comput. complex. (2023) 32:12

1016-3328/23/020001-45
published online November 12, 2023
https://doi.org/10.1007/s00037-023-00242-z

computational complexity

ON VANISHING SUMS OF ROOTS OF UNITY IN POLYNOMIAL CALCULUS AND SUM-OF-SQUARES

Ilario Bonacina, Nicola Galesi, and Massimo Lauria

Abstract. We introduce a novel take on sum-of-squares that is able to reason with complex numbers and still make use of polynomial inequalities. This proof system might be of independent interest since it allows to represent multivalued domains both with Boolean and Fourier encoding. We show degree and size lower bounds in this system for a natural generalization of knapsack: the vanishing sums of roots of unity. These lower bounds naturally apply to polynomial calculus as-well.

Keywords. polynomial calculus, sum-of-squares, roots of unity, knapsack

Subject classification. 03F20, 68T15.

1. Introduction

Problems in combinatorics, constraint satisfaction, arithmetic circuit design, or algebra, can be formalized in a variety of languages. The popular propositional logic approach, based on the *Conflict-Driven-Clause-Learning* SAT solvers (Bayardo Jr & Schrag 1997; Marques-Silva & Sakallah 1999; Moskewicz *et al.* 2001), fails to exploit the algebraic structure of the problem and often resorts to inefficient brute-force.

Maintaining the algebraic representation allows to use Hilbert's Nullstellensatz, Gröbner basis computation, or semidefinite

programming (Cox *et al.* 2007; Lasserre 2001; Parrilo 2003). These tools have been successful in practice, for instance to solve κ-COLORING (De Loera *et al.* 2009, 2011, 2015) and to verify arithmetic multiplier circuits (Kaufmann & Biere 2020; Kaufmann *et al.* 2019, 2020).

CSP problems over domains of size κ, e.g. κ-COLORING, can be naturally represented using either the *Fourier encoding* or the *Boolean encoding*. The Fourier encoding 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. The Boolean encoding uses $\{0,1\}$-valued indicator variables $x_1, \ldots, x_\kappa$, equipped with the additional constraint $x_1 + \cdots + x_\kappa = 1$.

A good encoding is essential to leverage the algebraic structure of a problem: even simple variations may give significant speedups both in theory and in practice (Kaufmann *et al.* 2022; de Rezende *et al.* 2021).

In this paper, 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.

We focus on *polynomial calculus* and *sum-of-squares* proof systems. Polynomial calculus is a well-studied proof system that captures Hilbert's Nullstellensatz and Gröbner basis computations, and certifies the unsatisfiability of sets of polynomial equations (Buss *et al.* 2001). Sum-of-squares certifies 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 constraints $\{p = 0 : p \in P\} \cup \{h \geq 0 : h \in H\}$ 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. Sum-of-squares p-simulates polynomial calculus over the reals on $\{0,1\}$-valued and $\{\pm 1\}$-valued variables (Berkholz 2018; Sokolov 2020).

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 with complex coefficients. As in the real case $\mathsf{SoS}_{\mathbb{C}}$ p-simulates $\mathsf{PC}_{\mathbb{C}}$, see Section 2 for more details.

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 *size* of the proof measured as number of monomials involved in the whole proof when polynomials are written explicitly as sums of monomials. The degree is a very rough measure of the proof search space, and 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 such as the *Smolensky's method* in circuit complexity. Smolensky (1987) 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 (1998) and Buss *et al.* (2001) for the Tseitin principle over p-valued variables and the MOD_p principles.

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 (Atserias & Ochremiak 2018; Grigoriev 2001; Potechin 2020; Schoenebeck 2008; Tulsiani 2009). Over Boolean variables a strong degree lower bound implies immediately a size

lower bounds thanks to degree-size trade-offs: if a set of polynomials *over Boolean variables* has no refutation of degree at most D, then it has no refutation containing less than $2^{\Omega(\frac{(D-d)^2}{n})}$ monomials (Atserias & Hakoniemi 2019; Impagliazzo *et al.* 1999).

No such result exists for Fourier variables. Indeed, Tseitin contradictions over $\{0,1\}$-valued variables 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 $\{\pm 1\}$-valued variables (Buss *et al.* 2001).

To the best of our knowledge, the first size lower bounds in $\mathsf{PC}/\mathsf{SoS}_{\mathbb{R}}$ for polynomials with $\{\pm 1\}$-valued variables are proved by Sokolov (2020) for the pigeonhole principle and random 11-CNFs. Moreover, (Sokolov 2020) gives a technique to turn strong degree lower bounds to strong size lower bounds via the composition 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 the KNAPSACK problem.

The classical KNAPSACK problem corresponds to the set of polynomials

$$\left\{ \sum_{i=1}^{n} c_i x_i - r \ , \quad x_1^2 - x_1, \ldots, x_n^2 - x_n \right\}, \tag{1.1}$$

where $r, c_1, \ldots, c_n \in \mathbb{C}$.

KNAPSACK requires a linear degree to be refuted in PC (Impagliazzo *et al.* 1999, Theorem 5.1) regardless of the coefficients $r, c_1, \ldots, c_n \in \mathbb{R}$.

Grigoriev (2001) showed that, when all the c_is are 1 and $r \in \mathbb{R}$, KNAPSACK requires degree at least $\min\{2\lfloor \min\{r, n-r\} \rfloor + 3, n\}$ to be refuted in $\mathsf{SoS}_{\mathbb{R}}$.

Size lower bounds follow via the respective size-degree trade-offs.

1.1. 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

$$\mathsf{SRU}_n^{\kappa,r} := \Big\{ \sum_{i\in[n]} z_i - r,\ z_1^\kappa - 1, \ldots, z_n^\kappa - 1 \Big\}. \tag{1.2}$$

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 (Conway & Jones 1976), and have been extensively studied in the literature, for instance (Dvornicich & Zannier 2002, 2000).

When κ divides n, $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable, because the κth roots of unity sum to zero. For κ that is a power of a prime number p this is indeed the only possibility (Proposition 2.2 in Section 2). Lam & Leung (2000) proved a complete characterization of when $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable. In particular, when κ is not a power of a prime 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.

1.2. 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. A preliminary version of this work appeared in the proceedings of MFCS'22 (Bonacina *et al.* 2022).

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 Grigoriev (2001) lower bound extends 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 1.3 (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 *et al.* (1999, Theorem 5.1) proved a linear degree lower bound for KNAPSACK and therefore $\mathsf{SRU}_n^{2,r}$ for any r (see Section 3). 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 2.4. 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 1.3), first we construct a candidate pseudo-expectation based on the symmetries of $\mathsf{SRU}_n^{\kappa,r}$. Then, we prove its correctness, following a generalization to $\mathsf{SoS}_{\mathbb{C}}$ of the approach by Blekherman *et al.* (2016) and Blekherman & Riener (2020) as presented in (Lee *et al.* 2016, Theorem B.11).

We also prove a size lower bound for $\mathsf{SRU}_n^{\kappa,0}$ in $\mathsf{SoS}_{\mathbb{C}}$. The lift of degree lower bounds to size lower bounds on κ-valued Fourier variables generalizes the lifting approach due to Sokolov (2020) on real valued polynomials and $\{\pm 1\}$-variables.

THEOREM 1.4 (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 $2^{o(n)}$.*

For $\kappa = 2$, Theorem 1.4 follows easily from Sokolov's (2020) techniques and Grigoriev's (2001) degree lower bound for KNAPSACK.

For $\kappa > 2$, Theorem 1.4 requires some non-trivial generalization of the lifting technique from (Sokolov 2020). This generalization is Theorem 4.10 in Section 4.

Theorem 1.3 and Theorem 1.4 also hold for $\mathsf{PC}_{\mathbb{C}}$, since $\mathsf{SoS}_{\mathbb{C}}$ simulates $\mathsf{PC}_{\mathbb{C}}$.

1.3. Related works. Recently and independently of us, Impagliazzo *et al.* (2022) generalized Sokolov's (2020) approach for proving size and degree lower bounds in PC to the case of $\mathsf{PC}_{\mathbb{C}}$ equipped with certain limited extension axioms and where variables are taking values in the κth roots of unity. They prove lower bounds in $\mathsf{PC}_{\mathbb{C}}$ with limited extensions for unsatisfiable systems of random linear equations lifted by certain hardness functions.

Our results on the vanishing root principle $\mathsf{SRU}_n^{\kappa,r}$ are incomparable with the results from (Impagliazzo *et al.* 2022). First, $\mathsf{SRU}_n^{\kappa,r}$ is a generalization of the KNAPSACK problem and, to our knowledge, not related or reducible in $\mathsf{PC}_{\mathbb{C}}$ to the case of random linear equations, even adding to $\mathsf{PC}_{\mathbb{C}}$ the extra limited extension axioms used in (Impagliazzo *et al.* 2022). Furthermore, one of the main results in our work is the degree lower bound for $\mathsf{SRU}_n^{\kappa,0}$ in $\mathsf{SoS}_{\mathbb{C}}$, while the same degree lower bound for $\mathsf{PC}_{\mathbb{C}}$ follows essentially as a corollary of known results.

$\mathsf{SoS}_{\mathbb{C}}$ and $\mathsf{PC}_{\mathbb{C}}$ proofs deal with arbitrary polynomial systems rather than simply encodings of CNF formulas. In the literature, several algebraic proof systems extending PC were considered, among these the Ideal Proof System (IPS) from (Grochow & Pitassi 2018), the Cone Proof System (CPS) from (Alekseev *et al.* 2020), a version of PC working with bounded k-conjunctions (Galesi & Lauria 2010), and a version of PC working with depth-d algebraic circuits (Grigoriev & Hirsch 2003; Impagliazzo *et al.* 2020).

IPS and CPS are, at least on variables taking Boolean values, strictly stronger than PC and SoS (Grochow & Pitassi (2018)). Interestingly to this work, the complexity of proofs for IPS and CPS was studied by using a particular subset-sum principle, the Binary Value Principle (BVP) expressing the fact that natural numbers written in binary cannot be negative. Moving from a technique of Forbes *et al.* (2021), Alekseev *et al.* (2020) proved that the BVP is conditionally hard to refute in IPS modulo the Shub-Smale conjecture on the hardness of computing factorials. Alekseev *et al.* (2020) prove lower bounds on the magnitude of the coefficients and this is completely different from the techniques developed in this article. Despite being seemingly hard for a strong proof system like IPS, the binary value principle is easy to refute in $\mathsf{SoS}_{\mathbb{C}}$, contrary to other subset-sum principles. Hence, to the best of our knowledge, no immediate relation can be drawn between our results and the previous results on BVP.

1.4. Structure of the paper. In the next section, we give the necessary preliminaries on roots of unity and the formal definition of $\mathsf{SoS}_{\mathbb{C}}$. The proof of the main degree lower bound (Theorem 1.3) is in *Section 3*. In *Section 4*, we lift degree lower bounds to size

lower bounds for sets of polynomials over the roots of unity and we prove Theorem 1.4. The main technical ingredient of this proof is Theorem 4.8. Its proof is deferred to *Section 5*.

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 usually denote with $\boldsymbol{x}$ Boolean variables, with $\boldsymbol{z}$ κ-valued Fourier 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 $\mathbb{C}[\boldsymbol{y}]$.

2.1. Vanishing sums of roots of unity. For $\kappa \in \mathbb{N}$, a *κth root of unity* is a root of the polynomial $X^\kappa - 1$. All the roots of unity except 1 are also roots of the polynomial $1 + X + \cdots + X^{\kappa-1}$, indeed $X^\kappa - 1 = (X-1) \cdot (1 + X + \cdots + X^{\kappa-1})$. 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 $\mathrm{e}^{2\pi i/\kappa}$, 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.

