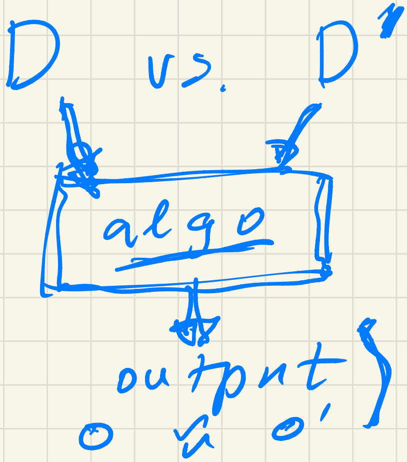
- anonymity (e.g. K-anon.)
- aggregation
- "no harm"

- DP: no harm to you specifically due to your data

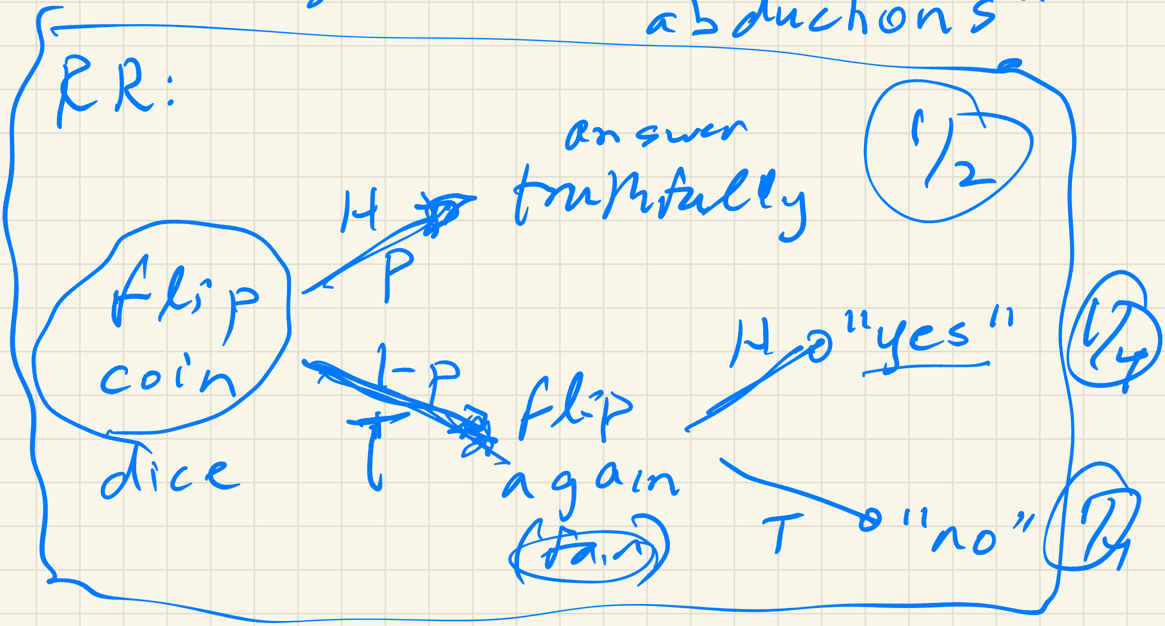


Randomized Response

- embarrassing questions:

"Have you ever shoplifted?"

"Do you believe in alien abductions"



Utility/accuracy analysis

- population of size n all follows Mg's RR
- use $\{\underline{y}, \underline{n}\}$ as underlying true answers & $\{\underline{\text{"y"}}, \underline{\text{"n"}}\}$ as responses to RR.
- $\underline{t = \text{fraction of pop. with truth} = y}$

$$\Pr[\text{"}\underline{y}\text{"} \mid \underline{y}] = \underset{H}{(1/2)} \cdot 1 + \underset{T}{(1/2)} \underset{\text{"y"}}{(1/2)}$$

$$= 1/2 + 1/4 = \boxed{3/4} \leftarrow$$

$$\Pr[\text{"y"} \mid \underline{n}] = \underset{H}{(1/2)} \cdot 0 + \underset{T}{(1/2)} \underset{\text{"y"}}{(1/2)}$$

$$= \boxed{1/4} \leftarrow$$

$$\boxed{\Pr[\text{"y"}]} = t\left(\tfrac{3}{4}\right) + (1-t)\left(\tfrac{1}{4}\right)$$

$$= \tfrac{1}{4} + \tfrac{t}{2}$$

frac of "y" responses out

"y"

