Optimization over the Boolean Hypercube via Sums of Nonnegative Circuit Polynomials

Mareike Dressler
Goethe-Universität, FB 12 – Institut für Mathematik,
Robert-Mayer-Str. 6-10, 60054 Frankfurt am Main, Germany
dressler@math.uni-frankfurt.de

Adam Kurpisz[1]
ETH Zürich, Department of Mathematics,
Rämistrasse 101, 8092 Zürich, Switzerland
adam.kurpisz@ifor.math.ethz.ch

Timo de Wolff[2]
Technische Universität Berlin, Institut für Mathematik,
Straße des 17. Juni 136, 10623 Berlin, Germany
dewolff@math.tu-berlin.de

Abstract

Various key problems from theoretical computer science can be expressed as polynomial optimization problems over the boolean hypercube. One particularly successful way to prove complexity bounds for these types of problems are based on sums of squares (SOS) as nonnegativity certificates. In this article, we initiate optimization over the boolean hypercube via a recent, alternative certificate called sums of nonnegative circuit polynomials (SONC). We show that key results for SOS based certificates remain valid: First, there exists a SONC certificate of degree at most $n + d$ for polynomials which are nonnegative over the n-variate boolean hypercube with constraints of degree d. Second, if there exists a degree d SONC certificate for nonnegativity of a polynomial over the boolean hypercube, then there also exists a short degree d SONC certificate, that includes at most $n^{O(d)}$ nonnegative circuit polynomials. Finally, we show certain differences between SOS and SONC cones: we prove that, in contrast to SOS, the SONC cone is not closed under taking affine transformation of variables and that for SONC there does not exist an equivalent to Putinar's Positivestellensatz. We discuss these results both from algebraic and optimization perspective.

2012 ACM Subject Classification Mathematics of computing → Convex optimization

Keywords and phrases nonnegativity certificate, hypercube optimization, sums of nonnegative circuit polynomials, relative entropy programming, sums of squares

Digital Object Identifier 10.4230/LIPIcs.MFCS.2018.82

1 Introduction

An *optimization problem over a boolean hypercube* is an n-variate (constrained) polynomial optimization problem where the feasibility set is restricted to some vertices of an n-dimensional hypercube. This class of optimization problems belongs to the core of theoretical computer

[1] Swiss National Science Foundation project PZ00P2_174117 "Theory and Applications of Linear and Semidefinite Relaxations for Combinatorial Optimization Problems"
[2] DFG grant WO 2206/1-1

© Mareike Dressler, Adam Kurpisz, and Timo de Wolff;
licensed under Creative Commons License CC-BY

science. However, it is known that solving them is NP-hard in general, since one can easily cast, e.g., the Independent Set problem in this framework.

One of the most promising approaches in constructing theoretically efficient algorithms is the *sum of squares (SOS) hierarchy* [23, 45, 48, 55], also known as *Lasserre relaxation* [34]. The method is based on a Positivstellensatz result [50] saying that the polynomial f, which is nonnegative over the feasibility set, can be expressed as a sum of squares times the constraints defining the set. Bounding a maximum degree of a polynomial used in a representation of f provides a family of algorithms parametrized by an integer d. Finding a degree d SOS certificate for nonnegativity of f can be performed by solving a *semidefinite programming* (SDP) formulation of size $n^{O(d)}$. Finally, for every (feasible) n-variate hypercube optimization problem, with constraints of degree at most d, there exists a degree $2(n + \lceil d/2 \rceil)$ SOS certificate.

The SOS algorithm is a frontier method in algorithm design. It provides the best available algorithms used for a wide variety of optimization problems. The degree 2 SOS for the Independent Set problem implies the Lovász θ-function [40] and gives the Goemans-Williamson relaxation [20] for the Max Cut problem. The Goemans-Linial relaxation for the Sparsest Cut problem (analyzed in [2]) can be captured by the SOS of degree 6. Finally, the subexponential time algorithm for Unique Games [1] is implied by a SOS of sublinear degree [4, 24]. Moreover, it has been shown that SOS is equivalent in power to any SDP extended formulation of comparable size in approximating maximum constraint satisfaction problems (CSP) [39]. Recently SOS has been also applied to problems in dictionary learning [6, 54], tensor completion and decomposition [7, 26, 49], and robust estimation [28]. Other applications of the SOS method can be found in [4, 8, 12, 13, 16, 17, 24, 41, 42, 51], see also the surveys [14, 35, 37].

On the other hand it is known that the SOS algorithm admits certain weaknesses. For example, Grigoriev shows in [21] that a $\Omega(n)$ degree SOS certificate is needed to detect a simple integrality argument for the Knapsack problem, see also [22, 31, 36]. Other SOS degree lower bounds for Knapsack problems appeared in [11, 32]. Some lower bounds on the effectiveness of SOS has been shown for CSP problems [29, 56] and for planted clique problem [3, 43]. Finally degree $\Omega(\sqrt{n})$ SOS was proved to have problems scheduling unit size jobs on a single machine to minimize the number of late jobs [33]. The problem is solvable in polynomial time using the Moore-Hodgson algorithm. Finally, SOS has hard time proving global nonnegativity, as first proved by Hilbert [25]. Later an explicit example was given by Motzkin [44]. Moreover, as shown by Blekherman [9], there are significantly more nonnegative polynomials than SOS polynomials. The above arguments motivate the search of new nonnegativity certificates for solving optimization problems efficiently.

In this article, we initiate an analysis of hypercube optimization problems via *sums of nonnegative circuit polynomials (SONC)*. SONCs are a nonnegativity certificate introduced in [27], which are independent of sums of squares; see Definition 1 and Theorem 5 for further details. This means particularly that certain polynomials like the Motzkin polynomial, which have no SOS certificate for global nonnegativity, can be certified as nonnegative via SONCs. Moreover, SONCs generalize polynomials which are certified to be nonnegative via the arithmetic-geometric mean inequality [52]. Similarly as Lasserre relaxation for SOS, a Schmüdgen-like Positivstellensatz yields a converging hierarchy of lower bounds for polynomial optimization problems with compact constraint set; see [19, Theorem 4.8] and Theorem 6. These bounds can be computed via a convex optimization program called *relative entropy programming* [19, Theorem 5.3]. Our main question in this article is:

Can SONC certificates be an alternative for SOS methods for optimization problems over the hypercube?

We answer this question affirmatively in the sense that we prove SONC complexity bounds for boolean hypercube optimization analogous to the SOS bounds mentioned above. More specifically, we show:

1. For every polynomial which is nonnegative over an n-variate hypercube with constraints of degree at most d there exists a SONC certificate of nonnegativity of degree at most $n + d$; see Theorem 16 and Corollary 17.
2. If a polynomial f admits a degree d SONC certificate of nonnegativity over an n-variate hypercube, then the polynomial f admits also a *short* degree d SONC certificate that includes at most $n^{O(d)}$ nonnegative circuit polynomials; see Theorem 18.

Furthermore, we show some structural properties of SONCs:

1. We give a simple, constructive example showing that the SONC cone is not closed under multiplication. Subsequently we use this construction to show that the SONC cone is neither closed under taking affine transformations of variables, see Lemma 8 and Corollary 9 and the discussion afterwards.
2. We address an open problem raised in [19] asking whether the Schmüdgen-like Positivstellensatz for SONCs (Theorem 6) can be improved to an equivalent of Putinar's Positivstellensatz [50]. We answer this question negatively by showing an explicit hypercube optimization example, which provably does not admit a Putinar representation for SONCs; see Theorem 19 and the discussion afterwards.

Our article is organized as follows: In Section 2 we introduce the necessary background from theoretical computer sciences and about SONCs. In Section 3 we show that the SONC cone is closed neither under multiplication nor under affine transformations. In Section 4 we provide our two main results regarding the degree bounds for SONC certificates over the hypercube. In Section 5 we prove the non-existence of an equivalent of Putinar's Positivstellensatz for SONCs and discuss this result.

2 Preliminaries

In this section we collect basic notions and statements on sums of nonnegative circuit polynomials (SONC).

