第 63 回実函数論・函数解析学
合同シンポジウム
講演集

期日：2024 年 9 月 9 日（月）〜 9 月 11 日（水）
会場：東京大学駒場キャンパス数理科学研究科棟

まえがき

本講演集は，2024 年 9 月 9 日 (月) から 9 月 11 日までの 3 日間にわたり，東京大学駒場キャンパス数理科学研究科棟で開催された第 63 回実函数論・函数解析学合同シンポジウムの講演集です.

本シンポジウムの開催のために多くの方々にご協力をいただきましたが，関係者各位のご尽力によって，講演者の方々の素晴らしい論文を本講演集で発表することができました．各グループの責任者の方々，講演者の皆様，本シンポジウム参加者の皆様方に深く感謝いたします.

伊藤 健一 （東京大学・数理科学研究科）
佐々木 格 （信州大学・理学部）
鈴木 智成 （九州工業大学・工学研究院）

第 63 回実函数論・函数解析学合同シンポジウム
プログラム

期日：2024 年 9 月 9 日 (月) 13:30 〜 9 月 11 日 (水) 11:45

会場：東京大学駒場キャンパス・数理科学研究科棟・大講義室

〒 153-8914 東京都目黒区駒場 3-8-1

https://www.ms.u-tokyo.ac.jp/access/index.html

9 月 9 日（月）

13:30 –14:30：中里 亮介（信州大学・工学部）

“Fourier-Herz 空間上での Navier-Stokes 方程式の解析性とその応用”

14:45 –15:45：川﨑 敏治（玉川大学・工学部）

“Fixed point and convergence theorems for mappings determined by several parameters”

16:00 –17:00：紅村 冬大（理化学研究所・革新知能統合研究センター）

“*-homomorphisms between groupoid C*-algebras”

9 月 10 日（火）

9:30 –10:30：内田 匠風（日本大学・理工学部）

“Pearcey 系に対する WKB 解の Borel 和の接続公式について”

10:45 –11:45：関口 英子（東京大学・数理科学研究科）

“不定値グラスマン多様体上のコホモロジーの同型について”

13:45 –14:45：神保 洸貴（東京理科大学・創域理工学部）

“非対称鍵共有法の数学的特徴付けと応用について”

15:00 –16:00：至田 直人（名古屋大学・多元数理科学研究科）
“Bilinear oscillatory Fourier multipliers”

16:15 –17:15：森 迪也（東京大学・数理科学研究科）
“The distance from a projection to nilpotents”

9 月 11 日（水）

9:30 –10:30：嵐 晃一（東京学芸大学・教育学部）
“冪零リー群の表現と擬対称領域上の核関数”

10:45 –11:45：波多野 修也（中央大学・理工学部）
“Smoothing estimate for the heat semigroup with a homogeneous weight on Morrey spaces”

※ 合同シンポジウム委員会で検討した結果，懇親会はなしとさせていただきます．

代表者：伊藤健一（東京大学・数理科学研究科）
佐々木格（信州大学・理学部）
鈴木智成（九州工業大学・工学研究院）

目次

FOURIER-HERZ 空間上での NAVIER-STOKES 方程式の解析性とその応用

中里 亮介 (信州大学 工学部)*

1. Introduction; Navier-Stokes equations, Function spaces

1.1. **Navier-Stokes 方程式に対する問題意識.** 本稿では, 流体力学の基礎方程式, 特に水などの粘性流体の運動を記述する非圧縮性 Navier-Stokes 方程式の初期値問題を, d 次元ユークリッド空間 $\mathbb{R}^d$ $(d \geq 2)$ 上で考察する:

$$\begin{cases} \partial_t u - \nu\Delta u + \operatorname{div}(u\otimes u) + \nabla p = 0, & t>0,\ x\in\mathbb{R}^d, \\ \operatorname{div} u = 0, & t>0,\ x\in\mathbb{R}^d, \\ u|_{t=0} = u_0, & x\in\mathbb{R}^d. \end{cases} \tag{1.1}$$

ただし $u = u(t,x) : \mathbb{R}_+ \times \mathbb{R}^d \to \mathbb{R}^d$, $p = p(t,x) : \mathbb{R}_+ \times \mathbb{R}^d \to \mathbb{R}^d$ はそれぞれ, 流体の速度ベクトル場と圧力を表す未知函数であるとし, $u_0 = u_0(x) : \mathbb{R}^d \to \mathbb{R}^d$ は初期流速を表す. また $\nu > 0$ は粘性係数を表し, テンソル積 $u\otimes u$ は d 次正方行列 $(u_i u_j)_{i,j}$ (u_i は流速ベクトル場 u の第 i 成分を表す) で定義される. $\operatorname{div} u = 0$ の条件下では, $\operatorname{div}(u\otimes u) = (u\cdot\nabla)u$ が成り立つ.

この初期値問題 (1.1) に対する著名な未解決問題の一つとして, 2000 年にクレイ数学研究所から提唱された, 「Navier-Stokes 方程式の解の存在と滑らかさ」が挙げられる†. その解決のためのアプローチの一つとして, 解の「適切性」と呼ばれる性質を,「臨界空間」と呼ばれる低正則函数空間上で調べる研究が, これまで盛んに行われてきた. ここで「適切性」とは, Hadamard により提唱されたもので, 初期値問題の解の (1) 存在性, (2) 一意性, (3) 初期値連続依存性 (初期値 u_0 近傍での解写像の安定性) の総称である. もし (1) から (3) の性質の内一つでも否定された場合, その初期値問題は「非適切」であるという. また「臨界空間」は, 方程式を不変に保つ時空スケール変換に対し, ノルム不変となる函数空間と定義する. 例えば, 初期値問題 (1.1) の解 (u,p) と任意のパラメータ $\lambda > 0$ に対して, スケール変換した関数の組 $(u_\lambda, p_\lambda) = (u_\lambda(t,x), p_\lambda(t,x))$ を

$$\begin{cases} u_\lambda(t,x) = \lambda u(\lambda^2 t, \lambda x), \\ p_\lambda(t,x) = \lambda^2 p(\lambda^2 t, \lambda x), \end{cases} \tag{1.2}$$

と定義すると, (u_λ, p_λ) もまた方程式 (1.1) の解となることがわかる. このスケール変換に対しノルム不変になる時空函数空間として, Bochner 空間 $L^r(\mathbb{R}_+; X)$ $(1 \leq r \leq \infty)$ において X を斉次 Sobolev 空間 $\dot{H}^s_p(\mathbb{R}^d)$ $(s\in\mathbb{R},\ 1\leq p\leq\infty)$ と選んだときの函数空間 $L^r(\mathbb{R}_+; \dot{H}^s_p)$ を例として考えて

*〒 380-8553 長野県長野市若里 4-17-1 信州大学 長野キャンパス 総合研究棟 (W2 棟) 6 階 602-5.
信州大学 工学部 工学基礎部門 数学教室 助教. E-mail: nakasato@shinshu-u.ac.jp

