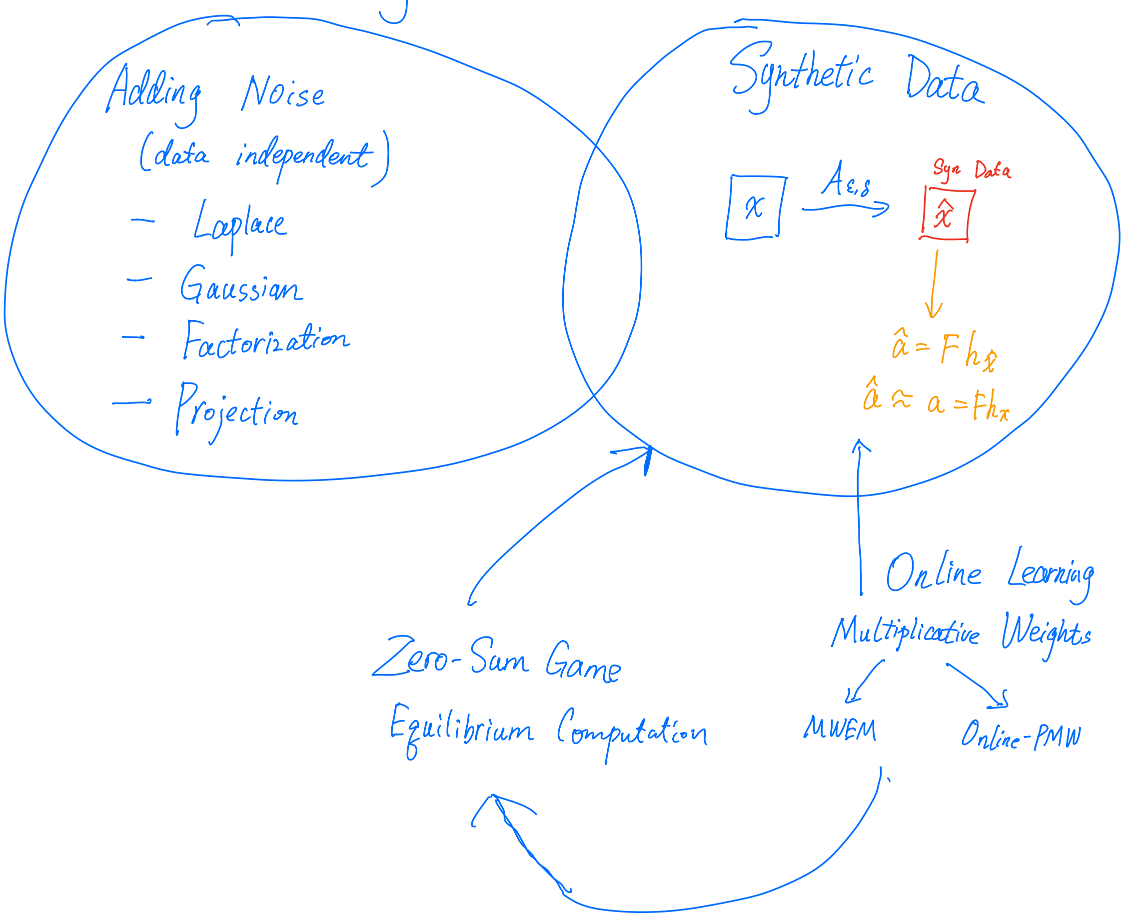
- Recap: Multiplicative Weights w/ Exp Mechanism (MWEM)
- Zero-Sum Game
  - Minimax Theorem (von Neumann)
  - Prove it via No-Regret (Online Learning)

Projects Proposal

HW3

Query Release



Multiplicative Weights (MW)

$w_a^1 = 1$ for all $a \in [k]$

For $t=1$ to T:

$$Z_t = \sum_{a=1}^{k} w_a^t$$

$$\vec{p}^{\,t} = \frac{\vec{w}^{\,t}}{Z_t} \qquad \text{"probability vector"}$$

Observes $C^t \in [0,1]^k$

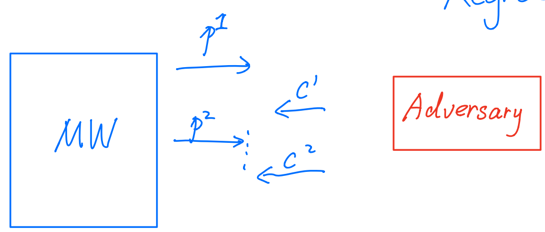
Update: for each a

$$w_a^{t+1} = w_a^t \cdot (1-\eta)^{C_a^t}$$

$$= \prod_{i=1}^{t} (1-\eta)^{C_a^i} = (1-\eta)^{C_a^{<t+1}}$$

Theorem. $\forall$ adversary $\forall\, p^* \in \Delta([m])$

$$\frac{1}{T}\sum_{t=1}^{T} \langle c^t, p^t \rangle - \min_{p^*} \frac{1}{T}\sum_{t=1}^{T} \langle c^t, p^* \rangle \leq \underbrace{2\sqrt{\frac{\ln(m)}{T}}}_{\text{Regret}}$$