Throughout the paper, we use bold letters for vectors, e.g., $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$. Let $\mathbb{N}^* = \mathbb{N} \setminus \{\mathbf{0}\}$ and $\mathbb{R}_{\geq 0}$ ($\mathbb{R}_{>0}$) be the set of nonnegative (positive) real numbers. Furthermore let $\mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1, \dots, x_n]$ be the ring of real n-variate polynomials and the set of all n-variate polynomials of degree less than or equal to $2d$ is denoted by $\mathbb{R}[\mathbf{x}]_{n,2d}$. We denote by $[n]$ the set $\{1, \dots, n\}$ and the sum of binomial coefficients $\sum_{k=0}^{d} \binom{n}{k}$ is abbreviated by $\binom{n}{\leq d}$. Let $\mathbf{e_1}, \dots, \mathbf{e_n}$ denote the canonical basis vectors in $\mathbb{R}^n$.

2.1 Sums of Nonnegative Circuit Polynomials

Let $A \subset \mathbb{N}^n$ be a finite set. In what follows, we consider polynomials $f \in \mathbb{R}[\mathbf{x}]$ supported on A. Thus, f is of the form $f(\mathbf{x}) = \sum_{\boldsymbol{\alpha} \in A} f_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$ with $f_{\boldsymbol{\alpha}} \in \mathbb{R}$ and $\mathbf{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. A lattice point is called *even* if it is in $(2\mathbb{N})^n$ and a term $f_{\boldsymbol{\alpha}} \mathbf{x}^{\boldsymbol{\alpha}}$ is called a *monomial square* if $f_{\boldsymbol{\alpha}} > 0$ and α even. We denote by $\mathrm{New}(f) = \mathrm{conv}\{\boldsymbol{\alpha} \in \mathbb{N}^n : f_{\boldsymbol{\alpha}} \neq 0\}$ the Newton polytope of f.

Initially, we introduce the foundation of SONC polynomials, namely *circuit polynomials*; see also [27]:

▶ **Definition 1.** A polynomial $f \in \mathbb{R}[\mathbf{x}]$ is called a *circuit polynomial* if it is of the form

$$f(\mathbf{x}) \;:=\; f_{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\beta}} + \sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)}\mathbf{x}^{\boldsymbol{\alpha}(j)}, \tag{2.1}$$

with $r \leq n$, exponents $\boldsymbol{\alpha}(j)$, $\boldsymbol{\beta} \in A$, and coefficients $f_{\boldsymbol{\alpha}(j)} \in \mathbb{R}_{>0}$, $f_{\boldsymbol{\beta}} \in \mathbb{R}$, such that the following conditions hold:

(C1) $\mathrm{New}(f)$ is a simplex with all even vertices $\boldsymbol{\alpha}(0), \boldsymbol{\alpha}(1), \ldots, \boldsymbol{\alpha}(r) \in \mathbb{Z}^n$.

(C2) The exponent $\boldsymbol{\beta}$ is in the strict interior of $\mathrm{New}(f)$. Hence, there exist unique *barycentric coordinates* λ_j relative to the vertices $\boldsymbol{\alpha}(j)$ with $j = 0, \ldots, r$ satisfying

$$\boldsymbol{\beta} \;=\; \sum_{j=0}^{r} \lambda_j \boldsymbol{\alpha}(j) \;\text{ with }\; \lambda_j \;>\; 0 \;\text{ and }\; \sum_{j=0}^{r} \lambda_j \;=\; 1.$$

We call the terms $f_{\boldsymbol{\alpha}(0)}\mathbf{x}^{\boldsymbol{\alpha}(0)}, \ldots, f_{\boldsymbol{\alpha}(r)}\mathbf{x}^{\boldsymbol{\alpha}(r)}$ the *outer terms* and $f_{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\beta}}$ the *inner term* of f.

For every circuit polynomial we define the corresponding *circuit number* as

$$\Theta_f \;:=\; \prod_{j=0}^{r} \left(\frac{f_{\boldsymbol{\alpha}(j)}}{\lambda_j}\right)^{\lambda_j}. \tag{2.2}$$

Note that the name of these polynomials is motivated by the fact that their support set forms a *circuit*, i.e. a minimal affine dependent set, see e.g. [47]. The first fundamental statement about circuit polynomials is that its nonnegativity is determined by its circuit number Θ_f and f_β entirely:

▶ **Theorem 2** ([27], Theorem 3.8)**.** *Let f be a circuit polynomial with inner term $f_{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\beta}}$ and let Θ_f be the corresponding circuit number, as defined in* (2.2)*. Then the following statements are equivalent:*

1. *f is nonnegative.*
2. *$|f_{\boldsymbol{\beta}}| \leq \Theta_f$ and $\boldsymbol{\beta} \notin (2\mathbb{N})^n$ or $f_{\boldsymbol{\beta}} \geq -\Theta_f$ and $\boldsymbol{\beta} \in (2\mathbb{N})^n$.*

We illustrate the previous definition and theorem by an example:

▶ **Example 3.** The *Motzkin polynomial* [44] is given by

$$M(x_1, x_2) \;:=\; x_1^4x_2^2 + x_1^2x_2^4 - 3x_1^2x_2^2 + 1.$$

It is a circuit polynomial since $\mathrm{New}(f) = \{(4,2), (2,4), (0,0)\}$, and $\boldsymbol{\beta} = (2,2)$ with $\lambda_0, \lambda_1, \lambda_2 = 1/3$. We have $|f_{\boldsymbol{\beta}}| = 3$ and compute $\Theta_f \;=\; \sqrt[3]{\left(\frac{1}{1/3}\right)^3} \;=\; 3$. Hence, we can conclude that $M(x_1, x_2)$ is nonnegative by Theorem 2.

▶ **Definition 4.** We define for every $n, d \in \mathbb{N}^*$ the set of *sums of nonnegative circuit polynomials* (SONC) in n variables of degree $2d$ as

$$C_{n,2d} \;:=\; \left\{ f \in \mathbb{R}[\mathbf{x}]_{n,2d} \;:\; f = \sum_{i=1}^{k} p_i,\; p_i \text{ is a nonnegative circuit polynomial},\; k \in \mathbb{N}^* \right\}$$

Note that the degree is attained at the outer terms and hence it is even.

We denote by SONC both the set of SONC polynomials and the property of a polynomial to be a sum of nonnegative circuit polynomials.

In what follows let $P_{n,2d}$ be the cone of nonnegative n-variate polynomials of degree at most $2d$ and $\Sigma_{n,2d}$ be the corresponding cone of sums of squares respectively. An important observation is, that SONC polynomials form a convex cone independent of the SOS cone:

▶ **Theorem 5** ([27], Proposition 7.2). *$C_{n,2d}$ is a convex cone satisfying:*

1. *$C_{n,2d} \subseteq P_{n,2d}$ for all $n, d \in \mathbb{N}^*$,*
2. *$C_{n,2d} \subseteq \Sigma_{n,2d}$ if and only if $(n, 2d) \in \{(1, 2d), (n, 2), (2, 4)\}$,*
3. *$\Sigma_{n,2d} \not\subseteq C_{n,2d}$ for all $(n, 2d)$ with $2d \geq 6$.*

For further details about the SONC cone see [18, 19, 27].

2.2 SONC certificates over a Constrained Set

In [19, Theorem 4.8], Iliman, the first, and the third author showed that for an arbitrary real polynomial which is strictly positive on a compact, basic closed semialgebraic set K there exists a SONC certificate of nonnegativity. Hereinafter we recall this result.

We assume that K is given by polynomial inequalities $g_i(\mathbf{x}) \geq 0$ for $i = 1, \ldots, s$ and is compact. For technical reason we add $2n$ redundant box constraints $l_j(\mathbf{x}) := N \pm x_j \geq 0$ for some sufficiently large $N \in \mathbb{N}$, which always exists due to our assumption of compactness of K; see [19] for further details. Hence, we have

$$K \;:=\; \{\mathbf{x} \in \mathbb{R}^n : g_i(\mathbf{x}) \geq 0 \text{ for } i \in [s] \text{ and } l_j(\mathbf{x}) \geq 0 \text{ for } j \in [2n]\}. \tag{2.3}$$

In what follows we consider polynomials $H^{(q)}(\mathbf{x})$ defined as products of at most $q \in \mathbb{N}^*$ of the polynomials g_i, l_j and 1, i.e.,

$$H^{(q)}(\mathbf{x}) \;:=\; \prod_{k=1}^{q} h_k(\mathbf{x}), \tag{2.4}$$

where $h_k \in \{1, g_1, \ldots, g_s, l_1, \ldots, l_{2n}\}$. Now we can state:

▶ **Theorem 6** ([19], Theorem 4.8). *Let $f, g_1, \ldots, g_s \in \mathbb{R}[\mathbf{x}]$ be real polynomials and K be a compact, basic closed semialgebraic set as in (2.3). If $f > 0$ on K then there exist $d, q \in \mathbb{N}^*$ such that we have an explicit representation of f of the form:*

$$f(\mathbf{x}) \;=\; \sum_{\text{finite}} s(\mathbf{x}) H^{(q)}(\mathbf{x}),$$

where the $s(\mathbf{x})$ are contained in $C_{n,2d}$ and every $H^{(q)}(\mathbf{x})$ is a product as in (2.4).

