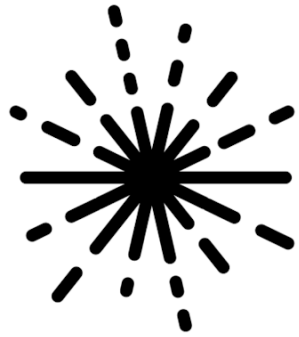


CS208: Applied Privacy for Data Science
DP Foundations: the Gaussian Mechanism

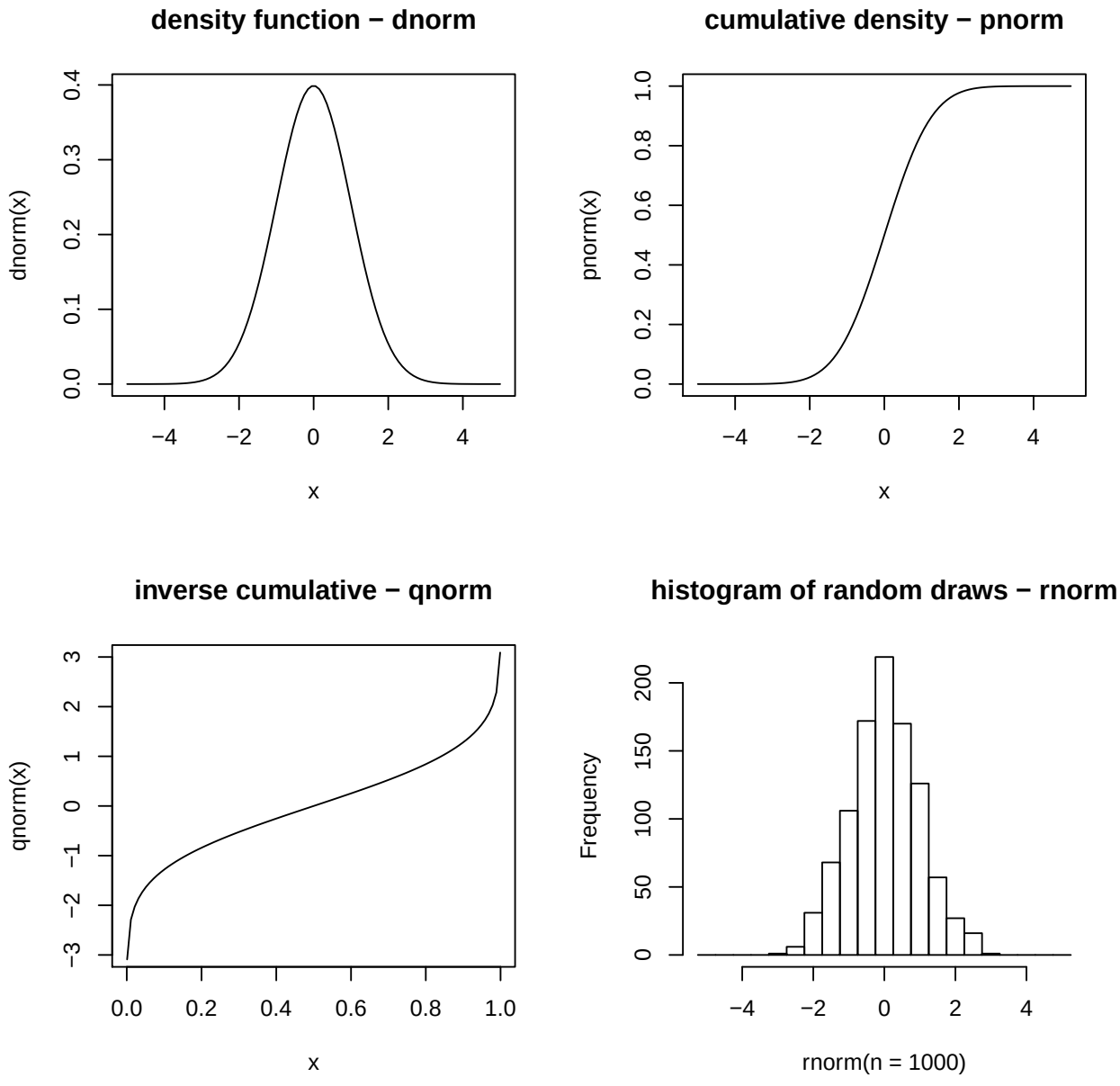
School of Engineering & Applied Sciences
Harvard University

