［招待講演］
セキュリティを考慮した2つの問題に対する情報理論的解析について
～ Local Differential Privacyの下でのパラメータ推定問題と、プライバシーと有用性のトレードオフ問題 ～

電子情報通信学会　RCC・ISEC・IT・WBS合同研究会
2023年3月14日
齋藤 翔太（群馬大学）

本日の発表の概要

準備

Local Differential Privacyの下での
パラメータ推定問題

プライバシーと有用性の
トレードオフ問題

本講演の内容

本講演では、

- (ϵ, δ) –local differential privacyの下でのパラメータ推定問題
- 有用性とプライバシーのトレードオフ問題

という二つの問題に対して、

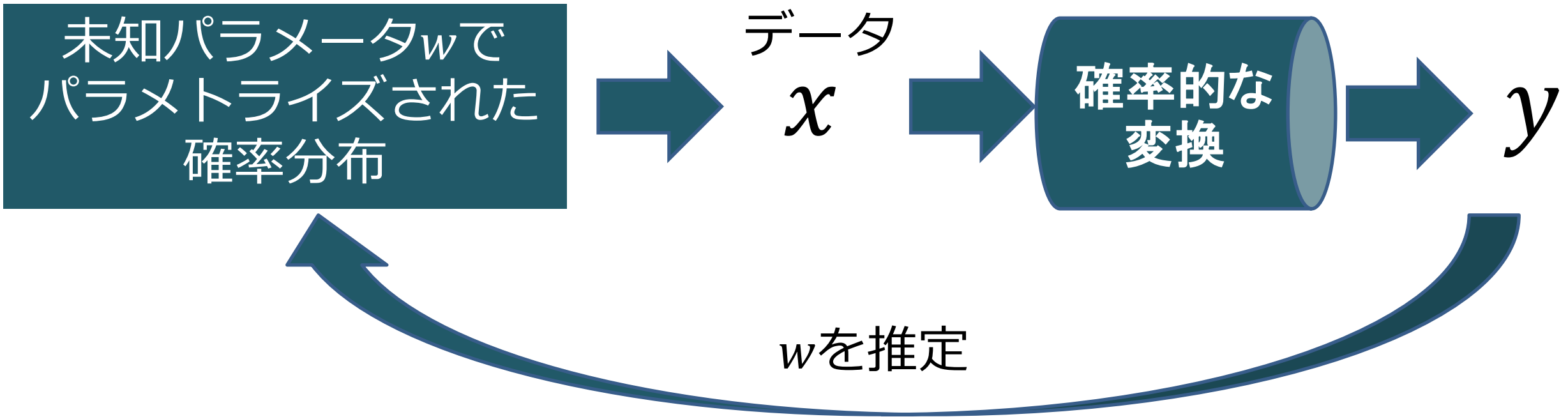
◆ 問題設定
◆ 評価基準
◆ その評価基準のもとでの理論限界

を解説する。

パラメータ推定問題 (1/2)

データxから未知パラメータwを推定する問題は、
統計学や機械学習等において基本的で重要な問題

パラメータ推定問題 (2/2)



データxを確率的に変換したデータyをもとに
未知パラメータwを推定する問題を考える。

推定の良さを測る評価基準は？
その評価基準のもとで、理論限界は？

プライバシーと有用性のトレードオフ問題

数学的な定式化は？
情報理論的な評価は？

本日の発表の概要

準備

Local Differential Privacyの下での
パラメータ推定問題

プライバシーと有用性の
トレードオフ問題

準備①：ノーテーションに関する約束

準備②： ○○ダイバージェンスと○○情報量

準備③：ランダム化メカニズム（通信路）

ノーテーションに関する約束（1/2）

- 登場する確率変数は、すべて離散確率変数
- **確率変数**はアルファベットの**大文字**、その**実現値**は**小文字**で表す
- **花文字**でその確率変数が値をとる集合を表す