The central object of interest is the smallest value of d and q that allows f a decomposition as in Theorem 6. This motivates the following definition of a *degree d SONC certificate*.

▶ **Definition 7.** Let $f \in \mathbb{R}[\mathbf{x}]$ such that f is positive on the set K given in (2.3). Then f has a *degree d SONC certificate* if it admits for some $q \in \mathbb{N}^*$ the following decomposition:

$$f(\mathbf{x}) \;=\; \sum_{\text{finite}} s(\mathbf{x}) H^{(q)}(\mathbf{x}),$$

for $s(\mathbf{x})$ SONCs, the $H^{(q)}(\mathbf{x})$ products as in (2.4), and $\deg\left(\sum s(\mathbf{x}) H^{(q)}(\mathbf{x})\right) \;\leq\; d$.

For a given set $A \subseteq \mathbb{N}^n$, searching through the space of degree d certificates can be computed via a *relative entropy program (REP)* [19] of size $n^{O(d)}$. REPs are convex optimization programs which are slightly more general than geometric programs but still efficiently solvable with interior point methods; see e.g. [10, 46] for more details.

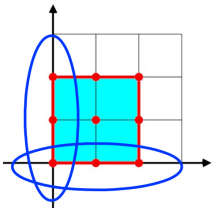

Figure 1 The Newton polytope and the support set of $r(x_1, x_k)$ with the supports of p_1 and p_2 in blue ovals.

3 Properties of the SONC cone

In this section we show that the SONC cone is neither closed under multiplication nor under affine transformations. First, we give a constructive proof for the fact that the SONC cone is not closed under multiplication, which is simpler than the initial proof of this fact in [19, Lemma 4.1]. Second, we use our construction to show that the SONC cone is not closed under affine transformation of variables.

▶ **Lemma 8.** *For every $d \geq 2$, $n \in \mathbb{N}^*$ the SONC cone $C_{n,d}$ is not closed under multiplication in the following sense: if $p_1, p_2 \in C_{n,d}$, then $p_1 \cdot p_2 \notin C_{n,2d}$ in general.*

Proof. For every $d = 2n$, $n \in \mathbb{N}^*$ we construct two SONC polynomials p_1, $p_2 \in C_{n,d}$ such that the product $p_1 p_2$ is an n variate, degree $2d$ polynomial that is not inside $C_{n,2d}$.

Let $n = 2$. We construct the following two polynomials $p_1,\ p_2 \in \mathbb{R}[x_1, x_2]$:

$$p_1(x_1, x_2) \ := \ (1 - x_1)^2, \qquad p_2(x_1, x_2) \ := \ (1 - x_2)^2.$$

First, observe that p_1, p_2 are nonnegative circuit polynomials, since, in both cases, $\lambda_1 = \lambda_2 = 1/2$, $f_{\boldsymbol{\alpha}(1)} = f_{\boldsymbol{\alpha}(2)} = 1$, and $f_{\boldsymbol{\beta}} = -2$, thus $2 = \Theta_f \geq |f_{\boldsymbol{\beta}}|$.

Now consider the polynomial $r(x_1, x_2) = ((1 - x_1)(1 - x_2))^2$. We show that this polynomial, even though it is nonnegative, is not a SONC polynomial. Note that $r(x_1, x_2) = 1 - 2x_1 - 2x_2 + 4x_1x_2 + x_1^2 + x_2^2 - 2x_1^2x_2 - 2x_1x_2^2 + x_1^2x_2^2$; the support of r is shown in Figure 1. Assume that $r \in C_{2,4}$, i.e., r has a SONC decomposition. This implies that the term $-2x_1$ has to be an inner term of some nonnegative circuit polynomial r_1 in this representation. Such a circuit polynomial necessarily has the terms 1 and x_1^2 as outer terms, that is, $r_1(x_1) = p_1(x_1, x_2) = 1 + x_1^2 - 2x_1$. Since $\Theta_{r_1} = 2$ the polynomial r_1 is indeed nonnegative and, in addition, we cannot choose a smaller constant term and preserve nonnegativity without simultaneously increasing the coefficient x_1^2. Next, also the term $-2x_2$ has to be an inner term of SONC r_2. Since this term again is on the boundary of New(r) the only option for such an r_2 is: $r_2(x_2) = p_2(x_1, x_2) = 1 + x_2^2 - 2x_2$. However, the term 1 has been already used in r_1, which leads to a contradiction, i.e., $r \notin C_{2,4}$. Since $C_{n,2d} \subseteq C_{n+1,2d}$, the general statement follows. ◀

Hereinafter we show another operation, which behaves differently for SONC than it does for SOS: Similarly as for multiplications, affine transformations also do not preserve the SONC structure. This observation is important for possible degree bounds on SONC certificates, when considering optimization problems over distinct descriptions of the hypercube.

▶ **Corollary 9.** *For every $d \geq 4$, $n \in \mathbb{N}^*$ the SONC cone $C_{n,d}$ is not closed under affine transformation of variables.*

Proof. Consider the polynomial $f(x_1, x_2) = x_1^2 x_2^2$. Clearly, the polynomial f is a nonnegative circuit polynomial since it is a monomial square, hence $u \in C_{n,d}$. Now consider the following affine transformation of the variables x_1 and x_2: $x_1 \to 1 - x_1$, $x_2 \to 1 - x_2$. After applying the transformation the polynomial f equals the polynomial $p_1 p_2$ from the proof of Lemma 8 and thus is not inside $C_{n,d}$. ◀

Corollary 9, from optimization perspective, implies that problem formulations obtained by applying affine transformations of variables can lead to problems of different tractability when using the SONC method. This means, on the one hand, that a choice of representation has to be done carefully, which makes the process of algorithm design more demanding. On the other hand, even a small change of representation might allow to find a SONC certificate or simplify an existing one. Note that whatever affine transformation of variables is applied to the Motzkin polynomial it *never* has a SOS certificate over reals, as the SOS cone is closed under affine transformations. The affine closure of the SONC cone, however, strictly contains the SONC cone and still yields a certificate of nonnegativity. In this sense, Corollary 9 motivates the following future research question:

Find an efficient algorithm to determine whether an affine transformation of a given polynomial f admits a SONC representation.

4 An Upper Bound on the Degree of SONC Certificates over the Hypercube

In this section we prove that every n-variate polynomial which is nonnegative over the boolean hypercube has a degree n SONC certificate. Moreover, if the hypercube is additionally constrained with some polynomials of degree at most d, then the nonnegative polynomial over such a set has degree $n + d$ SONC certificate. Motivated by the Corollary 9 and the discussion afterwards, we show this fact for *all* affine transformations of the 0/1 hypercube, that is for hypercubes $\{a_i, b_i\}^n$.

Formally, we consider the following setting: We investigate real multivariate polynomials in $\mathbb{R}[\mathbf{x}]$. For $j \in [n]$, and $a_j, b_j \in \mathbb{R}$, such that $a_j < b_j$ let

$$g_j(\mathbf{x}) \;:=\; (x_j - a_j)(x_j - b_j)$$

be a *quadratic polynomial with two distinct real roots*. Let $\mathcal{H} \subset \mathbb{R}^n$ denote the *n-dimensional hypercube* given by $\prod_{j=1}^n \{a_j, b_j\}$. Moreover, let

$$\mathcal{P} \;:=\; \{p_1, \ldots, p_m :\; p_i \in \mathbb{R}[\mathbf{x}],\; i \in [m]\}$$

be a set of polynomials, which we consider as constraints $p_i(\mathbf{x}) \geq 0$ with $\deg(p_i(\mathbf{x})) \leq d$ for all $i \in [n]$ as follows. We define

$$\mathcal{H}_{\mathcal{P}} \;:=\; \{\mathbf{x} \in \mathbb{R}^n :\; g_j(\mathbf{x}) = 0,\; j \in [n],\; p(\mathbf{x}) \geq 0,\; p \in \mathcal{P}\}$$

as the *n-dimensional hypercube $\mathcal{H}$ constrained by polynomial inequalities given by $\mathcal{P}$*. Throughout the paper we assume that $|\mathcal{P}| = \text{poly}(n)$, i.e. the size of the constraint set $\mathcal{P}$ is polynomial in n. This is usually the case, since otherwise the problem gets less tractable from the optimization point of view.

