On vanishing sums of roots of unity in polynomial calculus and sum-of-squares

Ilario Bonacina ✉
Universitat Politècnica de Catalunya

Nicola Galesi ✉
Sapienza Università di Roma

Massimo Lauria ✉
Sapienza Università di Roma

Abstract

Vanishing sums of roots of unity can be seen as a natural generalization of knapsack from Boolean variables to variables taking values over the roots of unity. We show that these sums are hard to prove for polynomial calculus and for sum-of-squares, both in terms of degree and size.

2012 ACM Subject Classification Theory of computation → Proof complexity; Computing methodologies → Representation of polynomials

Keywords and phrases polynomial calculus, sum-of-squares, roots of unity, knapsack

Digital Object Identifier 10.4230/LIPIcs.MFCS.2022.18

Funding The first author was supported by the MICIN grants PID2019-109137GB-C22 and IJC2018-035334-I, and partially by the grant PID2019-109137GB-C21.

1 Introduction

Statements from combinatorics, constraint satisfaction problems (CSP), arithmetic circuit design, and algebra itself can be formalized either as statements about polynomial equalities (and inequalities), or via propositional logic. The approach based on propositional logic is amenable to *state-of-the-art* algorithms for satisfiability (SAT), usually variations of *Conflict-Driven-Clause-Learning* SAT solvers (CDCL), see for instance [28, 29, 3]. These solvers are surprisingly efficient, but their reasoning is ultimately based on the *resolution* proof system. On problems coming from algebra, CDCL solvers do not exploit the algebraic aspects of the problem, and therefore are typically unable to solve them. Switching to algebra allows to leverage on tools as Hilbert's Nullstellensatz and Gröbner basis computation in order to solve systems of polynomial equations [10], or semidefinite programming to solve systems of polynomial inequalities [30, 25]. These algebraic tools have been successful in practice for instance to solve κ-COLORING [11, 12, 13] and the verification of arithmetic multiplier circuits [22, 21, 23]. κ-COLORING, and in general CSP problems over finite domains of size κ, are naturally encoded using κ-valued variables. In particular, the algebraic tools for κ-COLORING use the *Fourier encoding*, which represents values via complex variables z subjected to the constraint $z^\kappa = 1$ and hence such that

$$z \in \{1, \zeta, \zeta^2, \ldots, \zeta^{\kappa-1}\} ,$$

where ζ is a primitive κth root of unity. A κ-valued variable z can be alternatively represented as a collection of indicator Boolean variables $x_1, \ldots, x_\kappa$ equipped with the additional constraint $x_1 + \cdots + x_\kappa = 1$.

Picking the right encoding is essential to leverage the algebraic structure of the problem. Even simple changes, for instance adding new variables to represent Boolean negations may already give significant speedups both in theory and in practice [14, 20].

47th International Symposium on Mathematical Foundations of Computer Science (MFCS 2022).
Editors: Stefan Szeider, Robert Ganian, and Alexandra Silva; Article No. 18; pp. 18:1–18:15
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In this paper, following a general approach from proof complexity, we show that algorithms leveraging Hilbert's Nullstellensatz or Gröbner basis computations cannot prove efficiently the unsatisfiability of some natural sets of polynomials equations over the Fourier variables.

The proof systems we consider are *polynomial calculus* and *sum-of-squares*. Polynomial calculus is a well studied proof system that captures Hilbert's Nullstellensatz and Gröbner basis computations. It is a system that certifies the unsatisfiability of sets of polynomial equations. It has been studied for polynomials over different fields or rings and, in particular, also for polynomials over the complex numbers $\mathbb{C}$, see for instance [7]. Given polynomials $p_1, \ldots, p_m$ with coefficients in a field $\mathbb{F}$, a refutation of $\{p_1 = 0, \ldots, p_m = 0\}$ in *polynomial calculus over* $\mathbb{F}$, denoted as $\mathsf{PC}_{\mathbb{F}}$, is a sequence of polynomials $p_1, \ldots, p_s$ over $\mathbb{F}$ such that $p_s = 1$ and each $p_{m+1}, \ldots, p_s$ is either (1) $r \cdot p_k$ for some polynomial r with coeffcients in $\mathbb{F}$ and some $k < i$; or (2) a linear combination $\alpha p_j + \beta p_k$ for $j, k < i$ and $\alpha, \beta \in \mathbb{F}$.

Regarding sum-of-squares, it is a systems to certify the unsatisfiability of sets of polynomial equations *and inequalities* over $\mathbb{R}$. A sum-of-squares $\mathsf{SoS}_{\mathbb{R}}$ refutation of the set of contraints $\{p = 0 : p \in P\} \cup \{h \geq 0 : h \in H\}$ is an identity of the form

$$-1 = \sum_{p \in P} q_p \cdot p + \sum_{h \in H} q_h \cdot h + \sum_{s \in S} s^2 ,$$

where the s, q_p, q_h are polynomials over $\mathbb{R}$ and moreover the q_hs are sums of squared polynomials. In presence of Boolean or $\{\pm 1\}$-valued variables, $\mathsf{SoS}_{\mathbb{R}}$ p-simulates $\mathsf{PC}_{\mathbb{R}}$ [4, 34].

In this paper, we introduce a generalization of sum-of-squares with polynomials over $\mathbb{C}$, $\mathsf{SoS}_{\mathbb{C}}$ (see Section 2 for the formal definition). Since $\mathbb{C}$ is not an ordered field, this generalization of sum-of-squares to $\mathbb{C}$ can only be used to certify the unsatisfiability of sets of polynomial *equations*. For sets of polynomial equations over $\mathbb{R}$ and in the presence of Boolean variables, $\mathsf{SoS}_{\mathbb{C}}$ coincides with the usual notion of sum-of-squares over $\mathbb{R}$, but the generalization is necessary to deal with Fourier variables or to reason about polynomials over $\mathbb{C}$. In presence of Fourier variables, $\mathsf{SoS}_{\mathbb{C}}$ p-simulates $\mathsf{PC}_{\mathbb{C}}$, see Section 2 for more details.

PC and SoS can be used to solve computational problems once they are encoded as sets of polynomials equations. It is customary to discuss sets of polynomial equations simply as sets of polynomials. We adopt this custom and we say that a set of polynomials over $\mathbb{C}$ is *satisfiable* when it has a common zero $\boldsymbol{\alpha} \in \mathbb{C}^n$. The most naïve algebraic encoding is to use variables ranging over $\{0, 1\}$ to represent the truth values of variables. This Boolean nature of a variable x is enforced via the polynomial $x^2 - x$. With this encoding then, for example, the satisfiability of a propositional clause $x \vee \neg y \vee z$ can be encoded as the satisfiability of the set of polynomials $\{(1-x)y(1-z),\ x^2 - x,\ y^2 - y,\ z^2 - z\}$. Truth values of variables are sometimes also encoded in the Fourier basis $\{\pm 1\}$ and, as we already mentioned, for some CSPs it is convenient to use κ-valued variables using the κth roots of unity.

Finding deductions in PC/SoS may be hard, and in general there are important proxy measures to estimate such hardness: the maximum *degree* of the polynomials involved in the deductions, and the number of monomials involved in the whole proof when polynomials are written explicitly as sums of monomials (*size*). The degree is a very rough measure of the proof search space, the size is a lower bound on the time required to produce the proof.

Studying size and degree complexity in algebraic systems over Fourier encodings is particularly relevant to understand how to leverage to proof complexity techniques like the *Smolensky's method* in circuit complexity [33]. He proved exponential lower bounds to compute the MOD_p function by bounded-depth circuits using the unbounded gates in $\{\wedge, \vee, \mathrm{MOD}_q\}$, for p and q relatively prime, employing a reduction to low-degree polynomials over $\mathrm{GF}(q)$ approximating such circuits. In proof complexity, it is a long-standing problem to obtain lower bounds for proof systems over bounded-depth formulas with modular gates.

Non-trivial degree lower bounds for Fourier encodings were first obtained for the Nullstellensatz proof system and PC by Grigoriev in [18] and Buss *et al.* in [7] for the Tseitin principle over p-valued variables (instead of the usual $\{0,1\}$) and the so-called MOD_p principles [7].

For $\mathsf{PC}/\mathsf{SoS}_{\mathbb{R}}$ over Boolean variables we know degree and size lower bounds for the encodings of several computational problems, see for instance [2, 17, 31, 32, 35]. For the size lower bounds in PC and $\mathsf{SoS}_{\mathbb{R}}$ this is essentially due to degree-size tradeoffs: if a set of polynomials *over Boolean variables* has no refutation in $\mathsf{PC}/\mathsf{SoS}_{\mathbb{R}}$ of degree at most D, then it has no refutation containing less than $2^{\Omega\left(\frac{(D-d)^2}{n}\right)}$ monomials, see [1, 19].

