Class 11

Practice with LLL

Quick Recap
derandomization via conditional expectation

- Probabilistic method:
  - Let $G = (V, E)$ be a graph.
  - Let X be the number of edges that cross a random cut $(S, \bar{S})$
  - $\mathbb{E}[\mathrm{X}] = |E|/2$
  - There is a cut with more than |E|/2 edges crossing it!

Quick Recap
derandomization via conditional expectation

- Probabilistic method:
  - Let $G = (V, E)$ be a graph.
  - Let X be the number of edges that cross a random cut $(S, \bar{S})$
  - $\mathbb{E}[X] = |E|/2$
  - There is a cut with more than |E|/2 edges crossing it!

- How do we find it?
  - First choose whether $v_1 \in S$ or not.
  - Choose it so that $\mathbb{E}[X \mid \text{choice for } v_1] \geq |E|/2$
  - Iterate!

Quick Recap
derandomization via conditional expectation

- Suppose you know that $\mathbf{E}[\text{something}]$ is good

- Suppose you can build [something] one choice at a time

- Then assuming that

$$\mathbf{E}[\text{something} \mid \text{choices } 1,2 \ \ldots, t-1\,] \text{ is good,}$$

  there is a way to make t^th^ choice so that

$$\mathbf{E}[\text{something} \mid \text{choices } 1,2 \ \ldots, t\,] \text{ is good.}$$

- If you can find that way to make the t^{th} choice efficiently, you have an algorithm!

Another example if you want more practice

(check out agenda from Class 10)

$$\varphi = (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_2 \vee \overline{x_4} \vee x_1) \wedge \cdots$$

- Say φ is a 3-CNF formula with n variables and m clauses, and 3 distinct variables in each clause.
- Show how to (efficiently) find a satisfying assignment so that at least 7/8 of the clauses are satisfied.

If you finish today's material early, try this

Recap: 2nd moment method and LLL

- Second Moment Method

$$\mathbb{P}[X=0] \leqslant \frac{\mathrm{Var}(X)}{(\mathbb{E}X)^2}$$

- Lovasz Local Lemma (LLL)

Say that $A_1, A_2, \ldots, A_m$ are BAD EVENTS so that:

- $\mathbb{P}[A_i] \leq p \quad \forall i$
- For each A_i, there is a set $S_i \subseteq [m]$ so that A_i is mutually indep. from $\{A_r : r \notin S_i\}$ and $|S_i| \leq d$
- $4pd \leq 1$ OR $ep(d+1) \leq 1$

Then

$$\mathbb{P}\left[\bigcap_i \bar{A_i}\right] > 0.$$

Questions?

2^{nd} MM, LLL, Quiz, …?

Q1: n'th moment method

Let X be a real-valued random variable. Which of the following is always true? Check all that apply.

- [x] $\Pr[X=0] \le \frac{\mathbb{E}[(X-\mathbb{E}[X])^2]}{(\mathbb{E}[X])^2}$
- [ ] $\Pr[X=0] \le \frac{\mathbb{E}[(X-\mathbb{E}[X])^3]}{(\mathbb{E}[X])^3}$ ← the RHS could be negative, eg $X = \begin{cases} +1 & \text{pr } 3/4 \\ -1 & \text{pr } 1/4 \end{cases}$
- [x] $\Pr[X=0] \le \frac{\mathbb{E}[(X-\mathbb{E}[X])^4]}{(\mathbb{E}[X])^4}$

Q2: Applying the 2nd moment method

Suppose that $X_1, \ldots, X_n$ are independent random variables so that for all i, X_i is $+1$ with probability $1/4$ and -1 with probability $3/4$. Let $X = \sum_{i=1}^{n} X_i$. What does the second-moment method say about X?

