Real τ-Conjecture for sum-of-squares: A unified approach to lower bound and derandomization

Pranjal Dutta[1]

Chennai Mathematical Institute, India
pranjal@cmi.ac.in

Abstract. Koiran's real τ-conjecture asserts that if a non-zero real univariate polynomial f can be written as $\sum_{i=1}^{k}\prod_{j=1}^{m} f_{ij}$, where each f_{ij} contains at most t monomials, then the number of distinct real roots of f is polynomially bounded in kmt. Assuming the conjecture with parameter $m = \omega(1)$, one can show that $\mathsf{VP} \neq \mathsf{VNP}$ (i.e. symbolic permanent requires superpolynomial-size circuit). In this paper, we propose a τ-conjecture for sum-of-squares (SOS) model (equivalently, $m = 2$). For a univariate polynomial f, we study the *sum-of-squares* representation (SOS), i.e. $f = \sum_{i\in[s]} c_i f_i^2$, where c_i are field elements and the f_i's are univariate polynomials. The size of the representation is the number of monomials that appear across the f_i's. Its minimum is the *support-sum* $S(f)$ of f. We *conjecture* that any real univariate f can have at most $O(S(f))$-many real roots. A random polynomial satisfies this property. We connect this conjecture with two central open questions in algebraic complexity– matrix rigidity and VP vs. VNP.
The concept of matrix rigidity was introduced by Valiant (MFCS 1977) and independently by Grigoriev (1976) in the context of computing linear transformations. A matrix is rigid if it is far (in terms of Hamming distance) from any low rank matrix. We know that rigid matrices exist, yet their explicit construction is still a major open question. Here, we show that SOS-τ-conjecture implies construction of such matrices. Moreover, the conjecture also implies the famous Valiant's hypothesis (Valiant, STOC 1979) that VNP is exponentially harder than VP. Thus, this new conjecture implies both the fundamental problems by Valiant. Furthermore, strengthening the conjecture to sum-of-cubes (SOC) implies that blackbox-PIT (Polynomial Identity Testing) is in P. This is the first time a τ-conjecture has been shown to give a polynomial-time PIT. We also establish some special cases of this conjecture, and prove tight lower bounds for restricted depth-2 models.

Keywords: τ-conjecture · matrix rigidity · real root · VP · VNP · PIT

1 Introduction

An *algebraic circuit* over an underlying field $\mathbb{F}$ is a natural model that represents a polynomial compactly. It is a layered directed acyclic graph with the leaf nodes as the input variables $x_1, \ldots, x_n$, and constants from $\mathbb{F}$. All the other nodes are labeled as + and × gates. The output of the root node is the polynomial computed by the circuit. Two important complexity parameters of a circuit are: **1)** the *size*, the number of edges and nodes, **2)** the *depth*, the number of layers.

The famous Shub-Smale τ-conjecture [48] is a conjecture in algebraic complexity, asserting that a univariate polynomial which is computable by a small algebraic circuit has a small number of integer roots. It was established in [48] that the τ-conjecture implies $\mathsf{P}_{\mathbb{C}} \neq \mathsf{NP}_{\mathbb{C}}$, for the Blum–Shub–Smale (BSS) model of computation over the complex numbers [6,7]. Bürgisser [9] obtained a similar result for the algebraic version of P vs. NP, namely, VP vs. VNP (informally defined below), which was originally proposed by Valiant [53].

The class $\mathsf{VP}_{\mathbb{F}}$ contains the families of n-variate polynomials of degree $\mathsf{poly}(n)$ over $\mathbb{F}$, computed by circuits of $\mathsf{poly}(n)$-size. The class $\mathsf{VNP}_{\mathbb{F}}$ can be seen as a non-deterministic analog of the class $\mathsf{VP}_{\mathbb{F}}$[1]. Informally, it contains the families of n-variate polynomials that can be written as an exponential sum of polynomials in VP; for formal definitions, see Section 2. VP is contained in VNP, and it is believed that this containment is *strict* (Valiant's Hypothesis [53]). For more details, see [11, 31, 47]. Unless specified otherwise, we consider field $\mathbb{F} = \mathbb{R}$, the field of real numbers, or $\mathbb{C}$, the field of complex numbers.

One possible disadvantage of the τ-conjecture is the reference of *integer roots*. As a natural approach to the τ-conjecture, one can try to bound the number of *real roots* instead of integer roots. However, a mere replacement of "integer roots" by "real roots" fails miserably as the number of real roots of a univariate polynomial can be *exponential* in its circuit size; for e.g. Chebyshev polynomials [49]. Interestingly, Koiran [24] came up with the following τ-conjecture for the *restricted* (depth-4) circuits. It states that if $f \in \mathbb{R}[x]$ is a polynomial of the form $f = \sum_{i=1}^{k} \prod_{j=1}^{m} f_{ij}$, where each $f_{ij} \in \mathbb{R}[x]$ is t-sparse [2], then the number of *distinct* real roots of f can at most be $\mathsf{poly}(kmt)$. Note that, the conjecture is true for $m = 1$, by Descartes' rule of signs (Lemma 5). Using the celebrated depth-4 reduction [2,25], it was established that real τ-conjecture with $m = \omega(1)$, yields a strong separation in the *constant-free* settings, i.e. $\mathsf{VP}_0 \neq \mathsf{VNP}_0$. Later, it was shown to imply $\mathsf{VP} \neq \mathsf{VNP}$, see [16, 50].

Before trying to prove a lower bound in the general settings, we would like to remark that one of the major open problems in algebraic complexity is to prove any *super-linear* lower bound for *linear circuits*. These are simple circuits where we are only allowed to use addition and multiplication by a scalar. By definition, they can only compute linear (affine) functions. In fact, any algebraic circuit, computing a set of linear functions, can be converted into a linear circuit with only a constant blow-up in size, see [11, Theorem 13.1]. Clearly, every set of n linear functions on n variables can be represented by a matrix in $\mathbb{F}^{n \times n}$, which can be computed by a linear circuit of size $O(n^2)$.

Given the ubiquitous role linear transformations play in computing, understanding the inherent complexity of explicit linear transformations is important. Using dimension argument/counting, it can be shown that a random matrix re-

[1] We will drop the subscript $\mathbb{F}$ whenever $\mathbb{F}$ is implicitly clear or does not matter.

[2] $f := \sum_{i=0}^{n} a_i\, x^i$ is t-sparse if at most t of the coefficients $a_0, \ldots, a_n$ are non-zero.

quires $\Omega(n^2)$-size circuit. However, showing the same for an explicit $A_n \in \mathbb{F}^{n\times n}$, still remains open. The standard notion of explicitness is that there is a deterministic algorithm which outputs the matrix A_n in $\mathsf{poly}(n)$-time. Weak super-linear lower bounds are known for constant-depth linear circuits, using superconcentrators and their minimal size, see [5,37,39,51]. It is also known that this technique alone is *insufficient* for proving lower bounds for logarithmic depth.

The quest for showing super-linear lower bound for logarithmic-depth lead to the notion of *matrix rigidity*, a pseudorandom property of matrices, introduced by Valiant [52], and independently by Grigoriev [17].

Definition 1 (Matrix rigidity). *A matrix A over $\mathbb{F}$ is* (r, s)-rigid*, if one needs to change $> s$ entries in A to obtain a matrix of rank $\leq r$. That is, one* cannot *decompose A into $A = R + S$, where* $\text{rank}(R) \leq r$ *and* $\text{sp}(S) \leq s$*, where* $\text{sp}(S)$ *is the* sparsity of *S, i.e., the number of nonzero entries in S.*

Valiant [52] showed that an explicit construction of a $(\epsilon{\cdot}n, n^{1+\delta})$-rigid matrix, for some $\epsilon, \delta > 0$, will imply a *super-linear* lower bound for linear circuits of depth $O(\log n)$; for a simple proof, see [47, Theorem 3.22]. Pudlak [38] observed that similar rigidity parameters will imply even *stronger* lower bounds for constant depth circuits. Here, we remark that a random matrix is $(r, (n-r)^2)$-rigid, but the best explicit constructions have rigidity $(r, n^2/r \cdot \log(n/r))$ [15,46], which is *insufficient* for proving lower bounds. For recent works, we refer to [4,14,41].

The interplay between proving lower bounds and derandomization is one of the central themes in complexity theory [34]. In algebraic complexity, the central derandomization question is to design an efficient deterministic algorithm for *Polynomial Identity Testing* (PIT) in the *blackbox* model, i.e. to test the zeroness of a given algebraic circuit via query access. Though the celebrated *Polynomial Identity Lemma* [12,35,45,55]) gives a randomized polynomial-time algorithm for blackbox-PIT, finding a deterministic polynomial-time algorithm has been a long-standing open question. The problem also naturally appears in the geometric approaches to the $\mathsf{P} \neq \mathsf{NP}$ question, e.g. [18,32,33].

Efficient blackbox-PIT and circuit lower bounds are strongly intertwined [1,19,23]. However, any connection between constructing explicit rigid matrix and proving $\mathsf{VP} \neq \mathsf{VNP}$ (or PIT $\in \mathsf{P}$) is not *clear*. Further, to the best of our knowledge, we do not know any *singular* problem that solves these *central* problems. Towards that, we conjecture 1, the SOS-τ-conjecture, and prove Theorems 1,2, & 5, below stated:

> *If the number of real roots of any $f \in \mathbb{R}[x]$ is bounded by a constant multiple of the sum of the sparsity of the univariates when written as sum-of-squares, then there exists an explicit $(\epsilon \cdot n, n^{1+\delta})$-rigid matrix for $\epsilon, \delta > 0$. It also implies exponential separation between $\mathsf{VP}_{\mathbb{C}}$ and $\mathsf{VNP}_{\mathbb{C}}$. Further, strengthening the requirement to sum-of-cubes, puts blackbox-PIT in P.*

The novelty of this work is to introduce the τ-conjecture in the SOS (or SOC)-model and link with the three main problems in algebraic complexity. The sum-of-squares representation (SOS) is one of the most fundamental in number theory and algebra [36,40]; it has found many applications in approximation & optimization, see [29,30,43]. Intuitively, the analytic nature of SOS makes this conjecture a *viable* path to resolve the long standing questions.

1.1 Sum-of-squares (SOS) model and a τ-conjecture

We say that a univariate polynomial $f(x) \in R[x]$ over a ring R is computed as a *sum-of-squares* (SOS) if

$$f \;=\; \sum_{i=1}^{s} c_i f_i^2 \;, \tag{1}$$

for some *top-fanin* s, where $f_i(x) \in R[x]$ and $c_i \in R$.

Definition 2 (Support-sum size $S_R(f)$, [13]). *The* size *of the representation of f in (1) is the* support-sum*, the sum of the sparsity (or support size) of the polynomials f_i. The* support-sum size *of f, denoted by $S_R(f)$* [3]*, is defined as the minimal support-sum of f.*

Let $|f|_0$ denote the sparsity of f. For any field $R = \mathbb{F}$ of characteristic $\neq 2$, we have $\sqrt{|f|_0} \;\leq\; S_{\mathbb{F}}(f) \;\leq\; 2\,|f|_0 + 2$. The lower bound can be shown by counting monomials. The upper bound follows from the identity: $f = (f+1)^2/4 - (f-1)^2/4$. In particular, the SOS-model is *complete* for any field of characteristic $\neq 2$. Further, a standard geometric-dimension argument implies that $S_{\mathbb{F}}(f) = \Theta(d)$, for *most* univariate polynomials f of degree d, since $|f|_0 = \Theta(d)$, for a random f.

