

Name	Chosen Party
Alice	Gyudon Party
Bob	Melon-pan Party
Charles	Melon-pan Party
Doe	Melon-pan Party

→ This village chooses Melon-pan Party
private information

public information

- We cannot add noise to the party's name.

Utility of telling that the winning party is Melon-pan = # persons voted for Melon-pan - # persons voted for Gyudon

Utility of reporting that the winning party is Gyudon = # persons voted for Gyudon - # persons voted for Melon-pan

* If the vote differences is not large, it is somewhat ok to have an incorrect report. [The utility is then not that different.]

* If the differences is large, we will ^{definitely} report the correct choice.

$$\Delta \text{Utility} := \max_{T, T': \text{neighboring tables}} \max_P \left| \text{Utility}(T, P) - \text{Utility}(T', P) \right|$$

↑
all possible reports

When one person switches from Gyudon party to Melon-pan party;

- # melon-pan increased by 1
- # gyudon decreased by 1.

Utility of reporting Melon-pan increased by 2!!!

$$\Delta \text{Utility} = 2$$

$$h_T(p) := \exp\left(\frac{\epsilon \cdot \text{Utility}(T, p)}{2 \Delta \text{Utility}}\right) \Rightarrow \text{The report } p \text{ that has higher utility will have larger } h_T(p)$$

When $\Delta \text{Utility}$ is large all $h_T(p)$ will be one.

$$P_T[\text{Out}(T) = p] = \frac{h_T(p)}{\sum_{p'} h_T(p')} \Rightarrow \text{With normalization, we almost have a uniform distribution.}$$

normalization

Ex In our table, T

$$\text{Utility}(T, \text{Melon-pan}) = 2 \quad \epsilon = 0.1$$

$$\text{Utility}(T, \text{Gyudon}) = -2$$

$$h_T(\text{Melon-pan}) = \exp\left(\frac{0.1 \cdot 2}{2 \cdot 2}\right) = 1.05$$

$$h_T(\text{Gyudon}) = \exp\left(\frac{0.1 \cdot (-2)}{2 \cdot 2}\right) = 0.95$$

$$P_T[\text{Out}(T) = \text{Melon-pan}] = \frac{1.05}{1.05 + 0.95} = 0.525$$

Almost same

$$P_T[\text{Out}(T) = \text{Gyudon}] = \frac{0.95}{1.05 + 0.95} = 0.475$$

If # Melon-pan - # Gyudon = 50,

$$\text{Utility}(T, \text{Melon-pan}) = 50$$

$$\text{Utility}(T, \text{Gyudon}) = -50$$

$$h_T(\text{Melon-pan}) = \exp\left(\frac{0.1 \cdot 50}{2 \cdot 2}\right) = 3.49$$

$$h_T(\text{Gyudon}) = \exp\left(\frac{0.1 \cdot (-50)}{2 \cdot 2}\right) = 0.29$$

$$P_T[\text{Out}(T) = \text{Melon-pan}] = \frac{3.49}{3.49 + 0.29} = 0.92$$

$$P_T[\text{Out}(T) = \text{Gyudon}] = \frac{0.29}{3.49 + 0.29} = 0.08$$

Theorem [Privacy of exponential mechanism] For all p , neighboring tables T and T'

$$e^{-\epsilon} \leq \frac{\Pr[\text{Out}(T)=p]}{\Pr[\text{Out}(T')=p]} \leq e^{\epsilon}$$

[exponential mechanism is ϵ -differentially private]

Proof

$$\frac{\Pr[\text{Out}(T)=p]}{\Pr[\text{Out}(T')=p]} = \frac{h_T(p) / \sum_{p'} h_T(p')}{h_{T'}(p) / \sum_{p'} h_{T'}(p')} = \frac{h_T(p)}{h_{T'}(p)} \cdot \frac{\sum_{p'} h_T(p')}{\sum_{p'} h_{T'}(p')}$$

$$\frac{h_T(p)}{h_{T'}(p)} = \frac{\exp\left(\frac{\epsilon \cdot \text{Utility}(T,p)}{2 \Delta \text{Utility}}\right)}{\exp\left(\frac{\epsilon \cdot \text{Utility}(T',p)}{2 \cdot \Delta \text{Utility}}\right)} = \exp\left[\frac{\epsilon \cdot \text{Utility}(T,p)}{2 \cdot \Delta \text{Utility}} - \frac{\epsilon \cdot \text{Utility}(T',p)}{2 \cdot \Delta \text{Utility}}\right]$$

$$= \exp\left[\frac{\epsilon}{2 \cdot \Delta \text{Utility}} [\text{Utility}(T,p) - \text{Utility}(T',p)]\right]$$