$\Pr[X = 0] \leq$ ________

- ○ $\frac{1}{4n}$
- ◉ $\frac{3}{n}$
- ○ $\frac{4}{n^2}$
- ○ $\frac{1}{4n^2}$

$\mathbb{E}[X_i^2] = 1$

$\mathbb{E}[X_i] = -1/2$

$Var(X) = \sum_{i=1}^{n} Var(X_i)$

$= n \cdot \left[\mathbb{E}[X_1^2] - \mathbb{E}[X_1]^2 \right]$

$= n\left[1 - 1/4 \right] = \frac{3n}{4}$

$\mathbb{P}[X=0] \leq \frac{Var[X]}{(\mathbb{E}X)^2} = \frac{3n/4}{n^2/4} = \frac{3}{n}$

Q3:

- Color edges of K_n blue or red
- A_S is the event that clique formed by S is monochromatic, for |S|=4.
- WTS $\Pr[\cap_S \overline{A_S}] \geq$ ____

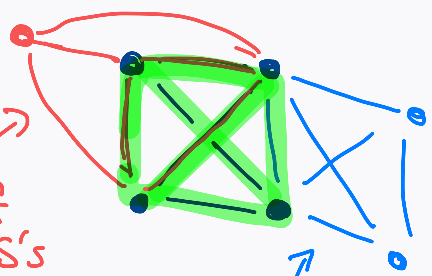
What is the smallest you can take the parameter "p" to be in the LLL?

- ○ 1/2
- ○ 1/8
- ◉ **1/32**
- ○ $(1/e)^6$

$$\mathbb{P}[\text{monochromatic}] = \frac{2 \text{ options}}{2^6 \text{ options}} = 1/32$$

What is the smallest that you can take the parameter "d" to be in the LLL, for large n?

- ○ $\Theta(n)$
- ◉ $\Theta(n^2)$
- ○ $\Theta(n^3)$
- ○ $\Theta(n^6)$



Q3:

- Color edges of K_n blue or red
- A_S is the event that clique formed by S is monochromatic, for |S|=4.
- WTS $\Pr[\cap_S \overline{A_S}] \geq$ ____

$\mathbb{P}[\cap_S \bar{A}_S] > 0$

$\Rightarrow \exists$ coloring w/ no monochromatic K_4 in K_n
for $n \leq n_0$

If $R_4 < n_0$, then there MUST be a monochromatic K_4 in K_{n_0} ...

so $R_4 \geq n_0$

Q3.3

2 Points

Suppose that you got a statement of the form $\Pr[\bigcap_S \overline{A_S}] > 0$, under the assumption that $n \leq n_0$ for some constant n_0.

What would this statement imply for R_4, the fourth Ramsey number?

- (◉) It would give a lower bound on R_4.
- ( ) It would give an upper bound on R_4.
- ( ) It would not directly imply anything about R_4.

Plan for today

- More practice with LLL
    - Application to k-SAT
    - (Closure on the example set up in the minilecture video!)
- Yet more practice with the LLL
    - An example where the “mutually independent” definition is a bit more tricky!
- (If there’s extra time we can go back to derandomization via conditional expectation)

Recall k-SAT

$$\varphi = (x_1 \vee \overline{x_2} \vee x_3) \wedge (x_2 \vee \overline{x_4} \vee x_1) \wedge \cdots$$

- n variables, m clauses.
- For today, each clause has exactly k distinct variables.
- Goal: a statement of the form:

As long as each variable appears in no more than ______ clauses, then φ is satisfiable.

Let's practice the LLL!

Group Work

Suppose that each variable x_i is in at most t clauses, for some parameter t that will depend on k and that you'll work out in this problem. Apply the LLL to get a statement like the following:

Suppose that each variable is in at most t clauses of φ. Then φ is satisfiable.

- n variables, m clauses.
- For today, each clause has exactly k distinct variables.

Solutions

Suppose each variable is in $\leq$ ________________ clauses of φ.

Then φ is satisfiable.

Solutions

<u>Thm</u> Say each clause has EXACTLY k literals, and each variable appears in $\leq \underbrace{2^{k-2}/k}_{\text{this is our } t}$ clauses

Then φ is satisfiable.

Setting up the LLL

- What are the A_i?

- What is "p"?

Setting up the LLL

- What are the A_i?

A_i = event that clause i is unsatisfied

- What is "p"?

$\mathbb{P}[A_i] = \frac{1}{2^k}$, so $p \leftarrow 1/2^k$

$A_i = \{ i^{th} \text{ clause NOT satisfied} \}$

What is the parameter "d"?

$A_i = \{ i^{th} \text{ clause NOT satisfied} \}$

What is the parameter "d"?

Fix $i \in [m]$

Let $S_i \subseteq [m]$ be the set of j s.t. clause j and clause i share some variable.

