Problem Set 2 CS265/CME309, Autumn 2022

Due: 10/14 (Friday) at 11:59pm on Gradescope

Group members: Rylan Schaeffer, Connor Settle

Please follow the homework policies on the course website.

---

1. **(8 pt.) [Counting small cuts.]**

   Recall that a cut of an undirected graph $G = (V, E)$ is a partition of the vertices V into nonempty disjoint sets A and B. A *min cut* of G is a cut that minimizes the number of edges that cross the cut (have one endpoint in A and one in B).

   In the following problems, assume G is a connected graph on n vertices (i.e., there is no cut with 0 edges that cross it).

   (a) **(2 pt.)** A graph may have many possible min cuts. Prove that G has *at most* $n(n-1)/2$ min cuts.

   (b) **(2 pt.)** Show that part (a) is tight; for every $n \geq 2$, give a connected graph on n vertices with exactly $n(n-1)/2$ min cuts.

   (c) **(4 pt.)** Let α be a positive integer. Suppose that any min cut of G has k edges that cross the cut. An α-*small* cut of G is a cut that has at most αk edges that cross the cut. Prove that the number of such cuts is at most $O(n^{2\alpha})$.

   [**Note:** If you find it easier, you'll still get full credit if you prove a bound of $O((2n)^{2\alpha})$.]

   [**HINT:** *Consider stopping Karger's algorithm early and then outputting a random cut in the contracted graph. What is the probability that this returns a fixed α-small cut of G?*]

   (d) **(0 pt.) [Optional: this won't be graded]** Let $f(n, \alpha)$ be the maximum number of α-small cuts that an n vertex graph can have. What are the tightest upper and lower bounds you can find for $f(n, \alpha)$?

SOLUTION:

(a) Lecture 2 Theorem 2.2's proof states the probability that a specific min cut C is found is $\geq \frac{2}{n(n-1)}$. Suppose, for purposes of contradiction, the number of min cuts is $> \frac{n(n-1)}{2}$. Then the total probability of finding these min cuts is $> \frac{2}{n(n-1)} \frac{n(n-1)}{2} = 1$, which is impossible.

(b) Let G be a cycle graph. This graph has exactly $n(n-1)/2$ min cuts, where each min cut is given by choosing a start node and an end node, and taking all nodes in between them as one partition and the complement as the other partition. There are $\binom{n}{2} = \frac{n(n-1)}{2}$ possible ways to pick the start and end nodes.

(c) Consider a particular α-small cut. Suppose we run Karger's algorithm until 2α edges remain. The probability that Karger's algorithm, prematurely ended, doesn't contract an edge in that α-small cut is:

$$Pr[\text{not violating the cut}] \geq \frac{n-2\alpha}{n}\frac{n-2\alpha-1}{n-1}...\frac{1}{2\alpha+1}$$

Annihilating terms gives:

$$Pr[\text{not violating the cut}] \geq \frac{(2\alpha)...(3)(2)(1)}{n(n-1)...(n-2\alpha+1)}$$

With 2α remaining vertices, $2^{2\alpha}-1$ partitions are possible; a random sampling of the possible partitions chooses our particular α-small cut is $1/2^{2\alpha}$. Thus, the probability we select our particular α-small cut is:

$$\begin{aligned} Pr[\text{select this particular cut}] &= \frac{1}{2^{2\alpha}}Pr[\text{not violating the cut}] \\ &\geq \frac{1}{n(n-1)...(n-2\alpha+1)} \\ &\geq n^{-2\alpha} \end{aligned}$$

Since the summed probability of all α-small cuts must not exceed 1, the total number of α-small cuts must be $O(n^{2\alpha})$

2. **(12 pt.) [Tightness of Markov's and Chebyshev's Inequalities]**

   (a) **(4 pt.)** Show that Markov's inequality is tight. Specifically, for each value $c > 1$, describe a distribution D_c supported on non-negative real numbers such that if the random variable X is drawn according to D_c then (1) $\mathbb{E}[X] > 0$ and (2) $\Pr[X \geq c\mathbb{E}[X]] = 1/c$.

