A largish sum-of-squares implies circuit hardness (& derandomization)

Nitin Saxena (CSE@IIT Kanpur, India)

(ITCS’21, with Pranjal Dutta & Thomas Thierauf)

July 2021, IISER Pune (virtually)
Sum of Squares (SOS) Representation
SOS hardness

Algebraic Circuits
SOS hardness => Circuit hardness

Blackbox Identity Testing (PIT)

Sum-of-Cubes (SOC) hardness
SOC hardness => Blackbox PIT

Conclusion
Sum-of-Squares (SOS) Representation

- For a polynomial $f$ over $\mathbb{F}$, the SOS representation is:
  - $f = c_1 f_1^2 + \ldots + c_t f_t^2$, where $c_i \in \mathbb{F}$, $f_i \in \mathbb{F}[x_1, \ldots, x_n]$.
  - **Size** is number of monomials $\sum_i |f_i|_0$.
  - Denote the minimal size by support-sum $S(f)$.

- It's a *complete* model, if $\text{char} \mathbb{F} \neq 2$.
  - Trivially, $S(f) \leq 4 \cdot |f|_0$.

- For simplicity, consider *univariate* SOS representations ($n=1$).

**Example:** For $\deg d$ univariate $f(x)$, simply use monomials
\[ \{ x^i, x^{i/d} \mid 0 \leq i < \sqrt{d} \} . \]
- (Agrawal'20) $t = 2 \cdot \sqrt{d}$ many squares suffice for any $f$.
- Overall, expect $S(f) \geq 2 \sqrt{d} \cdot 2 \sqrt{d} = 4d$.
SOS Representation

- Does there exist degree-\(d\) \(f(x)\) with \(S(f) \geq \Omega(d)\)?
  - By dimension-argument it exists!
  - Assume \(\mathbb{F} = \mathbb{C}\).

- To be of any help in complexity theory, we have to study SOS for polynomials that are explicit.
  - We would work with several definitions.
  - Eg. \((x+1)^d\) is `explicit'.
SOS Representation – History

- (1770) Lagrange's 4-squares thm: Integer as SOS of 4 squares.
  - Several such examples in number theory (Ramanujan 1917).
  - Pythagorean triples, Fermat's 2-squares, Legendre's 3-squares

- (1900) Hilbert's 17th Problem: Positive Real polynomials as SOS of rational functions?
  - Note: $c_i = 1$.

- (1990s) SOS constraints in convex optimization.
  - Lasserre hierarchy of relaxations in SDP (based on deg).
Contents

- Sum-of-Squares (SOS) Representation
- **SOS hardness**
- Algebraic Circuits
- SOS hardness => Circuit hardness
- Blackbox Identity Testing (PIT)
- Sum-of-Cubes (SOC) hardness
- SOC hardness => Blackbox PIT
- Conclusion
SOS Hardness

**Defn:** A degree-\(d\) \(f(x)\) is **explicit** if it's coefficient-function \(\text{coef}(x_i^j)(f)\) is `easy':
- Given \((i,j)\) the \(j\)-th bit of coef\((x_i^j)(f)\) is polylog\((d)\)-time.
- Or, ...is in \#P/poly.
- Or, ...is in \(\text{CH}\).

**SOS-hard:** There's an explicit \(f\) and \(\epsilon > 0\) with \(S(f) > d^{\epsilon+0.5}\).
- \(\epsilon = 0\) trivial. Existentially, much stronger property holds.

- There are numerous candidates for \(f(x)\):
  - \((x+1)^d\)
  - \(\sum_i 2^{i^2} x^i\)
  - \(\prod_i (x+i)\)

\(\sum_i 2^i x^i\) is not a candidate!

Sub-constant/ vanishing fn?

