PROOF COMPLEXITY AS A COMPUTATIONAL LENS

LECTURE 6

CLB RECAP I

Average-case $n^{\Omega(k)}$ lower bounds for k-clique formulas for regular resolution

$G \sim G\left(n, n^{-\frac{2}{k-1}}\right)$ Erdős-Rényi random graph $\eta > 1$

Regular resolution: Along every path in proof DAG, every variable resolved at most once

$\Updownarrow$

Read-once branching program (ROBP) solving falsified clause search problem for clique formula

Read-once: along every path, query every variable at most once

Take regular resolution refutation and flip edges $\Rightarrow$ ROBP

Clique formula for $G=(V,E)$

$x_{v,i}$ $\quad v \in V = [n]$ $\quad i \in [k]$

CLIQUE AXIOMS	$\bigvee_{v \in V} x_{v,i}$	$i \in [k]$
EDGE AXIOMS	$\bar{x}_{u,i} \vee \bar{x}_{v,j}$	$i \neq j \in [k]$, $(u,v) \in E$
FUNCTIONALITY AXIOMS	$\bar{x}_{u,i} \vee \bar{x}_{v,i}$	$i \in [k]$, $u \neq v \in V$
We will ignore ORDERING AXIOMS	$\bar{x}_{u,i} \vee \bar{x}_{v,j}$	$u < v \in V$, $(u,v) \in E$, $i > j \in [k]$

for simplicity of exposition

CLB
RECAP II

THEOREM [ABdR2NR '21]

For constants $\varepsilon > 0$, $\eta > 1$, $k \leq n^{1/4-\varepsilon}$,
k-clique formula for $G \sim G(n, n^{-(2\eta)/(k-1)})$
requires regular resolution length $n^{\Omega(k)}$ a.a.s.

Prove this lower bound for read-once branching programs

ROBP: NODES a, b, c

Graph $G = (V, E)$ VERTICES u, v, w

$\beta(a)$ = variable assignments common for every sourcepath to a

Variable x is FORGOTTEN AT a if
- $\exists$ source path α to a that sees x
- $x \notin \mathrm{dom}(\beta(a))$

OBSERVATION 1

If x forgotten at a and $\exists$ path $a \rightsquigarrow b$, then x forgotten at b

Index i is FORGOTTEN AT a if for some $v \in V$ $x_{v,i}$ is forgotten at a

OBSERVATION 2

If sourcepath α rules out index i at sink b, then i is not forgotten at b

Source path α RULES OUT INDEX i if ends at clique axiom $\bigvee_{v \in V} x_{v,i}$

CLB RECAP III

Random distribution $\mathcal{D}$ over paths α

start with (current node a) := start node

Suppose α queries $x_{v,i}$

FORCED
(a) If $\beta(a) \cup \{x_{v,i} \mapsto 1\}$ falsifies edge or functionality axiom, take 0-edge from a (set $x_{v,i} \mapsto 0$)
(b) if i forgotten at a, take 0-edge from a

FREE
(c) Otherwise, flip $n^{-\delta}$-biased coin, $\delta > 0$
$x_{v,i} \mapsto 1$ with probability $n^{-\delta}$
$x_{v,i} \mapsto 0$ with probability $1 - n^{-\delta}$

OBSERVATION 3

Any $\alpha \sim \mathcal{D}$
(i) rules out some index i^* (i.e., never falsifies functionality or edge axiom)
(ii) sets at most k variables x_{v,i^*} to 1

Last lecture
- Define "useful pair (a,b)" on α ruling out i^* — segment of path where many $x_{u,i^*} \mapsto 0$
- Argue every α goes through some useful pair (a,b)
- Tried to argue for fixed useful pair (a,b) that $\Pr_{\alpha \sim \mathcal{D}}[\alpha \text{ goes through } (a,b)] \leq n^{-\Omega(k)}$

But proof crashed — once $\beta(a)$ contains subclique, many $x_{u,i^*} = 0$ can be forced

ACTUAL PROOF (EXCEPT FOR SOME CALCULATIONS)