Any $\#\mathsf{P}/\mathsf{poly}$-explicit f_d (for definition, see Section 2), which satisfies $S(f_d) \geq \Omega(d^{1/2+\varepsilon})$, for some sub-constant function $\varepsilon(d)$, implies $\mathsf{VP} \neq \mathsf{VNP}$ [13, Theorem 6]. However, in this work, we are interested in the number of real roots of f in terms of $S(f)$. Since the sparsity of f can be at most $S(f)^2$, f can have at most $S(f)^2$-many real roots by Descartes' rule of signs (Lemma 5). Further, it can be shown that a random polynomial f can have at most $O(S(f))$-many real roots, similar to [8, Theorem 1.1 with $k=2$].

Moreover, if f and g have sparsity s, is the number of real roots of $fg+1$ linear in s? This question was originally designed by Arkadev Chattopadhyay, as the simplest case of Koiran's tau-conjecture; unfortunately we do not yet understand it. Motivated thus, we conjecture the following. Motivated thus, we conjecture the following.

Conjecture 1 (SOS-τ-conjecture). Consider any non-zero polynomial $f(x) \in \mathbb{R}[x]$. Then, there exists a positive constant $c > 0$ such that the number of distinct real roots of f is at most $c \cdot S_{\mathbb{R}}(f)$.

Remarks. 1. One can show that Conjecture 1 implies $S_{\mathbb{C}}((x+1)^d) \geq \Omega(d)$; see Lemma 9. This is almost identical to [21,22], where strong distribution property

[3] We will write $S(f)$ whenever the underlying ring is clear or does not matter.

of complex roots with multiplicities were shown to be implied, from the real τ-conjecture.

2. In the Equation (1), we could restrict the degrees of f_i to be $O(d \log d)$. This might help us proving the conjecture; for details, see Section 3.2 (& remark).

3. The $fg+1$ case happens to be a special case of this new conjecture for 3 squares. For the two squares,i.e. any $f \in \mathbb{R}[x]$ of the form $c_1 f_1^2 + c_2 f_2^2$, can have at most $O(|f_1|_0 + |f_2|_0)$-many real roots; for details see Theorem 9 in Section 6.1.

1.2 Main results

The leitmotif of this paper is the interplay between the SOS-τ-conjecture and derandomization/hardness questions in algebraic complexity. We start by asking: can the τ-conjecture in the SOS-model imply the existence of explicit rigid matrices? We evince a positive answer. This is the first time a τ-conjecture has been shown to solve the long-awaited matrix rigidity problem.

Theorem 1. *If Conjecture 1 holds, then there exist $\epsilon > 0$ and a "very"-explicit family of real matrices $(A_n)_n$ such that A_n is $(\epsilon \cdot n, n^{1+\delta})$-rigid, for any $\delta < 1$.*

Remarks. 1. The matrix A_n is not only $\mathsf{poly}(n)$-explicit, it is 'very' explicit in the good common sense: one could consider as simple as binomial coefficients, recorded one row at a time. This is quite interesting given the recent dramatic developments that have killed virtually all known candidates.

2. Our proof requires the upper bound of $O(S(f))$ in Conjecture 1; any weaker upper bound *does not* yield the same rigidity parameter.

Theorem 1 implies *super-linear* lower bound for linear circuits [52]. Interestingly, Conjecture 1 is robust enough to show strong lower bounds in the *general* circuit settings as well.

Theorem 2. *Conjecture 1 implies that* $\mathsf{VNP}_{\mathbb{C}}$ *is exponentially harder than* $\mathsf{VP}_{\mathbb{C}}$*.*

Remarks. 1. One could directly obtain that Conjecture 1 implies $S_{\mathbb{R}}(f_d) \geq \Omega(d)$, where $f_d := \prod_{i=1}^{d}(x-i)$. However, to separate VP and VNP, using the proof techniques of [13] (with $\varepsilon = 1$) *require* GRH (Generalized Riemann Hypothesis).

2. To show an unconditional lower bound, we work with $f_d := \sum_{i=0}^{d} 2^{2i(d-i)} \cdot x^i$ (a similar family was considered in [16, Equation 8]). However, the hardness proof is completely different from [16], due to disparate settings and parameters.

3. The hardness proof presented here does not require any *fine-grained* decomposition, as required in [13],i.e. via algebraic branching programs (ABP) or circuit-depth boosting techniques. For the simplicity and completeness, we present a self-contained proof in Section 3.2.

4. The exponential separation puts blackbox-PIT $\in \mathsf{QP}$ (*Quasi*poly) [23].

We introduce a τ-conjecture for the sum-of-cubes (SOC-model) in Section 4, and show that sufficient strengthening (of the measure) gives a *polynomial*-time PIT for general circuits (Theorem 5). This is the *first* time a τ-conjecture has been shown to derandomize PIT *completely.*

We also show lower bounds for symmetric depth-2 circuits and invertible depth-2 circuits in Section 5, by studying $S(f_d)$, for different explicit polynomials f_d (in the restricted sense); for details see Theorem 6.

1.3 Proof ideas

The τ-conjecture for $\sum^k \prod^m \sum^t \prod$-model (with $m = \omega(1)$) has been shown to imply circuit hardness [16, 24, 26]. This work is more about remodeling the τ-conjecture in the *simplest* format possible and viewing this as the pivotal problem of interest. Although the proofs of the theorems are standard and obtained from clever maneuvering of the existing techniques, the implications are quite far-reaching. Moreover, the τ-conjecture for $m = 1$ is true using Descartes' rule (Lemma 5) while $m = 2$ (*equivalent* to SOS-model) *solves* almost everything. This makes the whole regime tantalisingly close to being realisable.

Proof idea of Theorem 1. If A is not $(\epsilon n, n^{1+\delta})$-rigid, then one can show that A can be written as BC, where 'sparse' matrices B and C can have at most $2\epsilon n^2 + 2n^{1+\delta}$ non-zero entries (item 1-4 in Section 3.1). Now, the idea is to use $f_d := \prod_{i \in [d]} (x - i)$, to construct matrices A_n that cannot be factored thus.

Define $d := n^2 - 1$, $[x_1]_n := \begin{bmatrix} 1 & x_1 & \cdots & x_1^{n-1} \end{bmatrix}$, and similarly $[x_2]_n$. Define polynomial $g_n(x_1, x_2)$ such that after Kronecker substitution: $g_n(x_1, x_2) \mapsto g_n(x, x^n) = f_d$. Finally, define matrix A_n such that $[x_2]_n A_n [x_1]_n^T = g_n(x_1, x_2)$. Note that A_n is $\mathsf{poly}(n)$-explicit.

Assume Conjecture 1. Then, $S_{\mathbb{R}}(f_d) > \delta' \cdot d$ for some $\delta' > 0$. We show that any layered linear circuit of depth-2 computing A_n has size $> (\delta'/2) \cdot d$. Suppose not, i.e. $A_n = BC$, with $B \in \mathbb{R}^{n \times t}$, $C \in \mathbb{R}^{t \times n}$ such that $t \leq (\delta'/2) \cdot d$. Then, $[x_2]_n B\, C\, [x_1]_n^T = g_n(x_1, x_2)$. We deduce that $f_d = \sum_{i \in [t]} \ell_i(x)\, \tilde{\ell}_i(x^n)$, where $([x_2]_n B)_i =: \tilde{\ell}_i(x_2)$ and $(C\, [x]_n^T)_i =: \ell_i(x_1)$. Note that, f_d can easily be written as sum of $2t$ squares with sum of sparsity $\leq \delta' \cdot d$, a contradiction.

This ensures that the number of nonzero entries in B and C is 'large'. Therefore, choosing ϵ and δ carefully, we have A_n *is rigid*. We remark that we can also work with $f_d = (x+1)^d$, but one needs to use Lemma 9.

Proof idea of Theorem 2. We work with $f_d := \sum_{i=0}^{d} 2^{2i(d-i)} \cdot x^i$. Note that, f_d satisfies the Kurtz condition (Theorem 3). Thus, assuming Conjecture 1, $S_{\mathbb{R}}(f_d) \geq \Omega(d)$, which further implies $S_{\mathbb{C}}(f_d) \geq \Omega(d)$ (Lemma 10). This implies exponential hardness of VP, by [13, Theorem 6] (with $\varepsilon = 1$); however in this setting, the hardness proof is much *simpler* due to stronger hardness assumption and a classical decomposition (Lemma 1), instead of a convoluted one, *via* ABPs, required in [13] (for general ε).

The overall idea is to convert f_d to an *exponentially hard* multivariate polynomial. Usually, (inverse) Kronecker type substitution is used for univariate to multivariate conversion ([16, 24]); here we *do not* use the Kronecker due to a technical barrier [4]. Instead, we use a *multilinear* map ϕ [13] that sends x^i

[4] Kronecker would give a *naive* bound of $\binom{k+kn/2}{k} > (n+1)^k > d$; which is useless.

to $\phi(x^i) := \prod_{j\in[n],\,\ell\in[0\ldots k-1]} y_{j,\ell}$, where $\ell \cdot k^{j-1}$ contributes to the base$_k(i)$-*representation* in the j-th position; here $n = O(\log d)$ and k is a large constant.

Define, $\phi(f_d) =: P_{n,k}$, by linear extension. By construction, $P_{n,k}$ is a kn-variate degree-n multilinear polynomial. For large constant k, we show that $\text{size}(P_{n,k}) > d^{1/7} = 2^{\Omega(kn)}$. The proof goes via contradiction. If the size is smaller, then using a classical decomposition (Lemma 1), $P_{n,k}$ can be written as sum of $\leq O(d^{1/7}\cdot n^2)$-many Q_i^2's; where the intermediate polynomial Q_i (kn-variate) has degree at most $2n/3$. Thus, a naive upper bound on the support-sum $S_{\mathbb{C}}(f_d)$ is $O(d^{1/7}\cdot n^2 \cdot \binom{kn+2n/3}{2n/3}) = O(d^{6/7}\log^2 d) = o(d)$, a contradiction.

As the coefficients are *easy* to compute, $(P_{n,k})_n \in \mathsf{VNP}$, by Valiant's criterion (Theorem 4). Therefore, the conclusion follows.

1.4 Comparison with prior works

Technically, our SOS-τ-conjecture is incomparable to the earlier τ-conjectures as all of the previous works [16, 24, 26] used the standard depth-reduction results [1, 2, 20, 25], hence, they were concerned with the sum-of unbounded-powers $\sum\prod^m\sum\prod$, with $m = \omega(1)$, while we work with $m = 2$. As mentioned earlier, this is the *first* time we are showing connections to matrix-rigidity and PIT; these were perhaps always desired of, nonetheless *never achieved*.

