Sum-of-squares lower bounds for planted clique

Raghu Meka, Aaron Potechin and Avi Wigderson
Presenter: Kiran Shiragur

June 13, 2017

Problem Definition: Planted Clique

$$G(n, \frac{1}{2}) \quad v/s \quad G(n, \frac{1}{2}, k)$$

- We are given a graph G, from one of these distributions.
- Need to find which distribution it came from.

Facts and Results:

- $G(n, \frac{1}{2})$ has clique of size at most $(2 + o(1)) \log n$ w.h.p
- We have a spectral algorithm when $|k| = k(\sqrt{n})$.
- What happens in the range $3 \log n \leq k \leq o(\sqrt{n})$ (Information theoretically possible)

Attempt: Optimization Problem

Lets write this identification problem as an optimization problem:
Variables: $x_i \in \{0, 1\}$

$$\max \sum_i x_i$$

$$\text{clique constraints}$$

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

If we could solve this ILP exaclty, then we can actually identify from which distribution graph is from.

Attempt: Optimization Problem

Lets write this identification problem as an optimization problem:
Variables: $x_i \in [0, 1]$

$$\max \sum_i x_i$$

clique constraints

$$0 \leq x_i \leq 1$$

Main Theorem

Theorem

With high probability, for $G \leftarrow G(n, 1/2)$ the natural r-round SOS relaxation of the maximum clique problem has an integrality gap of at least

$$\frac{n^{1/2r}}{Cr(logn)^2}$$

$$\text{Integrality gap of r-round SOS} = \max_{\text{all Instances}} \frac{\text{Objective value of r-round SOS}}{\text{actual optimum value}}$$

$$\frac{\text{Objective value of r-round SOS}}{(2 + o(1))\log n} \geq \frac{n^{1/2r}}{Cr(logn)^2}$$

$$\text{Objective value of r-round SOS} \geq \frac{n^{1/2r}}{Cr(logn)^2}(2 + o(1))\log n \approx n^{1/2r}$$

Lower bound here implies:

- Poly time (when the number of rounds r is constant) cannot handle even $k = n^{o(1)}$.
- $(logn)^{1/2}$ rounds cannot handle $k = (logn)^{O(1)}$.

Best result so far:

- Poly time (when the number of rounds r is constant) cannot handle even $k \approx n^{1/2}$ (Next talk! [BHKKMP16])

Axioms for Planted Clique

Suppose we want to show there exist no x such that:

$$f_1(x) = 0, \ldots, f_n(x) = 0$$

Given a graph G, let $Clique(G, k)$ denote the following set of polynomial axioms:

$$\begin{aligned}(Max - Clique) :& x_i^2 - xi, \forall i \in [n] \\ & x_i.x_j, \forall pairs\{i, j\} \notin G \\ & \sum_i x_i - k\end{aligned} \tag{1}$$

SOS REFUTATIONS

Definition

(Positivstellensatz Refutation, [GV01]). Let $F = \{f_1, \ldots, f_n : \mathbb{R}^n \to \mathbb{R}\}$, be a system of axioms, where each f_i is a real n-variate polynomial. A positivstellensatz refutation of degree r ($PS(r)$ refutation, henceforth) for F is an identity of the form

$$\sum_{i=1}^{m} f_i g_i = 1 + \sum_{i=1}^{N} h_i^2$$

where $g_1, \ldots, g_m, h_1, \ldots, h_N$ are n-variate polynomials such that $deg(f_i g_i) \leq 2r$ for all $i \in [m]$ and $deg(h_j) \leq r$ for all $j \in [N]$.

Theorem

With high probability over $G \leftarrow G(n, 1/2)$, the system Clique(G, k) has no PS(r) refutation for

$$k \leq \frac{n^{1/2r}}{Cr(logn)^{1/r}}$$

Defintions

Definition (PSD Mappings)

A linear mapping $\mathcal{M} : \mathcal{P}(n, 2r) \to \mathbb{R}$ is said to be positive semi-definite (PSD) if $\mathcal{M}(P^2) \geq 0$ for all n-variate polynomials P of degree at most r.

Definition (Dual Certificates)

Given a set of axioms $f_1, \ldots, f_m$, a dual certificate for the axioms is a PSD mapping $\mathcal{M} : \mathcal{P}(n, 2r) \to \mathbb{R}$ such that $\mathcal{M}(f_i g) = 0$ for all $i \in [m]$ and all polynomials g such that $deg(f_i g) \leq 2r$.

