On Vanishing Sums of Roots of Unity in Polynomial Calculus and Sum-of-“Squares”

Ilario Bonacina

UPC Barcelona Tech

Haifa, August 1 2022 Proof Complexity Workshop

Joint work with Nicola Galesi and Massimo Lauria (to appear in MFCS’22)

Plan of the talk

- Non-Boolean encodings
- Polynomial Calculus over $\mathbb{C}$
- Sum-of-“Squares” over $\mathbb{R}$ and $\mathbb{C}$
- Sums of Roots of Unity and Knapsack
- Hint on lower bound techniques

Definitions **Results** **Examples**

Boolean and Fourier encodings

Two natural encodings for CSPs

Fourier variables $z^\kappa = 1$

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

where ζ is a primitive κ-th root of unity

Boolean variables $x^2 = x$

$$x \in \{0,1\}$$

Two natural encodings for CSPs

Fourier variables $z^\kappa = 1$

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

where ζ is a primitive κ-th root of unity

$z = x_0 + x_1\zeta + \cdots + \zeta^{\kappa-1}x_{\kappa-1}$

Together with the constraints

$x_0 + \cdots + x_{\kappa-1} = 1$

and $x_0^2 = x_0, \ldots, x_{k-1}^2 = x_{k-1}$

Boolean variables $x^2 = x$

$x \in \{0,1\}$

Given $G = (V, E)$ a graph. Is G 3-colorable?

Boolean encoding

x_{vc} "the vertex v gets color c"

$$\left.\begin{array}{l} x_{v0} + x_{v1} + x_{v2} = 1 \\ x_{v0}^2 = x_{v0} \quad x_{v1}^2 = x_{v1} \quad x_{v2}^2 = x_{v2} \end{array}\right\} \quad \forall v \in G$$

$$\left.\begin{array}{r} x_{v0}x_{w0} = 0 \\ x_{v1}x_{w1} = 0 \\ x_{v2}x_{w2} = 0 \end{array}\right\} \quad \forall \{v, w\} \in E$$

Fourier encoding

z_v "the color given to vertex v"

$$\forall v \in G \quad \left\{ z_v^3 = 1 \right.$$

$$\forall \{v, w\} \in E \quad \left\{ z_v^2 + z_v z_w + z_w^2 = 0 \right.$$

A practical motivation

The Fourier encoding is actually used in practice to solve k-**COLORING** and **verification of arithmetic multiplier circuits** via Groebner basis computations.

Polynomial Calculus

Polynomial Calculus over $\mathbb{C}$ ($PC_{\mathbb{C}}$)

Y set of n variables, $P = \{p_1 = 0, \ \dots \ , p_m = 0\}$ where $p_j \in \mathbb{C}[Y]$

Proof of unsatisfiability of P

from P derive $1 = 0$ using the inference rules

$$\frac{p = 0}{qp = 0} \qquad\qquad \frac{p = 0 \quad q = 0}{p + q = 0}$$

Complexity measures

Degree: max degree of a polynomial

Size: number of monomials

Remarks on $PC_{\mathbb{C}}$

THM. Degree D lower bounds in $PC_{\mathbb{C}}$, over **Boolean** variables imply size $\exp\left(\frac{(D-d)^2}{n}\right)$ lower bounds [IPS'99]

No such result could exist over the Fourier variables.

PC over Fourier variables was also studied in [BGIP'01], but only for degree

$PC_{\mathbb{C}}$ on Fourier variables - *a "problematic" example*

Tseitin over Fourier variables

$G = (V, E)$ with $|V|$ odd

$$\prod_{e \ni v} x_e = -1 \text{ for all } v \in V$$

$x_e^2 = 1$ for all $e \in E$

$PC_{\mathbb{C}}$ on Fourier variables - *a "problematic" example*

Tseitin over Fourier variables

$G = (V, E)$ with $|V|$ odd

$$\prod_{e \ni v} x_e = -1 \text{ for all } v \in V$$

$x_e^2 = 1$ for all $e \in E$

- short $PC_{\mathbb{C}}$ proofs
- $\Omega(n)$ degree lower bound on expander graphs
- hence no size-degree tradeoff when using Fourier variables