（例）確率変数 A は集合 $\mathcal{A}$ に値をとり、その実現値を $a \in \mathcal{A}$ と表す

- 確率変数 A の確率関数を $P_A(a)$ や $Q_A(a)$ 等と表し、
  確率変数 A と確率変数 B の同時確率関数を $P_{A,B}(a,b)$ 、
  条件付き確率関数を $P_{B|A}(b|a)$ 等と表記する

- 確率関数 $P_A(a)$ による期待値を $\mathbb{E}_{P_A}\left[\cdot\right]$ 等と表す

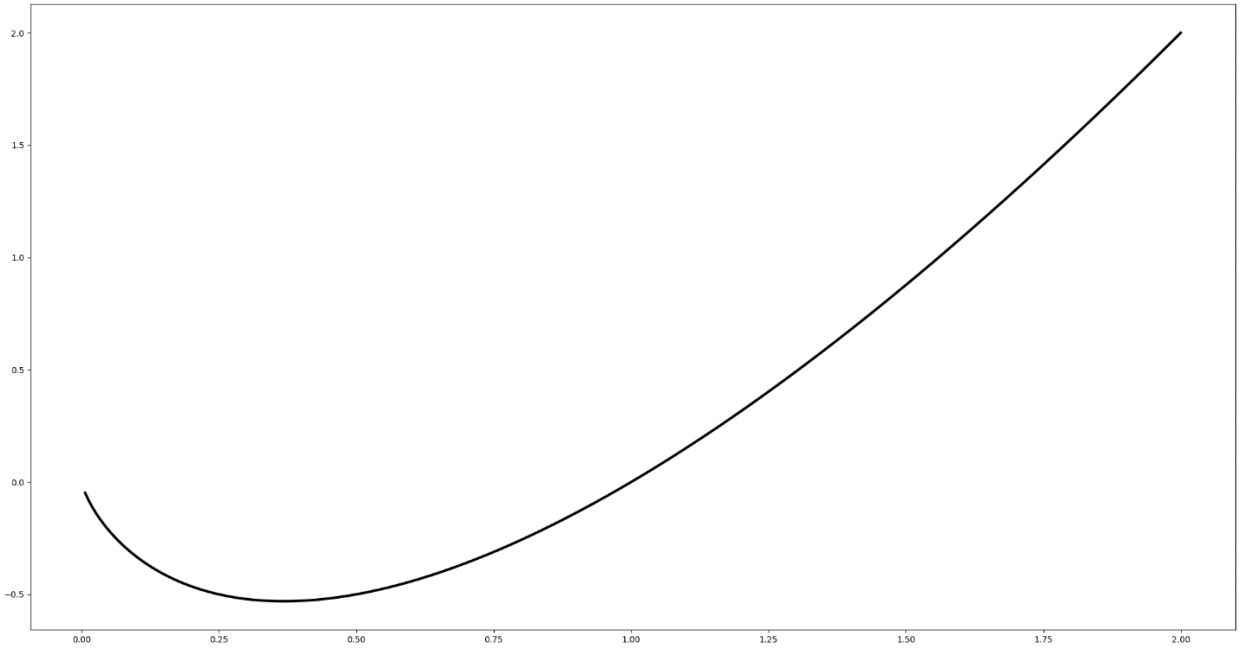
ノーテーションに関する約束（2/2）

- $\log x$ と書いたら、 $\log_e x$ を表すとする（**自然対数**）
- **関数fと書いたら、$f(1) = 0$を満たす下に凸な関数**

