



Local Differential Privacy

≡

Contraction of Hockey-Stick Divergence

Shahab Asoodeh

shahab@seas.harvard.edu

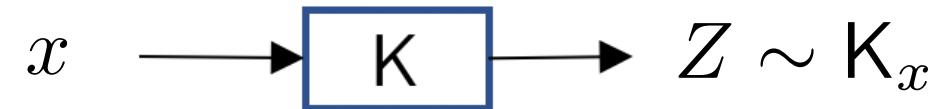
Privacy Tools DP Meeting
January 25, 2021

Joint work with: Maryam Aliakbarpour and Flavio Calmon

Outline

- Approximate LDP
- f -Divergence and Contraction Coefficient
- Equivalent Expression for LDP via Contraction Coefficient of f -Divergences
- Applications:
 - Lower Bounds on Minimax and Bayesian Risks under LDP
 - Binary Hypothesis Testing Problems under LDP

Local DP



K is called (ε, δ) -LDP if

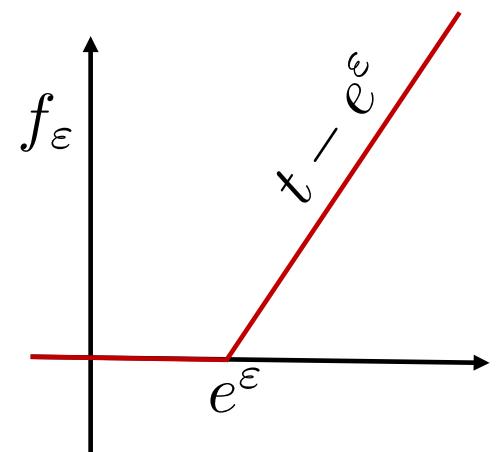
$$\sup_A [K_x(A) - e^\varepsilon K_{x'}(A)] \leq \delta, \quad \forall x, x'$$

f -divergences

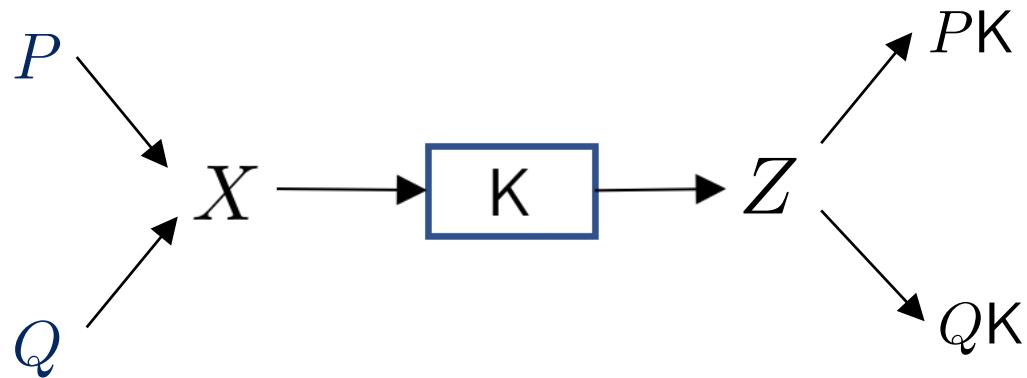
Given convex function f satisfying $f(1) = 0$: $D_f(P\|Q) \triangleq \mathbb{E}_Q \left[f\left(\frac{dP}{dQ}\right) \right]$

- $f(t) = t \log t$: $\text{KL}(P\|Q) \triangleq D_f(P\|Q) = \sum_x P(x) \log \frac{P(x)}{Q(x)}$
- $f(t) = \frac{1}{2}|t - 1|$: $\text{TV}(P\|Q) \triangleq D_f(P\|Q) = \frac{1}{2} \sum_x |P(x) - Q(x)|$
- $f(t) = (1 - \sqrt{x})^2 \implies$ Hellinger distance
- $f(t) = (t - 1)^2 \implies \chi^2$ -divergence
- $f(t) = \frac{t^\alpha - 1}{\alpha - 1} \implies \chi^\alpha$ -divergence [also Rényi divergence]
- $f_\varepsilon(t) \triangleq \max(t - e^\varepsilon, 0)$

$$\mathsf{E}_\varepsilon(P\|Q) \triangleq D_{f_\varepsilon}(P\|Q) = \sum_x \max\{P(x) - e^\varepsilon Q(x), 0\}$$



Contraction coefficient



$$\text{DPI: } D_f(PK\|QK) \leq D_f(P\|Q)$$

What is the **smallest** $\eta \leq 1$ s.t. $D_f(PK\|QK) \leq \eta D_f(P\|Q)$?