The κth *cyclotomic polynomial* is the unique irreducible univariate polynomial in $\mathbb{Z}[X]$ that divides $X^\kappa - 1$ and does not divides $X^{\kappa'} - 1$ for any $\kappa' \in [\kappa - 1]$. The κth cyclotomic polynomial is denoted as $\Phi_\kappa(X)$. If κ is prime, then

$$\Phi_\kappa(X) = 1 + X + \cdots + X^{\kappa-1}.$$

Proposition 2.1. *Let κ be a prime number. The set of polynomials $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable over $\mathbb{C}$ if and only if $\kappa \mid n$.*

PROOF. Let ζ be a primitive κth root of unity. That is ζ is a root of the κth cyclotomic polynomial $\Phi_\kappa(X)$. If $\kappa \mid n$, say $n = \kappa \cdot a$, then a solution is trivial to construct:

$$\underbrace{1+\cdots+1}_{a}+\underbrace{\zeta+\cdots+\zeta}_{a}+\cdots+\underbrace{\zeta^{\kappa-1}+\cdots+\zeta^{\kappa-1}}_{a}=a\Phi_\kappa(\zeta)=0.$$

Suppose now the set of polynomials $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable over $\mathbb{C}$. Let $y_1, \ldots, y_n$ be a solution. For $j = 0, \ldots, \kappa - 1$, let

$$\alpha_j = |\{\ell \in [n] \ : \ y_\ell = \zeta^j\}|.$$

From the definition, it follows immediately that $\sum_{j=0}^{\kappa-1} \alpha_j = n$ and that for some $j > 0$, $\alpha_j \neq 0$.

That is, ζ is a root of the polynomial $p(X) = \sum_{j=0}^{\kappa-1} \alpha_j X^j$, but then ζ is also a root of $p(X) - \alpha_{\kappa-1}\Phi_\kappa(X) = \sum_{j=0}^{\kappa-2}(\alpha_j - \alpha_{\kappa-1})X^j$. This polynomial has degree strictly less than $\kappa-1$ and hence it must be identically 0, i.e. $\alpha_0 = \alpha_1 = \cdots = \alpha_{\kappa-1}$. Since $\sum_{j=0}^{\kappa-1} \alpha_j = n$ this implies $\kappa \mid n$. □

If $\kappa = p^m$ for some prime p and integer m, then the κth cyclotomic polynomial is

$$\Phi_\kappa(X) = 1 + X^{p^{m-1}} + X^{2p^{m-1}} + \cdots + X^{(p-1)p^{m-1}}.$$

Using this fact, it is immediate to generalize the proof of Proposition 2.1 to κ power of a prime.

PROPOSITION 2.2. *Let κ be a power of a prime number p. The set of polynomials $\mathsf{SRU}_n^{\kappa,0}$ is satisfiable over $\mathbb{C}$ if and only if $p \mid n$.*

2.2. Proof systems. The proof systems of interest in this work are polynomial calculus and a variant of Sum-of-Squares designed to deal with complex numbers and complex roots of unity.

2.2.1. Polynomial calculus (PC) over $\mathbb{C}$. Given a set of polynomials $P \subset \mathbb{C}[\boldsymbol{y}]$ and $q \in \mathbb{C}[\boldsymbol{y}]$, a refutation of P in *polynomial calculus over* $\mathbb{C}$, denoted as $\mathsf{PC}_\mathbb{C}$, is a sequence of polynomials $p_1, \ldots, p_s$ in $\mathbb{C}[\boldsymbol{y}]$ such that $p_s = 1$, and each p_i is either

1. a polynomial from the set P;

2. $y_j \cdot p_k$ for some variable y_j and some $k < i$; or

3. a linear combination $\alpha p_j + \beta p_k$ for $j, k < i$ and $\alpha, \beta \in \mathbb{C}$.

The *degree* of the refutation is $\max_i\{\deg(p_i)\}$ and the size of the refutation is the sum of the number of monomials among all p_is.

2.3. Sum-of-Squares (SoS) over $\mathbb{C}$. 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 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^*: we call it *formal conjugate* of p. To have such polynomial representation, 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 t, the conjugate $(z^t)^*$ is $z^{\kappa\lceil t/\kappa\rceil - t}$. In particular when $0 < t < \kappa$ the conjugate of z^t is $z^{\kappa - t}$. For example consider $\kappa = 7$, then z^3 is the conjugate of z^4, z^{11}, z^{18}, ...

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 2.3 (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*

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

where $s \in S$ 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.

To further clarify the notion of $\mathsf{SoS}_{\mathbb{C}}$ and formal conjugates consider the following examples.

Example 2.4. Let $\underline{i}$ be the imaginary unit in $\mathbb{C}$, i.e. $\underline{i}^2 = -1$ and $r \in \mathbb{C} \setminus \mathbb{R}$, that is $r = a + \underline{i}b$ with $a, b \in \mathbb{R}$ and $b \neq 0$. The set of polynomials

$$\{\sum_{j \in [n]} c_j x_j - r, \ x_1^2 - x_1, \ldots, \ x_n^2 - x_n\},$$

when all c_j's are real, has a simple $\mathsf{SoS}_{\mathbb{C}}$ refutation:

$$-b^2 = -(\sum_{j \in [n]} c_j x_j - a - \underline{i}b)(\sum_{j \in [n]} c_j x_j - a + \underline{i}b) + (\sum_{j \in [n]} c_j x_j - a)^2,$$

that is, the set of polynomials corresponding to knapsack in eq. (1.1) when $r \in \mathbb{C} \setminus \mathbb{R}$ and all c_is are real always has small $\mathsf{SoS}_{\mathbb{C}}$ refutations. ◊

Impagliazzo *et al.* (1999, Theorem 5.1) proved that the previous set of polynomials, when $r \in \mathbb{R}$, is hard for $\mathsf{PC}_{\mathbb{C}}$, but their argument also works for $r, c_1, \ldots, c_n \in \mathbb{C}$.

Now we give an example over the Fourier encoding.

Example 2.5. As a second example we consider a set of polynomials saying that a sum of n Fourier variables equals $2n+1$. This is the set of polynomials

$$\{\sum_{j\in[n]} z_j - 2n - 1,\ z_1^\kappa - 1, \ldots,\ z_n^\kappa - 1\}.$$

This has a simple $\mathsf{SoS}_{\mathbb{C}}$ refutation:

$$\begin{aligned} -1 = &\left(1 - \frac{\sum_{j\in[n]} z_j^{\kappa-1}}{2n+1}\right)\left(\sum_{j\in[n]} z_j - 2n - 1\right) \\ &+ \sum_{j\in[n]} (1-z_j)(1-z_j^{\kappa-1}) \\ &+ \frac{1}{2n+1}\left(\sum_{j\in[n]} z_j\right)\left(\sum_{j\in[n]} z_j^{\kappa-1}\right). \end{aligned}$$ ◊

These examples hint that $\mathsf{SoS}_{\mathbb{C}}$ is strictly stronger than $\mathsf{PC}_{\mathbb{C}}$, indeed in presence of the axioms $z_i^\kappa - 1$, $\mathsf{SoS}_{\mathbb{C}}$ p-simulates $\mathsf{PC}_{\mathbb{C}}$, that is $\mathsf{PC}_{\mathbb{C}}$ refutations can be efficiently converted to $\mathsf{SoS}_{\mathbb{C}}$ refutations.

Proposition 2.6. *Let $\boldsymbol{z} = (z_1, \ldots, z_n)$ and let $P \subseteq \mathbb{C}[\boldsymbol{z}]$. For any $\kappa \geq 2$, if there is a $\mathsf{PC}_{\mathbb{C}}$ refutation of $P \cup \{z_j^\kappa - 1 :\ j \in [n]\}$ of size s and degree d, then there is a $\mathsf{SoS}_{\mathbb{C}}$ refutation of $P \cup \{z_j^\kappa - 1 :\ j \in [n]\}$ of degree $2d$ and size $s^{O(1)}$.*

The proof is a simple modification of Lemma 3.1 in (Berkholz 2018) and of an analogous result in (Sokolov 2020). We include it here for completeness.

Proof. Let $p_1, \ldots, p_\tau$ the $\mathsf{PC}_{\mathbb{C}}$ refutation of $P \cup \{z_j^\kappa - 1 :\ j \in [n]\}$. By induction over $t \leq \tau$, we show that there is a $\mathsf{SoS}_{\mathbb{C}}$ proof of $-p_t p_t^*$ of size $s^{O(1)}$ and degree $2d$. This produces an efficient simulation because $-p_\tau p_\tau^* = -1$. Formally, for each polynomial p_t in the polynomial calculus proof, we build an $\mathsf{SoS}_{\mathbb{C}}$ proof

$$\sum_{p\in P} (-a_{t,p} p^*) p + \sum_{i\leq t} c_{i,t} q_i q_i^* + Z_t = -p_t p_t^*,$$

where $a_{t,p}$ and $c_{i,t}$ are real numbers, $c_{i,t} \geq 0$, q_i are polynomials in $\mathbb{C}[\boldsymbol{z}]$, and Z_t is a polynomial in the ideal $\langle z_j^\kappa - 1 : \ j \in [n]\rangle$. We consider different cases, depending on which rule was originally used to derive p_t.

If $p_t \in P$ then $-p_t^* p_t$ is a valid $\mathsf{SoS}_\mathbb{C}$ proof in this form because $p_t^* p_t = p_t p_t^*$.

If $p_t = z_j^\kappa - 1$, then $-p_t^* p_t$ is a valid $\mathsf{SoS}_\mathbb{C}$ proof in this form since $-p_t^* p_t \in Z_t$.

If $p_t = z_j p_{t'}$ for some $j \in [n]$ and $t' < t$ observe that

$$-p_t p_t^* = -z_j p_{t'} z^{\kappa-1} p_{t'}^* = -p_{t'} p_{t'}^* + (1 - z_j^\kappa) p_{t'} p_{t'}^*$$

and by induction hypothesis $-p_{t'} p_{t'}^*$ has an $\mathsf{SoS}_\mathbb{C}$ proof of the desired form.

The remaining case is when $p_t = \alpha p_u + \beta p_v$ for $u, v < t$ and $\alpha, \beta \in \mathbb{C}$. By induction we have

$$\sum_{p \in P} (-a_{u,p} \cdot p^*) p + \sum_{i \leq u} c_{u,i} q_i q_i^* + Z_u = -p_u \cdot p_u^*$$
$$\sum_{p \in P} (-a_{v,p} \cdot p^*) p + \sum_{i \leq v} c_{v,i} q_i q_i^* + Z_v = -p_v \cdot p_v^*$$

We do a positive combination of the two proofs. We set

$$\begin{aligned} a'_{t,p} &= 2|\alpha|^2 a_{u,p} + 2|\beta|^2 a_{v,p} \\ c'_{t,i} &= 2|\alpha|^2 c_{u,i} + 2|\beta|^2 c_{v,i} \\ Z_t &= 2|\alpha|^2 Z_u + 2|\beta|^2 Z_v \end{aligned}$$

and get

$$\sum_{p \in P} (-a'_{t,p} \cdot p^*) p + \sum_{i \leq t-1} c'_{t,i} q_i q_i^* + Z_t = -2|\alpha|^2 p_u \cdot p_u^* - 2|\beta|^2 p_v \cdot p_v^* \,. \tag{2.7}$$

We set $q_t := \alpha p_u - \beta p_v$ and observe that

$$q_t q_t^* = (\alpha p_u - \beta p_v)(\alpha p_u - \beta p_v)^* \tag{2.8}$$
$$= 2|\alpha|^2 p_u p_u^* + 2|\beta|^2 p_v p_v^* - (\alpha p_u + \beta p_v)(\alpha p_u + \beta p_v)^* \tag{2.9}$$
$$= 2|\alpha|^2 p_u p_u^* + 2|\beta|^2 p_v p_v^* - p_t p_t^* \,. \tag{2.10}$$

Summing (2.11) and (2.8) and setting $c_{t,t} = 1$ we get

$$\sum_{p\in P}(-a'_{t,p}\cdot p^*)p + \sum_{i\le t} c'_{t,i}q_i q_i^* + Z_t = -p_t\cdot p_t^*\ . \tag{2.11}$$

Now we discuss size and degree of the proof we just built. Notice immediately that the polynomial Z_t is in a binomial ideal, i.e. all generators have at most two monomials. For this reason, it is immediate to see that the number of monomials in Z_t is rest of the proof. Likewise the degree of Z_t is at most the degree of the rest of the proof. Now we focus on the degree and size of the various q_i. By construction, each of them has degree at most d and the size at most twice the size of the largest polynomial in the original proof. Hence, the proof has degree at most $2d$ and size at most $s^{O(1)}$.

