負のℓ_2正則化に基づく大規模スパースデータに対する差分プライバシーの適用

松本 一佐[1,a)]　松井 秀俊[2]　寺田 雅之[3,4,5]

概要：現実世界のデータは，しばしば非負性やスパース性といった構造的特徴を有する．これらのデータへ差分プライバシー（Differential privacy）を適用する際，単純なノイズ付加はデータの有用性を損なうため，本来の構造を維持する設計が不可欠となる．特に，非負性，スパース性に加え，人口統計における総人口のように合計値を保持する総数制約は実用上きわめて重要である．スパース性を保証する方法としてスパース推定を適用する方法が考えられるが，既存のスパース推定法の多くは非負性および総数制約を保証しない．一方で，これらの制約を考慮した手法はスパース性の回復が不十分であったり，推定値にバイアスが生じたりする課題があった．そこで本研究では，負のℓ_2正則化項を導入したスパース推定法の適用を提案する．本手法は，非負制約と総数制約を厳密に満たしつつ，適切なスパース性の回復と推定バイアスの低減を同時に達成する．シミュレーションデータを用いた実験およびメッシュ人口データへの適用を通して，提案手法の有効性を検証する．

キーワード：差分プライバシー，スパース推定，単体制約

Differential Privacy for Large-Scale Sparse Data via Negative ℓ_2 Regularization

Kazusa Matsumoto[1,a)]　Hidetoshi Matsui[2]　Masayuki Terada[3,4,5]

Abstract: Real-world data often exhibit structural properties such as non-negativity and sparsity. When applying Differential Privacy (DP) to such data, naive noise addition can severely degrade utility, making it essential to design mechanisms that preserve the original structure. In particular, in addition to non-negativity and sparsity, sum constraints—such as preserving the total population in demographic data—are critically important in practice. However, many existing sparse estimation methods do not guarantee these constraints. On the other hand, methods that consider such constraints often struggle to recover sparsity accurately or suffer from biased estimates. To address these issues, we propose applying a sparse estimation method incorporating a negative ℓ_2 regularization term. It strictly satisfies non-negativity and sum constraints while simultaneously achieving appropriate sparsity recovery and reduced estimation bias. Through experiments on simulated data, we demonstrate the effectiveness of the proposed method, and we further validate its practical utility by applying it to real-world mesh population data.

Keywords: Differential privacy, Sparse estimation, Simplex constraint

1. はじめに

近年，ビッグデータや人工知能（AI）の急速な発展に伴

[1] 滋賀大学大学院データサイエンス研究科
Graduate School of Data Science, Shiga University
[2] 滋賀大学データサイエンス学部
Faculty of Data Science, Shiga University
[3] 京都橘大学工学部
Faculty of Engineering, Kyoto Tachibana University
[4] 滋賀大学データサイエンス・AI イノベーション研究推進センター
Data Science and AI Innovation Research Promotion Center, Shiga University
[5] (株) NTT ドコモ
NTT DOCOMO, Inc.
[a)] s6025167@st.shiga-u.ac.jp

い，大量のデータを活用した高度な解析が日常的に行われるようになってきた．しかし，このようなデータ活用の拡大とともに，個人情報の保護に対する懸念が強まってきており，特にデータが第三者に渡る際のプライバシー侵害リスクが深刻な課題として挙げられている．集計データもその例に漏れず，公開する際にプライバシー保護が求められる．集計データは，データベース内の特定の条件を満たすレコードを数え上げた数値（セル）の集合のことであり，特にそれぞれの条件が互いに排反である場合は分割表とよばれる．本稿では，分割表に対するプライバシー保護の方法について検討する．データの開示においては，プライバシー保護の指標が不可欠であり，同時にプライバシー保護とデータの有用性の両立が重要な課題となる．

このような背景の中で，数学的に証明可能なプライバシー保証を提供する技術として注目されているのが，差分プライバシー（Differential privacy）である．差分プライバシーとは，個人情報が暴露されるリスクを抑えながら精度よい統計分析を行うためのプライバシー保護の枠組みである．差分プライバシーは特定のプライバシー保護手段を指すものではなく，具体的な保護手段はメカニズムとよばれる．最も代表的なメカニズムである Laplace メカニズム [2] は，データに Laplace 分布に従うランダムなノイズを加えることで，個々のデータが解析結果に与える影響を曖昧にし，プライバシーを保護する．しかし，スパースなデータ，すなわち要素の多くが 0 であるデータに対して Laplace メカニズムを適用すると，スパース性を喪失してしまうという問題がある．加えて，Laplace メカニズムの出力は非負性および総数制約（これらを併せて単体制約という）を満たさない．このことから，Laplace メカニズムは容易に差分プライバシーを実現できるものの，スパース性や単体制約といった実データの重要な構造を保持できず，実用性の観点からは課題がある．

このような課題に対処する方法として，Laplace メカニズムの出力に対して，Lasso に代表されるスパースモデリング [5], [10] を適用し，元データのスパース性を回復する手法が考えられる．Lasso は正則化パラメータを調整することでスパース性の強さを柔軟に制御できるため，用途に応じた復元が可能である．さらに，出力ベクトルに非負性が求められる場合には，係数に非負制約を課した非負 Lasso（nonnegative Lasso）を用いることで，負の値の混入を防ぐことができる．一方，これらは総数制約を満たさないため，復元後にスケーリングや加算補正といった後処理が必要となる．また，非ゼロ成分を縮小推定することによるバイアスや，最適化に比較的高い計算コストを要することも課題として挙げられる．このように，Lasso や非負 Lasso によるスパース推定は，Laplace メカニズムによって損なわれたスパース性の回復には有効な手法であるが，総数制約の取り扱いや推定バイアス，計算効率といった点で依然として実用上の課題が残る．