\(\text{exp}(x) \leq d := \sum_{i=0}^{d} x^i/i!\)

Yet useful?
SOS Hardness – Comparisons

- Concept is quite **weak/ incomparable** to earlier ones about uni/multi-variate polynomials. As they needed sum-of **unbounded-powers** (or `power'ful):
  - (AV'08)..(GKKS'13)..(AGS'18) *Hardness* for special depth-4/3.
  - (Koiran'10) *Tau-conjecture* about roots of depth-4 expressions.
  - (KPTT'15) *Newton-polygon-Tau-conjecture* for sum-of unbounded-powers.
  - (Raz'08) **Super-poly-elusive** functions eluding degree-2 maps.

- \((x+1)^d\) good candidate for SOS-hardness. Not so, for the earlier conjectures.

**SOS-hard (n-variate):** There's *explicit* \( f(x_1,\ldots,x_n) \) and \( \varepsilon > 0 \) with \( S(f) > \binom{n+d}{n} \varepsilon + 0.5 \).

- Constant \( n \).
Contents

- Sum-of-Squares (SOS) Representation
- SOS hardness
- Algebraic Circuits
- SOS hardness => Circuit hardness
- Blackbox Identity Testing (PIT)
- Sum-of-Cubes (SOC) hardness
- SOC hardness => Blackbox PIT
- Conclusion
Algebraic Circuits

- Circuit has addition/multiplication gates; connected by wires.
  - Input variables at leaves are $x_1, ..., x_n$; output $f(x)$.
  - size($f$) is minimum graph-size of such a circuit.

- (1979) Valiant's Conjecture: $VP \neq VNP$.
  - VP – polynomial-families, poly($n$)-degree, poly($n$)-size.
  - VNP – exp.sum over a VP polynomial-family.

- Reduces to highly-specialized depth-4,3/width-2 questions.
  - ...(VSBR'83)...(AV'08)(R'08)(R'10)...(SSS'09)...(K'11)...(GKKS'13)...(KPTT'15)
    (KKPS'15)...(AGS'18)...(KPTT'15)
  - Qn: Does it reduce to a model as weak as SOS(1-var)?

- Goal: Squash circuit to SOS($n$-var) with nontrivial property.
  - Else, it won't lift to proving circuit lower bounds.
  - Hint: Few squares, Low-degrees.
Algebraic Circuits – to SOS(n-var)

(VSBR'83) $\deg(f) \leq d$, $\text{size}(f) \leq s$ can be rewritten:
- Exists circuit $C'$ of size $\text{poly}(sd)$ and depth $\log d$.
- Exists formula $F$ of size $s^{O(\log d)}$ and depth $\log d$.
- Exists ABP $B$ of size $s^{O(\log d)}$; layers-$d$ homogeneous.

Cut at the $d/2$ layer to get:
- $f = \sum_{i \leq |B|} f_{i,1} f_{i,2}$, where $\deg(f_{i,j}) \leq d/2$.

Use $4f_1 f_2 = (f_1 + f_2)^2 - (f_1 - f_2)^2$ to derive:

Theorem 1: $\deg(f) \leq d$, $\text{size}(f) \leq s$ implies $f = \sum_{i \leq s'} f_i^2$
- where $s' \leq s^{O(\log d)}$ and $\deg(f_i) \leq d/2$.

\[\square\]
Contents

- Sum-of-Squares (SOS) Representation
- SOS hardness

- Algebraic Circuits
  - SOS hardness => Circuit hardness

- Blackbox Identity Testing (PIT)

- Sum-of-Cubes (SOC) hardness
  - SOC hardness => Blackbox PIT

- Conclusion
**Theorem 2:** SOS-hard implies $\text{VP} \neq \text{VNP}$.

**Pf idea:** Consider SOS-hard $f(x)$. Define $(k-1)^\varepsilon \geq 6$. Convert $f$ to multilinear, $kn$-variate, degree-$n$ polynomial $F(y)$.