So far we argued about degree and monomial size, and now we discuss the size of the coefficients. We define M to be the smallest integer so that for any coefficient c occurring in the polynomial calculus proof, we have $\frac{1}{M} \le 4|c|^2 \le M$. Observe that at each step in our construction, the coefficients are multiplied by a factor $2|\alpha|^2+2|\beta|^2$, for some α and β which are coefficients in the original proof, thus we have $\frac{1}{M} \le 2|\alpha|^2 + 2|\beta|^2 \le M$. By the end of the proof, all coefficients are between $\frac{1}{M^\tau}$ and M^τ, and therefore have binary representation of length which is polynomial with respect to the size of the original coefficients, and to the length of the proof. □

3. Degree lower bounds

We first prove a degree lower bound for a weighted version of $\mathsf{SRU}_n^{\kappa,r}$ in polynomial calculus. This is not hard: the lower bound essentially is implied by the knapsack lower bound in polynomial calculus.

Theorem 3.1. *Let $c_1,\dots,c_n \in \mathbb{C}\setminus\{0\}$, $r\in\mathbb{C}$ and $\kappa\in\mathbb{N}$. The set of polynomials*

$$\Big\{\sum_{i=1}^n c_i z_i - r,\ z_1^\kappa - 1,\dots,z_n^\kappa - 1\Big\} \tag{3.2}$$

has no refutations of degree smaller than $\lfloor\frac{n}{2}\rfloor$ in $\mathsf{PC}_\mathbb{C}$.

PROOF. Let ζ be a primitive κth root of unity. If the set of polynomials in (3.2) is satisfiable, then the degree lower bound is obviously true. Suppose then it is unsatisfiable. This means the set of polynomials

$$\left\{ \sum_{i=1}^{n} c_i z_i - r, (z_1 - 1)(z_1 - \zeta), \ldots, (z_n - 1)(z_n - \zeta) \right\} \tag{3.3}$$

is unsatisfiable too. To prove a degree lower bound for the $\mathsf{PC}_{\mathbb{C}}$-refutations of (3.2) is then enough to prove a degree lower bound for the $\mathsf{PC}_{\mathbb{C}}$-refutations of (3.3).

Now, the set of polynomials in (3.3) is unsatisfiable if and only if the set of polynomials

$$\left\{ \sum_{i=1}^{n} c_i x_i - \frac{r - \sum_{i\in[n]} c_i}{\zeta - 1}, x_1^2 - x_1, \ldots, x_n^2 - x_n \right\} \tag{3.4}$$

is unsatisfiable. Moreover, via a linear transformation we can transform $\mathsf{PC}_{\mathbb{C}}$-refutations of (3.3) into $\mathsf{PC}_{\mathbb{C}}$-refutations of (3.4) and viceversa. The linear transformation is $z_i = x_i(\zeta - 1) + 1$. This transformation does not preserve the size $\mathsf{PC}_{\mathbb{C}}$-refutations but, being linear, it preserves the degree. By Theorem 5.1 in (Impagliazzo *et al.* 1999)[1] applied with $m = \frac{r - \sum_{i\in[n]} c_i}{\zeta - 1}$ we get the desired degree lower bound for (3.4) and hence for (3.3) and (3.2). □

Notice that, the lower bound in Theorem 3.1 also holds if instead of $z_1^\kappa - 1, \ldots, z_n^\kappa - 1$, we have $p(z_0), \ldots, p(z_n)$ where p is an arbitrary univariate polynomial with at least two distinct roots.

The rest of the section is to prove the degree lower bound for $\mathsf{SRU}_n^{\kappa,r}$ in $\mathsf{SoS}_{\mathbb{C}}$ (Theorem 1.3).

3.1. High level structure of the argument. To show a $\mathsf{SoS}_{\mathbb{C}}$ degree-d lower bound for some set of polynomials P, it is enough to construct a degree-d *pseudo-expectation* for P. That is a linear operator $\tilde{\mathbb{E}} : \mathbb{C}[\boldsymbol{x}] \to \mathbb{C}$ such that

[1] We recall that the theorem was originally stated for real numbers, but it holds for complex numbers, too.

- $\tilde{\mathbb{E}}(1) = 1$,
- $\tilde{\mathbb{E}}(mp) = 0$, for every $p \in P$ and m monomial such that $\deg(p) + \deg(m) \leq d$,
- $\tilde{\mathbb{E}}(s \cdot s^*) \in \mathbb{R}_{\geq 0}$, for every polynomial s s.t. $\deg(s \cdot s^*) \leq d$.

It is immediate 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 $\mathsf{SoS}_{\mathbb{C}}$.

It turns out it is easier to construct a pseudo-expectation for a Boolean encoding of $\mathsf{SRU}_n^{\kappa,r}$. This Boolean encoding is $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$.

First, we show (Proposition 3.6) that the degree needed to refute $\mathsf{SRU}_n^{\kappa,r}$ in PC and $\mathsf{SoS}_{\mathbb{C}}$ is at least the degree needed to refute $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$.

Secondly, we construct a pseudo-expectation for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ and this implies a $\mathsf{SoS}_{\mathbb{C}}$ lower bound both for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ and $\mathsf{SRU}_n^{\kappa,r}$.

After imposing some natural symmetry assumption there is only one candidate pseudo-expectation $\tilde{\mathbb{E}}$ for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ satisfying the first two properties of the definition of pseudo-expectation (Theorem 3.10). To show that the candidate pseudo-expectation satisfies also the third property is more involved but it follows some standard structure of the arguments used to construct pseudo-expectations in the context of $\mathsf{SoS}_{\mathbb{R}}$.

3.2. A Boolean encoding of $\mathsf{SRU}_n^{\kappa,r}$. We consider a Boolean encoding of the sums of roots of unity. This is the set $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ consisting of the following polynomials for every $i \in [n]$ and $j \in [\kappa]$

$$\sum_{i\in[n]} \Big(\sum_{j\in[\kappa]} \zeta^{j-1} x_{ij} \Big) - r,\ x_{ij}^2 - x_{ij},\ \sum_{j\in[\kappa]} x_{ij} - 1 \tag{3.5}$$

The set of polynomials $\mathsf{SRU}_n^{\kappa,r}$ uses variables taking values in Ω_κ, while the encoding in eq. (3.5) uses indicator variables to select the appropriate power of ζ. To prove Theorem 1.3, it is enough to prove the degree lower bound for $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$.

PROPOSITION 3.6. *The degree needed to refute* $\mathsf{SRU}_n^{\kappa,r}$ *in* $\mathsf{PC}_{\mathbb{C}}$ *(resp.* $\mathsf{SoS}_{\mathbb{C}}$*) is at least the degree needed to refute* $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ *in* $\mathsf{PC}_{\mathbb{C}}$ *(resp.* $\mathsf{SoS}_{\mathbb{C}}$*).*

PROOF. (sketch) Take a refutation of $\mathsf{SRU}_n^{\kappa,r}$ of degree D. Necessarily $\kappa \leq D$. We want to argue that $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ has a refutation of degree D, as well. To avoid ambiguity, we consider $\mathsf{SRU}_n^{\kappa,r}$ defined on variables $\boldsymbol{z}$ and $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ on variables $\boldsymbol{x}$. We apply the linear substitution

$$z_i \mapsto \sum_{j\in[\kappa]} \zeta^{j-1} x_{ij},$$

to the degree D refutation of $\mathsf{SRU}_n^{\kappa,r}$. We get a refutation of degree D of the resulting set of polynomials. It is sufficient to show we can infer these polynomials in low degree $\mathsf{PC}_{\mathbb{C}}$ from the axioms of $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$. Indeed, from $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$, we can easily infer $x_{ij}x_{ij'} = 0$ for each $i \in [n]$ and $j \neq j' \in [\kappa]$; hence, we have

$$\Big(\sum_{j\in[\kappa]} \zeta^{j-1} x_{ij}\Big)^{\kappa} =_{\mathsf{PC}} \sum_{j\in[\kappa]} \zeta^{(j-1)k} x_{ij}^{\kappa} =_{\mathsf{PC}} \sum_{j\in[\kappa]} x_{ij} =_{\mathsf{PC}} 1,$$

where with $p =_{\mathsf{PC}} q$ we mean that $p - q$ is derivable in PC. The whole derivation of $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ has degree D. □

3.3. Notation. 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 $\boldsymbol{x}^{(j)} = (x_{1j}, \ldots, x_{nj})$. That is, $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ is a set of polynomials in $\mathbb{C}[\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(\kappa)}]$. Given a tuple of sets $\boldsymbol{I} = (I_1, \ldots, I_\kappa)$, where $I_j \subseteq [n]$, let $|\boldsymbol{I}| = (|I_1|, \ldots, |I_\kappa|)$ and 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 $\sum_{i\in[n]} x_{ij}$.

Given a variable X and $t \in \mathbb{N}$, let $\binom{X}{t}$ be the univariate polynomial

$$\frac{X(X-1)\cdots(X-t+1)}{t!}.$$

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

LEMMA 3.7. *Given a vector of variables* $\boldsymbol{y} = (y_1, \ldots, y_m)$, *we have that*

$$\binom{\|\boldsymbol{y}\|}{t} \equiv \sum_{\substack{I \subseteq [n] \\ |I|=t}} Y_I.$$

PROOF. To prove the equality proceed by induction on t. The base case $t = 1$ is immediate: $\binom{\|\boldsymbol{y}\|}{1} = \|\boldsymbol{y}\| = \sum_{i \in [n]} y_i$. For $t > 1$,

$$\sum_{i \in [n]} y_i \sum_{\substack{I \subseteq [n] \\ |I|=t-1}} Y_I \equiv t \sum_{\substack{I \subseteq [n] \\ |I|=t}} Y_I + (t-1) \sum_{\substack{I \subseteq [n] \\ |I|=t-1}} Y_I.$$

That is, using the inductive hypothesis,

$$\|\boldsymbol{y}\| \binom{\|\boldsymbol{y}\|}{t-1} \equiv t \sum_{\substack{I \subseteq [n] \\ |I|=t}} Y_I + (t-1) \binom{\|\boldsymbol{y}\|}{t-1},$$

and therefore

$$\sum_{\substack{I \subseteq [n] \\ |I|=t}} Y_I \equiv \frac{\|\boldsymbol{y}\| - t + 1}{t} \binom{\|\boldsymbol{y}\|}{t-1} = \binom{\|\boldsymbol{y}\|}{t}. \qquad \square$$

3.4. The candidate pseudo-expectation. A potential satisfying assignment of $\mathsf{bool\text{-}SRU}_n^{\kappa,r}$ consists of $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_\kappa)$, the allocation of the n roots of unity in the directions $\zeta^0, \ldots, \zeta^{\kappa-1}$. 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 intuition leads to the definitions

$$\begin{cases} \gamma_1 = \frac{n-r_1-r_2}{\kappa} + r_1, \\ \gamma_2 = \frac{n-r_1-r_2}{\kappa} + r_2, \\ \gamma_j = \frac{n-r_1-r_2}{\kappa} \quad \text{for } j \geq 3. \end{cases} \tag{3.8}$$

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 $\boldsymbol{t} = (t_1, \ldots, t_\kappa) \in [n]^\kappa$, and variables $\boldsymbol{v} = (v_1, \ldots, v_\kappa)$, let $S_{\boldsymbol{t}}$ be the polynomial in the variables $\boldsymbol{v}$ given by

$$S_{\boldsymbol{t}}(\boldsymbol{v}) = \frac{(n - \|\boldsymbol{t}\|)!}{n!} \prod_{j \in [\kappa]} t_j! \cdot \prod_{j \in [\kappa]} \binom{v_j}{t_j}.$$

Notice that for every $j \in [\kappa]$, $S_{\boldsymbol{t}+\boldsymbol{e}_j}(\boldsymbol{v}) = S_{\boldsymbol{t}}(\boldsymbol{v}) \cdot \frac{v_j - t_j}{n - \|\boldsymbol{t}\|}$.