Moreover, the measure $S(f)$ in the τ-conjecture is different from the usual circuit-size. If we consider the expression in (1) as a $\sum\bigwedge^2\sum\prod$-formula, then the support-sum is the number of $\prod$-operations directly above the input level. However, the usual measure is the size of the depth-4 circuit $\sum^k\prod^m\sum^t\prod$. Even if we substitute $m = 2$, there is *no* direct dependence of t (individual sparsity of the intermediate polynomials f_i) on $S(f)$, which implies that the sparsity of some f_i could be *large*. However, the upper bound requirement in [24] is $\mathsf{poly}(kmt)$ while the SOS-τ-conjecture *demands* a linear (*stronger*) dependence on $S(f)$.

Further, the polynomial family and the proof used in [16, 24] are *different* from those in Theorem 2, as it relies on depth-4 reduction and the usual Kronecker map while our proof relies on multilinearization ([13]) and a folklore decomposition (Lemma 1), see [42, 44, 47]. In [13], a *fine-grained* decomposition (using algebraic branching programs) was used which made the parameters and the hardness proof more intricate; this is *not at all* required in this work.

2 Preliminaries

Basic notation. Let $[n] = \{1,\ldots,n\}$. In general, for $a < b$, $[a,b]$ denotes all integers $a \leq i \leq b$. For $i \in \mathbb{N}$ and $b \geq 2$, we denote by base$_b(i)$ the unique k-tuple $(i_1,\ldots,i_k)$ such that $i = \sum_{j=1}^{k} i_j\, b^{j-1}$. In the special case $b = 2$, we define $\text{bin}(i) := \text{base}_2(i)$. $\mathbb{R}$ denotes the real field while $\mathbb{C}$ denotes the complex field.

For a matrix S, $\text{sp}(S)$, the sparsity of S, is the number of non-zero entries.

Binomial inequality. We use the following standard bound on binomial coefficients for $1 \leq k \leq n$,

$$\binom{n}{k} \leq \left(\frac{en}{k}\right)^k . \tag{2}$$

Polynomials and real roots. For a polynomial $p \in \mathbb{F}[x]$, $\mathrm{supp}(p)$, the *support of* p is the set of nonzero monomials in p. The *sparsity* or *support size of* p is $|p|_0 = |\mathrm{supp}(p)|$. By $\mathrm{coef}(p)$ we denote the *coefficient vector* of p (in some order).

For an exponent vector $\boldsymbol{e} = (e_1, \ldots, e_k)$, $\boldsymbol{x}^{\boldsymbol{e}}$ denotes the monomial $x_1^{e_1} \ldots x_k^{e_k}$.

When are all the roots of a univariate polynomial *real* and *distinct*? Kurtz [28] came up with the following *tight* and *sufficient* condition.

Theorem 3 ([28]). *Let f be a real polynomial of degree $n \geq 2$ with* positive *coefficients. If*

$$a_i^2 > 4a_{i-1}a_{i+1} , \ \forall\, i \in [n-1] ,$$

then all the roots of f are real and distinct.

Primer on Algebraic complexity. The *algebraic circuit complexity* of a polynomial f, denoted by $\mathrm{size}(f)$, is the size of the smallest circuit computing f. A family of n-variate polynomials $(f_n)_n$ over $\mathbb{F}$ is in VNP if there exists a family of polynomials $(g_n)_n$ in VP such that for every $\boldsymbol{x} = (x_1, \ldots, x_n)$ one can write $f_n(\boldsymbol{x}) = \sum_{w \in \{0,1\}^{t(n)}} g_n(\boldsymbol{x}, w)$, for some polynomial $t(n)$ which is called the *witness size.*

VP and VNP have several closure properties. In particular, they are closed under substitution. That is, for a polynomial $f(\boldsymbol{x}, \boldsymbol{y}) \in \mathsf{VP}$ (or VNP), also $f(\boldsymbol{x}, \boldsymbol{y}_0) \in \mathsf{VP}$ (respectively VNP), for any values $\boldsymbol{y}_0$ from $\mathbb{F}$ assigned to the variables in $\boldsymbol{y}$.

The explicitness of the family plays a major role in its usefulness in algebraic complexity.

Definition 3 (Explicit functions). *Let $(f_d)_d$ be a polynomial family, where $f_d(x)$ is of degree d. The family is* explicit*, if its coefficient-function is computable in time $\mathsf{poly}\log(d)$ and each coefficient can be at most $\mathsf{poly}(d)$-bits long. The coefficient-function gets input (j, i, d) and outputs the j-th bit of the coefficient of x^i in f_d.*

Valiant [53] gave a useful *sufficient* condition for the explicitness of a polynomial family $f_n(\boldsymbol{x})$ so that it is in VNP. For a proof, see [10, Proposition 2.20].

Theorem 4 (Valiant's criterion, [53]). *Let function $\phi : \{0,1\}^n \to \{0,1\}^n$ be computable in $\mathsf{P/poly}$. Then, the family of polynomials defined by $f_n(\boldsymbol{x}) := \sum_{\boldsymbol{e} \in \{0,1\}^n} \phi(\boldsymbol{e}) \cdot \boldsymbol{x}^{\boldsymbol{e}}$, is in VNP.*

The following lemma is a classical decomposition lemma using frontiers, for details see [3, 42, 54]. For a proof, see [44, Lemma 5.12] (with frontier $m = d/3$).

Lemma 1 (Sum of product-of-2). *Let $f(\boldsymbol{x})$ be an n-variate, homogeneous, degree d polynomial computed by a homogeneous circuit Φ of size s. Then, there exist polynomials $f_{ij} \in \mathbb{F}[\boldsymbol{x}]$ s.t.*

$$f(\boldsymbol{x}) \;=\; \sum_{i=1}^{s} f_{i1} \cdot f_{i2}\ , \quad \textit{with the following properties:} \tag{3}$$

1) $d/3 \leq \deg(f_{i1}), \deg(f_{i2}) \;\leq\; 2d/3, \forall\, i \in [s]$*, and* **2)** $\deg(f_{i1}) + \deg(f_{i2}) = d, \forall\, i \in [s]$.

Remark. It is well known that each homogeneous part can be computed by a homogeneous circuit of size $O(sd^2)$. Thus, for non-homogeneous polynomials, s can be replaced by $O(sd^2)$.

3 Proof of the main results

In this section, we prove the main theorems, namely Theorem 1-2.

3.1 SOS-τ-conjecture to matrix rigidity: Proof of Theorem 1

We argue via *linear circuits* which we have defined in Section 1. Linear circuits can compute linear functions (see [27, Sec.1.2]). As a graph, the nodes of a linear circuits are either input nodes or addition nodes, and the edges are labeled by scalars. If an edge from u to v is labeled by $c \in \mathbb{F}$, then the output of u is multiplied by c and then given as input to v.

We eventually establish that any matrix $A \in \mathbb{R}^{n\times n}$ which is not (r,s)-rigid, for some r, s, can be computed by a depth-2 circuit of size $2rn+s+n$; see item 1-4 below. This will be crucial in the proof of Theorem 1. We give this bound over any general field $\mathbb{F}$.

1. Let $\boldsymbol{a} = (a_1, \ldots, a_n)$ be a vector. Consider $\boldsymbol{a}$ as a linear function $\mathbb{F}^n \to \mathbb{F}$. It can be computed by a linear circuit of depth 1 with n inputs and one addition-gate as output gate. The edge from the i-th input is labeled by a_i. The size of the circuit is n. However, we omit edges labeled by 0. Hence, the size of the circuit is actually $\mathrm{sp}(\boldsymbol{a}) \leq n$, the sparsity of $\boldsymbol{a}$.
   Similarly, we consider an $n\times n$ matrix A as a linear transformation $\mathbb{F}^n \to \mathbb{F}^n$. For each row vector of A we get a linear circuit as described above. Hence we represent A by circuit of depth 1 with n output gates and size $\mathrm{sp}(A) \leq n^2$.
2. The model gets already interesting for linear circuits of depth 2. Suppose $A = BC$, where B is a $n \times r$ matrix and C is a $r \times n$ matrix. Then we can take the depth-1 circuit for C at the bottom as in item 1 and combine it with the depth-1 circuit for B on top. The resulting depth-2 circuit is *layered*: all edges go either from the bottom to the middle layer, or from the middle to the top layer. The size of the circuit is $\mathrm{sp}(B) + \mathrm{sp}(C) \leq 2rn$.
   In particular, there is a representation $A = BC$ with $r = \mathrm{rank}(A)$. Hence the rank of A is involved in the circuit size bound for A. Also note that r is bounded by the size of the circuit because be omit all zero-edges.

Note that any layered linear circuit of depth 2 in turn gives a factorization of A as a product of 2 matrices, $A = BC$, where the top edges define B and the bottom edges C.

3. Let $A = BC + D$, where B, C are as above and D is a $n \times n$ matrix. Then we can represent A by a depth-2 circuit for BC as in item 2 plus edges from the inputs directly to the output nodes to represent D as in item 1. The resulting circuit has depth 2 and size $\mathrm{sp}(B) + \mathrm{sp}(C) + \mathrm{sp}(D) \leq 2rn + n^2$, but it would not be layered. We can transform it into a layered circuit by writing A as $A = BC + ID$, where I is the $n \times n$ identity matrix. Then we get a depth-2 circuit for ID similar to BC and can combine the two circuits into one. The size increases by $\leq n$ edges for I.
4. Now consider matrix A that is not (r, s)-rigid, for some r, s. Hence, we can write A as $A = R + S$, where $\mathrm{rank}(R) = r$ and $\mathrm{sp}(S) = s$. Then R can be written as as $R = BC$, where B is a $n \times r$ matrix and C is a $r \times n$ matrix. From item 3, we have that $A = BC + S$ has a layered linear circuit of depth 2 of size $\leq 2rn + s + n$.

Proof (Proof of Theorem 1). Consider the polynomial family $f_d := \prod_{i \in [d]}(x - i)$. Let $d =: n^2 - 1$, for some $n \in \mathbb{N}$. Conjecture 1 implies that $S_{\mathbb{R}}(f_d) > \delta' \cdot d$, for some $\delta' > 0$. Note that $\delta' \leq 2$, as $S_{\mathbb{R}}(f_d) \leq 2d + 2$, from the upper bound (see Section 1.1). This δ' will play a crucial role in the proof.

Define the bivariate polynomial $g_n \in \mathbb{R}[x_1, x_2]$ from f_d such that after the Kronecker substitution, $g_n(x, x^n) = f_d$. It is easy to construct g_n from a given d; just convert every x^e, for $e \in [0, d]$ to $x_1^{e_1} \cdot x_2^{e_2}$, where $e =: e_1 + e_2 \cdot n$, and $0 \leq e_i \leq n - 1$. Thus, the individual degree of each x_i in g_n is at most $n - 1$.

