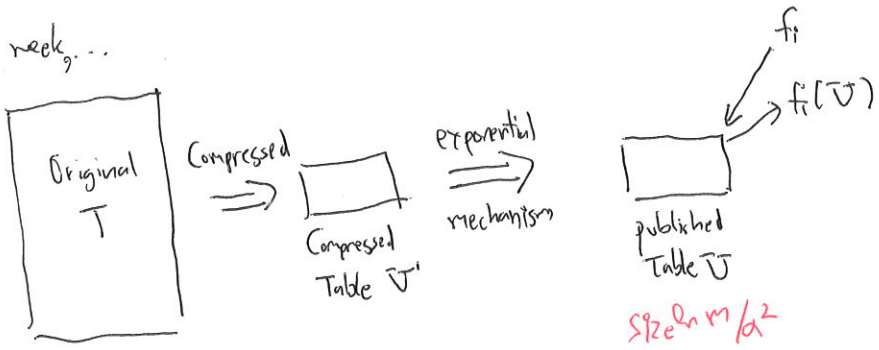
From last week...



Theorem For any T and $f_1, \dots, f_m$, there exists a table $\bar{T}$ with size $\ln m/\alpha^2$ where

$$\max_i |f_i(T) - f_i(\bar{T})| \le \alpha$$

$$\text{Utility}(T, \bar{T}) = -\max_i |f_i(T) - f_i(\bar{T})|$$

There exists $\bar{T}^*$ such that $\text{Utility}(T, \bar{T}^*) \ge -\alpha$

$$OPT \ge -\alpha$$

By the assumption on f_i, we have $\Delta\text{Utility} = \frac{1}{\|T\|}$

Theorem # choices (# possible tables) = (# possible values at each record)$^{\#\text{records}}$ $\ln m/\alpha^2$

Theorem $\Pr[E \le OPT - \frac{2 \cdot \Delta\text{Utility}}{\varepsilon}(\ln(\#\text{choices}) + t)] \le e^{-t}$

when E is utility for publishing table $\bar{T}$.

$$\Pr[E \le -\alpha - \frac{2}{\varepsilon\|T\|}[\ln(\#\text{possible}^{\#\text{records}}) + t]] \le e^{-t} \quad \ln m/\alpha^2 \quad t := -\ln\beta$$

$$\Pr[E \le -\alpha - \frac{2}{\varepsilon\|T\|}(\frac{\ln m}{\alpha^2} \cdot \ln(\#\text{possible}) - \ln\beta)] \le \exp[+\ln\beta] = \beta \quad \sigma := 2\cdot\alpha$$

α : $\sigma/2$; $\frac{\ln m}{\alpha^2}$: $\alpha\sigma/2$; $-\sigma$

$$+\sigma \le -\alpha + \sigma/2 + \frac{2}{\varepsilon\|T\|}[\frac{\ln m}{\alpha^2} \cdot \ln(\#\text{possible}) - \ln\beta] \quad \alpha^2\sigma^2/4$$

$$\sigma/2 \ge \frac{2}{\varepsilon\|T\|}[\frac{\ln m}{\alpha^2\sigma^2/4} \cdot \ln(\#\text{possible}) - \ln\beta]$$

$$\|T\| \ge \frac{4}{\varepsilon\cdot\sigma}[\frac{\ln m}{\sigma^2/4}\ln(\#\text{possible}) - \ln\beta]$$

when $\|T\| \ge \frac{4}{\varepsilon\cdot\sigma}[\frac{\ln m}{\sigma^2/4}\ln(\#\text{possible}) - \ln\beta]$, $\Pr[E \le -\sigma] \le \beta$.

Theorem When T is a table with size $\frac{\ln m}{\varepsilon^3/\alpha^2}$ selected using exponential mechanism, and $|T|$ is large enough.

$$\Pr[E \le \alpha] \le \beta$$

The difference in every result is no more than α.