To define the candidate pseudo-expectation $\tilde{\mathbb{E}}$, by linearity, it is enough to define it on monomials. For a monomial of the form $X_{\boldsymbol{I}}$ we define it as

$$\tilde{\mathbb{E}}(X_{\boldsymbol{I}}) = \begin{cases} S_{|\boldsymbol{I}|}(\boldsymbol{\gamma}) & \text{if the sets in } \boldsymbol{I} \text{ are pair-wise disjoint,} \\ 0 & \text{otherwise.} \end{cases}$$

For a general monomial m, possibly not multilinear, we define $\tilde{\mathbb{E}}(m)$ as $\tilde{\mathbb{E}}(X_{\boldsymbol{I}})$ where $X_{\boldsymbol{I}}$ is the unique multilinear monomial equivalent to m modulo $\mathbb{B}$, that is such that $m \equiv X_{\boldsymbol{I}}$. We show that, for the range of parameters of Theorem 1.3, $\tilde{\mathbb{E}}$ is a pseudo-expectation for $\mathsf{bool\text{-}Kn}_n^{\kappa,r}$.

Lemma 3.9. *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 $\tilde{\mathbb{E}}(p) = \tilde{\mathbb{E}}(q)$. □

The definition of $\tilde{\mathbb{E}}$ is to enforce that $\tilde{\mathbb{E}}(pq) = 0$ for every $p \in \mathsf{bool\text{-}SRU}_n^{\kappa,r}$.

Theorem 3.10. *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 $\tilde{\mathbb{E}}$.

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.

CASE 1. If $i \in \bigcup_{j\in[\kappa]} I_j$, then

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

CASE 2. If $i \notin \bigcup_{j\in[\kappa]} I_j$, then

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

since $\|\boldsymbol{\gamma}\| = n$.

We now prove that

$$\tilde{\mathbb{E}}(X_{\boldsymbol{I}}(\sum_{j\in[\kappa]} \zeta^{j-1}\|\boldsymbol{x}^{(j)}\| - r_1 - \zeta r_2)) = 0. \tag{3.11}$$

Let T be the LHS of eq. (3.11). The following chain of equalities gives $T = 0$.

$$T = S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \sum_{j\in[\kappa]} \zeta^{j-1} t_j + \sum_{i\notin\bigcup_{j\in[\kappa]} I_j} (\sum_{j\in[\kappa]} \zeta^{j-1} S_{\boldsymbol{t}+\boldsymbol{e}_j}(\boldsymbol{\gamma})) - (r_1 + \zeta r_2) S_{\boldsymbol{t}}(\boldsymbol{\gamma})$$

$$
\begin{aligned}
&= S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \sum_{j\in[\kappa]} \zeta^{j-1} t_j + (n - \|\boldsymbol{t}\|) \sum_{j\in[\kappa]} \zeta^{j-1} S_{\boldsymbol{t}+\boldsymbol{e}_j}(\boldsymbol{\gamma}) - (r_1 + \zeta r_2) S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \\
&= S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \sum_{j\in[\kappa]} \zeta^{j-1} t_j + S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \sum_{j\in[\kappa]} \zeta^{j-1}(\gamma_j - t_j) - (r_1 + \zeta r_2) S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \\
&= S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \cdot \left(\sum_{j\in[\kappa]} \zeta^{j-1} t_j + \sum_{j\in[\kappa]} \zeta^{j-1}(\gamma_j - t_j) - (r_1 + \zeta r_2) \right) \\
&= S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \cdot \left(\sum_{j\in[\kappa]} \zeta^{j-1} \gamma_j - (r_1 + \zeta r_2) \right) \\
&= S_{\boldsymbol{t}}(\boldsymbol{\gamma}) \cdot \left(\sum_{j\in[\kappa]} \zeta^{j-1} \hat{\gamma} + \sum_{j\in[\kappa]} \zeta^{j-1} r_j - (r_1 + \zeta r_2) \right) \\
&= 0,
\end{aligned}
$$

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

We now use Blekherman's approach (Lee *et al.* 2016, Appendix B,C) to prove that, for a suitable range of parameters, $\tilde{\mathbb{E}}(p \cdot p^*) \in \mathbb{R}_{\geq 0}$.

First we introduce some notation on the symmetric group and how it acts on polynomials. Let $\mathfrak{S}_n$ be the group of permutations over 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 $\boldsymbol{y} = (y_1, \ldots, y_n)$. 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

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

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

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

Lee *et al.* (2016, Theorem B.11), following Blekherman, prove a decomposition for $\mathrm{Sym}(p^2)(\boldsymbol{y})$ analog as the one in the following theorem.

THEOREM 3.12 (adaptation of Lee *et al.* 2016, Theorem B.11).

Given Boolean variables $\boldsymbol{y} = (y_1, \ldots, y_n)$ *and* $p \in \mathbb{C}[\boldsymbol{y}]$ *with degree at most* $d \leq n/2$,

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

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* $(d-j)/2$.

REMARK. *Theorem B.11 in (Lee* et al. *2016) is proved for real polynomials and a crucial notion in its proof is the inner product* $\langle \cdot, \cdot \rangle$ *on the space of degree-t homogenous multilinear polynomials: for* $p = \sum_m p_m m$ *and* $q = \sum_m q_m m$, $\langle p, q \rangle$ *is defined as* $\sum_m p_m q_m$. *We can likewise define a Hermitian inner product* $\langle \cdot, \cdot \rangle$ *on the space of degree-t homogenous multilinear polynomials with complex coefficients as* $\langle p, q \rangle = \sum_m p_m q^*_m$. *With this change, the proof of Theorem B.11 in (Lee* et al. *2016) generalizes to complex polynomials and gives Theorem 3.12.*

We want to use Theorem 3.12 and to do so we extend the polynomial $S_{|\boldsymbol{I}|}(\boldsymbol{v})$ in the following way: given $p = \sum_{\boldsymbol{I}} \alpha_{\boldsymbol{I}} X_{\boldsymbol{I}}$ with $\alpha_{\boldsymbol{I}} \in \mathbb{C}$, let

$$S(p)(\boldsymbol{v}) = \sum_{\boldsymbol{I}} \alpha_{\boldsymbol{I}} S_{|\boldsymbol{I}|}(\boldsymbol{v}).$$

The polynomial $S(p)$ is useful since it is both connected to $\tilde{\mathbb{E}}$ and to $\mathrm{Sym}(p)$. The connection with $\tilde{\mathbb{E}}$ is trivial: $\tilde{\mathbb{E}}(p) = S(p)(\boldsymbol{\gamma})$. The connection with $\mathrm{Sym}(p)$ is the content of the following theorem.

THEOREM 3.13. *Given* $p \in \mathbb{C}[\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(\kappa)}]$,

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

where ρ *is the substitution given by*

$$\rho(x_{ij}) = y_i + \frac{r_j}{n}$$

where $r_3 = \cdots = r_\kappa = 0$.

PROOF. Lemma 3.7 implies that

$$\prod_{j\in[\kappa]} \binom{\|\boldsymbol{x}^{(j)}\|}{t_j} \equiv \sum_{\substack{\boldsymbol{I}=(I_1,\dots,I_\kappa),\ I_j\subseteq[n]\\ |I_j|=t_j}} X_{\boldsymbol{I}}. \tag{3.14}$$

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

$$\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} \sigma p \equiv S(p)(\|\boldsymbol{x}^{(1)}\|, \dots, \|\boldsymbol{x}^{(\kappa)}\|). \tag{3.15}$$

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

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

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 $\boldsymbol{I} = (I_1, \dots, I_\kappa)$ and the sets I_j are pair-wise disjoint. Let $t_j = |I_j|$, then

$$\begin{aligned}
\frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n} X_{\sigma\boldsymbol{I}} &= \frac{(n-\|\boldsymbol{t}\|)!\prod_{j\in[\kappa]} t_j!}{n!} \cdot \sum_{\substack{\boldsymbol{S}=(S_1,\dots,S_\kappa)\\ \text{pair-wise disj.}\\ |S_j|=t_j}} X_{\boldsymbol{S}} \\
&\equiv \frac{(n-\|\boldsymbol{t}\|)!\prod_{j\in[\kappa]} t_j!}{n!} \cdot \sum_{\substack{\boldsymbol{S}=(S_1,\dots,S_\kappa)\\ |S_j|=t_j}} X_{\boldsymbol{S}} \\
&\equiv \frac{(n-\|\boldsymbol{t}\|)!}{n!}\prod_{j\in[\kappa]} t_j! \cdot \prod_{j\in[\kappa]} \binom{\|\boldsymbol{x}^{(j)}\|}{t_j} \\
&= S(X_{\boldsymbol{I}})(\|\boldsymbol{x}^{(1)}\|, \dots, \|\boldsymbol{x}^{(\kappa)}\|),
\end{aligned} \tag{3.16}$$

where the equality in eq. (3.16) follows from eq. (3.14).

To conclude, it is then enough to observe that the statement we want to prove follows from eq. (3.15) restricting both sides of the equality by ρ. To prove this, we use that $\sigma X_{\boldsymbol{I}}\restriction_\rho = \sigma(X_{\boldsymbol{I}}\restriction_\rho)$. □

We now prove the degree lower bound for $\mathsf{SRU}_n^{\kappa,r}$ in $\mathsf{SoS}_{\mathbb{C}}$, that is Theorem 1.3, restated here for convenience of the reader.

THEOREM 1.3 (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 $\mathsf{SoS}_{\mathbb{C}}$.

PROOF. We show that $\tilde{\mathbb{E}}$ is a degree-d pseudo-expectation. Theorem 3.10 already showed that for every $p \in \mathsf{bool\text{-}SRU}_n^{\kappa,r}$, $\tilde{\mathbb{E}}(qp) = 0$. Therefore, it is enough to show that, whenever the condition on d is satisfied, for every polynomial $p \in \mathbb{C}[\boldsymbol{x}^{(1)}, \ldots, \boldsymbol{x}^{(\kappa)}]$ of degree at most d, $\tilde{\mathbb{E}}(p \cdot p^*) \in \mathbb{R}_{\geq 0}$ where p^* is the formal conjugate of p,

Let $\boldsymbol{\gamma}$ be defined as in eq. (3.8). Recall that $\hat{\gamma} = \frac{n - r_1 - r_2}{\kappa}$ and $S(p)(\boldsymbol{\gamma}) = \tilde{\mathbb{E}}(p)$. We have that

$$\begin{aligned}
\tilde{\mathbb{E}}(p \cdot p^*) &= S(p \cdot p^*)(\boldsymbol{\gamma}) \\
&= S(p \cdot p^*)(r_1 + \hat{\gamma}, r_2 + \hat{\gamma}, \ldots, r_\kappa + \hat{\gamma}) && \text{[by def. of } \boldsymbol{\gamma}] \\
&= \mathrm{Sym}(p\restriction_\rho \cdot p\restriction_\rho^*)(\hat{\gamma}\boldsymbol{e}_1) && \text{[by Theorem 3.13]} \\
&= \textstyle\sum_{j=0}^{d} p_{d-j}(\hat{\gamma}) \cdot p^*_{d-j}(\hat{\gamma}) \prod_{i=0}^{j-1} (\hat{\gamma} - i)(n - \hat{\gamma} - i)
\end{aligned}$$

where the last equality follows from Theorem 3.12 and ρ is the substitution given by $\rho(x_{ij}) = y_i + \frac{r_j}{n}$ (recall that $r_3 = \cdots = r_\kappa = 0$). 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 $\prod_{i=0}^{j-1}(\hat{\gamma} - i)(n - \hat{\gamma} - i) \geq 0$. This is true if $\hat{\gamma} - d + 1 \geq 0$ and $n - \hat{\gamma} - d + 1 \geq 0$. That is if

$$-(\kappa - 1)n + \kappa d - \kappa \leq r_1 + r_2 \leq n - \kappa d + \kappa. \qquad \square$$

4. Size lower bounds

In this section, we prove the size lower bound for $\mathsf{SRU}_n^{\kappa,0}$ in $\mathsf{SoS}_{\mathbb{C}}$ (Theorem 1.4) from the the corresponding degree lower bound (Theorem 1.3).

4.1. High level structure of the argument. A way to prove Theorem 1.4 from Theorem 1.3 is the following. 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 $\mathsf{SRU}_n^{\kappa,r} \circ \boldsymbol{g}$ (see Definition 4.3). We are interested in composing polynomials with $\boldsymbol{g}$ with good properties (see Definition 4.1). Then a lifting theorem shows that degree lower bounds on $\mathsf{SRU}_n^{\kappa,r}$ imply size lower bounds on $\mathsf{SRU}_n^{\kappa,r} \circ \boldsymbol{g}$ (Theorem 4.10). The overall structure of this size lower bound it follows the typical structure of size-degree trade-offs, see for instance (Atserias & Hakoniemi 2019; Clegg *et al.* 1996; Sokolov 2020) for other examples of size-degree trade-offs. The idea is to show, first, that there exists a relatively long sequence of restrictions such that the restricted polynomials have small degree refutations (Theorem 4.8) and, secondly, that each individual restriction can only make the degree decrease a little (Lemma 4.9). These two components will imply that the sequence of restrictions must be very long and this will imply the size-degree trade-off (Theorem 4.10).

