1) + (k-b)(a-k+1)\big)\, q_k(x)$ as

$$\begin{aligned}
&(|x|-a)(|x|-b)\\
&= \big((k-a)(|x|-k+1) + (a-k+1)(|x|-k)\big)\big((k-b)(|x|-k+1) + (b-k+1)(|x|-k)\big)\\
&= (k-a)(k-b)(|x|-k+1)^2 + (a-k+1)(b-k+1)(|x|-k)^2\\
&+ \big((k-a)(b-k+1) + (k-b)(a-k+1)\big)(|x|-k+1)(x-|k|)
\end{aligned}$$

and invoke Theorem 1 to conclude the proof. ◀

3.1 Proof of Theorem 8

We construct $s(x)$ in two steps. We first construct a polynomial $s_1(x)$ which is a sum of squares (modulo the Boolean axioms), is less than or equal to $(x-k+1)(x-k)$ on the interval $[0,2k-1]$, and is not too large on the interval $[2k-1,n]$. We then construct a polynomial $s_2(x)$ which is a sum of squares, is less than or equal to 1 on the intervals $[0,k-1]$ and $[k,2k-1]$, is greater than or equal to 1 on the interval $[k-1,k]$, and is very small on the interval $[2k-1,n]$. We then take $s(x) = s_1(x)s_2(x)$. More precisely, we have the following conditions on s_1 and s_2:

1. $s_1\left(\sum_{i=1}^n x_i\right)$ is a sum of squares (modulo the Boolean axioms) and $s_2(x)$ is a sum of squares.
2. For all $x \in [k-1,k]$, $\frac{s_1(x)}{(x-k+1)(x-k)} \geqslant 1$ and $s_2(x) \geqslant 1$.
3. For all $x \in [0,k-1] \cup [k,2k-1]$, $\frac{s_1(x)}{(x-k+1)(x-k)} \leqslant 1$ and $s_2(x) \leqslant 1$.
4. For all $x \in [2k-1,n]$, $\left|\frac{s_1(x)}{(x-k+1)(x-k)}\right| \leqslant n^{40k}$ and $s_2(x) \leqslant n^{-40k}$.
5. $s_1(x)$ has degree $O(k)$ and $s_2(x)$ has degree $O(\sqrt{nk}\log(n))$.

▶ **Proposition 10.** *If $s_1(x)$ and $s_2(x)$ satisfy the above conditions and we take $s(x) = s_1(x)s_2(x)$ then $s\left(\sum_{i=1}^n x_i\right)$ is a sum of squares (modulo the Boolean axioms) and for all $x \in [0,n]$, $(x-k+1)(x-k) - s(x) \geqslant 0$.*

Proof. We make the following observations:

1. Since $s_1\left(\sum_{i=1}^n x_i\right)$ is a sum of squares (modulo the Boolean axioms) and $s_2(x)$ is a sum of squares, the product $s\left(\sum_{i=1}^n x_i\right) = s_1\left(\sum_{i=1}^n x_i\right) s_2\left(\sum_{i=1}^n x_i\right)$ is a sum of squares (modulo the Boolean axioms).
2. For all $x \in [0,k-1] \cup [k,2k-1]$, since $(x-k+1)(x-k) \geqslant 0$, $\frac{s_1(x)}{(x-k+1)(x-k)} \leqslant 1$, and $0 \leqslant s_2(x) \leqslant 1$,
$$(x-k+1)(x-k) - s(x) = (x-k+1)(x-k)\left(1 - s_2(x)\frac{s_1(x)}{(x-k+1)(x-k)}\right) \geqslant 0.$$
3. For all $x \in [k-1,k]$, since $(x-k+1)(x-k) \leqslant 0$, $\frac{s_1(x)}{(x-k+1)(x-k)} \geqslant 1$, and $s_2(x) \geqslant 1$,
$$(x-k+1)(x-k) - s(x) = (x-k+1)(x-k)\left(1 - s_2(x)\frac{s_1(x)}{(x-k+1)(x-k)}\right) \geqslant 0.$$
4. For all $x \in [2k-1,n]$, since $(x-k+1)(x-k) \geqslant 0$, $\left|\frac{s_1(x)}{(x-k+1)(x-k)}\right| \leqslant n^{40k}$ and $|s_2(x)| \leqslant n^{-40k}$,
$$(x-k+1)(x-k) - s(x) = (x-k+1)(x-k)\left(1 - s_2(x)\frac{s_1(x)}{(x-k+1)(x-k)}\right) \geqslant 0. \blacktriangleleft$$

Thus, we have an SoS proof of degree $O(\sqrt{kn}log(n))$ that $(|x|-k+1)(|x|-k) \geqslant 0$.

3.1.1 Constructing the polynomial $s_1(x)$

We now construct the polynomial $s_1(x)$.

▶ **Lemma 11.** *For $n \in \mathbb{N}$ and all $k \in [n]$, there exists a polynomial $s_1(x)$ such that*

1. *$s_1\left(\sum_{i=1}^n x_i\right)$ has a degree $O(k)$ sum of squares (modulo the Boolean axioms) certificate.*
2. *For all $x \in [k-1,k]$, $\frac{s_1(x)}{(x-k+1)(x-k)} \geqslant 1$.*
3. *For all $x \in [0,k-1] \cup [k,2k-1]$, $\frac{s_1(x)}{(x-k+1)(x-k)} \leqslant 1$.*
4. *For all $x \in [2k-1,n]$, $\left|\frac{s_1(x)}{(x-k+1)(x-k)}\right| \leqslant n^{40k}$.*

Proof. For $k=1$, we can take $s_1(x) = x(x-1)$ so we can assume that $n \geqslant k \geqslant 2$. For $k \geqslant 2$, we use the following construction.[1]

▶ **Definition 12.** *For all natural numbers $k \geqslant 2$, define $g_k(x)$ to be the polynomial*
$$g_k(x) = x^{16k}(x-2k+1)^{16k} \prod_{i \in \{0,\ldots,2k-1\} \setminus \{k-1,k\}} (x-i).$$

▶ **Definition 13.** *Given a natural number n and $k \in \{2,3,\ldots,n\}$, we define $s_1(x)$ as follows:*

1. *If k is odd, then we define $s_1(x) = \frac{g_k(x)}{g_k(k-1)}(x-k+1)(x-k)$.*
2. *If k is even, then we define $s_1(x) = -\frac{g_k(x)(x+1)(x-2k)}{g_k(k-1)k(k+1)}(x-k+1)(x-k)$.*

[1] Definitions 12 and 13 are only used in the current section, Section 3.

We verify the desired properties. We first show that $s_1\left(\sum_{i=1}^n x_i\right)$ is a sum of squares (modulo the Boolean axioms). If k is odd, then since $g_k(k-1) > 0$, $\prod_{i=0}^{2k-1}\left(\left(\sum_{i=1}^n x_i\right) - i\right)$ is a sum of squares (modulo the Boolean axioms), and by [33, Lemma 4.4],

$$s_1\left(\sum_{i=1}^n x_i\right) = \frac{\left(\sum_{i=1}^n x_i\right)^{16k}\left(\left(\sum_{i=1}^n x_i\right) - 2k+1\right)^{16k}}{g_k(k-1)}\prod_{i=0}^{2k-1}\left(\left(\sum_{i=1}^n x_i\right) - i\right)$$

is a sum of squares (modulo the Boolean axioms). If k is even, then since $g_k(k-1) < 0$, $\left(\sum_{i=1}^n x_i\right) + 1$ and $\prod_{i=0}^{2k}\left(\left(\sum_{i=1}^n x_i\right) - i\right)$ are sum of squares (modulo the Boolean axioms),

$$s_1\left(\sum_{i=1}^n x_i\right) = -\frac{\left(\sum_{i=1}^n x_i\right)^{16k}\left(\left(\sum_{i=1}^n x_i\right) - 2k+1\right)^{16k}}{g_k(k-1)k(k+1)}\left(\left(\sum_{i=1}^n x_i\right) + 1\right)\prod_{i=0}^{2k}\left(\left(\sum_{i=1}^n x_i\right) - i\right)$$

is a sum of squares (modulo the Boolean axioms). Finally, to argue about the degree, note that by [33, Lemma 4.4], $\prod_{i=0}^{2k-1}\left(\left(\sum_{i=1}^n x_i\right) - i\right)$ has a sum of squares (modulo the Boolean axioms) certificate of degree $2k$ and thus, for all k, $s_1\left(\sum_{i=1}^n x_i\right)$ has a sum of squares (modulo the Boolean axioms) certificate of degree $O(k)$.