   (b) **(4 pt.)** Show that Chebyshev's inequality is tight. Specifically, for each value $c > 1$, describe a distribution D_c supported on real numbers such that if the random variable X is drawn according to D_c then (1) $\mathbb{E}[X] = 0$ and $\mathrm{Var}[X] = 1$ and (2) $\Pr[|X - \mathbb{E}[X]| \geq c\sqrt{\mathrm{Var}[X]}] = 1/c^2$.

   (c) **(4 pt.)** [One-sided version of Chebyshev's Inequality] Prove a one-sided bound on the distribution of a random variable X given its variance. That is, if $\mathrm{Var}[X] = 1$, what the best upper bound on $\Pr[X - \mathbb{E}[X] \geq t]$? Give your answer in terms of t. Prove your bound (a) is true and (b) is tight by coming up with a variable X with distribution D_t and variance 1 for which $\Pr[X - \mathbb{E}[X] \geq t]$ equals your answer.

SOLUTION:

(a) Fix $c > 1$. Define the distribution $D_c(x) = (1 - \frac{1}{c})\delta_0(x) + \frac{1}{c}\delta_1(x)$, where $\delta_\cdot(x)$ is the Dirac measure. Note that the first condition is met:

$$\mathbb{E}[X] = \Big(1 - \frac{1}{c}\Big)0 + \Big(\frac{1}{c}\Big)1 = \frac{1}{c} > 0$$

Note that the second condition is also met:

$$Pr[X \geq c\mathbb{E}[X] = c\frac{1}{c} = 1] = \frac{1}{c}$$

(b) Define $D_c(x) = \frac{1}{2c^2}\delta_{-c}(x) + \frac{1}{2c^2}\delta_c(x) + (1 - \frac{1}{c^2})\delta_0(x)$, where δ is again a Dirac measure. Note that the first condition is met:

$$\mathbb{E}[X] = \Big(\frac{1}{2c^2}\Big)(-c) + \Big(\frac{1}{2c^2}\Big)(c) + \Big(1 - \frac{1}{c^2}\Big)(0) = 0$$

Note that the second condition is also met:

$$\mathbb{V}[X] = \Big(\frac{1}{2c^2}\Big)(-c)^2 + \Big(\frac{1}{2c^2}\Big)(c)^2 = \frac{1}{2} + \frac{1}{2} = 1$$

Note that the third condition is also met:

$$Pr(|X - \mathbb{E}[X]| \geq c) = \frac{1}{c^2}$$

(c) I'm going to answer the questions in reverse order. I'll first show that a distribution D_t exists with a particular probability, then show that this is an upper bound. Define a distribution $D_t = (1 - \frac{1}{1+t^2})\delta_{-1/t}(x) + \frac{1}{1+t^2}\delta_t(x)$. Note that the variance is 1:

$$\mathbb{V}[X] = (1 - \frac{1}{1+t^2})(-1/t)^2 + \frac{1}{1+t^2}t^2 = -\frac{t^2}{1+t^2} + \frac{t^2}{1+t^2} = 1$$

For this D_t, $Pr[X - \mathbb{E}[X] \geq t] = \frac{1}{1+t^2}$. I claim that this is an upper bound i.e. that for all distributions with variance 1, $Pr[X - \mathbb{E}[X] \geq t] \leq \frac{1}{1+t^2}$:

$$\begin{aligned}
Pr[X - \mathbb{E}[X] \geq t] &= Pr[X - \mathbb{E}[X] + \frac{\mathbb{V}[X]}{t} \geq t + \frac{\mathbb{V}[X]}{t}] \\
&\leq Pr\left[(X - \mathbb{E}[X] + \frac{\mathbb{V}[X]}{t})^2 \geq (t + \frac{\mathbb{V}[X]}{t})^2\right] \\
&\leq \frac{\mathbb{V}[X] + \mathbb{V}[X]^2/t^2}{(\mathbb{V}[X]/t + t)^2} \\
&= \frac{\mathbb{V}[X](t^2 + \mathbb{V}[X])}{(\mathbb{V}[X] + t^2)^2} \\
&= \frac{\mathbb{V}[X]}{\mathbb{V}[X] + t^2}
\end{aligned}$$

This bound is tight because the D_t we defined earlier meets the equality.

