

多次元データに対する局所差分 プライバシー手法CALMの評価

菊池研究室 B4 山本 悠太



研究背景

- 企業や政府機関が収集するデータの量は増大し、同意のない情報提供によるプライバシー侵害などに対する個人情報の保護が重要な課題となっている。
- プライバシー侵害のリスク軽減対策としてユーザサイドで情報を加工し送信する**Local Differential Privacy**(以下**LDP**)が存在する。
 - 応用例：Appleの絵文字使用頻度解析など
- 1次元に対するLDP方式はRR, CMS, RAPPORなど多数存在するが、多次元データに対するLDP方式に関しては十分な検討がなされていない。

LDPの概要

- 「好きな絵文字」を調査しているとする    
 - しかし、好きな絵文字を言うのをためらう人がいるかもしれない
- そこで、以下のように調査をする
 1. コインを投げる
 2. 表なら、本当に好きな絵文字を答える
 3. 裏なら、選択肢の中からランダムな絵文字を答える
 - 表と裏が出る確率はプライバシー予算 ϵ というパラメータで決定される
 - ϵ が大きいほど「表」が出やすい
- このようにすると、「個人がどの絵文字が好きなのか」はわからないが全体の傾向は統計的に推定できる

多次元のLDPの困難点

- コストの問題

- 考慮する属性数が増えることによりプライバシー予算 ϵ が莫大に
- 属性間の依存関係について考慮する必要がある, 計算コストも増大する

- 例

- 「好きな絵文字の質問」と、「好きなLINEスタンプの質問」
- 質問が2個になると、コインを振る回数が2回になる→ ϵ が倍に
- 「絵文字」と「LINEスタンプ」の嗜好には関連がありそうだが、別個で集計をすると関連性が見えなくなる→依存関係を保ちつつ計算を行う必要性



多次元のLDPの先行研究：CALM[Zhang, 2018]

- 1. データ収集：** 各ユーザーは、自身の多次元データを持つ
 - 例：**k=3次元** **メインディッシュ** 🍕（ピザ / ハンバーガー / パスタ）、**サイドメニュー** 🍟（フライドポテト / サラダ / スープ）、**ドリンク** 🥤（コーラ / お茶 / コーヒー）
 - ユーザーは、各属性の値をローカルでランダム化し、ノイズを加える
- 2. 周辺分布の推定：** 収集されたノイズ付きデータを基に、集計者はk次元の周辺分布を推定する
 - 集計者（レストラン）は、お客さんが送ったノイズ付きデータを集めて、「どのメニューの組み合わせが人気か？」を推測する
 - ただし、データは完全に独立しているわけではない。例えば、「ピザを頼む人は、コーラを選ぶ傾向がある」「サラダを頼む人は、お茶を選ぶ傾向がある」といった依存関係を考慮する
- 3. データの再構築：** 推定された周辺分布を使用して、元の多次元データの統計的性質を再現する

CALMの実行例

- $n=32$ 人のユーザが3つの属性"Gender", "Age", "Mar"
 - それぞれの属性の値は、"Gender" ∈ {Male, Female}, "Age" ∈ {Adult, Elder}, "Mar" ∈ {Married, Unmarried}

このセルは {Female, Elder, *} = 12人であることを示す

	Married		Unmarried	
	Adult	Elder	Adult	Elder
Male	1	3	5	7
Female	2	4	6	8

全体の頻度分布, $k = 3$

この全体の分布を、 $\ell < k$ 次元の周辺頻度を集計する分割表(view)から求める

それぞれの分割表は、 $\ell = 2$ 次元の周辺頻度を得る, そこから全体の分布に対する制約条件を得る

	Adult	Elder
M	6	10
F	8	12

GenderとAgeの分割表, $\ell = 2$

$$\begin{cases} x_1 + x_5 = 6 \\ x_2 + x_6 = 8 \\ x_3 + x_7 = 10 \\ x_4 + x_8 = 12 \end{cases} \quad (1)$$

	Married	Unmarried
M	4	12
F	6	14

GenderとMaritalの分割表, $\ell = 2$

$$\begin{cases} x_1 + x_3 = 4 \\ x_2 + x_4 = 6 \\ x_3 + x_7 = 12 \\ x_4 + x_8 = 14 \end{cases} \quad (2)$$

(1), (2)を制約条件とした凸最適化問題を解くことで全体の頻度推定を行う

研究目的

- 多次元データへのLDP方式CALMでは, $\ell = 2$ 次元のviewから $k(\ell < k)$ 次元の確率分布を推定することは可能か？
 - $k = 3, 4, 5, \dots$ としたときに推定結果は変化するか？

実験

- $n=64$ 人のデータ
- a_1, a_2, a_3, a_4, a_5 の属性
 - すべての属性が0,1のバイナリ
 - 各属性値は $P(0) = 0.9, P(1) = 0.1$
- $k = 5$ 次元の確率分布を $\ell = 2$ 次元の分割表を用いて推定する
- プライバシーコストは $\varepsilon \rightarrow \infty$

$\{a_1, a_2, a_3, a_4, a_5\}$	P
$\{0,0,0,0,0\}$	0.500
$\{0,0,0,0,1\}$	0.047
$\{0,0,0,1,0\}$	0.093
$\{0,0,0,1,1\}$	0.016
$\{0,0,1,0,0\}$	0.141
$\{0,1,0,0,0\}$	0.047
$\{0,1,0,0,1\}$	0.016
$\{0,1,1,1,0\}$	0.016
$\{1,0,0,0,0\}$	0.109
$\{1,0,0,1,0\}$	0.016
他	0