For the fourth property, observe that for $x \in [0, n]$, every term in the numerator (except for $(x+1)$ when k is even) has magnitude at most n, every term in the denominator has magnitude at least 1, and there are less than $40k$ terms in the numerator.

The second and third properties follow immediately from the following lemma.

▶ **Lemma 14.** *For all natural numbers $k \geqslant 2$, $g_k(x)$ satisfies the following properties:*

1. *For all $x \in [0, 2k-1]$, $g_k(2k-1-x) = g_k(x)$.*
2. *For all $x \in [k-1, k]$, $\frac{g_k(x)}{g_k(k-1)} \geqslant 1$.*
3. *For all $x \in [0, k-1] \cup [k, 2k-1]$, $\left|\frac{g_k(x)}{g_k(k-1)}\right| \leqslant 1$.*

Proof. Since the first and second properties hold for every term in the product $g_k(x) = (-1)^{k-1}\left(x(x-2k+1)\right)^{16k}\left(\prod_{i=0}^{k-2}(x-i)(2k-1-x-i)\right)$, they hold for $g_k(x)$ as well.

By symmetry, it suffices to show the third property for $x \in [0, k-1]$. For $x \in \{0, 1, \ldots, k-2\}$, $g_k(x) = 0$ and for $x \in (k-2, k-1)$, the third property holds for every term in this product, so it holds for $g_k(x)$ as well. To show that the third property holds for $x \in [0, k-2] \backslash \{0, 1, \ldots, k-2\}$, we compare $g_k(x-m)$ and $g_k(x)$, where $x \in (k-2, k-1)$ and $m \in \{0, 1, \ldots, k-2\}$. For this, we decompose $g_k(x)$ as $g_k(x) = a_k(x)b_k(x)^{16k}$, where $a_k(x) = \prod_{i \in \{0,\ldots,2k-1\}\backslash\{k-1,k\}}(x-i)$ and $b_k(x) = x(2k-1-x)$.

▶ **Lemma 15.** *Let $a_k(x) = \prod_{i \in \{0,\ldots,2k-1\}\backslash\{k-1,k\}}(x-i) = \left(\prod_{i=0}^{k-2}(x-i)\right)\left(\prod_{i=k+1}^{2k-1}(x-i)\right)$. For all $x \in (k-2, k-1)$ and all $m \in \{1, \ldots, k-2\}$, $\left|\frac{a_k(x-m)}{a_k(x)}\right| \leqslant e^{\frac{16m^2}{k}}$.*

Proof. Observe that

$$\begin{aligned}
\left|\frac{a_k(x-m)}{a_k(x)}\right| &= \left|\frac{\prod_{j=1}^m (x-k+2-j)}{\prod_{j=1}^m (x+1-j)} \cdot \frac{\prod_{j=1}^m (x-2k+1-j)}{\prod_{j=1}^m (x-k-j)}\right| \\
&= \left|\frac{\prod_{j=1}^m (k-2-x+j)}{\prod_{j=1}^m (k-x+j)} \cdot \frac{\prod_{j=1}^m (2k-x-1+j)}{\prod_{j=1}^m (x-m+j)}\right| \\
&\leqslant \left|\prod_{j=1}^m \left(\frac{k+1+j}{k-2-m+j}\right)\right|.
\end{aligned}$$

We distinguish between two cases.

1. If $m \leqslant \frac{3k}{4} - 1$, observe that

$$\left|\prod_{j=1}^{m}\left(\frac{k+1+j}{k-2-m+j}\right)\right| = \prod_{j=1}^{m}\left(1+\frac{m+3}{k-2-m+j}\right)$$
$$\leqslant \prod_{j=1}^{m}\left(1+\frac{m+3}{k-m-1}\right) \leqslant \prod_{j=1}^{m} e^{\frac{m+3}{k-m-1}} = e^{\frac{m(m+3)}{(k-m+1)}} \leqslant e^{\frac{16m^2}{k}}.$$

2. If $m > \frac{3k}{4} - 1$, then $m \geqslant \frac{3k}{4} - \frac{3}{4} \geqslant \frac{3k}{8}$ (as $k \geqslant 2$). Thus,

$$\left|\prod_{j=1}^{m}\left(\frac{k+1+j}{k-2-m+j}\right)\right| \leqslant \prod_{j=1}^{k-2}\left(\frac{k+1+j}{j}\right) = \frac{(2k-1)!}{(k-2)!(k+1)!} \leqslant 2^{2k-1} \leqslant e^{\frac{16m^2}{k}}.$$ ◀

▶ **Lemma 16.** *Let $b_k(x) = x(2k-1-x)$. For $x \in (k-2, k-1)$ and $m \in [k-2]$, $\left|\frac{b_k(x-m)}{b_k(x)}\right| \leqslant e^{-\frac{m^2}{k^2}}$.*

Proof. Observe that

$$\frac{b_k(x-m)}{b_k(x)} = \frac{(x-m)(2k-1+m-x)}{x(2k-1-x)} = \frac{x(2k-1-x)-(2k-1-2x)m-m^2}{x(2k-1-x)}$$
$$\leqslant 1 - \frac{m^2}{x(2k-1-x)} \leqslant 1 - \frac{m^2}{k^2} \leqslant e^{-\frac{m^2}{k^2}}.$$ ◀

▶ **Corollary 17.** *For all $x \in (k-2, k-1)$ and $m \in \{1, \ldots, k-2\}$, $\left|\frac{g_k(x-m)}{g_k(x)}\right| \leqslant 1$.*

Proof. By Lemmas 15 and 16, $\left|\frac{g_k(x-m)}{g_k(x)}\right| = \left|\frac{a_k(x-m)}{a_k(x)}\right|\left|\frac{b_k(x-m)}{b_k(x)}\right|^{16k} \leqslant e^{\frac{16m^2}{k}}\left(e^{-\frac{m^2}{k^2}}\right)^{16k} = 1.$ ◀

◀

◀

3.1.2 Constructing the polynomial $s_2(x)$

We now construct the polynomial $s_2(x)$.

▶ **Lemma 18.** *For all $n \in \mathbb{N}$ and all $k \in [n]$, there exists a polynomial $s_2(x)$ of degree $O(\sqrt{kn}log(n))$ satisfying the following properties:*

1. *$s_2(x)$ is a sum of squares.*
2. *For all $x \in [k-1, k]$, $s_2(x) \geqslant 1$.*
3. *For all $x \in [0, k-1] \cup [k, 2k-1]$, $s_2(x) \leqslant 1$.*
4. *For all $x \in [2k-1, n]$, $s_2(x) \leqslant n^{-40k}$.*

Proof.

▶ **Lemma 19.** *For $C := e^{8\sqrt{3}}$ and $k \in \{0, \ldots, \lceil n/2 \rceil\}$, $H_k = T^2_{\sqrt{\frac{n}{k}}}\left(2\frac{x}{n} - 1 - 2\frac{2k-1}{n}\right)$ satisfies the following properties:*

1. *For all $x \in [2k-1, n]$, $H_k(x) \leqslant 1$.*
2. *For all $k \in [0, 2k-1]$, $H'_k(x) < 0$.*
3. *$H_k(0) \leqslant C$.*
4. *$H_k(k) \geqslant 1.5$.*

Proof. Note that $H_k(x) = T^2_{\sqrt{\frac{n}{k}}}\left(2\frac{x}{n} - 1 - 2\frac{2k-1}{n}\right)$. Hence, $H_k(2k-1) = T^2_{\sqrt{\frac{n}{k}}}(-1) = 1$ and $H_k(n) = T^2_{\sqrt{\frac{n}{k}}}\left(1 - 2\frac{2k-1}{n}\right) \leqslant 1$, which implies the first property. We prove Properties (2) and (3). By Lemma 7, for k such that $4k-2 \leqslant n$, we have

$$H_k(0) = T^2_{\sqrt{\frac{n}{k}}}\left(-1 - \frac{4k-2}{n}\right) \leqslant \left(1 + \sqrt{\frac{32k-16}{n}}\right)^{2\sqrt{\frac{n}{k}}} \leqslant e^{2\sqrt{\frac{32k-16}{k}}} \leqslant e^{8\sqrt{3}}$$

and for k such that $4k-2 \geqslant n$, by Lemma 7, for $c \geqslant n$, we have

$$H_k(0) = T^2_{\sqrt{\frac{n}{k}}}\left(-1 - \frac{4k-2}{n}\right) \leqslant \left(1 + \frac{12k}{n}\right)^{2\sqrt{\frac{n}{k}}} \leqslant \left(1 + \sqrt{\frac{12k}{n}}\right)^{4\sqrt{\frac{n}{k}}} \leqslant e^{4\sqrt{\frac{12k}{k}}} \leqslant e^{8\sqrt{3}}.$$

