局所差分プライバシー方式 GRRとOUEの精度比較

明治大学総合数理学部先端メディアサイエンス学科
菊池研究室 田代大晴

研究背景

- デジタル端末の普及に伴い，ビックデータが収集
- 情報の過度な集積によるプライバシーリスクの懸念

例：**ケンブリッジ・アナリティカ事件**

選挙コンサルの英CA社がFacebook利用者の個人情報や友人情報，**いいね**👍の情報収集

↓

性格特性を分析し，ターゲット広告を行う

↓

英EU離脱決定の国民投票(2016)や米大統領選トランプの勝利(2016)に関与？

サービス事業者 VS ユーザ

とはいえ．．広告で儲けているし..
ビックデータを活用したサービスも
提供していきたい！

VS

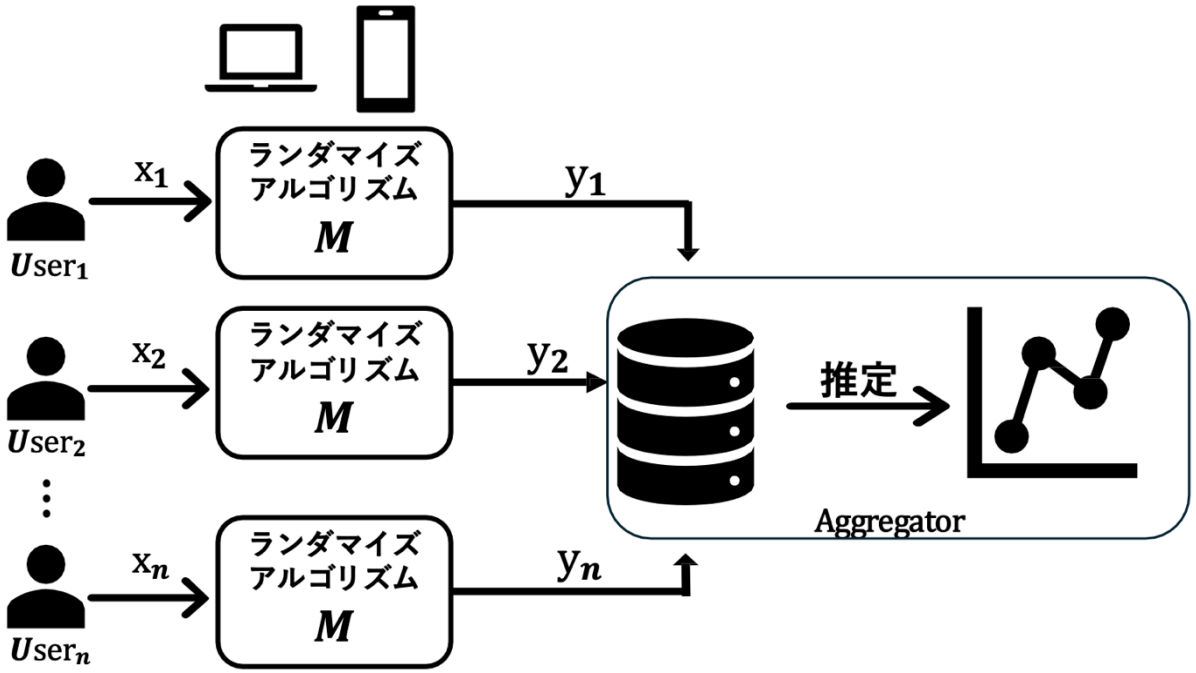
サービスの恩恵を受けてはいるけど
特定されるリスクがあるなんて．．
プライバシーの侵害だ！