Contraction coefficient of K under f -divergence

$$\eta_f(K) \triangleq \sup_{\substack{P, Q \\ D_f(P\|Q) \neq 0}} \frac{D_f(PK\|QK)}{D_f(P\|Q)}$$

$$D_f(PK\|QK) \leq \eta_f(K) D_f(P\|Q)$$

[Dobrushin'56], [Ahlswede, Gács'76], [Erkip, Cover'12], [Anantharam, Gohari, Kamath, Nair'13], [Raginsky'14], [Polyanskiy, Wu'15, '17], [Sason, Verdú'15], [Calmon, Polyanskiy, Wu'17], [Makur, Zhang'18], [Sason'18, '19]

Contraction coefficient

Contraction coefficient of K under f -divergence

$$\eta_f(K) \triangleq \sup_{\substack{P, Q \\ D_f(P||Q) \neq 0}} \frac{D_f(PK||QK)}{D_f(P||Q)}$$

- Under KL: Concentration inequalities (log Sobolev), decay rate of mutual information
[Ahlswede, Gács'76], [[Cohen, Iwasa, Rautu, Ruskai, Seneta'93], [Houdré and Tetali'01], [S. G. Bobkov and P. Tetali'06], [Anantharam, Gohari, Kamath, Nair'13], [Polyanskiy, Wu'15, '17]]
- Under TV: Mixing of random walks on graphs [Dobrushin'56], [Raginsky'14]
- Under χ^2 : Rényi maximal correlation [Erkip, Cover'12], [Makur, Zheng'20], [Makur, Y. Polyanskiy'18]
- Under E_ε : Central DP guarantees of iterative algorithms
[Balle, Barthe, Gaboardi, Geumlek'19], [A., Diaz, Calmon'20, '21], [A., Liao, Calmon, Kosut, Sankar'20, '21]

$$\eta_\varepsilon(K) \triangleq \sup_{\substack{P, Q \\ E_\varepsilon(P||Q) \neq 0}} \frac{E_\varepsilon(PK||QK)}{E_\varepsilon(P||Q)}$$

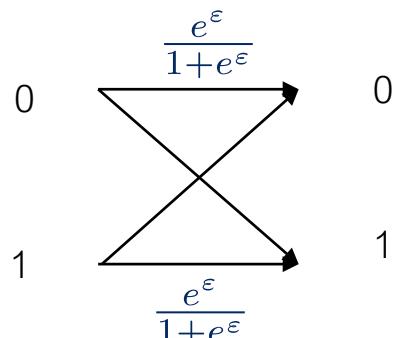
Main result

Theorem.

$$\begin{aligned} K \text{ is } (\varepsilon, \delta)\text{-LDP} &\iff \eta_\varepsilon(K) \leq \delta \\ &\iff E_\varepsilon(PK\|QK) \leq \delta E_\varepsilon(P\|Q), \quad \forall P, Q \end{aligned}$$

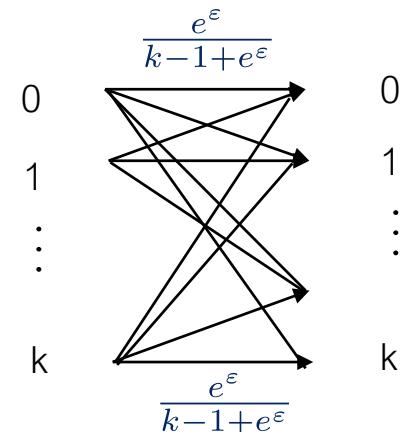
$$K \text{ is } \varepsilon\text{-LDP} \iff \eta_\varepsilon(K) = 0 \iff E_\varepsilon(PK\|QK) = 0 \quad \forall P, Q$$

Example. Binary-input binary-output with flipping prob. $\frac{1}{1+e^\varepsilon}$



(randomized response model)

$$E_\varepsilon(PK\|QK) = 0, \quad \forall P, Q \implies K \text{ is } \varepsilon\text{-LDP}$$



