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

Ilario Bonacina

UPC Barcelona Tech

June 30 2022, Workshop "Complexity Theory with a Human Face"

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

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

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

Complexity measures

Degree: max degree of a polynomial

Size: number of monomials

Two natural encodings for CSPs

Fourier variable $z^\kappa = 1$

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

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 variable $x^2 = x$

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

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

Boolean encoding

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

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

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

Fourier encoding

z_v "the color given to vertex v"

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

Sum-of-Squares

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

Proof Techniques

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

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

refutations of degree $\leq D$

$\Leftrightarrow$

$\exists$ **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. $\deg(s^2) \leq D$

Over **Boolean** variables,

Degree D lower bounds in

$SOS_{\mathbb{R}}$ imply size

$\exp\left((D-d)^2/n\right)$ lower

bounds [AH'19]

Over $\{\pm 1\}$ variables,

Degree D lower bounds imply size

$\exp\left((D-d)^2/n\right)$ **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

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

EX1. $P = \{ \sum_{j\in[n]} x_j = \underline{i},\ x_1^2 = x_1, \ldots, x_n^2 = x_n \}$

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

EX2. $P = \{ \sum_{j\in[n]} z_j = 1,\ \sum_{j\in[n]} z_j^{\kappa-1} = -1,\ z_1^{\kappa} = 1 \ldots, z_n^{\kappa} = 1 \}$

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

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

PROP. $SOS_{\mathbb{C}}$ 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].

PROP. 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

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

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

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

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 $SOS_{\mathbb{C}}$

Sums of Roots of Unity

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

(Interesting special case $r = 0$)

If κ not a power of a prime,

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

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

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

Ex. $PC_{\mathbb{C}}$ 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)

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

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

The reduction to knapsack <u>does not</u> 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 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 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 transforms instances of SRU into itself.

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 $SOS_{\mathbb{C}}$ 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?