Sum of Squares

Sum-of-Squares $SOS_{\mathbb{R}}$

Y set of n variables, $P = \{p_1 = 0, \ \dots \ , p_m = 0\}$ where $p_j \in \mathbb{R}[Y]$

Proof of unsatisfiability of P

$$p_1 q_1 + \dots + p_m q_m + s_1^2 + \dots + s_\ell^2 = -1$$

Complexity measures

Degree: $\max\{\deg(q_i p_i), \deg(s_j^2) : i \in [m], j \in [\ell]\}$

Size: number of monomials in the proof

Degree and Size

Degree and Size

THM. Over **Boolean** variables,

Degree D lower bounds in $SOS_{\mathbb{R}}$ imply size $\exp\left((D-d)^2/n\right)$

lower bounds [AH'19]

Degree and Size

THM. Over **Boolean** variables,

Degree D lower bounds in $SOS_{\mathbb{R}}$ imply size $\exp\left((D-d)^2/n\right)$

lower bounds [AH'19]

THM. Over **Fourier** $\{\pm 1\}$ variables,

Degree D lower bounds in $SOS_{\mathbb{R}}$ imply size $\exp\left((D-d)^2/n\right)$

lower bounds but **for a different set of polynomials** [S'20]

Sum-of-"Squares" over $\mathbb{C}$ $(SOS_{\mathbb{C}})$

Y set of variables, $P = \{p_1 = 0, \ \dots \ , p_m = 0\}$ where $p_j \in \mathbb{C}[Y]$

Proof of unsatisfiability of P

$$p_1 q_1 + \dots + p_m q_m + s_1 s_1^* + \dots + s_\ell s_\ell^* = -1$$

where s_j^* is the *formal conjugate* of s_j

Sum-of-"Squares" over $\mathbb{C}$ ($SOS_{\mathbb{C}}$)

Y set of variables, $P = \{p_1 = 0, \ \dots \ , p_m = 0\}$ where $p_j \in \mathbb{C}[Y]$

Proof of unsatisfiability of P

$$p_1 q_1 + \dots + p_m q_m + s_1 s_1^* + \dots + s_\ell s_\ell^* = -1$$

where s_j^* is the *formal conjugate* of s_j

on Boolean variables: s^* is the conjugate of s

Sum-of-"Squares" over $\mathbb{C}$ ($SOS_{\mathbb{C}}$)

Y set of variables, $P = \{p_1 = 0, \ \dots \ , p_m = 0\}$ where $p_j \in \mathbb{C}[Y]$

Proof of unsatisfiability of P

$$p_1 q_1 + \dots + p_m q_m + s_1 s_1^* + \dots + s_\ell s_\ell^* = -1$$

where s_j^* is the *formal conjugate* of s_j

on Boolean variables: s^* is the conjugate of s

on Fourier variables $z^\kappa = 1$: s^* is the conjugate of s after substituting z^j with $z^{\kappa - j}$

Sum-of-"Squares" over $\mathbb{C}$ ($SOS_{\mathbb{C}}$)

Y set of variables, $P = \{p_1 = 0, \ \dots \ , p_m = 0\}$ where $p_j \in \mathbb{C}[Y]$

Proof of unsatisfiability of P

$$p_1q_1 + \ldots + p_mq_m + s_1s_1^* + \ldots + s_\ell s_\ell^* = -1$$

where s_j^* is the *formal conjugate* of s_j

on Boolean variables: s^* is the conjugate of s

on Fourier variables $z^\kappa = 1$: s^* is the conjugate of s after substituting z^j with $z^{\kappa-j}$

Complexity measures

Degree: $\max\{\deg(q_ip_i), \deg(s_js_j^*) : i \in [m], j \in [\ell]\}$

Size: number of monomials in the proof

Examples of conjugate polynomials

On **Boolean** variables:

$$p = ix + 1 \qquad p^* = -ix + 1$$

$$pp^* = x^2 + 1$$

On **Fourier** variables ($z^\kappa = 1$):

$$p = iz + 1 \qquad p^* = -iz^{\kappa-1} + 1$$

$$pp^* = z^k + iz - iz^{\kappa-1} + 1$$

More Examples

Example 1. $P = \{ \sum_{j \in [n]} x_j = \underline{i},\ x_1^2 = x_1, \ldots, x_n^2 = x_n \}$

$$-(\sum_j x_j + \underline{i})(\sum_j x_j - \underline{i}) + (\sum_j x_j)^2 = -1$$

