解説論文

動的システムにおける レアイベントモデリングとその応用
—安定分布によるアプローチ—

Rare-event Modeling for Dynamical Systems and Its Applications: Stable Distribution Approach

伊藤海斗 Kaito ITO
加嶋健司 Kenji KASHIMA

アブストラクト　動的な現象をモデル化する際に，それが内包する確率的不確かさを適切にモデルに組み込むことは重要である．特に近年では，突風による風力発電量の急激な変動など，システムに大きな影響を与えるレアイベントを考慮した不確かさのモデリング・解析手法がますます求められている．動的システムにおける確率的不確かさを表現するのに最も用いられるのは，ガウス型の雑音であり，解析的な扱いやすさという大きな利点をもつ一方で，裾が急速に減衰するガウス分布では外れ値を表現することができない．そこで本稿ではレアイベントモデリングが可能，かつ，動的システムでの解析的扱いやすさを併せもつ，安定分布を利用したモデリング手法を解説する．また本枠組みの応用例として，等価線形化による非線形システム解析，動的システムにおけるプライバシー保護を紹介する．

キーワード　確率システム，レアイベント，安定分布，プライバシー

Abstract　When we model dynamic phenomena, it is important to properly incorporate their probabilistic uncertainty. In particular, there is an increasing need for modeling and analysis methods for rare events that cause severe impact, e.g., extreme wind power fluctuations due to gusts. For the modeling of the stochasticity in dynamical systems, Gaussian noise is often used because of its analytical tractability. However, it cannot represent outliers because of its rapidly decaying tails. In this context, this article introduces a modeling and analysis method using stable distributions. This framework is capable of modeling rare events while retaining the favorable properties equipped with the Gaussian. As applications, we also describe our results on stochastic linearization analysis and privacy protection in dynamical systems.

Key words　Stochastic System, Rare Event, Stable Distribution, Privacy

1. はじめに

多くの工学応用において，動的システムが内包する確率的不確かさの影響を見積もることは重要な課題となっている．例えば，風力発電が連系された電力系統を考えてみよう．再生可能エネルギーの重要性がますます高まる中で，風力発電の導入量をいかに増やすかが課題となっている．導入量増加に向けた大きな問題の一つが風力発電の不確かさである．風力は天候の影響を強く受けるため，発電量は不確かな振る舞いを見せる．更に突風や乱流の影響により，べき乗則に従うような極端に大きな発電量変動が生じることがある[(1)]．このような大変動が生じるのは稀 (レアイベント，外れ値) ではあるが，電力系統の周波数変動の原因となり，最悪の場合，大規模停電につながる恐れがある．よって，甚大な影響を与えうるレアイベントを適切に組み込んだモデルに基づいた解析が求められる．

伊藤海斗　京都大学大学院情報学研究科
E-mail ito.kaito@bode.amp.i.kyoto-u.ac.jp
加嶋健司　正員　京都大学大学院情報学研究科
E-mail kk@i.kyoto-u.ac.jp
Kaito ITO, Nonmember (Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan), Kenji KASHIMA, Member (Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.14 No.4 pp.269–278 2021 年 4 月
©電子情報通信学会 2021

このような問題に対して近年，著者らは安定分布を利用した動的システムのレアイベントモデリングに取り組んできた[(1)~(3)]．安定分布はガウス分布の自然な拡張であり，極端に大きな外れ値が無視できない割合で発生する確率分布族である．この安定分布を用いたモデリングは外れ値が考慮できるだけでなく，ガウス分布によるモデリングと同様の扱いやすい数学的性質を併せもつ．本稿の目的はこのモデリング手法を紹介し，どのような扱いが可能であるかを解説することである．

更に後半では安定分布を用いたモデリングの応用例を二つ紹介する．

（1）　入力飽和や摩擦といった静的非線形性が含まれるフィードバック系の近似解析手法として (確率) 等価線形化[(4)]とそれに対する精度保証について紹介する．

（2）　動的システムにおける信号が個人情報を含むとき，それが漏洩しないようなデータ加工が必要になる．保護対象のデータが急激な変動など，レアイベント的な振る舞いをもつ場合に，安定分布雑音を印加することでそのデータを守ることができる[(5)]．

本稿の構成は以下のとおりである．まず **2.** では，本稿で最も重要な道具である安定分布を導入し，その基本的な性質を説明する．つぎに **3.** では，線形システムに焦点を当て，安定分布を用いたレアイベントのモデリングを解説し，更にその諸性質を通して本モデリング手法の利点を明らかにする．この利点を踏

まえて，**4.** では静的非線形性を含んだ，安定分布雑音で駆動されるフィードバック系の近似評価手法として等価線形化を説明する．**5.** では，離散時間線形システムにおいて信号値を個人情報として保護したいときに，安定分布雑音がどのように活用できるかを紹介する．**6.** では，安定分布雑音で駆動されるシステムのシミュレーション法を紹介する．

記法　実数の集合，非負整数の集合をそれぞれ $\mathbb{R}$, $\mathbb{Z}_+$ で記す．虚数単位を j と記す．行列 A が正定値対称行列であることを $A \succ 0$ と書く．$\mathrm{diag}(k_1, \ldots, k_r)$ で対角成分 $(k_1, \ldots, k_r)$ をもつ対角行列を表す．$(\Omega, \mathcal{F}, \mathbb{P})$ を自然なフィルトレーション $\{\mathcal{F}_t\}_{t \geqq 0}$ をもつ完備確率空間とする(注1)．期待値を $\mathbb{E}$ で表し，対応する確率分布が明らかでない場合は添字で示す．確率過程 $\{x_t\}$ に対して，確率変数 x_∞ への法則収束[6] を $x_t \xrightarrow{d} x_\infty$ と表記し，x_∞ の確率分布を x_t の定常分布と呼ぶ．(行列) 指数関数を e^A あるいは $\exp(A)$ と記す．正の実定数 s, x に対して，ガンマ関数 $\Gamma(s)$，スケーリングした下側不完全ガンマ関数 $\Gamma_\ell(s, x)$ を

$$\Gamma(s) := \int_0^\infty t^{s-1}\mathrm{e}^{-t}\mathrm{d}t,\ \Gamma_\ell(s,x) := \frac{1}{\Gamma(s)}\int_0^x t^{s-1}\mathrm{e}^{-t}\mathrm{d}t$$

で定義する．本稿を通して，離散時間は k，連続時間は t を添字として時刻を表す．

2. 準備：安定分布とその性質

2.1 安定分布とべき乗則

通常時とは大きく外れた値をとるレアイベントは，確率分布での外れ値標本に対応する．よってレアイベントを確率分布でモデリングするためには，稀であるが無視できない確率で外れ値が発生する分布を用いる．つまり分布の裾が重い (厚い) ものがこれに適する．そこで本節では，裾の重い分布である安定分布を導入し，その諸性質をまとめる．安定分布は特に線形動的システムでの解析に適した顕著な性質をもつ．まずは天下り的に定義を与えよう[7]．

[定義 1]（単変量安定分布）　実数値確率変数 X がパラメータ $\alpha \in (0, 2]$, $\sigma > 0$, $\beta \in [-1, 1]$ について，

$$\mathbb{E}[\exp(\mathrm{j}\nu X)] = \begin{cases} \exp\left\{-\sigma^\alpha|\nu|^\alpha\left(1 - \mathrm{j}\beta\mathrm{sgn}(\nu)\tan\left(\frac{\pi\alpha}{2}\right)\right)\right\} & \text{if } \alpha \neq 1, \\ \exp\left\{-\sigma|\nu|\left(1 + \mathrm{j}\beta\frac{2}{\pi}\mathrm{sgn}(\nu)\log|\nu|\right)\right\} & \text{if } \alpha = 1, \end{cases}$$

$$\mathrm{sgn}(\nu) := \begin{cases} 1 & \text{if } \nu > 0, \\ 0 & \text{if } \nu = 0, \\ -1 & \text{if } \nu < 0, \end{cases}$$

を満たすとき，X は (単変量) **安定分布**に従うといい，$X \sim \boldsymbol{S}(\alpha, \sigma, \beta)$ で表す．特に $\beta = 0$ のとき，対称安定分布に従うといい，$X \sim \boldsymbol{S\alpha S}(\alpha, \sigma)$ と書く．◁