Moreover, by Lemma 7 we have

$$H_k(k) = T^2_{\sqrt{\frac{n}{k}}}\left(-1 - \frac{2k-2}{n}\right) \geqslant \frac{1}{4}\left(1 + \sqrt{\frac{4k-4}{n}}\right)^{2\sqrt{\frac{n}{k}}} \geqslant \frac{1}{4}\left(1 + \sqrt{\frac{2k}{n}}\right)^{2\sqrt{\frac{n}{k}}},$$

where the last inequality holds because $k \geqslant 2$. Finally, since $n \geqslant 2k$,

$$\frac{1}{4}\left(1 + \sqrt{\frac{2k}{n}}\right)^{2\sqrt{\frac{n}{k}}} \geqslant \frac{1}{4}2^{2\sqrt{\frac{n}{k}}\sqrt{\frac{2k}{n}}} = \frac{1}{4}2^{2\sqrt{2}} \geqslant 1.5.$$ ◀

▶ **Lemma 20.** *For any constants a, b, C such that $1.5 \leqslant a < b < C$, there is a sum of squares polynomial $p_{a,b,C}(x)$ of degree at most $8\lceil C^2\rceil$ such that the following hold:*
1. *For all $x \in [a, b]$, $p_{a,b,C}(x) \geqslant 1$.*
2. *For all $x \in [0, 1]$, $|p_{a,b,C}(x)| \leqslant \frac{1}{2}$.*
3. *For all $x \in [0, a] \cup [b, C]$, $|p_{a,b,C}(x)| \leqslant 1$.*

Proof. We can take the polynomial

$$p_{a,b,C}(x) = \left(1 - \frac{(x-a)(x-b)}{C^2}\right)^{4\lceil C^2\rceil}.$$

We now make the following observations:
1. For all $x \in [a, b]$, $1 - \frac{(x-a)(x-b)}{C^2} \geqslant 1$ so $p_{a,b,C}(x) \geqslant 1$.
2. For all $x \in [0, 1]$, $|1 - \frac{(x-a)(x-b)}{C^2}| \leqslant 1 - \frac{1}{4C^2}$ so $|p_{a,b,C}(x)| \leqslant \left(1 - \frac{1}{4C^2}\right)^{4\lceil C^2\rceil} \leqslant \frac{1}{2}$.
3. For all $x \in [0, a] \cup [b, C]$, $|1 - \frac{(x-a)(x-b)}{C^2}| \leqslant 1$ so $|p_{a,b,C}(x)| \leqslant 1$. ◀

We construct the polynomial $s_2(x)$. For $k \in \{2, \dots, \lceil n/2\rceil\}$, let $s_2(x) := p_{a,b,C}\left(H_k(x)\right)^{40\lceil k\log(n)\rceil}$, where $a = H_k(k)$, $b = H_k(k-1)$, and $C = e^{8\sqrt{3}}$ is the constant given by Lemma 19.

▶ **Lemma 21.** *For any $k \in \{2, \dots, \lceil n/2\rceil\}$, $s_2(x)$ satisfies the properties in Lemma 18.*

Proof. We make the following observations:
1. For all $x \in [0, k-1] \cup [k, 2k-1]$, $H_k(x) \in [0, H_k(k)] \cup [H_k(k-1), C]$ so $|p_{a,b,C}(H_k(x))| \leqslant 1$ and thus $s_2(x) = p_{a,b,C}\left(H_k(x)\right)^{40\lceil k\log(n)\rceil} \leqslant 1$.
2. For all $x \in [k-1, k]$, $H_k(x) \in [H_k(k), H_k(k-1)]$ so $p_{a,b,C}(H_k(x)) \geqslant 1$ and thus $s_2(x) = p_{a,b,C}\left(H_k(x)\right)^{40\lceil k\log(n)\rceil} \geqslant 1$.
3. For all $x \in [2k-1, n]$, $H_k(x) \in [0, 1]$ so $|p_{a,b,C}(H_k(x))| \leqslant 1$ and thus, $s_2(x) = p_{a,b,C}\left(H_k(x)\right)^{40\lceil k\log(n)\rceil} \leqslant n^{-40k}$. ◀

◀

4 SoS rank upper bound for the MK problem via SQF certification

In this section, we prove an upper bound of $O(\sqrt{n}\log(P))$ on the SoS rank for the MK problem, which, together with the lower bound presented in [28], constitutes proof of Theorem 2.

We first discuss the necessary properties a candidate SoS certificate for the MK problem has to satisfy. A degree d SoS certificate for the MK problem is of the form $\sum_{i\in[n]} x_i - 1 = s_0(\mathbf{x}) + s_1(\mathbf{x})\left(\sum_{i\in[n]} x_i - \frac{1}{P}\right)$, where s_0, s_1 are SoS polynomials of degree $2d+2$ and $2d$, respectively. Through permutation of indices, the existence of an SoS certificate for the MK problem implies the existence of an SoS certificate such that s_1 is symmetric, that is, there exists $\tilde{s}_1 \ : \mathbb{R} \to \mathbb{R}$ such that $s_1(\mathbf{x}) = \tilde{s}_1(|\mathbf{x}|)$ for all $\mathbf{x} \in \{0,1\}^n$. Since s_0 is globally nonnegative, $\tilde{s}_1$ needs to satisfy

$$|\mathbf{x}| - 1 \geqslant \tilde{s}_1(|\mathbf{x}|)\left(|\mathbf{x}| - \frac{1}{P}\right) \qquad \text{for all } \mathbf{x} \in \{0,1\}^n. \tag{4.1}$$

Thus, $\tilde{s}_1(0) \geqslant P$, $\tilde{s}_1(1) = 0$, and $\tilde{s}_1(x) \leqslant \frac{x-1}{x-\frac{1}{P}}$ for $x \in \{2,\dots,n\}$.

We will construct a sum of squares polynomial $\tilde{s}_1$ which satisfies the following slightly stronger conditions:

1. $\tilde{s}_1(0) > P$
2. For all $x \in [1,2]$, $\tilde{s}_1(x) \leqslant \frac{x-1}{2}$
3. For all $x \in [2,n]$, $\tilde{s}_1(x) \leqslant \frac{1}{2}$

We will then observe that these conditions imply that

$$\tilde{s}_0(|x|) = |x| - 1 - \tilde{s}_1(|x|)\left(|x| - \frac{1}{P}\right)$$

is positive for all $x \in \{0\} \cup (1,n]$ which is sufficient to show that $\tilde{s}_0(x)$ is a sum of squares modulo the Boolean constraints.

A polynomial $T_{2\sqrt{n}}(\frac{x-1+r_0}{n} - 1)$, where r_0 is the smallest root of the polynomial $T_{2\sqrt{n}}(\frac{x}{n} - 1)$, which for $P = 2$ satisfies similar requirements was constructed in [28, Lemma 15] using properties of Chebyshev polynomials.

To obtain our polynomial $\tilde{s}_1(x)$, we generalize this construction using three parameters, the degree d of the Chebyshev polynomial, a scaling factor α, and an even power m.

▶ **Definition 22.** *Given an $\alpha > 0$, a natural number d, and an even natural number m, define $\tilde{s}_{\alpha,d,m}(x) := \alpha T_d\left(\frac{x-1+r_0}{n} - 1\right)^m$, where r_0 is the smallest root of the polynomial $T_d\left(\frac{x}{n} - 1\right)$.*

▶ **Lemma 23.** $r_0 \leqslant \frac{\pi^2 n}{4d^2}$.