As a first step, we introduce a *Kronecker delta* function:

▶ **Definition 10.** For every $\mathbf{v} \in \mathcal{H}$ the function

$$\delta_{\mathbf{v}}(\mathbf{x}) \;:=\; \prod_{j \in [n]:\; v_j = a_j} \left(\frac{-x_j + b_j}{b_j - a_j}\right) \cdot \prod_{j \in [n]:\; v_j = b_j} \left(\frac{x_j - a_j}{b_j - a_j}\right) \tag{4.1}$$

is called the *Kronecker delta (function)* of the vector $\mathbf{v}$.

Next we justify the term "Kronecker delta", we show that for every $\mathbf{v} \in \mathcal{H}$ the function $\delta_{\mathbf{v}}(\mathbf{x})$ takes the value zero for all $\mathbf{x} \in \mathcal{H}$ except for $\mathbf{x} = \mathbf{v}$ where it takes the value one.

▶ **Lemma 11.** *For every $\mathbf{v} \in \mathcal{H}$ it holds that:*

$$\delta_{\mathbf{v}}(\mathbf{x}) \;=\; \begin{cases} 0, & \text{for every } \mathbf{x} \in \mathcal{H} \setminus \{\mathbf{v}\}, \\ 1, & \text{for } \mathbf{x} = \mathbf{v}. \end{cases}$$

Proof. On the one hand, if $\mathbf{x} \in \mathcal{H} \setminus \{\mathbf{v}\}$, then there exists an index k such that $\mathbf{x}_k \neq \mathbf{v}_k$. This implies that there exists at least one multiplicative factor in $\delta_{\mathbf{v}}$ which attains the value zero due to (4.1). On the other hand if $\mathbf{x} = \mathbf{v}$ then we have

$$\delta_{\mathbf{v}}(\mathbf{x}) \;=\; \prod_{j\in[n]:\ v_j=a_j} \left(\frac{-a_j+b_j}{b_j-a_j}\right) \prod_{j\in[n]:\ v_j=b_j} \left(\frac{b_j-a_j}{b_j-a_j}\right) \;=\; 1. \qquad \blacktriangleleft$$

The main result of this section is the following theorem.

▶ **Theorem 12.** *Let $f(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]_{n,n}$. Then $f(\mathbf{x}) \geq 0$ for every $\mathbf{x} \in \mathcal{H}_{\mathcal{P}}$ if and only if f has the following representation:*

$$f(\mathbf{x}) \;=\; \sum_{\mathbf{v}\in\mathcal{H}_{\mathcal{P}}} c_{\mathbf{v}}\delta_{\mathbf{v}}(\mathbf{x}) + \sum_{\mathbf{v}\in\mathcal{H}\setminus\mathcal{H}_{\mathcal{P}}} c_{\mathbf{v}}\delta_{\mathbf{v}}(\mathbf{x})p_{\mathbf{v}}(\mathbf{x}) + \sum_{j=1}^{n} s_j(\mathbf{x})g_j(\mathbf{x}) + \sum_{j=1}^{n} s_{n+j}(\mathbf{x})(-g_j(\mathbf{x})), \quad (4.2)$$

where $s_1, \ldots, s_{2n} \in C_{n,n-2}$, $c_{\mathbf{v}} \in \mathbb{R}_{\geq 0}$ and $p_{\mathbf{v}} \in \mathcal{P}$.

Since we are interested in optimization on the boolean hypercube $\mathcal{H}$, we assume without loss of generality that the polynomial f considered in Theorem 12 has degree at most n. Otherwise, one can efficiently reduce the degree of f by applying iteratively the polynomial division with respect to polynomials g_j with $j \in [n]$. The remainder of the division process is a polynomial with degree at most n that agrees with f on all the vertices of $\mathcal{H}$.

We begin with proving the easy direction of the equivalence stated in Theorem 12.

▶ **Lemma 13.** *If f admits a decomposition* (4.2)*, then $f(\mathbf{x})$ is nonnegative for all $\mathbf{x} \in \mathcal{H}_{\mathcal{P}}$.*

Proof. The coefficients $c_{\mathbf{v}}$ are nonnegative, all $s_j(\mathbf{x})$ are SONC and hence nonnegative on $\mathbb{R}^n$. We have $\pm g_j(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathcal{H}$, and for all choices of $\mathbf{v} \in \mathcal{H}$ we have $p_{\mathbf{v}}(\mathbf{x}) \geq 0$ for all $\mathbf{x} \in \mathcal{H}_{\mathcal{P}}$, and $\delta_{\mathbf{v}}(\mathbf{x}) \in \{0, 1\}$ for all $\mathbf{x} \in \mathcal{H}$. Thus, the right hand side of (4.2) is a sum of positive terms for all $\mathbf{x} \in \mathcal{H}_{\mathcal{P}}$. ◀

We postpone the rest of the proof of Theorem 12 to the end of the section. Now, we state a result about the presentation of the Kronecker delta function $\delta_{\mathbf{v}}$. In what follows let K be the basic closed semialgebraic set defined by $g_1, \ldots, g_n$ and $l_1, \ldots, l_{2n}$ as in (2.3).

▶ **Lemma 14.** *For every $\mathbf{v} \in \mathcal{H}$ the Kronecker delta function can be written as*

$$\delta_{\mathbf{v}} \;=\; \sum_{j=1}^{2^n} s_j H_j^{(n)},$$

for $s_1, \ldots, s_{2^n} \in \mathbb{R}_{\geq 0}$ and every $H_j^{(n)}$ given as in (2.4) *with $q = n$.*

Proof. First note that the function $\delta_{\mathbf{v}}$ can be rewritten as

$$\delta_{\mathbf{v}}(\mathbf{x}) \;=\; \prod_{j=1}^{2n} \frac{1}{b_j-a_j} \prod_{j\in[n]:\ v_j=a_j} (-x_j+b_j) \prod_{j\in[n]:\ v_j=b_j} (x_j-a_j)\,,$$

where $\prod_{j=1}^{n} \frac{1}{b_j-a_j} \in \mathbb{R}_{\geq 0}$. Now, the proof follows just by noting that for every $j \in [n]$ both inequalities $-x_j + b_j \geq 0$ and $x_j - a_j \geq 0$ are in K. ◀

The following statement is well-known in similar variations; see e.g. [5, Lemma 2.2 and its proof]. For clarity, we provide an own proof in the appendix.

▶ **Proposition 15.** *Let $f \in \mathbb{R}[\mathbf{x}]_{n,2d}$ be a polynomial vanishing on $\mathcal{H}$. Then $f = \sum_{j=1}^{n} p_j g_j$ for some polynomials $p_j \in \mathbb{R}[\mathbf{x}]_{n,2d-2}$.*

Proof. Let $\mathcal{J} := \langle g_1, \dots, g_n \rangle$ be the ideal generated by the g_j's. Let $\mathcal{V}(\mathcal{J})$ denote the affine variety corresponding to $\mathcal{J}$, $\mathcal{I}(\mathcal{V}(\mathcal{J}))$ denote its radical ideal, and let $\mathcal{I}(\mathcal{H})$ denote the ideal of $\mathcal{H}$. It follows from $\prod_{j=1}^{n} g_j \in \mathcal{J}$ that $\mathcal{V}(\mathcal{J}) \subseteq \mathcal{H}$ and hence $\mathcal{I}(\mathcal{H}) \subseteq \mathcal{I}(\mathcal{V}(\mathcal{J})) = \mathcal{J}$. The last equality holds since $\mathcal{J}$ itself is a radical ideal. This results from Seidenberg's Lemma; see [30, Proposition 3.7.15] by means of the following observations. The affine variety $\mathcal{V}(\mathcal{J})$ consists exactly of the points defining $\mathcal{H}$, therefore we know that $\mathcal{J}$ is a zero-dimensional ideal. Furthermore, for every $j \in [n]$ the polynomials g_j satisfy $g_j \in \mathcal{J} \cap K[x_j]$ and $\gcd(g_j, g_j') = 1$. Thus, every $f \in \mathcal{I}(\mathcal{H})$ is of the form $f = \sum_{j=1}^{n} p_j g_j$.