Finally, the size lower bound for $\mathsf{SRU}_n^{\kappa,r}$ (Theorem 1.4) is just a corollary of the size-degree trade-off (Theorem 4.10).

The rest of the section is just following this high level scheme. We first introduce the notion of compliant polynomials.

4.2. Composition with compliant polynomials. *Compliant polynomials* are a generalization of the compliant gadgets from (Sokolov 2020, Definition 2.1). The main difference with Sokolov's gadgets is that compliant gadgets are polynomials with real coefficients and taking values in $\{0,1\}$ or $\{\pm 1\}$, while ours are complex polynomials taking values in the set Ω_κ of κth roots of unity.

Definition 4.1 (compliant polynomial). *A polynomial* $g \in \mathbb{C}[y_1, \ldots, y_\ell]$ *is* compliant *if it is symmetric and there exists a function* $h : \Omega_\kappa \to \Omega_\kappa^\ell$ *such that*

(i) $g \circ h = \mathbf{id}$, *i.e. for all* $b \in \Omega_\kappa$, $g(h(b)) = b$;

(ii) for each $b \in \Omega_\kappa$, *the first* κ *coordinates of* $h(b)$ *list all the elements of* Ω_κ; *and*

(iii) for each $b \in \Omega_\kappa$, the product of all the coordinates of $h(b)$ is a fixed constant.

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

A relevant example of compliant polynomial is the following.

EXAMPLE 4.2. Let $\boldsymbol{y} = (y_1, \ldots, y_\ell)$. The polynomial

$$g(\boldsymbol{y}) := \frac{1}{\kappa}(\sum_{j\in[\ell]} y_j - (\ell - 2\kappa))$$

is compliant. Indeed, the polynomial g is symmetric and we can take as $h : \Omega_\kappa \to \Omega_\kappa^\ell$ the function mapping

$$h : \omega \mapsto (1, \zeta, \zeta^2, \ldots, \zeta^{\kappa-1}, \underbrace{1, 1, \ldots, 1}_{\ell-2\kappa}, \underbrace{\omega, \omega, \ldots, \omega}_{\kappa}),$$

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

$$\zeta^{\kappa(\kappa-1)/2}\omega^\kappa = \zeta^{\kappa(\kappa-1)/2}$$

since ω is a κth root of unity, and the product does not depend on ω. ◊

Now we want to *compose* polynomials with compliant gadgets. This is essentially the usual notion of composition of polynomials.

DEFINITION 4.3 (composition of polynomials). *Let $\boldsymbol{x}, \boldsymbol{y}_1, \ldots \boldsymbol{y}_n$ be tuples of distinct variables where $\boldsymbol{y}_j = (y_{j1}, \ldots, y_{j\ell_j})$. Given a polynomial $p \in \mathbb{C}[\boldsymbol{x}]$ and $\boldsymbol{g} = (g_1 \ldots, g_n)$ 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 $\mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$.*

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

To see a relevant example of composition of polynomials, we continue Example 4.2. Essentially, our interest in the polynomials in Example 4.2 is that they are linear and therefore, intuitively, composing $\mathsf{SRU}_n^{\kappa,r}$ with such polynomials results in a set of polynomials containing $\mathsf{SRU}_{n'}^{\kappa,r'}$.

EXAMPLE 4.2 CONTINUED. Consider the tuple of variables $\boldsymbol{y}_j = (y_{j1}, \ldots, y_{j\ell_j})$ and a tuple of compliant polynomials $\boldsymbol{g} = (g_1 \ldots, g_n)$ with $g_j \in \mathbb{C}[\boldsymbol{y}_j]$. In this example, we see how to get essentially $\mathsf{SRU}_n^{\kappa,0}$ (after renaming of variables) as a subset of

$$\mathsf{SRU}_{n'}^{\kappa,r} \circ \boldsymbol{g} \cup \{y_{ij}^{\kappa} - 1 \ : \ i \in [n'], \ j \in [\ell_i]\}, \tag{4.4}$$

for some r' and n'. The tuple of compliant polynomials $\boldsymbol{g}$ is based on the compliant polynomial in Example 4.2.

Let $n' \in \mathbb{N}$ with $n' > 2\kappa$ and $b \in \{0, \ldots, 2\kappa\}$ such that $n = (2\kappa+1)n' + b$. Let $\ell_1 = \cdots = \ell_b = 2\kappa + 2$ and $\ell_{b+1} = \cdots = \ell_{n'} = 2\kappa + 1$. In particular, the number of y_{ij} variables is exactly n and $\sum_{i\in[n']} \ell_i = (2\kappa+1)n' + b$.

Consider the tuple $\boldsymbol{g} = (g_1, \ldots, g_{n'})$ where $g_i \in \mathbb{C}[y_{i1}, \ldots, y_{i\ell_i}]$ are the polynomials in Example 4.2, i.e. g_i is the polynomial

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

We have that

$$\left\{\frac{1}{\kappa}\sum_{i\in[n'],j\in[\ell_i]} y_{ij}\right\} \cup \{y_{ij}^{\kappa} - 1 \ : \ i \in [n'], \ j \in [\ell_i]\} \tag{4.5}$$

is a subset of of

$$\mathsf{SRU}_{n'}^{\kappa,r} \circ \boldsymbol{g} \cup \{y_{ij}^{\kappa} - 1 \ : \ i \in [n'], \ j \in [\ell_i]\} \tag{4.6}$$

for $r = -\frac{n'+b}{\kappa}$. Notice that, the set of polynomials in (4.5) behaves exactly as $\mathsf{SRU}_n^{\kappa,0}$ from the point of view of $\mathsf{PC}/\mathsf{SoS}_{\mathbb{C}}$ refutations. Indeed, we can rename variables in a $\mathsf{SRU}_n^{\kappa,0}$ refutation and rescale everything by $\frac{1}{\kappa}$ to get a refutation of (4.5) and viceversa. ◊

4.3. The size-degree trade-off. To have a cleaner argument, we consider the notion of *reduced degree*.

Definition 4.7 (reduced degree). *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 2.3).*

Recall that the overall structure of the size-degree trade-off bound consists of two main components.

1. A theorem showing that there exists a relatively short sequence of restrictions such that the restricted polynomials have small degree refutations. This is Theorem 4.8 below.

2. A theorem showing that each individual restriction can only make the degree decrease a little. This is Lemma 4.9 below.

The first component is a generalization of (Sokolov 2020, Theorem 4.1). We postpone the proof to Section 5.

Theorem 4.8. *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* $g_i \in \mathbb{C}[y_{i1}, \ldots, y_{i\ell_i}]$ *and* $\omega_1, \omega_2, \ldots, \omega_m \in \Omega_\kappa$. *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* $x_{i_1}, \ldots, x_{i_m}$ *with* $m = \lceil \ell^\kappa n \ln(s)/D \rceil$ *such that*

(i) $\ell = \max_i \ell_i$;

(ii) the choice of x_{i_t} *only depends on* $\omega_1, \ldots, \omega_{t-1}$;

(iii) 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 component is the following lemma.

LEMMA 4.9. *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. 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. □

Now we put together Theorem 4.8 and Lemma 4.9 to get the size-degree trade-off, which is a generalization of (Sokolov 2020, Theorem 4.2).

THEOREM 4.10. *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 $g_i \in \mathbb{C}[y_{i1}, \ldots, y_{i\ell_i}]$. 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 $\ell = \max_{i\in[n]} \ell_i$.

PROOF. 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 4.8 to pick x_{i_t} with applications of Lemma 4.9 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 4.8, we can set $m = \lceil \ell^k n \ln(s)/D' \rceil$ 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 $\ln(s) \geq \frac{(D-d_0)^2}{8\ell^k n(\kappa-1)}$. □

Finally, using Theorem 1.3 and Theorem 4.10, we have the size lower bound for $\mathsf{SRU}_n^{\kappa,0}$ stated in Theorem 1.4.

THEOREM 1.4 (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. We proceed as in Example 4.2 continued. Let $n = (2\kappa + 1)n' + b$ with $b \in \{0, \ldots, 2\kappa\}$. Let $\ell_1 = \cdots = \ell_b = 2\kappa + 2$ and $\ell_{b+1} = \cdots = \ell_{n'} = 2\kappa + 1$. Consider the tuple $\boldsymbol{g} = (g_1, \ldots, g_{n'})$ where $g_i \in \mathbb{C}[y_{i1}, \ldots, y_{i\ell_i}]$ is the polynomial

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

As we saw in Example 4.2, each g_i is a compliant polynomial. From Example 4.2 continued, the set of polynomials

$$\left\{\frac{1}{\kappa} \sum_{i \in [n'], j \in [\ell_i]} y_{ij}\right\} \cup \{y_{ij}^{\kappa} - 1 : i \in [n'],\ j \in [\ell_i]\} \tag{4.11}$$

is a subset of

$$\mathsf{SRU}_{n'}^{\kappa,r} \circ \boldsymbol{g} \cup \{y_{ij}^{\kappa} - 1 : i \in [n'],\ j \in [\ell_i]\} \tag{4.12}$$

for $r = -\frac{n'+b}{\kappa}$. By Theorem 1.3, there are no $\mathsf{SoS}_{\mathbb{C}}$ refutations of $\mathsf{SRU}_{n'}^{\kappa,r}$ in degree $d = \frac{n'}{\kappa}$ since

$$\kappa d \leq \min\{r + (\kappa - 1)n' + \kappa,\ n' - r + \kappa\}.$$

By Theorem 4.10, the set of polynomials (4.6) 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, the same size lower bound must hold for the set of polynomials in (4.11) and for $\mathsf{SRU}_n^{\kappa,0}$. □

5. Proof of Theorem 4.8

This section contains the proof of Theorem 4.8. We follow the notations from Section 4, in particular the notion of compliant polynomial (Definition 4.1). The argument given in this section is a non-trivial generalization of the proof of (Sokolov 2020, Theorem 4.1).

5.1. Notation. Let $\ell_1, \ldots, \ell_n \in \mathbb{N}$. For each $i \in [n]$ we have a corresponding block of ℓ_i variables $\boldsymbol{y}_i = (y_{i1}, \ldots, y_{i\ell_i})$ and a compliant polynomial $g_i \in \mathbb{C}[\boldsymbol{y}_i]$. We use notation $\boldsymbol{g}$ for the tuple $(g_1, \ldots, g_n)$, and ζ for some fixed primitive κth root of unity.

Let $\mathcal{T}_n$ be the set of terms in $\mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$. For $i \in [n]$ and $\boldsymbol{\alpha}_i = (\alpha_{i1}, \ldots, \alpha_{i\ell_i}) \in \mathbb{N}^{\ell_i}$, we denote as $Y_i^{\boldsymbol{\alpha}_i}$ the monomial $\prod_{j\in[\ell_i]} y_{ij}^{\alpha_{ij}}$. We can uniquely write a term $t \in \mathcal{T}_n$ as

$$t = \prod_{i\in[n]} Y_i^{\boldsymbol{\alpha}_i},$$

for suitable $\boldsymbol{\alpha}_i \in \mathbb{N}^{\ell_i}$. We want to study the polynomials in $\mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$ under variable permutations of that do not swaps variables between blocks. We denote the group of permutations over the variables $\boldsymbol{y}_i$ as $\mathfrak{S}_i$. We are mostly interested in its κ-cycles, and the compliance of g_i guarantees that κ-cycles in $\mathfrak{S}_i$ exists because $\ell_i > \kappa$.