Warning: $E_\varepsilon(P\|Q) = 0 \not\implies P = Q$

Related work

- [Duchi et al'13]: K is ε -LDP $\implies \text{TV}(PK, QK) \leq \sqrt{2}(e^\varepsilon - 1)\text{TV}(P, Q)$ only for $\varepsilon \ll 1$
- [Kairouz et al'15]: K is ε -LDP $\implies \text{TV}(PK, QK) \leq \frac{e^\varepsilon - 1}{e^\varepsilon + 1} \text{TV}(P, Q)$
- [Kairouz et al'14]: K is ε -LDP $\implies \text{KL}(PK\|QK) + \text{KL}(QK\|PK) \leq 2\frac{(e^\varepsilon - 1)^2}{(e^\varepsilon + 1)} \text{TV}^2(P, Q)$ only for $\varepsilon \ll 1$
- [Duchi et al'14]: K is ε -LDP $\implies \boxed{\text{KL}(PK\|QK) + \text{KL}(QK\|PK)} \leq 4(e^\varepsilon - 1)^2 \text{TV}^2(P, Q)$

f -divergence with $f(t) = (t - 1) \log t$
(Jeffrey divergence)

All their proof techniques fail if $\delta > 0$

Main result

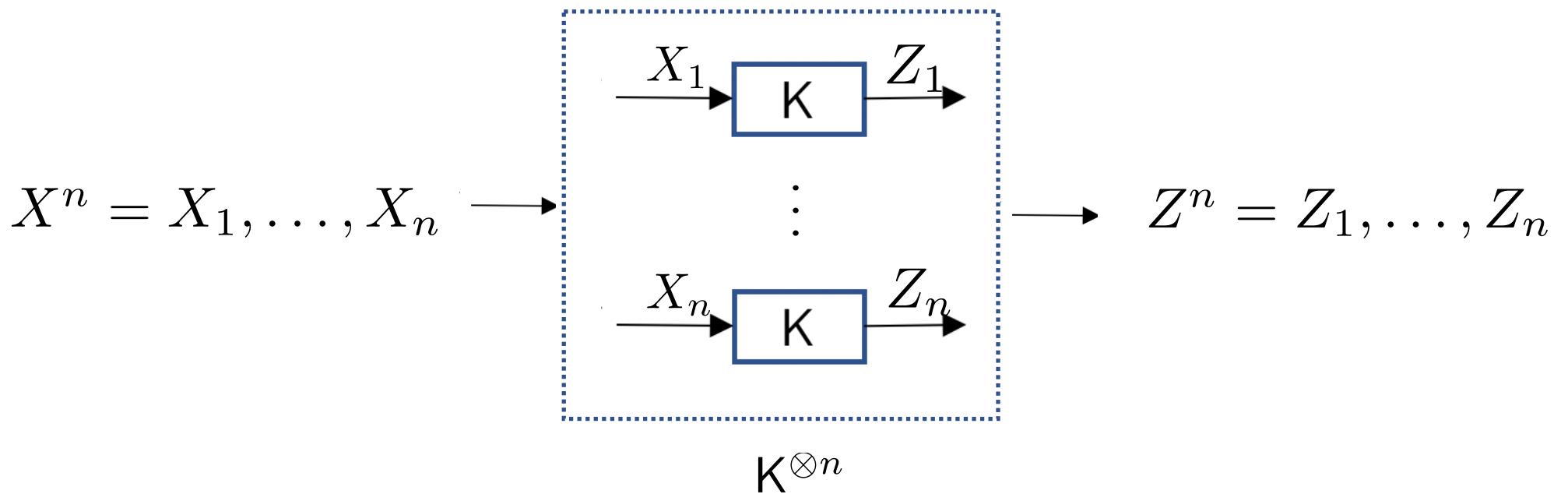
Theorem.

$$\begin{aligned} K \text{ is } (\varepsilon, \delta)\text{-DP} &\implies \eta_f(K) \leq \varphi(\varepsilon, \delta) \\ &\iff D_f(PK\|QK) \leq \varphi(\varepsilon, \delta)D_f(P\|Q) \end{aligned}$$

$$\text{where } \varphi(\varepsilon, \delta) \triangleq 1 - e^{-\varepsilon}(1 - \delta)$$

- Holds for **any** $\varepsilon \geq 0$ and $\delta \in [0, 1]$
- Holds for any arbitrary f -divergences

No interaction!



