Lecture 8. Lovász Local Lemma.

Dependency graph: $\forall A_i$ is independent from $\{A_j : j \neq i, j \notin N(i)\}$.

Theorem (Lovász local lemma. symmetric form).

Let $A_1 \dots A_n$ be events with $\Pr[A_i] \le p$. Suppose $\exists$ a dependency graph with maximum degree d, s.t. $ep(d+1) \le 1$. Then $\Pr[\cap \bar{A_i}] > 0$.

Theorem (Lovász local lemma. asymmetric / general form).

Let $A_1 \dots A_n$ be events, and A_i is independent from $\{A_j : \overset{j \neq i}{\checkmark} j \notin N(i)\}$.

If $\exists x_1 \dots x_n \in [0,1)$ such that $\Pr[A_i] \le x_i \prod_{j \in N(i)} (1-x_j)$. $\forall i$

then $\Pr[\cap \bar{A_i}] \ge \prod (1-x_i)$.

Remark. To see the symmetric form. set $x_i = 1/_{d+1} < 1$. for all i.

Then $x_i \prod_{j \in N(i)} (1-x_j) \ge \frac{1}{d+1}\left(1-\frac{1}{d+1}\right)^d > (e(d+1))^{-1} \ge p$.

Remark. The constant e is best possible. (Shearer 1985).

Proof. We claim that $\Pr[A_i \mid \bigcap_{j \in S} \bar{A_j}] \le x_i$. for all $i \notin S \subseteq [n]$.

If it holds. then $\Pr[\cap \bar{A_i}] = \Pr[\bar{A_1}] \Pr[\bar{A_2} \mid \bar{A_1}] \cdots \ge \prod (1-x_i)$.

Now prove our claim by induction. Trivial if $|S| = 0$.

Let $i \in S$. $S_1 = S \cap N(i)$. $S_2 = S \setminus S_1$. Then we have

$$\Pr[A_i \mid \bigcap_{j\in S} \bar{A_j}] = \frac{\Pr[A_i \cap (\bigcap_{j\in S_1} \bar{A_j}) \mid \bigcap_{j\in S_2} \bar{A_j}]}{\Pr[\bigcap_{j\in S_1} \bar{A_j} \mid \bigcap_{j\in S_2} \bar{A_j}]} = \frac{\alpha}{\beta}.$$

Note that $\alpha \le \Pr[A_i \mid \bigcap_{j\in S_2} \bar{A_j}] = \Pr[A_i] \le x_i \prod_{j\in N(i)} (1-x_j)$.

Let $S_1 = \{t_1, \dots, t_r\}$. $\beta = \prod_{k=1}^{r} \Pr[\bar{A}_{t_k} \mid (\bigcap_{l=1}^{k-1} \bar{A}_{t_l}) \cap (\bigcap_{j\in S_2} \bar{A_j})]$

(by induction hypothesis) $\ge (1-x_{t_1}) \cdots (1-x_{t_r}) \ge \prod_{j\in N(i)} (1-x_j)$. $\square$

Example. Let φ be a k-SAT formula. If each of clauses overlaps with $\le 2^{k-2}$ other clauses. then φ is satisfiable.

literal $\in \{x_i, \bar{x_i}\}$.

variable $= \{x_1, \dots, x_n\}$. clause e.g. $C = x_1 \vee \bar{x_2} \vee x_3$

$\varphi = C_1 \wedge C_2 \wedge \cdots \wedge C_m$. k-uniform 若 $|C_i| = k$. degree $\le 2^{k-2}/k$.

Question: can we find such a satisfying assignment in poly-time?

Algorithmic Lovász Local Lemma (2020 Godël prize).

Random variable model: each event only depends on some variables.

A computationally hard example: discrete logarithm.

Let $q = 2^k$. $f: [q] \to [q]$ be a bijection. $y \in [q]$ be an element

A_i be the bad event $f(x)$ and y disagree at ith bit. $x \sim [q]$.

All A_i's are mutually independent. so local lemma applies.

But computing $f^{-1}(y)$ may be hard. $f: \mathbb{F}_q \to \mathbb{F}_q = g^x$.

Algorithm:

step 1. Initialize each variable a random value independently.

step 2. While some bad event A_i occurs (pick A_i arbitrarily).

Resample all variables that A_i depends on. $vbl(A_i)$.

Theorem (Robin Moser & Gábor Tardos, 2010).

If the Lovász local lemma holds. then MT algorithm returns an assignment that none bad event occurs in expected linear time.

In particular, the expected rounds of resampling $\leq E = \sum_{i=1}^{n} \frac{x_i}{1-x_i}$.

Proof. Let the excution log L be the sequence of A_i's that are picked in step 2. $|L|$ may be infinite. but we claim $\mathbb{E}[|L|] \leq E$.