単体制約を満たしながらスパース推定を行う他のアプローチとしては，Laplace メカニズムの出力を単体上へ射影することで，元のスパースなデータを推定する手法 [13] がある．この手法は，Laplace メカニズムによって失われた単体制約を満たすよう推定を行うことで，スパースな出力を得ることができる．しかし，推定結果のスパース性が過小評価されたり，スパース性の調整が困難であり柔軟性に欠けるといった問題点がある．さらに，Lasso と同様に非ゼロセルを過小推定してしまうという傾向もあり，これにより復元誤差に悪影響を与えてしまうと考えられる．

そこで本稿では，これらの課題を解決する手法として，データの復元において，単体制約下で負の ℓ_2 正則化（negative ℓ_2 regularization）[6] に基づく推定を適用することで差分プライバシーを実現する方法を提案する．多くの正則化が，パラメータの ℓ_1 ノルムに対する制約を通じてスパース性を実現するのに対して，負の ℓ_2 正則化はパラメータの ℓ_2 ノルムを大きく保つことで，単体制約のもとでスパース推定を行うことができる．負の ℓ_2 正則化に基づく差分プライバシーの実現には次の利点がある．まず，特に大きな非ゼロ成分に対して負のノルム制約を課すことで，縮小バイアスを軽減すると同時に，単体制約との効果によりスパース性をより回復できると期待できる．また，正則化パラメータを調整することでスパース性の強さを柔軟に制御できるため，データの特性や目的に応じた推定が可能となる．これにより，スパースなデータに対しても，データのスパース性と非ゼロ成分の情報を保持したまま，実用的な出力を得ることができる．以上の効果を検証するために，数値シミュレーションデータに加えて，メッシュ人口データに提案手法を適用し，復元誤差やスパース性の回復の性能，計算負荷を他の手法と比較する．

2. 準備

2.1 差分プライバシー

差分プライバシーは，データベース内の個人情報が暴露されるリスクを低減しながらも，統計分析を安全に行うためのプライバシー保護の枠組みとして，近年大きな注目を集めている．差分プライバシーの基本的な考え方は，データベースに含まれる個々のレコードが結果に与える影響を最小限に抑えることで，外部の攻撃者が特定の個人情報を推定することを困難にすることである．いま，あるデータベース D_1 から 1 つのレコードを削除した D_2 があるとする．差分プライバシーの目的は，これらの「隣接するデータベース」に対する集計結果がほとんど同一であることを保証することで，個人データの保護を実現する点にある [12]．従来のプライバシー保護技術は，特定の攻撃手法に対してのみ有効なものであったが，差分プライバシーは未知の攻撃に対しても安全性を提供できる汎用性を備えていること

が大きな特徴である [11].

差分プライバシーを満たすための具体的な保護手段はメカニズムとよばれ，Laplace メカニズム [2] や Gaussian メカニズム [3]，圧縮メカニズム [8] など，さまざまな方法が提案されている．差分プライバシーは，これらさまざまなプライバシー保護手段に対して共通の安全性指標を提供する．この安全性指標は，プライバシー損失を表すパラメータ ε で調整され，ε の値が小さいほど強力なプライバシー保護が確保される．この安全性は，以下で定義される．

$$\Pr[\mathcal{K}(D_1) \in S] \leq e^{\varepsilon} \cdot \Pr[\mathcal{K}(D_2) \in S]\,. \tag{1}$$

ただし，$\mathcal{K}$ はメカニズムを表し，S は $\mathcal{K}$ の出力空間 $\mathcal{R}$ の任意の部分空間である（$S \subseteq \mathcal{R}$）．

2.2 Laplace メカニズム

差分プライバシーを実現する代表的なメカニズムである Laplace メカニズム [2] は，問い合わせ結果にノイズを加えることで，個人情報の露出を防ぎながらデータ解析を可能にする手法である．具体的には，位置パラメータが 0 の Laplace 分布に従う乱数（Laplace ノイズ）を，問い合わせ結果に付加することによって実現される．これにより，出力されたデータがある個人の影響を受けたかどうかが判別できないようにする．

一般に，Laplace メカニズムにおけるノイズの尺度は，プライバシー保護の強度を示すパラメータ ε と，ある個人のデータの変化が問い合わせ結果に与える影響度（感度）に基づいて決定される．感度は，隣接するデータベース間での関数の出力の最大変化を示すもので，次式で定義される．

$$\Delta f = \max_{D_1, D_2} \|f(D_1) - f(D_2)\|_1\,. \tag{2}$$

ここで，D_1 と D_2 は隣接するデータベースを表す．分割表に対しては並列合成定理が適用でき，各セル（集計値）に対して尺度パラメータ $1/\varepsilon$ の一律の Laplace ノイズを加えるだけで，ε-差分プライバシーを満たすことが知られている．この場合，感度は $\Delta f = 1$ に設定される．このとき，p 次元の元データベクトル $\boldsymbol{\beta}^* = (\beta_1^*, \ldots, \beta_p^*)^\top \in \mathbb{R}^p$ に対して，Laplace メカニズムによって生成されたノイズ付き出力 $\tilde{\boldsymbol{\beta}} = (\tilde{\beta}_1, \ldots, \tilde{\beta}_p)^\top \in \mathbb{R}^p$ は，次のように定義される．

$$\tilde{\beta}_i = \beta_i^* + Z_i,\quad Z_i \sim \mathrm{Laplace}\,(1/\varepsilon)\,,\quad i = 1, \ldots, p \tag{3}$$