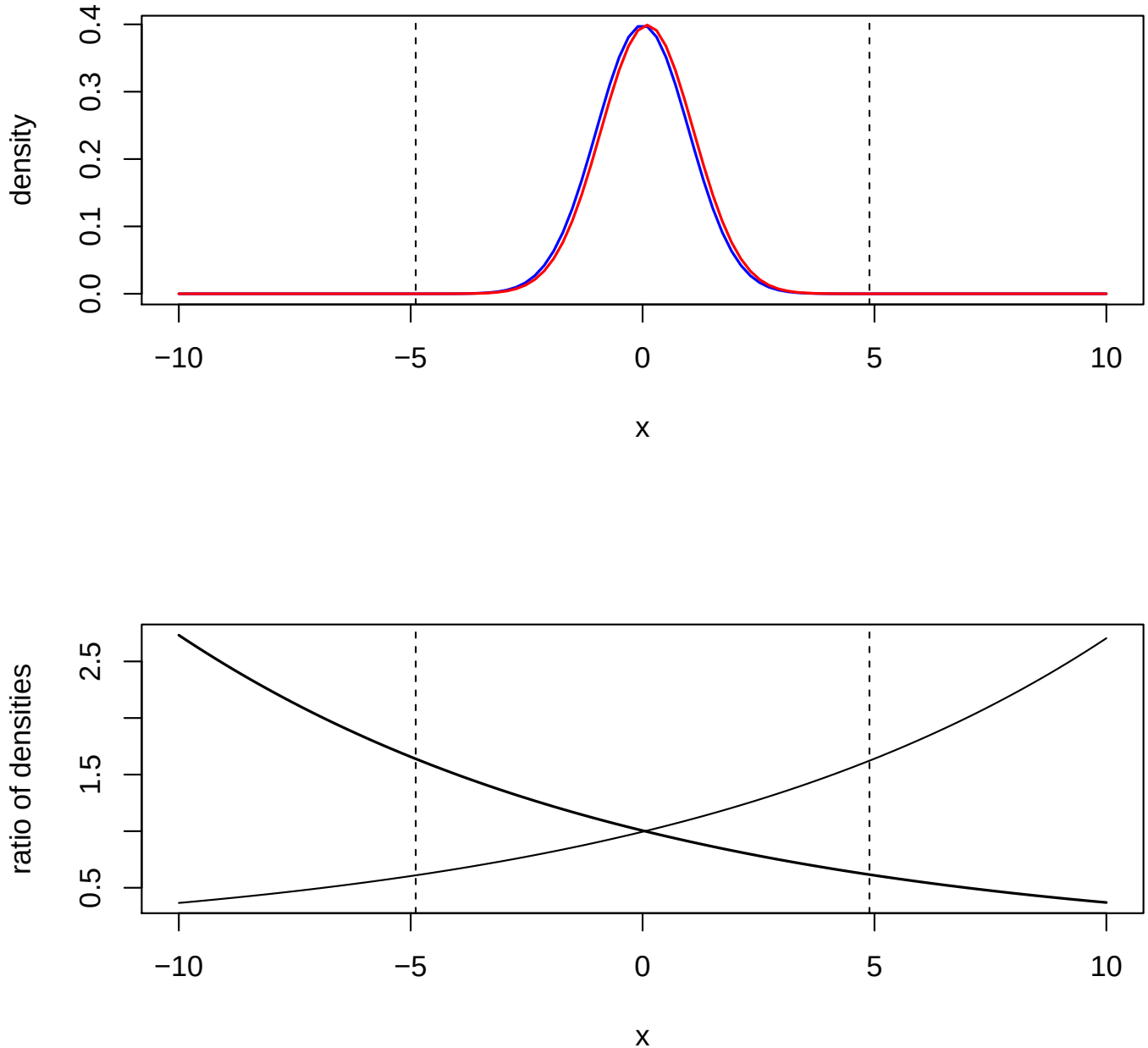
February 17, 2022

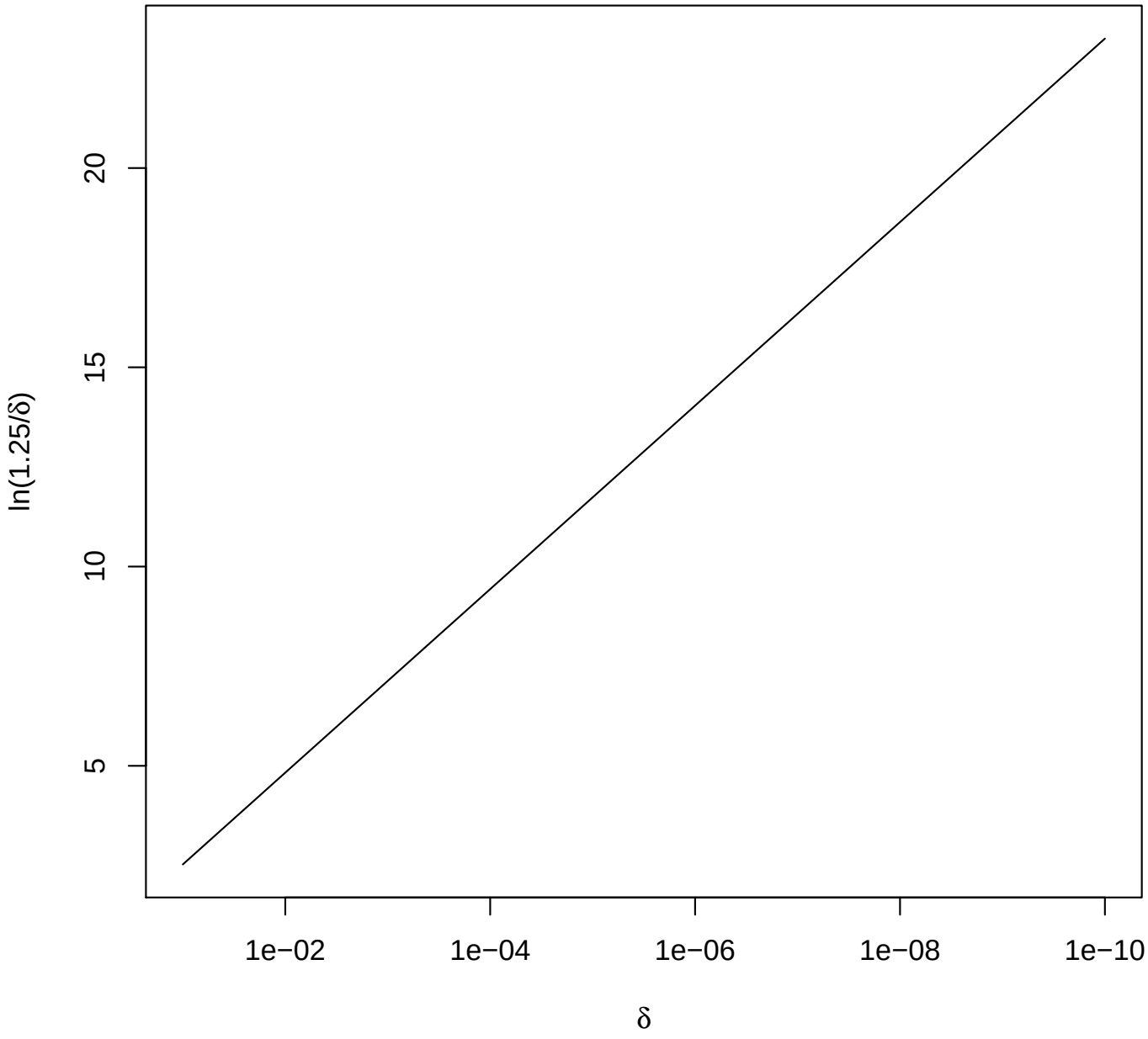