Theorem. K is (ε, δ) -DP $\implies \eta_f(K^{\otimes n}) \leq \varphi_n(\varepsilon, \delta)$

where $1 - e^{-n\varepsilon}(1 - \delta)^n$.

η_f seems difficult to compute (or bound) in case of interactivity

Application I: Minimax Risks

- $X^n \sim P$ i.i.d.
- $P \in \mathcal{P}$
- Each $X_i \mapsto Z_i$ via an (ε, δ) -LDP mechanism K_i
- We wish to estimate $\theta(P)$ using an estimator Ψ

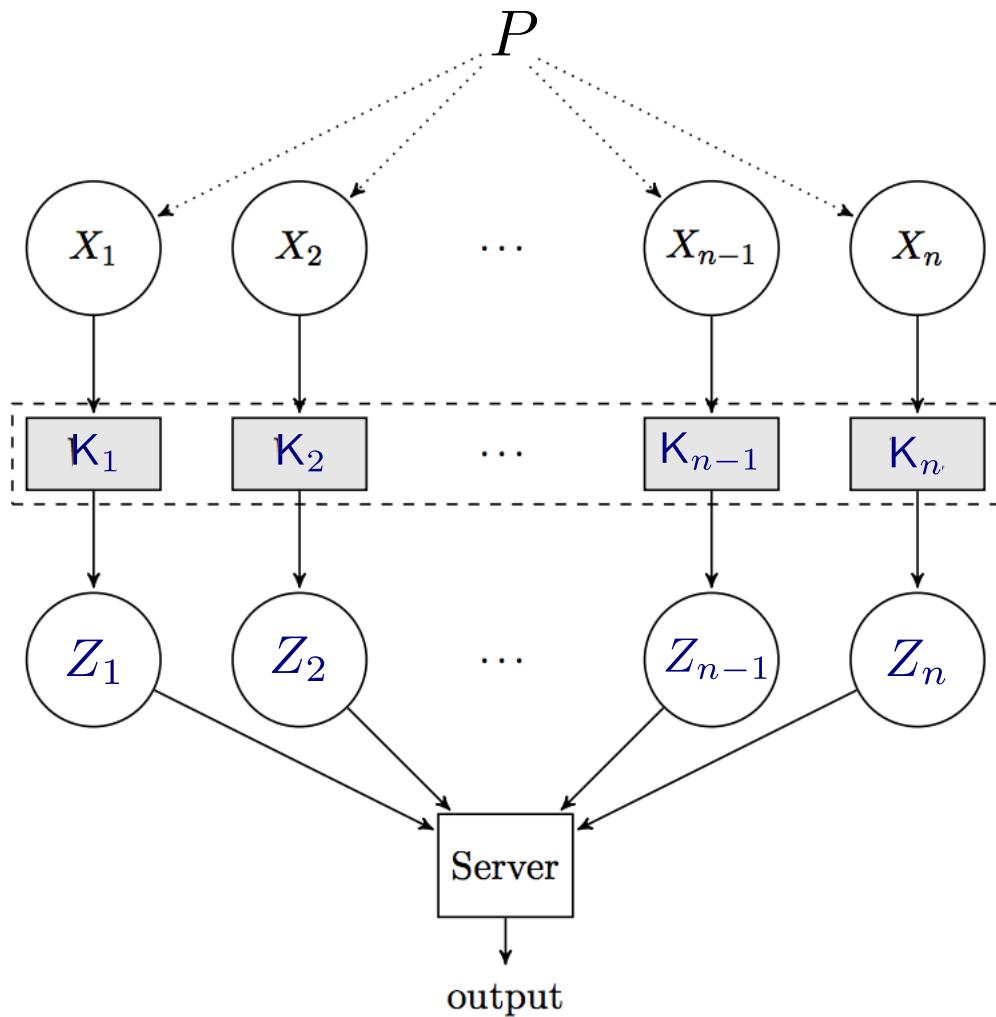
$$\mathcal{R}_n(\mathcal{P}, \ell, \varepsilon, \delta) \triangleq \inf_{\{K_i\} \in Q_{\varepsilon, \delta}} \inf_{\Psi} \sup_{P \in \mathcal{P}} \mathbb{E}[\ell(\Psi(Z^n), \theta(P))]$$