"No-Regret Algorithms"

Query Release via Synthetic Data Distributions

→ Given $F = \{ f_1, \dots, f_k \}$, $\quad f_i(x) = \frac{1}{n} \sum_{j=1}^{n} \varphi_i(x_j)$

$\varphi_i : \mathcal{X} \mapsto [0,1]$

→ Histogram $(h_x)_u = \frac{\# \{ j \mid x_j = u \}}{n}$

Goal: Design M, $\quad x \longrightarrow \boxed{M} \longrightarrow \hat{p} \in \Delta(\mathcal{X})$

$$\underbrace{\max_{\varphi_i} \langle \varphi_i, \hat{p} - h_x \rangle}_{} \leq \alpha$$

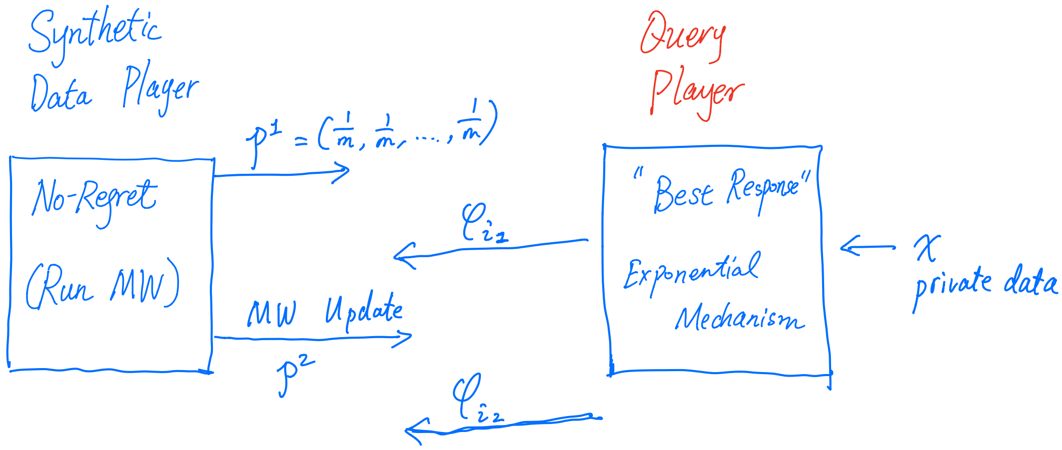
$$= \max_{\varphi_i} \left| \langle \varphi_i, \hat{p} - h_x \rangle \right| \quad \text{"max error"}$$

as long as F is closed under complement

$$\forall \varphi_i \in F, \quad 1 - \varphi_i \in F$$

From Online Learning to Query Release

Goal: Design M, $x \longrightarrow \boxed{M} \longrightarrow \hat{p}$, $\underbrace{\max_{i \in F} \langle \varphi_i, \hat{p} - h_x \rangle \leq \alpha}$



Multiplicative Weights w/ Exponential Mechanism (MWEM)

$p^1 \leftarrow (\frac{1}{m}, \dots, \frac{1}{m})$

for $t = 1, \dots T$.

Query: $i_t \longleftarrow M_0(x, \varepsilon_0, p^t)$

$c^t \longleftarrow \varphi_{i_t}$

Data: $p^{t+1} \longleftarrow \text{MW-Update}(p^t, c^t, \eta) \longleftarrow$ Cost vector $c^t = \varphi_{i_t}$

Return $\underbrace{\hat{p} = \frac{1}{T} \sum_t p^t}_{\text{avg distribution}}$

Exp Mech: choose φ_i w/ score fn $q(\varphi_i, x) = \langle \varphi_i, p^t - h_x \rangle$

How to analyze MWEM?

Privacy :

MWEM as a composition of T exp mech.
each satisfies $(\varepsilon_0, 0)$-DP.

$\Longrightarrow$ (ε, δ)-DP w/ advanced composition

for $\varepsilon \leq 1$, $\varepsilon_0 \approx \dfrac{\varepsilon}{\sqrt{T \ln(\frac{1}{\delta})}}$.

Accuracy ?

Two-Player Zero-Sum Game

- 2 Players (Row Col)
- Actions (R C)
- Pay-off Matrix $M \in \mathbb{R}^{|R| \times |C|}$

$M_{i,j}$ = \$ Row wins from Col.
if Row plays $i \in R$
Col plays $j \in C$.

Rock & Paper & Scissor

Row plays →

	R	P	S
R	0	-1	+1
P	+1	0	-1
S	-1	+1	0

Who goes first?

(1) Row goes first

- Row plays action $i \in R$.
- Col plays "best response"

$$j = \arg\min_{j'} M_{ij'}$$

$\Rightarrow$ Row should choose

$$i = \arg\max_{i'} \left(\min_{j'} M_{i'j'} \right)$$

$$\max_i \min_j M_{ij} = -1$$

(2) Col goes first

By symmetry

$$\min_j \max_i M_{ij} = 1$$

Everybody wants to go second

$$\min \max M_{ij} \geq \max \min M_{ij}.$$

Seems "Ordering matters".

