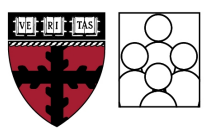
CS208: Applied Privacy for Data Science
DP Foundations: Exponential and Gaussian Mechanisms

James Honaker & Salil Vadhan

School of Engineering & Applied Sciences
Harvard University

March 1, 2019

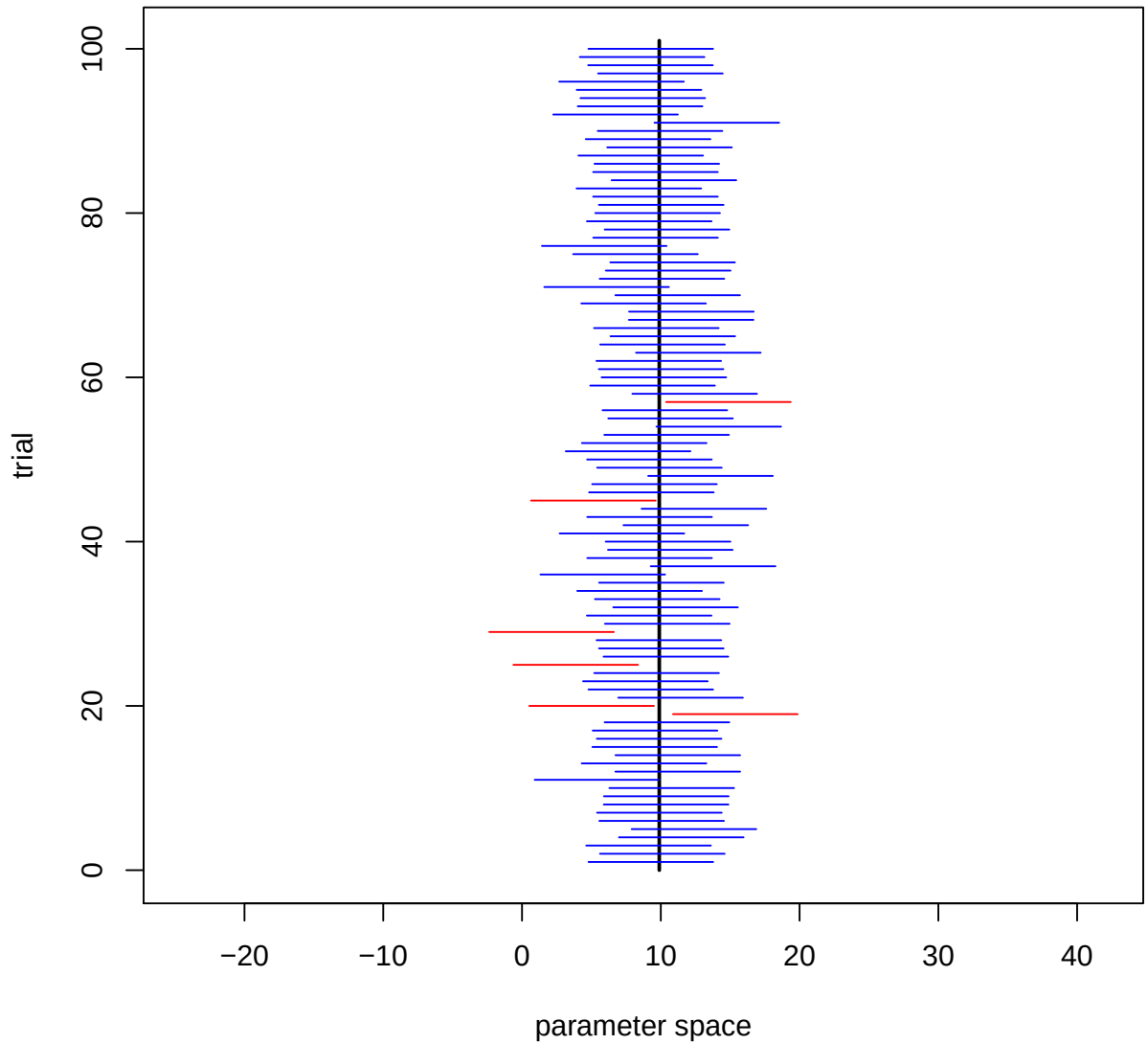


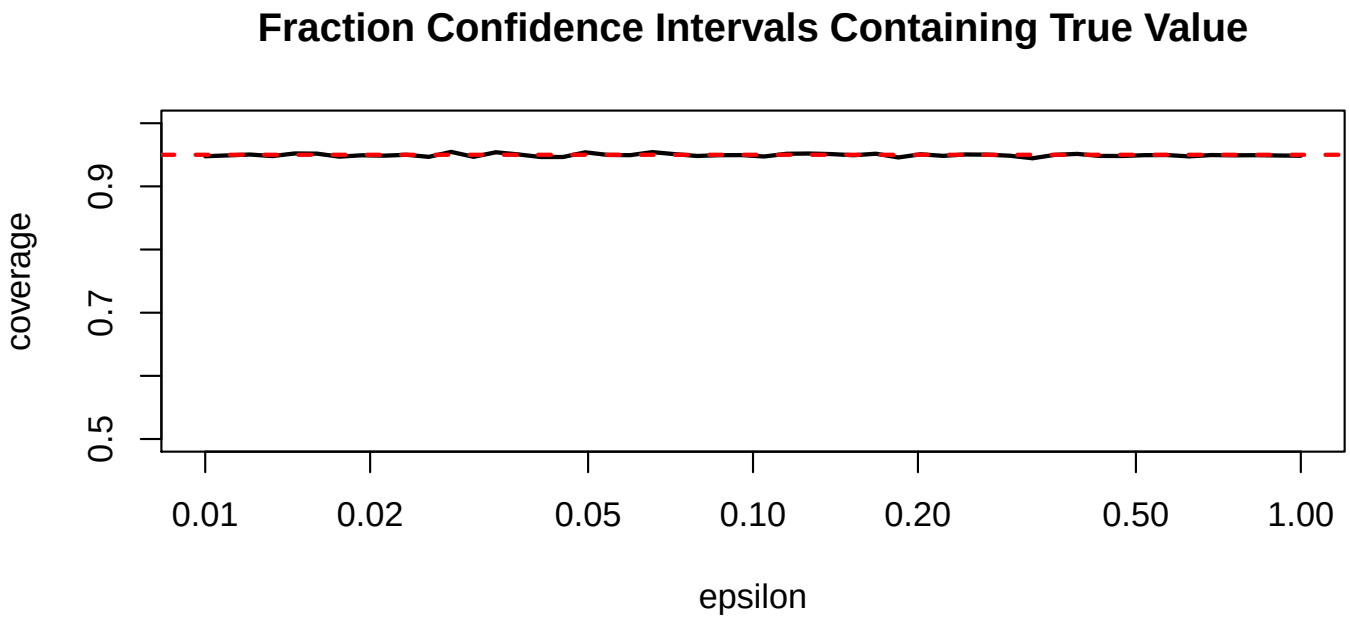
CRCS Center for Research on Computation and Society
at Harvard John A. Paulson School of Engineering and Applied Sciences