このように，各セルに独立な Laplace ノイズを付加することで，差分プライバシーを満たす分割表を作成できる．

その一方で，要素の多くがゼロであるスパースなデータに対して Laplace メカニズムを適用すると，ゼロ要素に対してもノイズが付加されるため，元々ゼロであるべき位置に非ゼロの値が生じ，データのスパース性を喪失してしまうという問題がある．加えて，ノイズの生成に使用される Laplace 分布は負の値が生じる確率も高いため，非負であるはずのデータに負の値が混入するという問題も発生する．また，Laplace メカニズムの出力は合計値の保持も保証しない．なお，すべての要素が非負であり，かつその合計値が元のデータと一致するという制約は，単体制約（simplex constraint）とよばれる．このように，Laplace メカニズムの出力は単体制約を満たさず，たとえばメッシュ人口データのような現実の応用においては，「負の人数」や「総人口の不整合」といった不適切な結果を生む可能性がある．

2.3 スパースモデリングを用いた復元

前節で説明した Laplace メカニズムにおけるスパース性喪失の課題に対処する方法として，Laplace メカニズムの出力に，Lasso をはじめとするスパースモデリング [5], [10] を適用し，元データのスパース性を回復する手法が考えられる．このアプローチでは，Laplace ノイズが付加された $\tilde{\boldsymbol{\beta}}$ を目的変数ベクトルとみなし，ノイズの影響を受ける前の真のベクトル $\boldsymbol{\beta}^*$ を，スパース推定によって復元する．具体的には，Lasso による復元は次のような最適化問題として定式化される．

$$\hat{\boldsymbol{\beta}} = \underset{\boldsymbol{\beta} \in \mathbb{R}^p}{\mathrm{argmin}} \left\{ \|\tilde{\boldsymbol{\beta}} - \boldsymbol{\beta}\|_2^2 + \lambda \|\boldsymbol{\beta}\|_1 \right\}. \tag{4}$$

ここで，$\lambda > 0$ は正則化パラメータであり，スパース性の強さを制御する役割を持つ．Lasso による復元を行うことで，Laplace ノイズが付加されスパース性を喪失した出力から，元のスパースな構造を持つベクトルを回復することが期待される．しかしながら，Lasso による推定結果には負の成分が現れる可能性があり，非負性が求められるデータにおいてはこの点が実用上の問題となる．また，Lasso による推定結果は総数制約も満たさないため，単体制約を満たす必要のあるデータには適さない．

これらの課題に対処する方法として，まず非負 Lasso によって復元を行う．非負 Lasso は次のような最適化問題として定式化される．

$$\hat{\boldsymbol{\beta}} = \underset{\boldsymbol{\beta} \in \mathbb{R}_+^p}{\mathrm{argmin}} \left\{ \|\tilde{\boldsymbol{\beta}} - \boldsymbol{\beta}\|_2^2 + \lambda \|\boldsymbol{\beta}\|_1 \right\}. \tag{5}$$

非負 Lasso により復元されたベクトルに対して，非ゼロ成分への一様な加算・減算，あるいは全体のスケーリングによって合計値を調整する．ただし，これらの補正は後処理的に制約を満たすものであり，最適化問題の制約として単体制約を直接組み込むことは，Lasso のような凸最適化の枠組みでは不可能である．また，Lasso や非負 Lasso による推定結果は，非ゼロ成分の推定値をゼロの方向へ縮小させるバイアスを持つという欠点があることも知られている．さらに，Lasso の最適化は凸最適化問題であるものの，後述する単体への射影を用いた手法と比較すると，計算コストが高くなるという課題もある．

2.4 単体への射影

単体制約を満たしながらスパース推定を行う他のアプローチとして，Laplace メカニズムの出力を単体上へ射影する手法 [1], [7], [13] がある．いま，p 次元空間における単体 $c\Delta^p$ を，次で定義する．

$$c\Delta^p = \left\{ \boldsymbol{\beta} \in \mathbb{R}_+^p \mid \mathbf{1}^\top \boldsymbol{\beta} = c \right\}. \tag{6}$$

ただし，$\mathbf{1}$ は全ての要素が 1 の p 次元ベクトルとする．真のベクトル $\boldsymbol{\beta}^* \in \mathbb{R}^p$ に Laplace ノイズが加えられたベクトル $\tilde{\boldsymbol{\beta}} \in \mathbb{R}^p$ に対して，単体 $c\Delta^p$ への射影 $\hat{\boldsymbol{\beta}}$ は，以下の最適化問題により定式化される．

$$\hat{\boldsymbol{\beta}} = \underset{\boldsymbol{\beta} \in c\Delta^p}{\operatorname{argmin}} \left\{ \|\tilde{\boldsymbol{\beta}} - \boldsymbol{\beta}\|_2^2 \right\}. \tag{7}$$

このとき，この問題の解 $\hat{\boldsymbol{\beta}}$ は，閾値 θ を用いて次のように一意に定まり，効率的に計算できる [4].

$$\hat{\beta}_i = \begin{cases} \tilde{\beta}_i - \theta & \text{if } \tilde{\beta}_i > \theta, \\ 0 & \text{otherwise,} \end{cases} \qquad i = 1, \ldots, p. \tag{8}$$

閾値 θ は以下の手順で求めることができる．まず，$\tilde{\boldsymbol{\beta}}$ の要素を降順にソートしたものを $\mu_1 \geq \mu_2 \geq \cdots \geq \mu_p$ とおく．次に，以下を満たす ρ を求める．

$$\rho = \max \left\{ j \in [p] \;\middle|\; \mu_j - \frac{1}{j} \left(\sum_{r=1}^{j} \mu_r - c \right) > 0 \right\}. \tag{9}$$