Gaussian Mechanism

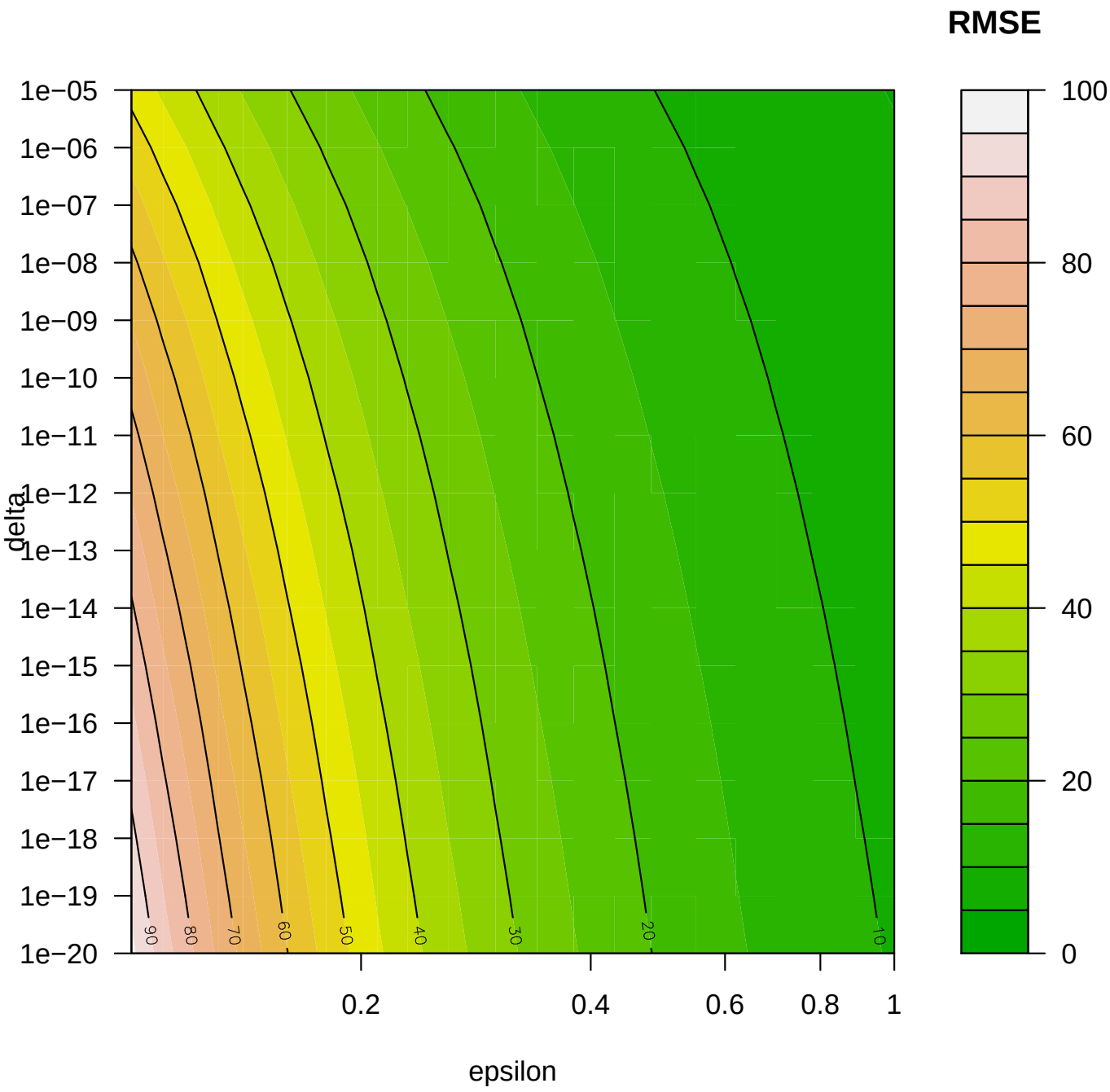
$$M(x, q) = q(x) + \mathcal{N}(0, \sigma^2),$$