Let $g_n(x_1, x_2) = \sum_{1 \leq i,j \leq n} a_{i,j}\, x_1^{i-1} x_2^{j-1}$. By the definition of f_d, $a_{i,j} = \mathrm{coef}_{x^{(i-1)+(j-1)n}}(f_d)$. Define the $n \times n$ matrix $A_n = (a_{i,j})_{1 \leq i,j \leq n}$ and vectors

$$[x_1]_n = \begin{pmatrix} 1 \; x_1 \; \cdots \; x_1^{n-1} \end{pmatrix}\,, \quad [x_2]_n = \begin{pmatrix} 1 \; x_2 \; \cdots \; x_2^{n-1} \end{pmatrix}\,.$$

Thus, $g_n(x_1, x_2) = [x_1]_n A_n [x_2]_n^T$. Further, $a_{i,j}$ is $\mathsf{poly}(n)$-computable implies A_n is $\mathsf{poly}(n)$-explicit. Next we show a lower bound on the linear circuit size of A_n.

Lemma 2. *Conjecture 1 $\implies$ any layered linear circuit of depth 2 that computes A_n, has size $> (\delta'/2) \cdot d$.*

Proof of Lemma 2. Conjecture 1 implies that $S_{\mathbb{R}}(f_d) > \delta' \cdot d$, for some $\delta' > 0$. We show that, size of the linear circuit computing A_n has size $> (\delta'/2) \cdot d$.

Assume that this is false. Then we can write $A_n = BC$, where $B \in \mathbb{R}^{n \times t}$, $C \in \mathbb{R}^{t \times n}$, such that $t \leq \mathrm{sp}(B) + \mathrm{sp}(C) \leq (\delta'/2) \cdot d$.

Denote

$[x_1]_n\, B = \begin{pmatrix} \ell_1(x_1)\, \ell_2(x_1) \cdots l_t(x_1) \end{pmatrix}$ and $C\, [x_2]_n^T = \begin{pmatrix} \tilde{\ell_1}(x_2)\, \tilde{\ell}_2(x_2) \cdots \tilde{\ell}_t(x_2) \end{pmatrix}^T$.

Then

$$g_n(x_1, x_2) = [x_1]_n\, A_n [x_2]_n^T = [x_1]_n\, B\, C [x_2]_n^T = \sum_{i=1}^{t} \ell_i(x_1)\, \tilde{\ell}_i(x_2)\,.$$

Since $\mathrm{sp}(B) + \mathrm{sp}(C) \le (\delta/2) \cdot d$, we have $\sum_{i=1}^{t}(|\ell_i|_0 + |\tilde{\ell}_i|_0) \le (\delta'/2) \cdot d$. Substituting $x_1 = x$ and $x_2 = x^n$, we get

$$f_d(x) \;=\; g(x, x^n) \;=\; \sum_{i=1}^{t} \ell_i(x)\, \tilde{\ell}_i(x^n) \;=\; \sum_{i=1}^{t} \left(\frac{\ell_i(x) + \tilde{\ell}_i(x^n)}{2}\right)^2 - \sum_{i=1}^{t} \left(\frac{\ell_i(x) - \tilde{\ell}_i(x^n)}{2}\right)^2 .$$

Thus, we have a representation of f_d as $\le 2t \le \delta' \cdot d$ sum of squares. Note that, this means

$$S_{\mathbb{R}}(f_d) \le \sum_{i=1}^{t} 2 \cdot \left(|\ell_i|_0 + |\tilde{\ell}_i|_0\right) \le \delta' \cdot d\,, \tag{4}$$

contradicting the assumption on the hardness of f_d. This proves Lemma 2.

We now show that A_n is $((\delta'/8) \cdot n, n^{1+\delta})$-rigid, for any $\delta < 1$. For the sake of contradiction, assume that this is false. Then there is a $\delta < 1$, and a decomposition $A_n = R + S$, where $\mathrm{rank}(R) = r = (\delta'/8) \cdot n$, and $\mathrm{sp}(S) = s = n^{1+\delta}$. By item 4 above, A_n has a layered linear circuit C_n of depth 2 of size

$$\mathrm{size}(C_n) \;\le\; 2rn + s + n \;\le\; \frac{\delta' \cdot n^2}{4} + 2n^{1+\delta}\,. \tag{5}$$

Recall that δ' is a constant and $\delta < 1$. Hence, for large enough n, we have $2n^{1+\delta} \;\le\; \delta' \cdot (\frac{n^2-2}{4})$. Note: $\delta = 1$ is not achievable as $\delta' \le 2$. Now, we can continue the inequalities in (5) by

$$\mathrm{size}(C_n) \;\le\; \delta' \cdot (\frac{n^2-1}{2}) \;=\; (\delta'/2) \cdot d\,. \tag{6}$$

For the last equation, recall that $d = n^2 - 1$. The bound in (6) contradicts Lemma 2. Therefore we conclude that A_n is $(\epsilon \cdot n, n^{1+\delta})$-rigid for any $\delta < 1$, where $\epsilon := \delta'/8$ (remember δ' was fixed at the beginning).

Remark. The same proof holds over $\mathbb{C}$, using Lemma 10.

3.2 SOS-τ-conjecture to exponential hardness: Proof of Theorem 2

Proof. We will construct an explicit (multivariate) polynomial family from the univariate $f_d := \sum_{i=0}^{d} 2^{2i(d-i)} \cdot x^i$, and show that it requires *exponential size* circuit (assuming Conjecture 1). Moreover, we show that the family is in VNP, and the conclusion would directly follow.

Kurtz condition. We show that the coefficients $a_i := 2^{2i(d-i)}$ satisfies the Kurtz condition (Theorem 3). For that, it suffices to check that

$$4\,i\,(d-i) \;>\; 2 \;+\; 2\,(i-1)\,(d-i+1) \;+\; 2\,(i+1)\,(d-i-1)\;,$$

which is true since LHS - RHS=2. Therefore, roots of f_d are all distinct and real.

Construction. We will construct $(P_{n,k})_n$ from f_d, where $P_{n,k}$ is a multilinear degree-n and kn-variate polynomial, where k is a fixed constant (to be fixed in Lemma 4), and $n = O(\log d)$; thus $kn = O(\log d)$.

The basic relation between d, n and k is that $k^n \geq d+1 > (k-1)^n$. Introduce kn many new variables $y_{j,\ell}$, where $1 \leq j \leq n$ and $0 \leq \ell \leq k-1$. Let $\phi_{n,k}$ be the map,

$$\phi_{n,k} \;:\; x^i \;\mapsto\; \prod_{j=1}^{n} y_{j,i_j} \;\text{, where }\; i \;=:\sum_{j=1}^{n} i_j \cdot k^{j-1},\;\; 0 \;\leq\; i_j \;\leq\; k-1 \;.$$

For $i \in [0,d]$, $\phi_{n,k}$ maps x^i uniquely to a multilinear monomial of degree n. By linear extension, define $\phi_{n,k}(f_d) \;=:\; P_{n,k}$. By construction, $P_{n,k}$ is n-degree, kn-variate multilinear polynomial. Let $\psi_{n,k}$ be the homomorphism that maps any degree-n multilinear monomial, defined on variables $y_{j,\ell}$, such that $y_{j,\ell} \mapsto x^{\ell \cdot k^{j-1}}$. Trivially, $\psi_{n,k} \circ \phi_{n,k}(f) = f$, for any degree $\leq d$ polynomial $f \in \mathbb{C}[x]$.

Lemma 3. $(P_{n,k})_n \in \mathsf{VNP}$.

Proof. By construction, $P_{n,k}$ is a kn-variate, individual degree-n multilinear polynomial. Hence,

$$P_{n,k} = \sum_{\boldsymbol{e} \in \{0,1\}^{kn}} \gamma(\boldsymbol{e}) \cdot \boldsymbol{y}^{\boldsymbol{e}} \;.$$

Here, $\boldsymbol{y}$ denotes the kn variables $y_{j,\ell}$ where $1 \leq j \leq n$ and $0 \leq \ell \leq k-1$, and $\boldsymbol{e}$ denotes the exponent-vector. As each x^e in $\operatorname{supp}(f_d)$ maps to a monomial $\boldsymbol{y}^{\boldsymbol{e}}$ *uniquely*; given $\boldsymbol{e}$, one can easily compute $e := \sum_{j=1}^{n} e_j \cdot k^{j-1}$, and thus $\gamma(\boldsymbol{e}) = \operatorname{coef}_{x^e}(f_d) = 2^{2e(d-e)}$. Note that, $\gamma(\boldsymbol{e}) < 2^{d^2}$, for all $\boldsymbol{e}$. We also remark that each bit of $\gamma(\boldsymbol{e})$ is computable in $\mathsf{poly}(\log d) = \mathsf{poly}(kn)$-time.

Write each $\gamma(\boldsymbol{e})$ in binary, i.e. $\gamma(\boldsymbol{e}) =: \sum_{j=0}^{d^2-1} \gamma_j(\boldsymbol{e}) \cdot 2^j$, where $\gamma_j(\boldsymbol{e}) \in \{0,1\}$ is computable in P. As $d^2 - 1 < k^{2n}$, introduce new variables $\boldsymbol{z} = (z_1, \ldots, z_m)$, where $m := 2n \log k = O(n)$ [so that, $d^2 - 1 \leq 2^m - 1$]; and consider the auxiliary polynomial $\tilde{\gamma}(\boldsymbol{e}, \boldsymbol{z}) := \sum_{j \in \{0,1\}^m} \gamma_{\boldsymbol{j}}(\boldsymbol{e}) \cdot \boldsymbol{z}^{\operatorname{bin}(j)}$. Here, we identify $j \in [0, 2^m - 1]$ as a unique $\boldsymbol{j} \in \{0,1\}^m$, via $\operatorname{bin}(j)$,i.e. $\gamma_{\boldsymbol{j}} = \gamma_j$. Let $\boldsymbol{z}_0 \;:=\; (2^{2^0}, \ldots, 2^{2^{m-1}})$. Note that, $\tilde{\gamma}(\boldsymbol{e}, \boldsymbol{z}_0) = \gamma(\boldsymbol{e})$. Finally, consider the $(m+kn)$-variate (where $m + kn = O(n)$) auxiliary polynomial $h_{n,k}(\boldsymbol{y}, \boldsymbol{z})$ as:

$$h_{n,k}(\boldsymbol{y}, \boldsymbol{z}) \;:=\; \sum_{\boldsymbol{e} \in \{0,1\}^{kn}} \tilde{\gamma}(\boldsymbol{e}, \boldsymbol{z}) \cdot \boldsymbol{y}^{\boldsymbol{e}} \;=\; \sum_{\boldsymbol{e} \in \{0,1\}^{kn}} \sum_{\boldsymbol{j} \in \{0,1\}^m} \gamma_{\boldsymbol{j}}(\boldsymbol{e}) \cdot \boldsymbol{z}^{\boldsymbol{j}} \cdot \boldsymbol{y}^{\boldsymbol{e}} \;.$$

Then, we have $h_{n,k}(\boldsymbol{y}, \boldsymbol{z}_0) \;=\; P_{n,k}(\boldsymbol{y})$. Since each bit $\gamma_{\boldsymbol{j}}(\boldsymbol{e})$ is computable in P, thus by Valiant's criterion (Theorem 4), we have $(h_{n,k}(\boldsymbol{y}, \boldsymbol{z}))_n \in \mathsf{VNP}$. As VNP is *closed* under substitution, it follows that $(P_{n,k}(\boldsymbol{y}))_n \in \mathsf{VNP}$.