Fix some $\hat{\imath} \in [n]$ and some κ-cycle σ in $\mathfrak{S}_i$. We define the map $(\sigma; \hat{\imath}) : \mathcal{T}_n \to \mathcal{T}_n$ on term $t = \prod_{i\in[n]} Y_i^{\boldsymbol{\alpha}_i}$ as

$$(\sigma;\hat{\imath})\left(\prod_{i\in[n]} Y_i^{\boldsymbol{\alpha}_i}\right) = \left(\prod_{j\in[\ell_i]} y_{\hat{\imath}\sigma(j)}^{\alpha_{ij}}\right) \cdot \prod_{i\in[n],i\neq\hat{\imath}} Y_i^{\boldsymbol{\alpha}_i}.$$

The map $(\sigma; \hat{\imath})$ is extended by linearity to all polynomials in the ring $\mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$. We say that a polynomial p is *invariant* under $(\sigma; \hat{\imath})$ if $(\sigma; \hat{\imath})(p) = p$.

Given a polynomial $p \in \mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$, the *symmetrization* of p with respect to $(\sigma; \hat{\imath})$ is the polynomial

$$\mathrm{SYM}_{\sigma,\hat{\imath}}(p) = \sum_{m=0}^{\kappa-1} (\sigma; \hat{\imath})^m(p),$$

where $(\sigma; \hat{\imath})^m$ is application of $(\sigma; \hat{\imath})$ m times, and $(\sigma; \hat{\imath})^0$ is the identity.

Example 5.1. Say $\ell_1 = \ell_2 = \ell_3 = 4$, $\kappa = 3$, and σ is the 3-cycle $(1\,2\,3)$. The term $t = y_{1,2}y_{1,3}^2y_{1,4}y_{2,2}$ is $Y_1^{\boldsymbol{\alpha}_1}Y_2^{\boldsymbol{\alpha}_2}$ with $\boldsymbol{\alpha}_1 = (0,1,2,1)$ and $\boldsymbol{\alpha}_2 = (0,1,0,0)$. Then, the maps $(\sigma;1)$ and $(\sigma;2)$ map t into:

$$\begin{aligned}(\sigma;1)(t) &= y_{1,3}y_{1,1}^2y_{1,4}y_{2,2},\\ (\sigma;2)(t) &= y_{1,2}^1y_{1,3}^2y_{1,4}y_{2,3},\\ (\sigma;3)(t) &= y_{1,2}y_{1,3}^2y_{1,4}y_{2,2}.\end{aligned}$$

Moreover,

$$\begin{aligned}\mathrm{SYM}_{\sigma,1}(t) &= (y_{1,2}^1y_{1,3}^2 + y_{1,3}^1y_{1,1}^2 + y_{1,1}^1y_{1,2}^2)y_{1,4}y_{2,2},\\ \mathrm{SYM}_{\sigma,2}(t) &= y_{1,2}y_{1,3}^2y_{1,4}(y_{2,1} + y_{2,2} + y_{2,3}),\\ \mathrm{SYM}_{\sigma,3}(t) &= 3y_{1,2}y_{1,3}^2y_{1,4}y_{2,2}.\end{aligned}$$ ◊

The example above already suggests the following lemma.

Lemma 5.2. *Let $p, q \in \mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$, $\hat{\imath} \in [n]$ and $\sigma \in \mathfrak{S}_{\hat{\imath}}$. If q is invariant under $(\sigma; \hat{\imath})$, then $\mathrm{SYM}_{\sigma,\hat{\imath}}(pq) = \mathrm{SYM}_{\sigma,\hat{\imath}}(p)q$.*

Proof. The action of $(\sigma; \hat{\imath})$ is multiplicative, therefore

$$\begin{aligned}\mathrm{SYM}_{\sigma,\hat{\imath}}(pq) &= \sum_{m=0}^{\kappa-1} (\sigma; \hat{\imath})^m(pq)\\ &= \sum_{m=0}^{\kappa-1} (\sigma; \hat{\imath})^m(p) \cdot (\sigma; \hat{\imath})^m(q)\\ &= \sum_{m=0}^{\kappa-1} (\sigma; \hat{\imath})^m(p) \cdot q \qquad [q \text{ is invariant under } (\sigma; \hat{\imath})]\\ &= \mathrm{SYM}_{\sigma,\hat{\imath}}(p)q.\end{aligned}$$ □

In the Boolean framework, it is possible to kill high degree terms by setting variables to zero, but in the Fourier framework, we cannot do that. Instead, we apply assignment $\beta_{\sigma,\hat{\imath}}$ to variables $\boldsymbol{y}_{\hat{\imath}}$ so that, together with symmetrization $\mathrm{SYM}_{\sigma,\hat{\imath}}(\cdot)$, it acts *as if* it was a partial restriction mapping some terms to 0.

Definition 5.3 (the partial assignment $\beta_{\sigma,\hat{\imath}}$). *For $\hat{\imath} \in [n]$ and a κ-cycle $\sigma = (j_0\ j_1\ \ldots\ j_{\kappa-1})$, let $\beta_{\sigma,\hat{\imath}}$ be the partial assignment on the variables $\boldsymbol{y}_{\hat{\imath}}$ mapping $y_{\hat{\imath},j_m}$ to ζ^m, for every $m = 0, \ldots, \kappa-1$ and mapping the remaining variables $y_{\hat{\imath},j}$ to themselves. We denote the partial assignment $\beta_{\sigma,\hat{\imath}}$ applied to a polynomial p as $p{\restriction}_{\beta_{\sigma,\hat{\imath}}}$.*

Since we mostly consider $\mathrm{SYM}_{\sigma,\hat{\imath}}(t)$ after the restriction by $\beta_{\sigma,\hat{\imath}}$ we introduce the notation

$$\mathcal{S}_{\sigma,\hat{\imath}}(t) = \mathrm{SYM}_{\sigma,\hat{\imath}}(t){\restriction}_{\beta_{\sigma,\hat{\imath}}}\ .$$

Example 5.1 continued. Using the notation of Example 5.1,

$$\begin{aligned}
\mathcal{S}_{\sigma,1}(t) &= (\zeta\zeta^4 + \zeta^2 + \zeta^2)y_{1,4}y_{2,2} = 3\zeta^2 y_{1,4}y_{2,2},\\
\mathcal{S}_{\sigma,2}(t) &= y_{1,2}y_{1,3}^2 y_{1,4}(\zeta^0 + \zeta^1 + \zeta^2) = 0,\\
\mathcal{S}_{\sigma,3}(t) &= 3y_{1,2}y_{1,3}^2 y_{1,4}y_{2,2}.
\end{aligned}$$

Notice that, $\mathcal{S}_{\sigma,1}(t) = 3t{\restriction}_{\beta_{\sigma,1}}$ and similarly $\mathcal{S}_{\sigma,3}(t) = 3t{\restriction}_{\beta_{\sigma,3}}$. This holds in general, as the next lemma shows. ◊

We show that $\mathcal{S}_{\sigma,\hat{\imath}}(t)$ acts as a sort of partial restriction that either maps the term t to 0 or to a restriction of t.

Lemma 5.4. *Let $\hat{\imath} \in [n]$ and $j_0, \ldots, j_{\kappa-1} \in [\ell_{\hat{\imath}}]$ be distinct indices. Let σ be the κ-cycle $(j_0\ j_1\ \ldots\ j_{\kappa-1})$. Let $t = \prod_{i\in[n]} Y_i^{\boldsymbol{\alpha}_i}$ be a term in $\mathcal{T}_n$. Then*

$$\mathcal{S}_{\sigma,\hat{\imath}}(t) = \begin{cases} 0 & \text{if } \kappa \nmid \sum_{m=0}^{\kappa-1} \alpha_{\hat{\imath},j_m} \\ \kappa \cdot t{\restriction}_{\beta_{\sigma,\hat{\imath}}} & \text{otherwise.} \end{cases}$$

Proof. Since $(\sigma;\hat{\imath})^0$ is the identity, we have $(\sigma;\hat{\imath})^0(t){\restriction}_{\beta_{\sigma,\hat{\imath}}} = t{\restriction}_{\beta_{\sigma,\hat{\imath}}}$. For $(\sigma;\hat{\imath})^1$, we can see that now $\beta_{\sigma,\hat{\imath}}$ maps the variable $y_{\hat{\imath}j_m}$ to ζ^{m+1}, that is

$$(\sigma;\hat{\imath})^1(t){\restriction}_{\beta_{\sigma,\hat{\imath}}} = \omega \cdot t{\restriction}_{\beta_{\sigma,\hat{\imath}}},$$

where $\omega = \zeta^{\sum_{m=0}^{\kappa-1} \alpha_{\hat{\imath} j_m}}$. Likewise, for every $0 \leq m < \kappa$, we have that

$$(\sigma, \hat{\imath})^m(t)\restriction_{\beta_{\sigma,\hat{\imath}}} = \omega^m \cdot t\restriction_{\beta_{\sigma,\hat{\imath}}} .$$

That is

$$\mathcal{S}_{\sigma,\hat{\imath}}(t) = \left(\sum_{m=0}^{\kappa-1} \omega^m\right) t\restriction_{\beta_{\sigma,\hat{\imath}}} = \begin{cases} 0 & \text{if } w \neq 1 \\ \kappa \cdot t\restriction_{\beta_{\sigma,\hat{\imath}}} & \text{otherwise,} \end{cases}$$

where the last equality follows since ω is a power of ζ, all powers of ζ except 1 are roots of polynomial $1 + X + X^2 + \cdots + X^{\kappa-1}$, and $\omega \neq 1$ if and only if $\kappa \nmid \sum_{m=0}^{k-1} \alpha_{\hat{\imath}, j_m}$. □

An immediate consequence of Lemma 5.4 is that if $\mathcal{S}_{\sigma,\hat{\imath}}(t) = 0$ then $\mathcal{S}_{\sigma,\hat{\imath}}(t^*) = 0$, where t^* is the formal conjugate of t.

LEMMA 5.5. *If $\mathcal{S}_{\sigma,\hat{\imath}}(t) = 0$ then $\mathcal{S}_{\sigma,\hat{\imath}}(t^*) = 0$, where t^* is the formal conjugate of t.*

PROOF. By Lemma 5.4, $\mathcal{S}_{\sigma,\hat{\imath}}(t) = 0$ implies that $\kappa \nmid \sum_{m=0}^{k-1} \alpha_{\hat{\imath}, j_m}$. The exponent of the variable $y_{\hat{\imath},j}$ in t^* is $(\kappa\lceil \alpha_{\hat{\imath},j}/\kappa \rceil - \alpha_{\hat{\imath},j})$, which is equal to $-\alpha_{\hat{\imath},j}$ modulo κ. Therefore $\kappa \nmid \sum_{m=0}^{k-1} (\kappa\lceil \alpha_{\hat{\imath},j_m}/\kappa \rceil - \alpha_{\hat{\imath},j_m})$. Hence, again by Lemma 5.4, $\mathcal{S}_{\sigma,\hat{\imath}}(t^*) = 0$. □

Another immediate consequence of Lemma 5.4 is that given a term $t = \prod_{i \in [n]} Y_i^{\boldsymbol{\alpha}_i}$ such the entries of the vector $\boldsymbol{\alpha}_{\hat{\imath}}$ are not all equal modulo κ, then there exist a κ-cycle σ such that $\mathcal{S}_{\sigma,\hat{\imath}}(t) = 0$.

LEMMA 5.6. *Let $t = \prod_{i \in [n]} Y_i^{\boldsymbol{\alpha}_i}$ a term in $\mathcal{T}_n$, and suppose the entries of the vector $\boldsymbol{\alpha}_{\hat{\imath}}$ are not all equal modulo κ. Then there exist a κ-cycle σ such that $\mathcal{S}_{\sigma,\hat{\imath}}(t) = 0$.*

PROOF. By Lemma 5.4, it is enough to show that there are κ distinct indices $j_0, \ldots, j_{\kappa-1} \in [\ell_{\hat{\imath}}]$ such that $\kappa \nmid \alpha_{\hat{\imath},j_0} + \cdots + \alpha_{\hat{\imath},j_{\kappa-1}}$. Consider two distinct indices j_0, j_1 such that $\alpha_{\hat{\imath},j_0} \neq \alpha_{\hat{\imath},j_1}$ modulo κ. Now consider arbitrary distinct indices $j_2, \ldots, j_\kappa \in [\ell_{\hat{\imath}}]$. We can find those indices since $\ell_{\hat{\imath}} \geq \kappa + 1$. It must be that either $\kappa \nmid \alpha_{\hat{\imath},j_0} + \sum_{m=2}^{\kappa} \alpha_{\hat{\imath},j_m}$ or $\kappa \nmid \alpha_{\hat{\imath},j_1} + \sum_{m=2}^{\kappa} \alpha_{\hat{\imath},j_m}$. □

By linearity, define $\mathcal{S}_{\sigma,\hat{\imath}}(p)$ for every $p \in \mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$. We show now this operator is well-behaved on polynomials of the form pp^*.