$$f : [0, +\infty) \to \mathbb{R}$$

のことを指すものとする

（例） $f(x) = x \log x$



準備①：ノーテーションに関する約束

準備②：　○○ダイバージェンスと○○情報量

準備③：ランダム化メカニズム（通信路）

KLダイバージェンスと相互情報量

確率関数 $P_A(a)$ ， $Q_A(a)$ に対する**KLダイバージェンス**

$$D(P_A \| Q_A) := \sum_{a \in \mathcal{A}} P_A(a) \log \frac{P_A(a)}{Q_A(a)}$$

確率変数Aと確率変数Bに対する**相互情報量**

$$I(A;B) := D(P_{A,B} \| P_A P_B)$$

相互情報量は、Aを知ることによって得たBの情報の量
（またはBを知ることによって得たAの情報の量）を表す

f –ダイバージェンスとf – informativity（1/2）

確率関数 $P_A(a)$ ， $Q_A(a)$ に対する**f –ダイバージェンス**

$$D_f(P_A\|Q_A) := \sum_{a\in\mathcal{A}} Q_A(a) f\left(\frac{P_A(a)}{Q_A(a)}\right)$$

$f(x) = x\log x$ とすると …

$$D_f(P_A\|Q_A) = \sum_{a\in\mathcal{A}} P_A(a)\log\frac{P_A(a)}{Q_A(a)} = D(P_A\|Q_A)$$

f –ダイバージェンスは、KLダイバージェンスを一般化した量

f –ダイバージェンスとf – informativity （2/2）

確率変数Aと確率変数Bに対する**f-informativity**

$$I_f(A;B) := \inf_{Q_B} \sum_{a \in \mathcal{A}} P_A(a) D_f(P_{B|A=a} \| Q_B)$$

$f(x) = x \log x$ とすると…

$$I_f(A;B) = \inf_{Q_B} \sum_{a \in \mathcal{A}} P_A(a) D(P_{B|A=a} \| Q_B) = I(A;B)$$

f –informativityは、相互情報量を一般化した量

準備①：ノーテーションに関する約束

準備②：　○○ダイバージェンスと○○情報量

準備③：ランダム化メカニズム（通信路）

ランダム化メカニズム（通信路）

この後に述べる二つの問題では、データXを確率的にデータYに変換するということを考える

これを **条件付き確率関数 $P_{Y|X}$** で表す

$P_{Y|X}$ は、**ランダム化メカニズム**と呼ばれたり、
情報理論では**通信路**と呼ばれたりする

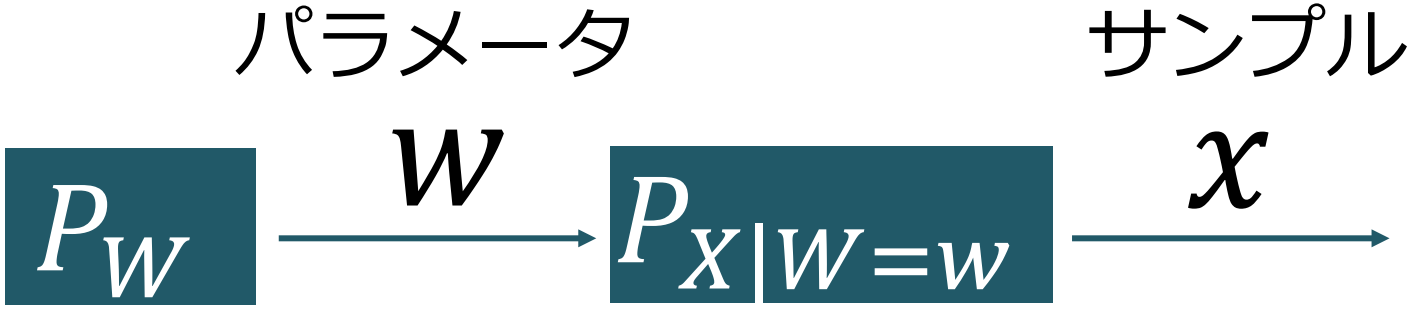
本日の発表の概要

準備

Local Differential Privacyの下での
パラメータ推定問題

プライバシーと有用性の
トレードオフ問題

問題設定 (1/3)