PAC Learning (Formal Definition)

Definition ~~For any~~ Our algorithm has access to $n = poly(1/\alpha, \log(1/\beta))^{V}$ independent random samples from any distribution $\mathcal{D}$. The algorithm is PAC learning if

$$\Pr[\text{error}(\text{learning output}) > \alpha] \le 1-\beta.$$

for any α and β.

Private PAC Learning Our algorithm has access to $n = poly(1/\varepsilon, 1/\alpha, \log(1/\beta))$ random samples from any distribution $\mathcal{D}$. The algorithm is private PAC learning if

1) The release of learning results is ε-differentially private

2) $\Pr[\text{error}(\text{learning results}) > \alpha] \le 1-\beta$

for any α, β, and ε.

Simple Algorithm (Occam's Razor)

Return learning result with smallest error, for the n samples

* We know from the first class that Occam's Razor is PAC learning.

Algorithm with Differential Privacy

$$Utility(T, \ell) := -[\text{error from learning result } \ell]$$

(error → # misclassification.)

$$h_T(\ell) = \exp\left(\frac{\varepsilon \cdot Utility(T, \ell)}{2 \cdot \Delta Utility}\right), \quad \Delta Utility = 1$$

The error will increase or decrease by 1 if one person change his/her data.

return ℓ with prob. $\frac{h_T(\ell)}{\sum_{\ell'} h_T(\ell')}$

(ℓ → all possible learning results.)

It is clear that this algorithm is ε-differentially private.

[by exponential mechanism]

Theorem By $n = O\left((\ln|\#\text{possible}| + \ln 1/\beta) \cdot \max\left\{\frac{1}{\varepsilon\alpha}, \frac{1}{\alpha^2}\right\}\right)$, we have

$$\Pr[\text{error}(\text{learning output}) > \alpha] \le 1-\beta$$

from the differencial privacy's version of Occam's Razor.

Proof

error (learning output) = Prob. that from $\mathcal{D}$ we will have a misclassification.

difference from definition in mechanism.

$\text{error}_{\text{mech.}}(\text{learning output}) = \#\text{samples} \cdot \text{error}_T(\ell)$

$$\text{error}_T(\text{learning output}) = \frac{\#\text{ samples in } T \text{ that is misclassified}}{\#\text{samples}} = \frac{\sum_{i=1}^{n} X_i}{\#\text{samples}} = S$$

X_i: Is sample i misclassified

expected value of $\text{error}_T(\text{learning output}) = \text{error}(\text{learning output})$

By Chernoff's bound,

$$\Pr[|\underbrace{\text{error}_T(\text{learning output})}_{S} - \underbrace{\text{error}(\text{learning output})}_{\mu}| \ge \rho] \le 2\cdot\exp(-2n\rho^2).$$

for all learning output.

$$\Pr[|\text{error}_T(\ell) - \text{error}(\ell)| \ge \rho \text{ for some learning output } \ell]$$
$$\le \sum_{\ell} \underbrace{\Pr[|\text{error}_T(\ell) - \text{error}(\ell)| \ge \rho]}_{\le 2\cdot\exp(-2n\rho^2)} \le |\#\text{possible output}| \cdot 2\cdot\exp(-2n\rho^2).$$

from now, assume that $|\text{error}_T(\ell) - \text{error}(\ell)| < \rho$ for all ℓ. The probability that we output a particular learning result ℓ is

$$\frac{\exp\left(-\frac{\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell)\right)}{\sum_{\ell'}\exp\left(\frac{-\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell')\right)} \le \frac{\exp\left(-\frac{\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell)\right)}{\max_{\ell'}\exp\left(-\frac{\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell')\right)} = \frac{\exp\left(-\frac{\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell)\right)}{\exp\left(\max_{\ell'} -\frac{\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell')\right)}$$