Randomized Response

ランダマイズド・レスポンスの例

※「はい」の割合を2倍にし，50％を引くと真の「はい」の割合が大体分かる

局所差分プライバシー



1. デバイス上でランダマイズ
   →プライバシー保護

2. ランダマイズ確率による推定
   →統計値の高い有用性

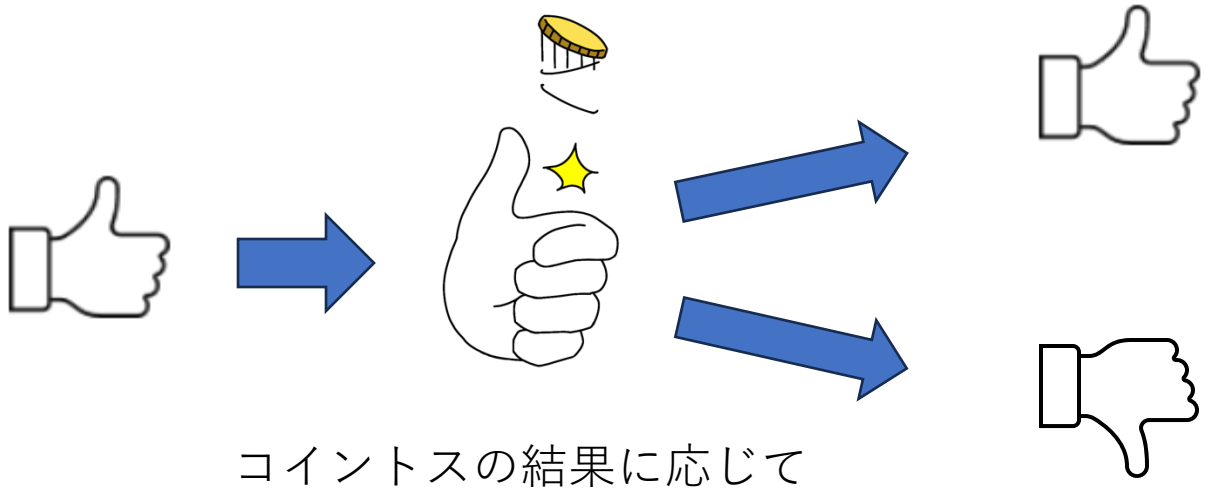
局所差分プライバシー方式 GRR

GRR：**Generalized** Randomized Response

一般化された　　ランダム化　　応答

従来のランダム化応答

例：  は好きか？



コイントスの結果に応じて
応答を変える

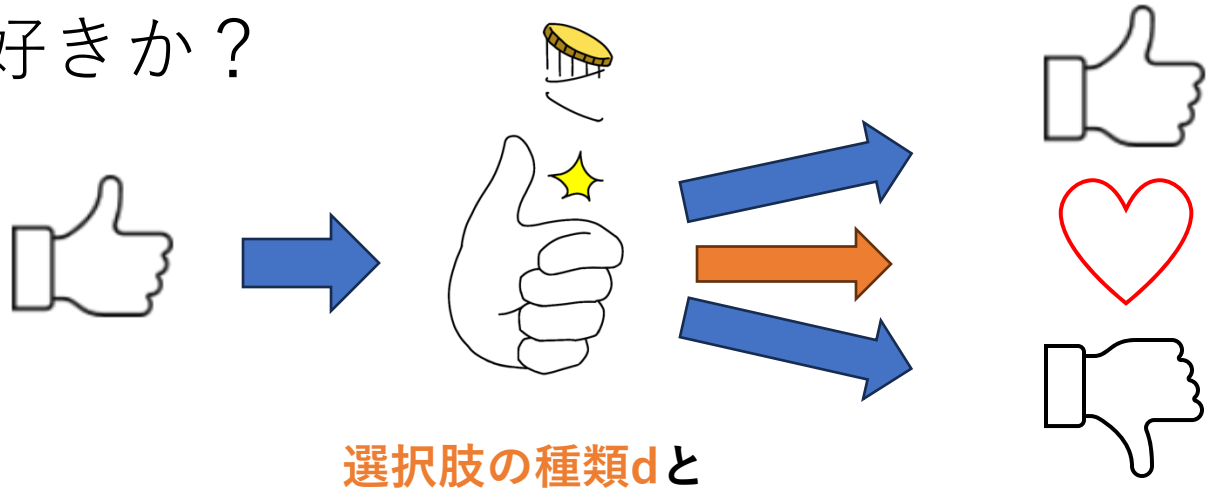
局所差分プライバシー方式 GRR

GRR：**Generalized** Randomized Response

一般化された　　ランダム化　　応答

Generalized RR

例：  は好きか？



3つ以上の選択肢

選択肢の種類dと
プライバシー予算ε
によって決定される確率

GRRの例

1. ユーザの選択肢の種類 $\mathrm{d} = 3$（A, B, Cとする.）
2. プライバシー予算 $\varepsilon = 2$
3. ユーザ数 $n = 10$

