DD2445 COMPLEXITY THEORY: LECTURE 23

Recap

Regular resolution

Clauses derived by resolution rule

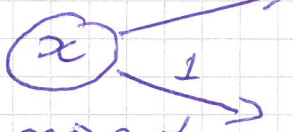
$$\frac{C \vee x \qquad D \vee \bar{x}}{C \vee D}$$

Represent refutation as DAG

Regular: On any path from source/axiom to sink/contradiction any variable resolved only once

Read-once branching program

One start node

Every non-sink 

Truth value assignment $\alpha \leadsto$ path

Every sink labelled by clause $C \in F$

Every α leading to sink should have $\alpha(C) = 0$

Read-once: Along any path, query any variable at most once

Size of ROBP = # nodes

Regular resolution refutation $\iff$ Read-once branching program

- Flip direction of edges
- query resolved variables.

(iii) Clique formula

$k \subset |V|$

Basically clique-colouring formula but with restriction $\mathcal{G}$ to $\vec{p}$-variables. But with extra twist to avoid formula being hard for "stupid reasons"

Variables $\boxed{x_{v,i}}$ = "v is ith member of clique"

$v \in V = \{1, 2, \ldots, n\} = [n]$

$i \in \{1, 2, \ldots, k\} = [k]$

Clique axioms $\boxed{\bigvee_{v \in V} x_{v,i}}$ $\quad i \in [k]$

Edge axioms $\boxed{\bar{x}_{u,i} \vee \bar{x}_{v,j}}$ $\quad i \neq j \in [k]$, $(u,v) \notin E$

Functionality axioms $\boxed{\bar{x}_{u,i} \vee \bar{x}_{v,i}}$ $\quad i \in [k]$, $u \neq v \in V$

Ordering axioms $\boxed{\bar{x}_{u,i} \vee \bar{x}_{v,j}}$ $\quad u < v \in V$, $(u,v) \in E$, $i > j \in [k]$

"If u and v both in clique and $u < v$, then clique index of $u <$ clique index of v"

Ordering axioms are important — but we will ignore them for simplicity (all key ideas still there, and even w/o ordering axioms the lower bound is actually non-trivial)

GOAL: Show lower bound $n^{\Omega(k)}$

(I.e., $\exists$ universal constant γ s.t. lower bound $n^{\gamma \cdot k}$)

PREVIOUSLY KNOWN

Tree-like resolution

$n^{\Omega(k)}$ lower bound for balanced complete $(k-1)$-partite graph

General resolution [Beame, Impagliazzo, Sabharwal '07]

Lower bound $\exp(n^{\varepsilon})$ for $k = n^{\delta}$, $\delta \geq 5/6$

Nothing known for smaller k

Regular resolution

Complete $(k-1)$-partite graphs easy

We ~~show~~ lower bound $n^{\Omega(k)}$ for $k \leq n^{1/2-\varepsilon}$ on average for random graphs

Should be true also for general resolution, but this remains open

---

From now on, talk only about branching programs

ROBP: ~~path~~ $\Leftrightarrow$ partial assignment

Branching program: nodes a, b

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

$\beta(a)$:= maximal partial assignment contained in any path from source to a

= all variable queries made along any path to a

"Assignments remembered at a"

Source path = path from source to same node

On path α x queried, edge $(x) \xrightarrow{b}$ taken

"α sets x to b"

If $\exists$ source path α to a such that
- α sets x
- $\beta(a)$ doesn't contain x

we say x FORGOTTEN at a

OBSERVATION 1

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

Proof Use read-once property.

$\exists$ α : source $\rightsquigarrow a$ not setting x

$\exists$ α' : source $\rightsquigarrow a$ setting x

Suppose $\exists$ $\gamma : a \rightsquigarrow b$ setting x

Then composed path $\alpha' \circ \gamma$ violates read-once property. ∎

Focusing on clique formulas

If $x_{v,i}$ forgotten at a for some $v \in V$, say INDEX i FORGOTTEN at a

If source path α ends at clique access $\bigvee_{v \in V} x_{v,i}$ (which it falsifies), say PATH α RULES OUT INDEX i

OBSERVATION 2

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

Proof Any α' ending at b must have queried all $x_{v,i}$, $v \in V$ (and have received answers 0), so no $x_{v,i}$ can be forgotten

For the rest of this lecture, fix arbitrary ROBP Π solving k-clique formula for $G=(V,E)$ without k-clique. Want to prove Π has size $n^{\Omega(k)}$ asymptotically almost surely if G random graph.

Define **distribution $\mathcal{D}$ over paths α** by following process, starting at source. Say current node a queries $x_{v,i}$.