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

$$(\sum_j z_j^{\kappa-1} - 1) - (\sum_j z_j + 1)(\sum_j z_j^{\kappa-1}) + \sum_j z_j \sum_j z_j^{\kappa-1} = -1$$

Some remarks on $SOS_{\mathbb{C}}$

THM. $SOS_{\mathbb{C}}$ over the Boolean/Fourier encoding p-simulates $PC_{\mathbb{C}}$ over the same encoding.

THM. For polynomials with real coefficients and Boolean encoding, $SOS_{\mathbb{C}}$ is equivalent to $SOS_{\mathbb{R}}$

Some remarks on $SOS_{\mathbb{C}}$

THM. $SOS_{\mathbb{C}}$ over the Boolean/Fourier encoding p-simulates $PC_{\mathbb{C}}$ over the same encoding.

Proof idea. A minor variation of Berkholtz's argument [B'18].

THM. For polynomials with real coefficients and Boolean encoding, $SOS_{\mathbb{C}}$ is equivalent to $SOS_{\mathbb{R}}$

Some remarks on $SOS_{\mathbb{C}}$

THM. $SOS_{\mathbb{C}}$ over the Boolean/Fourier encoding p-simulates $PC_{\mathbb{C}}$ over the same encoding.

Proof idea. A minor variation of Berkholtz's argument [B'18].

THM. For polynomials with real coefficients and Boolean encoding, $SOS_{\mathbb{C}}$ is equivalent to $SOS_{\mathbb{R}}$

Proof idea. The real part of the $SOS_{\mathbb{C}}$ refutation is a valid $SOS_{\mathbb{R}}$ refutation.

Knapsack & Sums of Roots of Unity

Knapsack & Sums of Roots of Unity

$$\mathrm{Kn}_{\vec{c},r} = \left\{ \sum_{i=1}^{n} c_i x_i = r \ , \quad x_1^2 = x_1 \ , \quad \ldots \quad , x_n^2 = x_n \right\} \text{ with } c_1, \ldots c_n, r \in \mathbb{C}$$

(Interesting special case $c_1, \ldots, c_n = 1$)

$$SRU_n^{\kappa,r} = \left\{ \sum_{i \in [n]} z_i = r, \quad z_1^\kappa = 1 \ , \quad \ldots \quad , z_n^\kappa = 1 \right\} \text{ with } r \in \mathbb{C}$$

(Interesting special case $r = 0$)

How hard is to refute $SRU_n^{\kappa,r}$ in $PC_{\mathbb{C}}/SOS_{\mathbb{C}}$?

Wait, when is $SRU_n^{\kappa,r}$ unsatisfiable?

$SRU_n^{\kappa,0}$ when is satisfiable?

Proof. Assume $SRU_n^{\kappa,0}$ is satisfiable, i.e. $\alpha_1 + \ldots + \alpha_n = 0$ for some κth roots of unity α_j. I.e. there are $a_0, \ldots, a_{\kappa-1} \in \mathbb{N}$ s.t.

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{\kappa-1}\zeta^{\kappa-1} = 0$$

where ζ is a primitive κth roots of unity (i.e. root of $X^{\kappa-1} + X^{\kappa-2} + \cdots + X + 1$). But then, ζ is a root of the polynomial

$$(a_0 - a_{\kappa-1}) + (a_1 - a_{\kappa-1})X + \cdots + (a_{\kappa-2} - a_{\kappa-1})X^{\kappa-2},$$

which then must be identically 0 and $a_0 = a_1 = a_2 = \ldots = a_{\kappa-1}$.

$SRU_n^{\kappa,0}$ when is satisfiable?

THM. If κ prime, $SRU_n^{\kappa,0}$ is satisfiable if and only if κ divides n.