†Navier-Stokes 方程式の解の存在と滑らかさについて:
(クレイ数学研究所の HP) http://www.claymath.org/millennium-problems/navier-stokes-equation

みる. もし (r,s,p) が $2/r+d/p=1+s$ を満たすならば,

$$\begin{aligned}\|u_\lambda\|^r_{L^r(\mathbb{R}_+;\dot{H}^s_p)} =&\int_0^\infty \left\|\mathcal{F}^{-1}\left[|\xi|^s\widehat{u}_\lambda\right]\right\|^r_{L^p}dt\\ =&\lambda^{(-\frac{2}{r}-\frac{d}{p}+1+s)r}\int_0^\infty \left\|\mathcal{F}^{-1}\left[|\xi|^s\widehat{u}\right]\right\|^r_{L^p}dt=\|u\|_{L^r(\mathbb{R}_+;\dot{H}^s_p)}\end{aligned}$$

が成り立つことから, $2/r+d/p=1+s$ を満たす指数対 (r,s,p) より定まる $L^r(\mathbb{R}_+;\dot{H}^s_p)$ は初期値問題 (1.1) の臨界空間となることがわかる.

1.2. **初期値問題 (1.1) の適切性・非適切性に関する先行研究.** $p=2$ としたときの臨界 Sobolev 空間 $\dot{H}^{-1+\frac{d}{2}}(\mathbb{R}^d)$ 上では, 1964 年に Fujita-Kato [12] により, 解の時間局所適切性 (i.e. 時間局所=解の存在時刻が有限) と, 初期値の $\dot{H}^{-1+\frac{d}{2}}(\mathbb{R}^d)$-ノルムが十分に小さいとき, 解 u は時間大域適切性を満たすことが明らかになった. この Fujita-Kato の先駆的な研究以降, 様々な臨界空間 ($L^d(\mathbb{R}^d)$, $\dot{B}^{-1+\frac{d}{p}}_{p,\infty}(\mathbb{R}^d)$ $(d\le p<\infty)$, $\dot{\mathcal{N}}^{-1+\frac{d}{p}}_{p,q,\infty}(\mathbb{R}^d)$, $BMO^{-1}(\mathbb{R}^d)\simeq\dot{F}^{-1}_{\infty,2}(\mathbb{R}^d)$) 上での研究成果が知られている (cf. Cannone-Meyer-Planchon [5], Kato [17], Koch-Tataru [18], Kozono-Yamazaki [20]). しかし, 端点 $p=\infty$ の場合の臨界 Besov 空間 $\dot{B}^{-1}_{\infty,\sigma}(\mathbb{R}^d)$ 上では, 解写像の初期値連続依存性がすべての $\sigma\in[1,\infty]$ に対して破綻するため, 初期値問題 (1.1) は非適切になることが知られている (cf. Bourgain-Pavlović [4], Wang [34], Yoneda [35]). ここで上述の函数空間に対して, 次の包含関係が成り立つことに注意する:

$$\dot{H}^{-1+\frac{d}{2}}(\mathbb{R}^d)\subset L^d(\mathbb{R}^d)\subset \dot{B}^{-1+\frac{d}{p}}_{p,\infty}(\mathbb{R}^d)\,(d\le p<\infty)\subset\dot{B}^{-1}_{\infty,\infty}(\mathbb{R}^d).$$

一方で, 端点 $p=\infty$ の場合については, 解の Fourier 像の遠方での挙動と特異性に着目した臨界空間上での研究が存在する. 先駆的な研究として, 2008 年に, Giga-Inui-Mahalov-Saal [13] により, 擬測度空間 $\mathcal{FM}^{-1}_{0,\sigma}(\mathbb{R}^d)$ において, 最大正則性評価と Coriolis 力付きの Navier-Stokes 方程式は時間大域適切であることが証明された. その後, Fourier-Herz 空間 $\widehat{\dot{B}}{}^{-1}_{\infty,\sigma}(\mathbb{R}^d)$ (cf. 後述の**定義 1.1**) 上で, 任意の $\sigma\in[1,2]$ に対し, 初期値問題 (1.1) の解は時間大域適切性を満たすことが証明された (cf. Cannone-Wu [6], Iwabuchi [15], Iwabuchi-Takada [16], Lei-Lin [21]). また論文 [16] では, $\sigma>2$ の場合は初期値問題 (1.1) は非適切であることも示されており, $\widehat{\dot{B}}{}^{-1}_{\infty,\sigma}(\mathbb{R}^d)$ 上では $\sigma=2$ を境に (1.1) の解の適切性・非適切性が分かれることが明らかになった.

本稿では, 特に, 時間大域適切性が得られる限界のクラス $\widehat{\dot{B}}{}^{-1}_{\infty,2}(\mathbb{R}^d)$ に焦点を当て, その上での解の強い正則性 (滑らかさ) と長時間挙動について考察したい.

1.3. **Fourier-Herz 空間と初期値問題 (1.1) の軟解の定義.** 以下では, 本稿を通して用いる函数空間と初期値問題 (1.1) の軟解に関し, それらの定義を述べる.

$d\ge1$, $1\le p\le\infty$ に対し, $L^p=L^p(\mathbb{R}^d)$ は Lebesgue 空間を表す. Schwartz 空間 $\mathcal{S}=\mathcal{S}(\mathbb{R}^d)$ に属する函数 f に対して, その Fourier 変換 $\widehat{f}=\widehat{f}(\xi)$ (または $\mathcal{F}[f]=\mathcal{F}[f](\xi)$) を

$$\widehat{f}(\xi)=\mathcal{F}[f](\xi):=\frac{1}{(2\pi)^{d/2}}\int_{\mathbb{R}^d}e^{-ix\cdot\xi}f(x)\,dx$$

と定義する．同様に, $g\in\mathcal{S}(\mathbb{R}^d_\xi)$ に対して, Fourier 逆変換 $\mathcal{F}^{-1}[g]=\mathcal{F}^{-1}[g](x)$ を

$$\mathcal{F}^{-1}[g](x):=\frac{1}{(2\pi)^{d/2}}\int_{\mathbb{R}^d}e^{ix\cdot\xi}g(\xi)\,d\xi$$

と定義する．また Fourier 像側での単位の分解としてよく用いられる, Littlewood-Paley の 2 進単位分解 $\{\phi_j\}_{j\in\mathbb{Z}}$ を導入する．$\{\phi_j\}_{j\in\mathbb{Z}}\subset\mathcal{S}$ は次の性質を満たす函数族である:

$$\widehat{\phi_j}(\xi):=\widehat{\phi}(2^{-j}\xi)\ (j\in\mathbb{Z}),\ \ \sum_{j\in\mathbb{Z}}\widehat{\phi}_j(\xi)=1\ (\xi\neq0)\ \text{ and }\ \operatorname{supp}\widehat{\phi}\subset\{\xi\in\mathbb{R}^d;\frac{1}{2}\leq|\xi|\leq2\}.$$