$N(v) = \{ u \mid (u,v) \in E \}$ neighbours of v

$\widehat{N}(R) = \bigcap_{v \in R} N(v)$ common neighbours of R

$\widehat{N}_W(R) = \widehat{N}(R) \cap W$ common neighbours of R in W

$W \subseteq V$ is q-NEIGHBOUR-DENSE FOR $R \subseteq V$ if $|\widehat{N}_W(R)| \geq q$

$W \subseteq V$ is (r,q)-NEIGHBOUR-DENSE if it is q-neighbour-dense $\forall R \subseteq V \quad |R| \leq r$

Means, in particular, that any clique of size r can be enlarged with vertex from W in $\geq q$ different ways

Should be likely to hold for moderate r, q for random graph. But as r, q get larger, property becomes more unlikely

If (r,q)-neighbour-denseness fails, want to find "mostly neighbour-dense" set W that fail only for few sets R.

Namely, exist set S such that $R \cap S$ is large for sets R that make W fail

In what follows, think of parameters as

$$r, r' = \Omega(k) \qquad r' \geq r$$
$$q' = n^{\gamma'}$$
$$s = n^{\gamma} \qquad 1 \gg \gamma' \gg \gamma > 0$$

$W \subseteq V$ is (r', r, q', s)-MOSTLY NEIGHBOUR-DENSE if $\exists\, S \subseteq V$ $|S| \leq s$ such that for every $R \subseteq V$, $|R| \leq r'$ for which W is not q'-neighbour-dense, it holds that $|R \cap S| \geq r$

Graph $G = (V, E)$ is (k, t, s, ε)-CLIQUE-DENSE for $k \in \mathbb{N}^+$, $t, s, \varepsilon \in \mathbb{R}^+$, $1 \leq t \leq k$, if $\exists\, r, q \in \mathbb{R}^+$, $r \geq 4k/t^2$, such that:

(1) V is (tr, tq)-neighbour-dense.

(2) Every (r,q)-neighbour-dense set $W \subseteq V$ is (tr, r, q', s)-mostly neighbour-dense for $q' = 3\varepsilon k s^{1+\varepsilon} \log s$

THEOREM 7

For constants $\varepsilon > 0$, $\eta > 1$ and n large enough, if $G \sim G(n, n^{-2\eta/(k-1)})$ then with probability $\geq 1 - \exp(-\sqrt{n})$ G is (k, t, s, ε)-clique-dense for $t = 6^k \eta/\varepsilon$ and $s = (n/\eta)^{1/2}$.

Proof A few pages of careful calculations...

THEOREM 8

If $k \in \mathbb{N}^+$ and $t, s, \varepsilon \in \mathbb{R}^+$ are such that G is (k, t, s, ε)-clique-dense, then regular resolution requires length at least

$$\frac{1}{\sqrt{2}} s^{\varepsilon k/t^2}$$

to refute the clique formula for G (without ordering axioms)

$n^{\Omega(k)}$

The proof of Thm 8 is what we will focus on. Reuse our previous approach, but with more careful definition of "useful"

For each $a \in \Pi$, $i \in [k]$, define

$$V_i^0(a) = \{ v \in V \mid \beta(a) \text{ sets } x_{v,i} \text{ to } 0 \}$$

$$V_i^1(a) = \{ v \in V \mid \beta(a) \text{ sets } x_{v,i} \text{ to } 1 \}$$

Keep distribution $\mathcal{D}$

Probability of coin flip 1 is

$$r s^{-(1+\varepsilon)} / 2ek \approx s^{-(1+\varepsilon)}$$

Observation 3 still true, since $\mathcal{D}$ is essentially the same

Say $(a,b) \in \Pi^2$ **(TRULY) USEFUL** if there is index i such that

(a) $V_i^1(b) = \emptyset$

(b) i is not forgotten at b

(c) $V_i^0(b) \setminus V_i^0(a)$ is (r,q)-neighbour-dense

For each useful pair (a,b), fix (arbitrarily) index $i = i(a,b)$ witnessing that (a,b) useful

Path α **USEFULLY TRAVERSES** useful pair (a,b) if α goes through a & b in that order and sets $\leq \lceil k/t \rceil$ variables to 1 between a and b (with a included and b excluded)

Theorem 8 follows by proof we did before from following two Lemmas

LEMMA 9 ($\Leftarrow$ Observation 4)
Every path $\alpha \sim \mathcal{D}$ usefully traverses a useful pair