(a) If $\beta(a) \cup \{x_{v,i} \mapsto 1\}$ falsifies edge or functionality axiom, take 0-edge (set $x_{v,i} \mapsto 0$) } (a)+(b) "FORCED CHOICES"

(b) If i forgotten at a, set $x_{v,i} \mapsto 0$

(c) Otherwise, flip $n^{-\delta}$-biased coin ($\delta > 0$)

$x_{v,i} \mapsto 1$ with probe $n^{-\delta}$

$x_{v,i} \mapsto 0$ otherwise (highly likely)

(c) "FREE COIN FLIPS"

OBSERVATION 3

(i) Any $\alpha \sim \mathcal{D}$ ends by ruling out some index i (never falsifies functionality or edge axioms)

(ii) Any $\alpha \sim \mathcal{D}$ sets at most k variables $x_{v,i}$ to 1

Proof Exercise. (Uses definition of $\mathcal{D}$, obviously)

FIRST PROOF IDEA (WON'T WORK)

Given any $\alpha \sim D$, define waypoints for $t \in \mathbb{N}^+$ fixed

a_0 = source

a_{i+1} = first time after a_i $\lceil k/t \rceil$ assignments $x_{v,i} \mapsto 1$ on α or sink of path, whichever comes first

Suppose α rules out i

Let $V_i = \{ v \mid x_{v,i} \mapsto 0$ between a_{i-1} and $a_i \}$

$V = V_1 \dot\cup \cdots \dot\cup V_{t'}$ $\quad t' \le t$

There must exist j s.t. $|V_j| \ge n/t$

i.e., between a_{j-1} and a_j we have $\ge n/t$ assignments $x_{v,i} = 0$

ROBP Π makes lots of progress in ruling out vertices

Call such pair (a_{j-1}, a_j) USEFUL*.
We just proved:

OBSERVATION 4

Any path $\alpha \sim D$ passes through a useful pair (a, G) with probability 1

Now we want to fix any pair (a, G) and argue that

$$\Pr_{\alpha \sim D}[\ (a,G) \text{ useful for } \alpha\ ] \le n^{-\Omega(k)}$$

If we can do this, then we're done!

We have

$$1 = \Pr_{\alpha \sim \mathcal{D}}[\exists (a,b) \in \Pi^2 \text{ useful for } \alpha]$$

$$\leq \sum_{(a,b) \in \Pi^2} \Pr_{\alpha}[(a,b) \text{ useful for } \alpha]$$

$$\leq |\Pi|^2 \cdot n^{-\Omega(k)}$$

So $|\Pi| \geq n^{-\Omega(k)}$

OBSERVATION 5 (CRUCIAL)

Suppose $\exists$ path $\alpha \sim \mathcal{D}$ s.t.
- α passes through a and b
- α assigns $x_{v,i} \mapsto 0$ for $v \in V_j$
- α rules out i

Then any path α' through a and b has to set $x_{v,i} \mapsto 0$ for exactly $v \in V_j$

Proof Exercise. (Use read-once property)

HOPEFUL CLAIM 6 (BROKEN)

For any $(a,b) \in \Pi^2$

$$\Pr_{\alpha \sim \mathcal{D}}[(a,b) \text{ useful for } \alpha] \leq n^{-\Omega(k)}$$

Attempt at proof

1) If (a,b) not useful for any path $\Rightarrow$ probability 0.
2) Suppose $S(a)$ contains $\Omega(k)$ assignments $x_{v,j} \mapsto 1$. Then

$$\Pr_{\alpha \sim \mathcal{D}}[\alpha \text{ passes through } a] \leq n^{-5k} \quad \text{– OK}$$

3) At a few 1s in $\beta(a)$ — Π knows $kC\overline{XII}$
almost nothing about the clique
Yet makes $\geq n/t$ assignments $x_{v,i} \mapsto 0$
Some of these might be forced.
But polynomial fraction should
be free coin flips. say n^δ $\gamma \gg \delta$

$\Pr[\text{all these free coin flips yield } 0] =$

$= (1-n^{-\delta})^{n^\delta} = \exp(-\Omega(n^{-(\gamma-\delta)}))$

Great ☺ Except case 3 broken.
We could have essentially all choices forced.
Need better notion of "useful"

ACTUAL PROOF (MODULO CALCULATIONS)

For any assignment β, let $\beta_1 = \{x_{v,j} \text{ in } \beta \text{ set to } 1\}$

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

$\Gamma_W(R) = \bigcap_{v \in R} \Gamma(v) \cap R$ common neighbours of R inside W

$W \subseteq V$ is **g-NEIGHBOUR-DENSE** for $R \subseteq V$
if $|\Gamma_W(R)| > g$

W is **(r,g)-NEIGHBOUR-DENSE** if it is
g-neighbour-dense $\forall R$, $|R| \leq r$

Means that any clique of size r can
be enlarged with vertex from W

Should be likely to hold for random graph
But as r, q get larger, property gets more unlikely
If it fails want to find "mostly neighbour-dense" set W for which few R make W fail.