Next we show that $P_{n,k}$ is exponentially hard assuming Conjecture 1.

Lemma 4. *Conjecture 1 implies $P_{n,k}$ requires exponential-size circuit.*

Proof. We show that over $\mathbb{C}$, size of the minimal circuit computing $P_{n,k}$, namely $\operatorname{size}(P_{n,k}) > d^{1/7} = 2^{\Omega(kn)}$. If not, then apply Lemma 1 to conclude that

$$P_{n,k} \;=\; \sum_{i=1}^{s} c_i \cdot Q_i^2 \;\;\Longrightarrow\;\; f_d \;=\; \sum_{i=1}^{s} c_i \cdot \psi_{n,k}(Q_i)^2 \;,$$

where, $\deg(Q_i) \leq 2n/3$, and $s = O(d^{1/7} \cdot n^2)$. Above equation implies: $S_{\mathbb{C}}(f_d) \leq s \cdot \binom{kn+2n/3}{2n/3}$. We want to show that $S_{\mathbb{C}}(f_d) \leq o(d)$, this will contradict Conjecture 1. This is because the coefficients of f_d satisfies the Kurtz condition implying f_d has all distinct real roots, then Conjecture 1 implies that $S_{\mathbb{R}}(f_d) \geq \Omega(d) \implies S_{\mathbb{C}}(f_d) \geq \Omega(d)$, from Lemma 10.

By assumption, $s \leq O(d^{1/7} \cdot \log^2 d)$. It suffices to show that $\binom{kn+2n/3}{2n/3} \leq d^{5/7}$, so that $S(f_d) \leq O(d^{6/7} \cdot \log^2 d) = o(d)$, the desired contradiction. Use Equation (2) to show the upper bound on the binomial:

$$\binom{kn+2n/3}{2n/3} \leq (e+3ek/2)^{2n/3} \leq (5(k-1))^{2n/3} \leq (k-1)^{5n/7} \leq d^{5/7} .$$

The second inequality holds for $e + 3ek/2, \leq 5(k-1)$; so $k \geq 9$ suffices. For the third inequality to be true, $(k-1)^{5/7} \geq (5(k-1))^{2/3}$ suffices; this holds true for $(k-1)^{1/21} \geq 5^{2/3} \iff k \geq 5^{14}+1$. We also used $d \geq (k-1)^n$ (by assumption).

Both the above Lemma 3-4 imply the desired conclusion.

Remark. As $\deg(Q_i) \leq 2n/3$, we have $\deg(\psi_{n,k}(Q_i)) \leq 2n/3 \cdot (k-1) \cdot k^{n-1} < n.k^n = O(nd) = O(d \log d)$. Thus, it is enough to consider the restricted-degree SOS representation, and prove the conjecture.

4 A $\boldsymbol{\tau}$-conjecture for sum-of-cubes and derandomization

It was shown in [13] that a strong lower bound in the sum-of-cubes model leads to a *complete* derandomization of blackbox-PIT. We say that a univariate polynomial $f(x) \in R[x]$ over a ring R is computed as a *sum-of-cubes* (SOC), if

$$f = \sum_{i=1}^{s} c_i f_i^3 , \tag{7}$$

for some top-fanin s, where $f_i(\boldsymbol{x}) \in R[\boldsymbol{x}]$ and $c_i \in R$.

Definition 4 (Support-union size $U_R(f,s)$, [13]). *The* size *of the representation of f in* (7) *is the size of the* support-union*, namely the number of distinct monomials in the representation, $\left|\bigcup_{i=1}^{s} \mathrm{supp}(f_i)\right|$, where* support $\mathrm{supp}(f_i)$ *denotes the set of monomials with a nonzero coefficient in the polynomial $f_i(\boldsymbol{x})$. The* support-union size *of f with respect to s, denoted $U_R(f,s)$, is defined as the minimal support-union size when f is written as in (7).*

If we consider the expression in (7) as a $\sum \bigwedge^3 \sum \prod$-circuit, then the support-union size is the number of $\prod$-operations directly above the input level (unlike $\sum \bigwedge^2 \sum \prod$-*formula* in Definition (2)).

The two measures– support-union and support-sum –are largely incomparable, since $U(\cdot)$ has the extra argument s.

Here, we remark that for any polynomial f, we have $|f|_0^{1/3} \leq U_{\mathbb{F}}(f,s) \leq |f|_0 + 1$, where the upper bound is for $s \geq 3$, and for fields $R = \mathbb{F}$ of characteristic $\neq 2, 3$. The upper bound follows from the identity: $f = (f+2)^3/24 + (f -$

$2)^3/24 - f^3/12$. Hence, the SOC-model is *complete* for any field of characteristic $\neq 2, 3$. The lower bound can be shown by counting monomials.

It is unclear whether an SOC representation with support-union $= o(d)$ exists for a very small fanin s over $\mathbb{F} = \mathbb{Q}$ [5]. This trade-off between the measure U, and the top-fanin s lead to the definition of hardness in the SOC-model.

Definition 5 (SOC-hardness, [13]). *A* $\mathsf{poly}(d)$*-time explicit univariate polynomial family* $(f_d)_d$ *is* SOC-hard*, if there exists a positive constant* $\varepsilon < 1/2$*, such that* $U_{\mathbb{F}}\left(f_d, d^{\varepsilon}\right) = \Omega(d)$*.*

The existence of an SOC-hard family implies blackbox-PIT $\in \mathsf{P}$ [13, Theorem 11]. Owing the same tenable approach to connect PIT with the number of real roots, we conjecture the following.

Conjecture 2 (SOC-τ-conjecture). Consider any non-zero polynomial $f \in \mathbb{R}[x]$. Then, there exist positive constants $\varepsilon < 1/2$, and c such that the number of distinct real roots of f is at most $c \cdot U_{\mathbb{R}}(f, d^{\varepsilon})$.

Remark. We show that $f = c_1 f_1^3 + c_2 f_2^3$, has at most $O(\text{supp}(f_1) \cup \text{supp}(f_2))$-many real roots (see Theorem 10).

Now, we show a complete derandomization of blackbox-PIT assuming Conjecture 2.

Theorem 5 (Derandomization). *If SOC-τ-conjecture holds, then blackbox-PIT* $\in \mathsf{P}$*.*

Proof sketch. Consider the polynomial family $f_d := \prod_{i \in [d]} (x - i)$. It is trivial to see that $(f_d)_d$ is $\mathsf{poly}(d)$-explicit. Moreover, if the SOC-τ-conjecture is true, then there exists a $\varepsilon < 1/2$, such that $U_{\mathbb{R}}(f_d, d^{\varepsilon}) = \Omega(d)$ implying $(f_d)_d$ is an explicit SOC-hard family. Invoking [13, Theorem 11], the conclusion follows.

5 Lower bound for restricted models

Kumar and Volk [27] showed a strong connection between matrix rigidity and depth-2 linear circuit lower bound. They argued (similarly done in [38] in a different language) that depth-2 $\Omega(n^2)$ lower bound for an explicit matrix is *necessary* and *sufficient* for proving *super*-linear lower bound for general $O(\log n)$-depth circuits (or matrix rigidity).

Symmetric depth-2 circuit. Over $\mathbb{R}$, it is a circuit of the form $B^T \cdot B$, for some $B \in \mathbb{R}^{m \times n}$. [Over $\mathbb{C}$, one should take the conjugate-transpose B^* instead of B^T.] Symmetric circuits are a natural computational model for computing a positive semi-definite (*PSD*) matrix.

[5] For large $s = \Omega(d^{1/2})$, $U_{\mathbb{C}}(f, s)$ is small [13, Corollary 10].

Invertible depth-2 circuit. It is a circuit $B \cdot C$, where at least one of the matrices B, C is invertible. We stress that invertible circuits can compute non-invertible matrices. Invertible circuits generalize many of the common matrix decompositions, such as QR decomposition, eigen decomposition, singular value decomposition (SVD), and LUP decomposition.

[27, Thms.1.3 & 1.5] prove asymptotically optimal lower bounds for both the models.

Theorem 6. [27] *There exists an explicit family of real $n \times n$ PSD matrices $(A_n)_{n\in\mathbb{N}}$ such that every symmetric circuit (respectively invertible circuits) computing A_n (over $\mathbb{R}$) has size $\Omega(n^2)$.*

We present a simple, *alternative* proof of Theorem 6 using lower bounds on the SOS representation (with restriction) of two different explicit families f_d over $\mathbb{R}$. For details, see Theorems 7, and 8, in Section 5.

Before going into details, we state a classical lemma due to Descartes which will be used throughout the paper.

Lemma 5 (Descartes' rule of signs). *Let $p(x) \in \mathbb{R}[x]$ be a polynomial with t many monomials. Then, number of distinct positive roots in $p(x)$ can be at most $t - 1$.*

Remark. An s-sparse polynomial $f \in \mathbb{C}[x]$ can have at most $2(s-1)$-many real roots. A real root a of f must be a real root of both the real part $\Re(f)$ and the imaginary part $\Im(f)$. By above, there can be at most $s-1$ many positive roots. The same bound holds for negative roots by $x \mapsto -x$.

5.1 Lower bound for symmetric circuits over $\mathbb{R}$: Proof of the first part of Theorem 6

We state a lemma from classical mathematics for the study of fewnomials and give a simple proof. This would be critical to prove explicit lower bounds.

Lemma 6 (Hajós Lemma). *Suppose $f(x) \in \mathbb{C}[x]$ be a univariate polynomial with $t \geq 1$ monomials. Let α be a non-zero root of $f(x)$. Then, the multiplicity of α in f can be at most $t - 1$.*

Proof. We will prove this by induction on t. When $t = 1$, $f(x) = a_m x^m$ for some m. It has no non-zero roots and we are trivially done. Assume that, it is true upto t. We want to prove the claim for $t + 1$.

Suppose $|f|_0 = t + 1$. There exists $m \geq 0$ such that $f(x) = x^m.g(x)$, with $|g|_0 = t + 1$ and $g(0) \neq 0$. It suffices to prove the claim for g. Let, α be a non-zero root of $g(x)$. Suppose, $g(x) = (x - \alpha)^s \cdot h(x)$, for some $s \geq 1$ and $h(\alpha) \neq 0$. Observe that, multiplicity of α in g' is $s - 1$. As $g(0) \neq 0$, $|g'|_0 = t$. Therefore by induction hypothesis, $s - 1 \leq t - 1 \implies s \leq t$. Hence, multiplicity of α in g (thus in f) can be at most t. This finishes the induction step.

Corollary 1. *Suppose $f(x) = (x+\alpha)^t \cdot g(x)$, for some non-zero α and $g(\cdot)$, then we must have $|f|_0 \geq t+1$.*

We prove an important lower bound on SOS representation for a non-zero multiple of $(x+1)^d$; it will be important to prove the first part of Theorem 6.