Proof. Observe that $T_d(x) = \cos(d\cos^{-1}(x))$ so the first zero of $T_d(x)$ is $\cos\left(-\pi + \frac{\pi}{2d}\right) \leqslant -1 + \frac{\pi^2}{4d^2}$. Thus, the first zero of $T_d\left(\frac{x}{n} - 1\right)$ is at most $\frac{\pi^2 n}{4d^2}$. ◀

▶ **Lemma 24.** *For $d > \frac{\pi}{2}\sqrt{n}$ the polynomial $\tilde{s}_{\alpha,d,m}(x)$ satisfies the following properties:*

1. *For all $x \in [1,n]$, $\tilde{s}_{\alpha,d,m}(x) \leqslant \min\left\{\frac{\alpha d^2}{n}(x-1), \alpha\right\}$.*
2. $\tilde{s}_{\alpha,d,m}(0) \geqslant \alpha\left(\frac{1}{4}\left(1 + \sqrt{\frac{2(1-r_0)}{n}}\right)^d\right)^m$.

Proof. For the first statement, observe that by the Markov Brothers' Theorem, since $|T_d(x)| \leqslant 1$ for all $x \in [-1,1]$, $|T'_d(x)| \leqslant d^2$ for all $x \in [-1,1]$. This implies that $\left|T'_d\left(\frac{x-1+r_0}{n} - 1\right)\right| \leqslant \frac{d^2}{n}$ for all $x \in [1-r_0, 2n+1-r_0]$. Since $T_d\left(\frac{x-1+r_0}{n} - 1\right) = 0$, when $x = 1$, $\left|T_d\left(\frac{x-1+r_0}{n} - 1\right)\right| \leqslant \min\{\frac{d^2(x-1)}{n}, 1\}$ for all $x \in [1,n]$, which implies the result.

For the second statement, by Lemma 7, if $0 \leqslant c \leqslant n$ then $|T_d(-1-\frac{c}{n})| \geqslant \frac{1}{4}\left(1+\sqrt{\frac{2c}{n}}\right)^d$. Applying this lemma with $c = 1 - r_0$, the result follows. ◀

▶ **Corollary 25.** *If the conditions*

1. $d \geqslant 3\sqrt{n}$,
2. $\alpha \leqslant \frac{n}{2d^2} \leqslant \frac{1}{2}$,
3. $m > \frac{\ln(P) - ln(\alpha)}{d\ln\left(1+\sqrt{\frac{2(1-r_0)}{n}}\right) - \ln(4)}$,

are satisfied, then the following properties hold:

1. $\tilde{s}_{\alpha,d,m}(0) > P$.
2. *For all* $x \in [1,2]$, $\tilde{s}_{\alpha,d,m}(x) \leqslant \frac{x-1}{2}$.
3. *For all* $x \in [2,n]$, $\tilde{s}_{\alpha,d,m}(x) \leqslant \frac{1}{2}$.

Thus, $(x-1) - \tilde{s}_{\alpha,d,m}(x)(x-\frac{1}{P}) > 0$ *whenever* $x \in \{0\} \cup (1,n]$.

Proof. The first statement follows from algebraic manipulations provided that $\frac{1}{4}\left(1+\sqrt{\frac{2(1-r_0)}{n}}\right)^d \geqslant 1$. To confirm that this holds, observe that $r_0 \leqslant \frac{\pi^2 n}{4d^2} \leqslant \frac{1}{2}$. Thus,

$$\left(1+\sqrt{\frac{2(1-r_0)}{n}}\right)^d \geqslant \left(1+\frac{1}{\sqrt{n}}\right)^d \geqslant 2^{\frac{d}{\sqrt{n}}} \geqslant 8.$$

For the second and third statements, we use the facts that for all $x \in [1,n]$, $\tilde{s}_{\alpha,d,m}(x) \leqslant \frac{\alpha d^2}{n}(x-1)$ and $\tilde{s}_{\alpha,d,m}(x) \leqslant \alpha$, respectively.

To show that $(x-1) - \tilde{s}_{\alpha,d,m}(x)(x-\frac{1}{P}) > 0$ whenever $x \in \{0\} \cup (1,n]$, we make the following observations:

1. For $x = 0$, $-1 - \tilde{s}_{\alpha,d,m}(0)(-\frac{1}{P}) > -1 - P\left(-\frac{1}{P}\right) = 0$.
2. For $x \in (1,2]$, $(x-1) - \tilde{s}_{\alpha,d,m}(x)(x-\frac{1}{P}) \leqslant (x-1) - \frac{x-1}{2}\left(x-\frac{1}{P}\right) > 0$.
3. For $x \in [2,n]$, $(x-1) - \tilde{s}_{\alpha,d,m}(x)(x-\frac{1}{P}) \leqslant (x-1) - \frac{1}{2}\left(x-\frac{1}{P}\right) > 0$. ◀

We now confirm that

$$\tilde{s}_0 = (x-1) - \tilde{s}_{\alpha,d,m}(x)\left(x-\frac{1}{P}\right)$$

is a sum of squares modulo the Boolean axioms. To see this, observe that since $\tilde{s}_0(x) > 0$ for $x \in \{0\} \cup (1,n]$, $\tilde{s}_0(x)$ must have an even number of roots in $(0,1]$ and no other roots in $[0,n]$. Thus, we can write

$$\tilde{s}_0(x) = p\prod_{i=1}^{l}(x-a_i)(x-b_i)$$

for some polynomial p which is positive on $[0,n]$ and some real roots $a_1,\ldots,a_l,b_1,\ldots,b_l \in (0,1]$. Since p is positive on $[0,n]$, p is a sum of squares modulo the Boolean axioms. By Corollary 9, since $|x|(|x|-1)$ is a sum of squares modulo the Boolean axioms, for each $i \in [l]$, $(x-a_i)(x-b_i)$ is also a sum of squares modulo the Boolean axioms. Thus, $\tilde{s}_0(x)$ is a sum of squares modulo the Boolean axioms.

Finally, we observe that we can satisfy the required conditions on d, α, and m by taking $d = \lceil 3\sqrt{n}\rceil$, $\alpha = \frac{1}{2d^2} \approx \frac{1}{18n}$, and $m = O(\log(P))$, which gives a sum of squares certificate of degree $O(\sqrt{n}\log(P))$.

5 SoS rank upper bound for the SC problem via SQF certification

In this section, we refute the Bienstock–Zuckenberg conjecture for the SC problem. We provide a degree $O(\sqrt{n}\log(n))$ SoS certificate for the SC problem on the Boolean hypercube, thus proving Theorem 3. For this proof, we use the SoS rank for certifying SQFs for $k = 2$ in Theorem 1. We present an alternative direct proof in Section 6.

We begin this section with a discussion on the properties necessary for an SoS polynomial s to even be considered as a possible candidate for an SoS certificate for the SC problem. An SoS certificate for the SC problem is of the form $\sum_{i\in[n]} x_i - 2 = s_0(\mathbf{x}) + \sum_{i\in[n]} s_i(\mathbf{x})g_i(\mathbf{x})$, where $g_i(\mathbf{x}) = \left(\sum_{j\in[n]\setminus\{i\}} x_j - 1\right)$. As opposed to the discussion in Section 4, an SoS certificate for the SC problem not only has multiple constraints but also displays a certain type of asymmetry, which is present in the formulation of the polynomials g_i for $i \in [n]$. One could hope to abuse this asymmetry by constructing different SoS polynomials $s_i \in \Sigma_{n,d}$ for certain $d \in [n]$, but for this proof, we proceed in a similar fashion as for the MK problem and instead construct only one symmetric SoS polynomial $s : \{0,1\}^n \to \mathbb{R}$ and look for the certificate of the form $\sum_{i\in[n]} x_i - 2 = s_0(\mathbf{x}) + \sum_{i\in[n]} s(\mathbf{x})g_i(\mathbf{x})$. Through permutation of indices, the existence of an SoS certificate for the SC problem implies the existence of an SoS certificate such that s is symmetric, that is, there exists an $\tilde{s} : \mathbb{R} \to \mathbb{R}$ such that $s(\mathbf{x}) = \tilde{s}(|\mathbf{x}|)$ for all $\mathbf{x} \in \{0,1\}^n$. As for the MK problem, we are interested in the requirements that polynomial $\tilde{s}$ needs to satisfy such that s constitutes part of an SoS certificate for the SC problem. Let $g(\mathbf{x}) := \sum_{i\in[n]} g_i(\mathbf{x}) = (n-1)(\sum_{i=1}^n x_i) - n$ and note that g is a symmetric polynomial; there exists a univariate polynomial $\tilde{g}$ such that $\tilde{g}(|\mathbf{x}|) = g(\mathbf{x})$ for all $\mathbf{x} \in \{0,1\}^n$. Since s_0 is globally nonnegative, this implies that s needs to satisfy

$$\begin{aligned}|\mathbf{x}| - 2 &\geqslant \tilde{s}(|\mathbf{x}|)\left(|\mathbf{x}|(|\mathbf{x}|-2) + (n-|\mathbf{x}|)(|\mathbf{x}|-1)\right)\\ &= \tilde{s}(|\mathbf{x}|)((n-1)|\mathbf{x}| - n) = \tilde{s}(|\mathbf{x}|)\tilde{g}(|\mathbf{x}|) \qquad \text{for all } \mathbf{x} \in \{0,1\}^n. \end{aligned} \tag{5.1}$$