No such degree-size relation holds for polynomials over the Fourier variables. For instance, it is well-known that Tseitin contradictions over the Boolean variables $\{0,1\}$ require an exponential number of monomials to be refuted in PC, while PC can refute them with a linear number of monomials if the encoding uses the variables $\{\pm 1\}$, see [7].

To the best of our knowledge, the first size lower bounds in $\mathsf{PC}/\mathsf{SoS}_{\mathbb{R}}$ for polynomials with $\{\pm 1\}$ variables are proved by [34] for the pigeonhole principle and random 11-CNFs. Moreover that work provides a technique to turn strong degree lower bounds in that framework into strong size lower bounds for the same polynomials composed with some carefully constructed gadgets. We extend this latter approach to get size lower bound under the Fourier encoding of κ-valued variables, and we apply it to a generalization of KNAPSACK for these variables.

The classical KNAPSACK problem corresponds to the set of polynomials

$$\left\{ \sum_{i=1}^{n} c_i x_i - r \ , \quad x_1^2 - x_1, \dots, x_n^2 - x_n \right\} , \tag{1}$$

where $r, c_1, \dots, c_n \in \mathbb{C}$. For KNAPSACK are known linear degree lower bounds in PC, see [19, Theorem 5.1], and, when all the c_is are 1 and $r \in \mathbb{R}$, degree lower bounds in $\mathsf{SoS}_{\mathbb{R}}$ of the form $\min\{2\lfloor \min\{r, n-r\}\rfloor + 3, n\}$, see [17]. Size lower bounds are also implied by the respective size-degree tradeoffs [19, 1].

Sums of roots of unity We consider the problem of when a sum of n variables with values in the κth roots of unity can be equal to some value $r \in \mathbb{C}$, that is the satisfiability of

$$\mathsf{SRU}_n^{\kappa,r} := \left\{ \sum_{i\in[n]} z_i - r, \ z_1^\kappa - 1, \dots, z_n^\kappa - 1 \right\} . \tag{2}$$

Linear relations of the form $\sum_{i=1}^n c_i\zeta_i = 0$, where c_i are complex numbers and ζ_i are roots of unity, arise naturally in several contexts [9], and have been extensively studied in the literature, see for instance [16, 15]. When κ divides n, $\kappa \mid n$, it is easy to see that $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable, because the κth roots of unity sum to zero.

When κ is a power of a prime number p, this is indeed the only possibility, that is $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable over $\mathbb{C}$ if and only if $p \mid n$. (For the simple proof of this fact see the full version.) For the general case of $\kappa \in \mathbb{N}$, Lam and Leung [24] characterize exactly the set of natural numbers n such that $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable. As a corollary of their results, if κ is not a power of a prime then, there exists a $n_0(\kappa)$ s.t. for every $n \geq n_0(\kappa)$ the set of polynomials $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable.

Our results In this paper we show the hardness to certify in PC and $\mathsf{SoS}_{\mathbb{C}}$ the unsatisfiability of $\mathsf{SRU}_n^{\kappa,0}$ when κ is a prime and does not divide n. For simplicity, we leave the discussion for the case when κ is a power of a prime for the journal version. Our main results regarding $\mathsf{PC}/\mathsf{SoS}_{\mathbb{C}}$ informally say that $\mathsf{SoS}_{\mathbb{C}}$ and $\mathsf{PC}_{\mathbb{C}}$ cannot capture divisibility arguments.

A linear degree lower bound for $\mathsf{SRU}_n^{2,0}$ follows immediately, via a linear transformation, from the known degree lower bound for KNAPSACK in SoS, since the Grigoriev's lower bound in [17] can easily extended to $\mathsf{SoS}_{\mathbb{C}}$. In this paper we generalize this result proving degree and size lower bounds in $\mathsf{SoS}_{\mathbb{C}}$ for $\mathsf{SRU}_n^{\kappa,r}$ for κ an odd prime.

▶ **Theorem 1** (Degree lower bound for $\mathsf{SRU}_n^{\kappa,r}$). *Let $n, d \in \mathbb{N}$, κ be a prime, $r \in \mathbb{C}$. Let r be written as $r_1 + \zeta r_2$, where $r_1, r_2 \in \mathbb{R}$ and ζ is some κth primitive root of unity. If*

$$\kappa d \leq \min\{r_1 + r_2 + (\kappa - 1)n + \kappa,\ n - r_1 - r_2 + \kappa\} ,$$

then there are no $\mathsf{SoS}_{\mathbb{C}}$-refutations of $\mathsf{SRU}_n^{\kappa,r}$ of degree at most d. In particular, $\mathsf{SRU}_n^{\kappa,0}$ requires refutations of degree $\Omega\left(\frac{n}{\kappa}\right)$ in $\mathsf{SoS}_{\mathbb{C}}$.

From the set of polynomials in $\mathsf{SRU}_n^{2,r}$ we can easily infer the polynomials in $\mathsf{SRU}_n^{\kappa,0}$, via a linear transformation and a weakening. This is enough to prove degree lower bounds for $\mathsf{SRU}_n^{\kappa,0}$ in $\mathsf{PC}_{\mathbb{C}}$ since, Impagliazzo, Pudlák, and Sgall [19, Theorem 5.1] proved a linear degree lower bound for KNAPSACK and therefore $\mathsf{SRU}_n^{2,r}$ for any r. This is not the case for $\mathsf{SoS}_{\mathbb{C}}$: $\mathsf{SRU}_n^{2,r}$ is refutable in small degree and size in $\mathsf{SoS}_{\mathbb{C}}$ if $r \in \mathbb{C} \setminus \mathbb{R}$, see Example 4. In other words, in $\mathsf{SoS}_{\mathbb{C}}$, unlike the case of PC, it is not possible to reduce the hardness of $\mathsf{SRU}_n^{\kappa,0}$, for $\kappa > 2$ to KNAPSACK.

To prove the degree lower bound in $\mathsf{SoS}_{\mathbb{C}}$ for $\mathsf{SRU}_n^{\kappa,r}$ (Theorem 1) first we construct a candidate pseudo-expectation for $\mathsf{SRU}_n^{\kappa,r}$ based on the symmetries of the set of polynomials. Then we prove its correctness, following the approach by Blekherman [5, 6] as presented in [27, Theorem B.11] but generalized to $\mathsf{SoS}_{\mathbb{C}}$. Due to page limitations we only show in Section 4 how to use the generalization of Blekherman's theorem (Theorem 13) to prove Theorem 1.

We also prove a size lower bound for $\mathsf{SRU}_n^{\kappa,0}$ in $\mathsf{SoS}_{\mathbb{C}}$. We lift degree lower bounds to size lower bounds generalizing to κ-valued Fourier variables the lifting approach due to Sokolov [34], originally designed for real valued polynomials and $\{\pm 1\}$-variables.

▶ **Theorem 2** (Size lower bound for $\mathsf{SRU}_n^{\kappa,0}$). *Let κ be a prime and $n \in \mathbb{N}$, if $n \gg \kappa$ then the set of polynomials $\mathsf{SRU}_n^{\kappa,0}$ has no refutation in $\mathsf{SoS}_{\mathbb{C}}$ within monomial size $2^{o(n)}$.*

Theorem 2, for $\kappa = 2$, follows easily from the techniques of Sokolov [34] and Grigoriev's degree lower bound for KNAPSACK [17]. For $\kappa > 2$ it requires some non-trivial extension of the lifting technique from [34]. That is, the composition of polynomials with appropriate gadgets (see Definition 6). Our generalization of the lifting from [34] is Theorem 7 in Section 3.

Theorem 1 and Theorem 2 also hold for $\mathsf{PC}_{\mathbb{C}}$, since $\mathsf{SoS}_{\mathbb{C}}$ simulates $\mathsf{PC}_{\mathbb{C}}$.

Structure of the paper In the next section, we give the necessary preliminaries on roots of unity and the formal definition of $\mathsf{SoS}_{\mathbb{C}}$. In Section 3 we layout the proof of a way to lift degree lower bounds to size lower bounds in $\mathsf{SoS}_{\mathbb{C}}$ for sets of polynomials over the Fourier variables (Theorem 7) and we show how to prove Theorem 2 from Theorem 1 and Theorem 7. The proof of Theorem 1 is in Section 4.

2 Preliminaries

Given $n, k \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$, and if k divides n we write $k \mid n$. For $a \in \mathbb{R}$ and $b \in \mathbb{N}$, let $\binom{a}{0} := 1$ and $\binom{a}{b} := \frac{a(a-1)\ldots(a-b+1)}{b!}$ for $b \geq 1$. **Boldface** symbols indicate vectors, and $\boldsymbol{x}$ denotes a vector with n elements $(x_1, \ldots, x_n)$. We denote with $\boldsymbol{x}$ Boolean variables, with $\boldsymbol{z}$ κ-valued variables and with $\boldsymbol{y}$ generic variables or auxiliary variables. Given a set of polynomials $P \subseteq \mathbb{C}[\boldsymbol{y}]$, $\langle P \rangle$ denotes the ideal generated by P in $\mathbb{C}[\boldsymbol{y}]$. Let $\underline{i}$ be the imaginary unit in $\mathbb{C}$, i.e. $\underline{i}^2 = -1$.