ランダマイズ確率

$$\begin{cases} P(\text{出力} = A|\text{入力} = A) = \dfrac{e^{\varepsilon}}{e^{\varepsilon} + d - 1} \sim 0.787 \\ P(\text{出力} = B|\text{入力} = A) = \dfrac{1}{e^{\varepsilon} + d - 1} \sim 0.107 \\ P(\text{出力} = C|\text{入力} = A) = \dfrac{1}{e^{\varepsilon} + d - 1} \sim 0.107 \end{cases}$$

GRRの例

入力: $\{A, A, A, B, B, C, C, C, C, C\}$

↓

出力: $\{A, A, \boldsymbol{C}, B, B, C, C, \boldsymbol{A}, C, C\}$

値	真の度数	出力度数	推定度数	誤差
A	3	3	2.843	-0.157
B	2	2	1.374	-0.636
C	5	5	5.783	+0.783

局所差分プライバシー方式 OUE

OUE：Optimized Unary Encoding

最適化された　単項の　エンコード

※Unary Encoding = One-Hot Encoding

$$A \rightarrow [1,0,0] \rightarrow [1,0,1]$$
$$B \rightarrow [0,1,0] \rightarrow [1,1,0]$$
$$C \rightarrow [0,0,1] \rightarrow [0,0,1]$$

One-Hot Encode　　各ビットごとにランダマイズ

OUEの例

1. ユーザの選択肢の種類 $\mathrm{d} = 3$
2. プライバシー予算 $\varepsilon = 2$
3. ユーザ数 $n = 10$

ランダマイズ確率

$$\begin{cases} P(\text{出力} = 1 | \text{入力} = 1) = \frac{1}{2} = 0.5 \\ P(\text{出力} = 1 | \text{入力} = 0) = \frac{1}{e^{\varepsilon} + 1} \sim 0.119 \end{cases}$$

OUEの例

入力	A	A	A	B	B	C	C	C	C	C
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
One-hot	$[1,0,0]$	$[1,0,0]$	$[1,0,0]$	$[0,1,0]$	$[0,1,0]$	$[0,0,1]$	$[0,0,1]$	$[0,0,1]$	$[0,0,1]$	$[0,0,1]$
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
出力	$[1,0,0]$	$[1,0,\mathbf{1}]$	$[1,\mathbf{1},\mathbf{1}]$	$[0,1,\mathbf{1}]$	$[\mathbf{1},1,0]$	$[0,0,1]$	$[\mathbf{1},0,\mathbf{0}]$	$[0,\mathbf{1},1]$	$[0,0,1]$	$[\mathbf{1},0,1]$

値	真の度数	出力度数	推定度数	誤差
A	3	6	12.32	+9.32
B	2	4	7.374	+5.374
C	5	7	15.52	+10.52

GRRとOUEの精度比較

使用データセット

1. お茶の銘柄のレビューデータ(d=5, n=14)
2. 購入履歴データ(d=44, n=49,742)