Construct witness trees as follows for each time $t \leq |L|$.

Let $L = (A_{\ell_1}, A_{\ell_2}, \ldots A_{\ell_t}, \cdots)$. read prefix $A_{\ell_t}, \ldots A_{\ell_1}$.

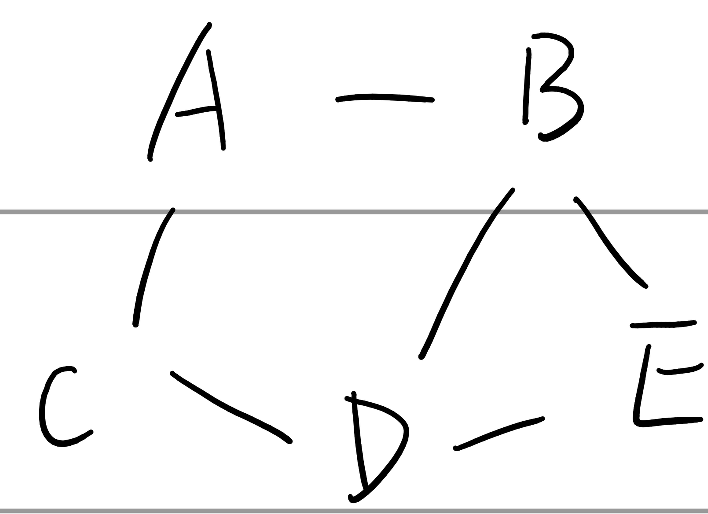
① Let the root of the witness tree T be A_{ℓ_t}.

② For $t' = t-1, \ldots, 1$.

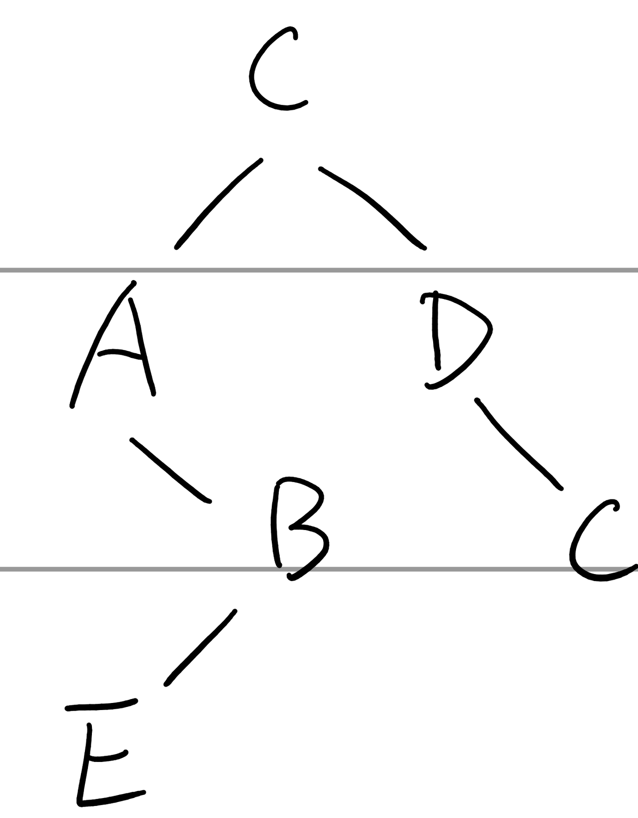
If none of vertices in T shares variables with $A_{\ell_{t'}}$. continue.

Otherwise find a deepest such node $A_{[v]}$. add $A_{\ell_{t'}}$ as its child.

Example:



$L = C\,E\,B\,D\,A\,B\,B\,E\,C$



Now consider properties of the witness trees.

(i). $T(t_1) \neq T(t_2)$ for different times $t_1 \neq t_2$.

if $A_{\ell_{t_1}} \neq A_{\ell_{t_2}}$, $T_1 = T(t_1)$, $T_2 = T(t_2)$ have different roots.

if $A_{\ell_{t_1}} = A_{\ell_{t_2}} = A_r$. A_r appears different times in T_1 and T_2.

(ii). $\forall T = T(t)$. $u, v \in T$ of same depth, $vbl(A_{[u]}) \cap vbl(A_{[v]}) = \phi$.

(i) $\Rightarrow$ $\mathbb{E}[|L|] = \sum_T \mathbb{E}[X_T] = \sum_T \Pr[T \text{ is a witness tree}]$.

(ii) $\Rightarrow$ $\Pr[T \text{ appears as a witness tree for some time } t] \leq \prod_{v \in T} \Pr[A_{[v]}]$

For example. consider $T = \overset{A}{\circ}$. If T is a valid witness tree for some time t. then A happens at beginning so $\Pr[T] \leq \Pr[A]$.

