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

Nitin Saxena (CSE@IIT Kanpur, India)

(Ongoing work with Pranjal Dutta & Thomas Thierauf)

July 2020, TIFR Mumbai (virtually)

Contents

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

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Testing (PIT)

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

- Conclusion

Sum-of-Squares (SOS) Representation

- For a polynomial f over F, the SOS representation is:
  - $f = c_1.f_1^2 + \ldots + c_t.f_t^2$, where $c_i \in F$, $f_i \in F[x_1,\ldots,x_n]$.
  - *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 $\mathrm{char}\ F \neq 2$.
  - Trivially, $S(f) \leq 2.|f|_0$.
- For simplicity, consider *univariate* SOS representations ($n=1$).
- **Example**: For degree-d univariate $f(x)$, simply use monomials
  $$\{ x^i , x^{i\sqrt{d}} \mid 0 \leq i \leq \sqrt{d} \} .$$
  - (Agrawal'20) $t = 2.\sqrt{d}$ many squares suffice for any f.
  - Overall, expect $S(f) \geq \sqrt{d}.\sqrt{d} = d$.

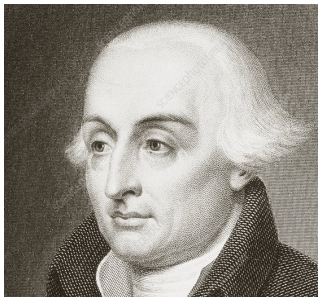
SOS Representation

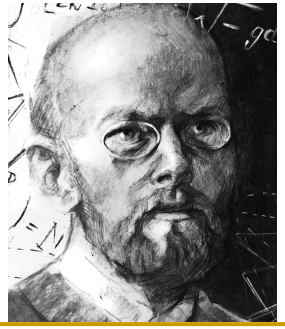
- Does there exist degree-d $f(x)$ with $S(f) \geq \Omega(d)$?
  - By *dimension*-argument it exists!
  - Assume $F = \mathbb{C}$.

- 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.
  - Pythagorean triples, Fermat's 2-squares, Legendre's 3-squares
- (1900) Hilbert's 17th Problem: *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 $\deg(f_i)$).





Contents

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

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Iesting (PIT)

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

- Conclusion

SOS Conjecture

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

- **SOS-Conjecture:** There's an *explicit* f and constant $\varepsilon > 1/2$ with $S(f) > d^{\varepsilon}$.
  - $\varepsilon = 1/2$ trivial. Existentially, much stronger property holds.

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

extremely small circuit complexity!

Yet useful?

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

$\sum_i 2^i x^i$ is not a candidate!

SOS Conjecture – Comparisons

- This conjecture is quite weak/ incomparable to earlier ones about uni/multi-variate polynomials. As they needed sum-of unbounded-powers (or powerful):
  - (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-Conjecture. *Not so* for the earlier conjectures.

- SOS-Conjecture (n-variate): There's *explicit* $f(x_1,\ldots,x_n)$ and constant $\varepsilon>1/2$ with $S(f)> \{n+d \text{ choose } n\}^{\varepsilon}$.
  - Constant n.

Contents

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

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Testing (PIT)

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

- Conclusion

Algebraic Circuits

- Circuit has addition/multiplication *gates*; connected by *wires*.
  - Input variables at *leaves* are $x_1,\ldots,x_n$; output $f(\bar{x})$.
  - 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 of VP polynomial-families.

- 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)...
  - ***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)≤d , size(f)≤s implies a normal-form:
  - $f = \sum_{i \le s'} f_{i,1}.f_{i,2}.f_{i,3}.f_{i,4}.f_{i,5}$,
  - where $s' \le poly(sd)$ and $deg(f_{i,j}) \le d/2$.
  - Imp.: $size(f_{i,j}) \le poly(sd)$ and *homogeneous*.

- Recursive application (m=constant times) gives:
  - $f = \sum_{i \le s'} f_{i,1} \dots f_{i,5\hat{}m}$, where $s' \le poly(sd)$ and $deg(f_{i,j}) \le d/2^m$.

- **Theorem.1:** $\delta > 1/2$, deg(f)≤d, size(f)≤s implies $f = \sum_{i \le s'} f_i^2$:
  - where $s' \le poly(sd)$ and $deg(f_i) \le \delta.d$.

- *Pf idea:* Fix $1/2^m \le (\delta - 0.5)$. Cluster $f_{i,j}$'s s.t. $d/2 < deg \le \delta.d$.
  - Remaining cluster has $deg < d/2$. Use $4ab = (a+b)^2 - (a-b)^2$. ❑

Contents

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

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Testing (PIT)

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

- Conclusion

SOS Conjecture => Circuit hardness

- **Theorem.2:** SOS-Conjecture implies VP ≠ VNP.