$\sum_{\ell'}\exp\left(\frac{-\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell')\right) \ge \max_{\ell'}\exp\left(\frac{-\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell')\right)$

$$= \exp\left(-\frac{\varepsilon}{2}\cdot n\,\text{error}_T(\ell) - \max_{\ell'}\left[-\frac{\varepsilon}{2}\cdot n\cdot \text{error}_T(\ell')\right]\right)$$

$$= \exp\left(-\frac{\varepsilon}{2}n\left(\text{error}_T(\ell) - \min_{\ell'}\text{error}_T(\ell')\right)\right)$$

$\min_{\ell'}\text{error}_T(\ell') \le \text{error}_T(\ell^*)$

$\le \underbrace{\text{error}(\ell^*)}_{OPT} + \delta$

$$\le \exp\left(-\frac{\varepsilon}{2}n\left(\text{error}_T(\ell) - OPT - \rho\right)\right)$$

Definition An algorithm is SQ learning if, by $n = \text{poly}(1/\varepsilon)$, SQ, we have a learning result with at most ε errors.

Certain not with prob. $1-\delta$

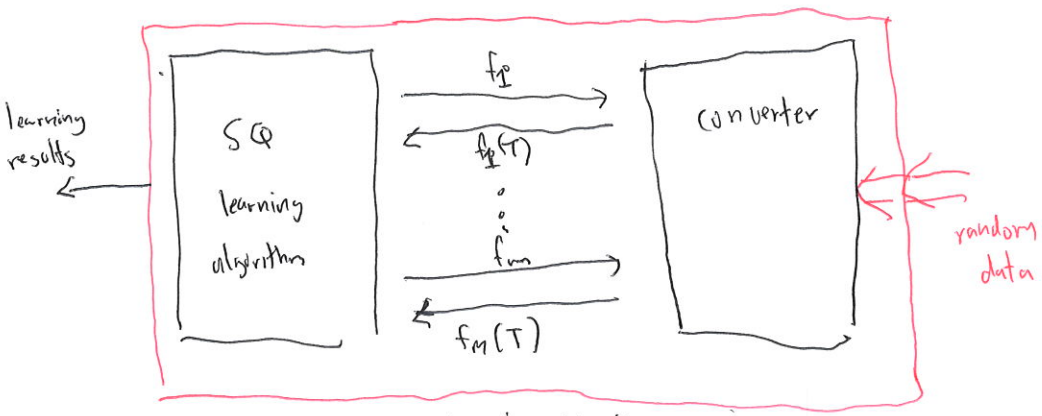
we have a lot of SQ learning algorithms!

Theorem An SQ learning algorithm is also a PAC learning algorithm.

In particular, if SQ learning uses M queries, we will have PAC learning with

$$O\left(\frac{M}{\varepsilon^2}\log\left(\frac{M}{\delta}\right)\right) \text{ queries.}$$

Proof



Converter will take $p = \frac{1}{\alpha^2}\log\left(\frac{M}{\delta}\right)$ ~~to answer~~ random data to answer each query.

~~Each query has. The expected value of all sample data is $f_i(T)$.~~

~~The converter will tell SQ learning algorithm that $f_i(T)$ = average of all samples~~

Suppose that the sample data are $T_{i_1}, \cdots, T_{i_p}$.

The converter will tell SQ learning algorithm that $f_i(T) = \frac{\sum f_i(T_{i_k})}{p}$ (X_k)

($f_i(T)$: S)

By Chernoff's bound, we have

$$\Pr[|S - f_i(T)| > \alpha] \le 2\exp(-2\cdot p\cdot\alpha^2)\cdot 2$$

($f_i(T)$: μ)

$$= \exp\left(-2\cdot\frac{1}{\alpha^2}\cdot\log\left(\frac{M}{\delta}\right)\cdot\alpha^2\right)\cdot 2$$

when

$$= \exp\left(-2\cdot\log\left(\frac{M}{\delta}\right)\right)\cdot 2$$

$$= \exp\left(\log\left(\frac{M}{\delta}\right)\right)^{-2} 2 = \left(\frac{M}{\delta}\right)^{-2}\cdot 2 = 2\frac{\delta^2}{M^2} \le \frac{\delta}{M}$$

when $\frac{\delta}{M} \le 0.5$ which is true when $M \ge 2$

$$\Pr[|S - f_i(T)| \le \alpha] \ge 1 - \frac{\delta}{M}$$

The probability that ℓ such that $\text{error}_T(\ell) \geq \text{OPT}+2\rho$ is returned.