$|S_i| \leq k \cdot t$

\# variables in clause i

bound on \# other clauses that that var. could be in.

$d \leftarrow kt$

Applying the LLL

Applying the LLL

We need $d \cdot p \leq 1/4$

$$kt \cdot \frac{1}{2^k} \leq 1/4$$

$$t \leq \frac{2^{k-2}}{k}$$

Conclusion

<u>Thm</u> Say each clause has EXACTLY k literals, and each variable appears in $\leq \underbrace{2^{k-2}/k}_{\text{this is our } t}$ clauses

Then φ is satisfiable.

Conclusion

Thm Say each clause has EXACTLY k literals,
and each variable appears in $\leq \underbrace{2^{k-2}/k}_{\text{this is our } t}$ clauses
Then φ is satisfiable.

- For example, if $k = 10$, then as long as each variable appears in at most $\frac{2^8}{10} = 25.6$ clauses (aka, in ≤ 25 clauses), then φ is ALWAYS satisfiable!!
  - No matter how many variables or how many clauses!

Next up…

sometimes computing "d" isn't so obvious

- Consider a set of m equations in n variables $x_1, \ldots, x_n$:

$$\sum_{j=1}^{n} a_j^{(1)} x_j \equiv b^{(1)} \mod 17$$

$$\sum_{j=1}^{n} a_j^{(2)} x_j \equiv b^{(2)} \mod 17$$

$$\vdots$$

$$\sum_{j=1}^{n} a_j^{(m)} x_j \equiv b^{(m)} \mod 17$$

(also assume that there's at least one nonzero term in each eqn.

$a_j^{(i)} \in \{0, 1, \ldots, 16\}$

$b^{(i)} \in \{0, 1, \ldots, 16\}$

Assume that each variable x_j appears in ≤ 4 equations.

(aka, $a_j^{(i)} = 0$ for all but 4 values of i)

Group Work

With the setup above, prove that there exists an assignment to the variables such that *none* of the equations are satisfied.

Hint: *Recall that because 17 is prime, for any* $a \in \{1, \ldots, 16\}$ *and any* $b \in \{0, \ldots, 16\}$*, the equation* $ax \equiv b \bmod 17$ *has a unique solution for* $x \in \{0, \ldots, 16\}$.

Hint: *It might be helpful to go back to the definition of mutual independence when arguing about the value of* d *when applying the LLL.*

Definition 1. *Given events* B *and* $B_1, \ldots, B_k$ *defined over some probability space,* B *is* mutually independent *of events* $\{B_1, \ldots, B_k\}$ *if the probability of* B *does not change if we condition on* any *subset of* $B_1, \ldots, B_k$*. Formally, for any subset* $J \subseteq \{1, \ldots, k\}$,

$$\Pr[B] = \Pr[B | \cap_{i \in J} B_i].$$

Setting up the LLL

- What are the A_i?

- What is "p"?

$$\sum_{j=1}^{n} a_j^{(1)} x_j \equiv b^{(1)} \mod 17$$
$$\sum_{j=1}^{n} a_j^{(2)} x_j \equiv b^{(2)} \mod 17$$
$$\vdots$$
$$\sum_{j=1}^{n} a_j^{(m)} x_j \equiv b^{(m)} \mod 17$$

Setting up the LLL

- What are the A_i?

A_i = event that eqn i is satisfied

- What is "p"?

$$\mathbb{P}[A_i] = \mathbb{P}\left[\sum_{j=1}^{n} a_j^{(i)} x_j \equiv b^{(i)} \mod 17\right]$$

$$= 1/17$$

To see this, say WLOG $a_1^{(i)} \neq 0$. Condition on $x_2, \ldots, x_n$

$$\mathbb{P}\left[a_1^{(i)} \cdot x_1 \equiv b^{(i)} - \sum_{j=2}^{n} a_j^{(i)} x_j \;\middle|\; x_2, \ldots, x_n\right] = 1/17.$$

$$\sum_{j=1}^{n} a_j^{(1)} x_j \equiv b^{(1)} \mod 17$$

$$\sum_{j=1}^{n} a_j^{(2)} x_j \equiv b^{(2)} \mod 17$$

$$\vdots$$

$$\sum_{j=1}^{n} a_j^{(m)} x_j \equiv b^{(m)} \mod 17$$

A_i is the event that equation i is satisfied

What is the parameter "d"?