best (ε, δ) private mechanisms

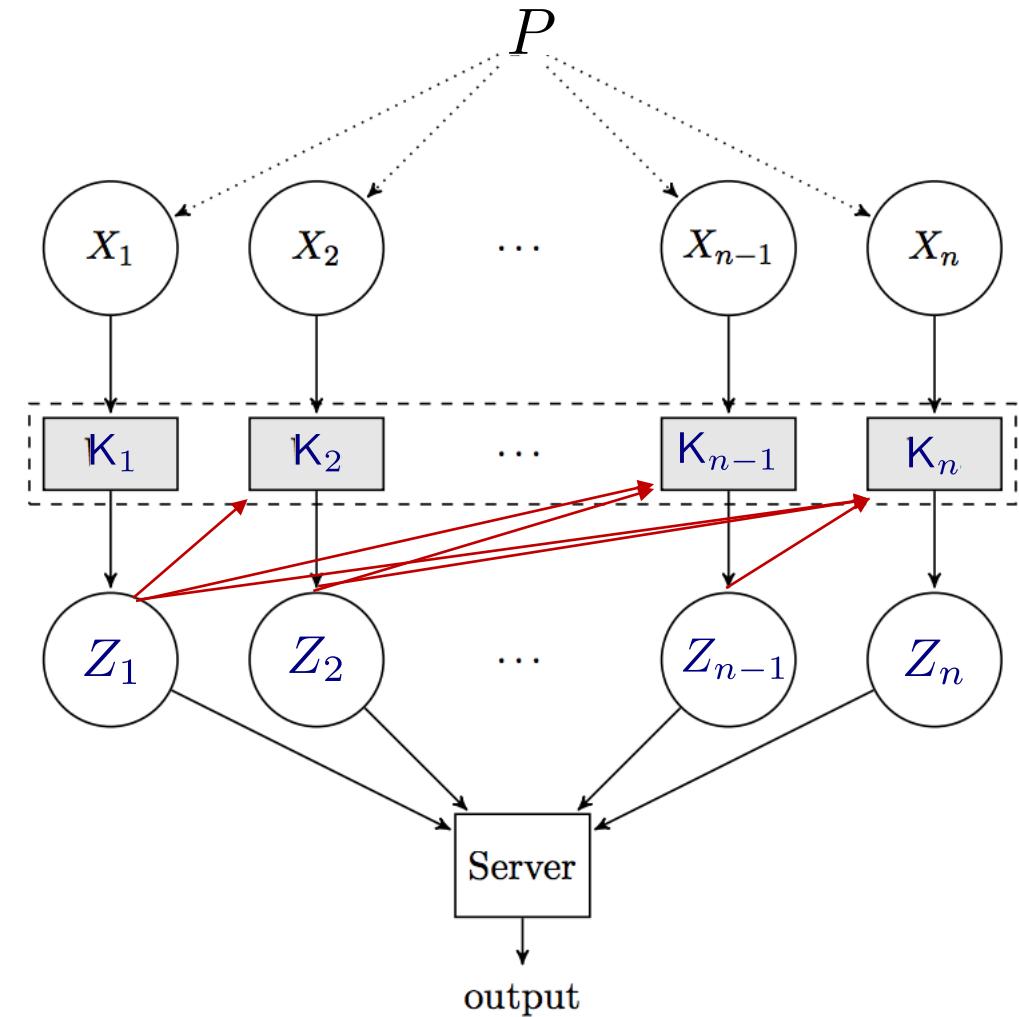
worst-case over family \mathcal{P}

best estimator Ψ

Application I: Minimax Risks



Non-interactive setting



Sequentially interactive setting

Application I: Minimax Risks

From estimation to testing:

- Construct an index set $\mathcal{V} = \{1, \dots, |\mathcal{V}|\}$
- Pick $\{P_v : v \in \mathcal{V}\} \subset \mathcal{P}$ s.t. $\ell(\theta(P_v), \theta(P_{v'})) \geq 2\tau, \forall v \neq v' \in \mathcal{V}$
- Nature chooses V uniformly from \mathcal{V}
- Given $V = v$, samples X^n are drawn i.i.d. from P_v

$$\mathcal{R}_n(\mathcal{P}, \ell, \infty, 1) \geq \inf_{\Psi} \tau \Pr(\Psi(X^n) \neq V) \quad [\text{Yang, Barron'99}], [\text{Tsybakov'08}]$$