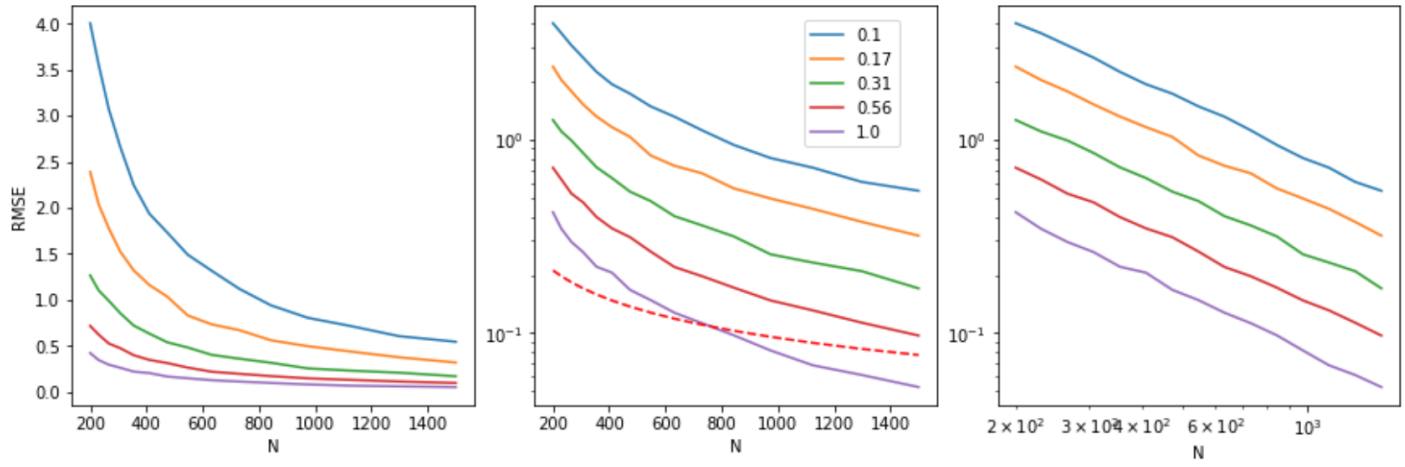
$$\text{for} \quad \sigma = \frac{GS_q}{\epsilon} \sqrt{2 \ln(1.25/\delta)}.$$


