1F-01

非負集計データのための部分和精度に優れた差分プライバシー適用手法二次元化の一考察Ⅱ

本郷 節之[1]　岡本 拓海[2]　飯塚 皇太[1]　寺田 雅之[3]　鈴木 昭弘[1]　稲垣 潤[1]
北海道科学大学[1]　三和工機株式会社[2]　株式会社ＮＴＴドコモ[3]

1 はじめに

本研究では，元のデータベースに含まれる個々のデータの集合体（個票）から，何らかの条件を満たすデータの個数を数えた数値データの集合体であり，さらに，全体的に疎な分布をとるような集計データを対象とする．集計データに対するプライバシー保護に関しては古くから検討されて来ているが，近年，Dwork らが提案した差分プライバシー基準[1] が，高い安全性を実現するための基準として注目を集めている．差分プライバシー基準は，データベースへの問い合わせを行った際に，「ある特定のデータがデータベースに含まれているか否かを問い合わせ結果から判別することが困難である」ことを安全性の根拠とするプライバシー保護基準である．この差分プライバシー基準を満たす代表的な手法に Laplace メカニズムがある．この手法は，データベースへの問い合わせ結果に対して，平均値が 0 の Laplace ノイズ（Laplace 分布に従う独立な乱数）を付加するものである．たとえば，構成する部分集合が互いに素であるとき，集計データの各セルに確率密度が$\ell = (\epsilon/2)\cdot e^{-\epsilon x}$に従う Laplace ノイズを加えることで差分プライバシーを満たすことができる（ϵはパラメータ）．

しかし，この Laplace メカニズムを大規模集計データに適用すると，「非負制約の逸脱」「部分和精度の劣化」「疎データの密度急増」といった問題への対処が必要となる．そこで，これら 3 点の課題を同時に解消・改善する手法として，我々は「非負精緻化を伴う Privelet 法」を提案した[2]．これは，Xiao らによって提案された Privelet 法[3] が有する，部分和精度が高いという性質を維持しつつも，「非負制約の逸脱」に対する回避と，「疎データの密度急増」の抑制を同時に実現する手法である．

A Study on Two-Dimensional Method for Applying Differential Privacy with High Accuracy in Local Summation
Sadayuki HONGO[1], Takumi OKAMOTO[2], Masayuki TERADA[3], Akihiro SUZUKI[1], Jun INAGAKI[1]
1 Hokkaido University of Science
2 Sanwa Koki Co., Ltd.
3 NTT DOCOMO Inc.

非負精緻化を伴う Privelet 法は，一次元データ列を対象としたものであり，二次元データに適用する際には，一旦一次元データ配列に変換を行った上でプライバシー保護処理を適用し，その上で，処理された一次元データを，改めて二次元データへ戻す処理が必要となっていた．しかし，上述した通り，地理的に分布した集計データは二次元状に分布していることから，そのプライバシー保護処理においても，二次元データに直接適用できる手法の開発が望まれる．そこで我々は，非負精緻化を伴う二次元 Privelet 法の開発を進めている．本研究ではその誤差（RMSE）特性の評価結果について述べる．

2 方法

我々は既に非負精緻化を伴う Privelet 法を二次元化する基本アルゴリズムの提案を行った[4]．いま，2×2 基本構造からなる二次元 Haar Wavelet を採用すると，図 1 に示す二次元ツリー構造が構成される．ここでリーフ層には，はじめ，秘匿対象となる集計データ$v_{x,y}$が格納されており，一方，ノード層には，Wavelet 係数($cA_{h,x,y}$または$cD_{h,x,y}$)が格納される（hは階層番号）．

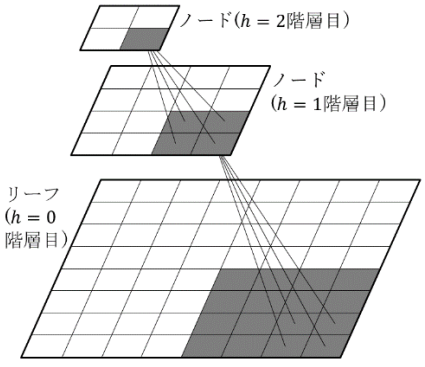


図 1　二次元ツリー構造

2.1 Wavelet 変換および逆 Wavelet 変換

いま，階層番号が$h=(0,1,2,\cdots,H)$で表され，1 層のリーフ($h=0$)とH層のノード($0<h\leq H$)から成る二次元ツリーを考える．最初の Wavelet 変換(第0階層)を行った際の近似係数$cA_{h,x,y}$および詳細係数$cD_{h,x,y}$は，次式で求められる．ここで

$x=(0,1,2,\cdots,X-1)$ および $y=(0,1,2,\cdots,Y-1)$ は各階層における二次元座標を表す．

$$
\begin{aligned}
cA_{0,0,0} &= \frac{v_{0,0}+v_{1,0}+v_{0,1}+v_{1,1}}{4} \\
cD_{0,1,0} &= \frac{v_{0,0}-v_{1,0}+v_{0,1}-v_{1,1}}{4} \\
cD_{0,0,1} &= \frac{v_{0,0}+v_{1,0}-v_{0,1}-v_{1,1}}{4} \\
cD_{0,1,1} &= \frac{v_{0,0}-v_{1,0}-v_{0,1}+v_{1,1}}{4}
\end{aligned} \qquad (1)
$$

続いて次階層の変換（第1階層）を行うのに先立って，$cA_{0,x,y}$の値を1階層上のノード$\left(1,\frac{x}{2},\frac{y}{2}\right)$へコピーする．その上で，第1階層の各ノードに対して，上記式(1)に準ずる処理を行う．以上の処理を最上位層まで再帰的に繰り返すことで二次元 Wavelet 変換を実現できる．