Lemma 7. *Let $f(x)$ be a non-zero polynomial in $\mathbb{R}[x]$. Suppose, there exist non-zero $\ell_i \in \mathbb{R}[x]$, for $i \in [m]$ such that $(x+1)^d \cdot f(x) = \sum_{i=1}^m \ell_i^2$. Then, $\sum_{i \in [m]} |\ell_i|_0 \geq m \cdot (\lfloor d/2 \rfloor + 1)$.*

Proof. Denote $g(x) := \gcd(\ell_1, \ldots, \ell_m)$. We will prove that $(x+1)^t \mid g(x)$ where $t := \lfloor d/2 \rfloor$. Suppose not, assume that $(x+1)^k || g(x)$ (i.e $(x+1)^{k+1} \nmid g(x)$) such that $k < t$ (and thus $d - 2k > 0$). Then, $g(x) = h(x) \cdot (x+1)^k$ where $h(x) \in \mathbb{R}[x]$ with $h(-1) \neq 0$. Define $\tilde{\ell}_i := \ell_i/(x+1)^k$. By assumption, $(x+1) \nmid \gcd(\tilde{\ell}_1, \ldots, \tilde{\ell}_m) =: h(x)$. Thus,

$$\begin{aligned}
\sum_{i=1}^{k} \ell_i(x)^2 \;=\; (x+1)^d \cdot f(x) &\implies \sum_{i=1}^{m} \tilde{\ell}_i(x)^2 \;=\; (x+1)^{d-2k} \cdot f(x) \\
&\implies \sum_{i=1}^{m} \tilde{\ell}_i(-1)^2 \;=\; 0 \\
&\implies \tilde{\ell}_i(-1) \;=\; 0 \;, \qquad \forall i \in [1, m] \\
&\implies (x+1) \mid \tilde{\ell}_i(x) \;, \qquad \forall i \in [1, m] \\
&\implies (x+1) \mid \gcd(\tilde{\ell}_1, \ldots, \tilde{\ell}_m) = h(x)
\end{aligned}$$

which is a contradiction. Thus, $k \geq t$.

This implies, each ℓ_i is non-zero polynomial multiple of $(x+1)^t$. Since Corollary 1 implies that $|\ell_i|_0 \geq t+1$, for all $i \in [m]$; the lemma follows.

Recall that a *symmetric* depth-2 circuit (over $\mathbb{R}$) is a circuit of the form $B^T \cdot B$ for some $B \in \mathbb{R}^{m \times n}$. We prove the *first* part of Theorem 6.

Theorem 7 (Reproving Theorem 1.3 of [27]). *There exists an explicit family of real $n \times n$ PSD matrices $\{A_n\}_{n \in \mathbb{N}}$ such that every symmetric circuit computing A_n (over $\mathbb{R}$) has size $\Omega(n^2)$.*

Proof. Denote $[x]_n := \begin{bmatrix} 1 \; x \; \ldots \; x^{n-1} \end{bmatrix}$. Denote $k := \lfloor n/2 \rfloor$. Define $g_i(x) := (x+1)^k \cdot x^{\lfloor (i-1)/2 \rfloor}$, for $i \in [n]$. Note that, $\deg(g_i) = k + \lfloor (i-1)/2 \rfloor \leq k + \lfloor (n-1)/2 \rfloor = n-1$. Define $n \times n$ matrix M_n such that

$$M_n \cdot [x]_n^T \;:=\; \begin{bmatrix} g_1(x) \\ g_2(x) \\ \vdots \\ g_n(x) \end{bmatrix} .$$

It is easy to see that $g_1, g_3, g_5, \ldots$ are linearly independent over $\mathbb{R}$. Therefore, $\text{rank}(M_n) = \text{rank}_{\mathbb{R}}(g_1(x), \ldots, g_n(x)) = \lfloor (n-1)/2 \rfloor + 1 = \lfloor (n+1)/2 \rfloor$.

Define $A_n := M_n^T \cdot M_n$. By definition, A_n is PSD and $\text{rank}(A_n) = \lfloor (n+1)/2 \rfloor$. This follows from the classical fact that for any matrix A over $\mathbb{R}$, $\text{rank}(A^T A) =$

rank(A). Also A_n is *explicit* (entries are P-computable from definition). Now, assume there is some $m \times n$ matrix B such that $A_n = B^T \cdot B$. Then, denote $B[x]_n := \left[\ell_1\ \ell_2\ \ldots\ \ell_m\right]^T$, where $\ell_i \in \mathbb{R}[x]$ are univariate polynomials of degree at most $n-1$. Observe that number of *non-zero* entries in B is precisely $\sum_{i\in[m]} |\ell_i|_0$. Thus, it suffices to show that $\sum_{i\in[m]} |\ell_i|_0 \geq \Omega(n^2)$.

As rank(B) = rank(B^TB) = rank$(A_n) = \lfloor (n+1)/2 \rfloor$, we must have $m \geq \lfloor (n+1)/2 \rfloor$. Thus,

$$\begin{aligned} A_n \ = \ B^T \cdot B \implies & [x]_n M_n^T \cdot M_n [x]_n^T \ = \ [x]_n B^T \cdot B[x]_n^T \\ \iff & \sum_{i=1}^{n} g_i(x)^2 \ = \ \sum_{i=1}^{m} \ell_i^2 \\ \iff & (x+1)^{2k} \cdot f(x) \ = \ \sum_{i=1}^{m} \ell_i^2 \qquad , \text{ where } f(x) \ := \ \sum_{i=1}^{n} x^{2\cdot\lfloor (i-1)/2 \rfloor} \\ \implies & \sum_{i=1}^{m} |\ell_i|_0 \ \geq \ (\lfloor (n+1)/2 \rfloor) \cdot (k+1) \ \geq \ \frac{n^2}{4} \qquad \text{by Lemma 7.} \end{aligned}$$

5.2 Lower bound for invertible circuits over $\mathbb{R}$: Proof of the second part of Theorem 6

This subsection is devoted to proving the *second* part of Theorem 6. This proof uses SOS lower bound for a bivariate polynomial. Investigating sum of product of two polynomials is similar to looking at the SOS; as, one can write $f \cdot g = ((f+g)/2)^2 - ((f-g)/2)^2$. The summand fan-in at most doubles. Thus, proving lower bound for sum of product of two polynomials is 'same' as proving SOS lower bound. The following lemma proves certain lower bound on sum of sparsity when a specific *bivariate* polynomial is written as sum of product of two polynomials (with certain restrictions).

Lemma 8. *Let $f_d := f_{d,t}(x,y) := \left(\prod_{i\in[d]}(x-i)(y-i)\right) \cdot p(x,y)$, for some polynomial $p \in \mathbb{R}[x,y]$ such that $deg_x(p) = deg_y(p) = t$. Suppose, $f_d = \sum_{i\in[d+t+1]} \ell_i(x) \cdot \tilde{\ell}_i(y)$, where $\ell_i, \tilde{\ell}_i$'s are polynomials of degree at most $d+t$; with the additional property that $\tilde{\ell}_1, \ldots, \tilde{\ell}_{d+t+1}$ are $\mathbb{R}$-linearly independent.*

Then, $\sum_{i=1}^{d+t+1} |\ell_i|_0 \ \geq \ m \cdot (d+1)$, where m is the number of non-zero ℓ_i.

Proof. Suppose, $g(x) := \gcd(\ell_1, \ldots, \ell_{d+t+1})$. We claim that $\prod_{i=1}^{d}(x-i) \mid g(x)$. Note that, it suffices to prove the claim; as, $\prod_{i=1}^{d}(x-i) \mid \ell_i(x)$ for each non-zero ℓ_i implies $|\ell_i|_0 \geq d+1$ by Lemma 5.

We prove the claim by contradiction. Suppose, there exists $j \in [d]$ such that $x - j \nmid g(x)$, so $g(j) \neq 0$. Fix this j. Hence, there exists i such that $\ell_i(j) \neq 0$.

In particular, $\boldsymbol{v} := \left[\ell_1(j)\ \ell_2(j)\ \ldots\ \ell_{d+t+1}(j)\right]^T \neq \mathbf{0}$. Define the $(d+t+1) \times (d+t+1)$ matrix A as

$$[y]_{d+t+1} \cdot A \ := \ \left[\tilde{\ell}_1\ \tilde{\ell}_2\ \ldots\ \tilde{\ell}_{d+t+1}\right] \ , \text{ where } [y]_{d+t+1} \ := \ \left[1\ y\ \ldots\ y^{d+t}\right] \ .$$

Observe: $\mathrm{rank}_{\mathbb{R}}(\tilde{\ell}_1, \ldots, \tilde{\ell}_{d+t+1}) = d + t + 1 \iff A$ is invertible. But,

$$\begin{aligned} \boldsymbol{v} \neq \mathbf{0} \text{ and } A \text{ is invertible } &\implies A \cdot \boldsymbol{v} \;\neq\; \mathbf{0} \\ &\implies [y]_{d+t+1} \cdot A\boldsymbol{v} \;\neq\; 0 \\ &\implies \sum_{i=1}^{d+t+1} \tilde{\ell}_i(y) \cdot \ell_i(j) \;\neq\; 0 \\ &\implies f_{d,t}(j, y) \;\neq\; 0 \end{aligned}$$

which is a contradiction! Therefore, $\prod_{i=1}^{d}(x - i) \mid g(x)$ and so we are done.

Recall that an *invertible* depth-2 circuit computes a matrix A such that whenever $A = BC$, either B or C has to be invertible. We prove the *second* part of Theorem 6.

Theorem 8 (Reproving Theorem 1.5 of [27]). *There exists an explicit family of $n \times n$ PSD matrices $\{A_n\}_{n\in\mathbb{N}}$ such that every invertible circuit over $\mathbb{R}$ computing A_n has size $\Omega(n^2)$.*

Proof. Denote $k := \lfloor n/2 \rfloor$. Define $g_i(x) := \prod_{i=1}^{k}(x - i) \cdot x^{\lfloor (i-1)/2 \rfloor}$, for $i \in [n]$. Note that $\deg(g_i) = k + \lfloor (i - 1)/2 \rfloor \le k + \lfloor (n - 1)/2 \rfloor = n - 1$. Define the $n \times n$ matrix M_n as

$$M_n \cdot [x]_n^T \;:=\; \begin{bmatrix} g_1(x) \\ g_2(x) \\ \vdots \\ g_n(x) \end{bmatrix} .$$

It is easy to see that $g_1, g_3, g_5, \ldots$ are linearly independent over $\mathbb{R}$. Therefore, $\mathrm{rank}(M_n) = \mathrm{rank}_{\mathbb{R}}\,(g_1(x), \ldots, g_n(x)) = \lfloor (n - 1)/2 \rfloor + 1 = \lfloor (n + 1)/2 \rfloor$.

Define $A_n := M_n^T \cdot M_n$. By definition, A_n is PSD and $\mathrm{rank}(A_n) = \lfloor (n+1)/2 \rfloor$. This follows from the classical fact that for any matrix A, $\mathrm{rank}(A^T A) = \mathrm{rank}(A)$ over $\mathbb{R}$. Also A_n is *explicit* (entries are P-computable from definition).