Proof. Assume $SRU_n^{\kappa,0}$ is satisfiable, i.e. $\alpha_1 + \ldots + \alpha_n = 0$ for some κth roots of unity α_j. I.e. there are $a_0, \ldots, a_{\kappa-1} \in \mathbb{N}$ s.t.

$$a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{\kappa-1}\zeta^{\kappa-1} = 0$$

where ζ is a primitive κth roots of unity (i.e. root of $X^{\kappa-1} + X^{\kappa-2} + \cdots + X + 1$).
But then, ζ is a root of the polynomial

$$(a_0 - a_{\kappa-1}) + (a_1 - a_{\kappa-1})X + \cdots + (a_{\kappa-2} - a_{\kappa-1})X^{\kappa-2},$$

which then must be identically 0 and $a_0 = a_1 = a_2 = \ldots = a_{\kappa-1}$.

Sums of Roots of Unity - *satisfiability*

$$SRU_n^{\kappa,r} = \left\{ \sum_{i\in[n]} z_i = r, \quad z_1^{\kappa} = 1\ , \quad \dots \quad , z_n^{\kappa} = 1 \right\} \text{ with } r \in \mathbb{C}$$

(Interesting special case $r = 0$)

THM. If $\kappa = p^m$ for some prime p,

$SRU_n^{\kappa,0}$ is satisfiable if and only if p divides n.

Sums of Roots of Unity - *satisfiability*

$$SRU_n^{\kappa,r} = \left\{ \sum_{i\in[n]} z_i = r, \quad z_1^\kappa = 1 \,, \quad \dots \quad , z_n^\kappa = 1 \right\}$$ with $r \in \mathbb{C}$

(Interesting special case $r = 0$)

THM. If $\kappa = p^m$ for some prime p,

$SRU_n^{\kappa,0}$ is satisfiable if and only if p divides n.

~~**THM.** If κ not a power of a prime,~~

~~$SRU_n^{\kappa,0}$ for n large enough is always satisfiable. [LL'01]~~

Knapsack - *results*

$$\mathrm{Kn}_{\vec{c},r} = \left\{ \sum_{i=1}^{n} c_i x_i = r \ , \quad x_1^2 = x_1 \ , \quad \dots \quad , x_n^2 = x_n \right\} \text{ with } c_1, \dots c_n, r \in \mathbb{C}$$

(Interesting special case $c_1, \dots, c_n = 1$)

Knapsack - *results*

$$\mathrm{Kn}_{\vec{c},r} = \left\{ \sum_{i=1}^{n} c_i x_i = r \ , \quad x_1^2 = x_1 \ , \quad \ldots \quad , x_n^2 = x_n \right\} \text{ with } c_1, \ldots c_n, r \in \mathbb{C}$$

(Interesting special case $c_1, \ldots, c_n = 1$)

THM. $\mathrm{Kn}_{\vec{c},r}$ is always hard to refute in $PC_{\mathbb{C}}$: degree $\Omega(n)$ and size $2^{\Omega(n)}$

[IPS'99]

Knapsack - *results*

$$\mathrm{Kn}_{\vec{c},r} = \left\{ \sum_{i=1}^{n} c_i x_i = r \ , \quad x_1^2 = x_1 \ , \quad \ldots \quad , x_n^2 = x_n \right\} \text{ with } c_1, \ldots c_n, r \in \mathbb{C}$$

(Interesting special case $c_1, \ldots, c_n = 1$)

THM. $\mathrm{Kn}_{\vec{c},r}$ is always hard to refute in $PC_{\mathbb{C}}$: degree $\Omega(n)$ and size $2^{\Omega(n)}$ [IPS'99]

THM. In $SOS_{\mathbb{C}}$ the hardness of $\mathrm{Kn}_{\vec{1},r}$ depends on r:

- $r \in \mathbb{R}$ the hardness is the same as for $SOS_{\mathbb{R}}$:

  degree $\geq \min\{n, 2\min\{r, n-r\} + 3\}$ [G'01]

-For $r \notin \mathbb{R}$ it is **easy** in $SOS_{\mathbb{C}}$

$SRU_n^{\kappa,r}$ requires large degree in $PC_{\mathbb{C}}$

What about SOS?

$SRU_n^{\kappa,r}$ requires large degree in $PC_{\mathbb{C}}$

THM. $PC_{\mathbb{C}}$ refutations of $SRU_n^{\kappa,r}$ require degree $\Omega(n)$.