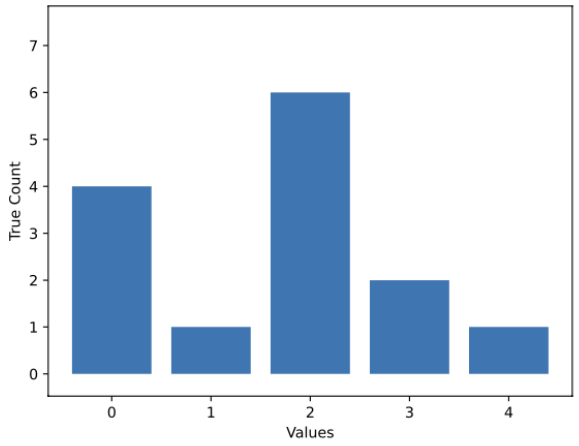


図 2　Dataset1 の頻度分布（お茶の銘柄の評価値）

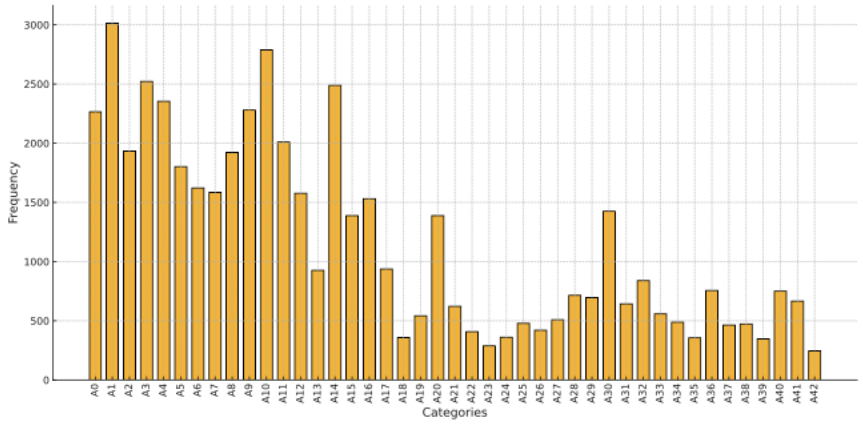


図 3　Dataset2 の頻度分布（ズボンの購入履歴）

※ 0: お～いお茶, 1: 伊右衛門, 2: 綾鷹, 3: 生茶, 4: 明大茶

GRRとOUEの精度比較

適用例($\epsilon = \log(20)$)