$$\sum_{j=1}^{n} a_j^{(1)} x_j \equiv b^{(1)} \mod 17$$

$$\sum_{j=1}^{n} a_j^{(2)} x_j \equiv b^{(2)} \mod 17$$

$$\vdots$$

$$\sum_{j=1}^{n} a_j^{(m)} x_j \equiv b^{(m)} \mod 17$$

Definition 1. *Given events B and $B_1, \ldots, B_k$ defined over some probability space, B is* mutually independent *of events $\{B_1, \ldots, B_k\}$ if the probability of B does not change if we condition on* any *subset of $B_1, \ldots, B_k$. Formally, for any subset $J \subseteq \{1, \ldots, k\}$,*

$$\Pr[B] = \Pr[B | \cap_{i \in J} B_i].$$

A_i is the event that equation i is satisfied

What is the parameter "d"?

First try: $d \leq 4 \cdot n$? ($\leq n$ vars per eqn, ≤ 4 other eqns per variable).

That's no good! We'd need:

$$dp \leq 1/4$$

$$(4n)\left(\frac{1}{17}\right) \leq \frac{1}{4}$$

$$n \leq 17/16 \ \ldots$$

Definition 1. *Given events B and $B_1, \ldots, B_k$ defined over some probability space, B is* mutually independent *of events $\{B_1, \ldots, B_k\}$ if the probability of B does not change if we condition on* any *subset of $B_1, \ldots, B_k$. Formally, for any subset $J \subseteq \{1, \ldots, k\}$,*

$$\Pr[B] = \Pr[B | \cap_{i \in J} B_i].$$

$$\sum_{j=1}^{n} a_j^{(1)} x_j \equiv b^{(1)} \mod 17$$
$$\sum_{j=1}^{n} a_j^{(2)} x_j \equiv b^{(2)} \mod 17$$
$$\vdots$$
$$\sum_{j=1}^{n} a_j^{(m)} x_j \equiv b^{(m)} \mod 17$$

A_i is the event that equation i is satisfied

What is the parameter "d"?

Next try: actually we can take $d = 4$.

Say WLOG $a_1^{(i)} \neq 0$, let $S_i = \{j$ s.t. x_j appears in eqn. $j\}$

Let $J \subseteq [m] \setminus S_i$.

Conditioning on $\bigcap_{j \in J} A_j$ doesn't say anything about x_1.

Thus $\mathbb{P}[A_i \mid \bigcap_{j \in J} A_j] = \frac{1}{17} = \mathbb{P}[A_i]$

by same argument as above.

Definition 1. *Given events* B *and* $B_1, \ldots, B_k$ *defined over some probability space,* B *is* mutually independent *of events* $\{B_1, \ldots, B_k\}$ *if the probability of* B *does not change if we condition on* any *subset of* $B_1, \ldots, B_k$. *Formally, for any subset* $J \subseteq \{1, \ldots, k\}$,

$$\Pr[B] = \Pr[B \mid \cap_{i \in J} B_i].$$

$$\sum_{j=1}^{n} a_j^{(1)} x_j \equiv b^{(1)} \mod 17$$
$$\sum_{j=1}^{n} a_j^{(2)} x_j \equiv b^{(2)} \mod 17$$
$$\vdots$$
$$\sum_{j=1}^{n} a_j^{(m)} x_j \equiv b^{(m)} \mod 17$$

$p \leftarrow 1/17 \quad , \quad d \leftarrow 4$

$p \cdot d = \frac{4}{17} < \frac{1}{4}$ ✓

Conclusion

- There exists an assignment so that **none** of these are satisfied!

each x_j
appears in ≤ 4 eqns.

$$\sum_{j=1}^{n} a_j^{(1)} x_j \equiv b^{(1)} \mod 17$$

$$\sum_{j=1}^{n} a_j^{(2)} x_j \equiv b^{(2)} \mod 17$$

$$\vdots$$

$$\sum_{j=1}^{n} a_j^{(m)} x_j \equiv b^{(m)} \mod 17$$

Recap

- More practice with the LLL!
  - We saw how the LLL applies to k-SAT – this will come up again in the minilectures for next time on the Algorithmic LLL.
  - The definition of "mutually independent" can be a bit subtle.