安定分布は特別なパラメータを除いて，確率密度関数を陽に書き下すことができないゆえに，特性関数 $\mathbb{E}[\exp(\mathrm{j}\nu X)]$ を経由した定義になっている．パラメータ α は分布の裾の重さ，すなわち確率密度関数の減衰の遅さを示す．特に，$\boldsymbol{S\alpha S}(2, \sigma)$ は分散が $2\sigma^2$ のガウス分布と一致する．σ はスケールパラメータであり，ガウス分布の標準偏差のような役割をもつ．以下では，$\sigma = 1$ のときは $X \sim \boldsymbol{S\alpha S}(\alpha)$ と省略して記し，定義より

$$\kappa X \sim \boldsymbol{S\alpha S}(\alpha, |\kappa|),\ \kappa \in \mathbb{R} \tag{1}$$

が成り立つ．β は歪度パラメータであり，$\beta = 0$ (対称安定分布) からのズレに従って密度関数の形状がひずんでいく．特に $\alpha < 1$ かつ $\beta = 1$ のとき，$X \sim \boldsymbol{S}(\alpha, \sigma, 1)$ は非負の値しかとらない．本稿で用いるのは $\beta = 0, 1$ の場合のみである．$X_\infty \sim \boldsymbol{S\alpha S}(\alpha, \sigma)$ を満たす X_∞ に対して，$X_t \xrightarrow{d} X_\infty$ が成り立つことを $X_t \xrightarrow{d} \boldsymbol{S\alpha S}(\alpha, \sigma)$ と表記する．安定分布の裾の性質はつぎのように特徴づけられる[7, Property 1.2.15]．

[命題 1]（べき乗則）　$X \sim \boldsymbol{S\alpha S}(\alpha)$, $\alpha \in (0, 2)$ について，

$$\lim_{\lambda\to\infty} \lambda^\alpha \mathbb{P}(X > \lambda) = \begin{cases} \frac{1-\alpha}{2\Gamma(2-\alpha)\cos\left(\frac{\pi\alpha}{2}\right)} & (\alpha \neq 1) \\ \frac{1}{\pi} & (\alpha = 1) \end{cases} \tag{2}$$

が成り立つ．◁

この命題は安定分布の**べき乗則** (スケールフリー性) を示す．つまり $\boldsymbol{S\alpha S}(\alpha)$ の確率密度関数 $p_\alpha(x)$ は x が十分大きいときに，両対数座標で傾き $-(\alpha + 1)$ の直線に近づく．このことから α が小さくなるにつれ，対応する分布はより重い裾をもつことが分かる．図 1 a に対称安定分布の確率密度関数(注2) を示す．$\alpha = 2$，つまりガウス分布は裾の部分で急激に減衰するが，$\alpha < 2$ のときは減衰が緩やかになる．この減衰の様子は両対数座標 (図 1 b) で見るとより顕著に表れる．このべき乗則により，$p \geqq \alpha$ に対する p 次モーメント $\mathbb{E}[|X|^p]$ は有限にならないという性質をもつ．α 次未満のモーメントは以下のように得られる[10, Example 25.10]．

[命題 2]　$X \sim \boldsymbol{S\alpha S}(\alpha, \sigma)$, $\alpha \in (0, 2)$ と $p \in (-1, \alpha)$ に対して，

$$\mathbb{E}[|X|^p] = \frac{(2\sigma)^p\Gamma\left(\frac{1+p}{2}\right)\Gamma\left(1 - \frac{p}{\alpha}\right)}{\sqrt{\pi}\Gamma\left(1 - \frac{p}{2}\right)} \tag{3}$$

が成り立つ．◁

ここまで，単変量の安定分布を紹介してきたが，**5.** では多変量安定分布を用いるので導入しておく[11]．

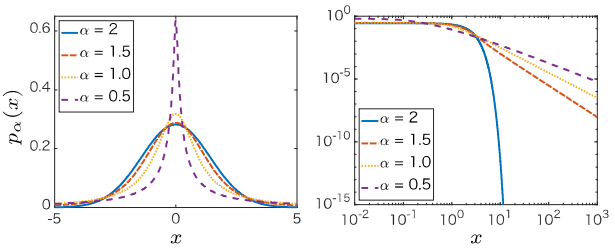
[定義 2]　$\mathbb{R}^d$-値確率ベクトル $X = [X_1 \cdots X_d]^\top$ がパラメータ $\alpha \in (0, 2]$ と $d \times d$ の行列 $\Sigma \succ 0$ について，

$$\mathbb{E}[\exp(\mathrm{j}\nu^\top X)] = \exp(-(\nu^\top\Sigma\nu)^{\alpha/2}),\ \nu \in \mathbb{R}^d \tag{4}$$

を満たすとき，X はだ円形安定分布に従うといい，$X \sim \boldsymbol{SG}_d(\alpha, \Sigma)$ で表す．◁

(注1)：この一文は確率過程を扱う際に最初に与える数学的なおまじないのようなもので，確率論に馴染みのない方は，$\mathbb{P}$ が事象を引数にとって，その事象が起こる確率を返す関数 (確率測度) ということだけ分かっていれば本稿では十分である．

(注2)：安定分布の確率密度関数の数値計算法については文献(8) を参照のこと．例えば MATLAB® [9] では安定分布のパラメータを指定すると密度関数の値が数値的に得られる関数 (`makedist`) が実装されている．



(a) (b)

図 1 (a) 安定分布 $\boldsymbol{S\alpha S}(\alpha)$ の確率密度関数 $p_\alpha(x)$ と (b) 両対数プロット

$\alpha = 2$ のとき，安定分布は平均 0，共分散行列 2Σ の多変量ガウス分布となる．ガウス分布の共分散行列と同様に Σ はだ円分布の形状を特徴づける．また，だ円形安定分布は線形変換について閉じている．すなわち，$X \sim \boldsymbol{SG}_d(\alpha, \Sigma)$ と行フルランクの行列 $N \in \mathbb{R}^{r\times d}$ に対して，$NX \sim \boldsymbol{SG}_r(\alpha, N\Sigma N^\top)$ が成り立つ．ガウス分布と異なる点として，$\alpha < 2$ のときは，裾の重さにより共分散行列が存在しないこと，そして Σ が対角行列でも，各成分は独立にならないことに注意されたい．

2.2 動的システム解析から見た安定分布の利点：再生性

さて，外れ値モデリングをかじったことのある方は，「裾の重い分布ならほかにも t 分布はべき乗則をもつし，何より t 分布は確率密度関数を陽に書き下せるから，安定分布より扱いやすそうではないか」と思うかもしれない．密度関数が陽に書けないという扱いづらさを差し引いても安定分布を用いる本質的理由が以下に示す**再生性**である[7, Property 1.2.1]．

［命題 3］（安定分布の再生性） $X_1 \sim \boldsymbol{S\alpha S}(\alpha, \sigma_1)$，$X_2 \sim \boldsymbol{S\alpha S}(\alpha, \sigma_2)$ が独立であるとする．このとき，任意の $a_1, a_2 \in \mathbb{R}$ について

$$a_1 X_1 + a_2 X_2 \sim \boldsymbol{S\alpha S}\left(\alpha, \{(|a_1|\sigma_1)^\alpha + (|a_2|\sigma_2)^\alpha\}^{1/\alpha}\right) \tag{5}$$

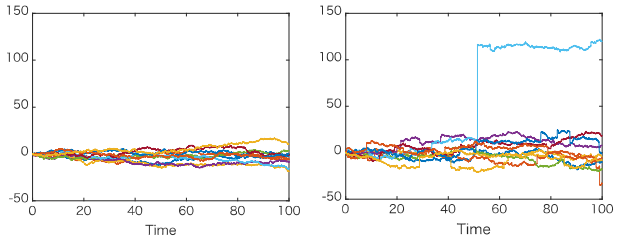
が成り立つ． ◁

再生性，すなわち独立な確率変数の和について分布が閉じている性質(注3)は，線形動的システムでの解析を格段に容易にしてくれる．例えば，以下のような雑音 w_k で駆動される離散時間のスカラー線形システムを考えてみよう．

$$x_{k+1} = ax_k + w_k,\ a \neq 0. \tag{6}$$

ここで $x_0 \sim \boldsymbol{S\alpha S}(\alpha, \sigma_0)$，$w_k \sim \boldsymbol{S\alpha S}(\alpha, \sigma_w)$ とし，$x_0, \{w_k\}_{k\geqq 0}$ は全て互いに独立であるとする．すると命題 3 から，$x_1 \sim \boldsymbol{S\alpha S}(\alpha, \{(|a|\sigma_0)^\alpha + \sigma_w^\alpha\}^{1/\alpha})$ であることが分かる．x_1 と w_1 も独立であるから，再び x_2 も安定分布に従い…