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)

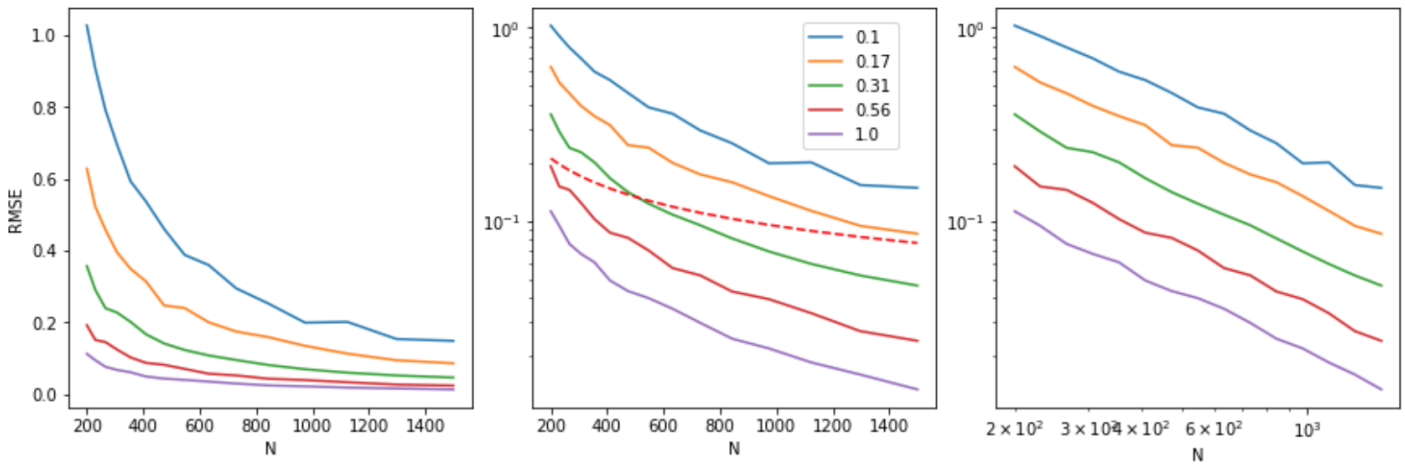

density
0.0
0.1
0.2
0.3
0.4
−10
−5
0
5
10
x
ratio of densities
0.5
1.5
2.5
−10
−5
0
5
10
x


