Randomness in Computing

LECTURE 21

CS 537

Last time

- Probabilistic method
  - Sample and Modify
  - The Second Moment Method

Today

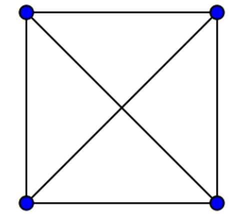
- Probabilistic method
  - Conditional Expectation Inequality
  - Lovasz Local Lemma

Last time: Threshold Behavior in $G_{n,p}$

Theorem

Let $G \sim G_{n,p}$ and $p^* = \Pr[G \text{ has a } K_4]$.

1. If $p \boxed{= \boldsymbol{o}\left(n^{-2/3}\right)}$ then $p^* \to 0$ as $n \to \infty$
2. If $p \boxed{= \boldsymbol{\omega}\left(n^{-2/3}\right)}$ then $p^* \to 1$ as $n \to \infty$



Proof: Let $X =$ number of 4-cliques in G.

For every subset C of 4 nodes, let X_C be the indicator for C being a K_4.

$$\mathbb{E}[X] = \sum_C \mathbb{E}[X_C] = \binom{n}{4} \cdot p^6$$

Conditional Expectation Inequality

Theorem

Let $X = \sum_{i\in[n]} X_i$, where each X_i is an indicator R.V. Then

$$\Pr[X > 0] \geq \sum_{i\in[n]} \frac{\Pr[X_i = 1]}{\mathbb{E}[X \mid X_i = 1]}$$

- Note that the indicators X_i need not be independent.

Proof: Let $\mathrm{Y} = \begin{cases} 1/\mathrm{X} & \text{if } X > 0; \\ 0 & \text{otherwise.} \end{cases}$ Then $\mathrm{XY} = \begin{cases} 1 & \text{if } X > 0; \\ 0 & \text{otherwise.} \end{cases}$

$$\Pr[X > 0] = \mathbb{E}[X\mathrm{Y}]$$

Conditional Expectation Inequality

CS 537

Theorem

Let $X=\sum_{i\in[n]} X_i$, where each X_i is an indicator R.V. Then

$$\Pr[X>0]\geq\sum_{i\in[n]}\frac{\Pr[X_i=1]}{\mathbb{E}[X\mid X_i=1]}$$

$$\mathrm{Y}=\begin{cases}1/\mathrm{X} & \text{if } X>0;\\ 0 & \text{otherwise.}\end{cases}$$

Proof: $\Pr[X>0]=\mathbb{E}[X\mathrm{Y}]$

Linearity of expectation

$\boldsymbol{X=\sum X_i}$

$$\overset{X=\sum X_i}{=}\mathbb{E}\left[\sum_{i\in[n]} X_i\,\mathrm{Y}\right]\overset{\text{Linearity of expectation}}{=}\sum_{i\in[n]}\mathbb{E}[X_iY]$$

Law of Total Expectation

$$\overset{\text{Law of Total Expectation}}{=}\sum_{i\in[n]}\mathbb{E}[X_iY\mid X_i=1]\cdot\Pr[X_i=1]+\sum_{i\in[n]}\underbrace{\mathbb{E}[X_iY\mid X_i=0]}_{=\,0}\cdot\Pr[X_i=0]$$

$\boldsymbol{X_i=1}$

$$=\sum_{i\in[n]}\mathbb{E}[Y\mid X_i=1]\cdot\Pr[X_i=1]\qquad=\sum_{i\in[n]}\mathbb{E}[1/X\mid X_i=1]\cdot\Pr[X_i=1]$$

$$\geq\sum_{i\in[n]}\frac{\Pr[X_i=1]}{\mathbb{E}[X\mid X_i=1]}$$

By Jensen's inequality for convex function $f(x)=1/x$,

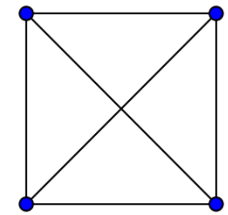
$$\mathbb{E}\left[\frac{1}{X}\right]\geq\frac{1}{\mathbb{E}[X]}$$

K_4 thm, part 2: Alternative proof

Theorem

Let $G \sim G_{n,p}$ and $p^* = \Pr[G \text{ has a } K_4]$.

2. If $p \boxed{= \omega\left(n^{-2/3}\right)}$ then $p^* \to 1$ as $n \to \infty$



Proof: Recall: X_C = the indicator for C being a K_4.

Conditional Expectation Inequality

Symmetry

$$\Pr[X > 0] \geq \sum_{C} \frac{\Pr[X_C = 1]}{\mathbb{E}[X \mid X_C = 1]} = \binom{n}{4} \frac{p^6}{\mathbb{E}[X \mid X_C = 1]}$$

$\boldsymbol{X = \sum X_{C'}}$

Linearity of expectation

$$\mathbb{E}[X \mid X_C = 1] = \mathbb{E}\Big[\sum_{C'} X_{C'} \mid X_C = 1\Big] = \sum_{C'} \mathbb{E}[X_{C'} \mid X_C = 1]$$

$X_{C'}$ is a 0-1 R.V.

$$= \sum_{C'} \Pr[X_{C'} = 1 \mid X_C = 1]$$

$\boldsymbol{C' = C}$ | $\boldsymbol{C' \cap C = \emptyset}$ | $\boldsymbol{|C' \cap C| = 1}$ | $\boldsymbol{|C' \cap C| = 2}$ | $\boldsymbol{|C' \cap C| = 3}$

$$= 1 + \binom{n-4}{4} p^6 + 4\binom{n-4}{3} p^6 + 6\binom{n-4}{2} p^5 + 4\binom{n-4}{1} p^3$$

Avoiding bad events

- Let B_1 and B_2 be (bad) events over a common probability space.