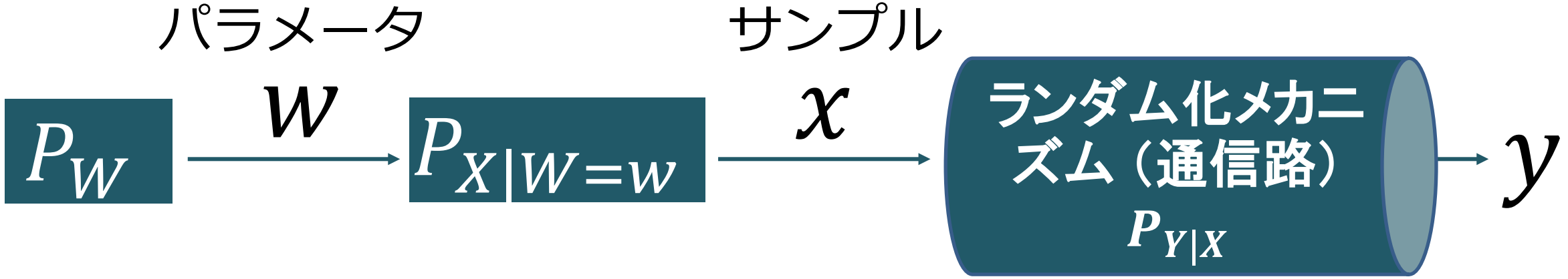
$\mathcal{W}$：パラメータ空間

W：パラメータ空間 $\mathcal{W}$ に値をとる確率変数

$W \sim P_W$ （←**事前分布**）

サンプル x は、パラメトライズされた分布 $P_{X|W=w}$ に従って発生する

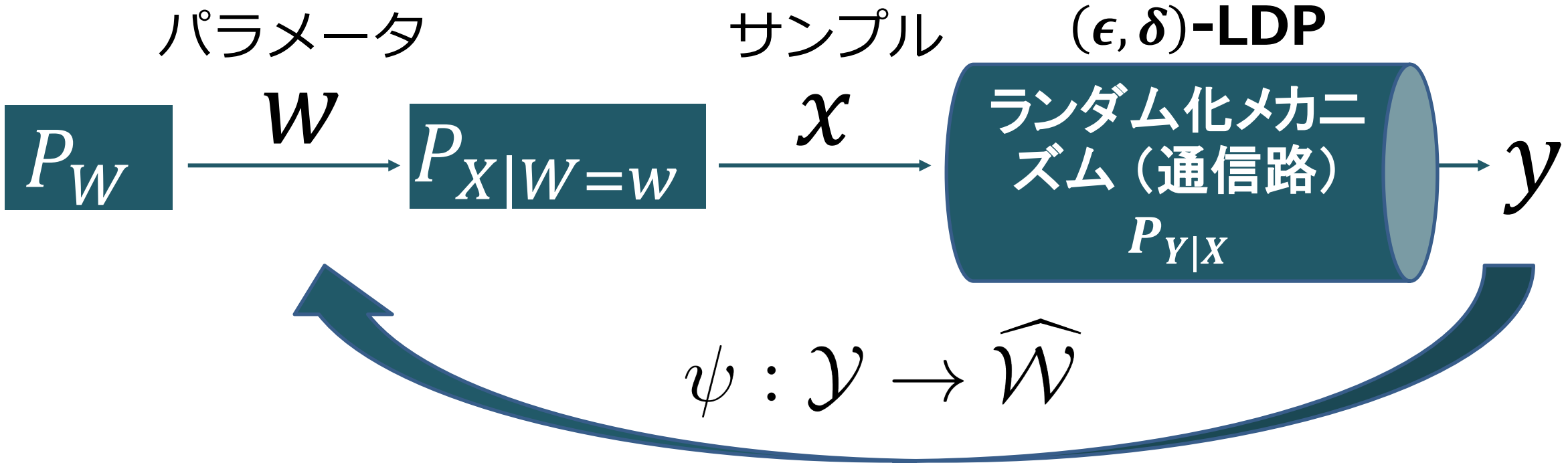
問題設定 (2/3)



