CS7880: Rigorous Approaches to Data Privacy, Spring 2017
POTW #4

Instructor: Jonathan Ullman

Due Fri, Feb 10th, 11:59pm
(Email to jullman+PrivacyS17@gmail.com)

- **You may work on this homework in pairs if you like. If you do, you must write your own solution and state who you worked with.**
- Solutions must be typed in LaTeX.
- Aim for clarity and brevity over low-level details.

Problem 1 (Differentially Private Global Minimum Cut)**.**

In this problem we will see a non-trivial, non-black-box application of the exponential mechanism to the global minimum cut problem. We will also see our first application of differential privacy to data represented by a graph.

Let $G = (V, E)$ be an undirected, unweighted graph. For every $S \subseteq V$, define

$$E(S) = |\{(u, v) \in E \mid u \in S, v \notin S\}|$$

to be the number of edges that have one endpoint in S and one in S^c. Informally, $E(S)$ is the number of edges "cut by S." The *global min-cut* problem is to find the set S that cuts the fewest edges. That is, to find

$$S_{OPT} = \arg\min_{S \subseteq V} |E(S)|.$$

Let $OPT = |E(S_{OPT})|$ be the number of edges crossing the global min-cut.

(a) Give an instantiation of the exponential mechanism that will output an $(\varepsilon, 0)$-differentially private set $\hat{S}$ that is an approximate global minimum cut in G. Here we refer to *edge-level* differential privacy, meaning that removing or adding one edge to the graph should not change the output distribution of the mechanism by more than an e^{ε} factor.[1]

(b) A nice property of global minimum cuts is that there cannot be too many *nearly-minimum* cuts. In particular, it is known that, for every $C \geq 1$, the number of cuts S such that

[1] A stronger requirement would be *node-level* differential privacy, meaning that removing or adding one vertex, with an arbitrary set of edges incident on that vertex, should not change the output distribution of the mechanism by more than an e^{ε} factor.

$|E(S)| \leq C \cdot OPT$ is at most $|V|^{2C}$. Use this fact to show that, when $OPT \geq 128 \log(|V|/\beta)/\varepsilon$ is not too small[2], with probability at least $1 - \beta$, your mechanism outputs a set $\hat{S}$ such that

$$|E(\hat{S})| \leq OPT + O\left(\frac{\log(|V|/\beta)}{\varepsilon}\right)$$

That is, so as long as the global min-cut in G doesn't cut too few edges, the exponential mechanism will privately find a nearly-minimum cut.

Hint: Since there are $2^{|V|}$ possible cuts, the result will not follow from the generic analysis of the exponential mechanism. You will have to use the additional structure of minimum cuts.

[2]The constant 128 can certainly be improved. I embiggened it to allow for some slack in the calculations.