$$\leq \exp\left(-\frac{\varepsilon}{2} n \left(\text{OPT}+2\rho - \rho - \text{OPT}\right)\right) = \exp\left(-\frac{\varepsilon}{2} n\rho\right).$$

The probability that some learning output such that $\text{error}_T(h) \geq \text{OPT}+2\rho$ is retured:

$$\leq \left|\#\text{possible outputs}\right| \cdot \exp\left(-\frac{\varepsilon}{2} n\rho\right)$$

Let $\rho = \alpha/3$.

$$\Pr\left[\left|\text{error}_T(\ell) - \text{error}(\ell)\right| \geq \alpha/3\right] \leq \left|\left|\#\text{possible outputs}\right|\right| \cdot 2\exp\left(-2n\left(\frac{\alpha}{3}\right)^2\right)$$

$$\Pr\left[\text{error}_T(\ell) \geq \text{OPT}+2\alpha/3\right] \leq \left|\left|\#\text{possible outputs}\right|\right| \cdot \exp\left(-\varepsilon/2\, n \cdot \frac{\alpha}{3}\right)$$

$$\Pr\left[\text{error}(\ell) \geq \text{OPT}+\alpha\right] \leq \Pr\left[\left|\text{error}_T(\ell) - \text{error}(\ell)\right| \geq \alpha_3 \text{ or } \text{error}_T(\ell) \geq \text{OPT}+2\alpha/3\right]$$

If both the events does not happen, $\text{error}(\ell) \leq \text{OPT}+\alpha$

$$\leq \Pr\left[\left|\text{error}_T(\ell) - \text{error}(\ell)\right| \geq \alpha/3\right] + \Pr\left[\text{error}_T(\ell) \geq \text{OPT}+2\alpha/3\right]$$

$$\leq \left|\left|\#\text{possible outputs}\right|\right| \cdot 2\exp\left(-2n\frac{\alpha^2}{9}\right) + \left|\left|\#\text{possible outputs}\right|\right| \cdot \exp\left(-\frac{\varepsilon n \alpha}{6}\right)$$

$$= \left|\left|\#\text{possible outputs}\right|\right| \left[2\exp\left(-2n\frac{\alpha^2}{9}\right) + \exp\left(-\frac{\varepsilon n\alpha}{6}\right)\right]$$

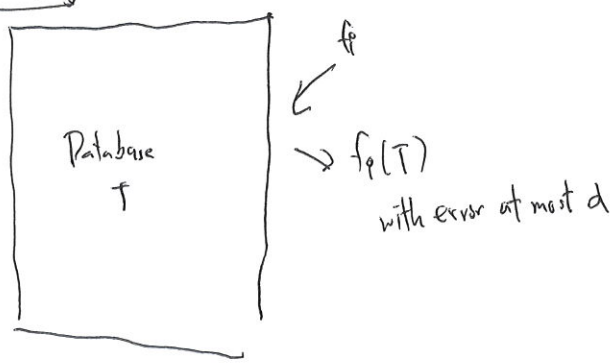
β

$$\left|\left|\#\text{possible outputs}\right|\right| \left[2\exp\left(-2n\frac{\alpha^2}{9}\right) + \exp\left(\frac{-\varepsilon n\alpha}{6}\right)\right] \leq \beta \quad \text{when}$$

$$n = O\left(\left(\ln\left|\#\text{possible}\right| + \ln 1/\beta\right) \cdot \max\left\{\frac{1}{\varepsilon\alpha}, \frac{1}{\alpha^2}\right\}\right)$$

Statistical Query Learning (SQ learning)

Statistical Query



$$f_i(T) = \sum_j f_i(T_j) / \|T\|$$

We almost obtain SQ ~~learning~~ query from small DB algorithm.