このとき，閾値 θ は次の式で与えられる．

$$\theta = \frac{1}{\rho} \left(\sum_{i=1}^{\rho} \mu_i - c \right). \tag{10}$$

人口データなど，セル値が整数であることが求められる場合は，$\hat{\boldsymbol{\beta}}$ に対してさらに整数制約も満たす必要がある．解 $\hat{\boldsymbol{\beta}}$ に最も近い $c\Delta^p$ 上の整数格子点は，単体制約・整数制約を同時に満たす．またこの点は，これらの制約を満たす点の中で，ノイズ付きベクトル $\tilde{\boldsymbol{\beta}}$ からの ℓ_2 距離も最小となることが知られている [13]．この補正は，各成分に対して小数点以下を切り上げ・切り下げることで容易に実装可能である．

この一連の射影手法は，単体制約を厳密に満たしながら，効率的に計算可能である点で有用である．また，式 (8) にも示されているように，閾値 θ 以下の値を切り捨てることにより，Laplace メカニズムによって喪失したスパース性の部分的な回復も実現できる．一方で，非ゼロ成分が一律に θ だけ削られるため，推定値全体にわたってバイアスが生じ，復元誤差に悪影響が出るという欠点がある．また，本手法はスパース性が十分に確保されない傾向があり，その強さを柔軟に制御することもできない．その結果，ゼロ成分をしばしば非ゼロと推定することがあり，さらにバイアスの影響により非ゼロ成分の推定値の妥当性が損なわれるといった問題が生じる．

3. 提案手法

3.1 負の ℓ_2 正則化

前節で述べたように，従来手法ではスパース性およびその調整，推定値に対するバイアスのいずれかについて課題が残る．これらの課題を解決するため，本稿では，Laplace メカニズムの出力に対して適用可能なスパース推定手法として，単体制約下における負の ℓ_2 正則化（negative ℓ_2 regularization）[6] の導入を提案する．なお，[6] では本手法を回帰モデルの推定法の一つとして提案しており，本研究はこれを Laplace メカニズムの出力に適用したものである．この手法の最適化問題は，次のように負の ℓ_2 ノルムの制約を導入した次の形で与えられる．

$$\hat{\boldsymbol{\beta}} = \underset{\boldsymbol{\beta} \in c\Delta^p}{\operatorname{argmin}} \left\{ \|\tilde{\boldsymbol{\beta}} - \boldsymbol{\beta}\|_2^2 - \lambda \|\boldsymbol{\beta}\|_2^2 \right\}. \tag{11}$$

ただし，$\lambda > 0$ は正則化パラメータとする．この制約により，単体制約を厳密に満たしながら，より極端な構成要素を持つ方向，すなわち一部の成分が大きく他がゼロとなるようなスパースな解を得やすくなり，さらに，従来手法で見られた非ゼロ要素に対するゼロ方向へのバイアスを低減することが期待される．また，正則化パラメータ λ の調整により，解のスパース性を柔軟に制御できる点も本手法の利点の一つである．

式 (11) は非凸であるため，そのままでは最適化が困難となる．そこで [6] は，目的関数を「凸関数 − 凸関数」の形に分解し，前者と後者で反復的に凸最適化問題を解くことで近似解を求める手法を用いた．具体的には，$-\lambda\|\boldsymbol{\beta}\|_2^2$ を $\boldsymbol{\beta}_0 \in \mathbb{R}^p$ のまわりで次のように線形近似する．

$$-\lambda\|\boldsymbol{\beta}\|_2^2 \approx -\lambda\|\boldsymbol{\beta}_0\|_2^2 - 2\lambda\boldsymbol{\beta}_0^\top(\boldsymbol{\beta} - \boldsymbol{\beta}_0). \tag{12}$$

最適化に関係のない定数項を除外すると，最適化問題 (11) は次で表される．

$$\hat{\boldsymbol{\beta}} = \underset{\boldsymbol{\beta} \in c\Delta^p}{\operatorname{argmin}} \left\{ \|\tilde{\boldsymbol{\beta}} - \boldsymbol{\beta}\|_2^2 - 2\lambda\boldsymbol{\beta}_0^\top\boldsymbol{\beta} \right\}. \tag{13}$$

$\boldsymbol{\beta}_0$ に対してこのような反復手順を繰り返すことで，元の非凸問題に対する近似解が得られる．本アルゴリズムは収束性も保証されており，安定した推定が期待できる．アルゴリズムの詳細や収束の理論的証明については，[6] を参照されたい．

3.2 単体への射影を適用したアルゴリズム

3.1 節で述べたアルゴリズムは反復的に凸最適化問題を解く必要があるため，大規模データに対しては計算コストが課題となる．これに対して，2.4 節で紹介した方法を応用することで，より高速に最適化問題を解くことができる．

最適化問題 (11) については，$\lambda < 1/n$ を満たす場合，次のように変形できる [6].

$$\hat{\boldsymbol{\beta}} = \underset{\boldsymbol{\beta}\in c\Delta^p}{\operatorname{argmin}} \left\{ \left\| \frac{\tilde{\boldsymbol{\beta}}}{\gamma} - \boldsymbol{\beta} \right\|_2^2 \right\}, \quad \gamma = 1 - n\lambda. \qquad (14)$$

これは，式 (7) における $\tilde{\boldsymbol{\beta}}$ を $1/\gamma$ 倍スケーリングしたものに対応している．すなわち，ノイズ付きベクトル $\tilde{\boldsymbol{\beta}}$ を $\tilde{\boldsymbol{\beta}}/\gamma$ にスケーリングした上で，単体に射影することにより，元の正則化付き目的関数の最適解が得られることを意味する．この射影操作は，2.4 節で述べたアルゴリズムによって同様に実行可能であり，反復最適化を行うことなく，計算コストを大幅に削減できる．