$$\Pr[\text{"y"}] = q$$

$$\hat{q} = \tfrac{1}{4} + t/2$$

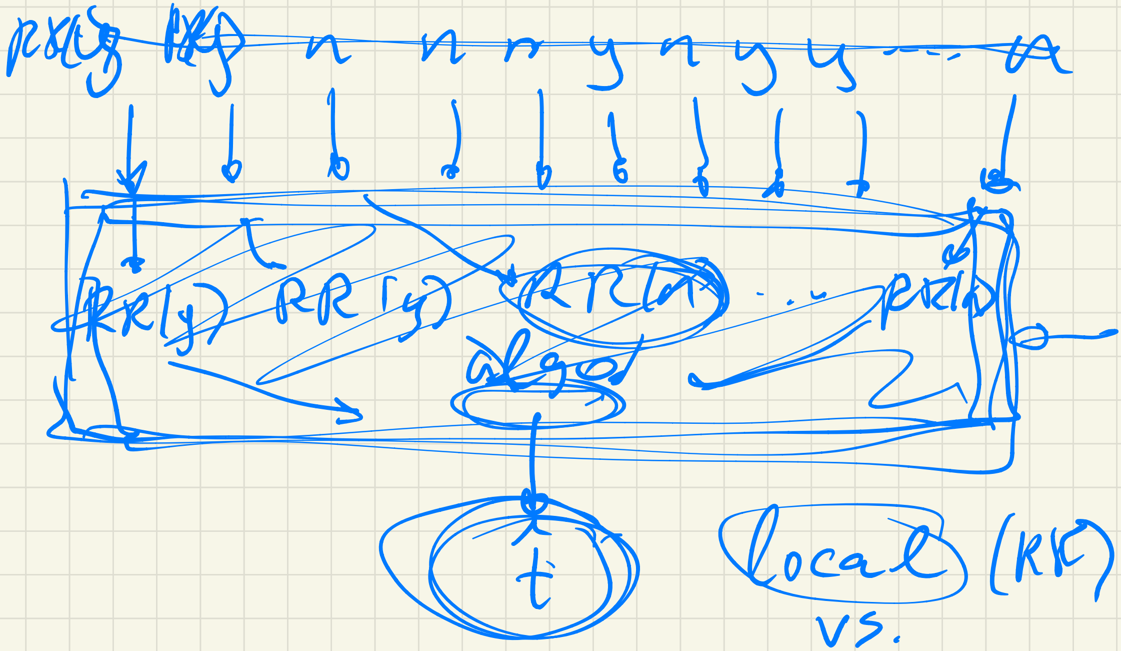
solve for t

$\hat{q}$ = estimate of q from running exp. n times

Fact. With very high prob.

$$|\hat{q} - q| \le 1/\sqrt{n} \to 0$$

$$\boxed{t \pm 1/\sqrt{n}}$$



local (RR)

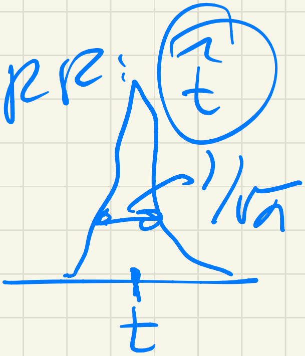
vs.

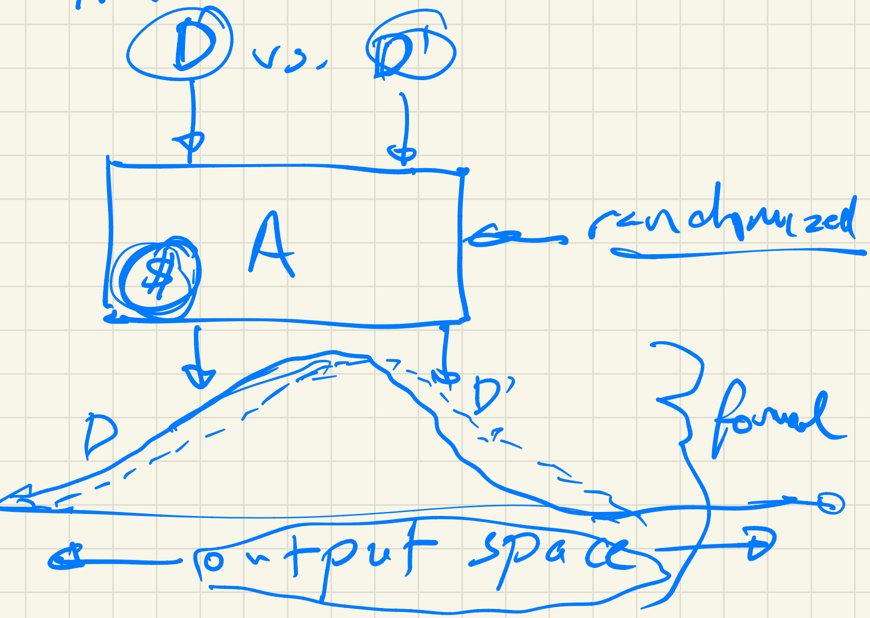
centralized

DP.

Definition of DP

We say than an algorithm A satisfies ε-DP if for <u>any</u> pair of <u>neighboring</u> inputs/DBs <u>D & D'</u> if:





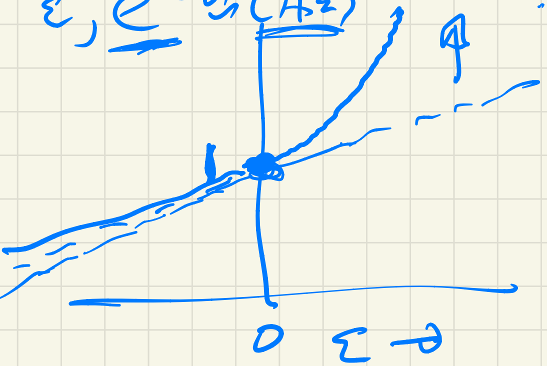
Formally:

- Let $A(D)$, $A(D')$ denote the random output of A under D, D'. We want that for any subset S of the output space of A

"bad"

$$\Pr[A(D) \in S] \le e^{\varepsilon} \Pr[A(D') \in S]$$

For small ε, $e^{\varepsilon} \approx (1+\varepsilon)$



$$\boxed{e^{-\varepsilon} \Pr[A(D') \in S] \le \Pr[A(D) \in S] \le e^{\varepsilon} \Pr[A(D') \in S]}$$