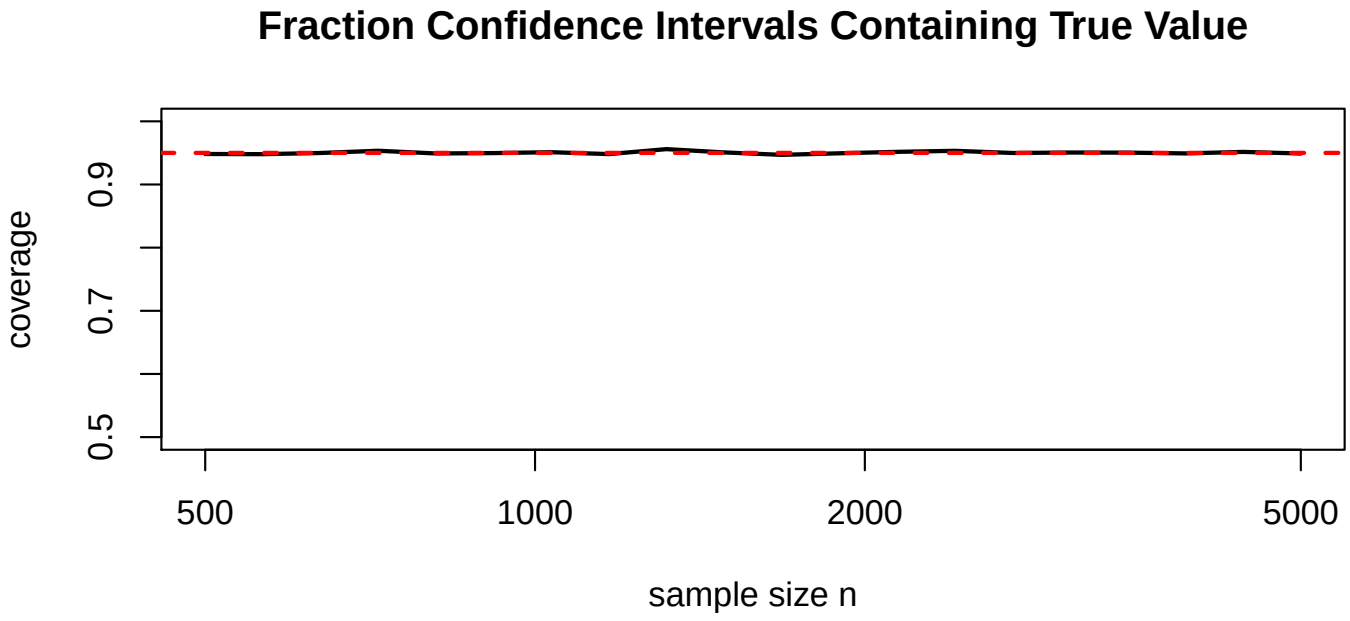
Confidence Interval Construction

Given an estimate $\hat{y}$, of a quantity y^*, a confidence interval, $\text{ci}(y^*|\hat{y}, \alpha) = [ci_{lower}, ci_{upper}]$ often simply $\text{ci}_{1-\alpha}(y^*)$, has *proper coverage* if:

$$\text{Prob}[y^* \in [ci_{lower}, ci_{upper}]] = 1 - \alpha$$


trial
0
20
40
60
80
100
−20
−10
0
10
20
30
40
parameter space

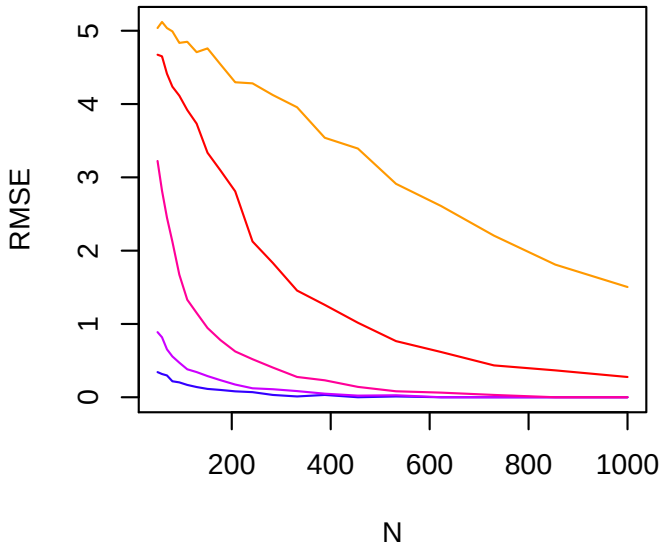

Fraction Confidence Intervals Containing True Value
coverage
0.5
0.7
0.9
0.01
0.02
0.05
0.10
0.20
0.50
1.00
epsilon

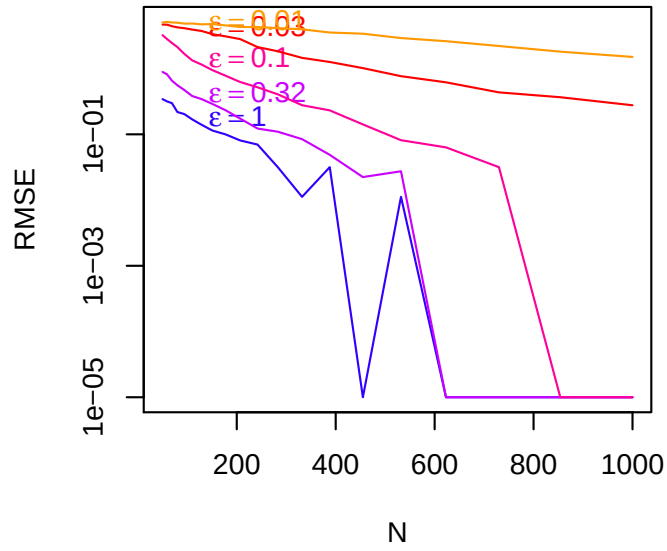

Fraction Confidence Intervals Containing True Value
coverage
0.5
0.7
0.9
500
1000
2000
5000
sample size n