本手法は単体制約を厳密に満たしながらスパース推定を行うことができる．また，Laplace メカニズムの出力に対する適用では，射影による高速な推定が可能となる点でも実用的である．3 節で述べた既存手法の課題であったスパース性の弱さや調整困難性を克服し，推定バイアスを低減する本手法は，プライバシー保護と実用性を両立させる有効なアプローチとして期待できる．

4. 実験

本章では，これまでに述べた提案手法（Proposed），単体への射影（Simplex），非負 Lasso（NNL），および Laplace メカニズム（LM）について，2 次元の地理空間データであるメッシュ人口データを模して生成した人工データと，国勢調査に基づく実際のメッシュ人口データを用いて数値的に検証を行う．特に，復元精度，推定バイアス，スパース性の回復，計算速度の観点から，各手法の性能を比較・評価する．

4.1 人工データによる検証

評価に用いるデータとしては，メッシュ人口統計を模して生成した 2 次元人口分布データを 1 次元ベクトルに平坦化したデータを使用する．具体的には，都市内人口密度分布モデル族の一つである，正規分布型モデルに従って人工的に生成した．正規分布型モデルは，平面直交座標系 (x, y) における人口密度 $d(x, y)$ を次の式で定義する．

$$d(x, y) = d_c \exp\left[-a\left\{(x - x_c)^2 + (y - y_c)^2\right\}\right]. \quad (15)$$

ここで，(x_c, y_c) は都心の座標であり，本評価では各データにおいて中心に設定した．パラメータ a は正規分布の広がりを，d_c は分布の最大値をそれぞれ制御するものであり，すべてのデータにおいて $d_c = 1000$ に固定した． まず，64×64（$= 4{,}096$ セル）のデータ（**図 1**）を用いて評価を行う．このデータは，非ゼロセルの割合が約 3.3 %となるようにパラメータ a を調整している．

このデータに対して，復元精度，推定バイアス，スパース性の回復，計算速度の観点から，各手法の性能を比較・評価する．復元精度の指標としては，データを一次元ベクトルに変換した元データ $\boldsymbol{\beta}^*$ と，復元後の出力 $\hat{\boldsymbol{\beta}}$ との

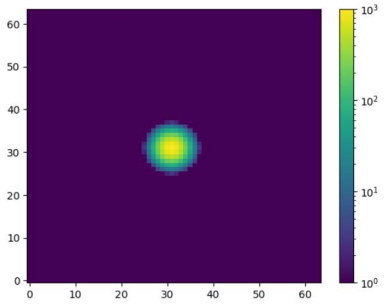

図 1: 評価用メッシュ人口データ（64×64）
Fig. 1 Evaluation mesh population data (64×64).

RMSE（Root Mean Squared Error）を用いて評価を行う．また，推定バイアスの指標として，ME（Mean Error）を用いる．スパース性の回復の指標については，出力に含まれる非ゼロ要素の割合を用いる．なお，人口データを模していることから，各指標の計算には整数補正後の数値を用いた．上記の設定に基づいて，各手法に対してノイズ付きデータの復元を行った．その際，1 つの元データ $\boldsymbol{\beta}^*$ に対して Laplace ノイズをランダムに加える処理を 100 回反復して行い，100 個のノイズ付きデータ $\tilde{\boldsymbol{\beta}}$ に対する復元結果の平均を記録した．また，計算に要する時間を比較するために，64×64（4,096 セル）のデータに加えて，256×256（65,536 セル），1024×1024（1,048,576 セル）の計 3 種類のデータに対して計算時間（100 回の合計）を記録した．なお，いずれのサイズのデータにおいても式 (15) に基づいて生成し，非ゼロセルの割合が約 3.3%になるよう調整している．

ここで，提案手法および非負 Lasso における正則化パラメータ λ の選定方法について述べる．上記の 100 個のノイズ付きデータ $\tilde{\boldsymbol{\beta}}$ それぞれに対して，複数の λ の値を用いて復元処理を行い，RMSE を算出する．そのうえで，すべての $\tilde{\boldsymbol{\beta}}$ に対する RMSE の平均が最小となる λ を最適値として選択した．なお，λ 選定時の RMSE の算出において真のベクトル $\boldsymbol{\beta}^*$ を参照しているため，厳密にはプライバシーバジェットを割く必要がある．しかし，実用上は元データに類似した分布を持つ既存のデータを用いれば十分である．例えば国勢調査の場合，前回の国勢調査の結果などを用いればよい [9].

実験結果を次に示す．まず，図 1 に示した 64×64 メッシュのデータに対して，安全性パラメータ ε を 0.1，1，10 に設定した場合の，データ全体に対する各手法の RMSE を，**表 1** に示す．次に，**図 2**〜**図 4** では，元データの値の範囲ごとにセルを分類し，それぞれに対する RMSE および ME の詳細な結果を示す．ここで，“0”，“1–9”，“10–99”，“100–” は，元データの値がそれぞれの範囲にあるセルのみを対象として RMSE および ME を算出したものである．また，各手法の出力結果に含まれる非ゼロ要素の割合を**表 2** に示す．計算時間の結果を**表 3** に示す．ここで，表

中の Proposed (fixed λ) は，最適な λ が既知であると仮定し，チューニング処理を行わなかった場合における提案手法の計算時間を示し，「-」は，メモリ不足により計算を実行できなかったことを表す．非負 Lasso については，パラメータチューニングを含む総計である．

表 1: 各 ε におけるデータ全体に対する RMSE
Table 1 RMSE over the entire dataset for each ε.