Randomized Strategies.

- Row $\quad x \in \Delta(R)$
- Col $\quad y \in \Delta(C)$

Expected Payoff

$$\mathop{\mathbb{E}}_{\substack{i \leftarrow x \\ j \leftarrow y}} [M_{ij}] = \sum_{\substack{i \in R \\ j \in C}} x_i \cdot y_j \cdot M_{ij} = \boxed{x^T M y}$$

Ordering matters still?

Row plays first $x \in \Delta(R)$

- gets payoff $\min_{y \in \Delta(C)} x^T M y$
- Optimize and get

$$\max_{x \in \Delta(R)} \min_{y \in \Delta(C)} x^T M y$$

Col plays first $y \in \Delta(C)$.

- get $\min_{y \in \Delta(C)} \max_{x \in \Delta(R)} x^T M y$.

"Prefers Playing Second"

$$\min \max x^T M y \geq \max \min x^T M y$$

Rock, Paper, Scissor

Row plays $\left(\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right)$

$$\min_y x^T M y = 0.$$

$$\max \min x^T M y = 0.$$

$$\min \max x^T M y = 0.$$

"Ordering does not matter".

Minimax Theorem (von Neumann '28)

There exists a value $\underbrace{val(M)}_{\text{game value}}$ s.t.

$$\max_x \min_y x^T M y = \min_y \max_x x^T M y = val(M)$$

(may not be zero)

A pair (x, y) such that $\begin{cases} \min_{y'} x^T M y' = val(M) \\ \max_{x'} x'^T M y = val(M) \end{cases}$

$x^T M y = val(M)$.

is called minimax equilibrium

Query Release as a Zero-Sum Game

Dataset (histogram) $h \in \Delta(\mathcal{X})$

Linear queries : $\varphi_1, \ldots, \varphi_k \in \mathbb{R}^{|\mathcal{X}|}$

"Data Player" — Col player — min

"Query Player" — Row player — max

$C = \mathcal{X}$ "data univ"

$R = \{\varphi_1, \ldots, \varphi_k\}$

$\forall (i, z) \in R \times C.$

$$M_{i,z} = \varphi_i(z) - \varphi_i(h_x)$$

h_x ← private data.

① A randomized strategy P for col is just a distribution over $\mathcal{X}$. (histogram / Data set)

② True private data set h_x is a strategy for the col player. What is the game value?

$\max_{\varphi_i} h_x^T M \varphi_i = 0$, $\underline{val(M) \leq 0}$

If $\hat{p}^T M \varphi_i < 0$ for some φ_i, then query player gets positive payoff

$\Rightarrow Val(M) = 0$.

③ MWEM is computing α-approx equilibrium

$\Longrightarrow$ accurate.

How to prove Minimax Theorem?

"As far as I can see, there could be no theory of games … without that theorem … I thought there was nothing worth publishing until the Minimax Theorem was proved"

-- John von Neumann

1928.

Proof using MW.

Recap: Min Player (Row) $y \in \Delta(R)$ — Max Player (Col) $x \in \Delta(C)$

Payoff: $U(x,y) = x^T M y$

We know $\min \max U \geq \max \min U$

our goal: show "="

Proof by contradiction. Assume ">"

There exists a game and $\delta > 0$

$$\min \max U = \max \min U + \delta.$$

Thought Experiment: Over rounds $t = 1, \dots, T$

Min Player: play MW y^t.

Max Player: play best-response $x^t = \arg\max_{x'} U(x', y^t)$.

Average plays $(\bar{x}, \bar{y})$ across rounds.

① "No-Regret" of min

Synthetic Data Player

$$\frac{1}{T}\sum_{t=1}^{T} U(x^t, y^t) \leq \frac{1}{T} \min_{y^*} \sum_{t=1}^{T} U(x^t, y^*) + Reg$$

$$= \min_{y^*} \frac{1}{T}\sum_{t=1}^{T} U(x^t, y^*) + Reg$$

$$= \min_{y^*} U(\bar{x}, y^*) + Reg$$

$$\leq \max_{x} \min_{y} U(x,y) + Reg \downarrow \sqrt{\tfrac{1}{T}}$$

② "Best Response" of max

Query Player w/ Exponential Mech.

$$\frac{1}{T}\sum_{t=1}^{T} U(x^t, y^t) = \frac{1}{T}\sum_{t=1}^{T} \max_{x^*} U(x^*, y^t)$$

$$\geq \frac{1}{T}\sum_{t=1}^{T} \min_{y} \max_{x} U(x, y)$$

$$= \min_{y} \max_{x} U(x, y)$$

$$\max \min U(x, y) + Reg \geq \min \max U(x, y)$$

By assumption

$$\max \min U(x, y) + \delta = \min \max U(x, y)$$

$$Reg = \sqrt{\frac{\ln |R|}{T}}$$ decreases with T.

$\longrightarrow$ Contradiction w/ constant gap $\delta > 0$.