ln(1.25/δ)
5
10
15
20
1e−02
1e−04
1e−06
1e−08
1e−10
δ


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



Gaussian Mechanism

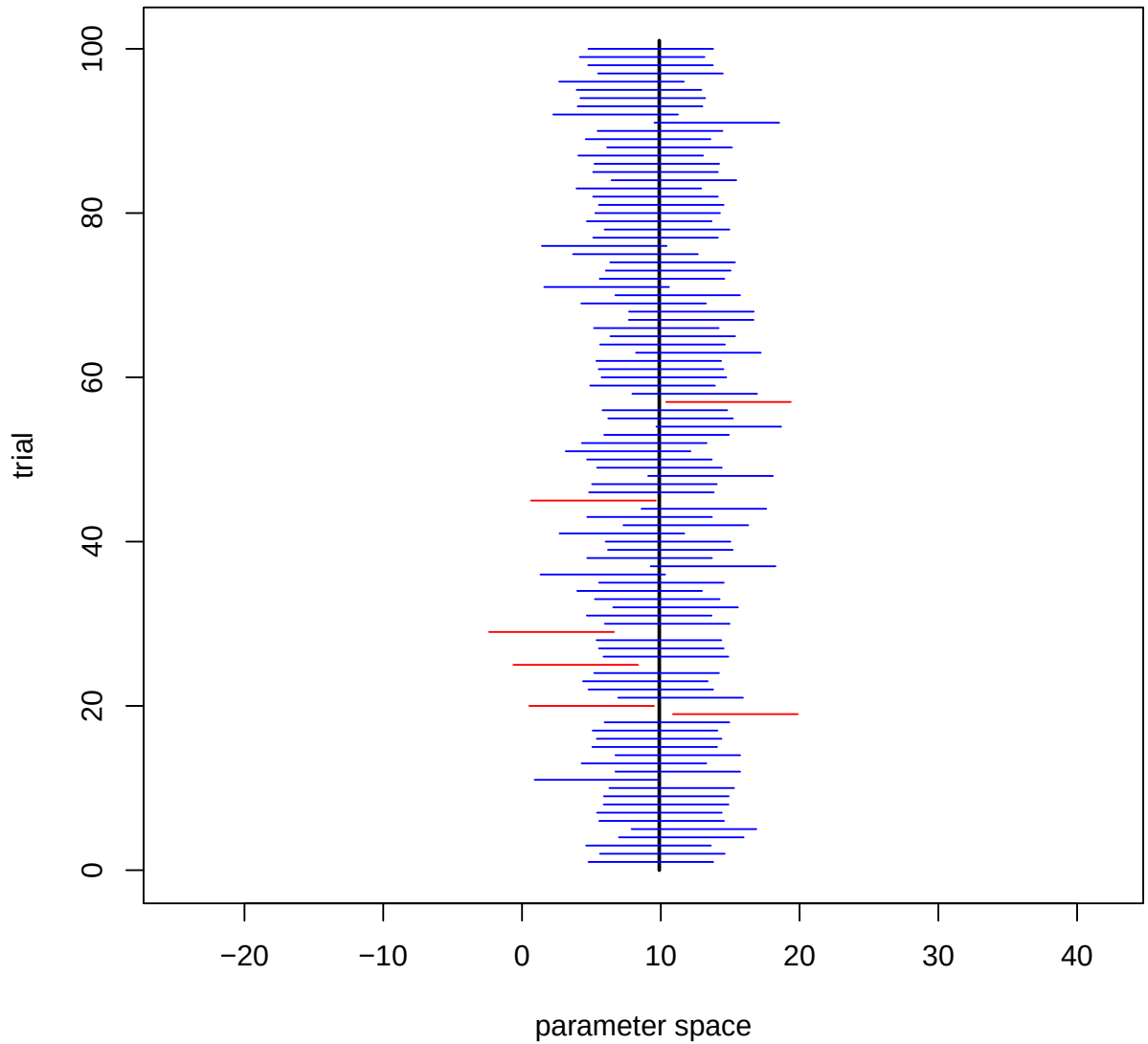


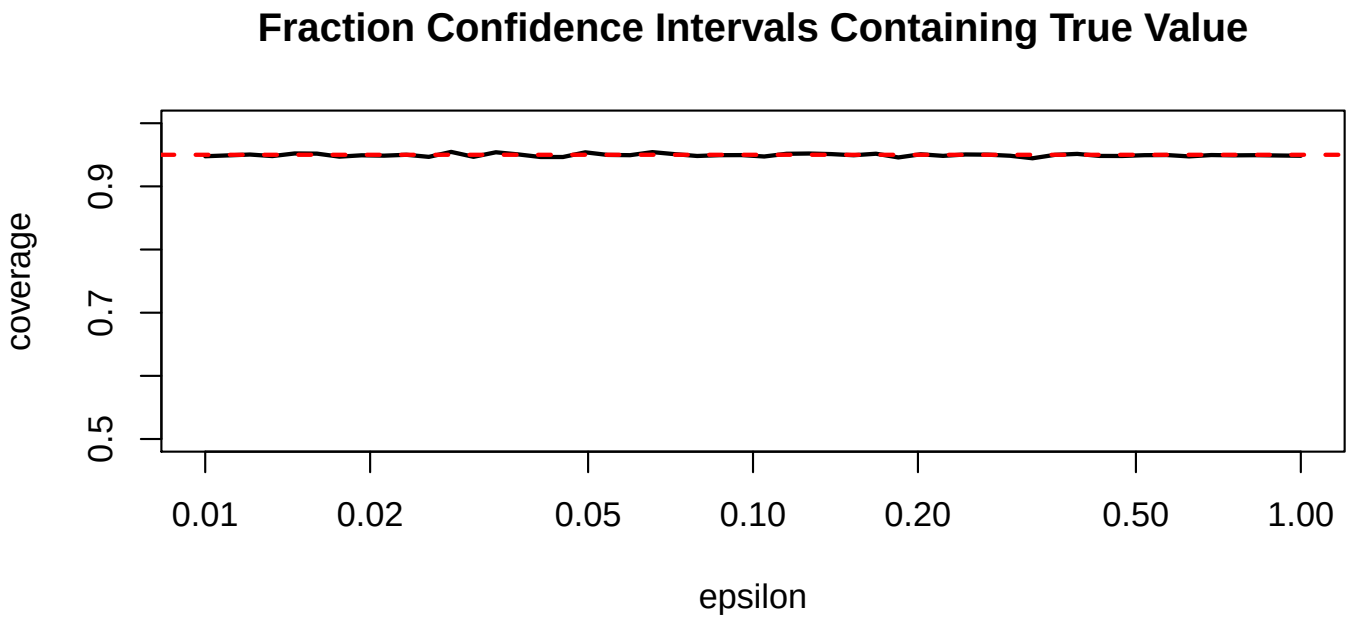
Laplace Mechanism

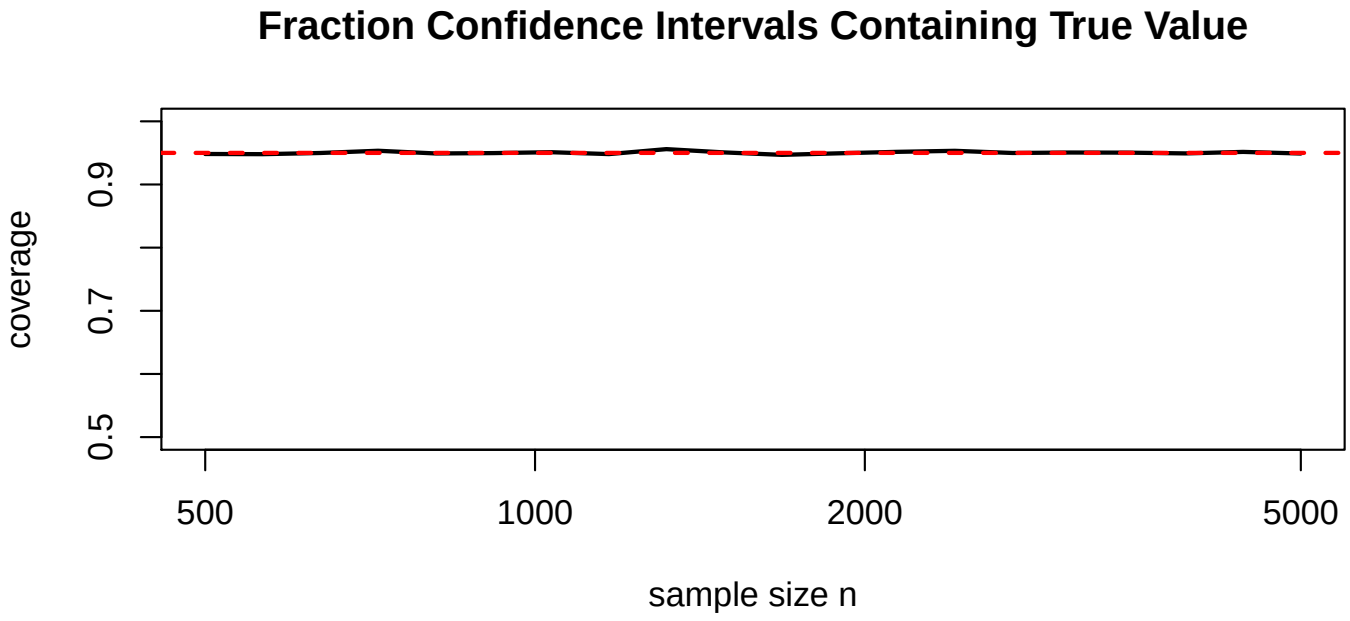
Confidence Interval Construction

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