手法	$\varepsilon = 0.1$	$\varepsilon = 1$	$\varepsilon = 10$
Proposed	**4.3133**	**0.5141**	**0.0319**
Simplex	4.8221	0.5538	0.0341
NNL	6.4286	0.6103	0.0324
LM	25.2317	4.6061	0.5069

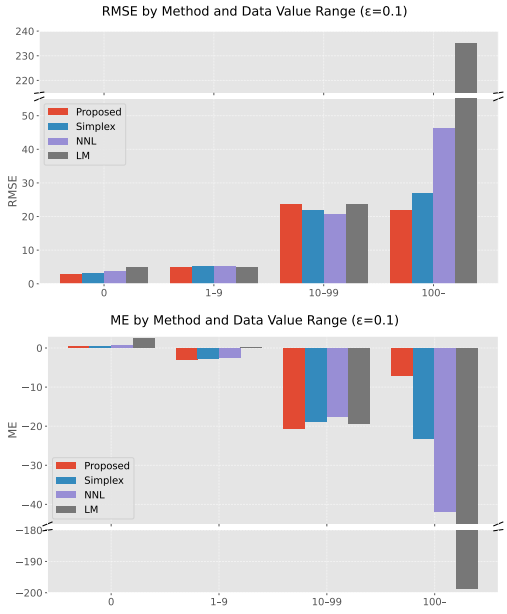

図 2: 人工データに対する RMSE と ME ($\varepsilon = 0.1$)
Fig. 2 RMSE and ME for simulation data at $\varepsilon = 0.1$

表 2: 各 ε における非ゼロ割合（%）
Table 2 Nonzero proportion (%) for each ε.

手法	$\varepsilon = 0.1$	$\varepsilon = 1$	$\varepsilon = 10$
Proposed	4.82	5.63	3.39
Simplex	6.54	6.76	3.40
NNL	8.82	7.23	3.39
LM	46.69	32.41	7.44

4.2 メッシュ人口データへの適用

本節では，各手法の実用性を検証するため，実データを用いた実験を行う．実験には，離島部を除く日本の 2020 年国勢調査に基づく 500m メッシュ人口データ（**図 5**）を用いる．非ゼロセルの割合は 2.10 %である．安全性パラメータとしては $\varepsilon = 0.1$ を設定した．このデータは，4096 × 4096（= 16,777,216 セル）の大規模な構造を持つため，4.1

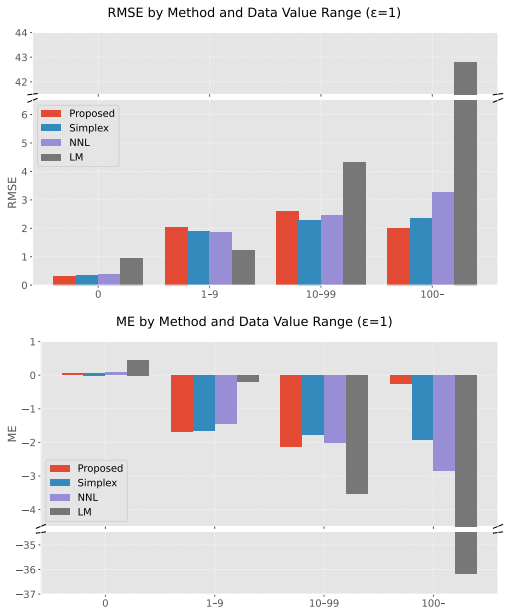

図 3: 人工データに対する RMSE と ME ($\varepsilon = 1$)
Fig. 3 RMSE and ME for simulation data at $\varepsilon = 1$

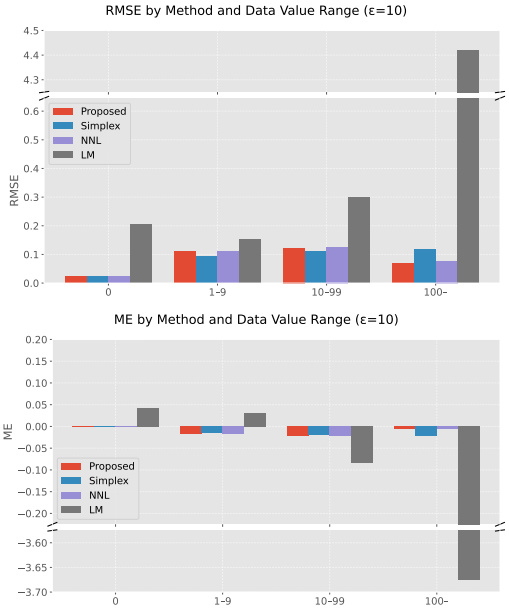

図 4: 人工データに対する RMSE と ME ($\varepsilon = 10$)
Fig. 4 RMSE and ME for simulation data at $\varepsilon = 10$

表 3: 各データサイズにおける計算時間（秒）
Table 3 Computation time (sec) for each data size.