If $T = \begin{matrix} \circ A \\ | \\ \circ B \end{matrix}$. Clearly B happens at beginning. After resampling $vbl(B)$. A occurs. So $\Pr[T] \leq \Pr[B]\Pr[A]$.

In general. consider the reverse BFS order of T: $v_1\ v_2, \ldots$

We claim $\Pr[T \text{ valid for some time } t] = \Pr[\cap A_{[v_i]} \text{ independently}]$.

construct a coupling. The key is to share randomness.

Assume for each variable, we have an infinite list of values. each of them is independently sampled and then fixed.

When simulate the MT algorithm or check $A_{[v_1]} A_{[v_2]} \cdots$ independently, we look up the value table of each variable instead of sampling.

Prove by induction on the depth from bottom to top.

For each $v \in T$, and any $u \in T$ with $vbl(A_{[u]}) \cap vbl(A_{[v]}) \neq \phi$. u is deeper than v iff $A_{[u]}$ appears before $A_{[v]}$ in the excution log.

For any $z \in vbl(A_{[v]})$. let $n_{z,v}$ be the number of u's before v s.t. $z \in vbl(A_{[u]})$. In the simulation of MT. when checking whether $A_{[v]}$ occurs. look up the $(n_{z,v}+1)$-th value of variable z. when checking the reverse BFS order sequence $A_{[v_1]}, A_{[v_2]}, \ldots$, we also look up the $(n_{z,v}+1)$-th value of variable z at the time checking $A_{[v]}$. So the event that T is valid has the same distribution as the sequence occur.

Namely. $Pr[T \text{ is valid for some time } t] = \prod_{v \in T} Pr[A_{[v]}]$

Of course. $Pr[T \text{ is a witness tree } T(t)] \leq \prod_{v \in T} Pr[A_{[v]}]$.

Let W be the set of all possible witness trees.

$$\mathbb{E}[|L|] = \sum_{T\in W} \Pr[T = T(t) \text{ for some } t]$$

$$\le \sum_{T\in W} \prod_{v\in T} \Pr[A_{[v]}].$$

If $T \in W$. then T satisfies $\begin{cases} \text{finite.} \\ u\to v \text{ then } A_{[u]}\ A_{[v]} \text{ overlap.} \\ \text{depth } u = \text{depth } v \text{ then } A_{[u]}\ A_{[v]} \text{ disjoint.} \end{cases}$

Let W' be the set of trees only satisfies "$u\to v$ then $A_{[u]}$. $A_{[v]}$ overlap."

W'_B be the set of trees in W' and rooted at event B.

Generate trees in W_B' by a random process (Galton–Watson tree).

root $= B$. for any vertex $A_{[v]}$. children $= N^+([v])$ that variable overlaps with $A_{[v]}$. for each children $A_{[u]}$. alive with $q_{[u]}$ and dying with $1-q_{[u]}$.

Now we compute $\Pr[\text{Galton–Watson process generates } T] \triangleq P_T$.

$$P_T = \frac{1}{q_B} \prod_{v\in T} q_{[v]} \prod_{v\in T} \prod_{k\in N^+([v])\setminus D(v)} (1-q_k) \qquad N^+([v]) = N([v]) \cup \{[v]\}.$$

$$= \frac{1-q_B}{q_B} \prod_{v\in T} \frac{q_{[v]}}{1-q_{[v]}} \prod_{k\in N^+([v])} (1-q_k). \qquad D(v) = \text{alive children of } v.$$

$$= \frac{1-q_B}{q_B} \prod_{v\in T} q_{[v]} \prod_{k\in N([v])} (1-q_k). \qquad \text{setting } q_k = x_k.$$

$$\ge \frac{1-x_B}{x_B} \prod_{v\in T} \Pr[A_{[v]}].$$

Clearly $\sum_{T\in W_B'} P_T = 1$. So. $\sum_{T\in W_B} \prod_{v\in T} \Pr[A_{[v]}] \le \sum_{T\in W_B'} P_T \cdot \frac{x_B}{1-x_B} = \frac{x_B}{1-x_B}$.

$\Rightarrow \mathbb{E}[|L|] \le \sum_{i=1}^{n} x_i/(1-x_i)$. $\square$.

Ramsey number revisit.

Theorem (Spencer, 1977). If $e\left(\binom{k}{2}\binom{n}{k-2}+1\right)2^{1-\binom{k}{2}}<1$. $R(k,k)>n$.

Proof. Color K_n randomly. For any R of size-k. let E_R be the event that R induces a monochromatic K_k. $\Pr[E_R]=2^{1-\binom{k}{2}}$.