(注3)：再生性と密接なつながりがある性質として安定性がある．確率変数 X と独立同分布に従う確率変数 X_1，X_2 を考える．任意の $a_1, a_2 > 0$ に対して，$a_1X_1 + a_2X_2$ と $cX + d$ の分布が一致するような $c > 0$，$d \in \mathbb{R}$ が存在するとき，X は安定であるという．実はこの X が従う分布こそが安定分布である．



(a) ウィーナ過程 (b) 安定過程 ($\alpha = 1.7$)

図 2 ウィーナ過程と安定過程の標本経路

といった具合に任意の時刻 k において，状態 x_k は安定分布に従い，スケールパラメータのみで分布の発展を解析することができる．このような顕著な性質は，ほかの非ガウス分布では成り立たない．例えば，x_0, w_0 が t 分布に従って独立であっても，つぎの時刻で x_1 は t 分布に従わず，分布の振る舞いを解析的に追っていくことは非常に困難になってしまう．こういった点から，線形システムでのレアイベントモデリングをする際は，安定分布を用いることで解析的扱いやすさという大きな利点が生まれる．また，非線形性がシステムに含まれる場合にも，この恩恵が享受できることを後に **4.** で紹介する．

2.3 連続時間の安定分布雑音

つぎに，連続時間の動的システムに安定分布型の不確かさを導入するために，安定分布から誘導される連続時間確率過程を与える．

［定義 3］ 確率過程 $\{L_t\}_{t\geqq 0}$ がパラメータ α の (標準) **安定過程**であるとは，

$$L_t \sim \boldsymbol{S\alpha S}\left(\alpha, t^{1/\alpha}\right) \tag{7}$$

が成り立つことをいう． ◁

$\alpha = 2$ のとき，$L_t/\sqrt{2}$ は (標準) ウィーナ過程に一致する．安定過程はレビー過程であり，すなわち定常独立増分をもつ[12]．したがって，ウィーナ過程に対する伊藤積分と同様に，安定過程に関しても (増分が安定分布に従う) 確率微分方程式を導入することが可能である[7]．図 2 にウィーナ過程と安定過程の標本経路を示す．連続な経路をもつウィーナ過程に対して，$\alpha < 2$ の安定過程では増分が裾の重い安定分布に従っているため，急激な変化が生じ，経路が不連続となっていることが見て取れる．このような確率過程を用いることで動的システムにおける急激な変化をモデリングすることが可能になる．

3. 安定過程雑音下での線形システム解析

本節では安定過程で駆動される線形システムに焦点を当てて，その性質を紹介する．具体的には以下のような確率微分方程式

$$\mathrm{d}x_t = Ax_t\mathrm{d}t + b\mathrm{d}L_t,\ y_t = cx_t \tag{8}$$

によるモデリングを考えてみよう．ここで $x_t \in \mathbb{R}^n$，$y_t \in \mathbb{R}$ はそれぞれ状態，出力を表す．$A \in \mathbb{R}^{n\times n}$ は安定行列，すなわち

全ての固有値の実部が負であるとし，b, $c^\top \in \mathbb{R}^n$ で，L_t はパラメータ $\alpha \in (0,2]$ の安定過程とする．確率微分方程式に馴染みのない方であれば，代わりに (8) を

$$\dot{x}_t = Ax_t + b\dot{L}_t,\ y_t = cx_t$$

と見て，通常の微分方程式に安定分布型の白色雑音 $\dot{L}_t$ が加わっているという形式的な理解で本稿では十分である．$\alpha = 2$ のときはおなじみの白色ガウス雑音で駆動される線形システムとなる．さて，再生性を通して離散時間線形システムでの安定分布の扱いやすさは見た．これは連続時間でも同様に当てはまる[2, Theorem 2]．

［定理 1］ 線形システム (8) を考える．このとき

$$y_t \xrightarrow{d} \boldsymbol{S\alpha S}(\alpha, \|\mathrm{c}\mathrm{e}^{At}b\|_\alpha) \tag{9}$$

が成り立つ．ここで，$\int_0^\infty |f(t)|^\alpha \mathrm{d}t < \infty$ を満たす実数値関数 $f(t)$ の L^α-ノルムは

$$\|f\|_\alpha := \left(\int_0^\infty |f(t)|^\alpha \mathrm{d}t\right)^{1/\alpha} \tag{10}$$

で定義される． ◁

定常分布の裾の重さパラメータは駆動雑音 L_t と同じ α であり，スケールパラメータはインパルス応答の L^α-ノルムとなる．このように線形システムの出力の定常分布が解析的に書き下せることが，安定分布をモデリングに用いることの最大の利点である．例えば制御入力 u_t が印加されるシステム

$$\mathrm{d}x_t = Ax_t\mathrm{d}t + Bu_t\mathrm{d}t + b\mathrm{d}L_t,\ z_t = c_z x_t$$

において，評価出力 $z_t \in \mathbb{R}$ の定常分布が所望の条件を満たすように制御則を設計したいとする．このとき，$A + BK$ が安定行列になるようにフィードバック制御 $u_t = Kx_t$ を施せば，定理 1 より，$z_\infty \sim \boldsymbol{S\alpha S}(\alpha, \|c_z\mathrm{e}^{(A+BK)t}b\|_\alpha)$ であることが分かる．よってインパルス応答のノルムのみに着目すればよいから，設計の見通しが非常によくなる．このような解析的扱いやすさは，**4.** の結果を導く際にも存分に活躍する．

つぎに標本ごとにどのような振る舞いが見られるかを例を通して確認しよう．以下のスカラーシステムを考える．

$$\mathrm{d}x_t = -0.1x_t + 0.5\mathrm{d}L_t,\ x_0 = 10,\ \alpha = 1.8.$$

x_t の標本経路を示したのが図 3 である．上式右辺 x_t の係数が負であるから，標本全体の傾向としては原点に近づいて揺らいでいるが，稀に大きな雑音が印加されることで不連続で急激な変動が生じていることが分かる．よって，安定分布を用いたモデリングは，べき乗則に従うような極端な外れ値・急激な変動をモデリングするのに適した枠組みであることが確認できた．

さて本節では最後に，時系列データからどのようにモデルパラメータを定めるかを説明する．ここでも安定分布の扱いやすさが発揮される．例えば風力発電量の変動を (8) の出力としてモデリングしようと考えたとき，発電量の時系列データからどのように伝達関数

$$G(s) := c(sI - A)^{-1}b \tag{11}$$

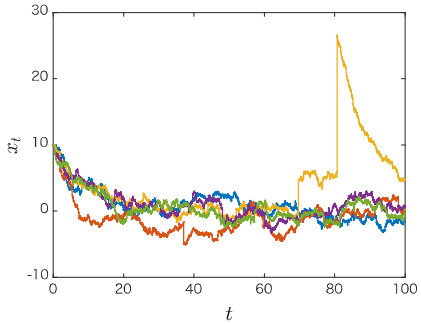


図 3 安定過程で駆動される線形システムの標本経路

と駆動雑音のパラメータ α を決定するかを考えよう．ここでは y_t の十分多くの長時間標本経路が利用可能であるとする．まず α については，定理 1 より y_t の定常分布の確率密度関数は両対数座標で傾き $-(\alpha+1)$ で減衰することから，y_t のヒストグラムをデータから作成し，両対数座標におけるその傾きから α を計算しそれを駆動雑音 L_t のパラメータとするのが妥当である．伝達関数について，$\alpha = 2$ の場合に最も簡単な $G(s)$ の選び方は $|G(\mathrm{j}\omega)|^2$ と出力のパワースペクトル密度が近くなるように決めることである．つぎの定理はこのようなゲイン線図近似の手法が $\alpha \in (0,2)$ の場合も可能であることを示している[2, Theorem 1]．

