Lecture 21 11/12/2025

Lovasz Local Lemma

LLL is a powerful tool in the probabilistic method and has found several highly non-trivial applications in algorithms.

In the probabilistic method we prove the existence of some object by running a probabilistic experiment and arguing that the object/property holds with non-zero probability.

First moment method

We use expectation analysis. As an example we showed that in any graph $G=(V,E)$ there exists a max-cut of value $\geq \frac{|E|}{2}$ by picking a random cut whose expectation is $\frac{|E|}{2}$.

Second moment method

Here we use variance analysis plus something like the Chebyshev bound.

Example: Let $G(n,p)$ be a random graph on n vertices where each edge is chosen independently with prob p. At what value of p will $G(n,p)$ have a clique of size 4? Clearly, when $p \to 0$ graph will be very sparse and there will not be a 4-clique. When $p \to 1$

there will be a 4-clique whp since graph becomes dense.

Turns out that $p = n^{2/3}$ is the "threshold".

To see one direction we use first moment method.

Let X be expected # of 4-cliques.

$X = \binom{n}{4} p^6$ since if we fix a set of 4 vertices it will be a clique iff all six edges are chosen.

If $p \leq c_1 n^{-2/3}$ for sufficiently small constant c_1, $E[X] < 0.1$

$Pr[X \geq 1] \leq E[X]$ for non-neg integer random variable.

$\Rightarrow Pr[X=0] \geq 1 - E[X] \geq 0.9$.

We would like to compute the variance of X.

Note that $X = \sum_{S \in \mathcal{S}} X_S$ where $\mathcal{S}$ ranges over all ~~fo~~ subsets of four vertices and X_S is indicator for S being a clique. $\Pr[X_S] = p^6$.

If $S_1, S_2 \in \mathcal{S}$ then X_{S_1} and X_{S_2} are independent if S_1 and S_2 do not share any edges. Otherwise they are dependent. To estimate $\mathrm{Var}(X)$ we write

$$E[X^2] = \sum_{S} E[X_S^2] + 2\sum_{S_1, S_2 \in \mathcal{S}} E[X_{S_1} X_{S_2}]$$

$$\geq \binom{n}{4} p^6 + 2 \cdot \sum_{S_1 \neq S_2} E[X_{S_1}] E[X_{S_2}]$$

where $S_1 \sim S_2 \Rightarrow S_1$ and S_2 are dependent and $S_1 \not\sim S_2$ means independent.

Suppose we pretend all S_1 and S_2 are independent. Then there are roughly n^8 such pairs and in that case

$$\mathrm{Var}(X) = \sum_{S \in \mathcal{S}} \mathrm{Var}(X_S) = \binom{n}{4} p^6 (1-p^6)$$

Then by Chebyshev

$$\Pr[X=0] = \Pr\left[|X - E[X]| > E[X]\right]$$

$$\le \frac{\mathrm{Var}(X)}{(E[X])^2}$$

$$\le \frac{\binom{n}{4} p^6 (1-p^6)}{\binom{n}{4}^2 \cdot p^{12}} \le \frac{1-p^6}{\binom{n}{4} p^6}$$

One can check that if $p = c_2 n^{-2/3}$ for sufficiently large c_2 then

$\Pr[X=0] < 0.1$

However X_{S_i} and X_{S_j} are not independent for all S_i and $S_j \in \mathcal{S}$.

But if we calculate $\mathrm{Var}(X)$ more carefully we see that

$$E[X^2] = \sum_{S \in \mathcal{S}} E[X_S^2] + \sum_{S_1, S_2 \in \mathcal{S}} E[X_{S_1} X_{S_2}]$$

$$\geq \sum_{S \in \mathcal{S}} E[X_S^2] + \sum_{S_1 \neq S_2} E[X_{S_1}] E[X_{S_2}]$$

There are $\binom{n}{4}\binom{n}{4}$ total pairs.

How many are "not" independent? $S_1 \sim S_2$ if they share at least one edge. But number of pairs is $O(n^7)$ while number of independent pairs is $\Omega(n^8)$ which is close to all pairs. So $\mathrm{Var}(X)$ still behaves as if ~~not~~ all pairs are indep and one can show that $p = c_2 n^{-2/3}$ for sufficiently large constant ensures $G(n,p)$ has a 4-clique with prob ≥ 0.1.