- Z^n are generated via K_1, \dots, K_n

$$\mathcal{R}_n(\mathcal{P}, \ell, \varepsilon, \delta) \geq \inf_{\{K_i\} \in \mathcal{Q}_{\varepsilon, \delta}} \inf_{\Psi} \tau \Pr(\Psi(Z^n) \neq V)$$

Application I: Minimax Risks

$$\mathcal{R}_n(\mathcal{P}, \ell, \varepsilon, \delta) \geq \inf_{\{\mathsf{K}_i\} \in \mathcal{Q}_{\varepsilon, \delta}} \inf_{\Psi} \tau \Pr(\Psi(Z^n) \neq V)$$

Le Cam's Method

- $|\mathcal{V}| = 2$
- $\{P_v : v \in \mathcal{V}\} = \{P_0, P_1\}$

$$\inf_{\Psi} \Pr(\Psi(X^n) \neq V) \geq \frac{1}{2} - \frac{1}{2} \text{TV}(P_0^{\otimes n}, P_1^{\otimes n})$$



- Consider $\{\mathsf{K}_i\}_{i=1}^n$

$$\inf_{\Psi} \Pr(\Psi(Z^n) \neq V) \geq \frac{1}{2} - \frac{1}{2} \text{TV}(M_0^n, M_1^n)$$

Fano's Method

- $|\mathcal{V}| = k$

$$\inf_{\Psi} \Pr(\Psi(X^n) \neq V) \geq 1 - \frac{I(X^n; V) + \log 2}{\log |\mathcal{V}|}$$

- Consider $\{\mathsf{K}_i\}_{i=1}^n$

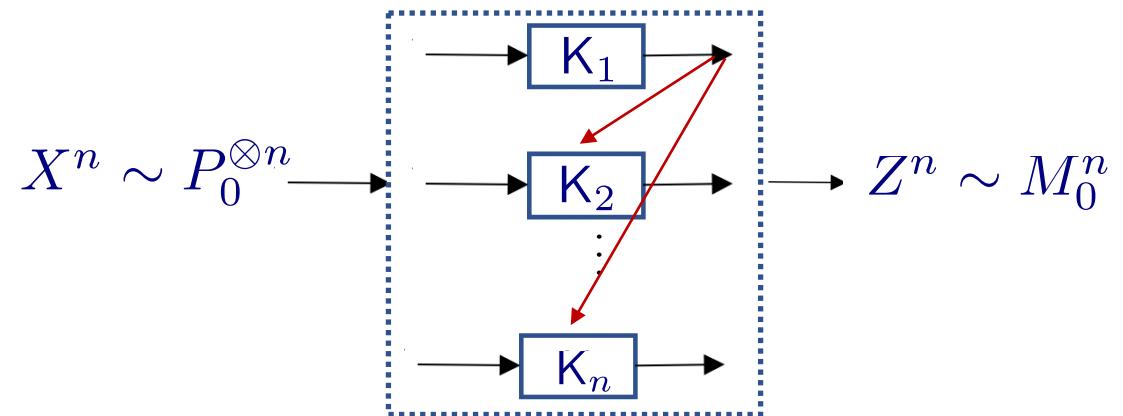
$$\inf_{\Psi} \Pr(\Psi(Z^n) \neq V) \geq 1 - \frac{I(Z^n; V) + \log 2}{\log |\mathcal{V}|}$$

Application I: Minimax Risks

Le Cam's Method

- Sequentially interactive setting

$$\begin{aligned} \text{TV}(M_0^n, M_1^n) &\leq \sqrt{\frac{1}{2} D(M_0^n \| M_1^n)} \\ &= \sqrt{\frac{1}{2} \sum_i \text{KL}(P_0 K_i \| P_1 K_i)} \\ &\leq \sqrt{n \varphi(\varepsilon, \delta) \text{KL}(P_0 \| P_1)} \end{aligned}$$



$$\mathcal{R}_n(\mathcal{P}, \ell, \varepsilon, \delta) \geq \frac{\tau}{2} \left[1 - \frac{1}{\sqrt{2}} \sqrt{n \varphi(\varepsilon, \delta) \text{KL}(P_0 \| P_1)} \right]$$