Roots of unity For a positive integer κ, a *κth root of unity* is a root of the polynomial $z^\kappa - 1$. All the roots of unity except 1 are also roots of the polynomial $1 + z + \cdots + z^{\kappa-1}$, indeed $z^\kappa - 1 = (z-1) \cdot (1 + z + \cdots + z^{\kappa-1})$. A κth root of unity ζ is called *primitive* if $\zeta^t \neq 1$ for all $1 \leq t < \kappa$. If this is the case the κth roots of unity are indeed $1, \zeta, \zeta^2, \ldots, \zeta^{\kappa-1}$. Some of the results of this paper hold for roots of unity in generic fields but, for sake of clarity, we only consider roots of unity in $\mathbb{C}$. Notice that the complex conjugate of ζ^t is $\zeta^{\kappa-t}$. For concreteness, we denote as ζ a specific primitive κth root of unity, for instance $\mathrm{e}^{2\pi\underline{i}/\kappa}$, and as Ω_κ the set $\{1, \zeta, \zeta^2, \ldots, \zeta^{\kappa-1}\}$. We often denote as ω a generic element in Ω_κ.

SoS over the complex numbers The key concept at the core of the sum-of-squares proof system is that squares of real valued polynomials are always positive. For a complex valued polynomial $p \in \mathbb{C}[\boldsymbol{y}]$ we use that $p \cdot p^* \geq 0$, where p^* is the function that maps the assignment $\boldsymbol{\alpha}$ to the complex conjugate of the value $p(\boldsymbol{\alpha})$. We need a polynomial representation of function p^* that we call *formal conjugate* of p. To have such polynomial, in general, we would need to use a twin formal variable to represent x^* for any original variable x. Furthermore we would need to add to the proof system various axioms to relate x and x^*. In this work we focus on $\mathsf{SoS}_\mathbb{C}$ under the Boolean and Fourier encodings, hence we can represent formal conjugates as polynomials without any additional axiom or variable. For a Boolean variable $x \in \{0,1\}$ we have that x^* is x itself. For a Fourier variable z raised to an integer power $0 \leq t < \kappa$, the function $(z^t)^*$ is $z^{\kappa-t}$. Then the operator * extends homomorphically on sums and products, and it is equal to the usual complex conjugate on complex number. We are now ready to define the sum-of-squares proof system over complex number.

▶ **Definition 3** (Sum-of-Squares over $\mathbb{C}$, $\mathsf{SoS}_\mathbb{C}$)**.** *Fix an integer $\kappa \geq 2$. Consider a set of polynomials $P \subseteq \mathbb{C}[\boldsymbol{x}, \boldsymbol{z}]$ where P contains $z^\kappa - 1$ and for each variable z, and contains $x^2 - x$ for each variable x. A* refutation of P in $\mathsf{SoS}_\mathbb{C}$ *is an equality of the form*

$$-1 = \sum_{p \in P} q_p \cdot p + \sum_{s \in S} s \cdot s^* \ ,$$

where the $s \in S$ and q_p for $p \in P$ are in $\mathbb{C}[\boldsymbol{x}, \boldsymbol{z}]$ and each s^* is the formal conjugate of s.

The degree *of the refutation is* $\max\{\deg(q_p) + \deg(p), \deg(s \cdot s^*) \ : \ p \in P, \ s \in S\}$*. The* size *of the refutation is the total number of monomials occurring with non-zero coefficients among polynomials* $\{q_p, p \ : \ p \in P\} \cup \{s, s^* \ : \ s \in S\}$*.*

Notice that, for polynomials $p, q \in \mathbb{R}[\boldsymbol{x}, \boldsymbol{z}]$, $(p + \underline{i}q)(p - \underline{i}q) = p^2 + q^2$. Therefore for $P \subseteq \mathbb{R}[\boldsymbol{x}]$ and containing $x_i^2 - x_i$ for every $i \in [n]$, the notion of $\mathsf{SoS}_\mathbb{C}$ and $\mathsf{SoS}_\mathbb{R}$ coincide.

By Hilbert's Nullstellensatz, $\mathsf{SoS}_\mathbb{C}$ is complete: for every unsatisfiable set of polynomials P there is a $\mathsf{SoS}_\mathbb{C}$-refutation. Conversely, only unsatisfiable sets of polynomials have $\mathsf{SoS}_\mathbb{C}$ refutations: for any assignment $\boldsymbol{\alpha}$ of a polynomial s, polynomial $s \cdot s^*$ evaluates to $|s(\boldsymbol{\alpha})|^2$ which is a non-negative real number.

▶ **Example 4.** The set of polynomials $\{\sum_{j \in [n]} x_j - \underline{i}, \ x_1^2 - x_1, \ldots, \ x_n^2 - x_n\}$ has a simple $\mathsf{SoS}_\mathbb{C}$ refutation:

$$-1 = -(\sum_{j \in [n]} x_j - \underline{i})(\sum_{j \in [n]} x_j + \underline{i}) + (\sum_{j \in [n]} x_j)^2 \ .$$

Via similar algebraic equalities it is not hard to see that $\mathsf{SoS}_{\mathbb{C}}$ can refute easily the set of polynomials corresponding to KNAPSACK in eq. (1) when $r \in \mathbb{C} \setminus \mathbb{R}$ and all c_is are real. By a simple modification of [4, Lemma 3.1] and [34], we also have that, in presence of the axioms $y_i^\kappa - 1$, $\mathsf{SoS}_{\mathbb{C}}$ simulates $\mathsf{PC}_{\mathbb{C}}$, that is $\mathsf{PC}_{\mathbb{C}}$ refutations can be converted to $\mathsf{SoS}_{\mathbb{C}}$ refutations with just a polynomial increase in size.[1] Impagliazzo, Pudlák, and Sgall in [19, Theorem 5.1] prove that the set of polynomials in eq. (1) is hard for $\mathsf{PC}_{\mathbb{C}}$, hence $\mathsf{SoS}_{\mathbb{C}}$ is strictly stronger than $\mathsf{PC}_{\mathbb{C}}$.

3 Size lower bounds in Sum-of-Squares

In this section we prove the size lower bound for $\mathsf{SRU}_n^{\kappa,0}$ in $\mathsf{SoS}_{\mathbb{C}}$ from the the corresponding degree lower bound. That is we show how to prove Theorem 2 from Theorem 1. On a very high level, this is done *composing* the polynomials in $\mathsf{SRU}_n^{\kappa,r}$ with some polynomials $\boldsymbol{g}$, obtaining then some new set of polynomials $\mathsf{SRU}_n^{\kappa,r} \circ \boldsymbol{g}$, and then via a lifting theorem showing how degree lower bounds on $\mathsf{SRU}_n^{\kappa,r}$ imply size lower bounds on $\mathsf{SRU}_n^{\kappa,r} \circ \boldsymbol{g}$.

▶ **Definition 5** (composition of polynomials)**.** *Let $\boldsymbol{x}, \boldsymbol{y}_1, \dots \boldsymbol{y}_n$ be tuples of distinct variables where $\boldsymbol{y}_j = (y_{j1}, \dots, y_{j\ell_j})$. Given a polynomial $p \in \mathbb{C}[\boldsymbol{x}]$ and $\boldsymbol{g} = (g_1 \dots, g_n)$ with $g_j \in \mathbb{C}[\boldsymbol{y}_j]$ we denote by $p \circ \boldsymbol{g}$ the polynomial obtained substituting each instance of the variable x_j in p with the polynomial $g_j(\boldsymbol{y}_j)$ and then expanding the obtained algebraic expression as a sum of monomials in the new variables. The polynomial $p \circ \boldsymbol{g}$ then belongs to the ring $\mathbb{C}[\boldsymbol{y}_1, \dots, \boldsymbol{y}_n]$.*

Similarly, for a set of polynomials $P \subset \mathbb{C}[\boldsymbol{x}]$ we denote as $P \circ \boldsymbol{g}$ the set of polynomials $\{p \circ \boldsymbol{g} \ : \ p \in P\}$.

We are only interested in composing polynomials with $\boldsymbol{g}$ when $\boldsymbol{g}$ has some good properties. Those are a generalization of the notion of *compliant gadgets* from [34, Definition 2.1].