Q. If $\Pr[B_1] < 1$ and $\Pr[B_2] < 1$, does it imply $\Pr[\overline{B_1} \cap \overline{B_2}] > 0$? (Is it possible to avoid both events)?

A. **Not necessarily.** E.g., for a single coin flip, let $B_1 = H, B_2 = T$ Then $\Pr[B_1] = \Pr[B_2] = 1/2$. But $\Pr[\overline{B_1} \cap \overline{B_2}] = 0$

Q. What if B_1 and B_2 are independent?

A. **Yes.** $\Pr[\overline{B_1} \cap \overline{B_2}] = \Pr[\overline{B_1}] \cdot \Pr[\overline{B_2}] > 0$

Q. What if $\Pr[B_1] < \frac{1}{2}$ and $\Pr[B_2] < \frac{1}{2}$ (but B_1, B_2 are dependent)?

A. **Yes.** By Union Bound, $\Pr[B_1 \cup B_2] \le \Pr[B_1] + \Pr[B_2] < 1$. So, $\Pr[\overline{B_1} \cap \overline{B_2}] > 0$.

Lovasz Local Lemma (LLL)

LLL states that as long as

1. bad events $B_1, \dots, B_n$ have small probability,
2. they are not ``too dependent'',

there is a non-zero probability of avoiding all of them.

Lovasz Local Lemma (LLL)

- Event E is mutually independent from the events $E_1, \ldots, E_n$ if, for any subset $I \subseteq [n]$,

$$\Pr[E \mid \bigcap_{j \in I} E_j] = \Pr[E].$$

- A dependency graph for events $B_1, \ldots, B_n$ is a graph with vertex set $[n]$ and edge set E, s.t. $\forall i \in [n]$, event B_i is mutually independent of all events $\{B_j \mid (i,j) \notin E\}$.

Lovasz Local Lemma

Let $B_1, \ldots, B_n$ be events over a common sample space s.t.

1. max degree of the dependency graph of $B_1, \ldots, B_n$ is at most $\boldsymbol{d-1}$
2. $\forall i \in [n], \Pr[B_i] \leq \boldsymbol{p}$

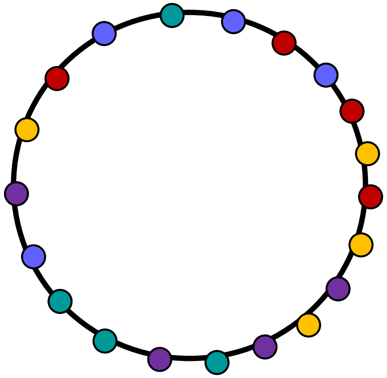
If $\boldsymbol{epd \leq 1}$ then $\Pr\left[\bigcap_{i \in [n]} \bar{B}_i\right] > 0$

Different meaning of d than in the book (to correspond to algorithmic LLL).

Example: Points on a circle

$11n$ points are placed on a circle and colored with n different colors, so that each color is applied to exactly 11 points.

Prove: There exists a set of n points, all colored differently, such that no two points in the set are adjacent.



Solution: Choose one point of each color u.i.r. from 11 points of that color.

- Bad events: B_{ij} for every adjacent pair (i, j), such that $color(i) \neq color(j)$

Application of LLL: edge-disjoint paths

- $\boldsymbol{n}$ pairs of users need to communicate using edge-disjoint paths
- $\forall i \in [n]$, pair i can choose a path from collection P_i of size $\boldsymbol{m}$.

Theorem

If $\forall i \neq j$, each path in P_i shares edges with at most $\boldsymbol{k}$ paths in P_j and $2\boldsymbol{enk} \leq \boldsymbol{m}$ then there is a way to choose $\boldsymbol{n}$ edge-disjoint paths.

Proof:

Algorithmic LLL

- Under the original distribution it is unlikely, but possible to avoid all bad events.

- Can we find a different distribution (specifically, a randomized algorithm) that is likely to avoid all bad events?

Canonical special case of LLL: *k*SAT

- Literal: a variable or its negation
- Clause: OR of literals
- CNF formula: AND of clauses
- kCNF: each clause involves k distinct variables

  E.g. $(x_1 \vee \overline{x_3} \vee x_7 \vee x_{13})$ is a 4CNF clause
- kSAT: Is a given a kCNF formula satisfiable?
- Notation: $n =$ number of variables, $m =$ number of clauses

Canonical special case of LLL: kSAT

- Literal: a variable or its negation
- Clause: OR of literals
- CNF formula: AND of clauses
- kCNF: each clause involves k distinct variables

E.g. $(x_1 \vee \overline{x_3} \vee x_7 \vee x_{13})$ is a 4CNF clause

- kSAT: Is a given a kCNF formula satisfiable?
- Notation: $n =$ number of variables, $m =$ number of clauses

Warm up: For each kCNF clause, there are $\boxed{?}$ possible assignments.

- Only one of them violates the clause. E.g. $\boxed{\boldsymbol{x_1 = 0, x_3 = 1, x_7 = 0, x_{13} = 0}}$
- The remaining $2^k - 1$ satisfy it.

Each clause ``forbids'' one particular assignment to a k-tuple of variables.

Recall from HW: A uniformly random assignment satisfies, in expectation, $m(1 - 2^{-k})$ clauses.

HW: show how to find such an assignment deterministically.

Canonical special case of LLL: *k*SAT

- Notation: n = number of variables, m = number of clauses

Observation: If $m < 2^k$, then the formula is satisfiable.

Proof:

- Pick a uniformly random assignment.
- Let B_i be the event that clause i is violated.