$\{\phi_j\}_{j\in\mathbb{Z}}$ の構成については, 例えば文献 [3, Proposition 2.10] を参照せよ．$\dot{\Delta}_jf:=\mathcal{F}^{-1}[\widehat{\phi}_j\widehat{f}]$ と定義すると, $\sum_{j\in\mathbb{Z}}\dot{\Delta}_jf=f$ が緩増加超関数 $\mathcal{S}'$ の位相で成り立つ．今導入した 2 進単位分解 $\{\phi_j\}_{j\in\mathbb{Z}}$ を用いて, Fourier-Herz 空間と Chemin-Lerener 型時空函数空間を以下で定義する．

定義 1.1 (*Fourier-Herz spaces* [14])**.** $s\in\mathbb{R}$, $1\leq p,\sigma\leq\infty$ とする．Fourier-Herz 空間 $\dot{\widehat{B}}^s_{p,\sigma}=\dot{\widehat{B}}^s_{p,\sigma}(\mathbb{R}^d)$ とそのノルム $\|\cdot\|_{\dot{\widehat{B}}^s_{p,\sigma}}$ を以下で定義する:

$$\dot{\widehat{B}}^s_{p,\sigma}:=\left\{f\in\mathcal{S}'(\mathbb{R}^d);\widehat{f}\in L^1_{loc}(\mathbb{R}^d),\|f\|_{\dot{\widehat{B}}^s_{p,\sigma}}<\infty\right\},\ \ \|f\|_{\dot{\widehat{B}}^s_{p,\sigma}}:=\left\|\left\{2^{sj}\|\dot{\Delta}_jf\|_{\widehat{L}^p}\right\}_{j\in\mathbb{Z}}\right\|_{\ell^\sigma}.$$

ただし Fourier-Lebesgue ノルム $\|\cdot\|_{\widehat{L}^p}$ を $\|f\|_{\widehat{L}^p}:=\|\widehat{f}\|_{L^{p'}_\xi}$ と定義し, p' は p の Hölder 共役を表す．

定義 1.2 (*Chemin-Lerner spaces* [8])**.** $s\in\mathbb{R}$, $1\leq p,\sigma,r\leq\infty$ とし, $T\in\mathbb{R}_+$ に対して $I=[0,T]$ と定める．Fourier-Herz 空間を基調とした Chemin-Lerner 空間を次のように定める:

$$\widetilde{L^r(I;\dot{\widehat{B}}^s_{p,\sigma})}:=\overline{C(I;\mathcal{S}_0)}^{\|\cdot\|_{\widetilde{L^r(I;\dot{\widehat{B}}^s_{p,\sigma})}}},\ \ \|f\|_{\widetilde{L^r(I;\dot{\widehat{B}}^s_{p,\sigma})}}:=\left\|\left\{2^{sj}\|\dot{\Delta}_jf\|_{L^r(I;\widehat{L}^p)}\right\}_{j\in\mathbb{Z}}\right\|_{\ell^\sigma}.$$

ただし $\mathcal{S}_0=\mathcal{S}_0(\mathbb{R}^d)$ は Schwartz 空間 $\mathcal{S}(\mathbb{R}^d)$ の部分集合であり, $\operatorname{supp}\widehat{f}\subset\mathbb{C}\backslash\{0\}$ を満たす函数全体の集合であるとする．もし $T=\infty$ と取れる場合, $\widetilde{L^r(\mathbb{R}_+;\dot{\widehat{B}}^s_{p,\sigma})}$ と表記する．

定義 1.3 (*Mild solution to* (1.1))**.** ある初期値 $u_0=u_0(x)$ に対し, $u\in L^2(\mathbb{R}_+;\widehat{L}^\infty)$ が次の積分方程式を満たすとき, u を初期値問題 (1.1) の解 (特に軟解) であるという:

$$u(t)=e^{t\nu\Delta}u_0-\int_0^te^{(t-\tau)\nu\Delta}\,\mathcal{P}_\sigma\operatorname{div}(u\otimes u)(\tau)\,d\tau\quad in\ \ L^2(\mathbb{R}_+;\widehat{L}^\infty).$$

ただし, $e^{t\nu\Delta}u_0:=\mathcal{F}^{-1}[e^{-t\nu|\xi|^2}\widehat{u}_0]$ であり, $\mathcal{P}_\sigma$ はソレノイダル空間への Helmholtz 射影作用素を表し, ベクトル場 $v\in\mathcal{S}'(\mathbb{R}^d)$ に対して, $\mathcal{P}_\sigma v:=v+(-\Delta)^{-1}\nabla\operatorname{div}v$ と定義される．

2. Main Results; Analyticity, Asymptotic behavior

2.1. **主結果 I (解析性と L^p-L^1 型減衰評価).** 以下では, $s\in\mathbb{R}$ と $v\in\mathcal{S}'(\mathbb{R}^d)$ に対し, $|\nabla|^sv:=\mathcal{F}^{-1}[|\xi|^s\widehat{v}]$ と定める．初期値問題 (1.1) に対して, 次の解析性と時間減衰評価に関する結果を得た．

定理 2.1 (*Global well-posedness and Analyticity* [29])**.** $\mathcal{S}'(\mathbb{R}^d)$ の意味で $\operatorname{div}u_0=0$ を満たす初期値 $u_0\in\dot{\widehat{B}}^{-1}_{\infty,2}(\mathbb{R}^d)$ に対して, ある十分に小さい定数 $\varepsilon_0>0$ が存在し, $\|u_0\|_{\dot{\widehat{B}}^{-1}_{\infty,2}}\leq\varepsilon_0$ が成り立つと

仮定する. このとき, 初期値問題 (1.1) の時間大域解 u が一意的に存在し, 次を満たす:

$$u \in C([0,\infty);\widehat{\dot{B}}^{-1}_{\infty,2}) \cap L^2(\mathbb{R}_+;\widehat{\dot{B}}^{0}_{\infty,1}) \cap \widetilde{L^1(\mathbb{R}_+};\widehat{\dot{B}}^{1}_{\infty,2}).$$

($Analyticity$) 更に, ある定数 $C>0$ が存在し, u は次の時間一様評価を満たす:

$$\|e^{\sqrt{\nu t}|\nabla|}u\|_{\widetilde{L^\infty(0,t};\widehat{\dot{B}}^{-1}_{\infty,2})\cap L^2(0,t;\widehat{\dot{B}}^{0}_{\infty,1})\cap\widetilde{L^1(0,t};\widehat{\dot{B}}^{1}_{\infty,2})} \le C\|u_0\|_{\widehat{\dot{B}}^{-1}_{\infty,2}} \quad \textit{for all } t>0. \tag{2.1}$$

注意 2.2. $\widehat{\dot{B}}^{-1}_{\infty,2}(\mathbb{R}^d)$ 上での時間大域適切性については, 論文 [6, 16] 内で既に証明されている. 定理 2.1 では, [6, 16] で得られた大域解 u が $u\in L^2(\mathbb{R}_+;\widehat{\dot{B}}^{0}_{\infty,1})$ と解析性評価 (2.1) を満たすことを明らかにした. 後述する定理 2.4 と 2.5 の証明では, (2.1) が本質的に重要な役割を果たす.