In what follows, think

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

W is (r, r', q, s) - MOSTLY NEIGHBOUR-DENSE
if $\exists\ S \subseteq V$, $|S| \leq s$ s.t. if for $R \subseteq V$, $|R| \geq r$, W is not q-neighbour dense for R, then $|R \cap S| \geq r'$

$G = (V, E)$ is (k, r, s, ε) - CLIQUE-DENSE
if $\exists\ t, q \in \mathbb{R}^+$ s.t.
(1) V is (tr, tq) - neighbour-dense
(2) Every (r, q)-neighbour-dense set W is (r^*, r', q', s) - mostly neighbour-dense for

$$r' = \varepsilon \cdot r / (2(1+\varepsilon))$$
$$r^* = r_{k/t} + r'$$
$$q' = (\varepsilon r/2)\, s^{1+\varepsilon} \log s$$

THEOREM 7 For n large enough, for appropriately chosen r, s as above, for ε small, $t = O(1)$, $q >> s^{y^{<1}}$ it holds that $G \sim G(n,p)$ for $p = n^{-2q/(k-1)}$ is (k, r, s, ε) - clique-dense.

Proof 3 pages of calculations ...

THEOREM 8
If $k \in \mathbb{N}^+$ and $r, s, \varepsilon \in \mathbb{R}^+$ are such that G is (k, r, s, ε)-clique-dense, then any regular resolution refutation of the clique formula for G requires length $\Omega(s^{\varepsilon r/4})$ (i.e., any ROBP requires this size).

Proof of Thm 8 is what we will focus on
Reuse our previous idea, but make better definition of useful

$$V_i(a) = \{ u \in V \mid \beta(a) \text{ sets } x_{u,i} \mapsto 0 \}$$
$$P_i(a) = \{ u \in V \mid \beta(a) \text{ sets } x_{u,i} \mapsto 1 \}$$

Keep distribution $\mathcal{D}$
Probability of coin flip 1 = $s^{-(1+\varepsilon)}$

Observation 3 still true

Fix t, q witnessing that G is (k, r, s, ε) - clique-dense.

$V \notin \bigcap_V \left(\bigcup_{j \in [4]} P_j(\epsilon) \right)$

$x_{v,i}$ a?

Forced choice (a) in $\mathcal{D}$ for node v if

Say $(a,b) \in \Pi^2$ | (TRULY) USEFUL if | KC XV
$\exists$ path α in Π s.t.
(1) α passes through a & b in that order
(2) $|B_1(b) \setminus B_1(a)| \leq \lceil k/t \rceil$, i.e. path sets at most that many 1s between a & b (a included; b excluded)
(3) α rules out some index i
(4) $N_i(b) \setminus N_i(a)$ is (r,q)-neighbour-dense

Key difference: (4)
Don't consider how many zeros filled in
Consider how hard/unlikely these zeros are

LEMMA 9 ($\Leftarrow$ OBS 4)
Say that path α in Π USEFULLY TRAVERSES (a,b) if (1), (2) & (4) hold
[Note that other paths can also go through (a,b)]
Then any path $\alpha \sim \mathcal{D}$ usefully traverses | (a,b) | some | with probability 1.

Proof Exercise. Use waypoints idea from Obs 4 + neighbour-denseness. Also use Obs 5.

LEMMA 10 ($\Leftarrow$ HOPEFUL CLAIM 6)
For any useful pair (a,b) it holds that
$$\Pr_{\alpha \sim \mathcal{D}}[\alpha \text{ traverses } (a,b)] \leq 2s^{-\varepsilon_0/2}.$$

Lemmas 9+10 immediately yield Thm 8 as per our previous proof idea.

Proof of Lemma 10

Fix useful pair (a,b)

Fix index i^* ruled out by same path witnessing the usefulness

$P := \bigcup_{j \in [k]} P_j(a)$ "clique members known at a"

$W := N_{i^*}(G) \setminus N_{i^*}(a)$ "vertices ruled out during $a \rightsquigarrow b$ for i^{th} member"

$W(r,q)$ - neighbour-dense by definition

+

$G(k,r,s,\varepsilon)$ - clique-dense $\Rightarrow$

W is mostly neighbour-dense

Let S be the set witnessing this

(Any R for which W fails to be neighbour-dense has large intersection with S)

Let E = event "α usefully traverses (a,b)"

Want to upper-bound $\mathbb{P}_{\alpha \sim \mathcal{D}}[E]$

Case analysis depending on $|P|$.

Case 1: $|P| > \varepsilon r/(2(1+\varepsilon))$

$\beta(a)$ contains many assignments $x_{v,j} \mapsto 1$.