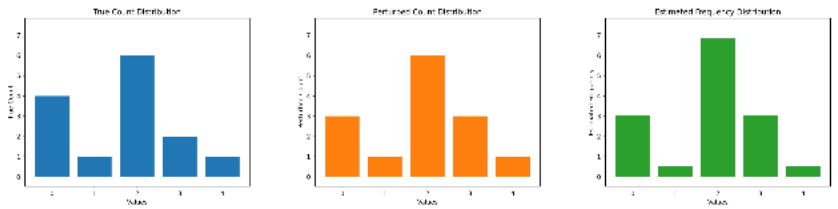


図 4　Dataset1 に GRR を適用した際の頻度分布の例

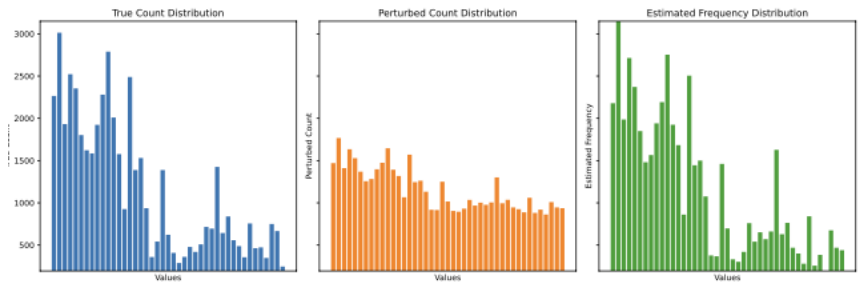


図 5　Dataset2 に GRR を適用した際の頻度分布の例

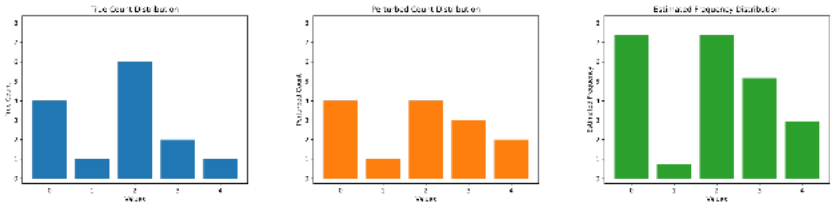


図 6　Dataset1 に OUE を適用した際の頻度分布の例

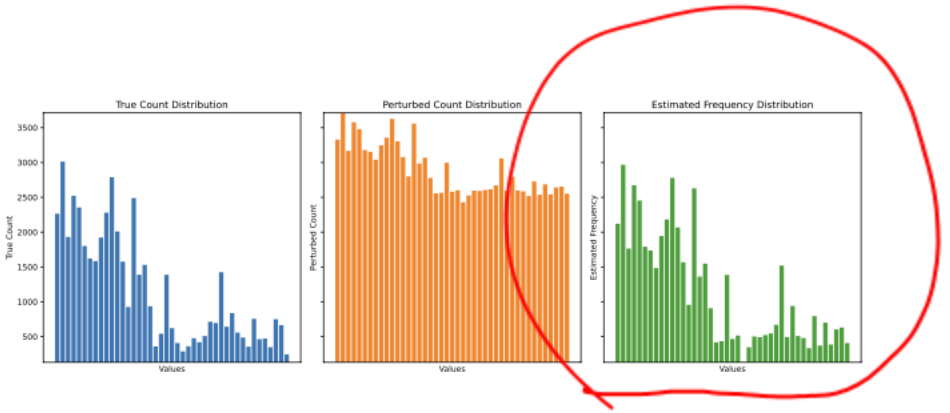


図 7　Dataset2 に OUE を適用した際の頻度分布の例

カテゴリーサイズが多いとOUEの精度は高い

GRRとOUEの精度比較

プライバシ予算を変化させMSEを比較

$\varepsilon < \log\frac{d-2}{3}$でOUEのMSEが小さくなる

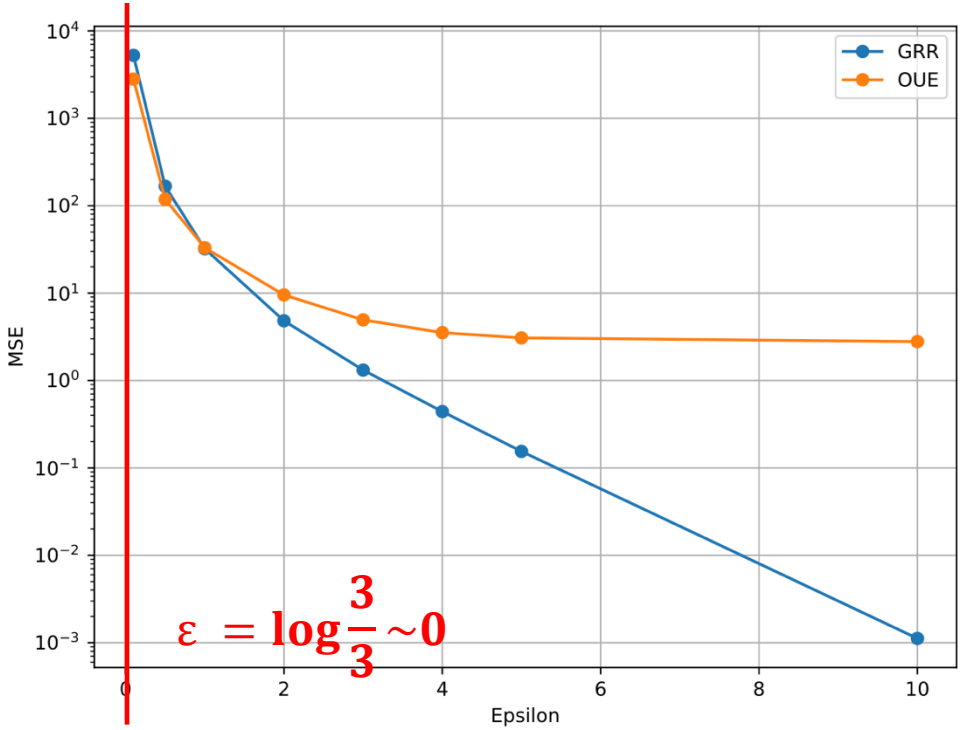


図 8　GRR と OUE の誤差比較（Dataset1）

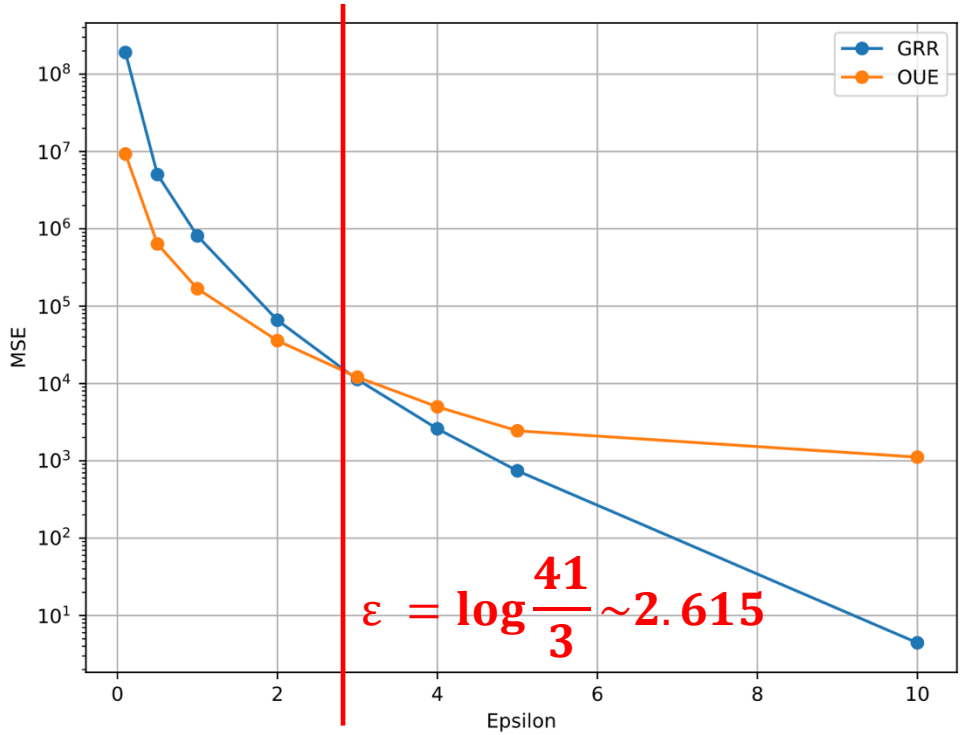


図 9　GRR と OUE の誤差比較（Dataset2）

GRRとOUE

	GRR	OUE
エンコード	しない	**Unaryエンコーディング**
ランダマイズ	元の値を報告する確率:$\frac{e^{\varepsilon}}{e^{\varepsilon}+d-1}$ 他の値を報告する確率:$\frac{1}{e^{\varepsilon}+d-1}$	各ビットに対して, $P(\text{出力}=1\|\text{入力}=1)=\frac{1}{2}$ $P(\text{出力}=1\|\text{入力}=0)=\frac{1}{e^{\varepsilon}+1}$
メリット	・**実装がシンプル** ・通信コストが低い ・$d < 3e^{\varepsilon}+2$だとOUEより精度高	・**ビットごとにノイズを付加するため，dが大きいと推定精度がGRRと比べて高くなる**
デメリット	・dが大きいとノイズが増えてしまい，推定精度が低い	・通信コストが高い ・計算コストがやや高い

感想

よかった点

1. GRRとOUEの精度比較を2つのDatasetを用いて行なった
2. $d < 3e^{\varepsilon} + 2$の点で精度が逆転することを確認
3. OUEがUnary Encodingとビットごとのノイズ付加によって最適化されていることを理解できた

今後の課題

1. 回答数nやdの大きさの未検証パターンがある
2. データの偏りの大小に関しても未検証パターンがある