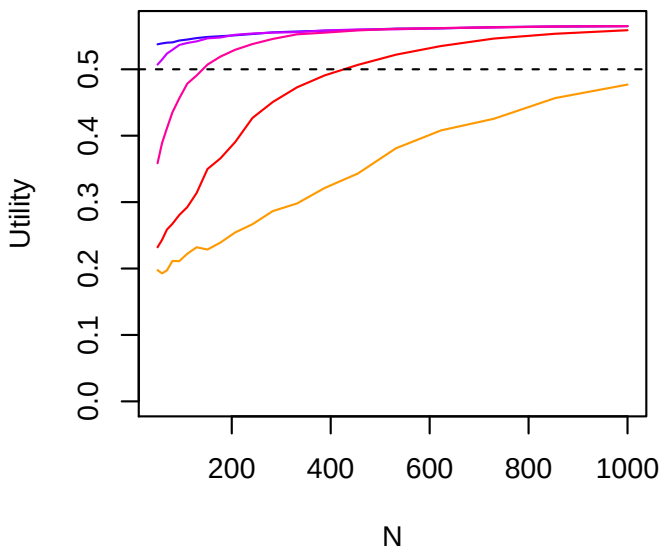
Exponential Mechanism for the Median

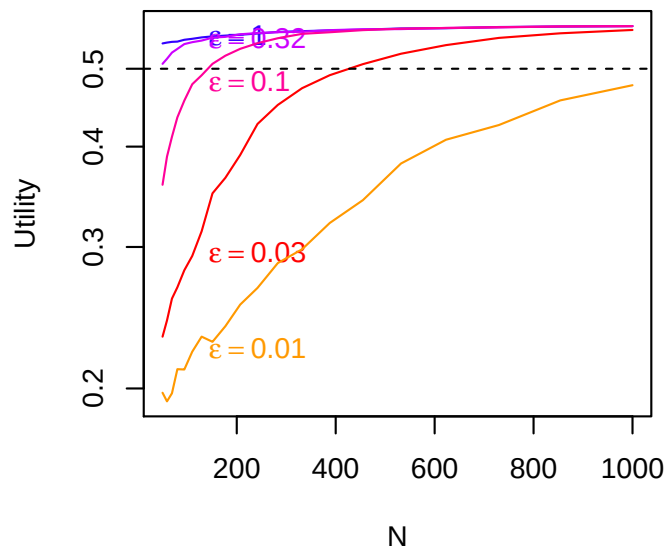
- Say $\mathcal{X} = \{1, 2, \cdots, M\}$.
- $M(x)$: output $y \in \mathcal{X}$ with prob $\propto \exp(\epsilon \cdot u(x, y)/2)$
  Where $u(x, y) = \min\{\#\{i : x_i \leq y\}, \#\{i : x_i \geq y\}\}$.
- Note that true median y^* has $u(x, y^*) \geq n/2$.
- Can show that for all x, with high probability,

$$u(x, M(x)) \geq n/2 - O(log(M)/\epsilon)$$


RMSE
0
1
2
3
4
5
200
400
600
800
1000
N


RMSE
1e−05
1e−03
1e−01
ε = 0.01
ε = 0.03
ε = 0.1
ε = 0.32
ε = 1
200
400
600
800
1000
N


Utility
0.0
0.1
0.2
0.3
0.4
0.5
200
400
600
800
1000
N


Utility
0.2
0.3
0.4
0.5
ε = 0.32
ε = 0.1
ε = 0.03
ε = 0.01
200
400
600
800
1000
N

Bounding Data

Action	Term	Domain	Library
Recode	Clip	Signal Processing	NumPy, pandas
	Clamp	Graphics, Geospatial	Torch
	Censor	Statistics	
	Top-code	Surveys	