(ϵ, δ)-局所差分プライバシー
(ϵ, δ)-local differential privacy

以降では、**(ϵ, δ)-LDP**と呼ぶ
詳細は後述

問題設定 (3/3)



データyから未知パラメータwを推定量 $\psi : \mathcal{Y} \to \widehat{\mathcal{W}}$ を用いて推定する

$\widehat{\mathcal{W}}$ と $\mathcal{W}$ は必ずしも一致していなくともよいとする

定義（ (ϵ, δ)-局所差分プライバシー）

$\epsilon \geq 0$と$\delta \in [0, 1]$に対して、ランダム化メカニズム$P_{Y|X}$が

$$\sup_{x, x' \in \mathcal{X}} \sup_{\mathcal{S} \subset \mathcal{Y}} \left[P_{Y|X}(\mathcal{S}|x) - e^{\epsilon} P_{Y|X}(\mathcal{S}|x') \right] \leq \delta$$

を満足するとき、(ϵ, δ)-局所差分プライバシー（ (ϵ, δ)-LDP ）を満たすという。ここで、

$$P_{Y|X}(\mathcal{S}|x) = \sum_{y \in \mathcal{S}} P_{Y|X}(y|x)$$

である。

(ϵ, δ)-LDP（(ϵ, δ)-局所差分プライバシー）

こちらの式について、少し考えてみる。

$$\sup_{x, x' \in \mathcal{X}} \sup_{\mathcal{S} \subset \mathcal{Y}} \left[P_{Y|X}(\mathcal{S}|x) - e^{\epsilon} P_{Y|X}(\mathcal{S}|x') \right] \leq \delta$$

簡単のため、supを無視すると…

(ϵ, δ)-LDP（(ϵ, δ)-局所差分プライバシー）

$$P_{Y|X}(\mathcal{S}|x) - e^{\epsilon} P_{Y|X}(\mathcal{S}|x') \leq \delta$$

$\delta = 0$とすると…

$$P_{Y|X}(\mathcal{S}|x) - e^{\epsilon} P_{Y|X}(\mathcal{S}|x') \leq 0$$

$$\Leftrightarrow \quad \log \frac{P_{Y|X}(\mathcal{S}|x)}{P_{Y|X}(\mathcal{S}|x')} \leq \epsilon$$

ベイズリスク

非負値損失関数 $\ell : \mathcal{W} \times \widehat{\mathcal{W}} \to \mathbb{R}^+$ と、(ϵ, δ)-LDPを満たす
ランダム化メカニズム$P_{Y|X}$が与えられたとき、**ベイズリスクR_B**は

$$R_B := \inf_{\psi} \mathbb{E}[\ell(W, \psi(Y))]$$

$$= \inf_{\psi} \sum_{w \in \mathcal{W}} \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \ell(w, \psi(y)) P_W(w) P_{X|W}(x|w) P_{Y|X}(y|x)$$

ベイズリスクR_Bは「平均的な損失の量」を表す。
そのため、ベイズリスクは小さいほうが嬉しいわけであるが、
どこまで小さくできるのだろうか？

ベイズリスクの下界

定理 1 [Asoodeh et al., 2021 IEEE ISIT]

任意の$\rho > 0$に対して、

$$R_B \geq \rho \left(1 - \frac{\varphi(\epsilon, \delta) I(W;X) + \log 2}{\log(1/\sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) \leq \rho])} \right)$$

が成り立つ。ここで、

$$\varphi(\epsilon, \delta) := 1 - (1-\delta)e^{-\epsilon}$$

$$\mathbb{P}[\ell(W, \widehat{w}) \leq \rho] = \sum_{\substack{w \in \mathcal{W}: \\ \ell(w, \widehat{w}) \leq \rho}} P_W(w)$$

