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

public information

→ This village chooses Melon-pan Party

private 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 report the correct choice. (definitely)

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

P: 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!!!

$\Delta\text{Utility} = 2$

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

$\Rightarrow$ When ΔUtility is large all $h_T(p)$ will be one.

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

↳ normalization

Ex In our table, T

Utility $(T,$ Melon-pan$) = 2$ $\quad \varepsilon = 0.1$

Utility $(T,$ Gyudon$) = -2$

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

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

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

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

If #Melon-pan − #Gyudon $= 50$,

Utility $(T,$ Melon-pan$) = 50$

Utility $(T,$ Gyudon$) = -50$.

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

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

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

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

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

$$e^{-\varepsilon} \le \frac{Pr[Out(T)=p]}{Pr[Out(T')=p]} \le e^{\varepsilon}$$

[exponential mechanism is ε-differentially private]

Proof

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

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

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

$\Delta Utility \ge Utility(T,p) - Utility(T',p)$ for all T, T' and p

$$\le \exp\left[\frac{\varepsilon}{2 \cdot \Delta Utility} \cdot \Delta Utility\right]$$

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

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

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

Using the similar idea, we have

$$\frac{Pr[Out(T')=p]}{Pr[Out(T)=p]} \le e^{\varepsilon}$$

That's why

$$e^{-\varepsilon} \le \frac{Pr[Out(T)=p]}{Pr[Out(T')=p]} \le e^{\varepsilon}$$

//

How good the mechanism is?

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

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

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

different from the best

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

more different

more likely that we do not fall into the situation.

Proof

$$\Pr[E \le c] = \sum_{p' : \text{Utility}(T,p') \le c} \Pr[\text{Out}(T) = p']$$

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

$$= \frac{1}{\sum_{p'} h_T(p')} \left| \sum_{p' : \text{Utility}(T,p') \le c} \right| \exp\left(\frac{\varepsilon \, \text{Utility}(T,p')}{2 \cdot \Delta \text{Utility}} \right)$$

($\text{Utility}(T,p') \le c$)

times sum is less than # choices.

$$\le \frac{1}{\sum_{p'} \exp\left(\frac{\varepsilon \, \text{Utility}(T,p')}{2 \Delta \text{Utility}} \right)} \sum_{p' : \text{Utility}(T,p') \le c} \exp\left(\frac{\varepsilon c}{2 \Delta \text{Utility}} \right)$$

($\text{Utility}(T,p') \ge OPT$)

$$\le \exp\left(\frac{\varepsilon \, OPT}{2 \Delta \text{Utility}} \right)$$

$$\le \frac{1}{\exp\left(\frac{\varepsilon \, OPT}{2 \Delta \text{Utility}} \right)} \cdot |\#\text{choices}| \cdot \exp\left(\frac{\varepsilon c}{2 \Delta \text{Utility}} \right)$$

$$= |\#\text{choices}| \cdot \exp\left(\frac{\varepsilon c}{2 \Delta \text{Utility}} - \frac{\varepsilon \, OPT}{2 \Delta \text{Utility}} \right)$$

$$c = OPT - \frac{2 \cdot \Delta \text{Utility}}{\varepsilon} \left[\ln(\#\text{choices}) + t \right]$$

$$= |\#\text{choices}| \cdot \exp\left(\frac{\varepsilon}{2 \Delta \text{Utility}} (c - OPT) \right)$$

$\le$

$$= |\#\text{choices}| \cdot \exp\left(\frac{\varepsilon}{2\Delta\text{Utility}}\left[OPT - \frac{2\cdot\Delta\text{Utility}}{\varepsilon}(\ln(\#\text{choices}) + t) - OPT\right]\right)$$

$$= |\#\text{choices}| \cdot \exp\left(\frac{\varepsilon}{2\Delta\text{Utility}}\left[-\frac{2\Delta\text{Utility}}{\varepsilon}(\ln(\#\text{choices}) + t)\right]\right)$$

$$= |\#\text{choices}| \cdot \exp(-\ln(\#\text{choices}) - t)$$

$$= |\#\text{choices}| \cdot \exp(-\ln(\#\text{choices})) \cdot \exp(-t)$$

$$= |\#\text{choices}| \cdot \frac{1}{|\#\text{choices}|} \cdot \exp(-t) = \exp(-t) \quad \square$$

Bonus Question

We will continue to work on minimum weight function.

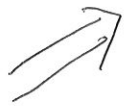
Suppose that the minimum weight is always between 30 to 40,
and we always say that the minimum weight is either 30 or 40.

- Design utility function
- Discuss why your utility function works for exponential mechanism

---

Composition Theorem

Name	Weight
Alice	40
Bob	60
Charles	80
Doe	60



Average Weight
Laplace mechanism
ε_1-differentially private

Minimum Weight
Exponential mechanism
ε_2-differentially private

Standard deviation
Laplace mechanism
ε_3-differentially private

Theorem The combination of two publications, with ε_1-differentially private and ε_2-differentially private, is $(\varepsilon_1+\varepsilon_2)$-differentially private. For any y_1, y_2 and neighboring tables T and T'.

$$e^{-(\varepsilon_1+\varepsilon_2)} \leq \frac{\Pr[(y_1,y_2) = (Out_1(T), Out_2(T))]}{\Pr[(y_1,y_2) = (Out_1(T'), Out_2(T'))]} \leq e^{\varepsilon_1+\varepsilon_2}$$

$$\frac{\Pr[(y_1,y_2) = (Out_1(T), Out_2(T))]}{\Pr[(y_1,y_2) = (Out_1(T'), Out_2(T'))]} = \frac{\Pr[y_1 = Out_1(T)]}{\Pr[y_1 = Out_1(T')]} \cdot \frac{\Pr[y_2 = Out_2(T)]}{\Pr[y_2 = Out_2(T')]}$$

y_1 and y_2 are drawn independently

$$\leq e^{\varepsilon_1} \qquad \leq e^{\varepsilon_2}$$

$$\leq e^{\varepsilon_1+\varepsilon_2}$$

The lower bound can be obtained from the similar proof. (!)

Differentially Private Infrastructure