The error $\leq \alpha$ is obtained with prob. $1-\rho$

$$\Pr\left[|S - f_i(T)| > \alpha \text{ for some } i\right] \le \sum_i \Pr\left[|S - f_i(T)| > \alpha\right]$$

$$\le M \cdot \frac{\delta}{M} = \delta$$

$$\Pr\left[|S - f_i(T)| \le \alpha \text{ for all } i\right] \ge 1 - \delta$$

SQ learning algorithm will work properly.

$$\Pr\left[\begin{array}{l}\text{We will have learning results}\\ \text{with error} \le \varepsilon\end{array}\right] \ge 1 - \delta$$

→ PAC learning

By Theorem We can have a private PAC learning algorithm from SQ learning algorithm.

↳ ε-differential private.

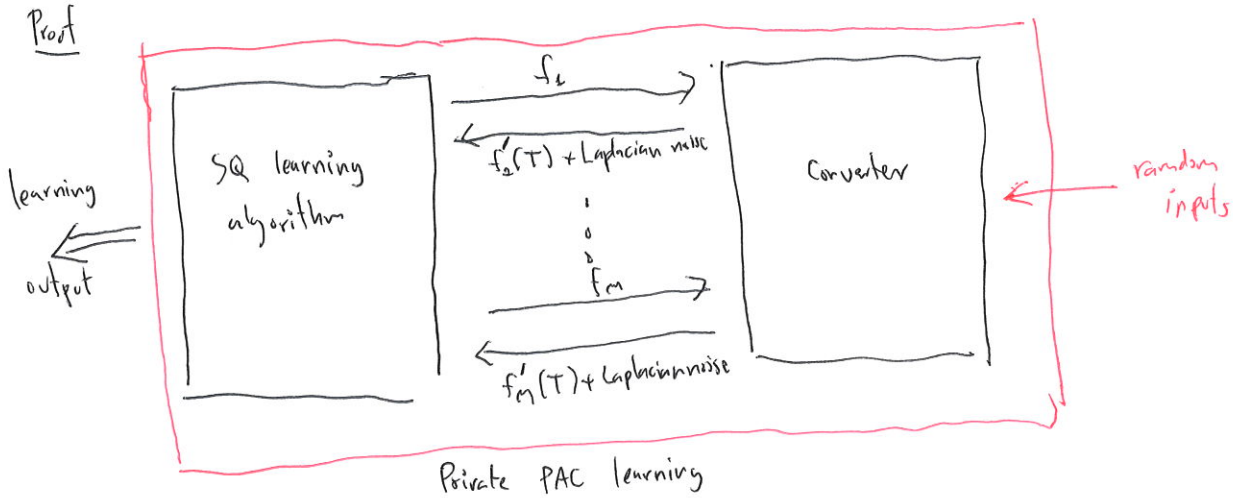
If we need M queries in the SQ learning algorithm, we need

$$O\left(\left[\frac{M}{\varepsilon\alpha} + \frac{M}{\alpha^2}\right] \cdot \log\left(\frac{M}{\delta}\right)\right) = 2\left\{\frac{M}{\varepsilon\alpha} + \frac{M}{\alpha^2}\right\} \cdot \log\left(\frac{M \cdot 4}{\delta}\right) := p$$

queries for the private PAC learning algorithm

$\frac{M}{\varepsilon\alpha}$: we have this term to have ε-differential private

Proof



For each answer, the converter will use $2\left\{\frac{1}{\varepsilon\alpha} + \frac{1}{\alpha^2}\right\} \log\left(\frac{4M}{\delta}\right)$.