定理1の考察 (1/3)

$$R_B \geq \rho \left(1 - \frac{\varphi(\epsilon, \delta) I(W;X) + \log 2}{\log(1/\sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) \leq \rho])} \right)$$

相互情報量$I(W;X)$は、サンプルXを知ることによって得られる
パラメータWの情報の量

▼

直感的には、相互情報量$I(W;X)$が大きいほど、パラメータ推定が
易しくなり、ベイズリスクは小さくなりそう

▼

上式を見ると、$I(W;X)$が大きいほどベイズリスクの下界が
小さくなることがわかる

定理1の考察 (2/3)

$$R_B \geq \rho \left(1 - \frac{\boxed{\varphi(\epsilon, \delta)} I(W;X) + \log 2}{\log(1/\sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) \leq \rho])} \right)$$

(ϵ, δ) –LDPのパラメータであるϵとδが小さくなると、プライバシーに関する制約が強くなり、パラメータ推定が難しくなるため、ベイズリスクは大きくなりそう

▼

$\varphi(\epsilon, \delta)$は$\epsilon$と$\delta$の非減少関数なので、$\epsilon$や$\delta$を小さくすると、上式よりベイズリスクの下界が大きくなる

$$\varphi(\epsilon, \delta) := 1 - (1 - \delta)e^{-\epsilon}$$

定理1の考察 (3/3)

$$R_B \geq \rho \left(1 - \frac{\varphi(\epsilon, \delta) I(W; X) + \log 2}{\log(1/\sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) \leq \rho])} \right)$$

$\sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) \leq \rho]$ が大きければ、直感的にはパラメータ推定がやりやすく、ベイズリスクは小さくなりそう

▼

上式より、 $\sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) \leq \rho]$ が大きいほど
ベイズリスクの下界が小さくなることがわかる

ベイズリスクの下界とマルコフの不等式

先ほどの定理1の不等式

$$R_B \geq \rho \left(1 - \frac{\varphi(\epsilon, \delta) I(W; X) + \log 2}{\log(1/\sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) \leq \rho])} \right)$$

は、マルコフの不等式に由来する。

非負値確率変数Aと任意の$\rho > 0$に対して $\mathbb{E}[A] \geq \rho \mathbb{P}[A \geq \rho]$

一方で、マルコフの不等式によらずに
ベイズリスクの下界を導出することもできる

ベイズリスクの下界

定理 3 [Saito, SITA2022]

$$R_B \geq \frac{1}{2} \sup \left\{ r > 0 : \sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) < r] < 1 - u_f\Big(\varphi(\epsilon, \delta) I_f(W; X)\Big) \right\}$$

ここで、$u_f\,(x)$はxの非減少関数（詳細は予稿を参照）

ベイズリスクの下界

定理3において、$f(x) = x \log x$ とおくと次の系が得られる。

系 1 [Saito, SITA2022]

$$R_B \geq \frac{1}{2} \sup \left\{ r > 0 : \sup_{\widehat{w} \in \widehat{\mathcal{W}}} \mathbb{P}[\ell(W, \widehat{w}) < r] < \frac{1}{2} - \frac{1}{2} \sqrt{1 - e^{-2\varphi(\epsilon,\delta) I(W;X)}} \right\}$$

系1に関する注意

- ベイズリスクの下界である系1は、定理3の一般公式のひとつの特別な場合にすぎない。しかしながら、簡単な例で数値実験をしてみると、定理に比べてタイトなバウンドになっている。

- 定理3において、関数fとして様々な設定を考えることで、ベイズリスクの下界に関する様々な結果が得られる。
  例えば、$f(x) = x^2 - 1$とすればカイ2乗ダイバージェンスを用いたバウンドが得られ、$f(x) = |x - 1|/2$とすれば変動距離を用いたバウンドが得られる。

本日の発表の概要

準備

Local Differential Privacyの下での パラメータ推定問題

プライバシーと有用性の トレードオフ問題

問題設定 (1/4)