This implies that $\tilde{s}(0) \geqslant \frac{2}{n}$, $\tilde{s}(1) \geqslant 1$, $\tilde{s}(2) = 0$ and $\tilde{s}(x) \leqslant \frac{x-2}{3(n-1)x-n}$ for all $x \in \{3,4,\ldots,n\}$. We will construct a sum of squares polynomial $\tilde{s}(x)$ which satisfies the following slightly stronger conditions:

1. $\tilde{s}(x) \geqslant 1$ for all $x \in [0,1]$.
2. For all $x \in [1,2)$, $\frac{\tilde{s}(x)}{x-2} < 0$ and $\frac{\tilde{s}(x)}{x-2}$ is increasing.
3. $\tilde{s}(x) \leqslant \frac{(x-2)}{2n}$ for all $x \in [2,3]$.
4. $\tilde{s}(x) \leqslant \frac{1}{2n}$ for all $x \in [3,n]$.

We will then observe that these conditions imply that $\tilde{s}_0(x) = x - 2 - \tilde{s}(x)((n-1)x - n)$ is positive for $x \in [0,1) \cup (2,n]$ and has exactly two zeros in the interval $[1,2]$, one of which is $x = 2$. We can then use Theorem 1 and Corollary 9 to show that $\tilde{s}_0$ is a sum of squares of degree $\deg(\tilde{s}) + O(\sqrt{n}\log(n))$ modulo the Boolean axioms.

▶ **Lemma 26.** *For $d = 3\sqrt{n}$, $\alpha = \frac{1}{18n}$, and $m = 2\lceil\log_2(\sqrt{18n})\rceil$ the polynomial $\tilde{s}(x) = \tilde{s}_{\alpha,d,m}(x-1)$ satisfies the following properties:*

1. *$\tilde{s}(x) \geqslant 1$ for all $x \in [0,1]$.*
2. *For all $x \in [1,2)$, $\frac{\tilde{s}(x)}{x-2} < 0$ and $\frac{\tilde{s}(x)}{x-2}$ is increasing.*
3. *$\tilde{s}(x) \leqslant \frac{(x-2)}{2n}$ for all $x \in [2,3]$.*
4. *$\tilde{s}(x) \leqslant \frac{1}{2n}$ for all $x \in [3,n]$.*

Proof. For the first statement, just as in the proof of Corollary 25, $r_0 \leqslant \frac{\pi^2 n}{4d^2} \leqslant \frac{1}{2}$. Thus,

$$\left(1+\sqrt{\frac{2(1-r_0)}{n}}\right)^d \geqslant \left(1+\frac{1}{\sqrt{n}}\right)^d \geqslant 2^{\frac{d}{\sqrt{n}}} \geqslant 8$$

Hence, by Lemma 24, $\tilde{s}(1) = \tilde{s}_{\alpha,d,m}(0) \geqslant \alpha 2^m \geqslant 1$. Since $deg(\tilde{s})$ is even, all roots of $\tilde{s}$ are real and the smallest root of $\tilde{s}$ is 2, $\tilde{s}$ is positive and decreasing when $x < 2$ so $\tilde{s}(x) \geqslant 1$ whenever $x \in [0,1]$, as needed.

For the second statement, observe that since $\deg(\tilde{s})$ is even, all roots of $\tilde{s}$ are real and the smallest root of $\tilde{s}$ is 2, $\frac{\tilde{s}(x)}{x-2}$ is negative and increasing whenever $x < 2$.

For the third statement, observe that by Lemma 24, for all $x \in [2,3]$, $\tilde{s}(x) = \tilde{s}_{\alpha,d,m}(x-1) \leqslant \alpha\frac{d^2}{n}(x-2) \leqslant \frac{x-2}{2n}$.

For the fourth statement, observe that by Lemma 24, for all $x \in [3,n]$, $\tilde{s}(x) = \tilde{s}_{\alpha,d,m}(x-1) \leqslant \alpha < \frac{1}{2n}$. ◀

▶ **Corollary 27.** *For $d = 3\sqrt{n}$, $\alpha = \frac{1}{n}$, $m = 2\lceil\log_2(n)\rceil$, and $\tilde{s}(x) = \tilde{s}_{\alpha,d,m}(x-1)$ the polynomial $\tilde{s}_0(x) = x-2-\tilde{s}(x)((n-1)x-n)$ is positive for $x \in [0,1) \cup (2,n]$ and has exactly two zeros in the interval $[1,2]$, one of which is $x = 2$.*

Proof. We make the following observations:

1. For all $x \in [0,1)$,
$$\tilde{s}_0(x) = x-2-\tilde{s}(x)((n-1)x-n) \geqslant x-2-((n-1)x-n) = (n-2)(1-x) > 0.$$
2. For all $x \in [1,2]$, $\frac{\tilde{s}_0}{x-2} = 1-((n-1)x-n)\frac{\tilde{s}}{x-2}$. When $x \in [\frac{n}{n-1},2]$, $((n-1)x-n)\frac{\tilde{s}}{x-2} \leqslant 0$ so $\frac{\tilde{s}}{x-2} > 0$. When $x \in [1,\frac{n}{n-1})$, both $((n-1)x-n)$ and $\frac{\tilde{s}}{x-2}$ are negative and increasing so $((n-1)x-n)\frac{\tilde{s}}{x-2}$ is positive and decreasing and thus $\frac{\tilde{s}_0}{x-2}$ is increasing. Since $\frac{\tilde{s}_0(1)}{1-2} \leqslant 0$ and $\frac{\tilde{s}_0(\frac{n}{n-1})}{\frac{n}{n-1}-2} > 0$, $\frac{\tilde{s}_0(x)}{x-2}$ must have exactly one zero in the interval $[1,\frac{n}{n-1}]$.
3. For all $x \in (2,3]$, $\tilde{s}_0(x) = x-2-\tilde{s}(x)((n-1)x-n) \geqslant x-2-\frac{(n-1)x-n}{2n}(x-2) > 0$.
4. For all $x \in [3,n]$, $\tilde{s}_0(x) = x-2-\tilde{s}(x)((n-1)x-n) \geqslant x-2-\frac{(n-1)x-n}{2n} > \frac{x}{2}-\frac{3}{2} \geqslant 0$.

◀

▶ **Corollary 28.** *$\tilde{s}_0(|x|)$ is a sum of squares of degree $O(\sqrt{n}\log(n))$ modulo the Boolean axioms.*

Proof. Since $\tilde{s}_0(x) = x-2-\tilde{s}(x)((n-1)x-n)$ is positive for $x \in [0,1) \cup (2,n]$ and has exactly two zeros in the interval $[1,2]$, one of which is $x = 2$, we can write

$$\tilde{s}_0(x) = \tilde{p}(x-a)(x-2),$$

for some $a \in [1,2)$ where $\tilde{p}(x)$ is positive for has no real roots in the interval $[0,n]$. Since $\tilde{p}(x)$ is positive and has no real roots in the interval $[0,n]$, $\tilde{p}(|x|)$ is a sum of squares modulo the Boolean axioms. By Theorem 1 and Corollary 9, $(x-a)(x-2)$ is a sum of squares of degree $O(\sqrt{n}\log(n))$ modulo the Boolean axioms. ◀

Thus, there exists a degree $O(\sqrt{n}\log(n))$ SoS certificate of nonnegativity for the SC problem.

6 Alternative Proof for the SoS rank upper bound for the SC problem

In this section, we provide an alternative proof of Theorem 3. More precisely, we prove an $O(\sqrt{n}\log(n))$ upper bound on the SoS rank for the SC problem without using Theorem 1.