LEMMA 5.7. *For every polynomial $p \in \mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$, every $\hat{\imath} \in [n]$ and every κ-cycle $\sigma \in \mathfrak{S}_{\ell_{\hat{\imath}}}$, there are polynomials $s_0, \ldots, s_{(\kappa-1)}$ such that*

$$\mathcal{S}_{\sigma,\hat{\imath}}(pp^*) = \sum_{j=0}^{\kappa-1} s_j s_j^*,$$

and moreover the total number of monomials in $\sum_{j=0}^{\kappa-1} s_j s_j^*$ before cancellations is at most the number of monomials in pp^* (again before cancellations).

PROOF. The permutation σ is a κ-cycle, say $(j_0\ j_1\ \ldots\ j_{\kappa-1})$. We focus on the set A of tuples of exponents for the variables $y_{\hat{\imath}j_0}, \ldots, y_{\hat{\imath}j_{\kappa-1}}$ that occur in the polynomial p. For each such $\boldsymbol{\alpha} \in A$, we define its norm $\|\boldsymbol{\alpha}\| = \sum_{m=0}^{\kappa-1} \alpha_{\hat{\imath},j_m}$.

Let $t(\boldsymbol{\alpha})$ be the monomial $\prod_{m=0}^{\kappa-1} y_{\hat{\imath}j_m}^{\alpha_{\hat{\imath}j_m}}$. By construction, the formal conjugate of $t(\boldsymbol{\alpha})$ can be written as $t(\kappa \boldsymbol{I}_{\boldsymbol{\alpha}} - \boldsymbol{\alpha})$ where $\boldsymbol{I}_{\boldsymbol{\alpha}}$ is some vector of integers.

We can partition A in $A_0, A_1, \ldots, A_{(\kappa-1)}$ based on the residue of their norm modulo κ. Namely $A_m = \{\boldsymbol{\alpha} \in A : \|\boldsymbol{\alpha}\| = m \pmod{\kappa}\}$. Then, we can write

$$p = \sum_{\boldsymbol{\alpha} \in A_0} p_{\boldsymbol{\alpha}} t(\boldsymbol{\alpha}) + \sum_{\boldsymbol{\alpha} \in A_1} p_{\boldsymbol{\alpha}} t(\boldsymbol{\alpha}) + \cdots + \sum_{\boldsymbol{\alpha} \in A_{(\kappa-1)}} p_{\boldsymbol{\alpha}} t(\boldsymbol{\alpha}).$$

where each $p_{\boldsymbol{\alpha}}$ is a polynomial not containing variables among $y_{\hat{\imath}j_0}, \ldots, y_{\hat{\imath}j_{\kappa-1}}$.

Observe that the polynomial $\mathcal{S}_{\sigma,\hat{\imath}}(t(\boldsymbol{\alpha})t(\boldsymbol{\alpha}')^*)$ is non-zero if and only if κ divides $\|\boldsymbol{\alpha}\| + \|\kappa \boldsymbol{I}_{\boldsymbol{\alpha}} - \boldsymbol{\alpha}'\|$ (by Lemma 5.4), which happens if and only if $\|\boldsymbol{\alpha}\| = \|\boldsymbol{\alpha}'\|$ modulo κ.

By linearity of $\mathrm{SYM}_{\sigma,\hat{\imath}}(\cdot)$ and this observation, we have that

$$\begin{aligned}
\mathcal{S}_{\sigma,\hat{\imath}}(pp^*) &= \sum_{\boldsymbol{\alpha},\boldsymbol{\alpha}' \in A} p_{\boldsymbol{\alpha}} p^*_{\boldsymbol{\alpha}'} \mathcal{S}_{\sigma,\hat{\imath}}(t(\boldsymbol{\alpha})t(\boldsymbol{\alpha}')^*) \\
&= \sum_{j=0}^{\kappa-1} \sum_{\boldsymbol{\alpha},\boldsymbol{\alpha}' \in A_j} p_{\boldsymbol{\alpha}} p^*_{\boldsymbol{\alpha}'} \mathcal{S}_{\sigma,\hat{\imath}}(t(\boldsymbol{\alpha})t(\boldsymbol{\alpha}')^*) \\
&= \kappa \sum_{j=0}^{\kappa-1} \sum_{\boldsymbol{\alpha},\boldsymbol{\alpha}' \in A_j} p_{\boldsymbol{\alpha}} p^*_{\boldsymbol{\alpha}'} t(\boldsymbol{\alpha}) \restriction_{\beta_{\sigma,\hat{\imath}}} t(\boldsymbol{\alpha}')^* \restriction_{\beta_{\sigma,\hat{\imath}}}
\end{aligned}$$

$$= \kappa \sum_{j=0}^{\kappa-1} \Big(\sum_{\boldsymbol{\alpha} \in A_j} p_{\boldsymbol{\alpha}} t(\boldsymbol{\alpha}) \restriction_{\beta_{\sigma,i}} \Big) \cdot \Big(\sum_{\boldsymbol{\alpha} \in A_j} p_{\boldsymbol{\alpha}} t(\boldsymbol{\alpha}) \restriction_{\beta_{\sigma,i}} \Big)^*$$
$$= \sum_{j=0}^{\kappa-1} s_j s_j^*,$$

where each s_j is $\sqrt{\kappa} \cdot \sum_{\boldsymbol{\alpha} \in A_j} p_{\boldsymbol{\alpha}} t(\boldsymbol{\alpha}) \restriction_{\beta_{\sigma,i}}$. We conclude the proof discussing the size. Let c_j be the number of monomials in the polynomial $\sum_{\boldsymbol{\alpha} \in A_j} p_{\boldsymbol{\alpha}} t(\boldsymbol{\alpha})$. The polynomial s_j has no more monomials than c_j, being its restriction. Hence, the total count of monomials in $\sum_{j=0}^{\kappa-1} s_j s_j^*$ before cancellations is at most $\sum_{j=0}^{\kappa-1} c_j^2$ which is less than $\left(\sum_{j=0}^{\kappa-1} c_j\right)^2$, the number of monomials in pp^* before cancellations. □

We now restate and prove Theorem 4.8.

THEOREM 4.8. *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 $g_i \in \mathbb{C}[y_{i1}, \ldots, y_{i\ell_i}]$ and $\omega_1, \omega_2, \ldots, \omega_m \in \Omega_\kappa$. 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 $x_{i_1}, \ldots, x_{i_m}$ with $m = \lceil \ell^\kappa n \ln(s)/D \rceil$ such that*

(i) $\ell = \max_i \ell_i$;

(ii) the choice of x_{i_t} only depends on $\omega_1, \ldots, \omega_{t-1}$;

(iii) 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 $D + d_0$.

PROOF. Let π be 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. Proof π has the form

$$-1 = \sum_{p \in P \circ \boldsymbol{g}} q_p \cdot p + \sum_{\substack{i \in [n] \\ j \in [\ell_i]}} q_{ij}(y_{ij}^\kappa - 1) + \sum_{q \in Q} q \cdot q^*, \tag{5.8}$$

where q_p, q_{ij}, qs are polynomials in $\mathbb{C}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_n]$. Without loss of generality we can consider a "multilinearized" version of (5.8) where all variables in polynomials q_p, qs are raised to powers at most $\kappa-1$. This assumption increases proof size only polynomially.

We say a term $t = \prod_{i\in[n]} Y_i^{\boldsymbol{\alpha}_i}$ is *fat* when there are at least D/κ distinct indices i so that the entries of the vector $\boldsymbol{\alpha}_i$ are not all equal. By Lemma 5.6, if a term is fat there are at least D/κ maps $(\sigma; i)$ with distinct indices i such that $\mathcal{S}_{\sigma,i}(t) = 0$.

Let F be the set of fat terms in the q_ps and in $q \cdot q^*$ before cancellations.[2] For each block of variables $\boldsymbol{y}_i$ we have at most $\ell(\ell-1)\ldots(\ell-\kappa+1)/\kappa \leq \ell^\kappa/\kappa$ possible κ-cycles in total, hence the maps $(\sigma; i)$ are at most $n \cdot \ell^\kappa/\kappa$. By averaging, we have a pair (σ_1, i_1) such that the number of fat terms $t \in F$ where $\mathcal{S}_{\sigma_1,i_1}(t) = 0$ are at least $\frac{k}{\ell^\kappa n} \cdot \frac{D}{\kappa} \cdot |F| = \frac{D}{\ell^\kappa n}|F|$.

Fix an arbitrary $\omega_1 \in \Omega_\kappa$. By applying $(\sigma_1; i_1)^0, \ldots, (\sigma_1; i_1)^{\kappa-1}$ to (5.8), summing and restricting by β_{i_1,σ_1} we obtain the equality

$$\begin{aligned} -\kappa \;=\; & \sum_{p\in P\circ\boldsymbol{g}} \mathcal{S}_{\sigma_1,i_1}(q_p \cdot p) + \sum_{\substack{i\in[n]\\ j\in[\ell_i]}} \mathcal{S}_{\sigma_1,i_1}(q_{ij}(y_{ij}^\kappa - 1)) \\ & + \sum_{q\in Q} \mathcal{S}_{\sigma_1,i_1}(q \cdot q^*). \end{aligned} \tag{5.9}$$

Now, since g is symmetric, p is invariant under the action of $(\sigma_1; i_1)$ and, by Lemma 5.2, then

$$\mathcal{S}_{\sigma_1,i_1}(q_p \cdot p) = \mathcal{S}_{\sigma_1,i_1}(q_p) \cdot p\restriction_{\beta_{i_1,\sigma_1}} .$$

For the same reason

$$\mathcal{S}_{\sigma_1,i_1}(q_{ij}(y_{ij}^\kappa - 1)) = \mathcal{S}_{\sigma_1,i_1}(q_{ij})(y_{ij}^\kappa - 1)\restriction_{\beta_{i_1,\sigma_1}} .$$

Therefore, by Lemma 5.7, the expression in (5.9) is a $\mathsf{SoS}_{\mathbb{C}}$ refutation π_1' of $(P\circ\boldsymbol{g})\restriction_{\beta_{i_1,\sigma_1}}$. Again, symmetry and the other compliance properties of $\boldsymbol{g}$ let us extend β_{i_1,σ_1} to some β' that sets all remaining variables in $\boldsymbol{y}_{i_1}$ and ensures $g_{i_1}(\beta'(y_{i_1,1}), \ldots, \beta'(y_{i_1,\ell_{i_1}})) = w_1$.

[2] This set of polynomials is the analog of the *quadratic representation* in (Sokolov 2020).

Restricting π'_1 by β' we obtain a $\mathsf{SoS}_{\mathbb{C}}$ refutation of the set of polynomials $(P\restriction_{x_{i_1}=\omega_1})\circ \boldsymbol{g}$. Let π_1 be this refutation. By Lemma 5.4 and Lemma 5.7, π_1 has size at most s and, by construction, contains at most $(1-\frac{D}{\ell^\kappa n})|F|$ fat terms.

By repeating this process m times, we get a partial assignment $x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m$ and a $\mathsf{SoS}_{\mathbb{C}}$ refutation π' of the set of polynomials $(P\restriction_{x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m})\circ \boldsymbol{g}$. Since by assumption $m=\lceil \ell^\kappa n\ln(s)/D\rceil$, the resulting π' does not have fat terms anymore, because

$$\left(1-\frac{D}{\ell^\kappa n}\right)^m s \le \exp\left(-\frac{Dm}{\ell^\kappa n}+\ln(s)\right)<1.$$

To conclude the argument, we need to transform π' into an $\mathsf{SoS}_{\mathbb{C}}$ refutation of $P\restriction_{x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m}$ of reduced degree at most $D+d_0$. More concretely for any unassigned x_i, we need to set variables y_{ij} to some univariate polynomial over x_i, so that the corresponding $g_i(\boldsymbol{y}_i)$ evaluates to x_i itself.