Moreover $G := \{g_1, \dots, g_n\}$ is a Gröbner basis for $\mathcal{J}$ with respect to the graded lexicographic order $\prec_{\text{glex}}$. This follows from Buchberger's Criterion, which says that G is a Gröbner basis for $\mathcal{J}$ if and only if for all pairs $i \neq j$ the remainder on the division of the S-polynomials $S(g_i, g_j)$ by G with respect to $\prec_{\text{glex}}$ is zero. Consider an arbitrary pair g_i, g_j with $i > j$. Then the corresponding S-polynomial is given by

$$S(g_i, g_j) \;=\; (a_j + b_j)x_i^2 x_j - (a_i + b_i)x_i x_j^2 - a_j b_j x_i^2 + a_i b_i x_j^2 \,.$$

Applying polynomial division with respect to $\prec_{\text{glex}}$ yields the remainder 0 and hence G is a Gröbner basis for $\mathcal{J}$ with respect to $\prec_{\text{glex}}$. Therefore, we conclude that if $f \in \mathbb{R}[\mathbf{x}]_{n,2d}$, then $\deg(p_j) \leq 2d - 2$. ◀

For an introduction to Gröbner bases see for example [15].

▶ **Theorem 16.** *Let $d \in \mathbb{N}$ and $f \in \mathbb{R}[\mathbf{x}]_{n,2d+2}$ such that f vanishes on $\mathcal{H}$. Then there exist $s_1, \dots, s_{2n} \in C_{n,2d}$ such that $f = \sum_{j=1}^{n} s_j g_j + \sum_{j=1}^{n} s_{n+j}(-g_j)$.*

Proof. By Proposition 15 we know that $f = \sum_{j=1}^{n} p_j g_j$ for some polynomials p_j of degree $\leq 2d$. Hence, it is sufficient to show that every single term $p_j g_j$ is of the form $\sum_{j=1}^{n} s_j g_j - \sum_{j=1}^{n} s_{n+j} g_j$ for some $s_1, \dots, s_{2n} \in C_{n,2d}$. Let $p_j = \sum_{i=1}^{\ell} a_{ji} m_{ji}$ where every $a_{ji} \in \mathbb{R}$ and every m_{ji} is a single monomial. We show that $p_j g_j$ has the desired form by investigating an arbitrary individual term $a_{ji} m_{ji} g_j$.

Case 1: Assume the exponent of m_{ji} is contained in $(2\mathbb{N})^n$. If $a_{ji} m_{ji}$ is a monomial square, then $a_{ji} m_{ji}$ is a circuit polynomial. If $a_{ji} < 0$, then $-a_{ji} m_{ji}$ is a monomial square. In both cases we obtain a representation $s_{ji}(\pm g_{ji})$, where $s_{ji} \in C_{n,2d}$.

Case 2: Assume the the exponent $\boldsymbol{\beta}$ of m_{ji} contains odd numbers. Without loss of generality, assume that $\boldsymbol{\beta} = (\beta_1, \dots, \beta_k, \beta_{k+1}, \dots, \beta_n)$ such that the first k entries are odd and the remaining $n - k$ entries are even. We construct a SONC polynomial $s_{ji} = a_{\boldsymbol{\alpha}(1)} \mathbf{x}^{\boldsymbol{\alpha}(1)} + a_{\boldsymbol{\alpha}(2)} \mathbf{x}^{\boldsymbol{\alpha}(2)} + a_{ji} \mathbf{x}^{\boldsymbol{\beta}}$ such that

$$\boldsymbol{\alpha}(1) \;=\; \boldsymbol{\beta} + \sum_{j=1}^{\lceil k/2 \rceil} \mathbf{e}_j - \sum_{j=\lceil k/2 \rceil + 1}^{k} \mathbf{e}_j, \qquad \boldsymbol{\alpha}(2) \;=\; \boldsymbol{\beta} - \sum_{j=1}^{\lceil k/2 \rceil} \mathbf{e}_j + \sum_{j=\lceil k/2 \rceil + 1}^{k} \mathbf{e}_j, \tag{4.3}$$

$$|a_{ji}| \;\leq\; \sqrt{2 a_{\boldsymbol{\alpha}(1)} a_{\boldsymbol{\alpha}(2)}}. \tag{4.4}$$

By the construction (4.3) $\boldsymbol{\alpha}(1), \boldsymbol{\alpha}(2) \in (2\mathbb{N})^n$ and $\boldsymbol{\beta} = 1/2(\boldsymbol{\alpha}(1) + \boldsymbol{\alpha}(2))$. Thus, s_{ji} is a circuit polynomial and by (4.4) the coefficients $a_{\boldsymbol{\alpha}(1)}, a_{\boldsymbol{\alpha}(2)}$ are chosen large enough such that $|a_{ji}|$ is bound by the circuit number $\sqrt{2 a_{\boldsymbol{\alpha}(1)} a_{\boldsymbol{\alpha}(2)}}$ corresponding to s_{ji}. Thus, s_{ji} is nonnegative by [27, Theorem 1.1]. Thus, we obtain

$$a_{ji} m_{ji} g_j \;=\; s_{ji} g_j + (a_{\boldsymbol{\alpha}(1)} \mathbf{x}^{\boldsymbol{\alpha}(1)} + a_{\boldsymbol{\alpha}(2)} \mathbf{x}^{\boldsymbol{\alpha}(2)})(-g_j),$$

where s_{ji}, $a_{\boldsymbol{\alpha}(1)} \mathbf{x}^{\boldsymbol{\alpha}(1)}$, and $a_{\boldsymbol{\alpha}(2)} \mathbf{x}^{\boldsymbol{\alpha}(2)}$ are nonnegative circuit polynomials.

Degree: All involved nonnegative circuit polynomials are of degree at most $2d$. In Case 1 this follows by construction. In Case 2 we have for the circuit polynomial s_{ji} that $\deg(\boldsymbol{\alpha}(1)), \deg(\boldsymbol{\alpha}(2)) = \deg(\boldsymbol{\beta})$ if k is even, and $\deg(\boldsymbol{\alpha}(1)) = \deg(\boldsymbol{\beta}) + 1$, $\deg(\boldsymbol{\alpha}(2)) = \deg(\boldsymbol{\beta})$ if k is odd. Since $\boldsymbol{\beta}$ is an exponent of the polynomial f, we know that $\deg(\boldsymbol{\beta}) \leq 2d$. If k is odd, however, then

$$\deg(\boldsymbol{\beta}) \;=\; \sum_{j=1}^{k} \underbrace{\beta_j}_{\text{odd number}} + \sum_{j=k+1}^{n} \underbrace{\beta_j}_{\text{even number}} \;,$$

i.e., $\deg(\boldsymbol{\beta})$ is a sum of k many odd numbers, with k being odd, plus a sum of even numbers. Thus, $\deg(\boldsymbol{\beta})$ has to be an odd number and hence $\deg(\boldsymbol{\beta}) < 2d$. Therefore, all degrees of terms in s_{ji} are bounded by $2d$ and thus $s_{ji} \in C_{n,2d}$.

Conclusion: We have that

$$f \;=\; \sum_{j=1}^{n} p_j g_j \;=\; \sum_{j=1}^{n} \sum_{i=1}^{\ell_j} a_{ji} m_{ji} g_j \;=\; \sum_{j=1}^{n} \sum_{i=1}^{\ell_j} s_{ji} g_j.$$

By Cases 1 and 2 and the degree argument, we have $s_{ji} \in C_{n,2d}$ for every i, j and by defining $s_j = \sum_{i=1}^{\ell_j} s_{ji} \in C_{n,2d}$ we obtain the desired representation of f. ◀

4.1 Proof of Theorem 12

In this section we combine the results of this section and finish the proof of Theorem 12.

Due to Lemma 13, it remains to show that $f(\mathbf{x})$ admits a decomposition of the form (4.2) with $\mathcal{H}_\mathcal{P} = \mathcal{H}$ if $f(\mathbf{x}) \geq 0$ for every $\mathbf{x} \in \mathcal{H}$.