▶ **Definition 6** (compliant polynomial)**.** *A polynomial $g \in \mathbb{C}[y_1, \dots, y_\ell]$ is* compliant *if it is symmetric and there exists a function $h : \Omega_\kappa \to \Omega_\kappa^\ell$ such that*

1. *$g \circ h = \mathbf{id}$, i.e. for all $b \in \Omega_\kappa$, $g(h(b)) = b$;*
2. *for each $b \in \Omega_\kappa$, the first κ coordinates of $h(b)$ list all the elements of Ω_κ; and*
3. *$\prod_{\omega \in \Omega_\kappa} h(\omega)$ is a constant function.*

We say that $\boldsymbol{g} = (g_1 \dots, g_n)$ with $g_j \in \mathbb{C}[\boldsymbol{y}_j]$ is compliant *when each g_j is compliant.*

The original definition of [34, Definition 2.1] focuses on real polynomials and sets of values $\{0, 1\}$ and $\{\pm 1\}$, while ours focuses on complex polynomials and the set of κth roots of unity.

The size lower bound on $\mathsf{SRU}_n^{\kappa,0}$ in $\mathsf{SoS}_{\mathbb{C}}$ follows from the following general result.

▶ **Theorem 7.** *Let P a finite set of polynomials of degree at most d_0 in $\mathbb{C}[\boldsymbol{x}]$ containing the polynomials $x_i^\kappa - 1$ for each $i \in [n]$. Let $\boldsymbol{g}$ be a tuple of compliant polynomials with $g_i \in \mathbb{C}[y_{i1}, \dots, y_{i\ell_i}]$. If P requires degree D to be refuted in $\mathsf{SoS}_{\mathbb{C}}$, then*

$$P \circ \boldsymbol{g} \cup \{y_{ij}^\kappa - 1 \ : \ i \in [n], \ j \in [\ell_i]\}$$

requires monomial size at least $\exp(\frac{(D-d_0)^2}{8\ell^\kappa(\kappa-1)n})$ to be refuted in $\mathsf{SoS}_{\mathbb{C}}$, where $\ell = \max_{i \in [n]} \ell_i$.

[1] The main difference with [4, Lemma 3.1] and [34] is to consider polynomials $s \cdot s^*$ instead of squares s^2 and then to use the algebraic equality $(p+q)(p+q)^* + (p-q)(p-q)^* = 2pp^* + 2qq^*$ instead of the one for the reals $(p+q)^2 + (p-q)^2 = 2p^2 + 2q^2$.

This result is a generalization of [34, Theorem 4.2]. Before seeing how to prove this result let us see how to apply it to prove a size lower bound for $\mathsf{SRU}_n^{\kappa,0}$, that is Theorem 2, restated below for convenience of the reader.

▶ **Theorem 2** (Size lower bound for $\mathsf{SRU}_n^{\kappa,0}$). *Let κ be a prime and $n \in \mathbb{N}$, if $n \gg \kappa$ then the set of polynomials $\mathsf{SRU}_n^{\kappa,0}$ has no refutation in $\mathsf{SoS}_{\mathbb{C}}$ within monomial size $2^{o(n)}$.*

Proof. Let $n = (2\kappa + 1)n' + b$ with $b \in \{0, \dots, 2\kappa\}$. Let $\ell_1 = \cdots = \ell_b = 2\kappa + 2$ and $\ell_{b+1} = \cdots = \ell_{n'} = 2\kappa + 1$. Consider the tuple $\boldsymbol{g} = (g_1, \dots, g_{n'})$ where $g_i \in \mathbb{C}[y_{i1}, \dots, y_{i\ell_i}]$ is the polynomial

$$g_i(y_{i1}, \dots, y_{i\ell_i}) := \frac{1}{\kappa}\Big(\sum_{j\in[\ell_i]} y_{ij} - (\ell_i - 2\kappa)\Big) \ .$$

We have that $\mathsf{SRU}_n^{\kappa,0}$ after renaming of variables is a subset of

$$\mathsf{SRU}_{n'}^{\kappa,r} \circ \boldsymbol{g} \cup \{y_{ij}^{\kappa} - 1 \ : \ i \in [n'],\ j \in [\ell_i]\} \tag{3}$$

with $r = -\frac{n'+b}{\kappa}$. By Theorem 1, there are no $\mathsf{SoS}_{\mathbb{C}}$ refutations of $\mathsf{SRU}_{n'}^{\kappa,r}$ in degree $\frac{n'}{\kappa}$. Each g_i is compliant. Indeed, the polynomial g_i is symmetric and we can take as $h_i : \Omega_\kappa \to \Omega_\kappa^{\ell_i}$ the function mapping

$$h_i : \omega \mapsto (1, \zeta, \zeta^2, \dots, \zeta^{\kappa-1}, \underbrace{1, 1, \dots, 1}_{\ell_i - 2\kappa}, \underbrace{\omega, \omega, \dots, \omega}_{\kappa}) \ ,$$

where ζ is a primitive κth root of unity in $\mathbb{C}$. Clearly, $g \circ h$ is the identity and

$$\prod_{\omega\in\Omega_\kappa} h_i(\omega) = \zeta^{\kappa(\kappa-1)/2}\omega^{\kappa} = \zeta^{\kappa(\kappa-1)/2}$$

since ω is a κth root of unity. By Theorem 7, the set of polynomials (3) requires $\mathsf{SoS}_{\mathbb{C}}$ refutations of monomial size at least $\exp(\frac{(\frac{n'}{\kappa}-\kappa)^2}{8\ell^{\kappa}(\kappa-1)n'}) = 2^{\Omega(n)}$ if $n \gg \kappa$. Therefore $\mathsf{SRU}_n^{\kappa,0}$ requires refutations size $2^{\Omega(n)}$, too. ◀

We conclude this section with a proof sketch of Theorem 7. The overall structure of the argument is that typical for size-degree trade-offs and can be found for instance in [8, 34, 1]. The idea is to show, on one side, that there exists a relatively long sequence of restrictions such that the restricted polynomials have small degree refutations (Theorem 8) and that each individual restriction can only make the degree decrease a little (Lemma 9). Those two facts will imply that the sequence of restrictions must be very long and this will imply the size-degree trade-off.

The *reduced degree* of a refutation in $\mathsf{SoS}_{\mathbb{C}}$ of a set of polynomials P containing the polynomials $x_j^{\kappa} - 1$ is the degree of the refutation where we do not take in account the degrees of the polynomials q_p where p is $x_j^{\kappa} - 1$ (see Definition 3).

Next theorem is the first ingredient for the proof of Theorem 7. It is a generalization of [34, Theorem 4.1] and its proof, an adaptation of the argument given in [34], is in the full version.

▶ **Theorem 8.** *Let P be finite a set of polynomials of degree d_0 in $\mathbb{C}[\boldsymbol{x}]$ containing the polynomials $x_j^{\kappa} - 1$ for each $j \in [n]$. Let $\boldsymbol{g}$ be a tuple of compliant polynomials with $g_i \in \mathbb{C}[y_{i1}, \dots, y_{i\ell_i}]$ and $\omega_1, \omega_2, \dots, \omega_m \in \Omega_\kappa$. If there is a $\mathsf{SoS}_{\mathbb{C}}$ refutation of $P \circ \boldsymbol{g} \cup \{y_{ij}^{\kappa} - 1 \ : \ i \in [n],\ j \in [\ell_i]\}$ of size s then there exists a sequence of variables $x_{i_1}, \dots, x_{i_m}$ with $m \geq \ell^{\kappa} n \ln(s)/D$ such that*

1. $\ell = \max_i \ell_i$;
2. the choice of x_{i_t} only depends on $\omega_1, \ldots, \omega_{t-1}$;
3. there is a $\mathsf{SoS}_{\mathbb{C}}$ refutation of $P\restriction_{x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m}$ of reduced degree at most $D + d_0$.

The second ingredient for the proof of Theorem 7 is the following lemma.

▶ **Lemma 9.** *Let P be a finite set of polynomials in $\mathbb{C}[\boldsymbol{x}]$ containing the polynomials $x_j^\kappa - 1$ for each $j \in [n]$. Suppose any $\mathsf{SoS}_{\mathbb{C}}$ refutation of P has reduced degree at least D. Then, for any variable x_j there is $\omega \in \Omega_\kappa$ such that $\mathsf{SoS}_{\mathbb{C}}$ refutations of $P\restriction_{x_j=\omega}$ must have reduced degree at least $D - 2\kappa + 2$.*

Proof. (sketch) For sake of contradiction, suppose there exists some variable x such that for every $\omega \in \Omega_\kappa$, $P\restriction_{x=\omega}$ has a refutation of reduced degree $D - 2\kappa + 1$. For every $\ell \in \mathbb{N}$, $x^\ell - \omega^\ell$ is a multiple of $x - \omega$. Therefore, for every $p \in P$, the polynomial $p - p\restriction_{x=\omega}$ belongs to the ideal generated by $x - \omega$. This means that we can transform refutations of $P\restriction_{x=\omega}$ into refutations of $P \cup \{x - \omega\}$ without increasing the degree. Hence, there are refutations of $P \cup \{x - \omega\}$ of reduced degree $D - 2\kappa + 1$ for every $\omega \in \Omega_\kappa$.