[Yang, Barron'99], [Tsybakov'08], [Yu'97]

$$\mathcal{R}_n(\mathcal{P}, \ell, \infty, 1) \geq \frac{\tau}{2} \left[1 - \frac{1}{\sqrt{2}} \sqrt{n \text{KL}(P_0 \| P_1)} \right]$$

reduction in effective sample size

Application I: Minimax Risks

Example.[one-dimensional mean estimation]

- For $k > 1$: $\mathcal{P}_k \triangleq \{P : |\mathbb{E}_P[X]| \leq 1, \mathbb{E}_P[|X|^k] \leq 1\}$
- $\theta(P) = \mathbb{E}_P[X]$ and $\ell = \ell_2^2$

We need to pick $P_0, P_1 \in \mathcal{P}_k$ with $\left|E_{P_0}[X] - E_{P_1}[X]\right|^2 \geq 2\tau$

Consider $\{-\omega^{-\frac{1}{k}}, 0, \omega^{-\frac{1}{k}}\}$ for some $\omega \in (0, 1]$

$$P_0(-\omega^{-\frac{1}{k}}) = \omega, \quad P_0(0) = 1 - \omega \quad P_1(\omega^{-\frac{1}{k}}) = \omega, \quad P_1(0) = 1 - \omega$$

Corollary.

$$\mathcal{R}_n(\mathcal{P}_k, \ell_2^2, \varepsilon, \delta) \gtrsim \min \left\{ 1, [n\varphi^2(\varepsilon, \delta)]^{-\frac{(k-1)}{k}} \right\}$$

[Duchi, Jordan, Wainwright'13]

$$\mathcal{R}_n(\mathcal{P}_k, \ell_2^2, \varepsilon, 0) \gtrsim \min \left\{ 1, [n\varepsilon^2(\varepsilon, \delta)]^{-\frac{(k-1)}{k}} \right\} \quad \text{only for } \varepsilon \leq 1$$

Application I: Minimax Risks

Fano's Method

- Non-interactive setting

$$\varphi_n(\varepsilon, \delta) \triangleq 1 - e^{-n\varepsilon}(1 - \delta)^n$$

Lemma.

$$I(Z^n; V) \leq \frac{n\varphi_n(\varepsilon, \delta)}{|\mathcal{V}|^2} \sum_{v, v' \in \mathcal{V}} \text{KL}(P_v \| P_{v'})$$

[Duchi, Jordan, Wainwright'14]

$$I(Z^n; V) \leq \frac{2n(e^\varepsilon - 1)}{|\mathcal{V}|^2} \sum_{v, v' \in \mathcal{V}} \text{KL}(P_v \| P_{v'})$$

Application I: Minimax Risks

Example.[high-dimensional mean estimation in ℓ_2 ball]

- $\mathcal{P} \triangleq \{\text{prob. on } \ell^2\text{-ball in } \mathbb{R}^d\}$
- $\theta(P) = \mathbb{E}_P[X]$
- $\ell = \ell_2^2$ We need to pick index set \mathcal{V} and $\{P_1, \dots, P_{|\mathcal{V}|}\} \subset \mathcal{P}$ with $\|E_{P_v}[X] - E_{P_{v'}}[X]\|_2^2 \geq 2\tau$

$$\varphi_n(\varepsilon, \delta) \triangleq 1 - e^{-n\varepsilon}(1 - \delta)^n$$