Concentration plus Union Bound

We saw several examples of using concentration bounds plus union bound. The general strategy is to show that for some events

$A_1, A_2, \ldots, A_n$

$\Pr[A_i] < \frac{1}{n}$ here A_i is a "bad" event

Then by the union bound

$$\Pr[A_1 \text{ or } A_2 \ldots \text{ or } A_n] < n \cdot \frac{1}{n} < 1.$$

$$\Rightarrow \Pr[\bar{A}_1 \wedge \bar{A}_2 \ldots \wedge \bar{A}_n] > 0$$

Thus we have all good events happening with non-zero probability and if we can express the property we want in those terms then we are done.

Ex: Routing paths.

We saw that we can convert fractional solution to integral solution by randomized rounding. We get $O\left(\frac{\log n}{\log\log n}\right)$ congestion by using Chernoff bounds on a ~~to~~ single edge and then union bound over all edges.

Local Phenomena

There are many situations where we cannot use union bound because the individual bad event probability is not that small.

If A_i are independent this does not matter because we have

$$Pr[\bar{A}_1 \cap \bar{A}_2 \ldots \cap \bar{A}_n]$$
$$= \prod (1 - Pr[A_i])$$

and hence all we need is for $Pr[A_i] < 1$.

However independence is rarely possible in complex events.

LLL considers a "local" setting where the events $A_1, \dots, A_n$ are not completely independent but there is some limited dependence. How can one capture such a scenario? For that we use a dependency graph on the events. The vertices are the events and we have ~~an~~ an edge (A_i, A_j) if A_i and A_j are dependent. No edge means that A_i and A_j are conditionally independent. That is, $\Pr[A_i \mid A_j] = \Pr[A_i]$. Note that A_i is conditionally independent of <u>all</u> <u>events</u> that it has no edges to. We define it formally.

<u>Defn</u>: An event A is conditionally independent wrt to $B_1, B_2, \ldots, B_\ell$ if $\forall S \subseteq \{1, 2, \ldots, \ell\}$

$$\Pr\left[A \,\middle|\, \bigcap_{i \in S} B_i\right] = \Pr[A].$$

When can we easily identify conditional independence?

<u>Claim</u>: Suppose $X_1, X_2, \ldots, X_\ell$ are <u>independent</u> random variables. Suppose each event A_i is completely determined by a subset $S_i \subseteq \{X_1, \ldots, X_\ell\}$. If $S_i \cap S_j = \emptyset$ for $j = j_1, j_2, \ldots, j_k$ then A_i is mutually independent of $\{A_{j_1}, \ldots, A_{j_k}\}$.

With this in place we state the symmetric version of the LLL.

<u>Theorem</u> [Symmetric LLL]
Suppose $A_1, A_2, \dots, A_n$ are events in an underlying probability space and let d be the max degree of the dependency graph and $\Pr[A_i] \leq p \ \forall i$. Then if

(i) If $pd \leq \frac{1}{4}$ then $\Pr[\bigcap_{i=1}^{n} \bar{A}_i] \geq (1-2p)^n > 0$

(ii) $p(d+1) \leq \frac{1}{e}$ then

$$\Pr[\bigcap_i \bar{A}_i] > \left(1 - \frac{1}{d+1}\right)^n > 0.$$

A more general version of the LLL called asymmetric or lop-sided LLL is the following.

<u>Theorem</u> [LLL]

Suppose $A_1, \ldots, A_n$ are events in a probability space and let G be the dependency graph. Suppose there exist numbers $x_1, x_2, \ldots, x_n \in (0,1)$ such that

$$\Pr[A_i] \leq x_i \prod_{j \in N(i)} (1 - x_j).$$

Then

$$\Pr\left[\bigwedge \bar{A}_i\right] > \prod_{i=1}^{n} (1 - x_i)$$

Here $N(i)$ is dependent neighbors of A_i.

Proof of symmetric version

The heart of the proof is the following lemma.