Lemma (Dual Certificate)

Given a system of axioms $((f_i))$, *there does not exist a* $\mathrm{PS}(r)$ *refutation of the system if there exists a dual certificate* $\mathcal{M} : \mathcal{P}(n, 2r) \to \mathbb{R}$ *for the axioms.*

Recipe for lower bounds

- Design a dual certificate $\mathcal{M}$ for the clique axioms we care about. (Guessing is easy, but showing $\mathcal{M}$ is PSD is hard!)
- Prove PSDness for $\mathcal{M}$.

Dual certificates for clique axioms

$$
\text{(Max-Clique):} \quad \begin{aligned} & x_i^2 - x_i, \ \ \forall i \in [n] \\ & x_i \cdot x_j, \ \ \forall \text{ pairs } \{i, j\} \notin G \\ & \sum_i x_i - k. \end{aligned} \tag{2}
$$

Define

$$
x_I := \prod_{i \in I} x_i
$$

The r-round SOS should satisfy:

$$
\begin{aligned} & \mathcal{M}(X_I) = 0, \ \forall I, \ |I| \leq 2r, \ I \text{ is not a clique in } G, \\ & \mathcal{M}\left(\left(\sum_{i=1}^{n} x_i - k \right) X_I \right) = 0, \ \forall I, \ |I| < 2r. \end{aligned} \tag{3}
$$

$I \subseteq [n]$, $|I| \le 2r$, let

$$deg_G(I) = |\{S \subseteq [n] : I \subseteq S,\ |S| = 2r,\ S \text{ is a clique in } G\}|.$$

For instance, if $r = 1$ and $v \in G$, then $deg_G(\{v\})$ is the degree of vertex v. We define $\mathcal{M} \equiv \mathcal{M}_G : \mathcal{P}(n, 2r) \to \mathbb{R}$ for monomials as follows: for $I \subseteq [n], |I| \le 2r$, let

$$\mathcal{M}\left(\prod_{i \in I} x_i\right) = \deg_G(I) \cdot \frac{\binom{k}{|I|}}{\binom{2r}{|I|}}. \tag{4}$$

Lemma

For any P of degree at most r we may write $P = P_1 + \sum_i P_{2i}(x_i^2 - x_i) + P_3(\sum_i x_i - k)$ where P_1 is multilinear and homogeneous of degree r, P_3 has degree at most $r-1$, and all P_{2i} have degree at most $r-2$.

Corollary

If $\mathcal{M}(P_1^2) \geq 0$ for all multilinear homogeneous P_1 of degree r then $\mathcal{M}$ is PSD.

Easy to work with Moment matrix

For $I, J \in \binom{[n]}{r}$

$$M(I,J) = deg_G(I \cup J) \cdot \frac{\binom{k}{|I \cup J|}}{\binom{2r}{|I \cup J|}} = deg_G(I \cup J)\beta(|I \cap J|)$$

- Show that M satisfies Clique r-round SOS constraints.
- Construct a new matrix M'.

$$\lambda_{min}(M) \geq \lambda_{min}(M')$$

-
$$M' = E + L + \Delta$$

- Show spectral bounds on these matrices:

$$\lambda_{min}(E) \geq k_r(k^r n^r)$$

$$\|L\| < Ck^{2r} n^{r-1/2} \log n$$

$$\|\Delta\| < Ck^{2r} n^{r-1/2} \log n$$

$$\lambda_{min}(M) \geq \lambda_{min}(M') \geq k_r(k^r n^r) - Ck^{2r} n^{r-1/2} \log n - Ck^{2r} n^{r-1/2} \log n$$

Steps of the overview of the proof

- Show that M satisfies Clique r-round SOS constraints.
- Construct a new matrix M'.

$$\lambda_{min}(M) \geq \lambda_{min}(M')$$

- $$M' = E + L + \Delta$$

- Show spectral bounds on these matrices:

$$\lambda_{min}(E) \geq k_r(k^r n^r)$$

$$\|L\| < Ck^{2r} n^{r-1/2} \log n$$

$$\|\Delta\| < Ck^{2r} n^{r-1/2} \log n$$

$$\lambda_{min}(M) \geq \lambda_{min}(M') \geq k^r n^r - k^{2r} n^{r-1/2}$$

$$\lambda_{min}(M) \geq \lambda_{min}(M') \geq k^r n^r - k^{2r} n^{r-1/2}$$

We want:

$$k^r n^r - k^{2r} n^{r-1/2} \geq 0$$

$$n^{1/2} \geq k^r$$

Substitute $k = n^{\alpha}$

$$n^{1/2} \geq n^{\alpha r}$$

$$\alpha \leq \frac{1}{2r}$$

$$k \leq n^{1/2r}$$

As long as this holds we can prove PSD of M', hence M.