Hence, when restricted to the hypercube $\mathcal{H}$, the polynomial f can be represented as:

$$\begin{aligned} f(\mathbf{x}) &= f(\mathbf{x}) \sum_{\mathbf{v} \in \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) + f(\mathbf{x}) \sum_{\mathbf{v} \in \mathcal{H} \setminus \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) \qquad \text{for all } \mathbf{x} \in \mathcal{H} \\ &= \sum_{\mathbf{v} \in \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) f(\mathbf{v}) + \sum_{\mathbf{v} \in \mathcal{H} \setminus \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) f(\mathbf{v}) \qquad \text{for all } \mathbf{x} \in \mathcal{H}, \end{aligned}$$

where the last equality follows by Lemma 11 .

Note that there might exist a vector $\mathbf{v} \in \mathcal{H} \setminus \mathcal{H}_\mathcal{P}$ such that f attains a negative value at $\mathbf{v}$. If $f(\mathbf{v}) < 0$, then let $p_\mathbf{v} \in \mathcal{P}$ be one of the polynomials among the constraints satisfying $p_\mathbf{v}(\mathbf{v}) < 0$. Otherwise, let $p_\mathbf{v} = 1$. Since by Lemma 11 we have $\delta_\mathbf{v}(\mathbf{x}) p_\mathbf{v}(\mathbf{x}) = \delta_\mathbf{v}(\mathbf{x}) p_\mathbf{v}(\mathbf{v})$ for every $\mathbf{v}, \mathbf{x} \in \mathcal{H}$, we can now write:

$$f(\mathbf{x}) \;=\; \sum_{\mathbf{v} \in \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) f(\mathbf{v}) + \sum_{\mathbf{v} \in \mathcal{H} \setminus \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) p_\mathbf{v}(\mathbf{x}) \frac{f(\mathbf{v})}{p_\mathbf{v}(\mathbf{v})} \qquad \text{for all } \mathbf{x} \in \mathcal{H}.$$

Thus, the polynomial $f(\mathbf{x}) - \sum_{\mathbf{v} \in \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) f(\mathbf{v}) - \sum_{\mathbf{v} \in \mathcal{H} \setminus \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) p_\mathbf{v}(\mathbf{x}) \frac{f(\mathbf{v})}{p_\mathbf{v}(\mathbf{v})}$ has degree at most $n + d$ and vanishes on $\mathcal{H}$. By Theorem 16 we finally get

$$f(\mathbf{x}) \;=\; \sum_{j=1}^{n} s_j(\mathbf{x}) g_j(\mathbf{x}) + \sum_{j=1}^{n} s_{n+j}(\mathbf{x})(-g_j(\mathbf{x})) + \sum_{\mathbf{v} \in \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) f(\mathbf{v}) + \sum_{\mathbf{v} \in \mathcal{H} \setminus \mathcal{H}_\mathcal{P}} \delta_\mathbf{v}(\mathbf{x}) p_\mathbf{v}(\mathbf{x}) \frac{f(\mathbf{v})}{p_\mathbf{v}(\mathbf{v})} \;,$$

for some $s_1, \ldots, s_{2n} \in C_{n,n-2}$ and $p_\mathbf{v} \in \mathcal{P}$. This finishes proof together with Lemma 14. ◀

▶ **Corollary 17.** *For every polynomial f, nonnegative over the boolean hypercube, constrained with polynomial inequalities of degree at most d, there exists a degree $n+d$ SONC certificate.*

Proof. The argument follows directly from Theorem 12 by noting that the right hand side of (4.2) is a SONC certificate of degree $n+d$ (see the Definition 7). ◀

4.2 Degree d SONC Certificates

In this section we show that if a polynomial f admits a degree d SONC certificate, then f also admits a short degree d certificate that involves at most $n^{O(d)}$ terms.

▶ **Theorem 18.** *Let f be an n-variate polynomial, nonnegative on the constrained hypercube $\mathcal{H}_\mathcal{P}$ with $|\mathcal{P}| = \text{poly}(n)$. Assume that there exists a degree d SONC certificate for f, then there exists a degree d SONC certificate for f involving at most $n^{O(d)}$ many nonnegative circuit polynomials.*

Proof. Since there exists a degree d SONC proof of the nonnegativity of f on $\mathcal{H}_\mathcal{P}$ we know that $f(\mathbf{x}) = \sum_j s_j H_j^{(q)}$, where the summation is finite, s_j's are SONCs, and $H_j^{(q)}$'s are product as defined in (2.4).

Step 1: We analyze the terms s_j. Since every s_j is a SONC, there exists a representation

$$s_j = \kappa_j \cdot \sum_{i=1}^{k_j} \mu_{ij} \cdot q_{ij}$$

such that $\kappa_j, \mu_{1j}, \ldots, \mu_{k_j j} \in \mathbb{R}_{>0}$, $\sum_{i=1}^{k_j} \mu_{ij} = 1$, and the q_{ij} are nonnegative circuit polynomials. Since s_j is of degree at most d, we know that $Q_j := \{q_{1j}, \ldots, q_{k_j j}\}$ is contained in $\mathbb{R}_{n,d}[\mathbf{x}]$, which is a real vector space of dimension $\binom{n+d}{d}$. Since s_j/κ_j is a convex combination of the q_{ij}, i.e. in the convex hull of Q_j, and $\dim(Q_j) \leq \binom{n+d}{d}$, applying Carathéodory's Theorem, see e.g. [57], yields that s_j/κ_j can be written as a convex combination of at most $\binom{n+d}{d}+1$ many of the q_{ij}.

Step 2: We analyze the terms $H_j^{(q)}$. By definition of the $\mathcal{H}_\mathcal{P}$ and the terms $H_j^{(q)}$ we have $H_j^{(q)} = g_{j_1} \cdots g_{j_s} \cdot l_{r_1} \cdots l_{r_t} \cdot p_{\ell_1} \cdot p_{\ell_v}$ with $j_1, \ldots, j_s \in [n]$, $r_1, \ldots, r_t \in [2n]$, and $\ell_1, \ldots, \ell_v \in [m]$. Since the maximal degree of $H_j^{(q)}$ is d, the number of different $H_j^{(q)}$'s is bounded from above by $\binom{n+2n+m}{d}$.

Conclusion: In summary, we obtain a representation:

$$f(\mathbf{x}) = \sum_{i=1}^{\binom{n+2n+m}{d}} H_j^{(q)} s_j = \sum_{i=1}^{\binom{n+2n+m}{d}} H_j^{(q)} \kappa_j \sum_{j=1}^{\binom{n+d}{d}+1} \mu_{ij} c_{ij}$$

Since we assume that m can bounded by $\text{poly}(n)$ the total number of summands is $\text{poly}(n)^{O(d)} = n^{O(d)}$, and we found a desired representation with at most $n^{O(d)}$ nonnegative circuit polynomials of degree at most d. ◀

The Theorem 18 states that when searching for a degree d SONC certificate it is enough to restrict to certificates containing at most $n^{O(d)}$ nonnegative circuit polynomials. Moreover, as proved in [19, Theorem 3.2] for a given set $A \subseteq \mathbb{N}^n$, searching through the space of degree d SONC certificates supported on a set A can be computed via a relative entropy program (REP) of size $n^{O(d)}$, see e.g. [19] for more information about REP. However, the above arguments do *not* necessarily imply that the search through the space of degree d SONC certificates can be performed in time $n^{O(d)}$. The difficulty is that one needs to restrict the

configuration space of n-variate degree d SONCs to a subset of order $n^{O(d)}$ to be able to *formulate* the corresponding REP in time $n^{O(d)}$. Since the current proof of Theorem 18 just guarantees the *existence* of a short SONC certificate, it is currently not clear, how to search for a short certificate efficiently. We leave this as an open problem.

5 There Exists No Equivalent to Putinar's Positivstellensatz for SONCs

In this section we address the open problem raised in [19] asking whether the Theorem 6 can be strengthened by requiring $q = 1$. Such a strengthening, for a positive polynomial over some basic closed semialgebraic set, would provide a SONC decomposition equivalent to Putinar's Positivstellensatz for SOS. The advantage of Putinar's Positivstellensatz over Schmüdgen's Positivstellensatz is that for every fixed degree d the cardinality of possible degree d certificates is smaller; for background see e.g., [38, 50] however, asymptotically still in both cases it is $n^{O(d)}$.