Lemma: For any $S \subset \{1, 2, \dots, n\}$ and $i \notin S$

$$\Pr\left[A_i \mid \bigcap_{j \in S} \bar{A}_j\right] \leq 2p.$$

Assuming lemma above the symmetric LLL (i) follows as below

$$\Pr\left[\bigcap_{i=1}^{n} \bar{A}_i\right] = \Pr[\bar{A}_1] \cdot \Pr[\bar{A}_2 \mid \bar{A}_1] \cdot \Pr[\bar{A}_3 \mid \bar{A}_1, \bar{A}_2] \cdots \Pr[\bar{A}_n \mid \bar{A}_1, \dots \bar{A}_{n-1}]$$

$$= (1 - \Pr[A_1]) \cdot (1 - \Pr[A_2 \mid \bar{A}_1]) \cdots (1 - \Pr[A_n \mid \bar{A}_1, \dots, \bar{A}_{n-1}])$$

$$\geq (1-2p)^n > 0.$$

Now we prove the lemma by induction on $|S|$.

Suppose $|S|=0$. Then

$$\Pr[A_i] \leq p \leq 2p.$$

Assume true for $|S| \leq k$.

Consider $|S| = k+1$. $i \notin S$.

Want to prove $\Pr[A_i \mid \bigcap_{j\in S} \bar{A}_j] \leq 2p$.

Let $S^{dep} = S \cap N(i)$ be the set of events in S that A_i is dependent on. $S^{ind} = S - S^{dep}$. Thus $S = S^{dep} \uplus S^{ind}$.

If $|S^{ind}| = k+1$ then $S = S^{ind}$

$$\Pr[A_i \mid \bigcap_{j\in S} \bar{A}_j] = \Pr[A_i] \leq p \leq 2p.$$

Thus we now consider

$$|S^{ind}| \le k.$$

We now use conditional probability or Bayes's theorem.

For events X, Y $\quad \Pr[X \mid Y] = \dfrac{\Pr[X \cap Y]}{\Pr[Y]}$

and for events X, Y, Z

$$\Pr[X \mid Y, Z] = \frac{\Pr[X \cap Y \mid Z]}{\Pr[Y \mid Z]}.$$

Applying with $X = A_i$

$$Y = \bigcap_{j \in S^{dep}} \bar{A}_j \quad \text{and} \quad Z = \bigcap_{j \in S^{ind}} \bar{A}_j$$

we have

$$\Pr\left[A_i \mid \bigcap_{j\in S} \bar{A}_j\right] = \frac{\Pr\left[A_i \text{ and } \bigcap_{j\in S^{dep}} \bar{A}_j \mid \bigcap_{j\in S^{ind}} \bar{A}_j\right]}{\Pr\left[\bigcap_{j\in S^{dep}} \bar{A}_j \mid \bigcap_{j\in S^{ind}} \bar{A}_j\right]}$$

Consider denominator. Via union bound

$$\Pr\left[\bigcap_{j\in S^{dep}} \bar{A}_j \mid \bigcap_{j\in S^{ind}} \bar{A}_j\right]$$

$$\geq 1 - \sum_{l\in S^{dep}} \Pr\left[A_l \mid \bigcap_{j\in S^{ind}} \bar{A}_j\right]$$

By induction hypothesis, since $|S^{ind}| \leq k$,

$$\Pr\left[A_l \mid \bigcap_{j\in S^{ind}} \bar{A}_j\right] \leq 2p.$$

and $|S^{dep}| \leq d$.

Hence

$$\Pr\left[\bigcap_{j \in S^{dep}} \bar{A}_j \,\middle|\, \bigcap_{j \in S^{ind}} \bar{A}_j\right] \geq 1 - 2pd \geq \frac{1}{2}.$$

Numerator is $\Pr\left[A_i \text{ and } \bigcap_{j \in S^{dep}} \bar{A}_j \,\middle|\, \bigcap_{j \in S^{ind}} \bar{A}_j\right]$

$$\leq \Pr\left[A_i \,\middle|\, \bigcap_{j \in S^{ind}} \bar{A}_j\right]$$

$$\leq \Pr[A_i] \leq p.$$

Hence. $\Pr\left[A_i \,\middle|\, \bigcap_{j \in S} \bar{A}_j\right] \leq \dfrac{p}{\frac{1}{2}} \leq 2p.$

$\square$.