一方，逆 Wavelet 変換の処理は，Wavelet 変換処理のプロセスを逆にたどる．これにより改めて第0階層においてリーフ値を得ることができる．

2.2 ノイズ付加

提案手法では，Wavelet 変換（順変換）の後，詳細係数$cD_{h,x,y}$（最上位層のみ近似係数$cA_{H,0,0}$含む）に対して確率分布$\ell\left(x:\lambda'(h)\right)=\frac{1}{2\lambda'(h)}e^{(-x/\lambda'(h))}$に従う Laplace ノイズを付加する．階層$h$におけるノイズ強度は$\lambda'(h)=\alpha\cdot\frac{H\cdot\lambda}{4^h}$とする（$\alpha=\frac{3}{4}$，最上位層のみ$\frac{4}{4}$）．ここで$\ell,x$および$\lambda=\frac{1}{\epsilon}$はそれぞれ確率密度，確率変数，ノイズ強度を表す．

2.3 非負精緻化

非負精緻化処理は，逆 Wavelet 変換処理の過程で負値の発生を排除する処理である．いま，h層での逆 Wavelet 変換処理の結果得られた 4 変数$cA^*_{h-1,2x,2y}, cA^*_{h-1,2x+2,2y}, cA^*_{h-1,2x,2y+2}, cA^*_{h-1,2x+2,2y+2}$のうちのいずれか（複数もあり得る）に負の値が現れたら，次式に従って，3 つの変数$cD^*_{h,x+1,y}$, $cD^*_{h,x,y+1}, cD^*_{h,x+1,y+1}$に対して非負精緻化処理を施し，精緻化後の$cD$値を用いて改めて逆 Wavelet 変換処理を行う（ノイズ付加の結果得られた値は*を付して，また，非負精緻化の結果得られた値は+を付して，それぞれ表している）．

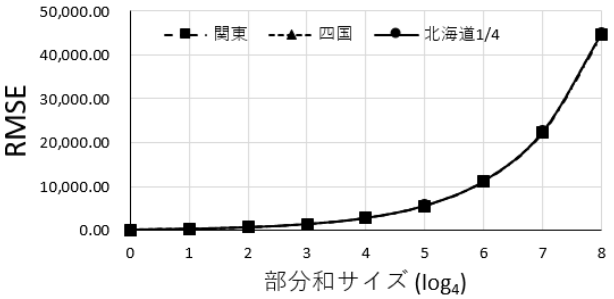
$$
cD^+_{h,x+1,y}=\beta\cdot cD^*_{h,x+1,y}, cD^+_{h,x,y+1}=\beta\cdot cD^*_{h,x,y+1}, cD^+_{h,x+1,y+1}=\beta\cdot cD^*_{h,x+1,y+1}
$$

$$
\beta=\frac{cA^*_{h,x,y}}{\left|Min\left(cA^*_{h-1,2x,2y}, cA^*_{h-1,2x+2,2y}, cA^*_{h-1,2x,2y+2}, cA^*_{h-1,2x+2,2y+2}\right)-cA^*_{h,x,y}\right|}
$$

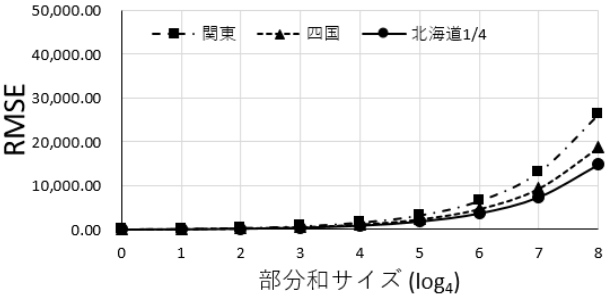
3 評価と考察

図２に二次元 Privelet 法を適用したメッシュ人口データ（関東，四国，北海道 1/4；メッシュ数 $2^8\times2^8$）の，部分和サイズによる RMSE の変化を示す．(b)の処理には非負精緻化を加えている．

(a)を見ると①どの地域もほぼ同程度の RMSE 値である ことがわかる．続いて(a)，(b)を見比べると，②非負精緻化により RMSE 値が小さくなっている．(b)では③データ密度（関東＞四国＞北海道）がより低い地域ほど非負精緻化の効果が大きい．これらの性質は全て一次元方式と同様であり，提案手法の妥当性を示唆している．



（a）非負精緻化なし



（b）非負精緻化あり

図２　部分和サイズによる RMSE の変化

4 おわりに

先に提案した非負精緻化を伴う二次元 Privelet 法の妥当性を誤差特性の観点から確認した．今後更に多角的な特性評価を進める必要がある．

謝辞

本研究は日本学術振興会科学研究費補助金基盤研究(C)（課題番号：19K11970）の補助を受けて行なわれた。

参考文献

[1] Dwork C.: Differential Privacy, Proc. 33rd Intl. Conf. Automata, Languages and Programming - Volume Part II, Bugliesi, M., Preneel, B., Sassone, V. and Wegener, I. (Eds.), Lecture Notes in Computer Science, 4052, Springer, pp. 1-12 (2006).

[2] 寺田雅之，鈴木亮平，山口高康，本郷節之：大規模集計データへの差分プライバシの適用，情処学論，56, No. 9, pp. 1801-1816 (2015).

[3] Xiao X., et. al.: Differential Privacy via Wavelet Transforms, IEEE Trans. Knowledge and Data Engineering, 23, No. 8, pp. 1200-1214 (2011).

[4] 本郷，寺田，鈴木，稲垣：非負集計データのための部分和精度に優れた差分プライバシー適用法二次元化の一考察Ｉ，電気・情報関係学会北海道支部連合大会，pp.129-130 (2019).