Class 11

Practice with LLL

Warm-Up

- In class, we said that the ”second moment method” was:

$$\text{For any real-valued } X,\ \Pr[X = 0] \leq \frac{\mathrm{Var}(X)}{(\mathbb{E}[X])^2}$$

- Another version is:

$$\text{For any non-negative } X,\ \Pr[X > 0] \geq \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]}$$

- Are these comparable? If so, which is stronger?

Announcements

- HW4 due Friday!
- HW5 out now!
  - Due 2/28
- No class Monday!
  - Happy President’s day!

Recap: 2nd moment method and LLL

- Second Moment Method

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

- Lovasz Local Lemma (LLL)

Let $A_1, \ldots, A_m$ be "bad" events, so that for all i:

- $\Pr[A_i] \leq p$
- A_i is mutually independent of all but d other events.

If $\left\{\begin{array}{c} p(d+1) \leq \frac{1}{e} \\ -\text{or}- \\ pd \leq \frac{1}{4} \end{array}\right\}$, then $\Pr[\text{No } A_i \text{ occurs}] > 0$.

Questions?

2nd MM, LLL, Quiz, …?

Warm-Up

- In class, we said that the ”second moment method” was:

$$\text{For any real-valued } X,\ \Pr[X = 0] \leq \frac{\mathrm{Var}(X)}{(\mathbb{E}[X])^2}$$

- Another version is:

$$\text{For any non-negative } X,\ \Pr[X > 0] \geq \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]}$$

- Are these comparable? If so, which is stronger?

For $X \geq 0$, the second implies the first: $\Pr[X = 0] \leq \frac{\mathbb{E}[X^2] - (\mathbb{E}[X])^2}{\mathbb{E}[X^2]} = \frac{\mathrm{Var}(X)}{\mathbb{E}[X^2]} \leq \frac{\mathrm{Var}(X)}{(\mathbb{E}[X])^2}$

But the first one works for any real-valued X, not just $X \geq 0$.

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 time) Practice with Second Moment Method

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

Let φ be a k-CNF formula, so that each clause has k distinct variables in it. 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.

(You should try to get t to be as large as possible. It's not hard to see that the statement above is true if, say, $t = 1$, but you should get a value of t that grows with k.)

LLL:

- Let $A_1, \ldots, A_m$ be "bad" events, so that for all i:
  - $\Pr[A_i] \leq p$
  - A_i is mutually independent of all but d other events.
- If $pd \leq \frac{1}{4}$, then $\Pr[\text{No } A_i \text{ occurs}] > 0$.

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

Solutions

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

$2^{k-2}/k$

For some constant C…

(a) $C \cdot 2^k$ (b) $C \cdot \frac{2^k}{k}$ (c) $C \cdot k^4$ (d) C

- 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!

Solutions: Setting up the LLL

- What are the A_i? A_i is the event that clause i is unsatisfied.
- What is "p"? $p = \frac{1}{2^k}$
- What is "d"? $d = kt$

A_i is mutually independent with
$S_i = \{A_j : \text{clause j and clause i don't share any variables}\}$
The number of A_ℓ not in S_i is:
- (k variables in clause i) × (t other clauses that variable could be in)

- What do we need?

$$dp \leq \frac{1}{4} \quad \Rightarrow kt2^{-k} \leq \frac{1}{4} \quad \Rightarrow t \leq \frac{2^{k-2}}{k}$$

Next up…

sometimes computing “d” isn’t so obvious

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

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

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

$$\vdots$$

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

Suppose that each x_j appears in at most 4 equations

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 $ax \equiv b \mod 17$ 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?

A_i is the event that equation i is satisfied.

- What is "p"? $p = \frac{1}{17}$.

e.g., say the first equation is:

$3x_1 +$ Ignore this stuff for a second

This is uniformly random in {0,1,…,16}

(no matter what this stuff is)

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

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

$$\vdots$$

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

A_i is the event that equation i is satisfied

What is the parameter "d"?

Try 1: $d \leq 4 \cdot n$

Each eqn has at most n variables, which appear in at most 4 other eqns.

Then we'd need $pd \leq \frac{1}{4}$ aka $\frac{4n}{17} \leq \frac{1}{4}$... ☹

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

Mutual Independence from all but S: $\Pr[A \mid \bigcap_{j \in J} B_j] = \Pr[A]$ for all $J \subseteq [m] \setminus S$

A_i is the event that equation i is satisfied

What is the parameter "d"?

Try 2: $d = 3$ This is what we need for $pd \leq \frac{1}{4}$, so let's go for it!

Fix some equation $\sum_{j=1}^{n} a_j^{(r)} x_j \equiv b^{(r)} \bmod 17$. Suppose $a_{j^*}^{(r)} \neq 0$.

Let $S = \{\, \ell \in [m] : x_{j^*} \text{ doesn't appear in eqn } \ell \,\}$ Note $|S| \leq 3$

For any $J \subseteq [m] \setminus S$, consider $\Pr[A_r \mid \cap_{\ell \in J} A_\ell] = \frac{1}{17} = \Pr[A_r]$

$a_{j^*}^{(r)} x_{j^*}$ + Ignore this stuff for a second

This is independent of $\cap_{\ell \in J} A_\ell$!