LEMMA 10 ($\Leftarrow$ Hopeful claim 6)
For every useful pair (a,b) $\Pr_{\alpha \sim \mathcal{D}}[\alpha \text{ usefully traverses } (a,b)] \leq 2s^{-Er/2}$

Proof of Lemma 9

Consider any $\alpha \sim \mathcal{D}$. Ends in i^*th clique axiom for some $i^* \in [k]$

Obs 3 $\Rightarrow$ α sets $\leq k$ variables to 1

Split α into t pieces source $= a_0 \rightsquigarrow a_1 \rightsquigarrow \ldots \rightsquigarrow a_t$ so that between a_j and $a_{j+1} \leq \lceil k/t \rceil$ variables set to 1.

clearly $V^1_{i^*}(a_j) = \emptyset$ and i^* not forgotten at a_j for all j.

Remains to prove for some j that

$$W_j = V^0_{i^*}(a_j) \setminus V^0_{i^*}(a_{j-1}) \qquad (\dagger)$$

is (r, q) - neighbour-dense. If so, (a_{j-1}, a_j) is a useful pair that is usefully traversed

Towards contradiction, suppose no W_j is (r, q) - neighbour-dense

That is, $\forall j \in [t] \;\; \exists \; R_j \subseteq V, |R_j| \leq r$, such that $|\hat{N}_{W_j}(R_j)| \leq q$ $\qquad (\ddagger)$

Let $R = \bigcup_{j \in [t]} R_j$

Path α ends in i^*th clique axiom

$\Rightarrow V^0_{i^*}(a_t) = V$

i^* is not forgotten along the path

$\Rightarrow V^0_{i^*}(a_{j-1}) \subseteq V^0_{i^*}(a_j) \quad \forall j \in [t]$

So sets $W_1, W_2, \ldots, W_t$ in $(\dagger)$ form partition of V, i.e.,

$$V = W_1 \dot\cup W_2 \dot\cup \cdots \dot\cup W_t$$

Hence

$$|\hat{N}_V(R)| = \sum_{j \in [t]} |\hat{N}_{W_j}(R)| \leq \sum_{j \in [t]} |\hat{N}_{W_j}(R_j)| \leq tq$$

by $(\ddagger)$. But this contradicts that V is (tr, tq) - neighbour-dense. Lemma 9 follows ☐

Proof of Lemma 10

Let us fix some notation

(a,b) fixed useful pair

$\mathcal{E} = \mathcal{E}_{a,b}$ = event that $\alpha \sim \mathcal{D}$ usefully traverses (a,b)

$i^* = i(a,b)$

$W = V^0_{i^*}(b) \setminus V^0_{i^*}(a)$

$V^1(a) = \bigcup_{j \in [k]} V^1_j(a)$

Want upper bound for $\Pr_{\alpha \sim \mathcal{D}}[\mathcal{E}_{a,b}]$

Note that for every $v \in V^1(a)$ $\exists$ unique j_v s.t. $\beta(a)$ sets $x_{v,j_v} = 1$ — $\beta(a)$ contains assignments made on all paths, and only one $x_{v,j}$ can be set to 1 along any path, so all paths have to agree on j

By definition of i^*, W is (r,q)-neighbour-dense

G is (k,t,s,ε)-clique dense by assumption

$\Rightarrow$ W is (tr, r, q', s)-mostly neighbour-dense

Fix set S of size $|S| = s$ witnessing this

That is, for all $R \subseteq V$, $|R| \leq tr$, such that

$$|\hat{N}_W(R)| < q' \Rightarrow |R \cap S| \geq r$$

Do proof by case analysis over $|V^1(a)|$

All probabilities in what follows are over $\alpha \sim \mathcal{D}$

Case 1: $|V^1(a)| > r/2$

This case was OK already before, and is still OK

In this case, probability of even reaching a is small enough.

For any assignment β, define $\beta^1 = \{x_{v,i} \text{ set to } 1 \text{ by } \beta\}$

Argued above $|\beta^1(a)| = |V^1(a)|$

All assignments in $B^1(a)$ are the results of free coin flips

By read-once property, only get one coin flip per variable – if wrong outcome, then won't reach a.