$\forall R.S.$ independent if $|R\cap S|<2$. So $|N(R)|\le\binom{k}{2}\binom{n}{k-2}$. $\square$.

Remark. Optimizating the choice of n. it gives the best bound so far

$$R(k,k)>\left(\sqrt{2}/e+o(1)\right)k\cdot 2^{k/2}.$$

Let $K=\binom{n}{k}$ be the number of all events. $d=|N(R)|\approx K^{1-O(1/k)}$.

So local lemma doesn't work well. On the other hand, consider small subsets. e.g. $|R|=3$. There are $K=\binom{n}{3}$ events, but only $d\le 3(n-3)$ dependency. Now we compute $R(k,3)$. Let p TBD.

Color 0 with probability p. and 1 with $1-p$. $|S|=3$. $|T|=k$.

clearly $\Pr[A_S]=p^3$. $\Pr[B_T]=(1-p)^{\binom{k}{2}}$. dependency: $|S\cap T|\ge 2$.

For A_S: adjacent to $\le 3(n-3)$ $A_{S'}$ and $\le\binom{n}{k}$ $B_{T'}$.

For B_T: adjacent to $\le\binom{k}{2}(n-2)<\frac{k^2n}{2}$ $A_{S'}$ and $\le\binom{n}{k}$ $B_{T'}$.

If $\exists p.x.y.$ s.t. $\begin{cases} p^3\le x(1-x)^{3n}(1-y)^{\binom{n}{k}} \\ (1-p)^{\binom{k}{2}}\le y(1-x)^{k^2n/2}(1-y)^{\binom{n}{k}} \end{cases}$ then $R(k,3)>n$.

Setting $p = c_1 n^{-1/2}$. $k = c_2 n^{1/2} \log n$ $x = c_3 n^{-3/2}$ and $y = c_4 / \binom{n}{k}$. it gives $R(k,3) > c_5 k^2/\log^2 k$. The best known lower bound is $c_6 k^2/\log k$.

Analogously. $R(k,4) > k^{\frac{5}{2}+o(1)}$. better than any known without LLL.

Large independent sets from partition.

Given a graph with maximum degree Δ. $\alpha \geq |V|/(\Delta+1)$. The following theorem shows that $\exists$ a large independent set from any partition.

Theorem: Let $G = (V, E)$ has degree $\leq \Delta$. and $V = V_1 \cup \cdots \cup V_r$ be a partition where $|V_i| \geq 2e\Delta$. Then $\exists$ ind set contains a vertex from each V_i.

Proof. Some choice of bad events is better than others.

Let $k = \lceil 2e\Delta \rceil$ and assume $|V_i| = k$ for all i. Pick $v_i \in V_i$ u.a.r.

Attempt 1 of bad events: $\forall 1 \leq i < j \leq r$. $A_{i,j} = \{v_i \sim v_j\}$

$\Pr[A_{i,j}] \leq \Delta/k$. $A_{i,j} = \phi$ if there is no edge between V_i and V_j.

Dependency: $A_{i,j} \sim A_{k,l}$ if $\{i,j\} \cap \{k,l\} \neq \phi$. $d \leq 2\Delta k$. too large.

Attempt 2 of bad events: $\forall e \in E$. B_e = two endpoints are chosen.

$\Pr[B_e] \leq \frac{1}{k^2}$ Dependency: $B_e \sim B_f$ if $\exists V_I$ intersects both e and f. $d \leq 2k\Delta$. Then local lemma applies. $\square$.

Directed cycles of length divisible by k.

Theorem. (Alon & Linial, 1989). $\forall$ directed G with min out-degree δ and max in-degree Δ contains a cycle of length divisible by k. if

$$k \leq \frac{\delta}{1+\log(1+\delta\Delta)}.$$

Proof. Assume every $v \in V$ has out-degree δ. Assign $x_v \in \mathbb{Z}/k\mathbb{Z}$ to v.

Now we look for cycles that the label increase by 1 at each step.

Let $A_v = \{$none outneighbor of v has label $x_v+1\}$.

$\Pr[A_v] = (1-1/k)^{\delta} \leq e^{-\delta/k}$.

$N^o(v)$: outneighbors of v.

Dependency: $A_u \sim A_v$ if $\{u\} \cup N^o(u)$ intersects $\{v\} \cup N^o(v)$

so $d \leq (\Delta+1)\delta$. local lemma applies if $e^{1-\delta/k}(1+(\Delta+1)\delta) \leq 1$.

Improvement: Note that A_v is independent of all A_u's where

$N^o(v)$ is disjoint from $\{u\} \cup N^o(u)$.

Thus. $d \leq \Delta\delta$, and we are done by the local lemma. $\square$.