- Monomial $x^i$ in $f(x)$ maps to $\varphi(x^i) := \prod \{ y_{j,l} \mid l \cdot k^{j-1} \text{ contributes place-value in base }_k(i) \}$.
- $k^n \geq d+1 > (k-1)^n$. So, $n := \Theta(\varepsilon \cdot \log d)$. $F$ is $kn$-variate.
- Suppose $\text{size}(F) \leq d^\mu$. Thm.1 gives SOS s.t.
  - $S(F) \leq (d^\mu n)^{O(\log n)} \cdot \{kn + n/2 \text{ choose } n/2\}$
  - $\leq d^{O(\mu \log n)} \cdot (6(k-1))^{n/2}$
  - $\leq d^{o(\varepsilon)} \cdot (k-1)^{(1+\varepsilon)n/2} \leq d^{o(\varepsilon) + (1+\varepsilon)/2} < d^{0.5+\varepsilon}$.
- $S(f) \leq S(\varphi f) = S(F) \leq d^{\varepsilon + 0.5}$ contradicts SOS-hardness.
- Thus, $F \in \text{VNP} \& > d^\mu = (kn)^{\omega(1)}$ hard.
- Finally, $F \in \text{VNP} \setminus \text{VP}$. □

\[\varepsilon := (\log d \cdot \log \log d)^{-0.5} > \omega(1/\varepsilon \cdot \log d)\]
Contents

- Sum-of-Squares (SOS) Representation
- SOS hardness
- Algebraic Circuits
- SOS hardness $\Rightarrow$ Circuit hardness

Blackbox Identity Testing (PIT)

- Sum-of-Cubes (SOC) hardness
- SOC hardness $\Rightarrow$ Blackbox PIT

Conclusion
Blackbox poly.id.testing (PIT)

- Given circuit $C(x_1, \ldots, x_n)$ of size $s$, whether it is zero?
  - In $\text{poly}(s)$ many bit operations?
  - Only $F = \text{finite field, rationals}$.
  - Brute-force expansion is as expensive as $s^s$.

- **Randomization** gives a practical, *blackbox* solution.
  - Evaluate $C(x_1, \ldots, x_n)$ at a random point in $F^n$. [P.I.Lemma]
  - (Ore 1922), (DeMillo & Lipton 1978), (Zippel 1979), (Schwartz 1980).

- Blackbox PIT is equivalent to designing hitting-set $H \subset F^n$.
  - $H$ contains non-root of each $C(x_1, \ldots, x_n)$ of size $s$.

- Appears in many CS contexts (both algos/lower bounds):
  - ...(Lovász'79)(Heintz,Schnorr'79)(Blum,et.al'80)(Babai,et.al'90)(Clausen,et.al'91)(AKS'02)
    (K'l'04)(A'05,'06)(Klivans, Shpilka'06)(DSY'09)(SV'10)(Mulmuley'11,'12,'17)(Kopparty, Saraf, Shpilka'14)(Pandey,S,Sinha Babu'16)(Guo,S, Sinhababu'18)....<many more>
Blackbox poly.id.testing (PIT)

- **Deterministic** PIT algs known only for restricted models.
  - Too diverse to list here...

- PIT exhibits some *amazing* phenomena:
  - Specific hitting-sets $\implies$ VP $\neq$ VNP. (A'11)(K'11,KP'11).
  - Hitting-sets *strongly* bootstrap. (AGS'18)(KST'19)(GKSS'19)
  - Exp.hardness $\implies$ Hitting-sets in QuasiP ($s^{O(\log s)}$). (KI'04)
  - Recall …reduces to *highly-specialized* depth-4,3/width-2.

**Qn:** Could SOS-hardness imply complete PIT?
- Up to QuasiP implied by Thm.2.
- Issue with *older conjectures* that imply VP $\neq$ VNP.

*We don't know…* [Thm.2/1 are `weak`: #Vars? Deg in SOS?]
- Modify Thm.2/1's proof to connect SOC (sum-of-cubes).
Contents

- Sum-of-Squares (SOS) Representation
- SOS hardness
- Algebraic Circuits
- SOS hardness => Circuit hardness
- Blackbox Identity Testing (PIT)
- Sum-of-Cubes (SOC) hardness
- SOC hardness => Blackbox PIT
- Conclusion
Sum-of-Cubes (SOC) Hardness

For a polynomial \( f \) over \( \mathbb{F} \), the SOC representation is:

\[ f = c_1 \cdot f_1^3 + \ldots + c_t \cdot f_t^3, \]

where \( c_i \in \mathbb{F}, f_i \in \mathbb{F}[x_1, \ldots, x_n] \).