［定理 2］ 線形システム (8) と任意の $\alpha \in (0,2)$, $p \in (-1,\alpha)$, $\omega > 0$ に対して

$$\lim_{T\to\infty} \mathbb{E}\left[\left|\frac{1}{T^{1/\alpha}}\int_0^T \mathrm{e}^{-\mathrm{j}\omega t}y_t\mathrm{d}t\right|^p\right] = \kappa_{(\alpha,p)}|\mathrm{G}(\mathrm{j}\omega)|^p \tag{12}$$

が成り立つ．ここで

$$\kappa_{(\alpha,p)} := \frac{(2\kappa_\alpha)^p\Gamma\left(1+\frac{p}{2}\right)\Gamma\left(1-\frac{p}{\alpha}\right)}{\Gamma\left(1-\frac{p}{2}\right)},$$

$$\kappa_\alpha := \left(\frac{1}{\pi}\int_0^\pi |\cos t|^\alpha \mathrm{d}t\right)^{1/\alpha}$$

である． ◁

式 (12) の左辺は $\alpha = p = 2$ のとき y_t のパワースペクトル密度となる．この定理より，事前に推定した α に対して，ゲイン $|G(\mathrm{j}\omega)|$ とデータから計算した式 (12) の左辺の近似値について関係式 (12) が満たされるように $G(s)$ を選べばよい．風力発電変動量のモデリングを行った具体例は拙著[1]を参照頂きたい．

4. 等価線形化による非線形システムの近似解析

ここまで線形システムに焦点を置いて，安定分布によるレアイベントモデリングを紹介してきた．しかし，実際のシステムは制御入力の飽和や摩擦など，無視できない非線形性が含まれることも多い．そこで本節では，静的な非線形性が含まれる場合にも，安定分布の扱いやすさを上手く利用した “等価線形化” によって，精度保証付きの近似解析が可能であることを説明する．

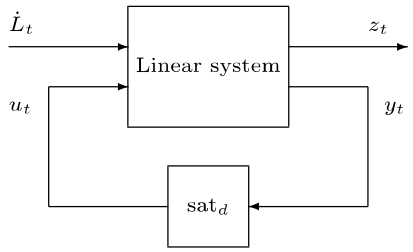


図 4　問題 1 のブロック線図

4.1　問題設定

既に説明したとおり，$\alpha \leqq 1$ の安定分布では絶対平均すら有限にならないため，以下では $\alpha \in (1,2]$ の場合のみを考える．本節で扱うのは図 4 で表される線形部と入力飽和の非線形部からなるフィードバック系：

$$\mathrm{d}x_t = Ax_t\mathrm{d}t + Bu_t\mathrm{d}t + b\mathrm{d}L_t, \tag{13}$$

$$z_t = c_z x_t, \tag{14}$$

$$y_t = C_y x_t, \tag{15}$$

$$u_t = \mathrm{sat}_d(y_t) \tag{16}$$

である．ここで $x_t \in \mathbb{R}^n$, $u_t \in \mathbb{R}^r$, $z_t \in \mathbb{R}$, $y_t \in \mathbb{R}^r$ はそれぞれ，状態，制御入力，評価出力，観測量を表す．b, $c_z^\top \in \mathbb{R}^n$ であり，A, B, C_y は適切なサイズの行列である．確率入力 L_t はパラメータ $\alpha \in (1,2]$ の安定過程であり，また与えられたしきい値ベクトル $d \in [0,\infty)^r$ に対して，

$$\mathrm{sat}_d(y) := \begin{bmatrix} \mathrm{sat}_{d_1}(y_1) \\ \vdots \\ \mathrm{sat}_{d_r}(y_r) \end{bmatrix}, \ \mathrm{sat}_{d_j}(y_j) := \begin{cases} -d_j, & y_j < -d_j, \\ y_j, & |y_j| \leqq d_j, \\ d_j, & y_j > d_j, \end{cases} \tag{17}$$

と定義する．ここで y_j, d_j はそれぞれ y, d の第 j 成分を表す．以上をもとに，つぎのような問題を考える．

［問題 1］　上で与えられる入力飽和を含むフィードバック系において，任意の $K \in \{\mathrm{diag}(k_1,\ldots,k_r) : k_j \in [0,1]\}$ に対して $A + BKC_y$ は安定行列とし，x_t は $t \to \infty$ のときに $\mathbb{R}^n$ 上で定義されたある確率変数 x_∞ に法則収束すると仮定する．また初期値 x_0 はある $p \in (1,\alpha)$ について有限な p 次モーメントをもつと仮定する．このとき z_t の定常分布を求めよ．　◁

［注意 1］　以下では飽和関数のみを議論で扱うが，図 5 で表されるような区分線形関数も同様の枠組みで扱うことが可能である．　◁

このような非線形性が含まれるシステムを解析的に調べることは一般に難しい．そこで多く用いられるのが，標本経路生成に基づいたモンテカルロ法による数値評価である．この手法は手軽ではあるものの，標本数と精度の関係が明らかではない，極端な外れ値の影響を捉えるにはしばしば莫大な標本数を必要とする，といった問題点がある[13]．特に，後者は外れ値の発生するシステムを扱う我々にとって無視できない問題である．この問題に対して提案されたのが等価線形化という近似解析手法である．以降，文献(2) で提案された，安定過程で駆動されるシステムの等価線形化について説明する．

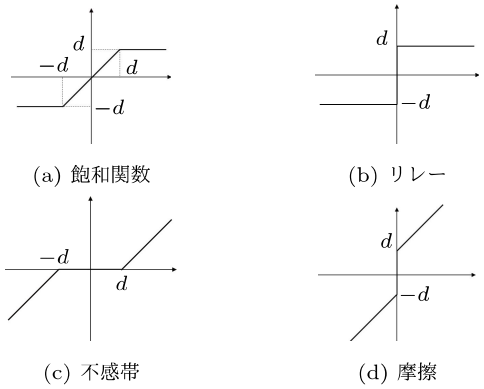


図 5　静的非線形性

4.2　等価線形化

(16) の非線形性をある線形ゲインで近似することを考えよう．具体的には，sat_d を $K \in \{\mathrm{diag}(k_1,\ldots,k_r) : k_j \in [0,1]\}$ で置き換えて得られる線形化システム

$$\mathrm{d}\tilde{x}_t = (A + BKC_y)\tilde{x}_t\mathrm{d}t + b\mathrm{d}L_t \tag{18}$$

を考える．定理 1 より

$$c_z\tilde{x}_t \xrightarrow{d} \boldsymbol{S\alpha S}(\alpha, \|c_z \mathrm{e}^{(A+BKC_y)t}b\|_\alpha) \tag{19}$$

が成り立つ．ここでうまく線形化ゲイン K を選べば式 (19) で与えられる分布が本来知りたい z_t の定常分布のよい近似になることが期待される．この K の選び方を与えるのが等価線形化である．その決定法を説明するために，まずつぎの定理を与える[2, Theorem 3]．

［定理 3］　与えられた $d > 0$, $\sigma > 0$, $\alpha \in (1,2)$ に対して，

$$\mathbb{E}_{Y \sim \boldsymbol{S\alpha S}(\alpha,\sigma)}[|\mathrm{sat}_d(Y) - kY|] \tag{20}$$

を最小にするゲイン $k > 0$ は

$$k_{\mathrm{sat}} := \min\left\{1, \frac{d}{\gamma_\alpha \sigma}\right\} \tag{21}$$

で与えられる．ここで γ_α は

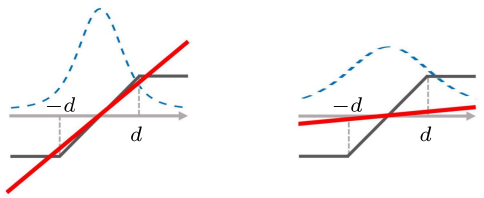
$$\int_0^{\frac{\pi}{2}} \mathcal{F}_\alpha(u)\Gamma_\ell\left(2 - \frac{1}{\alpha}, \left(\frac{\gamma}{\mathcal{F}_\alpha(u)}\right)^{\frac{\alpha}{\alpha-1}}\right) du = \frac{1}{2}\frac{\alpha}{\alpha-1} \tag{22}$$