We answer this question in a negative way. More precisely, we provide a polynomial f which is strictly positive over the hypercube $\{\pm 1\}^n$ such that there does not exist a SONC decomposition of f for $q = 1$. Moreover, we prove it not only for the most natural choice of the box constraints that is $l_i = 1 \pm x_i$, but for a generic type of box constraints of the form $\ell_i = 1 + c_i \pm x_i$, for $c_i \in \mathbb{R}_{\geq 0}$. We close the section with a short discussion.

Let $\mathcal{H} = \{\pm 1\}^n$ and consider the following family of polynomials parametrized by a natural number a:

$$f_a(\mathbf{x}) \;:=\; (a-1)\prod_{i=1}^{n}\left(\frac{x_i+1}{2}\right)+1.$$

These functions take the value a for a vector $\mathbf{e} = \sum_{i=1}^{n} \mathbf{e}_i$ and the value 1 for every other $\mathbf{x} \in \mathcal{H} \setminus \{\mathbf{e}\}$. We define for every $d \in \mathbb{N}$

$$S_d \;:=\; \left\{ \sum_{\text{finite}} s \cdot h \;:\; s \in C_{n,2d},\; h \in \left\{1, \pm(x_i^2-1), 1+c_i \pm x_i \;:\; i \in [n], c_i \in \mathbb{R}_{\geq 0}\right\} \right\}$$

be the set of polynomials admitting a SONC decomposition over $\mathcal{H}$ given by Theorem 6 for $q = 1$. The main result of this section is the following theorem.

▶ **Theorem 19.** *For every $a > \frac{2^n-1}{2^{n-2}-1}$ we have $f_a \notin S_d$ for all $d \in \mathbb{N}$.*

Before we prove this theorem, we show the following structural results. Note that similar observations were already made for AGIforms by Reznick in [52] using a different notation.

▶ **Lemma 20.** *Every $s(\mathbf{x}) \in C_{n,2d}$ attains at most two different values on $\mathcal{H} = \{\pm 1\}^n$. Moreover, if $s(\mathbf{x})$ attains two different values, then each value is attained for exactly the half of the hypercube vertices.*

Proof. By Definition 1 every nonnegative circuit polynomial is of the form:

$$s(\mathbf{x}) \;=\; \sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)}\mathbf{x}^{\boldsymbol{\alpha}(j)} + f_{\boldsymbol{\beta}}\mathbf{x}^{\boldsymbol{\beta}}.$$

Note that for $j = 0, \ldots, r$, we have $\boldsymbol{\alpha}(j) \in (2\mathbb{N})^n$. Hence when evaluated over the hypercube $\mathbf{x} \in \mathcal{H} = \{\pm 1\}^n$, $s(\mathbf{x})$ can take only one of at most two different values $\sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)} \pm f_{\boldsymbol{\beta}}$.

If $s(\mathbf{x})$ attains two different values over $\mathcal{H}$, then there has to exist a non empty subset of variables that have an odd entry in $\boldsymbol{\beta}$. Let $I \subseteq [n]$ be this subset. Then $s(\mathbf{x}) = \sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)}(\mathbf{x}) - f_{\boldsymbol{\beta}}(\mathbf{x})$, for $\mathbf{x} \in \mathcal{H}$ if and only if $\mathbf{x}$ has an odd number of -1 entries in the set I. The number of such vectors is equal to

$$2^{n-|I|} \sum_{\substack{i=0,\\ i \text{ odd}}}^{|I|} 2^i \;=\; 2^{n-|I|}2^{|I|-1} \;=\; 2^{n-1}. \qquad \blacktriangleleft$$

▶ **Lemma 21.** *Every polynomial $s(\mathbf{x})\ell_i(\mathbf{x})$, with $s \in C_{n,2d}$ and $\ell_i = 1 + c_i \pm x_i$ being a box constraint, attains at most four different values on $\mathcal{H} = \{\pm 1\}^n$. Moreover, each value is attained for at least one forth of the hypercube vertices.*

Proof. By Lemma 20, $s(\mathbf{x})$ attains at most the two values $\left(\sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)} \pm f_{\boldsymbol{\beta}}\right)$ on $\mathcal{H}$. Similarly, $\ell_i(\mathbf{x})$ attains at most the two values $1 + c_i \pm x_i$ over $\mathcal{H}$. Thus, a polynomial $s(\mathbf{x})\ell_i(\mathbf{x})$ attains at most the four different values $\left(\sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)} \pm f_{\boldsymbol{\beta}}\right)(1 + c_i \pm x_i)$ on $\mathcal{H}$.

Let I be as in the proof of Lemma 20, i.e., the subset of variables that have an odd entry in $\boldsymbol{\beta}$. If $I = \emptyset$, then the first term $\sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)} + f_{\boldsymbol{\beta}}$ is constant over the hypercube $\mathcal{H}$, thus $s(\mathbf{x})\ell_i(\mathbf{x})$ takes two different values depending on the i-th entry of the vector. Each value is attained for exactly half of the vectors.

If $I \neq \emptyset$ and $i \notin I$ the claim holds since the value of the first term depends only on the entries in I and the value of the second term depends on the i-th entry. Hence, the polynomial $s(\mathbf{x})\ell_i(\mathbf{x})$ attains four values each on exactly one fourth of $\mathcal{H}$ vectors.

Finally, let $I \neq \emptyset$ and $i \in I$. Partition the hypercube vertices into two sets depending on the i-th entry. Each set has cardinality 2^{n-1}. Consider the set with $x_i = 1$. For the vectors in this set the second term takes a constant value $2 + c$. Over this set the polynomial s takes one of the values $\sum_{j=0}^{r} f_{\boldsymbol{\alpha}(j)}(\mathbf{x}) \pm f_{\boldsymbol{\beta}}(\mathbf{x})$, depending on whether $\mathbf{x}$ has an odd or even number of -1 entries in the set $I \setminus \{-1\}$. In both cases the number of such vectors is equal to

$$2^{n-|I|} \sum_{\substack{i=0,\\ i \text{ odd}}}^{|I|-1} 2^i \;=\; 2^{n-|I|}2^{|I|-2} = 2^{n-2}.$$

The analysis for the case $x_i = -1$ is analogous. $\blacktriangleleft$

Now we can provide the proof of Theorem 19.

Proof of Theorem 19. Assume $f_a \in S_d$ for some $a \in \mathbb{N}$ and $d \in \mathbb{N}$. We prove that a has to be smaller or equal than $\frac{2^n-1}{2^{n-2}-1}$. Since $f_a \in S_d$ we know that

$$f_a(\mathbf{x}) \;=\; s_0(\mathbf{x}) + \sum_{i=1}^{n} s_i(\mathbf{x})\ell_i(\mathbf{x}) + \sum_{j=1}^{n} \tilde{s}_j(\mathbf{x})(x_j^2 - 1) + \tilde{s}_{j+n}(\mathbf{x})(1 - x_j^2)$$

with $s_0, \ldots, s_n, \tilde{s}_1, \ldots, \tilde{s}_{2n} \in C_{n,2d}$. Since $\pm(x_j^2 - 1)$ for $j \in [n]$ vanishes over the hypercube $\mathcal{H}$, for some $s_0,\ s_i \in C_{n,2d}$ we can conclude

$$f_a(\mathbf{x}) \;=\; s_0(\mathbf{x}) + \sum_{i=1}^{n} s_i(\mathbf{x})\ell_i(\mathbf{x}) \qquad \text{for all } \mathbf{x} \in \mathcal{H} \tag{5.1}$$