有用性 (Utility) ⟷ トレードオフ ⟷ **プライバシー (Privacy)**

問題設定 (2/4)

有用性の評価基準：XとYとの間の歪み関数

$$d : \mathcal{X} \times \mathcal{Y} \to [0, +\infty)$$

「オリジナルデータXと公開データYとの間の違い」を表す

問題設定 (3/4)

プライバシーの評価基準：f –informativity

$$I_f(X;Y) = \inf_{Q_Y} \sum_{x \in \mathcal{X}} P_X(x) D_f(P_{Y|X=x} \| Q_Y)$$

公開データYを知ることによって得られるオリジナルデータXの情報量（情報漏洩量）を表す

問題設定 (4/4)

有用性の評価基準
歪み関数
$d(X,Y)$

トレードオフ

プライバシーの評価基準
f-informativity
$I_f(X;Y)$

YとXの差異を測る

Yを知ることによって
得たXの情報量を測る

考える問題

歪み関数$d(X,Y)$に何らかの制約を課したもとで
ランダム化メカニズム$P_{Y|X}$ をいろいろ変えたとき、
情報漏洩量f –informativityをどこまで小さくできるのか？

すなわち、

$$\inf_{P_{Y|X}:} \quad I_f(X;Y)$$

$d(X,Y)$に関する何らかの制約式

の理論評価を考える

プライバシーと有用性のトレードオフの結果①

定理 4 [Liao et al., IEEE Trans. IT, 2019]

$$\inf_{\substack{P_{Y|X}:\\ \mathbb{P}[d(X,Y)>D]=0}} I_f(X;Y) = f(0) +$$

$$\inf_{Q_Y} \mathbb{E}_{P_X}\left[Q_Y(B_D(X))\left(f\left(\frac{1}{Q_Y(B_D(X))}\right) - f(0)\right)\right]$$

ここで、

$$B_D(x) := \{y \in \mathcal{Y} : d(x,y) \le D\}$$

$$Q_Y(B_D(x)) := \sum_{y \in B_D(x)} Q_Y(y)$$

定理の拡張

先ほどの定理4では、有用性に関する制約として

$$\mathbb{P}[d(X,Y) > D] = 0$$

を考えたが、この制約を少し緩くすることを考えてみる。
すなわち、$\epsilon \in [0,1)$に対して、

$$\mathbb{P}[d(X,Y) > D] \leq \epsilon$$

という制約を考えると、結果はどのようになるであろうか？

ϵ −cutoff random transformation

この問題を考えるにあたり、以下の定義を導入する。

定義 [Kostina et al., IEEE Trans. IT, 2015]

確率変数Zと$\epsilon \in [0,1)$に対して、ϵ −cutoff random transformationを、次式で定義する。

$$\langle Z \rangle_\epsilon := \begin{cases} Z & \text{if } Z < \eta, \\ \eta & \text{if } Z = \eta \text{ (with prob. } 1-\alpha), \\ 0 & \text{if } Z = \eta \text{ (with prob. } \alpha), \\ 0 & \text{otherwise,} \end{cases}$$

ここで、$\eta \in \mathbb{R}, \alpha \in [0,1)$ は、$\mathbb{P}[Z > \eta] + \alpha \mathbb{P}[Z = \eta] = \epsilon$ から定まる。

プライバシーと有用性のトレードオフの結果②

定理5 [Saito & Matsushima, IEICE Trans., 2022]

$$\inf_{\substack{P_{Y|X}: \\ \mathbb{P}[d(X,Y)>D]\leq\epsilon}} I_f(X;Y) \leq$$

$$\inf_{Q_Y} \sum_{\substack{x\in\mathcal{X}: \\ \left\langle \log \frac{1}{Q_Y(B_D(x))} \right\rangle_\epsilon >0}} P_X(x)\mathbb{E}_{Q_Y}\left[f\left(\frac{\mathbf{1}\{d(x,Y)\leq D\}}{Q_Y(B_D(x))} \right) \right]$$