Applications of LLL

K-Sat

Recall that a K-SAT formula is a Boolean formula in CNF form with each clause having <u>exactly</u> K literals (over distinct variables).

<u>Theorem</u>: Let Φ be a K-SAT formula in which each variable occurs in at most $\frac{2^{K-2}}{K}$ clauses. Then Φ is satisfiable.

Note that there is no limitation on number of variables or clauses!

Example: if $K=10$ then it is requiring each variable to be in at most 26 clauses.

The theorem may not be interesting from a SAT perspective but is mainly to showcase the power of LLL and a setting in which it applies.

We prove this by considering a random assignment to the variables. Let A_i be the event that a clause C_i is <u>not</u> satisfiable (bad event)

Then $Pr[A_i] \le \frac{1}{2^K}$.

What does A_i depend on?
C_i has k variables. Each variable that is in C_i is in at most $\frac{2^{k-2}}{k}$ other clauses. So C_i shares

a variable with at most $k \cdot \frac{2^{k-2}}{k} \leq 2^{k-2}$

other clauses.

If C_i and C_j do not share variables then A_i and A_j are mutually independent.

Thus we can apply symmetric LLL with $p = \frac{1}{2^k}$ and $d = 2^{k-2}$

Since $pd \leq \frac{1}{4}$.

$\Rightarrow \Pr\left[\bigcap_{i=1}^{m} \bar{A}_i\right] > 0$ where

m is # of clauses.

$\Rightarrow \Pr\{\Phi$ is satisfiable$] > 0$.

$\square$

Routing for Congestion Minimization

Recall that we saw the congestion minimization problem.

$G=(V,E)$ directed graph

$(s_1,t_1)\ \dots\ (s_k,t_k)$ k pairs

that we want to connect by paths

$P_1, P_2 \dots P_k$ s.t. we

$$\text{minimize} \max_{e\in E} \sum_{i=1}^{k} |P_i \cap e|$$

congestion on e.

We wrote an LP relaxation and found a fractional routing that minimizes max fractional congestion.

A fractional routing for a pair (s_i, t_i) is a probability distribution over paths $p \in \mathcal{P}_i$ where $\mathcal{P}_i$ is the set of all $s_i \to t_i$ paths.

We let x_p $p \in \mathcal{P}_i$ be the amount of flow routed ~~on~~ along p.

we have $\sum_{p \in \mathcal{P}_i} x_p = 1 \quad \forall i$.

Suppose $\sum_{i=1}^{k} \sum_{\substack{p \ni e \\ p \in \mathcal{P}_i}} x_p \leq 1 \quad \forall e$

ie the max fractional congestion is at most 1.

Randomized rounding picks a path

for each i independently according to the distribution x_p, $p \in P_i$.

Then we used Chernoff bounds to show that $\Pr\left[l(e) \geq c \dfrac{\log m}{\log \log m} \right] \leq \dfrac{1}{m^2}$

for some sufficiently large constant c.

Here $l(e)$ is the load on e, the # of paths that use e.

Then via the union bound we see that $\Pr\left[\max_e l(e) \geq \dfrac{c \log m}{\log \log m} \right]$

$$\leq m \cdot \frac{1}{m^2} \leq \frac{1}{m}.$$

Now we will prove a better bound when paths are short.

Suppose $x_p > 0 \Rightarrow |p| \leq h$ where h is some parameter. In many applications h is a small constant independent of m, n. This implies locality because even if the graph is large paths along which flow is routed are short.

<u>Theorem</u>: $\exists$ an integral routing where max congestion is $O\left(\frac{\log h}{\log \log h}\right)$.

Note bound does not depend on

graph & size!

In order to apply LLL we do some preprocessing. By discretization tricks we will assume that all x_p values that are non-zero have same value $\frac{1}{L}$ for some L. We may duplicate paths to achieve this. Thus each pair now has exactly L paths.

Then we do randomized rounding as before but with the discretized paths. So we pick one of the L paths for each pair.

How can we apply LLL here?

Need to set up the events carefully.

Let C be the threshold of congestion we want to avoid.

For edge let S_e be the set of all paths that use e.

Define $A_{e,S}$ for $e \in E$ $S \subseteq S_e$ and $|S| = C$ to be the event that S is the set of paths chosen.

