cs208 HW 2

Anthony Rentsch

3/12/2019

Question 1

(a) Both (i) and (iv) are (ϵ, 0)-differentially private. I demonstrate that below using two neighboring datasets, $x = [0, 0, ..., 0]$ amnd $x' = [0, 0, ..., 1]$.

(i)

$$\frac{P([\bar{x} + Z]_0^1 = r)}{P([\bar{x'} + Z]_0^1 = r)}$$

$$\frac{\frac{n}{4}exp(-\frac{n}{2}|r - \bar{x}|)}{\frac{n}{4}exp(-\frac{n}{2}|r - \bar{x'}|)}$$

$$exp(\frac{n}{2}|r - \bar{x'}| - |r - \bar{x}|)$$

By the triangle inequality, this expression is less than or equal to

$$exp(\frac{n}{2}|r - \bar{x'} - r + \bar{x}|) = exp(\frac{n}{2}|\bar{x} - \bar{x'}|)$$

Since $|\bar{x} - \bar{x'}|$ is just the global sensitivity, we get that

$$exp(\frac{n}{2}|\bar{x} - \bar{x'}|) = exp(\frac{n}{2}\frac{1}{n}) = exp(\frac{1}{2})$$

Thus, $M(x)$ is $(\epsilon, 0)$-differentially private for $\epsilon \geq 0.5$.

(iv)

$$\frac{exp(\frac{-n}{10}|y - \bar{x}|)}{exp(\frac{-n}{10}|y - \bar{x'}|)} * \frac{\int_0^1 exp(\frac{-n}{10}|z - \bar{x}|)dz}{\int_0^1 exp(\frac{-n}{10}|z - \bar{x'}|)dz}$$

I'll evaluate this term by term. First, the left term:

$$exp(\frac{n}{10}(-|y - \bar{x}| + |y - \bar{x'}|))$$

$$exp(\frac{n}{10}(-|y| + |y - \frac{1}{n}|))$$

By the triangle inequality, this is less than or equal to

$$exp(\frac{n}{10}(y - \frac{1}{n} - y)) = exp(\frac{1}{10})$$

Now, for the right term:

$$\frac{\int_0^1 exp(\frac{-n}{10}|z-\frac{1}{n}|)dz}{\int_0^1 exp(\frac{-nz}{10})dz}$$

$$\frac{\int_0^{\frac{1}{n}} exp(\frac{-n}{10}(z-\frac{1}{n}))dz + \int_{\frac{1}{n}}^1 exp(\frac{-n}{10}(z-\frac{1}{n}))dz}{\int_0^{\frac{1}{n}} exp(\frac{-nz}{10})dz + \int_{\frac{1}{n}}^1 exp(\frac{-nz}{10})dz}$$

$$\frac{exp(\frac{1}{10})\int_0^{\frac{1}{n}} exp(\frac{-nz}{10})dz + exp(\frac{1}{10})\int_{\frac{1}{n}}^1 exp(\frac{-nz}{10})dz}{\int_0^{\frac{1}{n}} exp(\frac{-nz}{10})dz + \int_{\frac{1}{n}}^1 exp(\frac{-nz}{10})dz}$$

This reduces to $exp(\frac{1}{10})$. Putting the two terms together, we have

$$exp(\frac{1}{10}) * exp(\frac{1}{10}) = exp(\frac{1}{5})$$

Thus, this mechanism is $(\epsilon, 0)$-differentially private for $\epsilon \geq 0.2$.

(b) Mechanisms (ii) and (iii) are not $(\epsilon, 0)$-differentially private. Below I'll provide a counterexample that demonstrates this and find a minimum value of δ for which they are (ϵ, δ)-differentially private.

(ii) Consider $x = [0, 0, ..., 0] and x' = [0, 0, ..., 1]$. Now, $P(M(x) = -1) \geq 0$ while $P(M(x') = -1) = 0$. This violates $P(M(x) = -1) \leq exp(\epsilon)P(M(x') = -1)$, so this mechanism is not $(\epsilon, 0)$-differentially private. Now let's consider the minimum value of δ for which it is (ϵ, δ)-differentially private.

$$4x$$

(iii) Consider $x = [0, 0, ..., 1] and x' = [0, 0, ..., 0]$. Now, $P(M(x) = 1) = \frac{1}{n}$ while $P(M(x') = 1) = 0$. This clearly violates $P(M(x) = 1) \leq exp(\epsilon)P(M(x') = 1)$, so this mechanism is not $(\epsilon, 0)$-differentially private. Now let's consider the minimum value of δ for which it is (ϵ, δ)-differentially private.

$$\delta \geq max_{x\ x'}[\Sigma_y max(P(M(x) = y) - exp(\epsilon)P(M(x') = y), 0)]$$