ここで、1{·}はインディケータ関数を表す

定理5の考察 (1/2)

定理5において、$\epsilon = 0$ とすると

$$\inf_{\substack{P_{Y|X}: \\ \mathbb{P}[d(X,Y)>D]=0}} I_f(X;Y) \leq f(0) + \inf_{Q_Y} \mathbb{E}_{P_X}\left[Q_Y(B_D(X))\left(f\left(\frac{1}{Q_Y(B_D(X))}\right) - f(0)\right)\right]$$

定理4を思い出せば、上式の不等号は実は等号であることがわかる
したがって、定理5の上界は、特別な場合にはタイトになっている

定理5の考察 (2/2)

定理5において、$f(x) = x \log x$ とおくと次の式が得られる。

$$\inf_{\substack{P_{Y|X}: \\ \mathbb{P}[d(X,Y)>D] \leq \epsilon}} I(X;Y) \leq \inf_{Q_Y} \mathbb{E}_{P_X} \left[\left\langle \log \frac{1}{Q_Y(B_D(X))} \right\rangle_\epsilon \right]$$

上式は、有歪み圧縮（非可逆圧縮）の研究におけるKostinaら[Kostina et al., IEEE Trans. IT, 2015]の結果と一致

このことから、本講演で考えているプライバシーと有用性のトレードオフ問題は、情報理論の有歪み圧縮と密接な関係があることがわかる

おわりに (1/2)

本講演では、

- (ϵ, δ) –local differential privacyの下でのパラメータ推定問題
- 有用性とプライバシーのトレードオフ問題

という二つの問題に対して、

◆ 問題設定
◆ 評価基準
◆ その評価基準のもとでの理論限界

を解説した。

おわりに (2/2)

私は、「**工学的操作の限界**」が「**数学的な量**」を用いて
特徴付けられるということが、情報理論の面白さのひとつ
と考えています。

情報理論をよくご存じの方には、この面白さを再確認して頂き、
情報理論にあまり詳しくない方には、この面白さが少しでも
伝われば幸いです。

参考文献 (1/2)

[Asoodeh et al., 2021 IEEE ISIT]
S. Asoodeh, M. Aliakbarpour, and F. P. Calmon, ``Local differential privacy is equivalent to contraction of an f-divergence,'' in Proc. 2021 IEEE International Symposium on Information Theory (ISIT), Melbourne, Australia, pp.545--550, 2021.

[Kostina et al., IEEE Trans. IT, 2015]
V. Kostina, Y. Polyanskiy, and S. Verd¥'u, ``Variable-length compression allowing errors,'' IEEE Trans. Inf. Theory, vol. 61, no. 8, pp. 4316--4330, Aug. 2015.

[Liao et al., IEEE Trans. IT, 2019]
J. Liao, O. Kosut, L. Sankar, and F. P. Calmon, ``Tunable measures for information leakage and applications to privacy-utility tradeoffs,'' IEEE Trans. Inf. Theory, vol. 65, no. 12, pp. 8043 -- 8066, Dec. 2019.

参考文献 (2/2)

[Saito, IEEE ISIT2022]
S. Saito, ``On meta-bound for lower bounds of Bayes risk,'' in Proc. 2022 IEEE International Symposium on Information Theory (ISIT), Espoo, Finland, pp. 3162--3167, 2022.

[Saito & Matsushima, IEICE Trans., 2022]
S. Saito and T. Matsushima, ``Upper Bound on Privacy-Utility Tradeoff Allowing Positive Excess Distortion Probability,'' IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E105.A, no.3, pp.425--427, 2022.

[Saito, SITA2022]
S. Saito, ``Lower Bound of Bayes Risk in Parameter Estimation under Local Differential Privacy,'' 第45回情報理論とその応用シンポジウム，2022年.