Let π_ω be a refutation of $P \cup \{x - \omega\}$ of reduced degree $D - 2\kappa + 1$. Let $q_\omega(x) = \prod_{\omega' \neq \omega}(x - \omega')$.

It is easy to see that multiplying π_ω by the polynomial $q_\omega q_\omega^*$ we get a derivation of $-q_\omega q_\omega^*$ from P. This new derivation has reduced degree $D-2\kappa+1+2(\kappa-1) = D-1$. Now we can take a linear combination (with *non-negative real* coefficients) of the previous derivations to get the derivation of -1. More precisely we need numbers $\alpha_\omega \geq 0$ such that $\sum_{\omega\in\Omega_\kappa} \alpha_\omega q_\omega q_\omega^* - 1 \in \langle x^\kappa - 1\rangle$. Setting $\alpha_\omega = 1/q_\omega(\omega)q_\omega(\omega)^*$ we get that that $\sum_{\omega\in\Omega_\kappa} \alpha_\omega q_\omega q_\omega^* - 1$ is zero for all $\omega \in \Omega_\kappa$ and therefore in the ideal $\langle x^\kappa - 1\rangle$. This finally gives a $\mathsf{SoS}_{\mathbb{C}}$ refutation of P in degree $D - 1$, contradicting the assumption on P. ◀

Proof of Theorem 7. Let s be the smallest size of a $\mathsf{SoS}_{\mathbb{C}}$ refutation of the set of polynomials $P \circ \boldsymbol{g} \cup \{y_{ij}^\kappa - 1 \,:\, i \in [n],\ j \in [\ell_i]\}$. We alternate applications of Theorem 8 to pick x_{i_t} with applications of Lemma 9 to pick ω_t, and in the end we have a sequence of variables/values $x_{i_1} = \omega_1, \ldots, x_{i_m} = \omega_m$. By these choices, the restricted set of polynomials $P\restriction_{x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m}$ requires refutations of reduced degree at least $D - 2\kappa m + 2m$. By Theorem 8, we can set $m = \ell^k n \ln(s)/D'$ for some $D' > 0$ and get a refutation of reduced degree at most $D' + d_0$. Hence, $D' + d_0 \geq D - 2m(\kappa - 1)$ and we get that $\ln(s) \geq \frac{D'(D-D'-d_0)}{2\ell^k n(\kappa-1)}$. The largest value is attained for $D' = (D - d_0)/2$ and we get $\ln(s) \geq \frac{(D-d_0)^2}{8\ell^k n(\kappa-1)}$. ◀

4 Degree lower bounds in $\mathsf{SoS}_{\mathbb{C}}$

In this section we prove Theorem 1, restated here for convenience of the reader.

▶ **Theorem 1** (Degree lower bound for $\mathsf{SRU}_n^{\kappa,r}$). *Let $n, d \in \mathbb{N}$, κ be a prime, $r \in \mathbb{C}$. Let r be written as $r_1 + \zeta r_2$, where $r_1, r_2 \in \mathbb{R}$ and ζ is some κth primitive root of unity. If*

$$\kappa d \leq \min\{r_1 + r_2 + (\kappa - 1)n + \kappa,\ n - r_1 - r_2 + \kappa\}\ ,$$

then there are no $\mathsf{SoS}_{\mathbb{C}}$-refutations of $\mathsf{SRU}_n^{\kappa,r}$ of degree at most d. In particular, $\mathsf{SRU}_n^{\kappa,0}$ requires refutations of degree $\Omega\left(\frac{n}{\kappa}\right)$ in $\mathsf{SoS}_{\mathbb{C}}$.

It is convenient to consider the following Boolean encoding of the sums of roots of unity,

$$\text{bool-}\mathsf{SRU}_n^{\kappa,r} := \left\{ \sum_{i\in[n]} \left(\sum_{j\in[\kappa]} \zeta^{j-1} x_{ij} \right) - r,\ x_{ij}^2 - x_{ij},\ \sum_{j\in[\kappa]} x_{ij} - 1 \,:\, i \in [n], j \in [\kappa] \right\} . \quad (4)$$

The set of equations $\mathsf{SRU}_n^{\kappa,r}$ uses variables taking values in $\{1,\zeta,\zeta^2,\dots,\zeta^{\kappa-1}\}$, the encoding in eq. (4) uses indicator variables to select the appropriate power of ζ. It is easy to see that the degree needed to refute $\mathsf{SRU}_n^{\kappa,r}$ in $\mathsf{PC}_{\mathbb{C}}/\mathsf{SoS}_{\mathbb{C}}$ is at least the degree needed to refute $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ in $\mathsf{PC}_{\mathbb{C}}/\mathsf{SoS}_{\mathbb{C}}$. Hence, it is enough to show the degree lower bound for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$. To show this we construct a degree-d *pseudo-expectation* for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$, i.e., a linear operator $\tilde{\mathbb{E}} : \mathbb{C}[\boldsymbol{x}] \to \mathbb{C}$ such that

- $\tilde{\mathbb{E}}(1) = 1$,
- $\tilde{\mathbb{E}}(mp) = 0$, for every $p \in \mathsf{bool\text{-}SRU}_n^{\kappa,r}$ and m monomial such that $\deg(p) + \deg(m) \le d$,
- $\tilde{\mathbb{E}}(s \cdot s^*) \in \mathbb{R}_{\ge 0}$, for every polynomial s s.t. $\deg(s \cdot s^*) \le d$.

It is easy to see that the existence of a degree-d pseudo-expectation for a set of polynomials P implies that P cannot be refuted in degree-d $\mathsf{SoS}_{\mathbb{C}}$. The construction of an appropriate pseudo-expectation $\tilde{\mathbb{E}}$ for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ is the goal of this section.

Some notation In this section we consider fixed $r \in \mathbb{C}$ and $r_1, r_2 \in \mathbb{R}$ such that $r = r_1 + \zeta r_2$. Let $\boldsymbol{e}_j$ be the vector of dimension κ with the jth entry 1 and all other entries 0. For $j \in [\kappa]$, let $\boldsymbol{x}^{(j)} := (x_{1j}, \dots, x_{nj})$. That is, $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ is a set of polynomials in $\mathbb{C}[\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(\kappa)}]$. Given a tuple of sets $\boldsymbol{I} = (I_1, \dots, I_\kappa)$, where $I_j \subseteq [n]$, let $X_{\boldsymbol{I}} := \prod_{j\in[\kappa]} \prod_{i \in I_j} x_{ij}$. With $\|\cdot\|$ we always denote the 1-norm. So $\|\boldsymbol{x}^{(j)}\|$ denotes the polynomial $\sum_{i\in[n]} x_{ij}$.

A potential satisfying assignment of $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ consists of $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_\kappa)$, the allocation of the n roots of unity in the directions $\zeta^0, \dots, \zeta^{\kappa-1}$. The sum $\sum_{j\in[\kappa]} \zeta^{j-1}\gamma_j$ must be equal to the target value $r = r_1 + \zeta r_2$, so we spread uniformly $n - r_1 - r_2$ among the γ_js, and then add r_1 and r_2 to γ_1 and γ_2 respectively. This leads to the definitions

$$\begin{cases} \gamma_1 = \frac{n-r_1-r_2}{\kappa} + r_1 \ , \\ \gamma_2 = \frac{n-r_1-r_2}{\kappa} + r_2 \ , \\ \gamma_j = \frac{n-r_1-r_2}{\kappa} \quad \text{for } j \ge 3 \ . \end{cases} \tag{5}$$

Observe that $\|\boldsymbol{\gamma}\| = n$. For ease of notation let $\hat{\gamma} = \frac{n-r_1-r_2}{\kappa}$ and $r_3 = \cdots = r_\kappa = 0$. Therefore, we can write $\gamma_j = \hat{\gamma} + r_j$ for each $j \in [\kappa]$.

Given $\boldsymbol{I} = (I_1, \dots, I_\kappa)$ with $I_j \subseteq [n]$, and variables $\boldsymbol{v} = (v_1, \dots, v_\kappa)$, let $S(X_{\boldsymbol{I}})$ be the polynomial in the variables $\boldsymbol{v}$ defined by

$$S(X_{\boldsymbol{I}}) := \begin{cases} \dfrac{(n - |\bigcup_{j\in[\kappa]} I_j|)!}{n!} \displaystyle\prod_{j\in[\kappa]} \prod_{\ell=0}^{|I_j|-1} (v_j - \ell) & \text{if the sets in } \boldsymbol{I} \text{ are pair-wise disjoint} \ , \\ 0 & \text{otherwise} \ . \end{cases} \tag{6}$$

By linearity, extend $S(\cdot)$ to all polynomials. That is, given $p = \sum_{\boldsymbol{I}} \alpha_{\boldsymbol{I}} X_{\boldsymbol{I}}$ with $\alpha_{\boldsymbol{I}} \in \mathbb{C}$, let $S(p) := \sum_{\boldsymbol{I}} \alpha_{\boldsymbol{I}} S(X_{\boldsymbol{I}})$. We define

$$\tilde{\mathbb{E}}(p) := S(p)(\boldsymbol{\gamma})$$

and we show that $\tilde{\mathbb{E}}$ is a pseudo-expectation for $\mathsf{bool\text{-}Kn}_n^{\kappa,r}$.