(Hint: focus on just two of the roots and via a linear transformation reduce to knapsack)

What about SOS?

Hardness of $SRU_n^{\kappa,r}$ in SOS

κ prime

ζ primitive κth root of unity

$r = r_1 + \zeta r_2$ with $r_1, r_2 \in \mathbb{R}$

THM. (Degree lower bound)

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

then $SOS_{\mathbb{C}}$ refutations of $SRU_n^{\kappa,r}$ require degree at least D

COR. $SOS_{\mathbb{C}}$ refutations of $SRU_n^{\kappa,0}$ require degree $\Omega(n/\kappa)$

THM. (Size lower bound)

If $n \gg \kappa$, $SOS_{\mathbb{C}}$ refutations of $SRU_n^{\kappa,0}$ require size $2^{\Omega(n)}$

Degree lower bounds

Proof Technique for degree in $SOS_{\mathbb{R}}$

$\{p_1 = 0, \; \dots \; , p_m = 0\}$

does not have $SOS_{\mathbb{R}}$

refutations of degree $\leq D$

$\Longleftrightarrow$

$\exists$ **Pseudo-expectation** $\mathbb{E} : \mathbb{R}[Y]_{\leq D} \to \mathbb{R}$ s.t.

- $\mathbb{E}(1) = 1$
- $\mathbb{E}$ linear
- $\mathbb{E}(q_j p_j) = 0$ for all q_j s.t $\deg(q_j p_j) \leq D$
- $\mathbb{E}(s^2) \geq 0$ for all s s.t. $\deg(s^2) \leq D$

Proof Technique for degree in $SOS_{\mathbb{C}}$

$\{p_1 = 0, \ \dots \ , p_m = 0\}$

does not have $SOS_{\mathbb{C}}$

refutations of degree $\leq D$

$\Longleftrightarrow$

$\exists$ **Pseudo-expectation** $\mathbb{E} : \mathbb{R}[Y]_{\leq D} \to \mathbb{R}$ s.t.

- $\mathbb{E}(1) = 1$
- $\mathbb{E}$ linear
- $\mathbb{E}(q_j p_j) = 0$ for all q_j s.t $\deg(q_j p_j) \leq D$
- $\mathbb{E}(ss^*) \geq 0$ for all s s.t. $\deg(ss^*) \leq D$

Degree lower bounds of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

The reduction to knapsack does not work for $SOS_{\mathbb{C}}$, instead:

Degree lower bounds of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

The reduction to knapsack does not work for $SOS_{\mathbb{C}}$, instead:

- Use the associate Boolean encoding of $SRU_n^{\kappa,r}$

Degree lower bounds of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

The reduction to knapsack does not work for $SOS_{\mathbb{C}}$, instead:

- Use the associate Boolean encoding of $SRU_n^{\kappa,r}$
- Construct a candidate pseudo-expectation E (only one choice under symmetry)

Degree lower bounds of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

The reduction to knapsack does not work for $SOS_{\mathbb{C}}$, instead:

- Use the associate Boolean encoding of $SRU_n^{\kappa,r}$
- Construct a candidate pseudo-expectation E (only one choice under symmetry)
- Interpret $E(p)$ as the evaluation of a symmetric polynomial S_E

Degree lower bounds of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

The reduction to knapsack does not work for $SOS_{\mathbb{C}}$, instead:

- Use the associate Boolean encoding of $SRU_n^{\kappa,r}$
- Construct a candidate pseudo-expectation E (only one choice under symmetry)
- Interpret $E(p)$ as the evaluation of a symmetric polynomial S_E
- Use **Bleckherman's theorem** (adapted to $\mathbb{C}$) to prove properties of S_E

Degree lower bounds of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

The reduction to knapsack does not work for $SOS_{\mathbb{C}}$, instead:

- Use the associate Boolean encoding of $SRU_n^{\kappa,r}$
- Construct a candidate pseudo-expectation E (only one choice under symmetry)
- Interpret $E(p)$ as the evaluation of a symmetric polynomial S_E
- Use **Bleckherman's theorem** (adapted to $\mathbb{C}$) to prove properties of S_E
- E is a pseudo-expectation