を満たす唯一の正定数であり，$\mathcal{F}_\alpha(u)$ は

$$\mathcal{F}_\alpha(u) := \frac{\sin(\alpha u)}{(\cos u)^{\frac{1}{\alpha}}}\{\cos((1-\alpha)u)\}^{\frac{1-\alpha}{\alpha}} \tag{23}$$

で定義される．　◁

図 6 に定理 3 の解釈図を示す．飽和の幅 d に対して分布のスケール σ が小さいとき (図 6 a)，ほとんどの標本が飽和に引っ



(a) $\sigma \ll d$ のとき　　(b) $\sigma \gg d$ のとき

図 6　雑音スケール σ，飽和幅 d と最適近似ゲイン k_{sat} (赤線) の関係

かからないため，飽和関数は線形部分に近いゲインで近似される．d に対して σ が大きい場合 (図 6 b) は，飽和に引っかかる標本の割合が大きくなり，定数関数 0 に近い近似ゲインが選ばれる．また α が小さくなる，つまり裾が重くなると γ_α は大きくなり，近似ゲインは 0 に近づく．

さて，y_j の定常分布を $\boldsymbol{S\alpha S}(\alpha, \sigma_{yj})$ で近似したとしよう．すると定理 3 より，$\mathrm{sat}_{d_j}(y_j)$ は線形ゲイン

$$k_j = \min\left\{1, \frac{d_j}{\gamma_\alpha \sigma_{yj}}\right\} \tag{24}$$

で近似することが妥当である．逆に，$j = 1, \ldots, r$ のそれぞれに対して $\mathrm{sat}_{d_j}(y_j)$ を線形ゲイン k_j で近似すると，定理 1 より y_j の定常分布は

$$\boldsymbol{S\alpha S}(\alpha, \|C_{yj}\mathrm{e}^{(A+BKC_y)t}b\|_\alpha),\ K := \mathrm{diag}(k_1, \ldots, k_r) \tag{25}$$

で与えられる．以上の議論から，式 (24) と (25) が同時に満たされる線形化ゲインがよい近似ゲインであるという考えのもとで提案されたのが，以下の線形化手法である．

等価線形化

連立方程式

$$k_j = \min\left\{1, \frac{d_j}{\gamma_\alpha \|C_{yj}\mathrm{e}^{(A+BKC_y)t}b\|_\alpha}\right\},\ j = 1, \ldots, r \tag{26}$$

を $K = \mathrm{diag}(k_1, \ldots, k_r)$ について解き，求めた K に対して

$$\boldsymbol{S\alpha S}(\alpha, \|c_z\mathrm{e}^{(A+BKC_y)t}b\|_\alpha)$$

を z_t の近似定常分布とみなす．

連立方程式 (26) は数値的に解く．このアルゴリズムにおいては標本経路の生成が一切必要なく，モンテカルロ法に比べて高速に評価することが可能である．更に，線形化によって得られる近似絶対平均値 $\mathbb{E}[|c_z\tilde{x}_\infty|]$ に対して，

$$\mathbb{E}[|c_z\tilde{x}_\infty|] - \mathcal{E} \leqq \mathbb{E}[|c_z x_\infty|] \leqq \mathbb{E}[|c_z\tilde{x}_\infty|] + \mathcal{E} \tag{27}$$

の形で近似誤差 $\mathcal{E} \geqq 0$ を理論的に評価することができる．詳しくは拙著[3]を参照頂きたい．

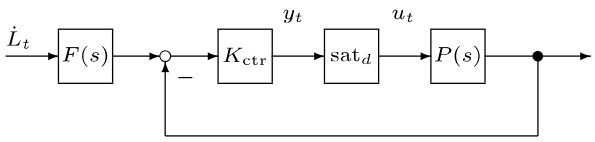


図 7　数値例のフィードバック系

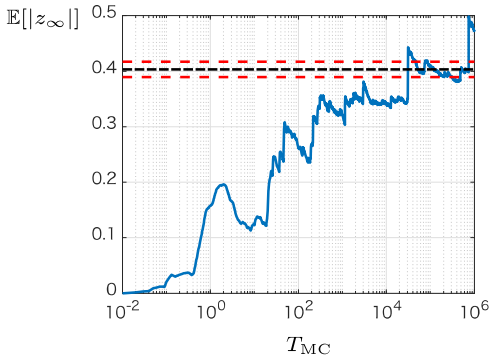


図 8　等価線形化による近似値 (黒，一点鎖線) と誤差上下界 (赤，鎖線)，長時間平均による近似値 (青線)

4.3　数　値　例

図 7 と以下のパラメータ・伝達関数で与えられるフィードバック系を考える．

$$F(s) = \frac{1}{s+1},\ K_{\mathrm{ctr}} = \begin{bmatrix} 0.2 & 0.5 \end{bmatrix}^\top,\ P(s) = \begin{bmatrix} \frac{1}{s+8} & \frac{1}{s+5} \end{bmatrix},$$

$d_1 = 0.7,\ d_2 = 0.1,\ \alpha = 1.3.$

評価出力 z_t は y_t の第一成分とする．ここで等価線形化を行うと近似ゲイン

$$K^* = \mathrm{diag}\,(0.625, 0.0356)$$

を得る．この線形化に基づくと，z_t の定常分布について近似評価は

$$\mathbb{E}[|z_\infty|] \simeq 0.403$$

で与えられる．更に文献 (3) の Theorem 1 により誤差評価

$$0.403 - 0.0137 \leqq \mathbb{E}[|z_\infty|] \leqq 0.403 + 0.0137$$

が得られる．つぎに本近似手法とモンテカルロ法を比較する．モンテカルロ法については，**6.** で紹介するオイラー・丸山法 (時間幅 $\mathrm{d}t = 0.01$) によって標本経路を生成し，長時間平均 $\int_0^{T_{\mathrm{MC}}} |z_t|\mathrm{d}t/T_{\mathrm{MC}}$ を計算する．図 8 に T_{MC} を変化させたときの長時間平均の振る舞いと等価線形化による近似評価値の比較を示す．非常に大きな T_{MC} に対して，モンテカルロ法は等価線形化の近似値に近づいてはいるものの，収束していないことが分かる．$T_{\mathrm{MC}} = 10^6$ で長時間平均を計算する時間は 20 分であったのに対し，等価線形化の計算時間は約 1 秒であった．ただし，用いた計算機の環境は Intel Core i5 を搭載した MacBook Pro である．このように，等価線形化はモンテカルロ法に比べて，高速に精度良く近似評価を行うことができる．

5. 安定分布雑音を活用したプライバシー保護

雑音は多くの場面で厄介者として捉えられるが，近年はプライバシー保護という文脈で，むしろ積極的に雑音を活用したデータ保護手法が注目されている[14]．本節では，安定分布雑音を活用した動的システムにおけるプライバシー保護について紹介する．本節でのみ用いる記法をここでまとめておく．

記法　ベクトル $x_1, \ldots, x_m \in \mathbb{R}^n$ を縦に並べたベクトル $[x_1^\top \ \cdots \ x_m^\top]^\top \in \mathbb{R}^{nm}$ を $[x_1; \cdots; x_m]$ で表す．信号 $u_k \in \mathbb{R}^m, k \in \mathbb{Z}_+$ に対して，時系列順に時刻 $T \in \mathbb{Z}_+$ まで並べたベクトルを，大文字のアルファベットを用いて，$U_T := [u_0; \cdots; u_T] \in \mathbb{R}^{(T+1)m}$ と表す．対称行列 $A \in \mathbb{R}^{n \times n}$ の最大・最小固有値をそれぞれ $\lambda_{\max}(A)$, $\lambda_{\min}(A)$ で表す．ベクトル $x = [x_1 \ \cdots \ x_n]^\top \in \mathbb{R}^n$ の p-ノルム $(p \geqq 1)$ を $\|x\|_p := (\sum_{i=1}^n |x_i|^p)^{1/p}$ と書く．また，行列 $A \succ 0$ で重み付けしたノルムを $\|x\|_A := (x^\top A x)^{1/2}$ で定義する．$\mathcal{Q}$ 関数を以下で定める．

$$\mathcal{Q}(x) := \frac{1}{\sqrt{2\pi}} \int_x^\infty \mathrm{e}^{-\frac{u^2}{2}} \mathrm{d}u, \ x \in \mathbb{R}.$$