注意 2.3. (2.1) のような解析性評価は, 1989 年に, Foias-Temam [10] により考案されたものである. Oliver-Titi [31, Theorem 6] と同様の議論で, 定理 2.1 で得られた解 u は, 実解析函数全体のクラスである $C^\omega(\mathbb{R}^d)$ に属することもわかる. 臨界空間上での解析性評価に関する研究としては, 例えば, Bae [1], Bae-Biswas-Tadmor [2], Lemarie [22, Chapter 24] が挙げられる. 圧縮性粘性流体の数理モデルへの応用については, Charve-Danchin-Xu [7], Song-Xu [32] を参照せよ.

定理 2.4 ($\widehat{L}^p$-$\widehat{L}^1$ *decay estimates* [29])**.** $1\le p\le\infty$ とする. 初期値 u_0 は定理 2.1 と同じ仮定を満たすとし, 更に $u_0\in\widehat{\dot{B}}^{0}_{1,\infty}(\mathbb{R}^d)$ も満たすと仮定する. このとき, 初期値問題 (1.1) の時間大域解 u は, 任意の $s>-d/p'$ に対して, 次の L^p-L^1 型の減衰評価を満たす:

$$\||\nabla|^s u(t)\|_{\widehat{L}^p} = O(t^{-\frac{d}{2}(1-\frac{1}{p})-\frac{s}{2}}) \quad (t\to\infty). \tag{2.2}$$

2.2. **主結果 II (Fujigaki-Miyakawa 型の漸近展開).** 定理 2.1 の (2.1) と定理 2.3 の応用で, Miyakawa [25, 26] や Fujigaki-Miyakawa [11] で得られている, Refined decay estimate や軟解の漸近展開についても導出が可能である. 重み付き Hardy 空間での減衰評価と漸近展開に関しては, Okabe-Tsutsui [30], Tsutsui [33] で導出されている.

ここでは論文 [11] に倣って, "summation convention" の形式で主定理を述べる.

定理 2.5 ($Asymptotic\ expansion$ [29])**.** $d\ge 3$, $1\le p\le\infty$ とする. 初期値 u_0 は定理 1.4 と同じ仮定を満たすとし, 更に $u_0\in L^1(\mathbb{R}^d)$, $x_k u_0\in L^1(\mathbb{R}^d)$ $(k=1,2,\dots,d)$ も満たすと仮定する. このとき, 初期値問題 (1.1) の時間大域解 u は,

$$s > -1-\min\left\{\frac{d}{p},\frac{d}{p'}\right\} \ \ if \ \ 1<p<\infty, \quad s\ge -1 \ \ if \ \ p=1,\infty$$

を満たすすべての $s\in\mathbb{R}$ に対して, 次の減衰評価を満たす:

$$\begin{aligned}\lim_{t\to\infty} t^{\frac{d}{2}(1-\frac{1}{p})+\frac{s+1}{2}} \Bigg\| |\nabla|^s \Bigg(& u(t) + (\partial_k G_t)(\cdot)\int_{\mathbb{R}^d} y_k u_0(y)dy \\ & + (\partial_k S_t)(\cdot)\int_0^\infty \int_{\mathbb{R}^d} (u_k u)(y,\tau)dyd\tau \Bigg)\Bigg\|_{\widehat{L}^p} = 0.\end{aligned}$$

ただし $G_t(x) := \mathcal{F}^{-1}[e^{-\nu t|\xi|^2}]$ (Gauss 核), $S_t(x) := \mathcal{F}^{-1}[e^{-\nu t|\xi|^2}P_\sigma(\xi)]$, $P_\sigma(\xi) := (\delta_{lm} - \frac{i\xi_l i\xi_m}{|\xi|^2})_{1\le l,m\le d}$ (Helmholtz 射影作用素 $\mathcal{P}_\sigma$ のシンボル) とする.

3. Preliminaries; Product estimates, maximal regularity

3.1. **Fourier-Herz 空間の基本性質.** ここではまず Fourier-Herz 空間の基本性質について幾つかを紹介する. 命題の証明やここでは取り上げない基本性質については, 論文 [9], [19], [23], [24], [27] などを参照せよ.

命題 3.1 (*Sobolev-type embedding* [27])**.** $s \in \mathbb{R}$, $d \geq 1$, $1 \leq p_1 \leq p_2 \leq \infty$, $1 \leq \sigma_1 \leq \sigma_2 \leq \infty$ とする. このとき, 次の連続な埋め込みが成り立つ:

$$\widehat{\dot{B}}^s_{p_1,\sigma_1}(\mathbb{R}^d) \hookrightarrow \widehat{\dot{B}}^{s-d(\frac{1}{p_1}-\frac{1}{p_2})}_{p_2,\sigma_2}(\mathbb{R}^d).$$

命題 3.2 ([9], [19])**.** $s \in \mathbb{R}$, $d \geq 1$, $1 \leq p \leq \infty$ とする. Fourier-Herz 空間 $\widehat{\dot{B}}^s_{p,p'}(\mathbb{R}^d)$ と Fourier-Sobolev 空間 $\widehat{\dot{H}}^s_p(\mathbb{R}^d)$ はノルム同値の意味で同相である; $\widehat{\dot{B}}^s_{p,p'}(\mathbb{R}^d) \simeq \widehat{\dot{H}}^s_p(\mathbb{R}^d)$. ここで Fourier-Sobolev 空間 $\widehat{\dot{H}}^s_p = \widehat{\dot{H}}^s_p(\mathbb{R}^d)$ は以下のように定義される:

$$\widehat{\dot{H}}^s_p(\mathbb{R}^d) = \{f \in \mathcal{S}'; \widehat{f} \in L^1_{loc}(\mathbb{R}^d), \|f\|_{\widehat{\dot{H}}^s_p} < \infty\}, \quad \|f\|_{\widehat{\dot{H}}^s_p} = \||\nabla|^s f\|_{\widehat{L}^p}.$$

3.2. **Fourier-Herz 空間上での非線形評価.** 次に Navier-Stokes 方程式のアプリオリ評価を導出する際の非線形項 $\mathrm{div}\,(u \otimes u)$ (または $(u \cdot \nabla)u$) に用いる, 函数の積評価をいくつか紹介する.