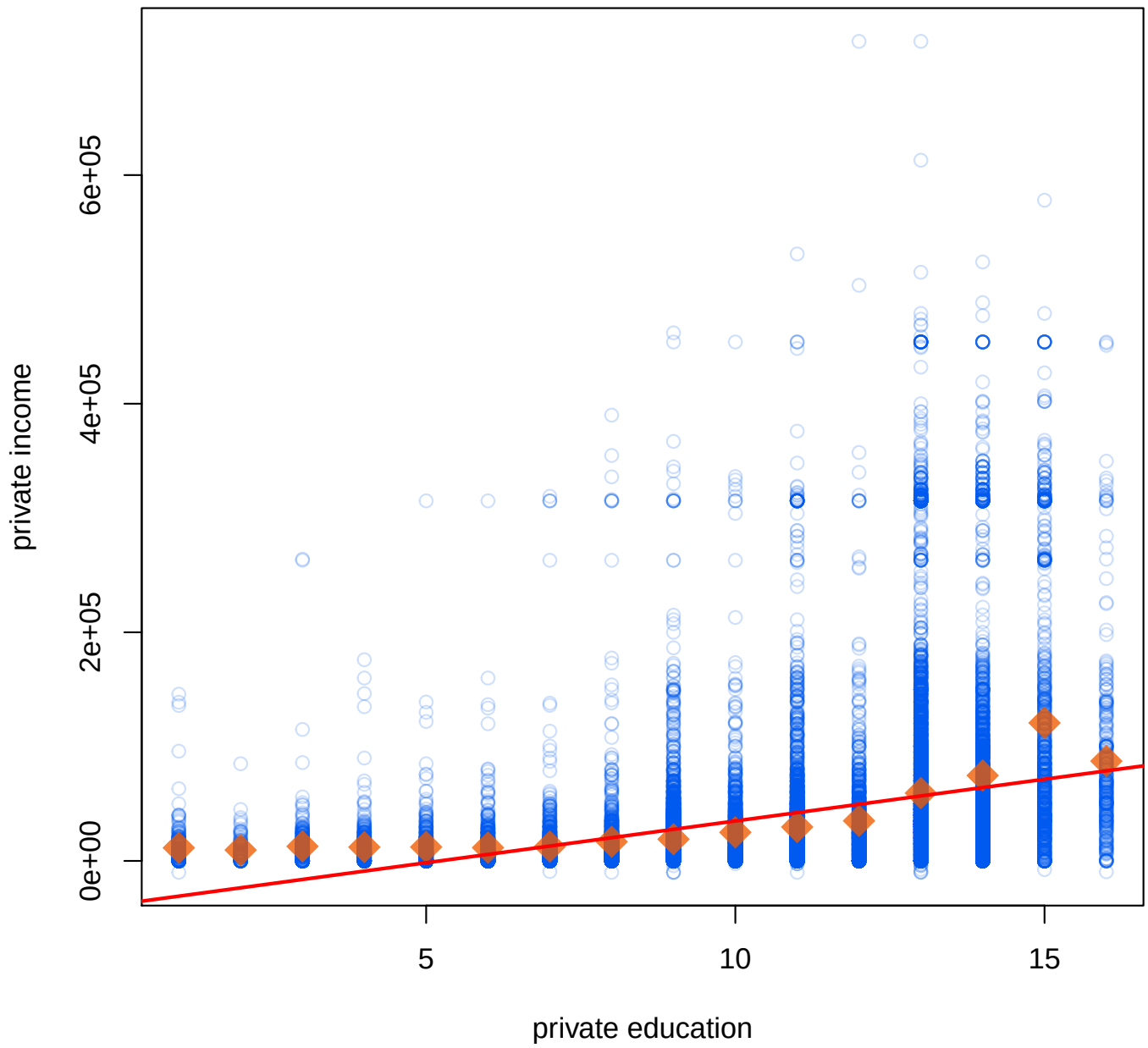

Fraction Confidence Intervals Containing True Value
coverage
0.5
0.7
0.9
0.01
0.02
0.05
0.10
0.20
0.50
1.00
epsilon


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

Education Values

Codebook for Census PUMS 5 Percent CS208 Datasets

`educ`	1:	No schooling completed,
	2:	Nursery school to 4th grade,
	3:	5th grade or 6th grade,
	4:	7th grade or 8th grade,
	5:	9th grade,
	6:	10th grade,
	7:	11th grade,
	8:	12th grade, no diploma,
	9:	High school graduate,
	10:	Some college, but less than 1 year,
	11:	One or more years of college, no degree,
	12:	Associate degree,
	13:	Bachelor's degree,
	14:	Master's degree,
	15:	Professional degree,
	16:	Doctorate degree.


private income
0e+00
2e+05
4e+05
6e+05
5
10
15
private education