5.1 線形システムにおけるプライバシー保護

まず，以下の確率性のない離散時間線形システム

$$\mathcal{S} : \begin{cases} x_{k+1} = Ax_k + Bu_k, \\ y_k = Cx_k + Du_k \end{cases}, \ k \in \mathbb{Z}_+ \tag{28}$$

を考える．ここで，$x_k \in \mathbb{R}^n$, $u_k \in \mathbb{R}^m$, $y_k \in \mathbb{R}^q$ はそれぞれ，状態，制御入力，出力を表し，A, B, C, D は適切な次元の行列である．表記の簡単のため，初期値 $x_0 = 0$ とするが，以降の議論は $x_0 \neq 0$ でも同様に成り立つ．(28) を用いると，終端時刻 T までの出力系列 $Y_T \in \mathbb{R}^{(T+1)q}$ は入力系列 $U_T \in \mathbb{R}^{(T+1)m}$ を用いて

$$Y_T = N_T U_T \tag{29}$$

と書き下すことができる．ただし $N_T \in \mathbb{R}^{(T+1)q \times (T+1)m}$ は

$$N_T := \begin{bmatrix} D & 0 & \cdots & \cdots & 0 \\ CB & D & \ddots & & \vdots \\ CAB & CB & D & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ CA^{T-1}B & CA^{T-2}B & \cdots & CB & D \end{bmatrix} \tag{30}$$

で定義される．

ここで出力 Y_T を公開データとして外部の制御器に提供することで，何らかの意味でよりよい制御が実現できるとしよう．ただし，出力の元となった入力データ U_T は個人情報を含んだデータとして漏洩したくないものとする．なお，初期状態 x_0 を保護したい場合も，以降の議論は同様に成り立つ．システム (28) が確定的であるがゆえに，入力 U_T が定まると Y_T が一意に決まってしまう．よって Y_T の値から U_T の値が特定される恐れがある．以上より，Y_T をそのまま公開することは危険であるから，図 9 のように各時刻で確率雑音 w_k を加えた出力 $y_{w,k} := y_k + w_k$ を代わりに公開することを考えよう．この新たな出力の系列 $Y_{w,T} = [y_{w,0}; \cdots; y_{w,T}]$ は

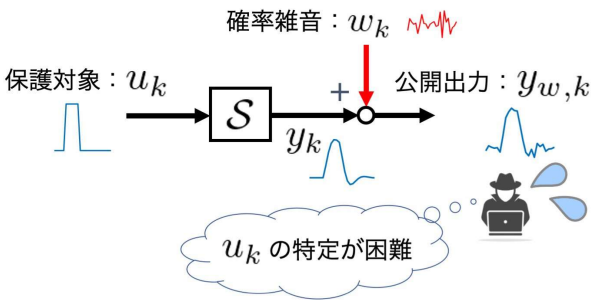


図 9　出力雑音付加による入力 u_k のプライバシー保護

$$Y_{w,T} = N_T U_T + W_T \tag{31}$$

と書ける．このデータ加工により，$Y_{w,T}$ から U_T を推定することが統計的に困難になる．ここで問題になるのは

Q1　雑音はどれぐらいの大きさ (スケール) にすれば十分か，

Q2　雑音 W_T の分布はどういったものがよいか，

である．前者について，雑音が大きいほど U_T の推定は困難になる一方で，大きすぎると元の信号 Y_T の情報が失われ，$Y_{w,T}$ は意味のない信号になってしまう．よって，プライバシーと情報有益性のトレードオフを考慮して雑音スケールを決めなければならない．後者の雑音分布について，静的データの保護ではラプラス雑音が標準的に用いられる[14]．その一方で，線形動的システムに対しては解析のしやすさから，文献(15) でガウス雑音を用いた保護手法の解析が行われている．しかし，保護対象 U_T に急激な変化が含まれる場合，外れ値がほとんど生じないガウス雑音ではその変化を隠蔽することができないという問題がある．

以下では，安定分布雑音を用いることでこの問題が解決することを，図 10 で示すイメージ図を用いて説明する (具体的な数値例については拙著[16]を参照)．まず，図中左の u_k に生じている突発的な変動を隠蔽したいとする．これが入力としてシステムに印加されて得られる出力が中央図の黒線である．そして赤線，青線はそれぞれ出力にガウス雑音，安定分布雑音を加えたものである．さて，この入力系列 U_T を推定しようとする攻撃者にシステムパラメータ，雑音分布，入力の事前分布 $\varphi(U_T)$ が漏洩しているという最悪ケースを考える．ここで，重要な情報をもつ外れ値が時折，入力に含まれる状況を表現するために，裾の重い事前分布とする．このとき，事前分布 $\varphi(U_T)$ とゆう度 $p(Y_{w,T}|U_T)$ から定まる事後分布

$$p^*(U_T|Y_{w,T}) \propto \varphi(U_T) p(Y_{w,T}|U_T)$$

で確率の高い部分を色付けると図 10 の右のように与えられる．

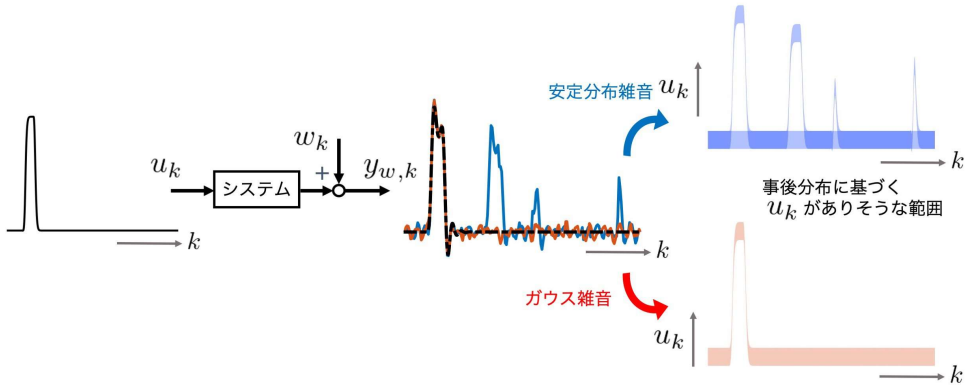


図 10　安定分布雑音が急激な変動を保護するイメージ図　u_k (左図) に対する出力 (中央図，黒鎖線) と雑音が加えられた出力 $y_{w,k}$ (中央図，青線：安定分布雑音，赤線：ガウス雑音)．公開出力 $y_{w,k}$ に条件付けられた事後分布 $p(U_T|Y_{w,T})$ に基づき，u_k がある確率が高い範囲を色付けしたのが右図．ガウス雑音では入力が変動していることが分かってしまう．一方，安定分布では中央図のように稀に大きな雑音が印加されうるので，入力に変動があったのか，出力からは確信できない．

ガウス雑音 (赤帯) では真値 u_k の周辺に標本が分布しており，ばらつきはあるものの u_k が急激に変化していることが攻撃者に漏洩してしまう．ガウス雑音を用いる限り，分散を大きくしてもこの状況は改善しない．一方，安定分布雑音を用いた場合 (青帯) では，公開出力が大きく変動している箇所の事後分布が二峰性を示している．すなわち，攻撃者は出力データの急激な変動が入力によるものなのか，それとも雑音が引き起こしたものなのかの区別が，統計的に困難であることを表している．実際，入力に外れ値が発生していない箇所においても，中央図のように大きな雑音が稀に印加されることで，事後分布が二峰に分かれている．以上をまとめると，ガウス雑音では本質的に，データの急激な変動を隠蔽することができないが，裾の重い安定分布雑音を用いることでこれを解決することができる．

5.2　差分プライバシー

図 10 を通して，安定分布雑音による急激な変動データの隠蔽効果を確認したが，つぎは違った切り口でプライバシーを考えることで，「雑音スケールの大きさをどうすればよいか」という問題に取り組もう．ある出力 $Y_{w,T}$ が得られたとき，その元となったデータが U_T であったのか，それとも U_T と似たデータ U'_T であったのかの区別が難しい状況であればプライバシー水準が高いといえそうである．この考え方を具体的にプライバシーの数学的定義に落とし込んだのが，**差分プライバシー**である[14]．差分プライバシーはもともと，静的なデータベースの保護という文脈で提案されたものであるが，近年では動的システムに対する差分プライバシーが研究されている[15],[17],[18]．以下，その定義を説明する．