So we have

$$\begin{aligned}
\Pr[\mathcal{E}_{a,b}] &\le \Pr[\alpha \text{ reaches } a] \\
&\le \Pr[\alpha \text{ sets } B^1(a) \text{ correctly}] \\
&= \left(\frac{r s^{-(1+\varepsilon)}}{2ck}\right)^{|B^1(a)|} \\
&\le s^{-\varepsilon |B^1(a)|} \\
&= s^{-\varepsilon |V^1(a)|} \\
&\le s^{-\varepsilon r/2}
\end{aligned}$$

$r \le k$, since $t r \le k$ and $t \ge 2$

Case 2: $|V^1(a)| \le r/2$

For path α, let $R(\alpha) = \{u \mid \text{some } x_{uj} \mapsto 1 \text{ in } [a,b)\}$

If α does not pass through (a,b) $R(\alpha) = \emptyset$

If $\alpha \in \mathcal{E}_{a,b}$, then $|R(\alpha)| \le \lceil k/t \rceil$

Hopeful claim 6 failed because dangerous vertices in $V^1(a) \cup R(\alpha)$ can make $N_W(V^1(a) \cup R(\alpha))$ shrink a lot, forcing many $x_{v,i} \mapsto 0$.

Since $|V^1(a)|$ small, $R(\alpha)$ plays important role and $R(\alpha)$ shows that W fails to be neighbour-dense

But W is mostly neighbour-dense, so such $R(\alpha)$ are rare and should be unlikely to arise. Do subcase analysis depending on whether $R(\alpha)$ is dangerous or not

Define

$$R_0 = \{ R : |R| \le \lceil k/t \rceil \text{ and } |\hat{N}_W(R \cup V^1(a))| < g' \}$$

$$R_1 = \{ R : |R| \le \lceil k/t \rceil \text{ and } |\hat{N}_W(R \cup V^1(a))| \ge g' \}$$

We have

$$\Pr[\mathcal{E}_{a,b}] = \Pr[\mathcal{E}_{a,b} \text{ and } R(\alpha) \in R_0] + \Pr[\mathcal{E}_{a,b} \text{ and } R(\alpha) \in R_1]$$

P_0 — DANGEROUS CASE; P_1 — SAFE CASE

SHOULD BE OK, SINCE MANY COIN FLIPS

For first term we have

$$P_0 \le \Pr[R(\alpha) \in R_0]$$

Since (writing $R = R(\alpha)$) it holds that

$$|R| \le \lceil k/t \rceil \le 2k/t = \frac{t}{2} \cdot \frac{4k}{t^2} \le \frac{t}{2} \cdot r \quad (*)$$

$r \ge 4k/t^2$ by clique-denseness

we have

$$|R \cup V^1(a)| \le |R| + |V^1(a)| \le \frac{rt}{2} + \frac{r}{2} \le rt$$

Since W is not g'-neighbour-dense for $R \cup V^1(a)$ but is mostly neighbour-dense, it holds that

$$|(R(\alpha) \cup V^1(a)) \cap S| \ge r$$

and hence

$$|R(\alpha) \cap S| \ge r/2 \qquad (|V^1(a)| \le \tfrac{r}{2})$$

Thus

$$\Pr[R(\alpha) \in R_0] \le \Pr[|R(\alpha) \cap S| \ge r/2] \quad (**)$$

But S is fairly small, so we can use union bound to get

$$\Pr[|R(\alpha) \cap S| \ge r/2] \le$$

$$\sum_{\substack{\text{choice of} \\ \{x_{v,j_v} \mid v \in S\}}} \Pr[\text{all } x_{v,j_v} \mapsto 1] \le$$

$$\binom{|S|k}{r/2} \left(\frac{r s^{-(1+\varepsilon)}}{2ek} \right)^{r/2} \le$$

$\binom{n}{k} \le \left(\frac{ne}{k}\right)^k$; $|S| \le s$

$$\leq \left(\frac{2esk}{r}\right)^{r/2}\left(\frac{rs^{-(1+\varepsilon)}}{2ek}\right)^{r/2}$$

$$= s^{-\varepsilon r/2} \qquad (***)$$

Combining (*), (**), and (***), we have

$$\boxed{\Pr[\mathcal{E}_{a,b} \text{ and } R(\alpha) \in \mathcal{R}_0] \leq s^{-\varepsilon r/2}} \qquad (P_0)$$

for the dangerous case.