Claim: If S contains two paths from path collection of same pair then $Pr[A_{e,S}] = 0$. Otherwise it is equal to $\frac{1}{L^C}$.

We use notation $S = \{(i_1, j_1), \ldots, (i_C, j_C)\}$ where $i_1, i_2, \ldots, i_C \in [K]$ and indicates the pair and $j_1, j_2, \ldots, j_C \in [L]$ to denote the index of the path in the L paths for pairs. (we order the paths in some fashion for each pair).

We let $P_{i,j}$ denote the jth path for pair i.

Dependencies Fix two events $A_{e,S}$ and $A_{e',S'}$ where S has paths from distinct pairs and similarly S'.

Suppose $S = \{(i_1, j_1), \ldots, (i_c, j_c)\}$

and $S' = \{(i_1', j_1'), \ldots, (i_c', j_c')\}$

If $\{i_1, i_2, \ldots, i_c\} \cap \{j_1, j_2, \ldots, j_c\} = \phi$

ie the pairs don't overlap then $A_{e,S}$ is independent of $A_{e,S'}$.

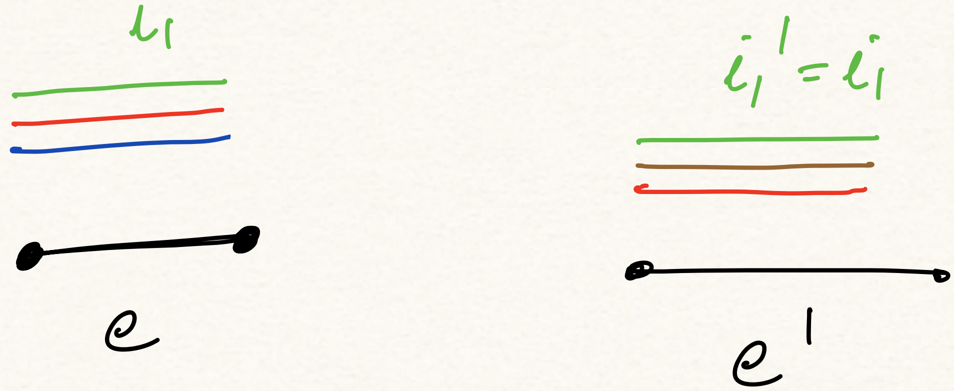
We need to understand how many other events does $A_{e,S}$ depend on.

Suppose $\{i_1, i_2, \dots, i_C\} \cap \{i_1', \dots, i_C'\} \neq \emptyset$

Say $i_1 = i_1'$.

How many choices of $i_2' \dots i_C'$ and $j_1', j_2', \dots, j_C'$ do we have.

L choices for j_1'. Fix one such choice.



Then we have path $P_{i_1', j_1'}$ (note $i_1 = i_1'$) and this paths has $\leq h$ edges.

So e' has h choices. For each such edge at most ~~we~~ L paths use the edge since total flow on each edge ≤ 1. And we can choose any $C-1$ paths from those L.

Thus for fixed choice of j_1' there are $h \cdot \binom{L}{C-1}$ choices.

Hence total is $L \cdot h \cdot \binom{L}{C-1}$.

There are C choices of pair overlap between S and S'.

Hence the neighborhood size of $A_{e,S}$ in the dependency graph is $\leq C \cdot L \cdot h \cdot \binom{L}{C-1}$.

$$\leq \frac{C \cdot h \cdot L^{C}}{(C-1)!}$$

To apply LLL we have

$$\Pr[A_{e,S}] = \frac{1}{L^{C}} = p$$

and $d \leq \dfrac{C \cdot h \cdot L^{C}}{(C-1)!}$

To ensure $pd \leq \frac{1}{4}$

we need

$$\frac{1}{L^C}\cdot\frac{C\cdot h\cdot L^C}{(C-1)!}\le\frac{1}{4}$$

$$\frac{C\,h}{(C-1)!}\le\frac{1}{4}.$$

$C=\Omega\left(\frac{\log h}{\log\log h}\right)$ suffices.

Note that if ~~not~~ no bad event $A_{e,S}$ happens then congestion is $\le C-1$.

$\square$.