手法	4,096	65,536	1,048,576
Proposed	1.43	19.36	467.63
Proposed (fixed λ)	0.16	2.24	48.25
Simplex	0.13	1.97	49.43
NNL	5.37	60.36	–
LM	0.10	1.59	34.42

節においてサイズ 1024×1024 の人工データで実行不能となった非負 Lasso は本実験から除外する．また，Laplace メカニズムについても，4.1 節における実験で RMSE や ME が他の手法に比べて特に大きかったため，ここでは除外する．残る提案手法および単体への射影を，Laplace ノイズを付加したデータに適用し，RMSE，ME，非ゼロ要素の割合，そして計算時間を算出した．なお，実データに対しては反復回数は 25 回とし，RMSE，ME，非ゼロ要素の割合についてはその平均を，計算時間は合計値を求めた．結果を**図 6** に示す．さらに，それぞれの出力に含まれる非ゼロ要素の割合および計算時間を，**表 4** にまとめた．

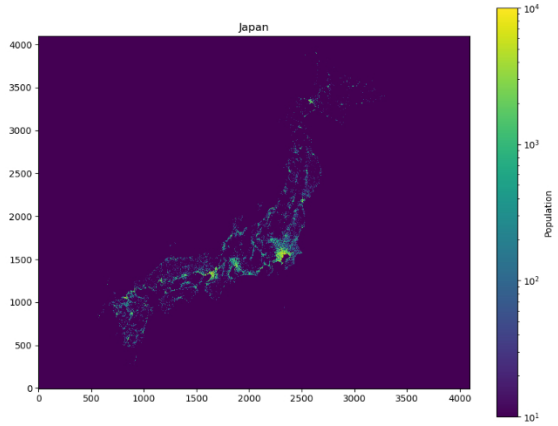

図 5: 2020 年国勢調査に基づく実データ（500m メッシュ）
Fig. 5 Real population mesh data based on the 2020 national census (500m resolution).

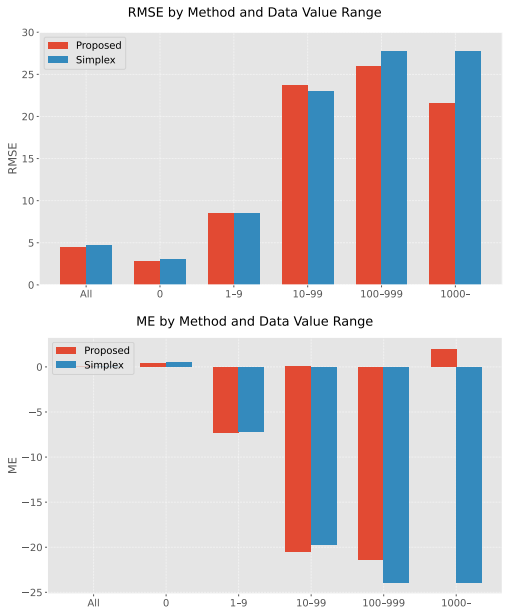

図 6: 実データに対する RMSE と ME ($\varepsilon = 0.1$)
Fig. 6 RMSE and ME for simulation data at $\varepsilon = 0.1$

表 4: 実データにおける非ゼロ割合（%）と計算時間（秒）
Table 4 Nonzero proportion (%) and computation time (sec) on real data.

手法	非ゼロ割合（%）	計算時間（秒）
Proposed	5.30	2409.15
Proposed (fixed λ)	5.30	250.62
Simplex	5.96	233.96

5. 考察

まず，提案手法と他の手法における RMSE および ME の結果を通して，復元誤差および推定バイアスについて考察する．人工データ全体に対する RMSE に関しては，表 1 に示すように，すべての ε で提案手法が最小となり，次いで Simplex，NNL，LM の順になった．ただし，$\varepsilon = 10$ の場合に限り NNL がわずかに Simplex よりも RMSE が小さくなった．なお，データ全体に対しては単体制約を満たすよう復元されているため，すべての手法で ME は 0 になった．実データ全体に対する結果（図 6 の “All”）でも同様の傾向が確かめられた．

RMSE や ME のより詳細な傾向を，元データの値の範囲に応じた結果（図 2 から図 4）から見てみる．真の値が 0 のセルでは，提案手法による RMSE や ME が最小となった．これは，後述するように提案手法が 0 のセルを適切に 0 と推定できたことによると考えられる．真の値が 1 から 99 の範囲では，提案手法は他の手法と比べて RMSE や ME が大きくなる傾向にあったが，100 以上の範囲では大幅に減少している．これは，提案手法の性質により，特に値が大きなデータに対しては逆にバイアスを低減させるという 3.1 節で述べた性質によるものと考えられる．一方で，Simplex では RMSE やバイアスがデータの値に応じて単調に増加傾向にある．これらの傾向は，実データに対する結果（図 6）でも同様である．NNL は，データの値が 99 以下の場合は提案手法や Simplex と同等の傾向を示しているが，100 以上での傾向が ε によって異なる結果となった．具体的には，$\varepsilon = 0.1, 1$ のときは RMSE, ME ともに大幅に悪化したが，$\varepsilon = 10$ ではデータの値が 1 以上 99 以下のセルよりもむしろ小さくなった．$\varepsilon = 0.1, 1$ では合計値が過大に推定されたため，単体制約の補正として出力全体をスケーリングする際に縮小補正によりゼロ方向へのバイアスが強まったことで RMSE が悪化した一方で，$\varepsilon = 10$ では合計値が過小に推定されたことで拡大補正によってバイアスが相殺され，その影響で特に値の大きなセルで精度が向上したと考えられる．LM については，単体制約の補正を行わない場合は理論上 RMSE は $\sqrt{2}/\varepsilon$ に，ME は 0 になる．今回の場合，$\varepsilon = 0.1, 1, 10$ ではそれぞれ RMSE が約 14, 1.4, 0.14 であるため，人工データ全体では他の手法に比べて RMSE が大きい．それに加えて，単体制約を満たす

ために負の推定値を補正した影響で大幅に悪化している．

次に，スパース性の回復について考察する．表 2，4 に示すように，すべての ε において，いずれも非ゼロ要素の割合を高めに推定する傾向が見られた．その中でも，提案手法は実データへの適用も含め，すべての条件において真の非ゼロ率に最も近い結果となり，Simplex，NNL が続く形となった．この結果は，負の ℓ_2 正則化がスパースな解を選好する方向に作用することに起因していると考えられる．このことも，RMSE や ME の減少に繋がったものと考えられる．LM においては，単体制約および非負補正の影響でスパース性が得られているが，ゼロのセルの多くを非ゼロと復元してしまっている．総じて，スパース性の観点では提案手法がノイズの強さにかかわらず安定した回復を実現している傾向がある．