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

Mutual Independence from all but S: $\Pr[\, A \mid \cap_{j \in J} B_j] = \Pr[A]$ for all $J \subseteq [m] \setminus S$

Conclusion

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

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

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

$$\vdots$$

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

A_i is the event that Eqn i is satisfied.

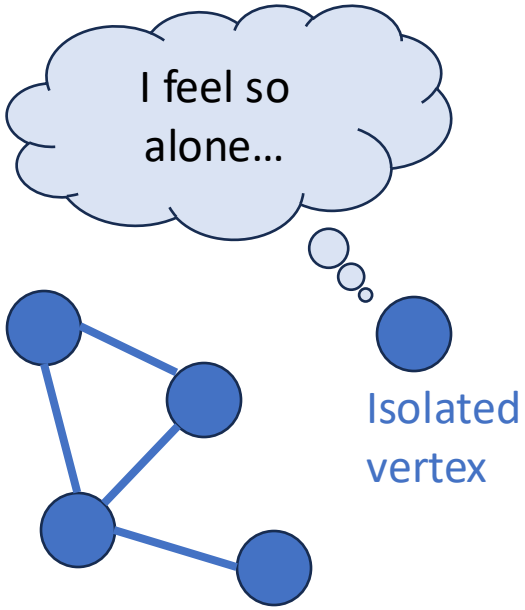
$$\Pr[\, A_i \,] \leq \frac{1}{17} =: p$$

$$d = 3$$

Need $pd \leq \frac{1}{4}$ aka $\frac{3}{17} \leq \frac{1}{4}$ which is **TRUE!**

If time… Back to Second Moment Method!

- Consider $G(n,p)$ for $p = \frac{c \ln n}{n}$ for some $c \in (0,1)$
  - Graph on n vertices
  - Each edge present independently with probability p



- Use the second moment method to show

$$\Pr[\text{ there is an isolated vertex }] = 1 - o(1)$$

- For any real-valued X, $\Pr[X = 0] \leq \frac{\mathrm{Var}(X)}{(\mathbb{E}[X])^2}$
- For any non-negative X, $\Pr[X > 0] \geq \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]}$

Either will work here

Feel free to use $e^x \approx 1 - x$ with abandon, and be fast and loose with the $o(1)$ terms…

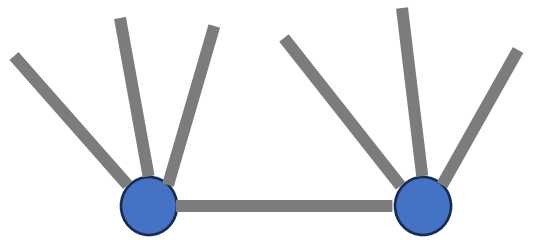
Solutions

$$p = \frac{c \ln n}{n}$$

- $X =$ number of isolated vertices $= \sum_{v \in V} 1[\ v$ is isolated $]$
- $\mathbb{E}X = \sum_{v \in V} \Pr[v \text{ is isolated }] = n(1-p)^{n-1} \approx n \exp(-pn) = n^{1-c}$

- $\mathbb{E}[X^2] = \sum_{v \in V} \Pr[v \text{ is isolated }] + \sum_{v \neq u} \Pr[\text{ both } v, u \text{ are isolated }]$

$\approx n^{1-c}$ $\quad = n(n-1)(1-p)^{2n-1}$



$2n - 1$ edges that need to not exist

Solutions

$$p = \frac{c \ln n}{n}$$

- $X =$ number of isolated vertices $= \sum_{v \in V} 1[\ v$ is isolated $]$
- $\mathbb{E}X = \sum_{v \in V} \Pr[v \text{ is isolated }] = n(1-p)^{n-1} \approx n \exp(-pn) = n^{1-c}$

- $\mathbb{E}[X^2] = \sum_{v \in V} \Pr[v \text{ is isolated }] + \sum_{v \neq u} \Pr[\text{ both } v, u \text{ are isolated }]$

$\approx n^{1-c}$

$= n(n-1)(1-p)^{2n-1}$

$\approx n^2 \exp(-2pn)$

$= n^{2(1-c)}$

Solutions

$$p = \frac{c \ln n}{n}$$

- X = number of isolated vertices $= \sum_{v \in V} 1[\, v \text{ is isolated }]$
- $\mathbb{E}X = \sum_{v \in V} \Pr[v \text{ is isolated }] = n(1-p)^{n-1} \approx n \exp(-pn) = n^{1-c}$

- $\mathbb{E}[X^2] = \sum_{v \in V} \Pr[v \text{ is isolated }] + \sum_{v \neq u} \Pr[\text{ both } v, u \text{ are isolated }]$

$$\approx n^{1-c} + n^{2(1-c)}$$

This is SUPER sloppy! (but it turns out to be okay). For a fun exercise, be less sloppy!

$$\Pr[\, X > 0] \geq \frac{n^{2(1-c)}}{n^{1-c} + n^{2(1-c)}} \quad \to 1 \text{ as } n \to \infty$$

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 time, more practice with 2^{nd} moment method!
  - Computing variances is fun!

Next time

- Have a nice long weekend!
- On **Wednesday** we'll make the LLL algorithmic!