確率変数 X の分布を $\mathbb{P}_X$ とし，$\mathbb{R}^{(T+1)q}$ 上の分布全体を $\mathcal{P}(\mathbb{R}^{(T+1)q})$ で表すものとする．すると (31) により，写像 $\mathcal{M} : \mathbb{R}^{(T+1)m} \times \mathcal{P}(\mathbb{R}^{(T+1)q}) \ni (U_T, \mathbb{P}_{W_T}) \mapsto \mathbb{P}_{Y_{w,T}} \in \mathcal{P}(\mathbb{R}^{(T+1)q})$ が定義される．差分プライバシー解析では，この写像をメカニズムと呼ぶ[14]．

まずデータが “似ている” ことを，以下で定義される隣接関係を満たしていることと定義する．

[定義 4]（隣接関係）　与えられた $c > 0$, $p \geqq 1$ に対して，入力データ組 $(U_T, U'_T) \in \mathbb{R}^{(T+1)m} \times \mathbb{R}^{(T+1)m}$ が p-ノルムについて，c-隣接関係にあるとは，$\|U_T - U'_T\|_p \leqq c$ が成り立つことをいい，c-隣接関係にある組全体を Adj_p^c で表す．　◁

この隣接関係を用いて，差分プライバシーは以下のように定義される．

[定義 5]（差分プライバシー）　$\mathcal{B}(\mathbb{R}^{(T+1)q})$ を $\mathbb{R}^{(T+1)q}$ 上のボレル集合族(注4)とする．与えられた $\varepsilon > 0$, $\delta \geqq 0$ に対し，メカニズム (31) が，Adj_p^c と有限時刻 $T \in \mathbb{Z}_+$ について，(ε, δ)-差分プライバシーを満たすとは，任意の $(U_T, U'_T) \in \mathrm{Adj}_p^c$ に対して，

$$\begin{aligned}&\mathbb{P}(N_T U_T + W_T \in S)\\ &\leqq \mathrm{e}^{\varepsilon}\mathbb{P}(N_T U'_T + W_T \in S) + \delta,\ \forall S \in \mathcal{B}(\mathbb{R}^{(T+1)q}) \quad (32)\end{aligned}$$

が成り立つことをいう．　◁

この定義の意味を説明するために，まず $\delta = 0$ として，(32) を以下のように式変形する．

$$\frac{\mathbb{P}(Y_{w,T} = N_T U_T + W_T \in S)}{\mathbb{P}(Y'_{w,T} = N_T U'_T + W_T \in S)} \leqq \mathrm{e}^{\varepsilon}.$$

隣接性の定義から上式は左辺の分母分子を入れ替えても成り立つ必要がある．このことから，

$$\mathrm{e}^{-\varepsilon}\mathbb{P}(Y'_{w,T} \in S) \leqq \mathbb{P}(Y_{w,T} \in S) \leqq \mathrm{e}^{\varepsilon}\mathbb{P}(Y'_{w,T} \in S).$$

すなわち，ε が小さくなると任意の集合 $S \in \mathcal{B}(\mathbb{R}^{(T+1)q})$ に対して，$\mathbb{P}(Y_{w,T} \in S)$ と $\mathbb{P}(Y'_{w,T} \in S)$ の値が近くなるような条件式になっている．これは $Y_{w,T}$, $Y'_{w,T}$ の分布が似ていることを意味し，出力の実現値から U_T, U'_T の区別が統計的に困難となる．また，δ はこの条件に対する緩和パラメータと捉えることができる．以上をまとめると，ε, δ ともに 0 に近いほど差分プ

(注4)：確率が定義できない病的な集合は除外した “$\mathbb{R}^{(T+1)q}$ 上の集合の集合” ぐらいの理解でよい．

ライバシーの意味でプライバシー水準が高いといえる．

以降では差分プライバシーを達成するために，安定分布雑音をどのように設計すればよいかを考える．

［問題 2］ 与えられた線形システム (28) と $\varepsilon, \delta > 0$ に対し，(32) を満たすような安定分布雑音 W_T を設計せよ． ◁

5.3 出力雑音・入力雑音による差分プライバシー解析

差分プライバシー解析の結果を述べるため，A_α で

$$A_\alpha \sim \boldsymbol{S}\left(\frac{\alpha}{2}, 2\left(\cos\frac{\pi\alpha}{4}\right)^{2/\alpha}, 1\right),\ \alpha \in (0,2) \tag{33}$$

を満たす確率変数を表すことにする．任意に定められた差分プライバシー水準に対して，それを達成する安定分布雑音が存在することが，以下に述べる定理から明らかになる[5],[16]．

［定理 4］（出力雑音による差分プライバシー条件）
$\alpha \in (0,2)$, $\varepsilon > 0$, $\delta \in (0,1)$ とする．$c > 0$ と $T \in \mathbb{Z}_+$，(33) で定まる A_α に対して，行列 $\Sigma \succ 0$ を

$$\lambda_{\max}^{1/2}(\mathcal{O}_{\Sigma,T}) \leqq \frac{1}{c}\mathcal{Q}_{\alpha,\varepsilon}^{-1}(\delta), \tag{34}$$

$$\mathcal{O}_{\Sigma,T} := N_T^\top \Sigma^{-1} N_T, \tag{35}$$

$$\mathcal{Q}_{\alpha,\varepsilon}(z) := \mathbb{E}\left[\mathcal{Q}\left(\frac{\varepsilon A_\alpha^{1/2}}{z} - \frac{z}{2A_\alpha^{1/2}}\right)\right],\ z > 0, \tag{36}$$

が成り立つように選ぶ．このとき，$W_t \sim \boldsymbol{SG}_{(T+1)q}(\alpha, \Sigma)$ により生成されるメカニズム (31) は Adj_2^c と有限時刻 T について，(ε, δ)-差分プライバシーを満たす． ◁

雑音のスケール Σ は (34) の左辺に現れる．大雑把にいえば，Σ が大きくなれば $\lambda_{\max}^{1/2}(\mathcal{O}_{\Sigma,T})$ は小さくなり，条件式 (34) は満たされやすくなる．これは雑音スケールが大きいほどプライバシー水準が高くなるという直感に合った結果であろう．また，ε, δ が小さくなると逆関数 $\mathcal{Q}_{\alpha,\varepsilon}^{-1}(\delta)$ は小さくなる．よって要求される差分プライバシー水準が高いほど，不等式条件 (34) が強い条件になる．なお $\mathcal{Q}_{\alpha,\varepsilon}^{-1}(\delta)$ は数値積分で計算できる．

以上より，「雑音をどれぐらい大きくすればよいか」という問いに差分プライバシーの側面から答えるならば，「所望のプライバシー水準 (ε, δ) に対して (34) を満たす最小限の雑音を用いればよい」ということになろう．

［補足 1］ Σ が単位行列のときは，(35) は現代制御論において入力可観測性グラミアンと呼ばれている行列である．この行列が特異に近いほど，出力から入力を推定することが困難になることが知られている．したがって定理 4 で得られている評価は，推定が容易なシステムに対してはより大きな雑音を加える必要があるという自然な解釈が可能である． ◁

ここまで，出力に雑音を加えることを考えてきたが，入力に直接，雑音を印加することで与えられた差分プライバシー水準を達成することも可能である．入力に雑音が加わった以下のシステムを考える．

$$\begin{cases} x_{k+1} = Ax_k + B(u_k + v_k), \\ y_{v,k} = Cx_k + D(u_k + v_k). \end{cases} \tag{37}$$

出力系列 $Y_{v,T} = [y_{v,0}; \cdots; y_{v,T}]$ は

$$Y_{v,T} = N_T U_T + N_T V_T \tag{38}$$

で与えられる．安定分布が線形変換について閉じていることを利用すると，定理 4 から以下の結果を得る[5],[16]．

［系 1］（入力雑音による差分プライバシー条件） D は正方行列かつ正則であるとし，$\alpha \in (0,2)$, $\varepsilon > 0$, $\delta \in (0,1)$ とする．$c > 0$ と $T \in \mathbb{Z}_+$，(33) で定まる A_α に対して，行列 $\Sigma \succ 0$ を

$$\lambda_{\min}^{1/2}(\Sigma) \geqq \frac{c}{\mathcal{Q}_{\alpha,\varepsilon}^{-1}(\delta)} \tag{39}$$