If there's more time...

- Derandomization via conditional expectation!

1. Let φ be a 3-CNF formula with n variables and m clauses, and 3 distinct variables in each clause. Use the method of derandomization via conditional expectation to give an efficient (polynomial in n, m) deterministic algorithm to find an assignment to φ so that at least a 7/8-fraction of the clauses are satisfied.

Recall that the expected number of clauses satisfied by a random assignment is $\frac{7}{8} \cdot m$

General strategy

Choose values (TRUE/FALSE) for $x_1, x_2, x_3, \dots, x_n$ one at a time.

At each step, make sure that $\mathbb{E}\left[\text{\# Sat. clauses} \;\middle|\; \text{choices for } x_1, \dots, x_t\right] \geq \frac{7m}{8}$

Why can we make a good choice?

Why can we make a good choice?

Induction!

let X = #SAT clauses

Base case: $\mathbb{E}[X \mid \text{(nothing)}] = \frac{7m}{8}$

by induction

$t \geq 1$: $\frac{7m}{8} \leq \mathbb{E}\left[X \,\middle|\, \begin{array}{l}\text{choices for}\\ x_1, \ldots, x_{t-1}\end{array}\right]$

$= \frac{1}{2}\mathbb{E}\left[X \,\middle|\, \begin{array}{l}\text{choices for}\\ x_1, \ldots, x_{t-1}\end{array}, x_t = \text{TRUE}\right] + \frac{1}{2}\mathbb{E}\left[X \,\middle|\, \begin{array}{l}\text{choices for}\\ x_1, \ldots, x_{t-1}\end{array}, x_t = \text{FALSE}\right]$

$\Rightarrow$ at least one of these is $\geq 7m/8$

How do we make this choice efficiently?

Want to know when this is larger than $\frac{7m}{8}$

$$\mathbb{E}\left[\begin{matrix}\#\text{sat}\\ \text{clauses}\end{matrix} \,\middle|\, \begin{matrix}\text{choices for}\\ x_1,\dots,x_{t-1}\end{matrix}, x_t = \text{TRUE}\right]$$

How do we make this choice efficiently?

Want to know when this is larger than $\frac{7m}{8}$

$$\mathbb{E}\left[\begin{array}{c}\#\text{sat.}\\ \text{clauses}\end{array} \,\middle|\, \begin{array}{c}\text{choices for}\\ x_1, \ldots, x_{t-1}\end{array}, x_t = \text{TRUE}\right] = \sum_{\text{clauses } C} \mathbb{P}\left\{ C = \text{TRUE} \,\middle|\, \begin{array}{c}\text{choices for}\\ x_1, \ldots, x_{t-1}\end{array}, x_t = \text{TRUE}\right\}$$

How do we make this choice efficiently?

Want to know when this is larger than $\frac{7m}{8}$

$$\mathbb{E}\left[\#\text{sat. clauses} \;\middle|\; \text{choices for } x_1, \ldots, x_{t-1},\; x_t = \text{TRUE} \right] = \sum_{\text{clauses } C} \underbrace{\mathbb{P}\left\{ C = \text{TRUE} \;\middle|\; \text{choices for } x_1, \ldots, x_{t-1},\; x_t = \text{TRUE} \right\}}$$

This is 1 if the choices have already made C true.

Otherwise it's $1 - 1/2^k$, where $k \in \{0,1,2,3\}$ is the # of free variables left in C.

How do we make this choice efficiently?

Want to know when this is larger than $\frac{7m}{8}$

$$\mathbb{E}\left[\begin{matrix}\#\text{sat.}\\ \text{clauses}\end{matrix} \;\middle|\; \begin{matrix}\text{choices for}\\ x_1, \ldots, x_{t-1}\end{matrix}, \; x_t = \text{TRUE} \right] = \sum_{\text{clauses } C} \underbrace{\mathbb{P}\left\{ C = \text{TRUE} \;\middle|\; \begin{matrix}\text{choices for}\\ x_1, \ldots, x_{t-1}\end{matrix}, \; x_t = \text{TRUE} \right\}}$$

This is 1 if the choices have already made C true.
Otherwise it's $1 - 1/2^k$, where $k \in \{0,1,2,3\}$ is the # of free variables left in C.

In particular, we can compute this efficiently.

Time $O(m)$!