CIS399: The Science of Data Ethics	Lecture 21: April 4, 2019
Instructor: Michael Kearns & Ani Nenkova Perelmuter	Scribes: Anant Kumar, Ethan

1 Recap of Laplace Mechanism

Last lecture, we discussed a mechanism, *Laplace Mechanism*, for implementing Differential Privacy on some function f that is to be executed on a database. The Laplace Mechanism accomplishes this by adding *noise* to the output of f, where the noise is computed under some given parameter ϵ as follows:
Let $f(x_1, x_2, ..., x_n)$ be a function on some data in a database x=$(x_1, x_2, ..., x_n)$. For example, f can be a function computing the average or the standard deviation on a set of values.
Let $\Delta f = Max_{x,x'}|f(x) - f(x')|$ over all neighboring databases x and x'. Thus, Δf is the "sensitivity" of f, the maximum difference in values f can take on when executed on neighboring databases x and x', databases that differ in exactly 1 piece of data. For example, if f computes the average of a set of values, then $\Delta f = \frac{1}{n}$, and if f computes the standard deviation on a set of values, then $\Delta f = \frac{1}{\sqrt{n}}$
Finally, let v be the noise added to the output of f, where v is drawn randomly from the following probability distribution that is symmetric around 0:

$$Pr[v] = \frac{1}{2b} e^{\frac{-|v|}{b}} \text{ where } b = \frac{\Delta f}{\epsilon}$$

Therefore, the output of executing f on some database x is $f(x) + v$.

1.1 Analysis of Laplace Mechanism

Let x and x' be 2 neighboring databases, and let p_x and $p_{x'}$ be output distributions. Let o be an arbitrary output value of f. Consider the ratio probabilities of f outputting o using the Laplace Mechanism on databases x and x'.

$$\frac{p_x(o)}{p_{x'}(o)} = \frac{\frac{1}{2b} e^{\frac{-|f(x)-o|}{b}}}{\frac{1}{2b} e^{\frac{-|f(x')-o|}{b}}} = e^{\frac{|f(x')-o|-|f(x)-o|}{b}} \leq e^{\frac{|f(x')-f(x)|}{b}}$$

Note that $b = \frac{\Delta f}{\epsilon}$, and $\Delta f \geq |f(x') - f(x)|$ on all neighboring databases. Therefore,

$$e^{\frac{|f(x')-f(x)|}{b}} \leq e^{\frac{\Delta f}{\frac{\Delta f}{\epsilon}}} = e^{\epsilon} \rightarrow \frac{p_x(o)}{p_{x'}(o)} \leq e^{\epsilon}$$

Therefore, the ratio of the probabilities, $\frac{p_x(o)}{p_{x'}(o)}$ is upper bounded by e^{ϵ}. In other words, as ϵ decreases, e^{ϵ} approaches 1. Thus, we see that applying the Laplace Mechanism to a function f with parameter ϵ allows the function to satisfy ϵ-DP.

2 Motivation for another mechanism

The Laplace Mechanism gives a *general purpose* way of adding noise to satisfy differential privacy. The Laplace Mechanism assumes that computing f accurately is the best measure of what we want to extract from our data. However, consider the following case we may want to apply differential privacy:
Input: x = A database of training data
Goal/Output: y = A neural network that minimizes the training error on x
The neural network returned is defined by a series of weights. If we were to apply the Laplace Mechanism to this function, Laplace noise would be added to the weights before returning the network. However, even small fluctuations in weights in a neural network may severely impact the performance of that network. Therefore, the returned network (with added noise) will likely behave very differently than the initial network found (before adding noise) that minimized error, and thus would have a unpredictably higher error than the minimal error network we desired. Thus, this presents us with motivation to create another mechanism to satisfy Differential Privacy in such cases where the Laplace Mechanism fails.

3 Exponential Mechanism Setup

Consider the generalized problem:
Input: $x \in X$ where X is a generic input space
Output: $o \in O$ where O is a generic output space
Let us define u as function that takes 2 parameters, x and o, and returns a real value $r \in R$ such that r is a measure of "how good" a solution o is for input x. Therefore, when solving this problem in the absence of any privacy constraint we desire to find $\max_{o \in O}\{u(x, o)\}$ i.e. the "best" solution for input x.
Now let us define a *generalized sensitivity* given some utility function u, Δu, as follows:

$$\Delta u = max_{o \in O}\{max_{x,x'}\{|u(x, o) - u(x', o)|\}\} \text{ over all neighboring databases x and x'}$$

4 The Exponential Mechanism

Rather than adding noise to the output of a function *f*, the exponential mechanism draws an output o from a probability distribution. Given a parameter ϵ, an input x, and a utility function u with generalized sensitivity Δu, we draw an output o from the following distribution:

$$Pr[o] = e^{\frac{\epsilon * u(x,o)}{2\Delta u}}$$

5 Composition Theorem for Differential Privacy

We have now learned two different mechanisms to increase privacy. The composition theorem for differential privacy works as follows:

Suppose we have two algorithms A_1 and A_2 with corresponding epsilon values of ϵ_1 and ϵ_2. Now let us create a new algorithm A_3 that runs A_1 on x and then A_2 on the result of the first algorithm.

The composition theorem states that $\epsilon_3 = \epsilon_1 + \epsilon_2$.

This holds true in the scenario that an algorithm is applied multiple times. For example, if algorithm A_1 is applied to an input x, m times, epsilon would be $\epsilon_1 \times$ m.

6 Privacy Budget

An individuals privacy budget is the limit of how much privacy they are ok with leaking. The concept arises from the issue that even though no single operation being done on data reveals who the subjects might be, by combining the data from multiple trials, one might be able to figure out details about an individual.
As a result, every person has a "privacy budget". Each time an individual is included in a differential privacy calculation, it eats away at their privacy budget (by ϵ). Most calculations in Machine Learning can done to give a differential privacy guarantee and a utility guarantee. This means that all these calculations can also be accounted for in the privacy budget.

7 Real World Examples

1. Apple and privacy budgets:
   A recent issue arose with apple as news came out that they were using differential privacy in order to maintain their users' privacy. They were running operations of the app data they were receiving from their devices and made sure to use ϵ values that would ensure the privacy budget for the users would not be exceeded. However, they broke the standard by resetting the privacy budget every day. Since the privacy budget is a value that is used cumulatively for life, this became a problem. Users were now no longer guaranteed privacy because no one was keeping track of their overall privacy budgets, they just knew that no single day's operations would result in a breach of privacy for a user.

2. 2020 Census:
   The 2020 Census announced that it would be using differential privacy in order to maintain the privacy of the American people. Specifically, they will do so by releasing all statistics in a deferentially private way. It has not yet been determined how epsilon and randomization of the data will occur. This is considered a big step forward because previous methods for maintaining privacy were dependent on a bunch of tricks that caused the data to be convoluted.
   This decision faces some backlash from the leaders of academic subfields devoted to interpreting the census. These people believe that the increased privacy provided by the new methods is not worth the trade-off for accuracy. A key point to learn from this example is that society needs to make the decision of which point in the privacy-accuracy spectrum we want to be at.