3. **(0 pt.)** **[This whole problem is optional and will not be graded.]** In this problem, you'll analyze a different primality test than we saw in class. This one is called the *Agrawal-Biswas Primality test.*

Given a degree d polynomial $p(x)$ with integer coefficients, for any polynomial $q(x)$ with integer coefficients, we say $q(x) \equiv t(x) \mod (p(x), n)$ if there exists some polynomial $s(x)$ such that $q(x) = s(x) \cdot p(x) + t(x) \mod n$. (Here, we say that $\sum_i c_i x^i = \sum_i c'_i x^i \mod n$ if and only if $c_i = c'_i \mod n$ for all i.) For example, $x^5 + 6x^4 + 3x + 1 \equiv 3x + 1 \mod (x^2 + x, 5)$, since $(x^3)(x^2 + x) + (3x + 1) = x^5 + x^4 + 3x + 1 \equiv x^5 + 6x^4 + 3x + 1 \mod 5$.

Agrawal-Biswas Primality Test.
Given n:

- If n is divisible by 2,3,5,7,11, or 13, or is a perfect power (i.e. $n = c^r$ for integers c and r) then output **composite**.
- Set d to be the smallest integer greater than $\log n$, and choose a random degree d polynomial with leading coefficient 1:

$$r(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_1 x + c_0,$$

  by choosing each coefficient c_i uniformly at random from $\{0, 1, \ldots, n-1\}$.
- If $(x + 1)^n \equiv x^n + 1 \mod (r(x), n)$ then output **prime**, else output **composite**.

Consider the following theorem (you can assume this if you like, or for even more optional work, try to prove it!):

Theorem 1 (Polynomial version of Fermat's little theorem)**.**

- *If n is prime, then for any integer a, $(x - a)^n = x^n - a \mod n$.*
- *If n is not prime and is not a power of a prime, then for any a s.t. $gcd(a, n) = 1$ and any prime factor p of n, $(x - a)^n \neq x^n - a \mod p$.*

First, show that if n is prime, then the Agrawal-Biswas primality test will always return **prime**.

Now, we will prove that if n is composite, the probability over random choices of $r(x)$ that the algorithm successfully finds a witness to the compositeness of n (and hence returns **composite**) is at least $\frac{1}{4d}$.

(a) Using the polynomial version of Fermat's Little Theorem, and the fact that, for prime q, every polynomial over $\mathbb{Z}_q$ that has leading coefficient 1 (i.e. that is "monic") has a unique factorization into irreducible monic polynomials, prove that the number of irreducible degree d factors that the polynomial $(x + 1)^n - (x^n + 1)$ has over $\mathbb{Z}_p$ is at most n/d, where p is any prime factor of n. (A polynomial is irreducible if it cannot be factored, for example $x^2 + 1 = (x + 1)(x + 1) \mod 2$ is not irreducible over $\mathbb{Z}_2$, but $x^2 + 1$ is irreducible over $\mathbb{Z}_3$.)
[**HINT:** *Even though this question sounds complicated, the proof is just one line...*]

(b) Let $f(d,p)$ denote the number of irreducible monic degree d polynomials over $\mathbb{Z}_p$. Prove that if n is composite, and not a power of a prime, the probability that $r(x)$ is a witness to the compositeness of n is at least $\frac{f(d,p)-n/d}{p^d}$, where p is a prime factor of n.

[**HINT:** *p^d is the total number of monic degree d polynomials over $\mathbb{Z}_p$.*]

(c) Now complete the proof, and prove that the algorithm succeeds with probability at least $1/(4d)$, leveraging the fact that the number of irreducible monic polynomials of degree d over $\mathbb{Z}_p$ is at least $p^d/d - p^{d/2}$. (You should be able to prove a much better bound, though $1/4d$ is fine.)

[**HINT:** *You will also need to leverage the fact that we chose $d > \log n$ and also explicitly made sure that n has no prime factors less than* 17.]

SOLUTION:

(a) asdf

(b)