Suppose, there exists $n \times n$ invertible matrix B and some $n \times n$ matrix C such that $A_n = B \cdot C$ (the other case where C is invertible is similar). Note that, from classical property of rank of matrices, $\mathrm{rank}(C) \ge \mathrm{rank}(A_n) = \lfloor (n + 1)/2 \rfloor$. With the usual notation of $[x]_n$ and $[y]_n$ used before, denote

$$[y]_n \cdot B \;:=\; \left[\tilde{\ell}_1(y)\; \tilde{\ell}_2(y) \ldots \tilde{\ell}_n(y)\,\right] \text{ and } C \cdot [x]_n^T \;:=\; \left[\ell_1(x)\; \ell_2(x) \ldots \ell_n(x)\right]^T .$$

Note that the degree of each $\ell_i, \tilde{\ell}_i$ can be at most $n - 1$. Thus,

$$\begin{aligned} A_n = B \cdot C \implies [y]_n M_n^T \cdot M_n [x]_n^T \;&=\; [y]_n \cdot B \cdot C \cdot [x]_n^T \\ \iff \sum_{i=1}^{n} g_i(x) \cdot g_i(y) \;&=\; \sum_{i=1}^{n} \ell_i(x) \cdot \tilde{\ell}_i(y) \\ \iff \left(\prod_{i=1}^{k}(x - i)(y - i)\right) \cdot p(x, y) \;&=\; \sum_{i=1}^{n} \ell_i(x) \cdot \tilde{\ell}_i(y) \end{aligned}$$

where $p(x, y) := \sum_{i\in[n]} (xy)^{\lfloor (i-1)/2 \rfloor}$. The LHS is actually of the form $f_{k,\lfloor (n-1)/2 \rfloor}(x, y)$ as in Lemma 8. From the lower bound on rank of C, we know that there must be at least $\lfloor (n+1)/2 \rfloor$ many non-zero ℓ_i's. Therefore, Lemma 8 gives us $\sum_{i=1}^{n} |\ell_i|_0 \;\geq\; \lfloor (n+1)/2 \rfloor \cdot (k+1) \;\geq\; n^2/4$.

Remark. The defined matrix A_n in the above proof *also* works for the theorem 7. For that, one needs to replace the polynomial $\prod_{i=1}^{d}(x-i)\cdot f(x)$, in theorem 7, and prove similar lower bound on sum of sparsity. The proof details of theorem remains *almost* unchanged until at the very end, one has to use Descartes' rule (lemma 5) instead of Lemma 1.

6 τ-conjectures for top-fanin 2 hold true

In this section we show that both SOS-τ-conjecture and SOC-τ-conjecture hold true for top fanin-2.

6.1 SOS-τ-conjecture for sum of two squares

We show that when f is a sum of two squares, number of real roots is indeed linear in the support-sum.

Theorem 9. *If $f = \sum_{i=1}^{s} c_i \cdot f_i^2 \in \mathbb{R}[x]$, where $s \leq 2$, then f can have at most $O(\sum_{i=1}^{s} |f_i|_0)$-many real roots.*

Proof. There are two cases to consider:

Case I ($s = 1$): In this case, $f = c_1 \cdot f_1^2$. Thus, the real roots of f are precisely the roots of f_1. However, by Descartes' rule (Lemma 5), f_1 can have at most $2(|f_1|_0 - 1)$-many real roots.

Case II ($s = 2$): Without loss of generality, assume that c_1 and c_2 are of opposite signs ; otherwise, any real root of f must also be roots of f_1 and f_2, and trivially we are done by Lemma 5. When, the signs are opposite, note that, f has the following factoring over $\mathbb{R}[x]$:

$$f \;=\; c_1 \cdot (f_1 + \gamma \cdot f_2) \cdot (f_1 - \gamma \cdot f_2) \;,\; \text{where } \gamma \;:=\; \sqrt{-c_2/c_1} \in \mathbb{R} \;.$$

It directly follows that $|f_1 \pm \gamma \cdot f_2|_0 \;\leq\; |f_1|_0 + |\gamma \cdot f_2|_0 \;=\; |f_1|_0 + |f_2|_0$. However, the real roots of f must also be real roots of $f_1 \pm \gamma \cdot f_2$. Each $f_1 \pm \gamma \cdot f_2$ can have at most $2(|f_1|_0 + |f_2|_0) - 2$ many real roots, by Descartes' rule (Lemma 5). Therefore, the conclusion follows.

Remark. We could strengthen the above theorem by replacing $O(|\bigcup_{i\in[2]} \mathrm{supp}(f_i)|)$. Since, $|\mathrm{supp}(f_1 \pm \gamma \cdot f_2)| \leq |\mathrm{supp}(f_1) \bigcup \mathrm{supp}(f_2)|$, using Lemma 5, the conclusion follows.

6.2 SOC-τ-conjecture for sum of two cubes

We show that when f is a sum of two squares, number of real roots is indeed linear in the support-union.

Theorem 10. *If $f = \sum_{i=1}^{s} c_i \cdot f_i^3 \in \mathbb{R}[x]$ where $s \leq 2$, then f can have at most $O(|\bigcup_{i=1}^{s} \operatorname{supp}(f_i)|)$-many real roots.*

Proof. There are two cases to consider:

Case I ($s = 1$): In this case, $f = c_1 \cdot f_1^3$. Thus, the real roots of f are precisely the roots of f_1. However, by Descartes' rule (Lemma 5), f_1 can have at most $2(|f_1|_0 - 1)$-many real roots.

Case II ($s = 2$): Note that, f has the following factoring over $\mathbb{R}[x]$:

$$f \ = \ c_1 \cdot (f_1 + \gamma \cdot f_2) \cdot (f_1^2 - \gamma \cdot f_1 f_2 + \gamma^2 \cdot f_2^2) \ , \text{ where } \gamma \ := \ \sqrt[3]{c_2/c_1} \in \mathbb{R} \ .$$

However,

$$f_1^2 - \gamma \cdot f_1 f_2 + \gamma^2 \cdot f_2^2 \ = \ (f_1 - \frac{\gamma}{2} \cdot f_2)^2 + (\frac{3\gamma^2}{4}) \cdot f_2^2 \ ,$$

which has $O(|\bigcup_{i=1}^{2} \operatorname{supp}(f_i)|)$-many real roots by Theorem 9 (and its remark). Also $f_1 + \gamma \cdot f_2$ has at most $O(|\bigcup_{i=1}^{2} \operatorname{supp}(f_i)|)$-many real roots by Descartes' rule (Lemma 5). Moreover, any real root of f must also be real roots of either $f_1 + \gamma \cdot f_2$ or $f_1^2 - \gamma \cdot f_1 f_2 + \gamma^2 \cdot f_2^2$. Therefore, the conclusion follows.

7 SOS-τ-conjecture to SOS lower bound on $(x + 1)^d$

Lemma 9. *If Conjecture 1 is true, then $S_{\mathbb{C}}(f_d) \geq \Omega(d)$, where $f_d := (x + a)^d$, for any $0 \neq a \in \mathbb{R}$.*

Before proving the above, we establish an interesting lemma. For $f \in \mathbb{C}[x]$, we denote $\Re(f)$ as the real part of f, and $\Im(f)$ as the imaginary part, i.e. $f = \Re(f) + \iota \cdot \Im(f)$. Note, $|\Re(f)|_0, |\Im(f)|_0 \leq |f|_0$.

Lemma 10. *$S_{\mathbb{R}}(\Re(f)) \leq 2 \cdot S_{\mathbb{C}}(f)$, for any $f \in \mathbb{C}[x]$.*

Proof. Suppose, $f(x) = \sum_{i=1}^{s} f_i^2$, for $f_i \in \mathbb{C}[x]$ is a *minimal* representation in SOS-model over $\mathbb{C}$ (we ignore the constants c_i as in Equation (1) as $\sqrt{c_i}$ can be taken inside), i.e. $S_{\mathbb{C}}(f) = \sum_{i=1}^{s} |f_i|_0$. Note that

$$\begin{aligned} \Re(f) \ &= \ \sum_{i=1}^{s} \Re(f_i^2) \ = \ \sum_{i=1}^{s} \Re(\Re(f_i) \ + \ \iota \cdot \Im(f_i))^2 \\ &= \ \sum_{i=1}^{s} (\Re(f_i)^2 - \Im(f_i)^2) \ . \end{aligned}$$

The last expression implies that

$$S_{\mathbb{R}}(\Re(f)) \ \leq \ \sum_{i=1}^{s} |\Re(f_i)|_0 + \sum_{i=1}^{s} |\Im(f_i)|_0 \ \leq \ \sum_{i=1}^{s} 2|f_i|_0 \ = \ 2 \cdot S_{\mathbb{C}}(f) \ .$$

Proof of Lemma 9. It suffices to prove the bound for $f_d = (x + 1)^d$, as $S_{\mathbb{C}}((x + a)^d) = S_{\mathbb{C}}((x + 1)^d)$ [just by replacing $x \mapsto x/a$]. Consider the complex polynomial $g_d(x) := f_d(\iota x) + f_d(-\iota x)$. Its degree is either d, if d is even, or $d - 1$, if it is odd. The roots are of the form

$$\iota \cdot \frac{1 - \zeta}{1 + \zeta} \ ,$$

where ζ is d-th root of -1 ($\zeta \neq 1$). There are again either d or $d-1$ such roots, depending on the parity of d. Further, they are all *distinct*. Since $|\zeta| = 1$, each root

$$\iota \cdot \frac{1-\zeta}{1+\zeta} \;=\; \iota \cdot \frac{(1-\zeta)(1+\overline{\zeta})}{(1+\zeta)(1+\overline{\zeta})} \;=\; \iota \cdot \frac{\overline{\zeta}-\zeta}{|1+\zeta|^2} \;=\; \frac{2\Im(\zeta)}{|1+\zeta|^2}$$

is real. Therefore, $g_d(x)$ must be a real polynomial with *distinct real* roots. Hence Conjecture 1 implies that $S_{\mathbb{R}}(g_d) = \Omega(d)$. Using Lemma 10, one can directly conclude that $S_{\mathbb{C}}(g_d) = \Omega(d)$. It is straightforward to see that $S_{\mathbb{C}}(f)$ remains unchanged under the map $x \mapsto c \cdot x$, for any $c \neq 0$. Therefore, in particular, $S_{\mathbb{C}}(f_d(\iota x)) = S_{\mathbb{C}}(f_d(-\iota x)) = S_{\mathbb{C}}(f_d)$. Finally, we must have

$$\Omega(d) \;=\; S_{\mathbb{C}}(g_d) \;\leq\; S_{\mathbb{C}}(f_d(\iota x)) \;+\; S_{\mathbb{C}}(f_d(-\iota x)) \;=\; 2 \cdot S_{\mathbb{C}}(f_d)\;.$$

Hence, the conclusion follows.

8 Conclusion

This work effectively establishes that studying the number of real roots of univariate polynomials for sum-of-squares representation (respectively cubes) is fecund. In fact, proving a strong upper bound suffices to solve three major open problems in algebraic complexity.