By the problem formulation, Definition (1.2), and Equation (2.1), the SoS rank for the SC Problem is the smallest d for which there exist SoS polynomials $s_0 \in \Sigma_{n,2d+2}$ and $s_i \in \Sigma_{n,2d}$ for $i \in [n]$ such that

$$\sum_{i=1}^{n} x_i - 2 = s_0(\mathbf{x}) + \sum_{i=1}^{n} s_i \left(\sum_{\substack{j=1 \\ j\neq i}}^{n} x_j - 1 \right).$$

Equivalently, it is the smallest positive integer d such that $\sum_{i=1}^{n} x_i - 2 \in \Sigma_{n,d}^{\mathcal{G}}$.

To prove the SoS rank upper bound for the SC problem, we define the polynomials $h_1(\mathbf{x}) := |\mathbf{x}| - 1$ and $h_2(\mathbf{x}) := |\mathbf{x}| \left(|\mathbf{x}| - 2\right)$ and require the following lemma, in which we use the asymmetry inherent to the constraints of the SC problem.

▶ **Lemma 29.** *For polynomials h_1, h_2 it holds that $h_1(\mathbf{x}) \in \Sigma_{n,0}^{\mathcal{G}}$ and $h_2(\mathbf{x}) \in \Sigma_{n,1}^{\mathcal{G}}$.*

Proof. Consider the first polynomial, h_1, and note that

$$\sum_{i=1}^{n} x_i - 1 = \frac{1}{n-1} \sum_{i=1}^{n} \left(\sum_{\substack{j=1 \\ j\neq i}}^{n} x_j - 1 \right) + \frac{1}{n-1} \in \Sigma_{n,0}^{\mathcal{G}}.$$

Polynomial h_2 can be written as

$$\begin{aligned} \sum_{j=1}^{n} x_j \left(\sum_{i=1}^{n} x_i - 2 \right) &= \sum_{j=1}^{n} \left(x_j \left(\sum_{i=1}^{n} x_i - x_j - 1 \right) + (x_j^2 - x_j) \right) \\ &= \sum_{j=1}^{n} \left(x_j^2 \left(\sum_{\substack{i=1 \\ i\neq j}}^{n} x_i - 1 \right) - (x_j^2 - x_j) \left(\sum_{\substack{i=1 \\ i\neq j}}^{n} x_i - 1 \right) + (x_j^2 - x_j) \right) \in \Sigma_{n,1}^{\mathcal{G}}. \end{aligned}$$ ◀

Although Lemma 29 uses asymmetry in the constraints of the SC problem, both h_1 and h_2 are symmetric polynomials. We can thus define polynomials $\tilde{h}_1,\ \tilde{h}_2 :\ \mathbb{R} \to \mathbb{R}$ such that $\tilde{h}_1(|\mathbf{x}|) = h_1(\mathbf{x})$, and $\tilde{h}_2(|\mathbf{x}|) = h_2(\mathbf{x})$, respectively. We are working towards a proof of the existence of polynomials $p_1, p_2 :\ \mathbb{R} \to \mathbb{R}$ such that

$$(x-2) - p_1(x)\tilde{h}_1(x) - p_2(x)\tilde{h}_2(x) \geqslant 0 \qquad \text{for all } x \in [0, n]. \tag{6.1}$$

6.1 Construction of polynomials $\mathbf{p_1, p_2}$

We consider necessary, but not sufficient requirements that the polynomials p_1 and p_2 have to satisfy, that is, $p_1(2)\tilde{h}_1(2)+p_2(2)\tilde{h}_2(2) = 0$, $\left[p_1\tilde{h}_1 + p_2\tilde{h}_2\right]'(2) = 1$, and $\left[p_1\tilde{h}_1 + p_2\tilde{h}_2\right]''(2) <$ 0. It is easy to check that these requirements are satisfied if p_1 has a double root at $x = 2$, $p_2(2) = 1/2$, and $1 + 4p_2'(2) + 2\frac{p_1(2)}{(x-2)^2} < 0$. We use these guidelines to construct polynomials

$$\begin{aligned} p_1(x) &:= \frac{1}{2n^2c_1}\ (x-2)^2\ T^2_{2\sqrt{n}\log(n)}\left(2\frac{x-2}{n} - 1\right), \\ p_2(x) &:= \frac{1}{2nc_2}\ T^2_{2\sqrt{n}\log(n)}\left(2\frac{x-3}{n} - 1\right), \end{aligned} \tag{6.2}$$

where c_1 and c_2 are constants equal to $\frac{1}{2n^2} T^2_{2\sqrt{n}\log(n)}\left(-\frac{2}{n}-1\right)$ and $\frac{1}{n}\, T^2_{2\sqrt{n}\log(n)}\left(-\frac{2}{n}-1\right)$, respectively, such that $p_1(1) = 1$ and $p_2(2) = 1/2$.

▶ **Lemma 30.** *There exists $C \in \mathbb{N}$ such that for $n \geqslant C$, the polynomial p_1 satisfies the following properties:*

1. $p_1(x) \geqslant 4$ *for* $x \in [0, \frac{1}{2}]$.
2. $p_1(x) \leqslant \left(-0.9(x-1)+1\right)(x-2)^2$ *for* $x \in [1, 2]$.
3. $p_1(x) \leqslant \frac{1}{2n^2}(x-2)^2$ *for* $x \in [2, n]$.

Proof. Since $p_1(x)$ is decreasing for $x \leqslant 1$, to prove Property (1) it is enough to show that $p_1(\frac{1}{2}) \geqslant 4$. By Lemma 7 and for sufficiently big n, it holds

$$p_1(1/2) = \frac{\frac{9}{4}\, T^2_{2\sqrt{n}\log(n)}\left(\frac{-3}{n}-1\right)}{T^2_{2\sqrt{n}\log(n)}\left(-\frac{2}{n}-1\right)} \geqslant \frac{1}{2}\left(\frac{1+\sqrt{\frac{6}{n}}}{1+\sqrt{\frac{5}{n}}}\right)^{4\sqrt{n}\log(n)}.$$

Since $\frac{1}{2}\left(\frac{1+\sqrt{\frac{6}{n}}}{1+\sqrt{\frac{5}{n}}}\right)^{4\sqrt{n}\log(n)} \geqslant 4$ for $n \geqslant 32$ and by monotonicity, Property (1) is satisfied.

To prove Property (3), note that for every $x \in [2, n]$ and $d \in \mathbb{N}$ we have $T_d^2(2\frac{x-2}{n} - 1) \leqslant 1$ and for every $n \geqslant 2$, by Lemma 7, we have $c_1 = \frac{1}{2n^2}\, T^2_{2\sqrt{n}\log(n)}\left(-\frac{2}{n}-1\right) \geqslant \frac{1}{2n^2}\frac{1}{4}\left(1+\sqrt{\frac{4}{n}}\right)^{4\sqrt{n}\log(n)} \geqslant 1$.

To prove Property (2), we show that $\frac{1}{2n^2} T^2_{2\sqrt{n}\log(n)}\left(2\frac{x-2}{n}-1\right) \leqslant \left(-0.9(x-1)+1\right)$ for every $x \in [1, 2]$. By construction, it is satisfied for $x = 1$ and by Property (3), it is satisfied for $x = 2$. Since the function $T^2_{2\sqrt{n}\log(n)}\left(2\frac{x-2}{n}-1\right)$ is convex in the interval $[1, 2]$, the property is satisfied for $x \in [1, 2]$. ◀

▶ **Lemma 31.** *There exists a constant $C \in \mathbb{N}$ such that for $n \geqslant C$, the polynomial p_2 satisfies the following properties:*

1. $p_2(x) \geqslant 4$ *for* $x \in [0, 1]$.
2. $p_2(2) = \frac{1}{2}$.
3. $p_2'(x) \leqslant -1$ *for* $x \in [1, 2]$.
4. $p_2(x) \leqslant -0.45(x-2) + \frac{1}{2}$ *for* $x \in [2, 3]$.
5. $p_2(x) \leqslant \frac{1}{2n}$ *for* $x \in [3, n]$.

Proof. Since $p_2(x)$ is decreasing for $x \leqslant 1$, to prove Property (1), it is enough to show that $p_2(1) \geqslant 4$. For sufficiently big n we get:

$$p_2(1) := \frac{\frac{1}{2}\, T^2_{2\sqrt{n}\log(n)}\left(-\frac{4}{n}-1\right)}{T^2_{2\sqrt{n}\log(n)}\left(-\frac{2}{n}-1\right)} \geqslant \frac{1}{8}\left(\frac{-1-\sqrt{\frac{8}{n}}}{-1-\sqrt{\frac{5}{n}}}\right)^{4\sqrt{n}\log(n)}.$$

Since $\frac{1}{8}\left(\frac{-1-\sqrt{\frac{8}{n}}}{-1-\sqrt{\frac{5}{n}}}\right)^{4\sqrt{n}\log(n)} \geqslant 4$ for $n \geqslant 13$ and by monotonicity, Property (1) is satisfied.