But these are all free coin flips $\Rightarrow \alpha$ very unlikely even to reach a (as argued before)

Formally

$$\Pr_{\alpha}[E] \leq \Pr_{\alpha}[\alpha \text{ passes through } a]$$
$$\leq \left(s^{-(1+\varepsilon)}\right)^{\varepsilon r/(2(1+\varepsilon))}$$
$$= s^{-\varepsilon r/2}$$

Case 2: $|P| \leq \varepsilon r/(2(1+\varepsilon))$

Let $R(\alpha) = \{u \mid \text{some } x_{u,j} \mapsto 1 \text{ between } a \text{ \& } b\}$

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

If $x \in E$, then $|R(\alpha)| \leq \lceil k/t \rceil$

In Hopeful Claim 6, failed because dangerous vertices in $R(\alpha)$ can make $T_W(R(\alpha))$ shrink a lot, forcing many $x_{v,i} \mapsto 0$.

But if so, $R(\alpha)$ is an example of W failing to be neighbour-dense.

And our W here is mostly neighbour-dense, so getting such $R(\alpha)$ shouldn't not be too likely.

Do subcase analysis based on whether $R(\alpha)$ is dangerous or not

kC XVIII

Dangerous

$$R_0 := \{R : |R| \le \lceil k/t \rceil, |T_W(R \cup P)| \le (\varepsilon r/2) s^{1+\varepsilon} \log s\}$$

$$R_1 := \{R : |R| \le \lceil k/t \rceil, |T_W(R \cup P)| > (\varepsilon r/2) s^{1+\varepsilon} \log s\}$$

$$\Pr[E] = \Pr[E \text{ and } R(\alpha) \in R_0] + \Pr[E \text{ and } R(\alpha) \in R_1]$$

Looks OK; previous argument should work

Dangerous case E and $R(\alpha) \in R_0$

$|R| \le \lceil k/t \rceil$, so

$$|R \cup P| \le \lceil k/t \rceil + \varepsilon r/(2(1+\varepsilon))$$

By mostly neighbour-denseness

$$|(R \cup P) \cap S| \ge \varepsilon r/(2(1+\varepsilon))$$

Our Paper claims $\ge \frac{r}{2}\left(1 + \frac{\varepsilon}{1+\varepsilon}\right)$

$$|P| \le \frac{r}{2} \cdot \frac{\varepsilon}{1+\varepsilon} \Rightarrow$$

$$|R \cap S| \ge r/2$$

Using this we get

$$\Pr[E \text{ and } R(\alpha) \in R_0] \le \Pr[R(\alpha) \in R_0]$$
$$\le \Pr[|R(\alpha) \cap S| \ge r/2]$$
$$\le \binom{|S|}{r/2} \left(s^{-(1+\varepsilon)}\right)^{r/2}$$
$$\le |S|^{r/2} s^{-(1+\varepsilon)r/2} \le s^{-\varepsilon r/2}$$

Safe case E and $R(\alpha) \in R_1$

For any $\alpha \sim D$ let $W^*(\alpha) \subseteq W$ be set of $u \in W$ s.t. α queries $x_{u,i*}$ and answer is coin flip. If α satisfies E, then

$$T_W(R(\alpha) \cup P) \subseteq W^*(\alpha)$$

(Because all of W queried, and max set of clique membership is $R(\alpha) \cup P$)

And all of these queries result in answers 0 (or else we can't reach b by Obs 5.

We don't know exactly which queries are free coinflips, but many of them have to be since we have lower bound on $|T_W(R \cup P)|$.

$$\Pr[E \text{ and } R(\alpha) \in R_1] \leq$$

$$\Pr\left[x_{v,i*} \mapsto 0 \ \forall v \in W \text{ and } |W^*(\alpha)| > \frac{\varepsilon r}{2} s^{1+\varepsilon} \log s\right] \leq$$

$$\Pr\left[x_{v,i*} \mapsto 0 \ \forall v \in W^*(\alpha) \text{ and } |W^*(\alpha)| > \frac{\varepsilon r}{2} s^{1+\varepsilon} \log s\right] \leq$$

$$\leq \left(1 - s^{-(1+\varepsilon)}\right)^{\frac{\varepsilon r}{2} s^{1+\varepsilon} \log s}$$

$$\leq e^{-\frac{\varepsilon r}{2} \log s} = s^{-\varepsilon r/2}$$

Adding dangerous case and safe case, get probability $\leq 2s^{-\varepsilon r/2}$ ☐

kc XX

This concludes the course

What did we see during 2nd half?

- Communication complexity
- Circuit complexity
- Proof complexity

Seemingly quite different, but many connections at deeper level

General phenomenon in TCS: often breakthrough results from unexpected connections.

At the end of the day:

Most of the questions we care about we <u>cannot</u> answer.

Such is research

But lots of beautiful results have been obtained while trying

Tried to show you a (biased) selection of such results