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

Ilario Bonacina

UPC Barcelona Tech

Wien, August 25 2022 MFCS

Joint work with Nicola Galesi and Massimo Lauria

This talk in one sentence

"Sum-of-Squares, the proof system underlying semi-definite programming, cannot reason about divisibility."

Plan of the talk

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

Definitions **Results** **Examples**

Boolean and Fourier encodings

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

Boolean encoding

x_{vc} “the vertex v gets color c”

Fourier encoding

z_v “the color given to vertex v”

$$\left.\begin{array}{l} x_{v0} + x_{v1} + x_{v2} = 1 \\ x_{v0}^2 = x_{v0} \quad x_{v1}^2 = x_{v1} \quad x_{v2}^2 = x_{v2} \end{array}\right\} \quad \forall v \in G \quad \left\{ z_v^3 = 1 \right.$$

$$\left.\begin{array}{l} x_{v0}x_{w0} = 0 \\ x_{v1}x_{w1} = 0 \\ x_{v2}x_{w2} = 0 \end{array}\right\} \quad \forall \{v, w\} \in E \quad \left\{ z_v^2 + z_v z_w + z_w^2 = 0 \right.$$

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

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

Boolean variables $x^2 = x$

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

together with the constraints

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

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

A practical motivation

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

Sum of Squares

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

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

Proof of unsatisfiability of P

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

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

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

Proof of unsatisfiability of P

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

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

Knapsack

$$\mathrm{Kn}_n^r = \left\{ \sum_{i=1}^{n} x_i = r \,, \quad x_1^2 = x_1 \,, \quad \ldots \quad , x_n^2 = x_n \right\}$$

(Interesting special case $r \approx \dfrac{n}{2}$)

Example. A refutation of Kn_n^{-1} in $SOS_{\mathbb{R}}$:

$$-(\sum_j x_j + 1) - \sum_j (x_j^2 - x_j) + \sum_j x_j^2 = -1$$

Thm. [G'01] The hardness of Kn_n^r in $SOS_{\mathbb{R}}$ depends on r:

degree $\geq \min\{n, 2\min\{r, n-r\} + 3\}$

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

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

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

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

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 $z^{\kappa-j}$

Complexity measures

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

Size: number of monomials in the proof

Examples of conjugate polynomials

On **Boolean** variables:

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

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

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

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

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

Knapsack (again)

Example. A refutation of Kn_n^{i} in $SOS_{\mathbb{R}}$:

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

THM. In $SOS_{\mathbb{C}}$ the hardness of Kn_n^{r} depends on r:

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

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

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

Thm. [AH'19] Over **Boolean** variables,

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

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

Thm. [AH'19] Over **Boolean** variables,

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

Thm. [S'20] 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**

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

Thm. [AH'19] Over **Boolean** variables,

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

Thm. [S'20] 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**

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.

Sums of Roots of Unity

Sums of Roots of Unity

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

(Interesting special case $r = 0$)

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]

Sums of Roots of Unity

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

(Interesting special case $r = 0$)

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]

SOS cannot reason about divisibility

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 lb in $SOS_{\mathbb{C}}$

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

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

refutations of degree $\leq D$

$\Leftrightarrow$

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

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

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

- 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

Size lower bounds

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.

Thanks!

Questions?

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

“Sum-of-Squares, the proof system underlying semi-definite programming, cannot reason about divisibility.”