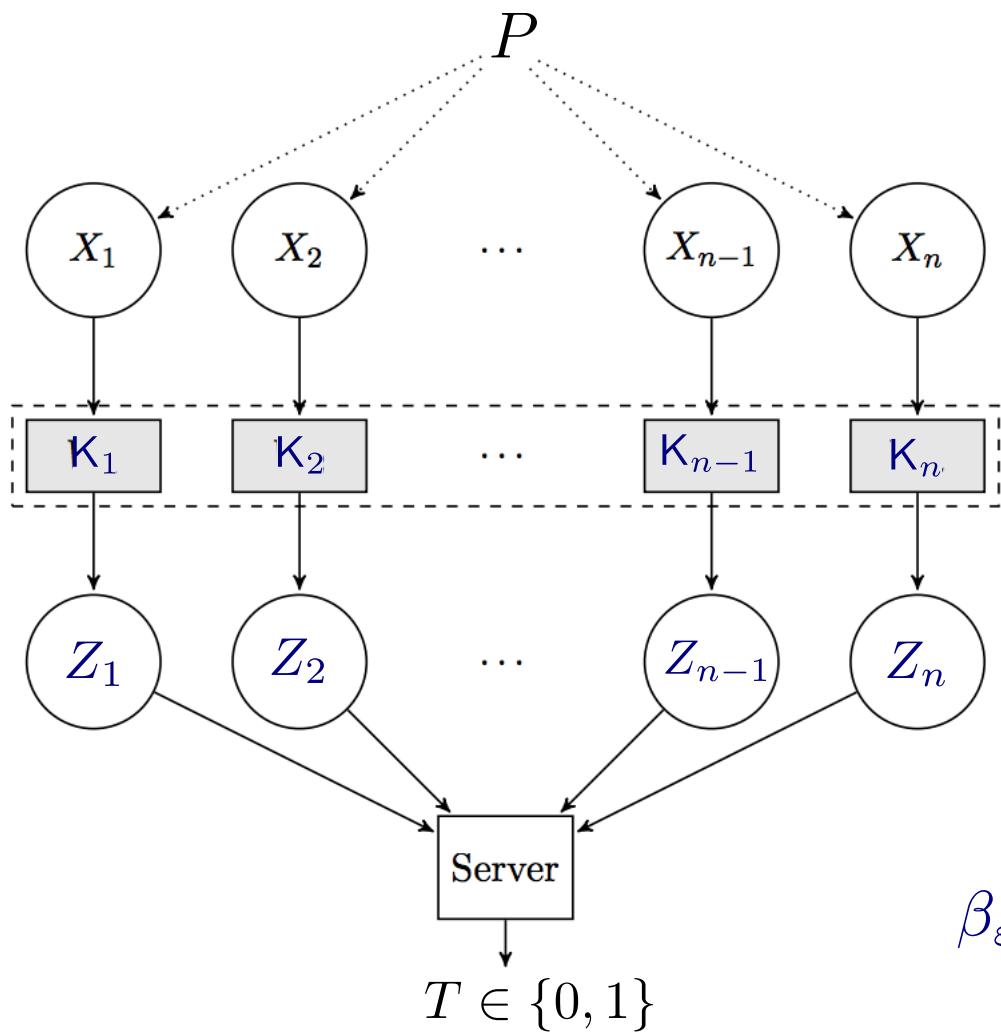
Corollary.

$$\mathcal{R}_n(\mathcal{P}, \ell_2^2, \varepsilon, \delta) \gtrsim \min \left\{ \frac{1}{n\varphi_n(\varepsilon, \delta)}, \frac{d}{n^2\varphi_n^2(\varepsilon, \delta)} \right\}$$

[Duchi, Jordan, Wainwright'14]

$$\mathcal{R}_n(\mathcal{P}, \ell_2^2, \varepsilon, 0) \gtrsim r^2 \min \left\{ \frac{1}{\varepsilon\sqrt{n}}, \frac{d}{n\varepsilon^2} \right\} \quad \text{only for } \varepsilon \leq 1$$

Application 2: Hypothesis Testing



$$H_0 : P = P_0$$

$$H_1 : P = P_1$$

Type I error: $\Pr(T = 1|H_0)$

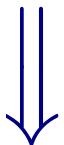
Type II error: $\Pr(T = 0|H_1)$

$$\beta_{\varepsilon, \delta}(\alpha) \triangleq \inf_{\{\mathsf{K}_i\} \in \mathcal{Q}_{\varepsilon, \delta}} \inf_{\substack{P_{T|Z^n}: \\ \Pr(T=1|H_0) \leq \alpha}} \Pr(T = 0|H_1)$$

Application 2: Hypothesis Testing

Chernoff-Stein lemma: non-private, i.e., $Z^n = X^n$

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n(\alpha) = -\text{KL}(P_0 \| P_1)$$



$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n^{\varepsilon, \delta}(\alpha) = - \sup_{K \in \mathcal{Q}_{\varepsilon, \delta}} \text{KL}(P_0 K \| P_1 K)$$

Lemma.

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n^{\varepsilon, \delta}(\alpha) \geq -\varphi(\varepsilon, \delta) \text{KL}(P_0 \| P_1)$$

$$\varphi(\varepsilon, \delta) \triangleq 1 - e^{-\varepsilon}(1 - \delta)$$

Wrap-up

- Equivalent expression for (ε, δ) -LDP in terms of HS divergence
- Use it to derive lower bound for estimation and testing problems