次の命題は論文 [24, Lemma 2.4] で証明されたものである:

命題 3.3 (*Bilinear estimate* [24])**.** $s > 0$, $1 \leq p, \sigma \leq \infty$ とする. このとき, ある定数 $C > 0$ が存在して次の双線形評価が成り立つ:

$$\|fg\|_{\widehat{\dot{B}}^s_{p,\sigma}} \leq C \left(\|f\|_{\widehat{L}^\infty} \|g\|_{\widehat{\dot{B}}^s_{p,\sigma}} + \|f\|_{\widehat{\dot{B}}^s_{p,\sigma}} \|g\|_{\widehat{L}^\infty} \right). \tag{3.1}$$

次の積評価は Besov 空間ではよく知られているものであり, それを Fourier-Herz 空間上で再現したものである (より一般的な主張については, 論文 [27, Lemmas 2.4-2.6], [28, Lemma 5.2] などを参照せよ). Besov 空間上の積評価に関しては, 例えば文献 [3, Theorems 2.82, 2.85] が詳しい.

命題 3.4 (*Product estimates* [27])**.** $1 \leq p, \sigma \leq \infty$ とする. もし $s \in \mathbb{R}$ が,

$$|s| < -\frac{d}{p} \quad if \quad 1 \leq p \leq 2, \qquad -\frac{d}{p'} < s < \frac{d}{p} \quad if \quad p > 2$$

を満たすならば, ある定数 $C > 0$ が存在して, 次の評価が成り立つ:

$$\|fg\|_{\widehat{\dot{B}}^s_{p,\sigma}} \leq C \|f\|_{\widehat{\dot{B}}^s_{p,\sigma}} \|g\|_{\widehat{L}^\infty \cap \widehat{\dot{B}}^{\frac{d}{p}}_{p,\infty}}. \tag{3.2}$$

命題 3.5 (*The estimate for* $\mathcal{B}_t(f,g)$ [29])**.** $1 \leq p, p_1, p_2 \leq \infty$ は $\frac{1}{p} = \frac{1}{p_1} + \frac{1}{p_2}$ を満たすと仮定する. このとき, ある定数 $C > 0$ が存在して, 全ての $t \geq 0$ に対して次の不等式が成り立つ:

$$\|\mathcal{B}_t(f,g)\|_{\widehat{L}^p} \leq C \|f\|_{\widehat{L}^{p_1}} \|g\|_{\widehat{L}^{p_2}},$$

ただし $\mathcal{B}_t(f,g) = \mathcal{B}_t(f,g)(t,x) := e^{\sqrt{\nu t}|\nabla|}(e^{-\sqrt{\nu t}|\nabla|} f e^{-\sqrt{\nu t}|\nabla|} g)(x)$, $\nu > 0$ である.

命題 3.5 の証明. はじめに $p \neq 1$ の場合を考える. 合成積に対する Young の不等式と三角不等式 $|\xi| \leq |\xi-\eta| + |\eta|$ より,

$$
\begin{aligned}
\|\mathcal{B}_t(f,g)\|_{\widehat{L}^p} &= \left\| e^{\sqrt{\nu t}|\xi|} \int_{\mathbb{R}^d} e^{-\sqrt{\nu t}|\xi-\eta|} \widehat{f}(\xi-\eta) e^{-\sqrt{\nu t}|\eta|} \widehat{g}(\eta) d\eta \right\|_{L^{p'}_\xi} \\
&\leq \left[\int_{\mathbb{R}^d} \left(\int_{\mathbb{R}^d} e^{\sqrt{\nu t}(|\xi|-|\xi-\eta|-|\eta|)} |\widehat{f}(\xi-\eta)||\widehat{g}(\eta)| d\eta \right)^{p'} d\xi \right]^{1/p'} \\
&\leq \left\| \int_{\mathbb{R}^d} |\widehat{f}(\xi-\eta)||\widehat{g}(\eta)| d\eta \right\|_{L^{p'}_\xi} \leq \|\widehat{f}\|_{L^{p_1'}} \|\widehat{g}\|_{L^{p_2'}} = \|f\|_{\widehat{L}^{p_1}} \|g\|_{\widehat{L}^{p_2}}
\end{aligned}
$$

が得られる. $p=1$ の場合に関しては, Hölder の不等式より

$$
\|\mathcal{B}_t(f,g)\|_{\widehat{L}^1} \leq \left\| \int_{\mathbb{R}^d} |\widehat{f}(\xi-\eta)||\widehat{g}(\eta)| d\eta \right\|_{L^\infty_\xi} \leq \|\widehat{f}\|_{L^{p_1'}} \|\widehat{g}\|_{L^{p_2'}} = \|f\|_{\widehat{L}^{p_1}} \|g\|_{\widehat{L}^{p_2}}
$$

がわかるため, 以上より命題 3.5 の証明が完了する. ❑

3.3. **熱方程式の最大正則性.** 圧縮性・非圧縮性粘性流体の数理モデルの臨界空間上での解析に大きく寄与したのは, 非線形放物型方程式の主要部が持つ「最大正則性」と呼ばれる性質である. ここでは, Fourier-Herz 空間上での熱方程式の最大正則性について, その主張を述べる.

初期値問題 (1.1) に $\mathcal{P}_\sigma$ を作用させることで, $\mathcal{P}_\sigma u = u$ ($\operatorname{div} u = 0$ から従う) と $\mathcal{P}_\sigma \nabla p = 0$ に注意し, 次の拡散係数を $\nu > 0$, 外力を f $(= -\mathcal{P}_\sigma \operatorname{div}(u \otimes u))$ とする非斉次熱方程式が得られる:

$$
\begin{cases}
\partial_t u - \nu \Delta u = f, & t > 0,\, x \in \mathbb{R}^d, \\
u|_{t=0} = u_0, & x \in \mathbb{R}^d.
\end{cases}
\tag{3.3}
$$

Duhamel の原理より, (3.3) の解 u は次の積分方程式の形で表せることに注意せよ:

$$
u = e^{t\nu\Delta} u_0 + \int_0^t e^{(t-\tau)\nu\Delta} f(\tau)\, d\tau
$$

(この議論から, 初期値問題 (1.1) の解 u を定義 1.3 の形で定義することは自然だといえる).