Let $\mathbb{B}$ be the ideal $\langle x_{ij}^2 - x_{ij},\ x_{ij}x_{ij'} : i \in [n],\ j, j' \in [\kappa],\ j \ne j' \rangle$. Given polynomials $p, q \in \mathbb{C}[\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(\kappa)}]$, we use the notation $p \equiv q$ to denote that $p - q \in \mathbb{B}$.

▶ **Lemma 10.** *If $p \equiv q$ then $\tilde{\mathbb{E}}(p) = \tilde{\mathbb{E}}(q)$.*

Proof. By definition $p \equiv q$ means there exists a polynomial $s \in \mathbb{B}$ such that $p = q + s$. By construction, $\tilde{\mathbb{E}}$ maps to 0 every polynomial in $\mathbb{B}$, in particular $\tilde{\mathbb{E}}(s) = 0$. By the linearity of $\tilde{\mathbb{E}}$, then $\tilde{\mathbb{E}}(p) = \tilde{\mathbb{E}}(q)$. ◀

From the definition of $\tilde{\mathbb{E}}$, it follows easily that the lifts of the polynomials in $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ are mapped to 0 by $\tilde{\mathbb{E}}$.

▶ **Theorem 11.** *For every $\boldsymbol{I} = (I_1, \ldots, I_\kappa)$ with $I_j \subseteq [n]$ and $i \in [n]$, and every $p \in \mathsf{bool\text{-}SRU}_n^{\kappa,r}$, $\tilde{\mathbb{E}}(X_{\boldsymbol{I}} p) = 0$.*

Proof. The fact that $\tilde{\mathbb{E}}(X_{\boldsymbol{I}}(x_{ij}^2 - x_{ij})) = 0$ is immediate by the definition of $\tilde{\mathbb{E}}$.

Given $\boldsymbol{a} = (a_1, \ldots, a_\kappa) \in [n]^\kappa$, let $E_{\boldsymbol{a}} := \frac{(n-\|\boldsymbol{a}\|)!}{n!} \prod_{j\in[\kappa]} \prod_{\ell=0}^{a_j-1} (\gamma_j - \ell)$. Notice that for every $j \in [\kappa]$, $E_{\boldsymbol{a}+\boldsymbol{e}_j} = E_{\boldsymbol{a}} \frac{\gamma_j - a_j}{n-\|\boldsymbol{a}\|}$. If the sets I_j are not pair-wise disjoint then, by definition, the pseudo-expectation is already 0, so it is enough to consider the case when the I_js are pair-wise disjoint.

Let $\boldsymbol{t} = (t_1, \ldots, t_\kappa)$ where $t_j = |I_j|$. To show that $\tilde{\mathbb{E}}(X_{\boldsymbol{I}}(\sum_{j\in[\kappa]} x_{ij} - 1)) = 0$ we have two cases. If $i \in \bigcup_{j\in[\kappa]} I_j$, then

$$\tilde{\mathbb{E}}(X_{\boldsymbol{I}}(\sum_{j\in[\kappa]} x_{ij} - 1)) = E_{\boldsymbol{t}} - E_{\boldsymbol{t}} = 0 \ .$$

If $i \notin \bigcup_{j\in[\kappa]} I_j$, then

$$\tilde{\mathbb{E}}(X_{\boldsymbol{I}}(\sum_{j\in[\kappa]} x_{ij} - 1)) = \sum_{j\in[\kappa]} E_{\boldsymbol{t}+\boldsymbol{e}_j} - E_{\boldsymbol{t}} = E_{\boldsymbol{t}} \cdot \left(\sum_{j\in[\kappa]} \frac{\gamma_j - t_j}{n - \|\boldsymbol{t}\|} - 1 \right) = E_{\boldsymbol{t}} \cdot \left(\frac{\|\boldsymbol{\gamma}\| - \|\boldsymbol{t}\|}{n - \|\boldsymbol{t}\|} - 1 \right) = 0 \ ,$$

since $\|\boldsymbol{\gamma}\| = n$.
Finally we prove that $\tilde{\mathbb{E}}(X_{\boldsymbol{I}}(\sum_{j\in[\kappa]} \zeta^{j-1} \|\boldsymbol{x}^{(j)}\| - r_1 - \zeta r_2)) = 0$:

$$\begin{aligned}
\tilde{\mathbb{E}}(X_{\boldsymbol{I}}(\sum_{j\in[\kappa]} \zeta^{j-1}\|\boldsymbol{x}^{(j)}\| - r_1 - \zeta r_2)) &= E_{\boldsymbol{t}} \sum_{j\in[\kappa]} \zeta^{j-1} t_j + \sum_{i\notin \bigcup_{j\in[\kappa]} I_j} (\sum_{j\in[\kappa]} \zeta^{j-1} E_{\boldsymbol{t}+\boldsymbol{e}_j}) - (r_1 + \zeta r_2) E_{\boldsymbol{t}} \\
&= E_{\boldsymbol{t}} \sum_{j\in[\kappa]} \zeta^{j-1} t_j + (n - \|\boldsymbol{t}\|) \sum_{j\in[\kappa]} \zeta^{j-1} E_{\boldsymbol{t}+\boldsymbol{e}_j} - (r_1 + \zeta r_2) E_{\boldsymbol{t}} \\
&= E_{\boldsymbol{t}} \sum_{j\in[\kappa]} \zeta^{j-1} t_j + E_{\boldsymbol{t}} \sum_{j\in[\kappa]} \zeta^{j-1} (\gamma_j - t_j) - (r_1 + \zeta r_2) E_{\boldsymbol{t}} \\
&= E_{\boldsymbol{t}} \cdot \left(\sum_{j\in[\kappa]} \zeta^{j-1} t_j + \sum_{j\in[\kappa]} \zeta^{j-1} (\gamma_j - t_j) - (r_1 + \zeta r_2) \right) \\
&= E_{\boldsymbol{t}} \cdot \left(\sum_{j\in[\kappa]} \zeta^{j-1} \gamma_j - (r_1 + \zeta r_2) \right) \\
&= E_{\boldsymbol{t}} \cdot \left(\sum_{j\in[\kappa]} \zeta^{j-1} \hat{\gamma} + \sum_{j\in[\kappa]} \zeta^{j-1} r_j - (r_1 + \zeta r_2) \right) \\
&= 0 \ ,
\end{aligned}$$

since $\gamma_j = \hat{\gamma} + r_j$, $r_j = 0$ for $j > 2$, and $\sum_{j\in[k]} \zeta^{j-1} = 0$. ◀

This result, together with Theorem 12 below, implies that $\tilde{\mathbb{E}}$ is a degree-d pseudo-expectation for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$, and therefore a degree-d lower bound for the refutations of $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ and $\mathsf{SRU}_n^{\kappa,r}$ in $\mathsf{SoS}_{\mathbb{C}}$, i.e. Theorem 1. The idea is to use to Blekherman's approach in [27, Appendix B,C]. Let us recall first some useful notation.

Let $\mathfrak{S}_n$ be the symmetric group of n elements. For a set $J \subseteq [n]$ and a permutation $\sigma \in \mathfrak{S}_n$, let $\sigma J := \{\sigma(j) : j \in J\}$. Consider variables $\boldsymbol{y} = (y_1, \dots, y_n)$. For a set $J \subseteq [n]$ let $Y_J := \prod_{j\in J} y_j$. Given a polynomial $p \in \mathbb{C}[\boldsymbol{y}]$, that is $p(\boldsymbol{y}) = \sum_{J\subseteq[n]} p_J Y_J$, with $p_J \in \mathbb{C}$, let

$$\sigma p(\boldsymbol{y}) := \sum_J p_J Y_{\sigma J} \ .$$

Then define the *symmetrization* of p as the polynomial $\mathrm{Sym}(p) \in \mathbb{C}[\boldsymbol{y}]$ given by

$$\mathrm{Sym}(p)(\boldsymbol{y}) := \frac{1}{n!} \sum_{\sigma\in\mathfrak{S}_n} \sigma p(\boldsymbol{y}) \ .$$

▶ **Theorem 12.** *For every polynomial $p \in \mathbb{C}[\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(\kappa)}]$ of degree at most d, if*

$$-(\kappa - 1)n + \kappa d - \kappa \le r_1 + r_2 \le n - \kappa d + \kappa \ ,$$

then $\tilde{\mathbb{E}}(p \cdot p^*) \ge 0$ where p^* is the formal conjugate of p.