Here are some immediate questions of interest which require rigorous investigation.

1. Does SOS-τ-conjecture solve PIT completely? The current proof technique fails to reduce from cubes to squares.
2. Prove the upper bound on the number of real roots for the *sum of constantly* many squares. Currently we only know it for $s = 2$ (Theorem 9).
3. Does SOC-τ-conjecture hold for a 'generic' polynomial f (over $\mathbb{Q}$)?
4. Can we *weaken* the requirement on the upper bound for matrix rigidity (Theorem 1)?

Acknowledgments. A part of this work was done when the author was a visiting scholar at IIT Kanpur. The author thanks Prof. Nitin Saxena and Prof. Thomas Thierauf for the initial discussions and encouragement to write the draft. The author is supported by Google Ph.D. Fellowship. The author would also like to thank Pranav Bisht, Bhargav CS and the anonymous reviewers for their important feedback.

References

1. Agrawal, M., Ghosh, S., Saxena, N.: Bootstrapping variables in algebraic circuits. Proceedings of the National Academy of Sciences **116**(17), 8107–8118 (2019). https://doi.org/10.1073/pnas.1901272116, earlier in Symposium on Theory of Computing, 2018 (STOC'18) 3, 7

2. Agrawal, M., Vinay, V.: Arithmetic Circuits: A Chasm at Depth Four. In: Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on. pp. 67–75. IEEE (2008) 2, 7
3. Allender, E., Jiao, J., Mahajan, M., Vinay, V.: Non-Commutative Arithmetic Circuits: Depth Reduction and Size Lower Bounds. Theoretical Computer Science **209**(1-2), 47–86 (1998). https://doi.org/10.1016/S0304-3975(97)00227-2, `https://doi.org/10.1016/S0304-3975(97)00227-2` 8
4. Alman, J., Chen, L.: Efficient construction of rigid matrices using an NP oracle. In: 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS). pp. 1034–1055. IEEE (2019) 3
5. Alon, N., Pudlak, P.: Superconcentrators of depths 2 and 3; odd levels help (rarely). Journal of Computer and System Sciences **48**(1), 194–202 (1994) 3
6. Blum, L., Cucker, F., Shub, M., Smale, S.: Algebraic settings for the problem "P$\neq$ NP?". In: The Collected Papers of Stephen Smale: Volume 3, pp. 1540–1559. World Scientific (2000) 2
7. Blum, L., Shub, M., Smale, S.: On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. Bulletin (New Series) of the American Mathematical Society **21**(1), 1–46 (1989) 2
8. Briquel, I., Bürgisser, P.: The real tau-conjecture is true on average. Random Structures & Algorithms (2020) 4
9. Bürgisser, P.: On Defining Integers and Proving Arithmetic Circuit Lower Bounds. Computational Complexity **18**(1), 81–103 (2009) 2
10. Bürgisser, P.: Completeness and Reduction in Algebraic Complexity Theory, vol. 7. Springer Science & Business Media (2013) 8
11. Bürgisser, P., Clausen, M., Shokrollahi, A.: Algebraic Complexity Theory, vol. 315. Springer Science & Business Media (2013) 2
12. Demillo, R.A., Lipton, R.J.: A probabilistic remark on algebraic program testing. Information Processing Letters **7**(4), 193 – 195 (1978) 3
13. Dutta, P., Saxena, N., Thierauf, T.: A Largish Sum-of-Squares Implies Circuit Hardness and Derandomization. 12th Innovations in Theoretical Computer Science (ITCS) (2021) 4, 5, 6, 7, 13, 14
14. Dvir, Z., Golovnev, A., Weinstein, O.: Static data structure lower bounds imply rigidity. In: Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing. pp. 967–978 (2019) 3
15. Friedman, J.: A note on matrix rigidity. Combinatorica **13**(2), 235–239 (1993) 3
16. Garcia-Marco, I., Koiran, P., Tavenas, S.: Log-concavity and lower bounds for arithmetic circuits. In: International Symposium on Mathematical Foundations of Computer Science. pp. 361–371. Springer (2015) 2, 5, 6, 7
17. Grigoriev, D.Y.: Using the notions of seperability and independence for proving the lower bounds on the circuit complexity. notes of the leningrad branch of the steklov mathematical institute (1976) 3
18. Grochow, J.A.: Unifying known lower bounds via geometric complexity theory. Computational Complexity **24**(2), 393–475 (2015) 3
19. Guo, Z., Kumar, M., Saptharishi, R., Solomon, N.: Derandomization from Algebraic Hardness: Treading the Borders. In: 60th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2019. pp. 147–157 (2019). https://doi.org/10.1109/FOCS.2019.00018, `https://doi.org/10.1109/FOCS.2019.00018`, online version: https://mrinalkr. bitbucket. io/papers/newprg. pdf 3

20. Gupta, A., Kamath, P., Kayal, N., Saptharishi, R.: Arithmetic circuits: A chasm at depth three. In: 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. pp. 578–587. IEEE (2013) 7
21. Hrubes, P.: On the Real τ-Conjecture and the Distribution of Complex Roots. Theory of Computing **9**(1), 403–411 (2013) 4
22. Hrubes, P.: On the distribution of runners on a circle. Eur. J. Comb. **89**, 103137 (2020). https://doi.org/10.1016/j.ejc.2020.103137, `https://doi.org/10.1016/j.ejc.2020.103137` 4
23. Kabanets, V., Impagliazzo, R.: Derandomizing polynomial identity tests means proving circuit lower bounds. Computational Complexity **13**(1-2), 1–46 (2004) 3, 5
24. Koiran, P.: Shallow circuits with high-powered inputs. In: Innovations in Computer Science - ICS (2011) 2, 6, 7
25. Koiran, P.: Arithmetic circuits: The chasm at depth four gets wider. Theoretical Computer Science **448**, 56–65 (2012) 2, 7
26. Koiran, P., Portier, N., Tavenas, S., Thomassé, S.: A τ-Conjecture for Newton Polygons. Foundations of computational mathematics **15**(1), 185–197 (2015) 6, 7
27. Kumar, M., Volk, B.L.: Lower Bounds for Matrix Factorization. In Proceedings of the 35th Computational Complexity Conference (CCC) (2020) 9, 14, 15, 16, 18
28. Kurtz, D.C.: A sufficient condition for all the roots of a polynomial to be real. The american mathematical monthly **99**(3), 259–263 (1992) 8
29. Lasserre, J.B.: A sum of squares approximation of nonnegative polynomials. SIAM review **49**(4), 651–669 (2007) 4
30. Laurent, M.: Sums of squares, moment matrices and optimization over polynomials. In: Emerging applications of algebraic geometry, pp. 157–270. Springer (2009) 4
31. Mahajan, M.: Algebraic Complexity Classes. In: Perspectives in Computational Complexity, pp. 51–75. Springer (2014) 2
32. Mulmuley, K.: Geometric complexity theory V: Efficient algorithms for Noether normalization. Journal of the American Mathematical Society **30**(1), 225–309 (2017) 3
33. Mulmuley, K.D.: Geometric Complexity Theory V: Equivalence between Blackbox Derandomization of Polynomial Identity Testing and Derandomization of Noether's Normalization Lemma. In: FOCS. pp. 629–638 (2012) 3
34. Nisan, N., Wigderson, A.: Hardness vs randomness. Journal of computer and System Sciences **49**(2), 149–167 (1994) 3
35. Ore, O.: Über höhere kongruenzen. Norsk Mat. Forenings Skrifter **1**(7), 15 (1922) 3
36. Pfister, A.: Hilbert's seventeenth problem and related problems on definite forms. In: Mathematical Developments Arising from Hilbert Problems, Proc. Sympos. Pure Math, XXVIII.2.AMS. vol. 28, pp. 483–489 (1976) 4
37. Pippenger, N.: Superconcentrators. SIAM Journal on Computing **6**(2), 298–304 (1977) 3
38. Pudlak, P.: Communication in bounded depth circuits. Combinatorica **14**(2), 203–216 (1994) 3, 14
39. Radhakrishnan, J., Ta-Shma, A.: Bounds for dispersers, extractors, and depth-two superconcentrators. SIAM Journal on Discrete Mathematics **13**(1), 2–24 (2000) 3
40. Ramanujan, S.: On the Expression of a Number in the Form axˆ 2+ byˆ 2+ czˆ 2+ duˆ 2. In: Proc. Cambridge Philos. Soc. vol. 19, pp. 11–21 (1917) 4
41. Ramya, C.: Recent progress on matrix rigidity–a survey. arXiv preprint arXiv:2009.09460 (2020) 3

42. Raz, R.: Elusive Functions and Lower Bounds for Arithmetic Circuits. Theory Comput. **6**(1), 135–177 (2010). https://doi.org/10.4086/toc.2010.v006a007, `https://doi.org/10.4086/toc.2010.v006a007` 7, 8
43. Reznick, B.: Extremal PSD forms with few terms. Duke mathematical journal **45**(2), 363–374 (1978) 4
44. Saptharishi, R.: A survey of lower bounds in arithmetic circuit complexity. Github survey (2019) 7, 8
45. Schwartz, J.T.: Fast Probabilistic Algorithms for Verification of Polynomial Identities. J. ACM **27**(4), 701–717 (Oct 1980) 3
46. Shokrollahi, M.A., Spielman, D.A., Stemann, V.: A remark on matrix rigidity. Information Processing Letters **64**(6), 283–285 (1997) 3
47. Shpilka, A., Yehudayoff, A.: Arithmetic Circuits: A survey of recent results and open questions. Foundations and Trends® in Theoretical Computer Science **5**(3–4), 207–388 (2010) 2, 3, 7
48. Shub, M., Smale, S.: On the intractability of Hilbert's Nullstellensatz and an algebraic version of " NP$\neq$ P?". Duke Mathematical Journal **81**(1), 47–54 (1995) 2
49. Smale, S.: Mathematical problems for the next century. The mathematical intelligencer **20**(2), 7–15 (1998) 2
50. Tavenas, S.: Bornes inferieures et superieures dans les circuits arithmetiques. Ph.D. thesis (2014) 2
51. Valiant, L.G.: On non-linear lower bounds in computational complexity. In: Proceedings of the seventh annual ACM symposium on Theory of computing. pp. 45–53 (1975) 3
52. Valiant, L.G.: Graph-theoretic arguments in low-level complexity. In: International Symposium on Mathematical Foundations of Computer Science. pp. 162–176. Springer (1977) 3, 5
53. Valiant, L.G.: Completeness classes in algebra. In: Proceedings of the 11th Annual ACM symposium on Theory of computing. pp. 249–261. ACM (1979) 2, 8
54. Valiant, L.G., Skyum, S., Berkowitz, S., Rackoff, C.: Fast Parallel Computation of Polynomials Using Few Processors. SIAM Journal of Computing **12**(4), 641–644 (1983). https://doi.org/10.1137/0212043, `https://doi.org/10.1137/0212043` 8
55. Zippel, R.: Probabilistic Algorithms for Sparse Polynomials. In: Proceedings of the International Symposium on Symbolic and Algebraic Computation. pp. 216–226. EUROSAM '79 (1979) 3