- *Pf idea:* Let conjecture hold for degree-d $f(x)$. Convert f to *multilinear*, $O(n)$-*variate*, *degree*-n polynomial $F(\bar{y})$.
  - Monomial x^i in $f(x)$ maps to $\varphi(x^i) :=$
  - $\Pi\{\, y_{j,l} \mid l.(k+1)^{j-1}$ contributes in $\text{base}_{k+1}(i)\,\}$.
  - $(k+1)^n \geq d+1 > k^n$. So, $n=O(\log d)$. F is $(k+1)n$-variate.
  - Suppose $\text{size}(F) \leq d^{\mu}$. Thm.1 gives δ_1 s.t.
  - $S(F) \leq d\hat{}\delta_1.\{(k+1)n + n\delta \text{ choose } n\delta\}$
  - $\leq d\hat{}\delta_1.(e+e(k+1)/\delta)^{n\delta}$
  - $\leq d\hat{}\delta_1.k\hat{}(n\delta_2) \leq d\hat{}(\delta_1+\delta_2) \leq d^{\varepsilon}$.
  - $S(f) \leq S(\varphi f) = S(F) \leq d^{\varepsilon}$ contradicts SOS-Conjecture.
  - Thus, $F \in$ VNP & $2^{\Omega(n)}$-hard. ❑

Dependency-chain on ε: $\delta_1, \delta_2, \mu, \delta, k$

Contents

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

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Testing (PIT)

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

- Conclusion

Blackbox poly.id.testing (PIT)

- Given circuit $C(x_1, \ldots, x_n)$ of size s, whether it is zero?
  - In $poly(s)$ many bit operations?
  - Only $F =$ 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)(KI'04)(A'05,'06)(Klivans, Shpilka'06)(DSY'09)(SV'10)(Mulmuley'11,'12,'17)(Kopparty,Saraf, Shpilka'14)(Pandey,S,Sinhababu'16)(Guo,S, Sinhababu'18)....<many more>

Blackbox poly.id.testing (PIT)

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

- PIT exhibits some *amazing* phenomena:
  - *Specific* hitting-sets => VP ≠ VNP. (A'11)(K'11,KP'11).
  - Hitting-sets *strongly* bootstrap. (AGS'18)(KST'19)(GKSS'19)
  - Exp.hardness => 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 ≠ VNP.

Give only log-var reduction, not O(1)-var

- *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 Conjecture

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Testing (PIT)

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

- Conclusion

Sum-of-Cubes (SOC) Conjecture

- For a polynomial f over F, the SOC representation is:
  - $f = c_1.f_1^3 + \ldots + c_t.f_t^3$, where $c_i \in F$, $f_i \in F[x_1,\ldots,x_n]$.
  - *Support-union* is *distinct* monomials $\cup_i \mathrm{supp}(f_i)$.
  - Denote the minimal size by support-union $U(f,t)$.

- **SOC-Conjecture:** There's poly(d)-time-*explicit* f and constant $\varepsilon' < 1/2$ with $U(f,d^{\varepsilon'}) \geq \Omega(d)$.
  - Seems false over $F=\mathbb{C}$, $\mathbb{R}$. [dim.argument]
  - Instead fix $F=\mathbb{Q}$ – natural choice for PIT.
  - *(Agrawal'20: False, if $\varepsilon' \geq 1/2$.)*

$x^2+y^2=3$: $\mathbb{R}$-roots; but no $\mathbb{Q}$-root.

- Again, numerous candidates for $f(x)$:
  - $(x+1)^d$, $\sum_i 2^{i\hat{}2}\, x^i$, $\prod_i (x+i)$, ...

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

Contents

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

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Testing (PIT)

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

- Conclusion

SOC Conjecture => Blackbox PIT

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

- *Pf idea:* Let conjecture hold for degree-d $f(x)$. Convert f to $O(1)$-*variate*, *ind-degree*-n polynomial $F(\bar{y})$.
  - Monomial x^i in $f(x)$ maps to $\varphi(x^i) :=$
  - $\Pi\{ y_j^l \mid l.(n+1)^{j-1}$ contributes in $\text{base}_{n+1}(i) \}$.
  - $(n+1)^k \geq d+1 > n^k$. So, $n=O(d^{1/k})$. F is k-variate.
  - Suppose $\text{size}(F) \leq d^\mu$. Thm.1(SOC), $1/e>\delta>1/3$, gives δ_1 s.t.
  - $U(F,d\hat{}\delta_1) \leq \{k + kn\delta$ choose $k\}$
  - $\leq (e+en\delta)^k \leq n^k.(2.8/3)^k \leq d.\delta_2 <$ SOC-Conj.
  - Contradicts $U(f,d^{\varepsilon'}) \geq \Omega(d)$.
  - => F is $k=O(1)$-*variate, ideg-n,* poly(n^k)-time-*explicit,* and
  - hardness $d^\mu \geq n^{\mu k} > \deg(F)^3$.
  - Apply (GKSS'19) for PIT. ❑

Dependency-chain on ε', δ_2: (δ_1,μ), (δ,k)

Contents

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

- Algebraic Circuits
- SOS Conjecture => Circuit hardness

- Blackbox Identity Testing (PIT)

- Sum-of-Cubes (SOC) Conjecture
- SOC Conjecture => 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-conjecture *heuristically* true (over $F=\mathbb{Q}$)?
  - Hybrid-Qn for SOS: $\varepsilon'<1/2<\varepsilon$ with $U(f,d^{\varepsilon'}) > d^{\varepsilon}$?
  - **=>** Thm.2 works as well!
- Prove: there's constant $\varepsilon>1/2$ with $S((x+1)^d)> d^{\varepsilon}$, over $F=\mathbb{C}$.

$> \sqrt{d}.(\log d)$?

Thank you!