$\Delta \text{Utility} \geq \text{Utility}(T,p) - \text{Utility}(T',p)$
for all T, T' and p

$$\leq \exp\left[\frac{\epsilon}{2 \cdot \Delta \text{Utility}} \cdot \Delta \text{Utility}\right]$$

$$= \exp\left(\frac{\epsilon}{2}\right)$$

$$\frac{\sum_{p'} h_{T'}(p')}{\sum_{p'} h_T(p')} \leq \max_{p'} \frac{h_{T'}(p')}{h_T(p')} \leq \exp\left(\frac{\epsilon}{2}\right)$$

$$\frac{\Pr[\text{Out}(T)=p]}{\Pr[\text{Out}(T')=p]} = \frac{h_T(p)}{h_{T'}(p)} \cdot \frac{\sum_{p'} h_T(p')}{\sum_{p'} h_{T'}(p')} \leq \exp\left(\frac{\epsilon}{2}\right) \cdot \exp\left(\frac{\epsilon}{2}\right) = \exp(\epsilon)$$

Using the similar idea, we have

$$\frac{\Pr[\text{Out}(T')=p]}{\Pr[\text{Out}(T)=p]} \leq e^{\epsilon}$$

That's why

$$e^{-\epsilon} \leq \frac{\Pr[\text{out}(T)=p]}{\Pr[\text{Out}(T')=p]} \leq e^{\epsilon}$$

□

How good the mechanism is?

Theorem Let OPT be the utility obtained from the correct report, and

$$[OPT := \max_{p'} \text{Utility}(T, p')]$$

E is the utility obtained from the exponential mechanism. We have. different from the best

$$\Pr \left[E \leq OPT - \frac{z \cdot \Delta \text{Utility}}{\epsilon} (\ln(\# \text{choices}) + t) \right] \leq e^{-t}$$

↑ more different

↓ more likely that we do not fall into the situation.

Proof

$$\Pr[E \leq c] = \sum_{p'} \Pr_{\#}[\text{Out}(T) = p' \mid \text{Utility}(T, p') \leq c]$$

$$= \sum_{p': \text{Utility}(T, p') \leq c} \frac{h_T(p')}{\sum_{p'} h_T(p')}$$

$$= \frac{1}{\sum_{p'} h_T(p')} \left[\sum_{p': \text{Utility}(T, p') \leq c} \exp\left(\frac{\epsilon \text{Utility}(T, p')}{z \cdot \Delta \text{Utility}}\right) \right]$$

#times sum is less than # choices.

$$\leq \frac{1}{\sum_{p'} \exp\left(\frac{\epsilon \text{Utility}(T, p')}{z \cdot \Delta \text{Utility}}\right)} \sum_{p': \text{Utility}(T, p') \leq c} \exp\left(\frac{\epsilon c}{z \cdot \Delta \text{Utility}}\right)$$

$$\leq \exp\left(\frac{\epsilon OPT}{z \cdot \Delta \text{Utility}}\right)$$

$$\leq \frac{1}{\exp\left(\frac{\epsilon OPT}{z \cdot \Delta \text{Utility}}\right)} \cdot |\# \text{choices}| \cdot \exp\left(\frac{\epsilon c}{z \cdot \Delta \text{Utility}}\right)$$

$$= |\# \text{choices}| \cdot \exp\left(\frac{\epsilon c}{z \cdot \Delta \text{Utility}} - \frac{\epsilon OPT}{z \cdot \Delta \text{Utility}}\right)$$

$$\leq \exp\left[\ln(\# \text{choices}) + \frac{\epsilon}{z \cdot \Delta \text{Utility}} (c - OPT) \right]$$

$$= |\# \text{choices}| \cdot \exp\left(\frac{\epsilon}{z \cdot \Delta \text{Utility}} (c - OPT)\right)$$

□