Proof. Let $\boldsymbol{\gamma}$ be defined as in eq. (5), and recall $\hat{\gamma} = \frac{n-r_1-r_2}{\kappa}$. Recall that the polynomial $S(X_{\boldsymbol{I}})$ when evaluated on $\boldsymbol{\gamma}$ is exactly $\tilde{\mathbb{E}}(X_{\boldsymbol{I}})$, see the comment after eq. (6). We have that

$$\begin{aligned}
\tilde{\mathbb{E}}(p \cdot p^*) &= S(p \cdot p^*)(\boldsymbol{\gamma}) && \text{[by the definition of } \tilde{\mathbb{E}}] \\
&= S(p \cdot p^*)(r_1 + \hat{\gamma}, r_2 + \hat{\gamma}, \dots, r_\kappa + \hat{\gamma}) && \text{[by the definition of } \boldsymbol{\gamma}] \\
&= \mathrm{Sym}(p\restriction_\rho \cdot p\restriction^*_\rho)(\hat{\gamma}\boldsymbol{e}_1) && \text{[by Theorem 14 below]} \\
&= \sum_{j=0}^{d} p_{d-j}(\hat{\gamma}) \cdot p^*_{d-j}(\hat{\gamma}) \prod_{i=0}^{j-1} (\hat{\gamma} - i)(n - \hat{\gamma} - i) \ , && \text{[by Theorem 13 below]}
\end{aligned}$$

where ρ is the substitution given by $\rho(x_{ij}) := y_i + \frac{r_j}{n}$ (recall that $r_3 = \dots = r_\kappa = 0$). Now, $p_{d-j}(\hat{\gamma}) \cdot p^*_{d-j}(\hat{\gamma})$ is always real and non-negative since it is the module of the complex number $p_{d-j}(\hat{\gamma})$, hence to enforce the non-negativity of $\tilde{\mathbb{E}}(p \cdot p^*)$ it is enough to argue that $\prod_{i=0}^{j-1} (\hat{\gamma} - i)(n - \hat{\gamma} - i) \ge 0$. This is true if $\hat{\gamma} - d + 1 \ge 0$ and $n - \hat{\gamma} - d + 1 \ge 0$. I.e. if

$$-(\kappa - 1)n + \kappa d - \kappa \le r_1 + r_2 \le n - \kappa d + \kappa \ . \qquad ◀$$

▶ **Theorem 13** (adaptation of [27, Theorem B.11])**.** *Given variables $\boldsymbol{y} = (y_1, \dots, y_n)$ and $p, q \in \mathbb{C}[\boldsymbol{y}]$ with degree at most $d \le n/2$,*

$$\mathrm{Sym}(p \cdot p^*)(\boldsymbol{y}) \equiv \sum_{j=0}^{d} p_{d-j}(\|\boldsymbol{y}\|) \cdot p^*_{d-j}(\|\boldsymbol{y}\|) \prod_{i=0}^{j-1} (\|\boldsymbol{y}\| - i)(n - \|\boldsymbol{y}\| - i) \ ,$$

where p_{d-j} is a univariate polynomial with coefficients in $\mathbb{C}$, p^*_{d-j} is the formal conjugate of p_{d-j} and the degree of both polynomials is at most $(d - j)/2$.

This result is provable using exactly the same argument of Blekherman in [27, Theorem B.11], adapted to complex numbers.

▶ **Theorem 14.** *Given $p \in \mathbb{C}[\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(\kappa)}]$,*

$$S(p)(r_1 + \|\boldsymbol{y}\|, r_2 + \|\boldsymbol{y}\|, r_3 + \|\boldsymbol{y}\|, \dots, r_\kappa + \|\boldsymbol{y}\|) \equiv \mathrm{Sym}(p\restriction_\rho)(\boldsymbol{y}) \ ,$$

where ρ is the substitution given by $\rho(x_{ij}) := y_i + \frac{r_j}{n}$ (recall that $r_3 = \dots = r_\kappa = 0$).

Proof. Given a vector of variables $\boldsymbol{y} = (y_1, \ldots, y_m)$, let $\binom{\|\boldsymbol{y}\|}{t}$ be the polynomial

$$\binom{\|\boldsymbol{y}\|}{t} := \frac{\|\boldsymbol{y}\|(\|\boldsymbol{y}\|-1)\cdots(\|\boldsymbol{y}\|-t+1)}{t!} \ .$$

It holds that $\binom{\|\boldsymbol{y}\|}{t} \equiv \sum_{\substack{I\subseteq[n] \\ |I|=t}} Y_I$. (A proof of this fact is in the full version.) This immediately implies that

$$\prod_{j\in[\kappa]} \binom{\|\boldsymbol{x}^{(j)}\|}{t_j} \equiv \sum_{\substack{\boldsymbol{I}=(I_1,\ldots,I_\kappa),\ I_j\subseteq[n] \\ |I_j|=t_j}} X_{\boldsymbol{I}} \ . \tag{7}$$

For a vector of sets $\boldsymbol{I} = (I_1, \ldots, I_\kappa)$ and a permutation $\sigma \in \mathfrak{S}_n$, let $\sigma\boldsymbol{I} := (\sigma I_1, \ldots, \sigma I_\kappa)$. Given a polynomial $p = \sum_{\boldsymbol{I}} p_{\boldsymbol{I}} X_{\boldsymbol{I}}$ in $\mathbb{C}[\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(\kappa)}]$ and a permutation $\sigma \in \mathfrak{S}_n$ let

$$\sigma p := \sum_{\boldsymbol{I}} p_{\boldsymbol{I}} X_{\sigma\boldsymbol{I}} \ .$$

Now, for any polynomial $p \in \mathbb{C}[\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(\kappa)}]$

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} \sigma p \equiv S(p)(\|\boldsymbol{x}^{(1)}\|, \ldots, \|\boldsymbol{x}^{(\kappa)}\|) \ . \tag{8}$$

To see this equivalence, by linearity, it is enough to show that for every $\boldsymbol{I}$ with $I_j \subseteq [n]$

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} X_{\sigma\boldsymbol{I}} \equiv S(X_{\boldsymbol{I}})(\|\boldsymbol{x}^{(1)}\|, \ldots, \|\boldsymbol{x}^{(\kappa)}\|) \ .$$

If the sets in $\boldsymbol{I}$ are not pair-wise disjoint it is immediate to see that $\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} X_{\sigma\boldsymbol{I}} \in \mathbb{B}$, and therefore $\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} X_{\sigma\boldsymbol{I}} \equiv 0$. Suppose then $\boldsymbol{I} = (I_1, \ldots, I_\kappa)$ and the sets I_j are pair-wise disjoint. Let $t_j = |I_j|$, then

$$\begin{aligned}
\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} X_{\sigma\boldsymbol{I}} &= \frac{(n-\|\boldsymbol{t}\|)!\prod_{j\in[\kappa]} t_j!}{n!} \cdot \sum_{\substack{\boldsymbol{S}=(S_1,\ldots,S_\kappa) \\ \text{pair-wise disj.} \\ |S_j|=t_j}} X_{\boldsymbol{S}} \\
&\equiv \frac{(n-\|\boldsymbol{t}\|)!\prod_{j\in[\kappa]} t_j!}{n!} \cdot \sum_{\substack{\boldsymbol{S}=(S_1,\ldots,S_\kappa) \\ |S_j|=t_j}} X_{\boldsymbol{S}} \\
&\equiv \frac{(n-\|\boldsymbol{t}\|)!}{n!} \prod_{j\in[\kappa]} t_j! \cdot \prod_{j\in[\kappa]} \binom{\|\boldsymbol{x}^{(j)}\|}{t_j} \qquad (9) \\
&= S(X_{\boldsymbol{I}})(\|\boldsymbol{x}^{(1)}\|, \ldots, \|\boldsymbol{x}^{(\kappa)}\|) \ ,
\end{aligned}$$

where the equality in eq. (9) follows from eq. (7).

To conclude, it is then enough to observe that the statement we want to prove follows from eq. (8) restricting both sides of the equality by ρ. To prove this we use that $\sigma X_{\boldsymbol{I}}\restriction_\rho = \sigma(X_{\boldsymbol{I}}\restriction_\rho)$. ◀

5 Conclusions

The study of algebraic proof systems under Fourier encoding is still at its infancy. There are many natural questions about its size efficiency. We understand reasonably well the strength relation between resolution and PC in the Boolean encoding. Sokolov [34] stresses that we do not even know yet whether PC with $\{\pm 1\}$ simulates resolution or not.