Blekherman's theorem

$Y = \{y_1, \ldots, y_n\}$ $\quad p \in \mathbb{C}[Y]$

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

$$\|Y\| = y_1 + \ldots + y_n$$

For **knapsack** and the **sum-of-roots-of-unity**,

$\mathbb{E}(p)$ and the evaluation of $\mathrm{Sym}(p)$ in some point are related

THM. (Blekherman) $p \in \mathbb{C}[Y]$ **of degree** d

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

Size lower bounds

Size lower bound of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

Size lower bound of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

- The technique is a non-trivial adaptation of Sokolov's **gadgets** from $\{\pm 1\}$ variables to generic Fourier variables. [S'20]

Size lower bound of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

- The technique is a non-trivial adaptation of Sokolov's **gadgets** from $\{\pm 1\}$ variables to generic Fourier variables. [S'20]
- A degree-D $SOS_{\mathbb{C}}$ lower bound for P, implies a monomial size lower bound for $P \circ \boldsymbol{g}$ of the form $\exp\left(\frac{(D-d)^2}{\kappa^\kappa n}\right)$

Size lower bound of $SRU_n^{\kappa,r}$ in $SOS_{\mathbb{C}}$

- The technique is a non-trivial adaptation of Sokolov's **gadgets** from $\{\pm 1\}$ variables to generic Fourier variables. [S'20]
- A degree-D $SOS_{\mathbb{C}}$ lower bound for P, implies a monomial size lower bound for $P \circ \boldsymbol{g}$ of the form $\exp\left(\frac{(D-d)^2}{\kappa^{\kappa} n}\right)$
- The gadget could be taken as a sum of variables and hence it transforms instances of SRU into itself.

Open problems

Open problems

For what $\overrightarrow{c}, r$ the knapsack $\mathrm{Kn}_{\overrightarrow{c},r}$ is hard for $SOS_{\mathbb{R}}$?

Open problems

For what $\overrightarrow{c}, r$ the knapsack $\mathrm{Kn}_{\overrightarrow{c},r}$ is hard for $SOS_{\mathbb{R}}$?

Does $SOS_{\mathbb{C}}$ over the $\{\pm 1\}$-encoding p-simulate resolution?

Open problems

For what $\overrightarrow{c}, r$ the knapsack $\mathrm{Kn}_{\overrightarrow{c},r}$ is hard for $SOS_{\mathbb{R}}$?

Find new techniques to prove size lower bounds in $SOS_{\mathbb{C}}$ for encodings based on non-binomial ideals, e.g. for the $\{1,2\}$-encoding.

Does $SOS_{\mathbb{C}}$ over the $\{\pm 1\}$-encoding p-simulate resolution?

Open problems

For what $\overrightarrow{c}, r$ the knapsack $\mathrm{Kn}_{\overrightarrow{c},r}$ is hard for $SOS_{\mathbb{R}}$?

Find new techniques to prove size lower bounds in $SOS_{\mathbb{C}}$ for encodings based on non-binomial ideals, e.g. for the $\{1,2\}$-encoding.

Does $SOS_{\mathbb{C}}$ over the $\{\pm 1\}$-encoding p-simulate resolution?

Open problems

For what $\overrightarrow{c}, r$ the knapsack $\mathrm{Kn}_{\overrightarrow{c},r}$ is hard for $SOS_{\mathbb{R}}$?

Find new techniques to prove size lower bounds in $SOS_{\mathbb{C}}$ for encodings based on non-binomial ideals, e.g. for the $\{1,2\}$-encoding.

Prove degree/size lower bounds in $PC_{\mathbb{C}}$/$SOS_{\mathbb{C}}$ for 3-Coloring on an Erdos-Renyi random graph and with the Fourier encoding.

Known worst case degree lower bounds in $PC_{\mathbb{C}}$ [LN'17]

Does $SOS_{\mathbb{C}}$ over the $\{\pm 1\}$-encoding p-simulate resolution?

Thanks!

Questions?

- Non-Boolean encodings
- Polynomial Calculus over $\mathbb{C}$
- Sum-of-“Squares” over $\mathbb{R}$ and $\mathbb{C}$
- Sums of Roots of Unity and Knapsack
- Lower bound techniques
- Open problems