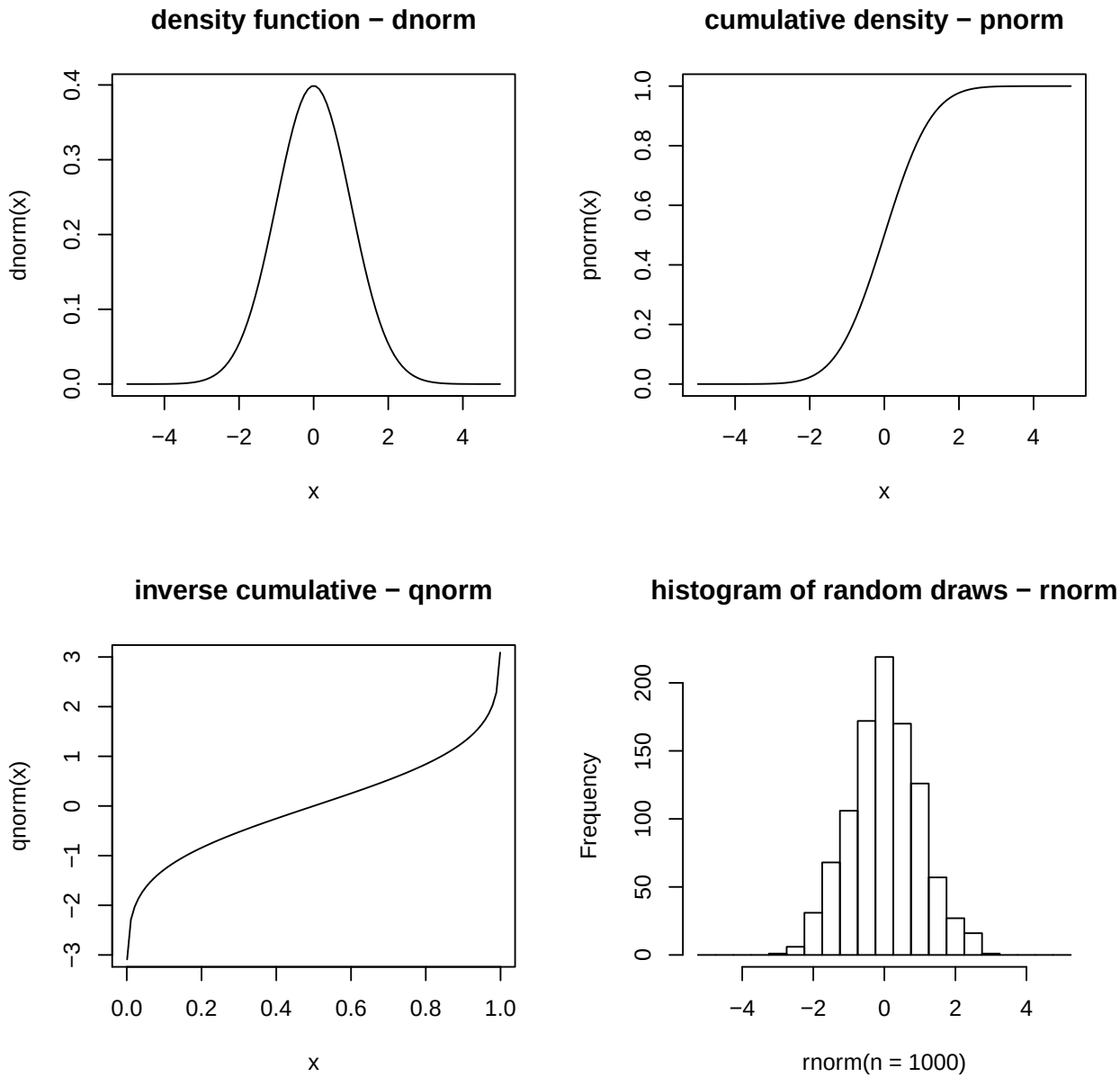
Bounding Data

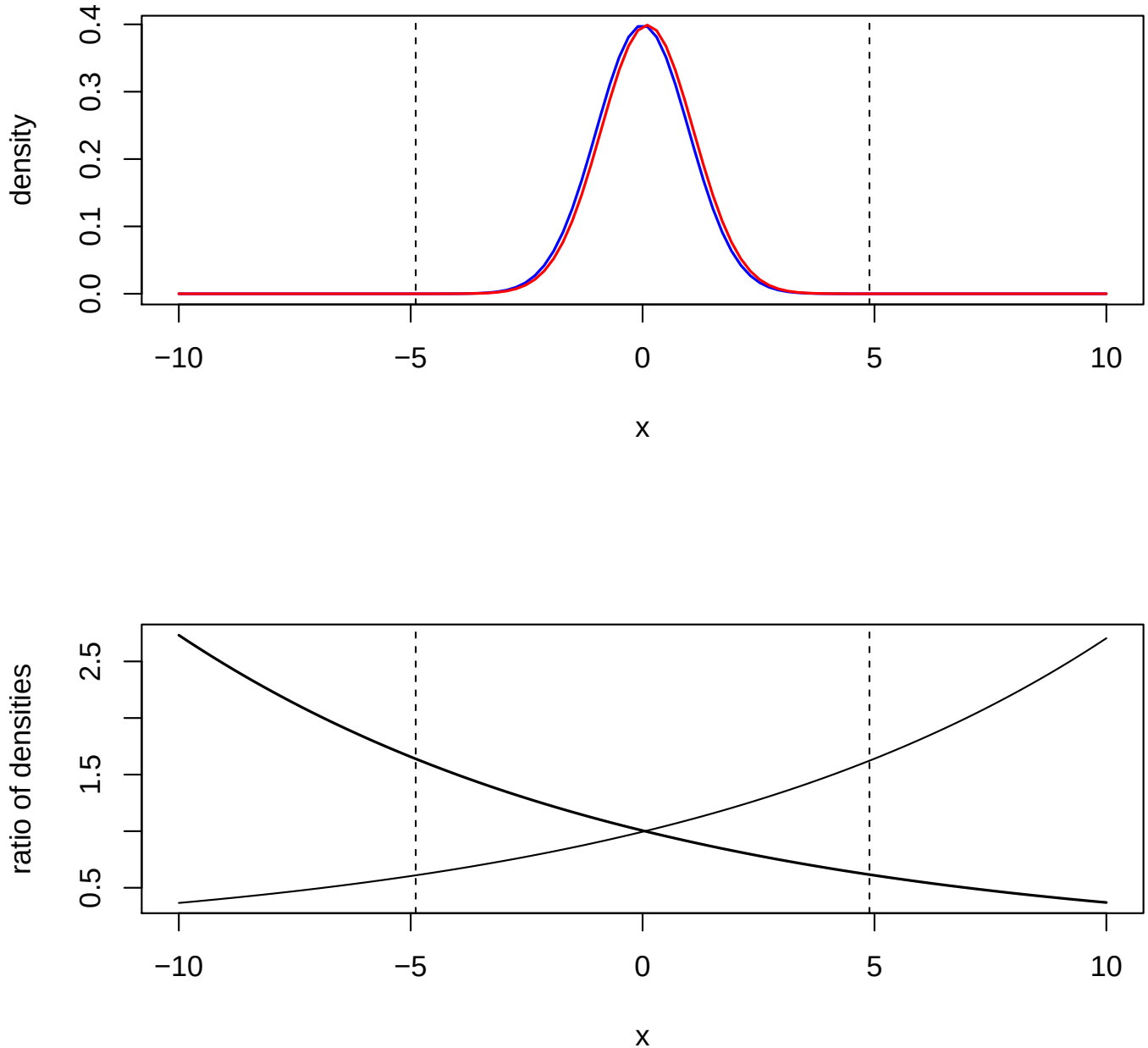
Action	Term	Domain	Library
Recode	Clip Clamp Censor Top-code	Signal Processing Graphics, Geospatial Statistics Surveys	NumPy, pandas Torch
Remove	Truncate Trim	Statistics Many	
Constrain	Winsorize	Statistics	