We mentioned already that the study of κ-COLORING of graphs is a very natural application of PC with Fourier encoding. There are some degree lower bounds in literature [26], but size lower bounds are still unknown. Understanding size would allow to understand larger classes of algebraic algorithms for this problem.

Acknowledgements The authors would like to thank Albert Atserias for fruitful discussions.

References

1 Albert Atserias and Tuomas Hakoniemi. Size-degree trade-offs for sums-of-squares and positivstellensatz proofs. In Amir Shpilka, editor, *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA*, volume 137 of *LIPIcs*, pages 24:1–24:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019. `doi:10.4230/LIPIcs.CCC.2019.24`.

2 Albert Atserias and Joanna Ochremiak. Proof complexity meets algebra. *ACM Trans. Comput. Logic*, 20(1), December 2018.

3 Roberto J Bayardo Jr and Robert Schrag. Using CSP look-back techniques to solve real-world SAT instances. In *AAAI/IAAI*, pages 203–208, 1997.

4 Christoph Berkholz. The Relation between Polynomial Calculus, Sherali-Adams, and Sum-of-Squares Proofs. In Rolf Niedermeier and Brigitte Vallée, editors, *35th Symposium on Theoretical Aspects of Computer Science (STACS 2018)*, volume 96 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 11:1–11:14, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

5 Grigoriy Blekherman, João Gouveia, and James Pfeiffer. Sums of squares on the hypercube. *Mathematische Zeitschrift*, pages 1–14, 2016. `doi:10.1007/s00209-016-1644-7`.

6 Grigoriy Blekherman and Cordian Riener. Symmetric non-negative forms and sums of squares. *Discrete and Computational Geometry*, 65(3):764–799, May 2020. `doi:10.1007/s00454-020-00208-w`.

7 Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo, and Toniann Pitassi. Linear gaps between degrees for the polynomial calculus modulo distinct primes. *J. Comput. Syst. Sci.*, 62(2):267–289, 2001. `doi:10.1006/jcss.2000.1726`.

8 Matthew Clegg, Jeff Edmonds, and Russell Impagliazzo. Using the Gröbner basis algorithm to find proofs of unsatisfiability. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 174–183. ACM, 1996.

9 John Conway and A. Jones. Trigonometric diophantine equations (on vanishing sums of roots of unity). *Acta Arithmetica*, 30(3):229–240, 1976. URL: `http://dx.doi.org/10.4064/aa-30-3-229-240`, `doi:10.4064/aa-30-3-229-240`.

10 David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms : An Introduction to Computational Algebraic Geometry and Commutative Algebra, 3rd edition.* Springer, 2007.

11 Jesús A De Loera, J. Lee, S. Margulies, and S. Onn. Expressing combinatorial problems by systems of polynomial equations and Hilbert's Nullstellensatz. *Comb. Probab. Comput.*, 18(4):551–582, July 2009. URL: `http://dx.doi.org/10.1017/S0963548309009894`, `doi:10.1017/S0963548309009894`.

12 Jesús A De Loera, Jon Lee, Peter N Malkin, and Susan Margulies. Computing infeasibility certificates for combinatorial problems through Hilbert's Nullstellensatz. *Journal of Symbolic Computation*, 46(11):1260–1283, 2011.

13 Jesús A De Loera, Susan Margulies, Michael Pernpeintner, Eric Riedl, David Rolnick, Gwen Spencer, Despina Stasi, and Jon Swenson. Graph-coloring ideals: Nullstellensatz certificates, Gröbner bases for chordal graphs, and hardness of Gröbner bases. In *Proceedings of the 2015*

ACM on International Symposium on Symbolic and Algebraic Computation, pages 133–140. ACM, 2015.

14 Susanna F. de Rezende, Massimo Lauria, Jakob Nordström, and Dmitry Sokolov. The Power of Negative Reasoning. In *36th Computational Complexity Conference (CCC 2021)*, volume 200 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 40:1–40:24, 2021. doi:10.4230/LIPIcs.CCC.2021.40.

15 R. Dvornicich and U. Zannier. Sums of roots of unity vanishing modulo a prime. *Archiv der Mathematik*, 79(2):104–108, Aug 2002. URL: http://dx.doi.org/10.1007/s00013-002-8291-4, doi:10.1007/s00013-002-8291-4.

16 Roberto Dvornicich and Umberto Zannier. On sums of roots of unity. *Monatshefte für Mathematik*, 129(2):97–108, Feb 2000. URL: http://dx.doi.org/10.1007/s006050050009, doi:10.1007/s006050050009.

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

18 Dima Grigoriev. Tseitin's tautologies and lower bounds for Nullstellensatz proofs. In *39th Annual Symposium on Foundations of Computer Science, FOCS '98, November 8-11, 1998, Palo Alto, California, USA*, pages 648–652. IEEE Computer Society, 1998. doi:10.1109/SFCS.1998.743515.

19 R. Impagliazzo, P. Pudlák, and J. Sgall. Lower bounds for the polynomial calculus and the Gröbner basis algorithm. *Computational Complexity*, 8(2):127–144, Nov 1999.

20 Daniela Kaufmann, Paul Beame, Armin Biere, and Jakob Nordström. Adding dual variables to algebraic reasoning for gate-level multiplier verification. In *Proceedings of the 25th Design, Automation and Test in Europe Conference (DATE'22)*, 2022.

21 Daniela Kaufmann and Armin Biere. Nullstellensatz-proofs for multiplier verification. In *Computer Algebra in Scientific Computing - 22nd International Workshop, CASC 2020, Linz, Austria, September 14-18, 2020, Proceedings*, pages 368–389, 2020. doi:10.1007/978-3-030-60026-6_21.

22 Daniela Kaufmann, Armin Biere, and Manuel Kauers. Verifying large multipliers by combining SAT and computer algebra. In *2019 Formal Methods in Computer Aided Design, FMCAD 2019, San Jose, CA, USA, October 22-25, 2019*, pages 28–36, 2019. doi:10.23919/FMCAD.2019.8894250.

23 Daniela Kaufmann, Armin Biere, and Manuel Kauers. From DRUP to PAC and back. In *2020 Design, Automation & Test in Europe Conference & Exhibition, DATE 2020, Grenoble, France, March 9-13, 2020*, pages 654–657, 2020. doi:10.23919/DATE48585.2020.9116276.

24 T.Y Lam and K.H Leung. On vanishing sums of roots of unity. *Journal of Algebra*, 224(1):91–109, 2000.

25 J. Lasserre. An explicit exact SDP relaxation for nonlinear 0-1 programs. *Integer Programming and Combinatorial Optimization*, pages 293–303, 2001.

26 Massimo Lauria and Jakob Nordström. Graph Colouring is Hard for Algorithms Based on Hilbert's Nullstellensatz and Gröbner Bases. In *32nd Computational Complexity Conference (CCC 2017)*, volume 79, pages 2:1–2:20, 2017. URL: http://drops.dagstuhl.de/opus/volltexte/2017/7541, doi:10.4230/LIPIcs.CCC.2017.2.

27 Troy Lee, Anupam Prakash, Ronald de Wolf, and Henry Yuen. On the sum-of-squares degree of symmetric quadratic functions. In *31st Conference on Computational Complexity*, volume 50 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 17, 31. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2016.

28 João P. Marques-Silva and Karem A. Sakallah. GRASP: A search algorithm for propositional satisfiability. *Computers, IEEE Transactions on*, 48(5):506–521, 1999.

29 M.W. Moskewicz, C.F. Madigan, Y. Zhao, L. Zhang, and S. Malik. Chaff: Engineering an efficient SAT solver. In *Proceedings of the 38th annual Design Automation Conference*, pages 530–535. ACM, 2001.

30 Pablo A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical programming*, 96(2):293–320, 2003.

31 Aaron Potechin. Sum of Squares Bounds for the Ordering Principle. In Shubhangi Saraf, editor, *35th Computational Complexity Conference (CCC 2020)*, volume 169 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 38:1–38:37, Dagstuhl, Germany, 2020. Schloss Dagstuhl–Leibniz-Zentrum für Informatik. URL: `https://drops.dagstuhl.de/opus/volltexte/2020/12590`, `doi:10.4230/LIPIcs.CCC.2020.38`.

32 Grant Schoenebeck. Linear level Lasserre lower bounds for certain k-CSPs. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 593–602. IEEE Computer Society, 2008. `doi:10.1109/FOCS.2008.74`.

33 Roman Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In Alfred V. Aho, editor, *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 77–82. ACM, 1987. `doi:10.1145/28395.28404`.

34 Dmitry Sokolov. (Semi)Algebraic proofs over $\{\pm 1\}$ variables. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*. ACM, jun 2020.

35 Madhur Tulsiani. CSP gaps and reductions in the Lasserre hierarchy. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 303–312. ACM, 2009. `doi:10.1145/1536414.1536457`.