The right hand side of this inequality reduces to

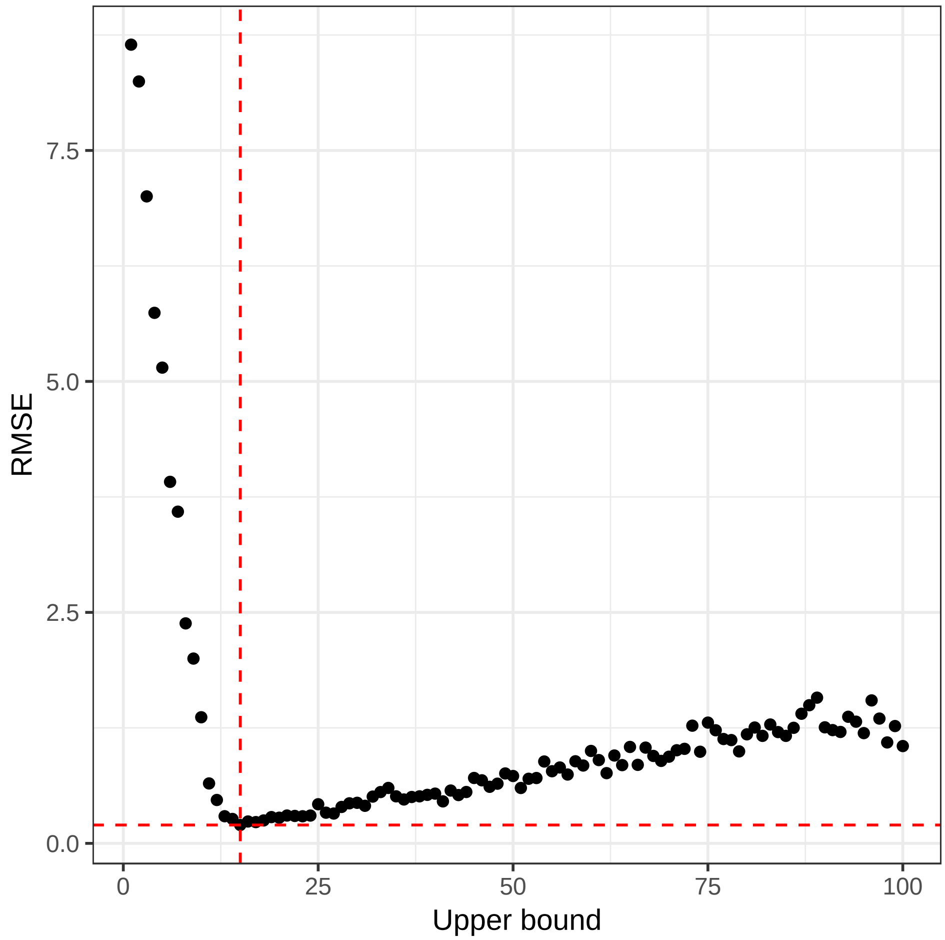
$$\Sigma_{y\in[0,1]}(P(M(x) = y) - exp(\epsilon)P(M(x') = y)$$
$$[P(M(x) = 1) - exp(\epsilon)P(M(x') = 1)] + [P(M(x) = 0) - exp(\epsilon)P(M(x') = 0)]$$

$$[\frac{1}{n} - exp(\epsilon) * 0] + [1 - \frac{1}{n} - exp(\epsilon) * 1] = 1 - exp(\epsilon)$$

This result seems wrong but I'm not sure what I did wrong with the math.

Question 2

For a,b,c see code in Appendix. Put plot for c in line. Optimal b: 19.