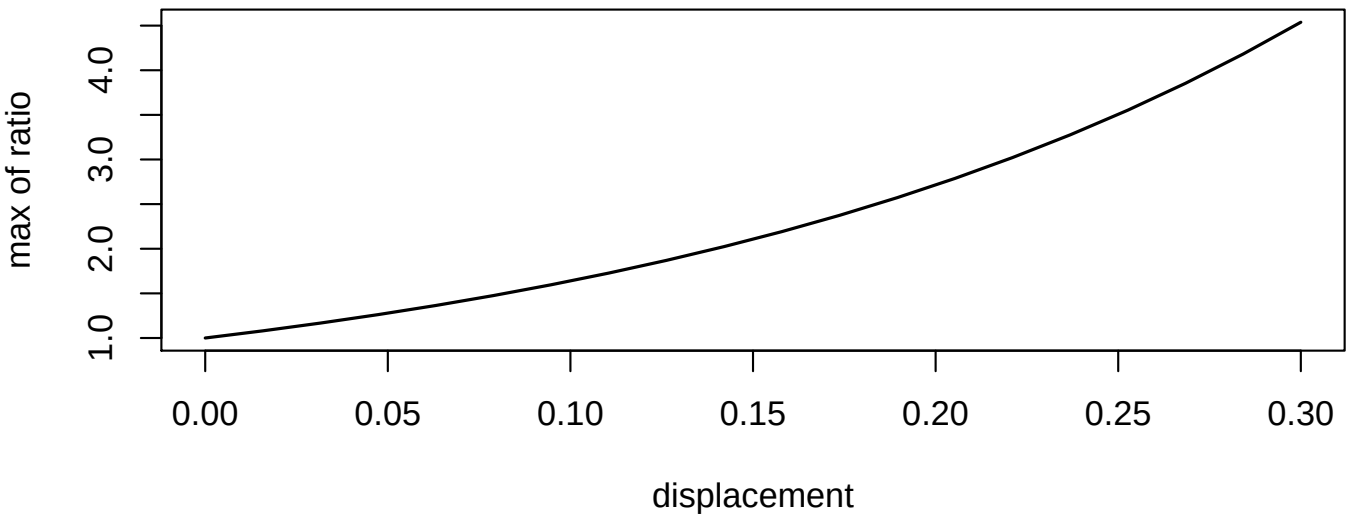
Gaussian Mechanism

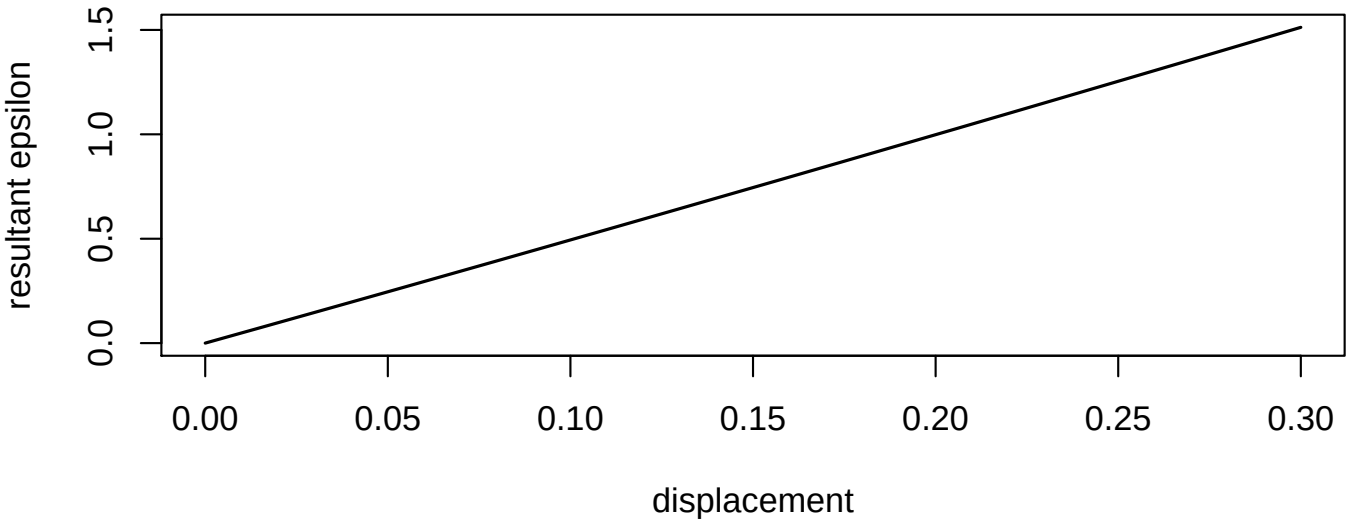
$$M(x, q) = q(x) + \mathcal{N}(0, \sigma^2),$$