Property (2) is satisfied by construction.

Since for every $x \in [3, n]$ and $d \in \mathbb{N}$ we have $\left|T_d(2\frac{x-3}{n} - 1)\right| \leqslant 1$ and for every $n \geqslant 2$, by Lemma 7, we have $c_2 = \frac{1}{n}\, T^2_{2\sqrt{n}\log(n)}\left(-\frac{2}{n}-1\right) \geqslant \frac{1}{n}\frac{1}{4}\left(-1-\sqrt{\frac{4}{n}}\right)^{4\sqrt{n}\log(n)} \geqslant 1$, Property (5) is satisfied.

Since $p_2(x)$ is convex for $x \in [1,2]$, to prove Property (3), it is enough to show $p_2'(2) \leqslant -1$. Note that $\frac{\partial T_d(x)}{\partial x} = dU_{d-1}(x)$ and $\frac{\partial T_d^2(x)}{\partial x} = 2dT_d(x)U_{d-1}(x)$, where $U_d(x)$ is a Chebyshev polynomial of the second type. Thus,

$$p_2'(x) = \frac{4\log(n) T_{2\sqrt{n}\log(n)}\left(\frac{2(x-3)}{n} - 1\right) U_{2\sqrt{n}\log(n)-1}\left(\frac{2(x-3)}{n} - 1\right)}{\sqrt{n} T_{2\sqrt{n}\log(n)}\left(-1 - \frac{2}{n}\right)},$$

which implies that

$$p_2'(2) = \frac{4\log(n) U_{2\sqrt{n}\log(n)-1}\left(-1 - \frac{2}{n}\right)}{\sqrt{n} T_{2\sqrt{n}\log(n)}\left(-1 - \frac{2}{n}\right)} = \left[\frac{\partial}{\partial x} \frac{T_{2\sqrt{n}\log(n)}\left(2\frac{x-3}{n} - 1\right)}{T_{2\sqrt{n}\log(n)}\left(-1 - \frac{2}{n}\right)}\right](2).$$

Since $T_{2\sqrt{n}\log(n)}\left(2\frac{x-3}{n} - 1\right)$ for $x = 2.5$ takes at most half of the value for $x = 2$ and since $T_{2\sqrt{n}\log(n)}\left(2\frac{x-3}{n} - 1\right)$ is convex in the interval $[2,3]$, $p_2'(x) \leqslant -1$. By Lemma 7,

$$\frac{T^2_{2\sqrt{n}\log(n)}\left(-\frac{2}{n} - 1\right)}{T^2_{2\sqrt{n}\log(n)}\left(-\frac{1}{n} - 1\right)} \geqslant \frac{1}{4}\left(\frac{-1 - \sqrt{\frac{4}{n}}}{-1 - \sqrt{\frac{3}{n}}}\right)^{2\sqrt{n}\log(n)}.$$

Since $\frac{1}{4}\left(\frac{-1-\sqrt{\frac{4}{n}}}{-1-\sqrt{\frac{3}{n}}}\right)^{2\sqrt{n}\log(n)} \geqslant 2$ for $n \geqslant 100$ and by monotonicity, Property (3) is satisfied.

By Property (2), Property (4) holds for $x = 2$. By Property (5), it holds for $x = 3$ and $n \geqslant 10$. Since $p_2(x)$ is convex for $x \in [2,3]$, the property holds for $x \in [2,3]$. ◀

Now we are ready to prove the main lemma of this section.

▶ **Lemma 32.** *It holds that*

$$f(x) := x - 2 - p_1(x)h_1(x) - p_2(x)h_2(x) \geqslant 0 \qquad \textit{for } x \in [0,n]. \tag{6.3}$$

Proof. Note that $h_1(x),\ h_2(x) \leqslant 0$ for $x \in [0,1]$. For all $x \in [0,\frac{1}{2}]$, $p_1(x)$ is decreasing and $h_1(x)$ is increasing in x. Thus, by Property (1), for $x \in [0,\frac{1}{2}]$, $f(x) \geqslant x - 2 - p_1(x)h_1(x) \geqslant -2 - p_1(1/2)h_1(1/2) \geqslant -2 + 4 \cdot \frac{1}{2} \geqslant 0$. For $x \in [\frac{1}{2},1]$, both $p_2(x)$ and $h_2(x)$ are decreasing. Thus, for $x \in [\frac{1}{2},1]$ and by Property (1), $f(x) \geqslant x - 2 - p_2(x)h_2(x) \geqslant -\frac{3}{2} - p_2(1)h_2(1/2) \geqslant -\frac{3}{2} + 4 \cdot \frac{3}{4} \geqslant 0$. To prove the statement for $x \in [1,2]$, we show that for every $a \in [0,1]$, we have $f(2-a) \geqslant 0$. By construction, we have $f(2) = 0$. Thus, the property holds for $a = 0$. By Property (2), for polynomial p_1, we have $p_1(2-a) \leqslant (0.9a + 0.1)a^2$. By Properties (2) and (3), for polynomial p_2, we have $p_2(2-a) \geqslant 1/2 + a$. Thus, $f(2-a) \geqslant -a - (0.9a + 0.1)a^2(1-a) + (1/2 + a)a(2-a) = a^2((0.9a - 1.8)a + 1.4)$, which is nonnegative for $a \in [0,1]$. This proves the statement for $x \in [1,2]$.

To prove the statement for $x \in [2,3]$ we show that for every $a \in [0,1]$, it holds that $f(2+a) \geqslant 0$. By Property (3), for $x \in [2,3]$ and $n \geqslant 2$, we get $p_1(2+a) \leqslant \frac{1}{4}a^2$. By Property (4), we get that $p_2(2+a) \leqslant -0.45a + \frac{1}{2}$. Thus, $f(2+a) \geqslant a - \frac{1}{4}a^2(1+a) - \left(-0.45a + \frac{1}{2}\right)(2+a)a = (0.15 + 0.2a)a^2$, which is non-negative for $a \in [0,1]$. This proves the statement for $x \in [2,3]$. Finally, for $x \in [3,n]$, we have $f(x) \geqslant x - 2 - \frac{1}{2n^2}(x-2)^2(x-1) - \frac{1}{2n}x(x-2) \geqslant 0$. ◀

6.2 Proof of Theorem 3

By Lemma 32, $x - 2 - p_1(x)h_1(x) - p_2(x)h_2(x) \geqslant 0$ for $x \in [0,n]$ and the degree of the polynomial on the LHS is at most $O(\sqrt{n}\log(n))$. Thus, by Theorem 6, there exist SoS polynomials s_0, s_1 such that $x - 2 - p_1(x)h_1(x) - p_2(x)h_2(x) = s_0(x) + x(n-x)s_1(x)$. Thus, $x - 2 = s_0(x) + x(n-x)s_1(x) + p_1(x)h_1(x) + p_2(x)h_2(x)$. Remark 5 and the fact that $|\mathbf{x}|(n - |\mathbf{x}|)$ has a degree 1 SoS certificate over the Boolean hypercube imply the existence of a degree $O(\sqrt{n}\log(n))$ certificate over the Boolean hypercube for the polynomial $\sum_{i=1}^{n} x_i - 2$.

References

1 S. Arora, S. Rao, and U. V. Vazirani. Expander flows, geometric embeddings and graph partitioning. *J. ACM*, 56(2):5:1–5:37, 2009.

2 B. Barak, S. B. Hopkins, J. A. Kelner, P. Kothari, A. Moitra, and A. 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.

3 B. Barak, J. A. Kelner, and D. Steurer. Dictionary learning and tensor decomposition via the sum-of-squares method. In *STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 143–151, 2015.

4 B. Barak and A. Moitra. Noisy tensor completion via the sum-of-squares hierarchy. In *COLT 2016, New York, USA, June 23-26, 2016*, pages 417–445, 2016.

5 B. Barak, P. Raghavendra, and D. Steurer. Rounding semidefinite programming hierarchies via global correlation. In *FOCS*, pages 472–481, 2011.

6 B. Barak and D. Steurer. Proofs, beliefs, and algorithms through the lens of sum-of-squares, 2016. URL: `https://www.sumofsquares.org`.