Let $s_{0,k}$, and $s_{i,j}$ be some nonnegative circuit polynomials such that $s_0 = \sum_k s_{0,k}$, and $s_i = \sum_j s_{i,j}$. Thus, we get

$$\begin{aligned}\sum_{\mathbf{x}\in\mathcal{H}} \left(s_0(\mathbf{x}) + \sum_i s_i(\mathbf{x})\ell_i(\mathbf{x}) \right) &= \sum_k \sum_{\mathbf{x}\in\mathcal{H}} s_{0,k}(\mathbf{x}) + \sum_i \sum_j \sum_{\mathbf{x}\in\mathcal{H}} s_{i,j}(\mathbf{x})\ell_{i,j}(\mathbf{x}) \\ &\geq \sum_k 2^{n-1} s_{0,k}(\mathbf{e}) + \sum_i \sum_j 2^{n-2} s_{i,j}(\mathbf{e})\ell_{i,j}(\mathbf{e}) \\ &\geq 2^{n-2} \left(s_0(\mathbf{e}) + \sum_i s_i(\mathbf{e})\ell_i(\mathbf{e}) \right) = 2^{n-2} a,\end{aligned}$$

where the first inequality comes from Lemma 20 and 21 and the last equality from the fact that $f_a(\mathbf{e}) = a$. On the other hand, by the properties of f_a and the equality (5.1), we know that

$$\sum_{\mathbf{x}\in\mathcal{H}} \left(s_0(\mathbf{x}) + \sum_i s_i(\mathbf{x})\ell_i(\mathbf{x}) \right) = 2^n - 1 + a,$$

which makes the subsequent inequality a necessary requirement for $f_a \in S_d$:

$$a \leq \frac{2^n - 1}{2^{n-2} - 1}. \qquad \blacktriangleleft$$

Note that an easier example of polynomial nonnegative over the set $\mathcal{H}$ exists, that does not attain a SONC decomposition for $q = 1$. Consider a polynomial $\delta_{\mathbf{v}}(\mathbf{x})$ defined in Definition 10 for $x \in \mathbb{R}^n$, for $n \geq 3$. The analysis for this example is easier since the polynomial is zero on all vertices of $\mathcal{H}$ but one, thus by Lemma 21 it is impossible to fit a SONC certificate that matches those values. However, an important fact is that, by Theorem 6 a polynomial to admit a SONC certificate has to necessarily be strictly positive over the given set, which is not the case for $\delta_{\mathbf{v}}(\mathbf{x})$ and the set $\mathcal{H}$.

Speaking from a broader perspective, we interpret Theorem 19 as an indication that the real algebraic structures, which we use to handle sums of squares, do not apply in the same generality to SONCs. We find this not at all surprising from the point of view that in the 19th century Hilbert initially used SOS as a certificate for nonnegativity and many of the algebraic structures in question where developed afterwards with Hilbert's results in mind; see [53] for a historic overview. Our previous work shows that SONCs, in contrast, can, e.g., very well be analyzed with combinatorial methods. We thus see Theorem 19 as further evidence about the very different behavior of SONCs and SOS and as an encouragement to take methods beside the traditional real algebraic ones into account for the successful application of SONCs in the future.

References

1 S. Arora, B. Barak, and D. Steurer. Subexponential algorithms for unique games and related problems. In *FOCS*, pages 563–572, 2010.

2 S. Arora, S. Rao, and U. V. Vazirani. Expander flows, geometric embeddings and graph partitioning. *J. ACM*, 56(2):5:1–5:37, 2009. doi:10.1145/1502793.1502794.

3 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.

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

5 B. Barak and D. Steurer. Sum-of-squares proofs and the quest toward optimal algorithms. *Electronic Colloquium on Computational Complexity (ECCC)*, 21:59, 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 on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 143–151, 2015.

7 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.

8 M. H. Bateni, M. Charikar, and V. Guruswami. Maxmin allocation via degree lower-bounded arborescences. In *STOC*, pages 543–552, 2009. doi:10.1145/1536414.1536488.

9 Grigoriy Blekherman. There are significantly more nonegative polynomials than sums of squares. *Israel Journal of Mathematics*, 153(1):355–380, Dec 2006.

10 V. Chandrasekaran and P. Shah. Relative entropy optimization and its applications. *Math. Program.*, 161(1-2):1–32, 2017.

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

12 E. Chlamtac. Approximation algorithms using hierarchies of semidefinite programming relaxations. In *FOCS*, pages 691–701, 2007.

13 E. Chlamtac and G. Singh. Improved approximation guarantees through higher levels of SDP hierarchies. In *APPROX-RANDOM*, pages 49–62, 2008.

14 E. Chlamtac and M. Tulsiani. Convex relaxations and integrality gaps. In *to appear in Handbook on semidefinite, conic and polynomial optimization*. Springer, 2012.

15 D.A. Cox and J. Little D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

16 M. Cygan, F. Grandoni, and M. Mastrolilli. How to sell hyperedges: The hypermatching assignment problem. In *SODA*, pages 342–351, 2013.

17 W. F. de la Vega and C. Kenyon-Mathieu. Linear programming relaxations of maxcut. In *SODA*, pages 53–61, 2007.

18 T. de Wolff. Amoebas, nonnegative polynomials and sums of squares supported on circuits. *Oberwolfach Rep.*, 23:53–56, 2015.

19 M. Dressler, S. Iliman, and T. de Wolff. A Positivstellensatz for Sums of Nonnegative Circuit Polynomials. *SIAM J. Appl. Algebra Geom.*, 1(1):536–555, 2017.

20 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.

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

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

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

24 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.

25 D. Hilbert. Uber die darstellung definiter formen als summe von formen-quadraten. *Annals of Mathematics*, 32:342–350, 1888.

26 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 *Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2016, Cambridge, MA, USA, June 18-21, 2016*, pages 178–191, 2016.

27 S. Iliman and T. de Wolff. Amoebas, nonnegative polynomials and sums of squares supported on circuits. *Res. Math. Sci.*, 3:3:9, 2016.

28 Pravesh Kothari, Jacob Steinhardt, and David Steurer. Robust moment estimation and improved clustering via sum of squares. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2018*, 2018.

29 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, Montreal, QC, Canada, June 19-23, 2017*, pages 132–145, 2017.

30 M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.

31 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.

32 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.

33 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.

34 J.B. Lasserre. Global optimization with polynomials and the problem of moments. *SIAM J. Optim.*, 11(3):796–817, 2000/01.

35 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.

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

37 M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*, volume 149 of *IMA Vol. Math. Appl.*, pages 157–270. Springer, New York, 2009.

38 M. Laurent. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*, volume 149 of *IMA Vol. Math. Appl.*, pages 157–270. Springer, New York, 2009.

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

40 L. Lovász. On the shannon capacity of a graph. *IEEE Trans. Inform. Theory*, 25:1–7, 1979.

41 A. Magen and M. Moharrami. Robust algorithms for on minor-free graphs based on the Sherali-Adams hierarchy. In *APPROX-RANDOM*, pages 258–271, 2009.

42 M. Mastrolilli. High degree sum of squares proofs, bienstock-zuckerberg hierarchy and CG cuts. In *Integer Programming and Combinatorial Optimization - 19th International Conference, IPCO 2017, Waterloo, ON, Canada, June 26-28, 2017, Proceedings*, pages 405–416, 2017.

43 R. Meka, A. Potechin, and A. Wigderson. Sum-of-squares lower bounds for planted clique. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 87–96, 2015.

44 T.S. Motzkin. The arithmetic-geometric inequality. *Symposium on Inequalities*, pages 205–224, 1967. cited By 1.

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

46 Y. Nesterov and A. Nemirovskii. *Interior Point Polynomial Algorithms in Convex Programming*. Studies in Applied Mathematics. Society for Industrial and Applied Mathematics, 1994.

47 J. Oxley. *Matroid theory*, volume 2 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, 2011.

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

49 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.

50 M. Putinar. Positive polynomials on compact semi-algebraic sets. *Indiana Univ. Math. J.*, 42(3):969–984, 1993.

51 P. Raghavendra and N. Tan. Approximating csps with global cardinality constraints using sdp hierarchies. In *SODA*, pages 373–387, 2012.

52 B. Reznick. Forms derived from the arithmetic-geometric inequality. *Math. Ann.*, 283(3):431–464, 1989.

53 B. Reznick. Some concrete aspects of Hilbert's 17th Problem. In *Real algebraic geometry and ordered structures (Baton Rouge, LA, 1996)*, volume 253 of *Contemp. Math.*, pages 251–272. Amer. Math. Soc., Providence, RI, 2000.

54 Tselil Schramm and David Steurer. Fast and robust tensor decomposition with applications to dictionary learning. In *Proceedings of the 30th Conference on Learning Theory, COLT 2017, Amsterdam, The Netherlands, 7-10 July 2017*, pages 1760–1793, 2017.

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

56 Johan Thapper and Stanislav Zivny. The limits of SDP relaxations for general-valued csps. In *32nd Annual ACM/IEEE Symposium on Logic in Computer Science, LICS 2017, Reykjavik, Iceland, June 20-23, 2017*, pages 1–12, 2017.

57 G.M. Ziegler. *Lectures on Polytopes*. Springer Verlag, 2007.