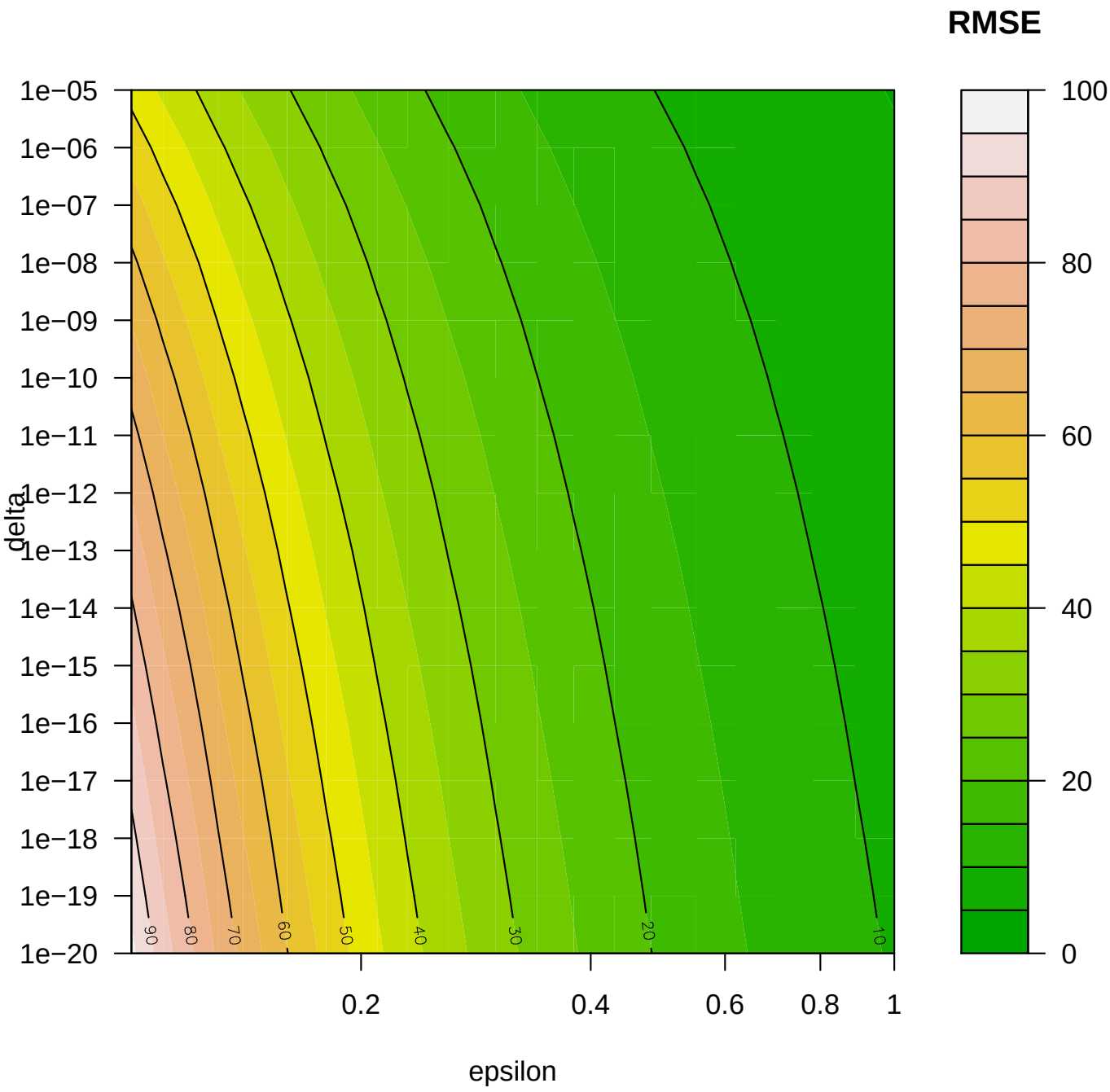
$$\text{for} \quad \sigma = \frac{GS_q}{\epsilon} \sqrt{2 \ln(1.25/\delta)}.$$


density function − dnorm
dnorm(x)
0.0
0.1
0.2
0.3
0.4
−4
−2
0
2
4
x
cumulative density − pnorm
pnorm(x)
0.0
0.2
0.4
0.6
0.8
1.0
−4
−2
0
2
4
x
inverse cumulative − qnorm
qnorm(x)
−3
−2
−1
0
1
2
3
0.0
0.2
0.4
0.6
0.8
1.0
x
histogram of random draws − rnorm
Frequency
0
50
100
150
200
−4
−2
0
2
4
rnorm(n = 1000)


density
0.0
0.1
0.2
0.3
0.4
−10
−5
0
5
10
x
ratio of densities
0.5
1.5
2.5
−10
−5
0
5
10
x


max of ratio
1.0
2.0
3.0
4.0
0.00
0.05
0.10
0.15
0.20
0.25
0.30
displacement


resultant epsilon
0.0
0.5
1.0
1.5
0.00
0.05
0.10
0.15
0.20
0.25
0.30
displacement


RMSE
1e−05
1e−06
1e−07
1e−08
1e−09
1e−10
1e−11
1e−12
1e−13
1e−14
1e−15
1e−16
1e−17
1e−18
1e−19
1e−20
delta
0.2
0.4
0.6
0.8
1
epsilon
90
80
70
60
50
40
30
20
10
100
80
60
40
20
0