We need the indicator function $\chi_a(X)$ for $a\in\{0,\ldots,\kappa-1\}$. More specifically, $\chi_a(X)$ is the univariate polynomial that evaluates to 1 when $X=\zeta^a$ and to 0 when $X=\zeta^b$ with $b\neq a$. That is, $\chi_a(X)$ is defined as

$$\chi_a(X):=\frac{1}{\prod_{0\le i<\kappa, i\neq a}(\zeta^a-\zeta^i)}\prod_{0\le i<\kappa, i\neq a}(X-\zeta^i)$$

expanded as a sum of monomials. Finally, we substitute all the occurrences of the variable y_{ij} in π' for each $i\in[n]$ and $j\in[\ell_i]$ with

$$\sum_{a=0}^{\kappa-1} h_i(\zeta^a)_j\chi_a(x_i). \tag{5.10}$$

We recall that $h_i:\Omega_\kappa\to\Omega_\kappa^{\ell_i}$ is the function witnessing that g_i is compliant, and that $h_i(\zeta^a)_j$ is the jth coordinate of its value on ζ^a.

Let π'' be the result applying the substitution (5.10) to π'. We have that no monomial in π'' has degree bigger than $\frac{D}{\kappa}(\kappa-1)<D$. We now modify π'' to get a proper refutation of $P\restriction_{x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m}$.

The part of π'' that is a "sum-of-squares", i.e., a sum of polynomials of the form ss^*, still remains a sum-of-squares after the substitution.

The only missing part is to derive in degree at most $D + d_0$ the axioms $(P\restriction_{x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m}) \circ \boldsymbol{g}$ to which substitution (5.10) was applied. We set up useful notation: given polynomials $p, q \in \mathbb{C}[\boldsymbol{x}]$, we write $p \equiv q$ to denote the fact that $p-q$ is in the ideal generated by $x_1^\kappa - 1, \ldots, x_n^\kappa - 1$. The following two equivalences

$$g_i\left(\sum_{a=0}^{\kappa-1} h_i(\zeta^a)_1 \chi_a(x_i),\ \ldots,\ \sum_{a=0}^{\kappa-1} h_i(\zeta^a)_{\ell_i} \chi_a(x_i)\right) \equiv x_i \tag{5.11}$$

and

$$\left(\sum_{a=0}^{\kappa-1} h_i(\zeta^a)_j \chi_a(x_i)\right)^\kappa \equiv 1 \tag{5.12}$$

are enough to see that proof π'' can be modified into a proof of $P\restriction_{x_{i_1}=\omega_1,\ldots,x_{i_m}=\omega_m}$ with reduced degree not exceeding $D + d_0$, and to conclude the proof.

To prove (5.11) and (5.12) notice that $\chi_a(x_i)^2 \equiv \chi_a(x_i)$ and, when $a \neq b$, that $\chi_a(x_i)\chi_b(x_i) \equiv 0$ To see (5.12) we have the calculation

$$\begin{aligned}\left(\sum_{a=0}^{\kappa-1} h(\zeta^a)_j \chi_a(x_i)\right)^\kappa &= \sum_{0\le a_1,\ldots,a_k<\kappa} \prod_{\ell\in[\kappa]} h(\zeta^{a_\ell})_j \chi_{a_\ell}(x_i) \\ &\equiv \sum_{a=0}^{\kappa-1} h(\zeta^a)_j^\kappa \cdot \chi_a(x_i) = \sum_{a=0}^{\kappa-1} \chi_a(x_i) = 1.\end{aligned}$$

A similar calculations gives (5.11).

$$\begin{aligned}&g_i\left(\sum_{a=0}^{\kappa-1} h_i(\zeta^a)_1 \chi_a(x_i),\ \ldots,\ \sum_{a=0}^{\kappa-1} h_i(\zeta^a)_{\ell_i} \chi_a(x_i)\right) \\ &\quad\equiv \sum_{a=0}^{\kappa-1} g_i \circ h_i(\zeta^a) \cdot \chi_a(x_i) \\ &\quad= \sum_{a=0}^{\kappa-1} \zeta^a \cdot \chi_a(x_i) = x_i\end{aligned}$$

The last equality holds because $\sum_{a=0}^{\kappa-1} \zeta^a \chi_a(x_i)$ and x_i are two polynomials of degree $< \kappa$ and are equal on all the κth roots of unity. □

6. 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 (2020) 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 Lauria & Nordström (2017), 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. The first author was supported by the Ministerio de Ciencia e Innovación MCIN/AEI/10.13039/501100011033, Spain [grant numbers PID2019-109137GB-C21, PID2019-109137GB-C22, and IJC2018-035334-I].

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

Yaroslav Alekseev, Dima Grigoriev, Edward A. Hirsch & Iddo Tzameret (2020). Semi-Algebraic Proofs, IPS Lower Bounds, and the τ-Conjecture: Can a Natural Number Be Negative? In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC'20)*, 54–67.

Albert Atserias & Tuomas Hakoniemi (2019). Size-Degree Trade-Offs for Sums-of-Squares and Positivstellensatz Proofs. In *Proceedings of the 34th Computational Complexity Conference (CCC'19)*, volume 137 of *LIPIcs*, 24:1–24:20.

Albert Atserias & Joanna Ochremiak (2018). Proof Complexity Meets Algebra. *ACM Trans. Comput. Logic* **20**(1).

Roberto J Bayardo Jr & Robert Schrag (1997). Using CSP look-back techniques to solve real-world SAT instances. In *Proceedings of the 14th National Conference on Artificial Intelligence and 9th Conference on Innovative Applications of Artificial Intelligence (AAAI'97/IAAI'97)*, 203–208.

Christoph Berkholz (2018). The Relation between Polynomial Calculus, Sherali-Adams, and Sum-of-Squares Proofs. In *Proceedings of the 35th Symposium on Theoretical Aspects of Computer Science (STACS'18)*, volume 96, 11:1–11:14.

Grigoriy Blekherman, João Gouveia & James Pfeiffer (2016). Sums of squares on the hypercube. *Mathematische Zeitschrift* 1–14.

Grigoriy Blekherman & Cordian Riener (2020). Symmetric Non-Negative Forms and Sums of Squares. *Discrete and Computational Geometry* **65**(3), 764–799.

Ilario Bonacina, Nicola Galesi & Massimo Lauria (2022). On Vanishing Sums of Roots of Unity in Polynomial Calculus and Sum-Of-Squares. In *Proceedings of the 47th International Symposium on Mathematical Foundations of Computer Science (MFCS'22)*, volume 241 of *LIPIcs*, 23:1–23:15.

Samuel R. Buss, Dima Grigoriev, Russell Impagliazzo & Toniann Pitassi (2001). Linear Gaps between Degrees for the Polynomial Calculus Modulo Distinct Primes. *J. Comput. Syst. Sci.* **62**(2), 267–289. https://doi.org/10.1006/jcss.2000.1726.

Matthew Clegg, Jeff Edmonds & Russell Impagliazzo (1996). Using the Gröbner Basis Algorithm to Find Proofs of Unsatisfiability. In *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC'96)*, 174–183.

John Conway & A. Jones (1976). Trigonometric diophantine equations (On vanishing sums of roots of unity). *Acta Arithmetica* **30**(3), 229–240.

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

Jesús A De Loera, J. Lee, S. Margulies & S. Onn (2009). Expressing Combinatorial Problems by Systems of Polynomial Equations and Hilbert's Nullstellensatz. *Comb. Probab. Comput.* **18**(4), 551–582.

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

Jesús A De Loera, Susan Margulies, Michael Pernpeintner, Eric Riedl, David Rolnick, Gwen Spencer, Despina Stasi & Jon Swenson (2015). 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 (ISSAC'15)*, 133–140.

R. Dvornicich & U. Zannier (2002). Sums of roots of unity vanishing modulo a prime. *Archiv der Mathematik* **79**(2), 104–108.

Roberto Dvornicich & Umberto Zannier (2000). On Sums of Roots of Unity. *Monatshefte für Mathematik* **129**(2), 97–108.

Michael A. Forbes, Amir Shpilka, Iddo Tzameret & Avi Wigderson (2021). Proof Complexity Lower Bounds from Algebraic Circuit Complexity. *Theory Comput.* **17**, 1–88.

Nicola Galesi & Massimo Lauria (2010). Optimality of size-degree tradeoffs for polynomial calculus. *ACM Trans. Comput. Log.* **12**(1), 4:1–4:22.

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

Dima Grigoriev (1998). Tseitin's Tautologies and Lower Bounds for Nullstellensatz Proofs. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS'98)*, 648–652.

Dima Grigoriev & Edward A. Hirsch (2003). Algebraic proof systems over formulas. *Theoretical Computer Science* **303**(1), 83 – 102.

Joshua A. Grochow & Toniann Pitassi (2018). Circuit Complexity, Proof Complexity, and Polynomial Identity Testing: The Ideal Proof System. *J. ACM* **65**(6), 37:1–37:59.

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

Russell Impagliazzo, Sasank Mouli & Toniann Pitassi (2020). The Surprising Power of Constant Depth Algebraic Proofs. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS'20)*, 591–603.

Russell Impagliazzo, Sasank Mouli & Toniann Pitassi (2022). Lower bounds for Polynomial Calculus with extension variables over finite fields. *Electron. Colloquium Comput. Complex.* **TR22-038**. URL https://eccc.weizmann.ac.il/report/2022/038.

Daniela Kaufmann, Paul Beame, Armin Biere & Jakob Nordström (2022). 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)*.

Daniela Kaufmann & Armin Biere (2020). Nullstellensatz-Proofs for Multiplier Verification. In *Proceedings of the 22nd International Workshop on Computer Algebra in Scientific Computing (CASC'20)*, 368–389.

Daniela Kaufmann, Armin Biere & Manuel Kauers (2019). Verifying Large Multipliers by Combining SAT and Computer Algebra. In *Proceedings of the 2019 Formal Methods in Computer Aided Design (FMCAD'19)*, 28–36.

Daniela Kaufmann, Armin Biere & Manuel Kauers (2020). From DRUP to PAC and Back. In *Proceedings of the 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE'20)*, 654–657.

T.Y Lam & K.H Leung (2000). On Vanishing Sums of Roots of Unity. *Journal of Algebra* **224**(1), 91–109.

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

Massimo Lauria & Jakob Nordström (2017). Graph Colouring is Hard for Algorithms Based on Hilbert's Nullstellensatz and Gröbner Bases. In *Proceedings of the 32nd Computational Complexity Conference (CCC'17)*, volume 79, 2:1–2:20.

Troy Lee, Anupam Prakash, Ronald de Wolf & Henry Yuen (2016). On the sum-of-squares degree of symmetric quadratic functions. In *Proceedings of the 31st Conference on Computational Complexity (CCC'16)*, volume 50 of *LIPIcs. Leibniz Int. Proc. Inform.*, Art. No. 17, 31.

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

M.W. Moskewicz, C.F. Madigan, Y. Zhao, L. Zhang & S. Malik (2001). Chaff: Engineering an efficient SAT solver. In *Proceedings of the 38th annual Design Automation Conference (DAC'01)*, 530–535.

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

Aaron Potechin (2020). Sum of Squares Bounds for the Ordering Principle. In *35th Computational Complexity Conference (CCC'20)*, volume 169 of *LIPIcs*, 38:1–38:37.

Susanna F. de Rezende, Massimo Lauria, Jakob Nordström & Dmitry Sokolov (2021). The Power of Negative Reasoning. In *Proceedings of the 36th Computational Complexity Conference (CCC'21)*, volume 200 of *LIPIcs*, 40:1–40:24.

Grant Schoenebeck (2008). Linear Level Lasserre Lower Bounds for Certain k-CSPs. In *49th Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, 593–602.

Roman Smolensky (1987). Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC'87)*, 77–82. ACM.

Dmitry Sokolov (2020). (Semi)Algebraic proofs over $\{\pm 1\}$ variables. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC'20)*.

Madhur Tulsiani (2009). CSP gaps and reductions in the Lasserre hierarchy. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC'09)*, 303–312. ACM.

Manuscript received 9 November 2022

Ilario Bonacina
UPC Barcelona Tech
Barcelona, Catalonia, Spain
ilario.bonacina@upc.edu

Nicola Galesi
Sapienza Università di Roma
Rome, Italy
nicola.galesi@uniroma1.it

Massimo Lauria
Sapienza Università di Roma
Rome, Italy
massimo.lauria@uniroma1.it