7 Aditya Bhaskara, Moses Charikar, Aravindan Vijayaraghavan, Venkatesan Guruswami, and Yuan Zhou. Polynomial integrality gaps for strong sdp relaxations of densest k-subgraph. In *SODA*, 2012.

8 D. Bienstock and M. Zuckerberg. Subset algebra lift operators for 0-1 integer programming (extended version), 2002. Extended version of: Subset algebra lift operators for 0-1 integer programming - SIAM Journal on Optimization, 1(15): 63-95, 2004. URL: `http://www.corc.ieor.columbia.edu/reports/techreports.html`.

9 Grigoriy Blekherman, Pablo A Parrilo, and Rekha R Thomas. *Semidefinite optimization and convex algebraic geometry.* SIAM, 2012.

10 K. K. H. Cheung. Computation of the Lasserre ranks of some polytopes. *Math. Oper. Res.*, 32(1):88–94, 2007.

11 W. Cook and S. Dash. On the matrix-cut rank of polyhedra. *Math. Oper. Res.*, 26(1):19–30, 2001.

12 Hamza Fawzi, James Saunderson, and Pablo A. Parrilo. Sparse sum-of-squares certificates on finite abelian groups. In *54th IEEE Conference on Decision and Control, CDC 2015, Osaka, Japan, December 15-18, 2015*, pages 5909–5914, 2015. `doi:10.1109/CDC.2015.7403148`.

13 Mrinalkanti Ghosh, Fernando Granha Jeronimo, Chris Jones, Aaron Potechin, and Goutham Rajendran. Sum-of-squares lower bounds for sherrington-kirkpatrick via planted affine planes. In *61st IEEE Annual Symposium on Foundations of Computer Science, FOCS*, pages 954–965, 2020.

14 M. X. Goemans and D. P. Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *J. Assoc. Comput. Mach.*, 42(6):1115–1145, 1995.

15 D. Grigoriev. Complexity of positivstellensatz proofs for the knapsack. *Comput. Complexity*, 10(2):139–154, 2001.

16 D. Grigoriev, E. A. Hirsch, and D. V. Pasechnik. Complexity of semi-algebraic proofs. In *STACS*, pages 419–430, 2002.

17 D. Grigoriev and N. Vorobjov. Complexity of null-and positivstellensatz proofs. *Ann. Pure App. Logic*, 113(1-3):153–160, 2001.

18 Dima Grigoriev. Linear lower bound on degrees of positivstellensatz calculus proofs for the parity. *Theoretical Computer Science*, 259(1-2):613–622, 2001.

19 V. Guruswami and A. K. Sinop. Lasserre hierarchy, higher eigenvalues, and approximation schemes for graph partitioning and quadratic integer programming with psd objectives. In *FOCS*, pages 482–491, 2011.

20 S. B. Hopkins, T. Schramm, J. Shi, and D. Steurer. Fast spectral algorithms from sum-of-squares proofs: tensor decomposition and planted sparse vectors. In *STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 178–191, 2016.

21 P. Kothari, J. Steinhardt, and D. Steurer. Robust moment estimation and improved clustering via sum of squares. In *STOC 2018*, 2018.

22 P. K. Kothari, R. Mori, R. O'Donnell, and D. 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, Montreal, QC, Canada, June 19-23, 2017*, pages 132–145, 2017.

23 Dmitriy Kunisky and Afonso S. Bandeira. A tight degree 4 sum-of-squares lower bound for the sherrington-kirkpatrick hamiltonian. *CoRR*, abs/1907.11686, 2019. `arXiv:1907.11686`.

24 A. Kurpisz, S. Leppänen, and M. Mastrolilli. Sum-of-squares hierarchy lower bounds for symmetric formulations. In *Integer Programming and Combinatorial Optimization - 18th International Conference, IPCO 2016, Liège, Belgium, June 1-3, 2016, Proceedings*, pages 362–374, 2016.

25 A. Kurpisz, S. Leppänen, and M. Mastrolilli. Tight sum-of-squares lower bounds for binary polynomial optimization problems. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, pages 78:1–78:14, 2016.

26 A. Kurpisz, S. Leppänen, and M. Mastrolilli. On the hardest problem formulations for the 0/1 lasserre hierarchy. *Math. Oper. Res.*, 42(1):135–143, 2017.

27 A. Kurpisz, S. Leppänen, and M. Mastrolilli. An unbounded sum-of-squares hierarchy integrality gap for a polynomially solvable problem. *Math. Program.*, 166(1-2):1–17, 2017.

28 Adam Kurpisz. Sum-of-squares bounds via boolean function analysis. In *ICALP July 9-12, 2019, Patras, Greece*, 2019.

29 J. B. Lasserre. An explicit exact SDP relaxation for nonlinear 0-1 programs. In *Integer Programming and Combinatorial Optimization, 8th International IPCO Conference, Utrecht, The Netherlands, June 13-15, 2001, Proceedings*, pages 293–303, 2001.

30 M. Laurent. A comparison of the Sherali-Adams, Lovász-Schrijver, and Lasserre relaxations for 0-1 programming. *Math. Oper. Res.*, 28(3):470–496, 2003.

31 M. Laurent. Lower bound for the number of iterations in semidefinite hierarchies for the cut polytope. *Math. Oper. Res.*, 28(4):871–883, 2003.

32 J. R. Lee, P. Raghavendra, and D. Steurer. Lower bounds on the size of semidefinite programming relaxations. In *STOC*, pages 567–576, 2015.

33 T. Lee, A. Prakash, R. Wolf, and H. Yuen. On the sum-of-squares degree of symmetric quadratic functions. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 17:1–17:31, 2016.

34 László Lovász. On the shannon capacity of a graph. *IEEE Transactions on Information Theory*, 25:1–7, 1979.

35 Raghu Meka, Aaron Potechin, and Avi Wigderson. Sum-of-squares lower bounds for planted clique. In *Proceedings of the 47th Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA*, pages 87–96, 2015.

36 M. J. Moore. An n job, one machine sequencing algorithm for minimizing the number of late jobs. *Management Science*, 15:102–109, 1968.

37 Katta G. Murty and Santosh N. Kabadi. Some np-complete problems in quadratic and nonlinear programming. *Mathematical Programming*, 39(2):117–129, 1987. `doi:10.1007/BF02592948`.

38 Y. Nesterov. *Global quadratic optimization via conic relaxation*, pages 363–384. Kluwer Academic Publishers, 2000.

39 P. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization.* PhD thesis, California Institute of Technology, 2000.

40 R. Paturi. On the degree of polynomials that approximate symmetric boolean functions (preliminary version). In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing, May 4-6, 1992, Victoria, British Columbia, Canada*, pages 468–474, 1992.

41 A. Potechin and D. Steurer. Exact tensor completion with sum-of-squares. In *COLT 2017, Amsterdam, The Netherlands, 7-10 July 2017*, pages 1619–1673, 2017.

42 Aaron Potechin. Sum of squares bounds for the ordering principle. In *Proceedings of the 35th Computational Complexity Conference*, pages 1–37, 2020.

43 T. Rivlin. The chebyshev polynomials. *SERBIULA (sistema Librum 2.0)*, February 1974.

44 S. Sakaue, A. Takeda, S. Kim, and N. Ito. Exact semidefinite programming relaxations with truncated moment matrix for binary polynomial optimization problems. *SIAM Journal on Optimization*, 27(1):565–582, 2017.

45 T. Schramm and D. Steurer. Fast and robust tensor decomposition with applications to dictionary learning. In *COLT 2017, Amsterdam, The Netherlands, 7-10 July 2017*, pages 1760–1793, 2017.

46 N. Shor. Class of global minimum bounds of polynomial functions. *Cybernetics*, 23(6):731–734, 1987.

47 Lucas Slot and Monique Laurent. Improved convergence analysis of lasserre's measure-based upper bounds for polynomial minimization on compact sets. *CoRR*, 2019. `doi:10.1007/s10107-020-01468-3`.

48 J. Thapper and S. Zivny. The power of sherali-adams relaxations for general-valued csps. *SIAM J. Comput.*, 46(4):1241–1279, 2017.

49 Madhur Tulsiani. Csp gaps and reductions in the lasserre hierarchy. In *STOC*, pages 303–312, 2009.

50 R. Wolf. A note on quantum algorithms and the minimal degree of ϵ-error polynomials for symmetric functions. *Quantum Information & Computation*, 8(10):943–950, 2010.