- **Support-union** is distinct monomials \( \bigcup_i \text{supp}(f_i) \).
- Denote the minimal size by \( \text{support-union} \ U(f, t) \).

**SOC-hard:** There's poly(d)-time-explicit \( f \) and constant \( \varepsilon' < 1/2 \) with \( U(f, d^{\varepsilon'}) \geq \Omega(d) \).

- Seems false over \( \mathbb{F} = \mathbb{C}, \mathbb{R} \). [dim.argument]
- Instead fix \( \mathbb{F} = \mathbb{Q} \) – natural choice for PIT.
- (Agrawal'20: False, if \( \varepsilon' \geq 1/2 \).)

Again, numerous candidates for \( f(x) \):

- \( (x+1)^d \), \( \sum_i 2^{i^2} x^i \), \( \prod_i (x+i) \), ....

\( \text{exp}(x) \leq d := \sum_{i=0}^{d} x^i/i! \)
Contents

- Sum-of-Squares (SOS) Representation
- SOS hardness
- Algebraic Circuits
- SOS hardness => Circuit hardness
- Blackbox Identity Testing (PIT)
- Sum-of-Cubes (SOC) hardness
  - SOC hardness => Blackbox PIT
- Conclusion
SOC Hardness $\Rightarrow$ Blackbox PIT

**Theorem.3:** SOC-hard implies blackbox-PIT in P.

**Pf idea:** Consider SOC-hard $f(x) : U(f,d^{\epsilon'}) \geq \delta \cdot d$. Convert $f$ to $k$-variate, ind-degree-$n$ polynomial $F(y)$.

- Monomial $x^i$ in $f(x)$ maps to $\varphi(x^i) := \prod \{ y_j \mid 1 \cdot (n+1)^{j-1} \text{ contributes place-value in base } _{n+1}(i) \}$.
- $(n+1)^k \geq d+1 > n^k$. So, $n := O(d^{1/k})$. $F$ is $k$-variate.
- Let $\text{size}(F) \leq d^\mu$. Thm.1(SOC), gives $(d^\mu \cdot kn)^c$ cubes of $4/11$-th degree:
  - $U(F, d^{(\mu+1/k)c}) \leq \binom{k + 4kn/11}{k} \leq (e + 4e \cdot n/11)^k < n^k \cdot (10.9/11)^k \leq \delta \cdot d$.
- Contradicts $U(f,d^{\epsilon'}) \geq \delta \cdot d$.
- $\Rightarrow$ $F$ is $k=O(1)$-variate, $\text{ideg}-n$, poly($n^k$)-time-explicit, and
- hardness $d^\mu \geq n^{nk} > \text{deg}(F)^3$.
- Apply (GKSS'19) for complete PIT.

Ensure $\epsilon'/c > (\mu+1/k)$, $\mu \cdot k \geq 4$
Contents

- Sum-of-Squares (SOS) Representation
- SOS hardness
- Algebraic Circuits
- SOS hardness => Circuit hardness
- Blackbox Identity Testing (PIT)
- Sum-of-Cubes (SOC) hardness
- SOC hardness => Blackbox PIT

Conclusion
At the end ...

- Largish SOS strong enough for circuit lower bounds. 
  - $\deg(f)_{i}$'s restricted below $\tilde{O}(d)$.

- SOS falls a bit short of derandomization. But, SOC suffices.
  - Could we improve this part?

- **Qn:** Is SOC-hardness heuristically true (over $F = \mathbb{Q}$) ?
  - Hybrid-Qn for SOS: $\varepsilon' < 1/2 < \varepsilon$ with $U(f, d^{\varepsilon'}) > d^{\varepsilon}$ ?
  - $\Rightarrow$ Thm.2 works as well!

- **Prove:** there's sub-constant $\varepsilon$ with $S((x+1)^d) > d^{\varepsilon+0.5}$, over $F = \mathbb{C}$.

Thank you!