が成り立つように選ぶ．このとき，$V_T \sim \boldsymbol{SG}_{(T+1)m}(\alpha, \Sigma)$ により生成されるメカニズム (38) は Adj_2^c と有限時刻 $T \in \mathbb{Z}_+$ について，(ε, δ)-差分プライバシーを満たす． ◁

本結果より，入力に直接雑音を加える場合，差分プライバシー水準はシステムそのものによらないということが分かる．これは，保護したい入力に対する雑音の SN 比を直接指定していることから導かれる結果と解釈できる．なお，系 1 では D は正方行列かつ正則としたが，文献(15) Corollary 2.16 で用いられている手法により，この仮定は緩めることができる．

6. 数値シミュレーション法

最後に数値シミュレーションの方法を簡単に紹介しておこう．まず安定分布の標本は以下の性質[7]

$$X = \frac{\sin(\alpha U)}{(\cos(U))^{\frac{1}{\alpha}}}\left(\frac{\cos((1-\alpha)U)}{E}\right)^{\frac{1-\alpha}{\alpha}} \sim \boldsymbol{S\alpha S}(\alpha) \tag{40}$$

を用いることで生成できる．ここで U, E はそれぞれ $(-\frac{\pi}{2}, \frac{\pi}{2})$ 上の一様分布，強度 1 の指数分布に従う確率変数で互いに独立である．つぎに，安定過程で駆動される連続時間動的システムのシミュレーションは

$$L_{t+\mathrm{d}t} - L_t \sim (\mathrm{d}t)^{1/\alpha}\boldsymbol{S\alpha S}(\alpha),\ \mathrm{d}t > 0$$

が成り立つことから，オイラー・丸山法[19]を用いることが可能である．例えば以下のシステム

$$\mathrm{d}x_t = f(t, x_t)\mathrm{d}t + g(t, x_t)\mathrm{d}L_t,\ x_0 = x_\mathrm{i}$$

の標本経路を生成したい場合，つぎのように `x[m]` を生成すると，時間幅 h が十分小さければ $t =$ `t[m]` における x_t のよい近似となる．

```
m=0;
t[m]=0; x[m]=x_i;
dt = h;
for
    t[m+1]=t[m]+dt;
    U = randu(); E = rande();
    noise = dt^(1/alpha)...
        *sin(alpha*U)/((cos(U))^(1/alpha))...
        *(cos((1-alpha)*U)/E)^((1-alpha)/alpha);
```

```
    x[m+1]=x[m]+f(t[m],x[m])*dt+g(t[m],x[m])*noise;
    m=m+1;
end
```

ただし rand*() はそれぞれ

- randu：$\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ 上の一様分布
- rande：強度 1 の指数分布

に従う独立同分布の乱数を発生する．alpha は安定過程 L_t のパラメータ α である．

7. おわりに

本稿では，レアイベントを考慮できるモデルとして安定分布雑音で駆動される確率システムを導入し，その基本的性質と解析的な扱いやすさを紹介した．そしてその性質を活用した例として等価線形化とプライバシー保護を紹介した．ここまで見てきたとおり，安定分布雑音はガウス雑音と似た性質を幾つももつ．しかしながら，ガウス分布から安定分布への結果の拡張は必ずしも自明ではない．例えばガウス分布，つまり $\alpha = 2$ の安定分布は有限な α $(= 2)$ 次モーメントをもつが，$\alpha < 2$ の安定分布では α 次モーメントは有限にならない．また本文中で述べたように密度関数が書き下せないというのも曲者である．これらにどう対処するかが主たる問題となるであろう．

レアイベントに関する研究は統計学や金融工学では盛んに取り組まれている話題であるが，制御工学の立場で取り組んだ研究は意外にも少ない．しかし風力発電の例から分かるようにレアイベントを考慮した枠組みでの議論は今後，更に求められるであろう．そして読者が安定分布に可能性を見いだし，新たな研究を生み出すきっかけに本稿がなれば，誠に幸いである．

謝辞　本研究は JSPS 科研費 (JP18H01461) の助成を受けたものです．

文　献

(1) 伊藤海斗，林輝，加嶋健司，加藤政一，“風力発電連係による擾乱のべき乗則の検証と確率システム解析，” 計測自動制御学会論文集，vol.54, no.12, pp.878–885, 2018.
(2) K. Kashima, H. Aoyama, and Y. Ohta, “Stable process approach to analysis of systems under heavy-tailed noise: Modeling and stochastic linearization,” IEEE Trans. Autom. Control, vol.64, no.4, pp.1344–1357, 2019.
(3) K. Ito and K. Kashima, “Theoretical error bounds for stochastic linearization of feedback systems,” 57th IEEE Conference on Decision and Control, pp.1065–1070, 2018.
(4) S. Ching, Y. Eun, C. Gokcek, P.T. Kabamba, and S.M. Meerkov, Quasilinear Control: Performance Analysis and Design of Feedback Systems with Nonlinear Sensors and Actuators, Cambridge University Press, 2011.
(5) 伊藤海斗，河野佑，加嶋健司，“線形システムに対する裾の重い雑音を用いたプライバシー保護，” 第 63 回自動制御連合講演会講演論文集，pp.907–910, 2020.
(6) P. Billingsley, Probability and Measure, Wiley, 2012.
(7) G. Samorodnitsky and M.S. Taqqu, Stable Non-Gaussian Random Processes: Stochastic Models with Infinite Variance, Chapman & Hall, 1994.
(8) J.P. Nolan, “Numerical calculation of stable densities and distribution functions,” Communications in Statistics: Stochastic Models, vol.13, no.4, pp.759–774, 1997.
(9) MATLAB, R2020b, The MathWorks Inc., Natick, Massachusetts, 2020.
(10) K. Sato, Lévy Processes and Infinitely Divisible Distributions, Cambridge University Press, 1999.
(11) J.P. Nolan, “Multivariate elliptically contoured stable distributions: Theory and estimation,” Computational Statistics, vol.28, no.5, pp.2067–2089, 2013.
(12) 加嶋健司，河合玲一郎，“レビー過程：白色雑音の一般化，” システム/制御/情報，vol.55, no.12, pp.505–512, 2011.
(13) J.A. Bucklew, Introduction to Rare Event Simulation, Springer, 2010.
(14) C. Dwork, F. McSherry, K. Nissim, and A. Smith, “Calibrating noise to sensitivity in private data analysis,” Theory of Cryptography Conference, pp.265–284, 2006.
(15) Y. Kawano and M. Cao, “Design of privacy-preserving dynamic controllers,” IEEE Trans. Autom. Control, vol.65, no.9, pp.3863–3878, 2020.
(16) K. Ito, Y. Kawano, and K. Kashima, “Privacy protection with heavy-tailed noise for linear dynamical systems,” Automatica, submitted.
(17) J. Le Ny and G.J. Pappas, “Differentially private filtering,” IEEE Trans. Autom. Control, vol.59, no.2, pp.341–354, 2014.
(18) Y. Kawano, K. Kashima, and M. Cao, “Modular control under privacy protection: Fundamental trade-offs,” Automatica, to appear.
(19) P.E. Kloeden and E. Platen, Numerical Solution of Stochastic Differential Equations, corrected edition, Springer, 2010.

（MSS 研究会提案，2020 年 12 月 9 日受付，
2021 年 1 月 6 日再受付）

伊藤海斗
2019 京都大学大学院情報学研究科修士課程修了．同年，同博士課程に進学し，現在に至る．非ガウス型の確率系のシステム制御理論及びその応用の研究に従事．

加嶋健司（正員）
2005 京都大学情報学研究科博士課程修了．東京工業大学大学院情報理工学研究科助教，Universität Stuttgart 滞在，大阪大学大学院基礎工学研究科准教授などを経て，2013 年 12 月より京都大学大学院情報学研究科准教授となり現在に至る．制御工学を専門とし，特に，確率制御理論と機械学習理論の融合に興味をもつ．2019 IEEE CSS Roberto Tempo Best CDC Paper Award, Alexander Humboldt Research Fellowship, SICE 論文賞武田賞，制御部門パイオニア賞，ISCIE 論文賞，産業技術賞などを受賞．