Main Theorem Restated

Theorem

With high probability, for $G \leftarrow G(n, 1/2)$ the natural r-round SOS relaxation of the maximum clique problem has objective value at least

$$\approx n^{1/2r}$$

Define $\beta(i) = \binom{k}{2r-i} / \binom{2r}{2r-i}$
Recall:

$$M(I,J) = deg_G(I \cup J) \cdot \frac{\binom{k}{|I \cup J|}}{\binom{2r}{|I \cup J|}} = deg_G(I \cup J)\beta(|I \cap J|)$$

where $deg_G(I) = |\{S \subseteq [n] : I \subseteq S,\ |S| = 2r,\ S \text{ is a clique in } G\}|$
For every $T \subseteq [n]$ $|T| = 2r$, let $M_T \in \mathbb{R}^{\binom{[n]}{r} \times \binom{[n]}{r}}$, with

$$\begin{aligned} M_T(I,J) &= \beta(|I \cap J|) \quad \textit{if} \quad I \cup J \subseteq T \text{ and } \mathcal{E}(T) \setminus \mathcal{E}(I) \cup \mathcal{E}(J) \subseteq E(G) \\ &= 0 \quad \textit{otherwise} \end{aligned}$$

$$M' = \sum_{T:|T|=2r} M_T$$

Matrix M'

$$M'(I,J) = M(I,J) \quad \text{if } I \cup J \text{ was a clique in the Graph } G$$

$$M'(I,J) \geq 0 \text{ and } M(I,J) = 0 \quad \textit{otherwise}$$

Matrix E

Recall:

$$
\begin{aligned}
M_T(I,J) &= \beta(|I\cap J|) \quad \textit{if} \quad I\cup J\subseteq T \text{ and } \mathcal{E}(T)\setminus\mathcal{E}(I)\cup\mathcal{E}(J)\subseteq E(G)\\
&= 0 \quad \textit{otherwise}
\end{aligned}
$$

$$M' = \sum_{T:|T|=2r} M_T$$

For $I,J\in\binom{n}{r}$, and $E=\mathbb{E}[M']$,

$$E(I,J) = p(|I\cap J|)\cdot\beta(|I\cap J|) =: \alpha(|I\cap J|) \tag{5}$$

where $p(|I\cap J|) = \binom{n-|I\cup J|}{2r-|I\cup J|}\cdot 2^{-r^2-\binom{|I\cap J|}{2}}$ is the probability that $\mathcal{E}(I\cup J)\setminus(\mathcal{E}(I)\cup\mathcal{E}(J))\subseteq G$

Johnson Scheme

Definition (Set-Symmetry)

A matrix $M \in \mathbb{R}^{\binom{[n]}{r} \times \binom{[n]}{r}}$ is set-symmetric if for every $I, J \in \binom{[n]}{r}$, $M(I, J)$ depends only on the size of $|I \cap J|$.

Definition (Johnson Scheme)

For $n, r \le n/2$, let $J_{n,r} \subseteq \mathbb{R}^{\binom{[n]}{r} \times \binom{[n]}{r}}$ be the subspace of all set-symmetric matrices. J is called the Johnson scheme.

Definition (D-Basis)

For $0 \le \ell \le r \le n$, let $D_\ell \equiv D_{n,r,\ell} \in \mathbb{R}^{\binom{[n]}{r} \times \binom{[n]}{r}}$ be defined by

$$D_\ell(I, J) = \begin{cases} 1 & |I \cap J| = \ell \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

Definition (P-Basis)

For $0 \le t \le r$, let $P_t \equiv P_{n,r,t} \in \mathbb{R}^{\binom{[n]}{r} \times \binom{[n]}{r}}$ be defined by

$$P_t(I, J) = \binom{|I \cap J|}{t}.$$

Claim

For fixed n, r, the following relations hold:

1. *For $0 \le t \le r$, $P_t = \sum_{\ell=t}^{r} \binom{\ell}{t} D_\ell$.*
2. *For $0 \le \ell \le r$, $D_\ell = \sum_{t=\ell}^{r} (-1)^{t-\ell} \binom{t}{\ell} P_t$.*

Lemma

Fix $n, r \leq n/2$ and let $J(n,r)$ be the Johnson scheme. Then, for P_t as defined before, there exist subspaces $V_0, V_1, \ldots, V_r \in \mathbb{R}^{\binom{[n]}{r}}$ that are orthogonal to one another such that:

1. *$V_0, \ldots, V_r$ are eigenspaces for $\{P_t : 0 \leq t \leq r\}$ and consequently for all matrices in $J(n,r)$.*
2. *For $0 \leq j \leq r$, $\dim(V_j) = \binom{n}{j} - \binom{n}{j-1}$.*
3. *For any matrix $Q \in J$, let $\lambda_j(Q)$ denote the eigenvalue of Q within the eigenspace V_j. Then,*

$$\lambda_j(P_t) = \begin{cases} \binom{n-t-j}{r-t} \cdot \binom{r-j}{t-j} & j \leq t \\ 0 & j > t \end{cases}. \tag{7}$$

Matrix E

$$E = \sum e_\ell D_\ell = \sum \alpha_t P_t$$

where $e_\ell = \binom{n-2r+l}{l} \cdot \frac{\binom{k}{2r-\ell}}{\binom{2r}{2r-\ell}} \cdot 2^{-r^2-\binom{\ell}{2}}$

$$\alpha_i >> \alpha_{i-1} (goemetrically)$$

that is $\alpha_r P_r$ dominates,

$$\alpha_r \geq 2^{-O(r^2)} k^r n^r$$

$$P_r = I$$

$$\lambda_{min}(E) \geq 2^{-O(r^2)} k^r n^r$$

Matrix L

Now, define $L \in \mathbb{R}^{\binom{[n]}{r} \times \binom{[n]}{r}}$ as follows: for $I, J \in \binom{[n]}{r}$,

$$L(I,J) = \begin{cases} \alpha(|I \cap J|) \cdot \frac{1-p(|I \cap J|)}{p(|I \cap J|)} & \text{if } \mathcal{E}(I \cup J) \setminus (\mathcal{E}(I) \cup \mathcal{E}(J)) \subseteq G \\ -\alpha(|I \cap J|) & \text{otherwise} \end{cases}. \quad (8)$$

where $p(|I \cap J|)$ is the probability that $\mathcal{E}(I \cup J) \setminus (\mathcal{E}(I) \cup \mathcal{E}(J)) \subseteq G$

Lemma

For some constant $C > 0$, with probability at least $1 - 1/n$ over the random graph G,

$$\|L\| \leq O(1) \cdot 2^{Cr^2} \cdot k^{2r} \cdot n^r \cdot \frac{\log n}{\sqrt{n}}.$$

Matrix Δ

$$\Delta = M' - E - L$$

$$\Delta(I,J) = \begin{cases} M'(I,J) - \alpha(|I \cap J|)/p(|I \cap J|) & \text{if } \mathcal{E}(I \cup J) \setminus (\mathcal{E}(I) \cup \mathcal{E}(J)) \subseteq G \\ 0 & \text{otherwise} \end{cases} \quad (9)$$

Let $\mathcal{A}$ be the event that $\mathcal{E}(I \cup J) \setminus (\mathcal{E}(I) \cup \mathcal{E}(J)) \subseteq G$
All we care about is:

$$\mathbb{E}[M'(I,J) \mid \mathcal{A}](Small!)$$

This is because ($i = |I \cap J|$):

$$\deg_G(I \cup J) \approx 2^{-\binom{2r}{2}+\binom{2r-i}{2}} \cdot \binom{n-2r+i}{i}$$

$$M'(I,J) \approx \beta(i) 2^{-\binom{2r}{2}+\binom{2r-i}{2}} \cdot \binom{n-2r+i}{i} = \alpha(|I \cap J|)/p(|I \cap J|)$$

Matrix Δ

$$M'(I,J) \approx \alpha(|I \cap J|)/p(|I \cap J|) = \alpha(|I \cap J|)/p(|I \cap J|) + noise$$

Lemma

For some universal constant C, and $n > C2^{4r^2}$, with probability at least $1 - 1/n$ over the random graph G, for all $I, J \in \binom{[n]}{r}$, with $i = |I \cap J|$,

$$|\Delta(I,J)| \leq 2^{Cr^2} \cdot k^{2r-i} \cdot n^i \cdot \frac{\log n}{\sqrt{n}}.$$

Lemma

For $n > C2^{4r^2}$, with probability at least $1 - 1/n$ over the random graph G,

$$\|\Delta\| \leq 2^{Cr^2} \cdot k^{2r} \cdot n^r \cdot \frac{\log n}{\sqrt{n}}.$$