命題 3.6 (*Smoothing estimates for* (3.3) [24], [27])**.** $s \in \mathbb{R}$, $1 \leq p, \sigma \leq \infty$, $1 \leq r_1 \leq r \leq \infty$ とし, $T \in \mathbb{R}_+$ に対し, $I := (0,T)$ とおく. また $u_0 \in \widehat{\dot{B}}{}^s_{p,\sigma}$, かつ $f \in \widetilde{L^{r_1}(I; \widehat{\dot{B}}{}^{s-2+2/r_1}_{p,\sigma})}$ を仮定する. このとき, 非斉次熱方程式 (3.3) の解 u に対し, 次の最大正則性型評価が成り立つ:

$$
\nu^{\frac{1}{r}} \|u\|_{\widetilde{L^r(I; \widehat{\dot{B}}{}^{s+\frac{2}{r}}_{p,\sigma})}} \leq C \left(\|u_0\|_{\widehat{\dot{B}}{}^s_{p,\sigma}} + \nu^{\frac{1}{r_1}-1} \|f\|_{\widetilde{L^{r_1}(I; \widehat{\dot{B}}{}^{s-2+\frac{2}{r_1}}_{p,\sigma})}} \right).
$$

命題 3.7 (Generalized maximal regularity [24])**.** $s \in \mathbb{R}$, $1 \leq r \leq \infty$ とし, $f \in L^1(\mathbb{R}_+; \widehat{\dot{B}}{}^s_{\infty,1})$ と仮定する. このとき, ある定数 $C > 0$ が存在して, 次の評価が成り立つ:

$$
\left\| |\nabla|^{\frac{2}{r}} \int_0^t e^{(t-s)\nu\Delta} f(s)\, ds \right\|_{L^r(\mathbb{R}_+; \widehat{\dot{B}}{}^s_{\infty,1})} \leq C \|f\|_{L^1(\mathbb{R}_+; \widehat{\dot{B}}{}^s_{\infty,1})}.
\tag{3.4}
$$

4. Outlined proof of the result on Analyticity and Time-Decay

4.1. **主定理証明のための鍵評価.** 本稿では, 定理 2.1 の (2.1) と定理 2.4 の証明の概略を述べる. 以下 2 つの補題は, そのための鍵となる評価であり, ここでは証明は述べずに結果のみを記載する.

補題 4.1 (*Bilinear estimate II* [29])**.** $T>0$ に対し, $I=(0,T)$ または $I=\mathbb{R}_+$ と定める. このとき, ある定数 $C>0$ が存在し, 次の双線形評価が成り立つ:

$$\left\| e^{\sqrt{\mu t}|\nabla|}(fg) \right\|_{\widetilde{L^1(I;\widehat{B}^0_{\infty,2})}} \le C\left(\|F\|_{\widetilde{L^\infty(I;\widehat{B}^{-1}_{\infty,2})}} \|G\|_{\widetilde{L^1(I;\widehat{B}^1_{\infty,2})}} + \|F\|_{\widetilde{L^1(I;\widehat{B}^1_{\infty,2})}} \|G\|_{\widetilde{L^\infty(I;\widehat{B}^{-1}_{\infty,2})}} \right).$$

ただし $F := e^{\sqrt{\mu t}|\nabla|}f$, $G := e^{\sqrt{\mu t}|\nabla|}g$ とした.

補題 4.2 (*Smoothing estimates for the linear solution* [29])**.** $1\le r<\infty$, $s\in\mathbb{R}$, $1\le p,\ \sigma\le\infty$, $c_0>0$ とする. このとき, ある定数 $C>0$ が存在し, 次の評価が成り立つ:

$$\left(\int_0^\infty \Big(\sum_{j\in\mathbb{Z}} e^{-c_0 t 2^{2j}\sigma} 2^{sj\sigma} \|\widehat{\phi}_j \widehat{v}\|^\sigma_{L^{p'}_\xi} \Big)^{\frac{r}{\sigma}} dt \right)^{\frac{1}{r}} \le C\|v\|_{\widehat{B}^{s-\frac{2}{r}}_{p,r}}.$$

4.2. **解析性評価 (2.1) の証明の概略.** 以下, $U=U(t,x):=e^{\sqrt{\nu t}|\nabla|}u(t,x)$ とする. u は初期値問題 (1.1) の軟解であるので, 定義 1.3 の式より $\widehat{U}=\widehat{U}(t,\xi)$ は

$$\begin{aligned} \widehat{U} =& e^{\sqrt{\nu t}|\xi|-\nu t|\xi|^2}\widehat{u}_0 - \int_0^t e^{\sqrt{\nu t}|\xi|-\nu(t-\tau)|\xi|^2} P(\xi) i\xi\cdot\mathcal{F}[u\otimes u]d\tau \\ =& e^{\sqrt{\nu t}|\xi|-\frac{\nu}{2}t|\xi|^2} e^{-\frac{\nu}{2}t|\xi|^2}\widehat{u}_0 \\ &- \int_0^t e^{\sqrt{\nu t}|\xi|-\sqrt{\nu\tau}|\xi|-\frac{\nu}{2}(t-\tau)|\xi|^2} e^{-\frac{\nu}{2}(t-\tau)|\xi|^2} P(\xi) i\xi\cdot\mathcal{F}[\widetilde{\mathcal{B}}_\tau(U,U)]d\tau \end{aligned} \tag{4.1}$$

を満たすことがわかる. ここで, $\mathbb{R}^d$-ベクトル場 a, b に対して, $\widetilde{\mathcal{B}}_t(a,b) := e^{\sqrt{\nu t}|\nabla|}(e^{-\sqrt{\nu t}|\nabla|}a\otimes e^{-\sqrt{\nu t}|\nabla|}b)$ とおいた. Fourier-Herz ノルムの評価を得るために, (4.1) の両辺に $\widehat{\phi}_j$ をかけると,

$$|\widehat{U}_j| \lesssim e^{-c_0 t 2^{2j}} |\widehat{\phi}_j\widehat{u}_0| + \int_0^t e^{-c_0(t-\tau)2^{2j}} 2^j |\widehat{\phi}_j \mathcal{F}[\widetilde{\mathcal{B}}_\tau(U,U)]| d\tau \tag{4.2}$$

が得られる. ここで $c_0=\nu/8$ とおき, (4.2) を得る際に次の一様評価を用いた:

$$e^{\sqrt{\nu t}|\xi|-\frac{\nu}{2}t|\xi|^2} \le \sqrt{e}, \quad e^{\sqrt{\nu t}|\xi|-\sqrt{\nu\tau}|\xi|-\frac{\nu}{2}(t-\tau)|\xi|^2} \le e^2.$$

(4.2) の両辺について, $L^{p'}_\xi(\mathbb{R}^d)$-ノルムをとることで

$$\|\widehat{U}_j(t)\|_{L^{p'}_\xi} \lesssim e^{-c_0 t 2^{2j}} \|\widehat{\phi}_j\widehat{u}_0\|_{L^{p'}_\xi} + \int_0^t e^{-c_0(t-\tau)2^{2j}} 2^j \|\widehat{\phi}_j \mathcal{F}[\widetilde{\mathcal{B}}_\tau(U,U)]\|_{L^{p'}_\xi} d\tau \tag{4.3}$$

を得る. また簡単な積分の計算より, すべての $1\le r\le\infty$ に対して,

$$\|e^{-c_0 2^{2j}\cdot}\|_{L^r(\mathbb{R}_+)} \lesssim (2^{2j})^{-\frac{1}{r}} \tag{4.4}$$