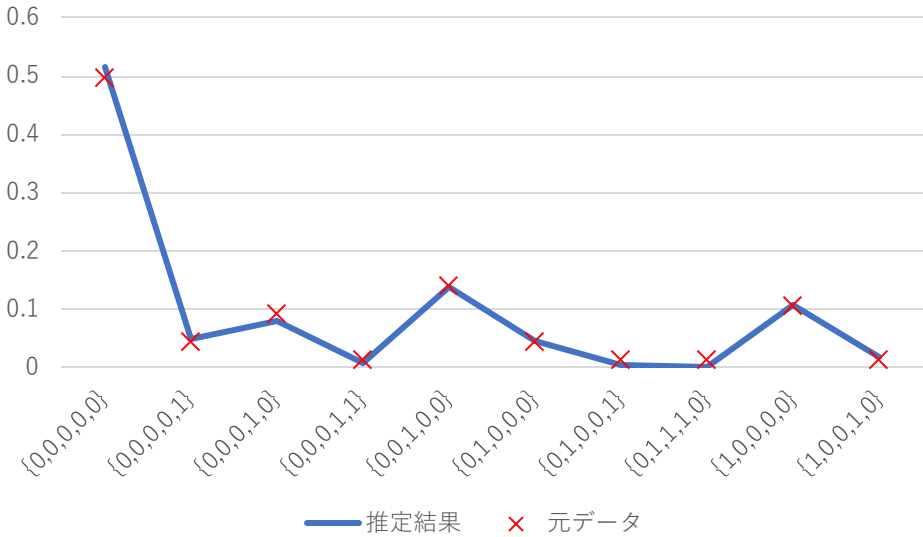
結果

推定結果

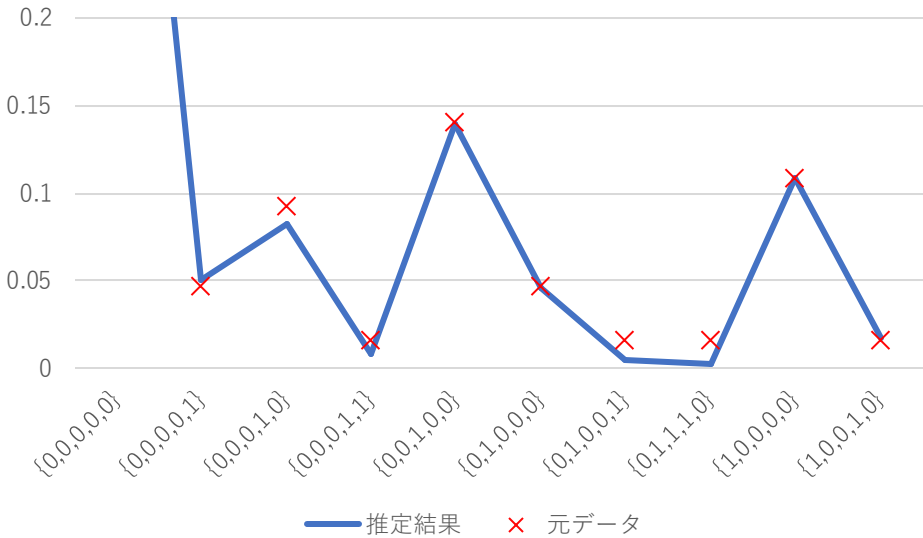
$\{a_1, a_2, a_3, a_4, a_5\}$	確率
$\{0,0,0,0,0\}$	0.516
$\{0,0,0,0,1\}$	0.051
$\{0,0,0,1,0\}$	0.082
$\{0,0,0,1,1\}$	0.008
$\{0,0,1,0,0\}$	0.140
$\{0,1,0,0,0\}$	0.046
$\{0,1,0,0,1\}$	0.005
$\{0,1,1,1,0\}$	0.003
$\{1,0,0,0,0\}$	0.109
$\{1,0,0,1,0\}$	0.017
他	0

元データ

$\{a_1, a_2, a_3, a_4, a_5\}$	確率
$\{0,0,0,0,0\}$	0.500
$\{0,0,0,0,1\}$	0.047
$\{0,0,0,1,0\}$	0.093
$\{0,0,0,1,1\}$	0.016
$\{0,0,1,0,0\}$	0.141
$\{0,1,0,0,0\}$	0.047
$\{0,1,0,0,1\}$	0.016
$\{0,1,1,1,0\}$	0.016
$\{1,0,0,0,0\}$	0.109
$\{1,0,0,1,0\}$	0.016
他	0



MAE=0.0064



考察

- $\ell = 2$ 次元の分割表から $k = 5$ 次元の確率分布を算出することが可能であることが確認できた
 - $k = 3, 4$ のケースは未確認であるが、可能であると予測する
 - それよりも大きな k に関しても、調査していきたい
- 本実験ではプライバシーコスト $\varepsilon \rightarrow \infty$ という極めて単純なケースのみを想定しているため、CALMの正確な評価を行えたとは言い切れない
 - 摂動の強さを変えた時の調査が不可欠である
- 分割表(view)の大きさについても検討の余地がある
 - 今回のケースだと $\ell = 2$ 次元の分割表から $k = 5$ 次元の分割表を得たが、 $\ell = 3, 4$ 次元の分割表から推定した場合、結果が変化するのではないか？

おわりに

- 多次元のLDP方式であるCALMについて、2次元の分割表から5次元の確率分布を推定する実験を行い、評価した。
 - プライバシーコスト $\varepsilon \rightarrow \infty$ の条件下では推定結果を得られ、 $MAE=0.0064$ であることが確認できた。
- 本実験には不十分な点があり、CALMの評価を正しく行うには条件を調整したさらなる実験を行う必要がある。
 - プライバシーコストの増減、分割表の次元の調整など