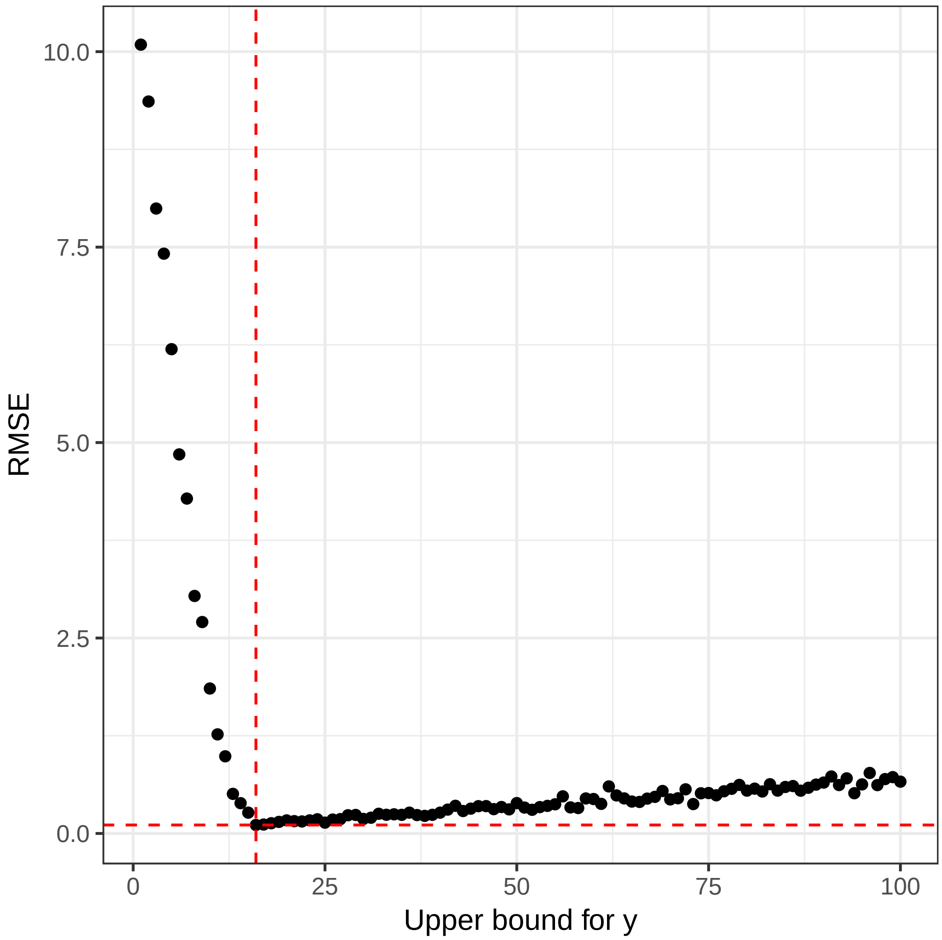


(d) -protecting outliers -why doesn't bootstrap do this

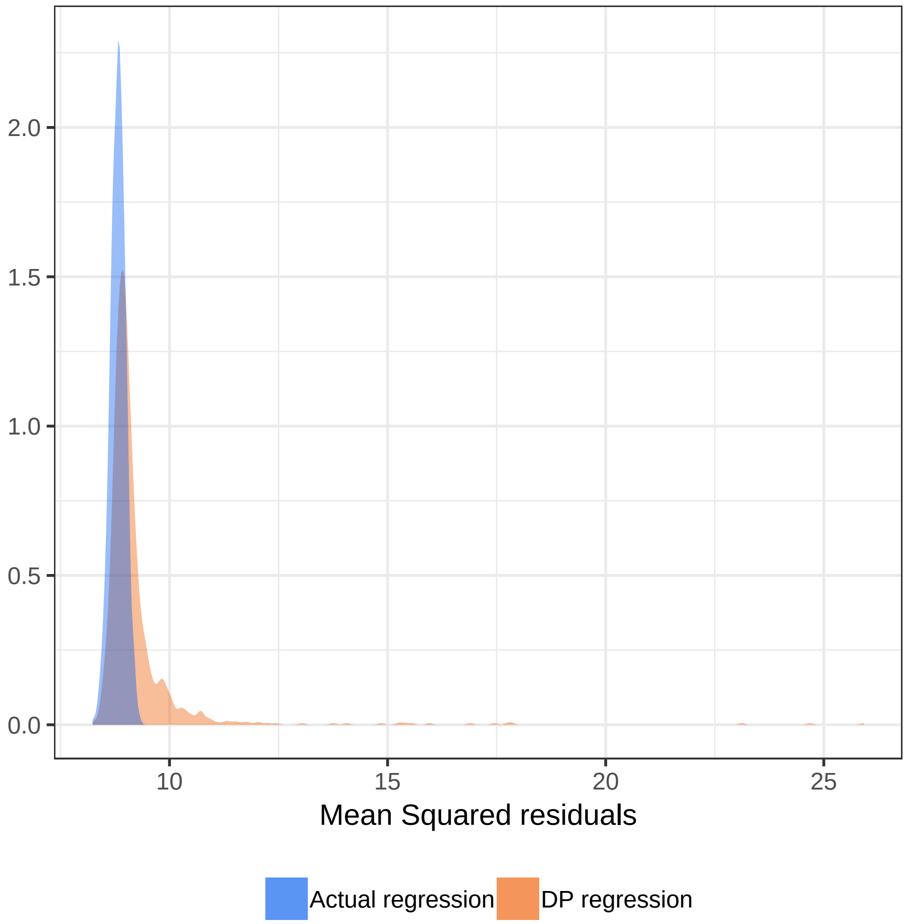
(e) -propose new mechanism -local sensitivity –> lower sensitivity in general, means thay we draw less noisy means -BOOM -or a diffeent statistic, different mechanism -see section notes

Question 3

(a) -4 DP subroutines: S_{xy}, S_{xx}, $\bar{x}$, and $\bar{y}$ and so we split epsilon over these (2 mean release and one regression coefccicient release) -how to clamp y? –> run same code as in 2, but generate poisson, plug that into noisy linear, and then find lowest rmse for some values of an upper bound for y —— 17 is the value I find



(b) -should true parameters be computed from clipped data?


2.0
1.5
1.0
0.5
0.0
10
15
20
25
Mean Squared residuals
Actual regression
DP regression