が得られるので, (4.3) の両辺 $L^r_t(I)$-ノルムをとり Young の不等式を用いることで,

$$\begin{aligned}\|\widehat{U}_j(t)\|_{L^r(I;L^{p'}_\xi)} \le &\|e^{-c_0 2^{2j}\cdot}\|_{L^r(\mathbb{R}_+)}\|\widehat{\phi}_j\widehat{u}_0\|_{L^{p'}_\xi} \\ &+ 2^j\|e^{-c_0 2^{2j}\cdot}\|_{L^\gamma(\mathbb{R}_+)}\|\widehat{\phi}_j\mathcal{F}[\widetilde{\mathcal{B}}_t(U,U)]\|_{L^{r_1}(I;L^{p'}_\xi)} \\ \lesssim\ & 2^{-\frac{2}{r}j}\|\widehat{\phi}_j\widehat{u}_0\|_{L^{p'}_\xi} + 2^{-\frac{2}{r}j}2^{(-1+\frac{2}{r_1})j}\|\widehat{\phi}_j\mathcal{F}[\widetilde{\mathcal{B}}_t(U,U)]\|_{L^{r_1}(I;L^{p'}_\xi)}\end{aligned} \tag{4.5}$$

が得られる. ただし, $1 \le r_1 \le r$ と γ は $\frac{1}{\gamma} = 1 + \frac{1}{r} - \frac{1}{r_1}$ を満たすように選んだ. (4.5) の両辺に 2^{sj} をかけて $\ell^\sigma(\mathbb{Z})$-ノルムをとることで,

$$\|U\|_{\widetilde{L^r(I;\widehat{B}^{s+\frac{2}{r}}_{p,\sigma})}} \lesssim \|u_0\|_{\widehat{B}^s_{p,\sigma}} + \|\widetilde{\mathcal{B}}_t(U,U)\|_{\widetilde{L^{r_1}(I;\widehat{B}^{s-1+\frac{2}{r_1}}_{p,\sigma})}} \tag{4.6}$$

を得る. (4.6) で $(r,s,p,\sigma) = (\infty,-1,\infty,2)$ or $(1,-1,\infty,2)$ と選び, 補題 4.1 を用いると,

$$\begin{aligned}\|U\|_{\widetilde{L^\infty(I;\widehat{B}^{-1}_{\infty,2})}\cap\widetilde{L^1(I;\widehat{B}^1_{\infty,2})}} &\lesssim \|u_0\|_{\widehat{B}^{-1}_{\infty,2}} + \|\widetilde{\mathcal{B}}_t(U,U)\|_{\widetilde{L^1(I;\widehat{B}^0_{\infty,2})}} \\ &\lesssim \|u_0\|_{\widehat{B}^{-1}_{\infty,2}} + \|U\|^2_{\widetilde{L^\infty(I;\widehat{B}^{-1}_{\infty,2})}\cap\widetilde{L^1(I;\widehat{B}^1_{\infty,2})}}\end{aligned} \tag{4.7}$$

が得られる.

最後に, U の $L^2(\mathbb{R}_+;\widehat{L}^\infty)$-ノルムの評価式を導出する. 先程得た $p=\infty$ の場合の (4.3) において, 両辺 $\ell^1(\mathbb{Z})$-ノルムと $L^2_t(I)$-ノルムをとることで,

$$\begin{aligned}\|U\|_{L^2(I;\widehat{B}^0_{\infty,1})} \lesssim &\left(\int_I\Big(\sum_{j\in\mathbb{Z}} e^{-c_0t2^{2j}}\|\widehat{\phi}_j\widehat{u}_0\|_{L^1_\xi}\Big)^2 dt\right)^{\frac{1}{2}} \\ &+ \left(\int_I\left(\int_0^t\sum_{j\in\mathbb{Z}} e^{-c_0(t-\tau)2^{2j}}2^j\|\widehat{\phi}_j\mathcal{F}[\widetilde{\mathcal{B}}_\tau(U,U)]\|_{L^1_\xi}\,d\tau\right)^2 dt\right)^{\frac{1}{2}} =: I_1 + I_2\end{aligned}$$

を得る. 補題 4.2 を用いると $I_1 \lesssim \|u_0\|_{\widehat{B}^{-1}_{\infty,2}}$ がわかる. I_2 の評価については, (4.4) と Hausdorff-Young の不等式 $\|f *_t g\|_{L^2(I)} \lesssim \|f\|_{L^2_t}\|g\|_{L^1_t}$ を用いることで,

$$\begin{aligned}I_2 &\lesssim \sum_{j\in\mathbb{Z}} 2^j\left(\int_I\left(\int_0^t e^{-c_0(t-\tau)2^{2j}}\|\widehat{\phi}_j\mathcal{F}[\widetilde{\mathcal{B}}_\tau(U,U)]\|_{L^1_\xi}\,d\tau\right)^2 dt\right)^{\frac{1}{2}} \\ &\lesssim \sum_{j\in\mathbb{Z}} 2^j\|e^{-c_0 2^{2j}\cdot}\|_{L^2(\mathbb{R}_+)}\int_I\|\widehat{\phi}_j\mathcal{F}[\widetilde{\mathcal{B}}_\tau(U,U)]\|_{L^1_\xi}dt \lesssim \|\widetilde{\mathcal{B}}_\tau(U,U)]\|_{L^1(I;\widehat{L}^\infty)}\end{aligned} \tag{4.8}$$

が得られる. 命題 3.2 より, $\widehat{L}^\infty(\mathbb{R}^d) \simeq \dot{\widehat{B}}{}^0_{\infty,1}(\mathbb{R}^d)$ が成り立つことに注意して, 得られた評価 (4.8) に Hausdorff-Young の不等式 $\|fg\|_{\widehat{L}^\infty} \lesssim \|f\|_{\widehat{L}^\infty}\|g\|_{\widehat{L}^\infty}$ を適用することで,

$$\|U\|_{L^2(I;\widehat{B}^0_{\infty,1})} \lesssim \|u_0\|_{\widehat{B}^{-1}_{\infty,2}} + \|U\|^2_{L^2(I;\widehat{B}^0_{\infty,1})} \tag{4.9}$$

を得る.