By Chernoff Bound,

$$\Pr\left[|f_i(T) - f_i'(T)| \ge \frac{\alpha}{2}\right] \le 2 \cdot \exp\left(-2 \cdot 2\left\{\frac{1}{\varepsilon\alpha} + \frac{1}{\alpha^2}\right\} \log\left(\frac{4M}{\delta}\right)\left(\frac{\alpha}{2}\right)^2\right)$$

$$\le 2 \cdot \exp\left(-\frac{1}{\alpha} \log\left(\frac{4M}{\delta}\right)\alpha\right)$$

$$= 2 \cdot \frac{\delta}{4M} = \frac{\delta}{2M}$$

$f_i(T)$: M, $f_i'(T)$: S

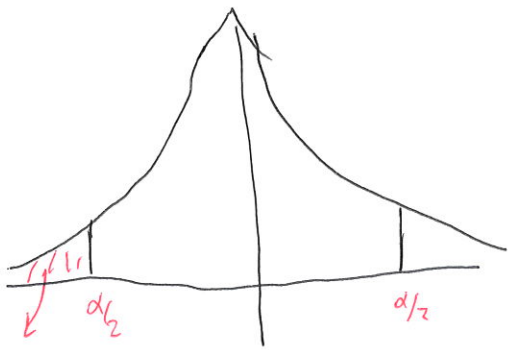
Added laplacian noise, with $\left(\varepsilon' = \frac{\varepsilon}{M}\right)$ - differential privacy.

- We publish M information. each with $\frac{\varepsilon}{M}$ -differential privacy.

We will have $\frac{\varepsilon}{M} \times M = \varepsilon$ - differentially private mechanism.

∴ The noise is $Lap\left(\frac{GS(f)}{\varepsilon}\right)$. $GS(f) = \frac{1}{P}$. The noise is then $Lap\left(\frac{1}{P\varepsilon/M}\right)$

$$= Lap\left(\frac{1}{2\left\{\frac{1}{1-\alpha} + \frac{1}{\alpha^2}\right\} \cdot \log\left(\frac{4M}{\delta}\right) \cdot \frac{\varepsilon}{e}}\right) \leq Lap\left(\frac{1}{2\left\{\frac{1}{\varepsilon\alpha}\right\} \cdot \log\left(\frac{4M}{\delta}\right) \cdot \varepsilon}\right) = Lap\left(\frac{\alpha}{2 \cdot \log\left(\frac{4M}{\delta}\right)}\right)$$



$\exp(-\alpha/2/b)$

$$Pr[\text{Noise} \geq \alpha/2] = 2 \cdot \exp(-\alpha/2/b) = 2 \cdot \exp\left(\frac{-\alpha/2}{\frac{\alpha}{2} \cdot \frac{1}{\log\left(\frac{4M}{\delta}\right)}}\right)$$

$$= 2 \cdot \exp\left(-\log\left(\frac{4M}{\delta}\right)\right)$$

$$= \frac{2 \cdot \delta}{4M} = \frac{\delta}{2M}$$

$$Pr[|f_i'(T) - f_i(T)| \geq \alpha/2] \leq \frac{\delta}{2M}$$

$$Pr[|\text{value given to SQ} - f_i(T)| \geq \alpha] \leq Pr[|f_i'(T) - f_i(T)| \geq \alpha/2 \text{ or Noise} \geq \alpha/2]$$

$$\leq Pr[|f_i'(T) - f_i(T)| \geq \alpha/2] + Pr[\text{Noise} \geq \alpha/2]$$

$$= \delta/2M + \frac{\delta}{2M} = \frac{\delta}{M}$$

$$Pr[|\text{value given to SQ} - f_i(T)| \leq \alpha] \geq 1 - \frac{\delta}{M}$$

$$Pr[\text{For all } i, |\text{value given to SQ} - f_i(T)| \geq \alpha] \geq 1 - \delta$$

∎