CS265, Winter 2026

Class 10: Agenda and Questions

1 Announcements

- Midterm on Wednesday!
- No class the Monday after that (Presidents' Day)
- HW5 will be due Friday 2/20.

2 Warm-Up

Group Work

In class, we said that the "second moment method" was to using the fact that

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

for all real-valued random variables X. There's another version that says that for any non-negative random variable X,

$$\Pr[X > 0] \geq \frac{(\mathbb{E}X)^2}{\mathbb{E}[X^2]}.$$

Is one of these stronger than the other? Are they incomparable?

Bonus question: prove this second version!

3 Recap/Questions?

Any questions from the minilectures and/or the quiz (second moment method and LLL)?

4 Practice with the LLL

Recall the *k-SAT* problem. There are n variables $x_1, \ldots, x_n$. We consider clauses that looks like $(x_{i_1} \vee x_{i_2} \vee \overline{x_{i_3}} \vee \cdots \vee x_{i_k})$; that is, a clause is the OR of k literals.

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.)

4.1 More Practice with LLL and Mutual Independence

Here's an example where the mutual independence requirement is a bit trickier to think about. Consider a set of m equations over variables $x_1, \ldots, x_n$:

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

where:

- For all $j = 1, \ldots, n$ and all $r = 1, \ldots, m$, the coefficients $a_j^{(r)} \in \{0, 1, 2, \ldots, 16\}$ are not all zero; and
- for all $r = 1, \ldots, m$, $b^{(r)} \in \{0, 1, \ldots, 16\}$.

Suppose that each variable x_j appears in at most 4 of the m equations. (That is, for each j, $a_j^{(r)} = 0$ for all but four values of r.)

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. Remember that* A *is mutually independent of events* $\{B_1, \ldots, B_\ell\}$*, if for any set* $J \subseteq \{1, 2, \ldots, \ell\}$, $\Pr[A | \cap_{j \in J} B_j] = \Pr[A]$. *Write down what that means in this context!*

Hint: *A bigger hint is given on the last page...*

5 (If time) Practice with the second moment method

In a graph $G = (V, E)$, say that a vertex v is **isolated** if it has no neighboring vertices.

Group Work

Let $G \sim G_{n,p}$ be a random graph where each edge is present independently with probability p, where $p = \frac{c \ln n}{n}$ for some constant $0 < c < 1$.

1. Use the Second Moment Method to show that, with probability at least $1 - o(1)$, there is some isolated vertex in G.

   For this exercise, feel free to use the approximation $e^{-x} \approx 1 - x$ when x is small as an equality without worrying about it.

   Feel free to use either the second moment method we saw in the mini-lecture videos, or the alternate form from the warm-up. (Either will work).

   ***Hint**: Consider the random variable X that is the number of isolated vertices in G.*

   ***Hint**: When computing the variance of X, you may want to consider the following question: given two distinct vertices u, v of G, what is the probability that* both *u and v are isolated?*

Extra hint for second group work: You can take $d = 3$. Why?