最後に，表 3 および 表 4 から，各手法の計算負荷について考察する．LM は，各要素に独立なランダムノイズを付加するだけの単純な処理であるため，計算量は $\mathcal{O}(n)$ で最も高速かつ安定した実行が可能であり，大規模データでも計算負荷は極めて小さい．提案手法と Simplex は，ともに同一の高速なアルゴリズムを基盤としており，計算量としてはデータのソートが支配的となるため $\mathcal{O}(n \log n)$ である．したがって，一度の復元処理に要する計算時間はほぼ同程度であった．一方，NNL は凸最適化問題であるものの，その計算には提案手法と比較して数倍の時間を要した．さらに，NNL を 1024×1024 という大規模なデータに対して適用を試みた際，メモリ不足により計算を実行できなかった．これに対して，提案手法および Simplex は，図 5 に示した実データ（16,777,216 セル）にも問題なく適用可能であり，大規模データに対しても実用的に運用可能な性能を有していることが確認された．

6. まとめ

本稿では，Laplace メカニズムによりノイズが付加されたデータから，スパース構造を保ちつつ高精度に元データを復元する手法として，単体制約下における負の ℓ_2 正則化の導入を提案した．本手法は，単体制約を厳密に満たしながら，従来手法で課題とされてきたスパース性の回復不足やその調整困難性，推定値のバイアスといった問題の改善が期待された．提案手法の有効性を検証するため，人工的に生成したデータおよび国勢調査に基づくメッシュ人口データを用い，非負 Lasso，単体への射影，Laplace メカニズムと比較実験を行った．その結果，提案手法は RMSE，ME の両観点において，ノイズの強さにかかわらず安定した推定精度を示し，特に元データの値が大きいセルに対するバイアス低減効果が顕著であった．また，スパース性の回復においても，他の手法と比較して構造を適切に復元でき，ノイズに対して堅牢に推定できることが確認された．さらに，大規模な実データに対する実験では，提案手法は単体への射影と同程度の計算時間で処理可能であり，非負 Lasso が処理不能となるような規模のデータに対しても適用可能であった．この結果は，提案手法がスパース推定手法としてだけでなく，現実的な計算資源のもとでも運用可能な高い実用性を備えていることを示している．

今後の課題としては，正則化パラメータ λ の選択方法が挙げられる．本研究では RMSE を基準にパラメータ選択を行ったが，これによりスパース性の調整可能性という提案手法の特長を十分に活かせていない．今後は，スパース性を指標としたパラメータ選択など，用途や目的に応じた柔軟な評価基準を検討する必要がある．さらに，小さな非ゼロ要素に対するバイアス低減や，より適切なスパース構造の復元を実現するために，他の非凸正則化手法との統合も今後の展望として挙げられる．また，データのスパース性を活用した計算量の削減についても検討したい．

謝辞　本研究は、JST 経済安全保障重要技術育成プログラム (JPMJKP24U5) の支援を受けたものです．

参考文献

[1] Condat, L.: Fast projection onto the simplex and the ℓ_1 ball. *Math. Program.*, 158(1):575-585, 2016.

[2] Dwork, C., McSherry, F., Nissim, K., and Smith, A.: Calibrating noise to sensitivity in private data analysis. *Lecture Notes in Computer Science*, 3876:265–284, 2006.

[3] Dwork, C. and Roth, A.: The algorithmic foundations of differential privacy. *Found. Trends. Theor. Comput. Sci.*, 9(3-4):211407, 2014.

[4] Duchi, J., Shalev-Shwartz, S., Singer, Y., and Chandra, T.: Efficient projections onto the ℓ_1-ball for learning in high dimensions. *Proc. 25th Int. Conf. Machine Learning (ICML)*, 272–279, 2008.

[5] Hastie, T., Tibshirani, R. and Wainwright, M. *Statistical learning with sparsity*. CRC Press, 2015.

[6] Li, P., Rangapuram, S. S., and Slawski, M.: Methods for Sparse and Low-Rank Recovery under Simplex Constraints. *Statist. Sinica*, 30(2):557–577, 2020.

[7] Li, X., Wang, C., and Cheng, G. Statistical Theory of Differentially Private Marginal-based Data Synthesis Algorithms. *11th Int. Conf. Learn. Represent. (ICLR)*. 2023.

[8] Li, Y. D., Zhang, Z., Winslett, M., and Yang, Y.: Compressive mechanism: Utilizing sparse representation in differential privacy. *Proc. 10th Annu. ACM Workshop Privacy Electron. Soc.*, 177–182, 2011.

[9] 加藤駿典, 松井秀俊, 寺田雅之: 圧縮メカニズム再考：スパースな観測行列を用いた圧縮センシングによる差分プライバシーの実現，情報処理学会論文誌 65(9):1324–1338.,2024.

[10] 川野秀一, 松井秀俊, 廣瀬慧: スパース推定法による統計モデリング，共立出版，2018.

[11] 寺田雅之: 差分プライバシーとは何か，情報処理学会論文誌 63(2):58–63，2019.

[12] 寺田雅之: 差分プライバシの基礎と動向，情報処理 61(6):591–599，2020.

[13] 寺田雅之, 山口高康, 本郷節之: 高次元大規模データへの差分プライバシー適用のための最適精緻化法，*2017 Symposium on Cryptography and Information Security*，2017.