For P_1 we have $R(\alpha) \in \mathcal{R}_1$, i.e.,

$|\vec{N}_W(R(\alpha) \cup V^1(a))| \geq q'$ (should be able to argue)

This seems safe(r), since lots of free choices in W to extend clique $R(\alpha) \cup V^1(a)$

By construction, all variables x_{u,i^*}, $u \in W$ must be set to 0 in α between a and b if α is to usefully traverse (a,b).

CLAIM

Any path α contributing to P_1 must set at least q' variables $x_{u,i^*} = 0$ for $u \in W$ as result of coin flip

Proof of claim

Since $V^1_{i^*}(b) = \emptyset$ and i^* not forgotten at b, same holds for every node along α before b.

So not answer x_{u,i^*} because of forgetfulness and also not due to functionality axiom

Also for all $c \in [a,b)$ on α it holds that

$$\boxed{V^1(c) \subseteq V^1(a) \cup R(\alpha)}$$

Therefore, for $u \in \hat{N}_W(R(\alpha) \cup V^1(a))$ x_{u,i^*} is not due to edge axiom, and $|\hat{N}_W(R(\alpha) \cup V^1(a))| \geq q'$ ▨

Again, by read-once property only one chance to get each x_{u,i^*} right

$$\Pr[\mathcal{E}_{a,b} \text{ and } R(\alpha) \in R_1] \leq$$

$$\leq \Pr[\alpha \text{ gets coin flips } x_{u,i^*}=0 \text{ for } q' \text{ vertices } u]$$

$$= \left(1 - \frac{r s^{-(1+\varepsilon)}}{2ek}\right)^{q'} \leq \quad 1-x \leq e^{-x}$$

$$\leq \exp\left(-\frac{r s^{-(1+\varepsilon)}}{2ek} q'\right)$$

$$= \exp\left(-\frac{r s^{-(1+\varepsilon)}}{2ek} \cdot 3\varepsilon k s^{1+\varepsilon} \log s\right)$$

$$\leq \exp((\log s) \cdot -\varepsilon r/2) \qquad (P_1)$$

$$= s^{-\varepsilon r/2}$$

Combining (P_0) and (P_1), we get

$$\Pr[\mathcal{E}_{a,b}] \leq 2 s^{-\varepsilon r/2}$$

as claimed in Lemma 10 ▨

(1) Generalize lower bound to general resolution
- Proof we did uses regularity heavily
- But mostly neighbour-dense property isn't "regular"

(2) And to polynomial calculus!

(3) Lower bounds for non-random graphs
- (Dense graphs (sufficiently) with good enough expansion?
- Ramsey graphs?

n-vertex graph is a RAMSEY GRAPH if no set of $\lceil 2\log_2 n \rceil$ vertices form clique or independent set

Possible to get $n^{-\Omega(\log n)}$ lower bound

$G \sim G(n, 1/2)$ is Ramsey with high probability, but can we get same lower bound for non-random graph under only promise that it is Ramsey

(4) Generalize lower bounds from clique to subgraph isomorphism problem for fixed pattern graph H that doesn't embed isomorphically into G

Clique lower bounds for circuits generalized to other subgraph isomorphism problems in [Lig Razborov, and Rossman '17]
[Kush and Rossman '23]

Problem (1) somewhat similar flavour to weak pigeonhole principle formulas (WPHP) with n holes and $m \gg n$ pigeons (think $m = \exp(n^\varepsilon)$)

[Buss & Pitassi '97] showed that WPHP gets easier for $m \approx \exp(\sqrt{n \log n})$
Haken's PHP lower bound (and the proof by Pudlák that we did) breaks down already at $m \approx n^2$

First lower bound for regular resolution by [Pitassi&Raz '04]

Lower bound technique made non-regular by [Raz '04] — much more careful book-keeping to deal with that x can be queried over and over again to get $x \mapsto 1$

Can the ideas that strengthened [Pitassi & Raz '04] to [Raz '04] be useful also for the clique problem

Clique formulas interesting because they break the tools in our resolution toolbox:

- random restrictions / bottleneck counting
- interpolation
- and size-width lower bounds, which is what we will see next lecture.