

## Gaussian Mechanism:

Add  $N(0, \frac{\epsilon^2}{\sigma^2})$  instead

of  $Lap(\frac{1}{\epsilon})$

$$\frac{e^{-x/\bar{\sigma}^2}}{e^{-(x+1)/\bar{\sigma}^2}} \approx e^{\frac{x}{\bar{\sigma}^2} - \frac{1}{2\bar{\sigma}^2}}$$

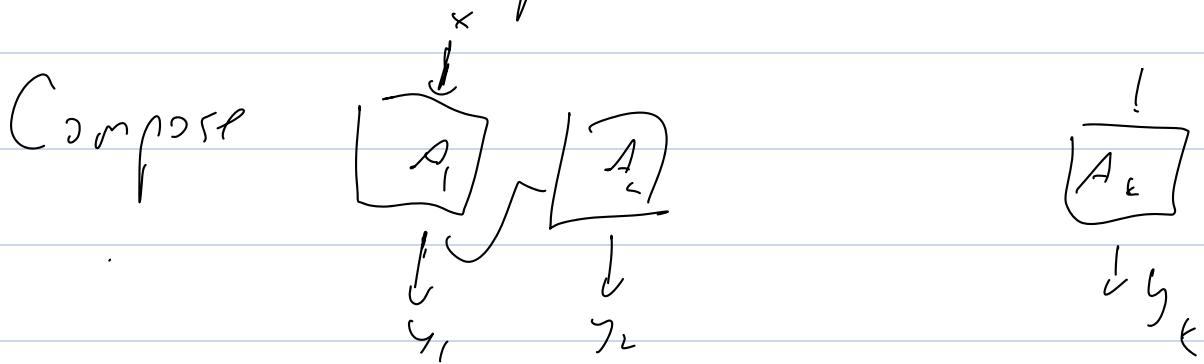
fine if  $x \leq \epsilon \bar{\sigma}^2$

$$\log \frac{1}{\delta} \leq \epsilon \bar{\sigma}^2$$

$$\frac{\log \frac{1}{\delta}}{\epsilon} \leq \bar{\sigma}^2$$



# Advanced Composition



(1)  $\bar{y}$  is  $\epsilon_k$  DP

(2)  $\bar{y}$  is  $\tilde{O}(\epsilon \sum_k + \epsilon^2 k)$ ,  $O(1)$  DP

Proof 2:

Lemma: If  $A$  is  $\epsilon$  DP then

$$\forall D \sim D' \quad KL(A(D) \| A(D')) \leq \epsilon^2$$

Pf:  $\underbrace{P(y)}_{\sim p} e^{\epsilon_y} = 1 \quad \epsilon_y \in [-\epsilon, \epsilon]$

$$1 = \left| \underset{y \sim p}{\mathbb{E}} e^{\epsilon_y} - \mathbb{H} \right| \underset{y \sim p}{\mathbb{E}} \epsilon_y^2 + \underset{y \sim p'}{\mathbb{E}} \epsilon_y^2 + \dots = 1 + \left| \underset{y \sim p}{\mathbb{E}} \epsilon_y + O(\epsilon^2) \right|$$

$$-\epsilon_y = 1 - \frac{p}{q}$$

Data Processing Inequalities

$$KL(y_1, \underbrace{y_k}_{\vdash} \| y'_1, \underbrace{y'_{\vdash}}_{\vdash}) \\ \leq \sum_{i=1}^k KL(y_i \| y'_i)$$

SGD: Given  $x_1, x_2 \rightarrow x_n$   
 $L(\theta, x) \in [0, 1]$   
 Let  $L_i(\theta) := L(\theta, x_i)$

(0)  $\theta_0 \sim \text{random}$

(1) Repeat  $T$  times;

(a) choose  $B \subseteq \mathbb{I}^n$   $|B| = b$

$$(b) \theta_{i+1} = \theta_i - \eta \left( \frac{1}{b} \sum_{i \in B} \nabla L_i(\theta) \right)$$

## DP-SGD

(0)  $\theta_0 \sim \text{random}$

(1) Repeat  $T$  times;

(a) choose  $B \subseteq \mathbb{I}^n$   $|B| = b$

$$(b) \theta_{i+1} = \theta_i - \eta \left[ \frac{1}{b} \sum_{i \in B} \nabla L_i(\theta) + \mathcal{N}(0, \Sigma^{-1}) \right]$$

Thm: DP-SGD is  $(\epsilon, \int)$  DP

pf:  $b = n$  (assume  $C = 1$ )

influence of  $i$

$$\frac{1}{n} \Rightarrow \text{use std } \frac{1}{\sqrt{n}}$$

Composition:

$$\epsilon = \sqrt{T} \cdot \frac{1}{\sqrt{n}}$$

and  $T \approx \frac{1}{\epsilon^2}$

$$\text{std} \approx \frac{\sqrt{\epsilon}}{\sqrt{n}}$$

Smaller  $b$ :

$$\frac{\Pr[\bar{A}(x)]}{\Pr[\bar{A}(x')]} = \frac{b}{n} \frac{\Pr[A(x)]}{\Pr[A(x')]} + 1$$

Cor: for ~~to~~ smaller  $\zeta$

$$\text{use std } \propto \sqrt{\frac{1}{n}}$$

inf  $\frac{1}{b}$  so basic mechanism

is  $\underbrace{\frac{n}{b\sqrt{t}}}_{\text{principle}}$

Subsampling  $\Rightarrow$  mechanism is

$$\frac{b}{n} \cdot \frac{n}{b} \frac{1}{\sqrt{t}} \text{ principle}$$

Composition  $\Rightarrow$  mechanism is

$$\sqrt{t} \cdot \frac{1}{\sqrt{t}} \propto O(1) \text{ principle}$$