$I=(0,t)$ とおいて,

$$\mathcal{X}_\infty(t) := \|U\|_{\widetilde{L^\infty(I;\widehat{B}^{-1}_{\infty,2})}\cap L^2(I;\widehat{L}^\infty)\cap\widetilde{L^1(I;\widehat{B}^1_{\infty,2})}}$$

と定義すると, (4.7) と (4.9) より, 次の 2 次不等式が得られる:

$$\mathcal{X}_\infty(t) \lesssim \|u_0\|_{\widehat{B}^{-1}_{\infty,2}} + \mathcal{X}_\infty(t)^2. \tag{4.10}$$

初期条件の小ささに関する条件 $\|u_0\|_{\widehat{B}^{-1}_{\infty,2}} \ll 1$ を用いて, (4.10) より結論 (2.1) を得る. □

4.3. $\widehat{L}^p$-$\widehat{L}^1$ **減衰評価 (2.2) の証明の概略.** 解析性評価 (2.1) の応用として, $\widehat{L}^p$-$\widehat{L}^1$ 減衰評価 (2.2) を証明する. §4.2 で示した (4.6) を用いて, 次の $\widehat{L}^1(\mathbb{R}^d)$ 上での一様評価を得る.

補題 4.3 ($\widehat{L}^1$-*Uniform estimate* [29])**.** 初期値 u_0 の仮定は定理 2.4 と同じであるとする. このとき, 定理 2.1 で得られる初期値問題 (1.1) の解 u は, 次の時間一様評価を満たす:

$$\|(u,U)\|_{L^\infty(\mathbb{R}_+;\widehat{B}^0_{1,\infty})\cap \widetilde{L^2(\mathbb{R}_+;\widehat{B}^1_{1,\infty})}} \le C\|u_0\|_{\widehat{B}^0_{1,\infty}}.$$

補題 4.4. $\delta_0 > 0$ とする. このとき, すべての $\sigma > 0$ に対して, ある定数 $C = C(\sigma) > 0$ が存在して,

$$\sup_{t\ge 0}\sum_{j\in\mathbb{Z}} \left(2^j t^{\frac{1}{2}}\right)^\sigma e^{-\sqrt{t}\delta_0 2^j} \le C$$

が成り立つ.

任意の $s > -d/p'$ に対して, 補題 4.3 と補題 4.4 を用いることで,

$$\begin{aligned}
t^{\frac{d}{2p'}+\frac{s}{2}}\||\nabla|^s u(t)\|_{\widehat{B}^0_{p,1}} &\lesssim t^{\frac{d}{2p'}+\frac{s}{2}}\||\nabla|^s u(t)\|_{\widehat{B}^{d/p'}_{1,1}} \\
&\lesssim t^{\frac{d}{2p'}+\frac{s}{2}}\sum_{j\in\mathbb{Z}} 2^{(s+\frac{d}{p'})j}\|\widehat{\phi}_j e^{-\sqrt{\nu t}|\cdot|}\widehat{U}(t)\|_{L^\infty_\xi} \\
&\lesssim \sum_{j\in\mathbb{Z}} 2^{(s+\frac{d}{p'})j} t^{\frac{d}{2p'}+\frac{s}{2}} e^{-c_0\sqrt{\nu t}2^j}\|\widehat{\phi}_j\widehat{U}(t)\|_{L^\infty_\xi} \\
&\lesssim \|U(t)\|_{\widehat{B}^0_{1,\infty}}\sum_{j\in\mathbb{Z}}(\sqrt{t}2^j)^{(s+\frac{d}{p'})}e^{-c_0\sqrt{\nu t}2^j} \lesssim \|u_0\|_{\widehat{B}^0_{1,\infty}}
\end{aligned}$$

を得る. 従って, 欲しかった評価である $\||\nabla|^s u(t)\|_{\widehat{B}^0_{p,1}} = O(t^{-\frac{d}{2p'}-\frac{s}{2}})$ $(t\to\infty)$ を得る. □

References

[1] Bae, H., *Existence and analyticity of Lei-Lin solution to the Navier-Stokes equations*, Proc. Amer. Math. Soc., **143** (2015) 2887–2892.

[2] Bae, H., Biswas, A., Tadmor, E., *Analyticity and decay estimates of the Navier-Stokes equations in critical Besov spaces*, Arch. Ration. Mech. Anal., **205** (2012) 963–991.

[3] Bahouri, H., Chemin, J.-Y., Danchin, R., "*Fourier analysis and nonlinear partial differential equations*", vol. 343, Springer, Heidelberg, 2011, xvi+523 pp.

[4] Bourgain, J., Pavlović, N., *Ill-posedness of the Navier-Stokes equations in a critical space in 3D*, J. Funct. Anal., **255** (2008) 2233–2247.

[5] Cannone, M., Meyer, Y., Planchon, F., *Solutions auto-similaires des équations de Navier-Stokes. (French) [Self-similar solutions of Navier-Stokes equations] Séminaire sur les Équations aux Dérivées Partielles*, 1993–1994, Exp. No. VIII, 12 pp., École Polytech., Palaiseau, 1994.

[6] Cannone, M., Wu, G., *Global well-posedness for Navier-Stokes equations in critical Fourier-Herz spaces*, Nonlinear Anal., **75** (2012) 3754–3760.

[7] Charve, F., Danchin, R., Xu, J., *Gevrey analyticity and decay for the compressible Navier-Stokes system with capillarity*, Indiana Univ. Math. J., **70** (2021) 1903–1944.

[8] Chemin, J.-Y., Lerner, N., *Flot de champs de vecteurs non lipschitziens et équations de Navier–Stokes*, J. Differential Equations, **121** (1995) 314–328.
[9] Chikami, N., *On Gagliardo-Nirenberg type inequalities in Fourier-Herz spaces*, J. Funct. Anal., **275** (2018) 1138–1172.
[10] Foias, C., Temam, R., *Gevrey class regularity for the solutions of the Navier-Stokes equations*, J. Funct. Anal., **87** (1989) 359–369.
[11] Fujigaki, Y., Miyakawa, T., *Asymptotic profiles of nonstationary incompressible Navier-Stokes flows in the whole space*, SIAM J. Math. Anal., **33** (2001) 523–544.
[12] Fujita, H., Kato, T., *On the Navier-Stokes initial value problem. I*, Arch. Ration. Mech. Anal., **16** (1964) 269–315.
[13] Giga, Y., Inui, K., Mahalov, A., Saal, J., *Uniform global solvability of the rotating Navier-Stokes equations for nondecaying initial data*, Indiana Univ. Math. J., **57** (2008) 2775–2791.
[14] Grünrock, A., *An improved local well-posedness result for the modified KdV equation*, Int. Math. Res. Not., (2004) 3287–3308.
[15] Iwabuchi, T., *Global well-posedness for Keller-Segel system in Besov type spaces*, J. Math. Anal. Appl., **379** (2011) 930–948.
[16] Iwabuchi, T., Takada, R., *Global well-posedness and ill-posedness for the Navier-Stokes equations with the Coriolis force in function spaces of Besov type*, J. Funct. Anal., **267** (2014), 1321–1337.
[17] Kato, T., *Strong L^p-solutions of the Navier–Stokes equation in $\mathbb{R}^m$, with applications to weak solutions*, Math. Z., **187** (1984) 471–480.
[18] Koch, T., Tataru, D., *Well-posedness for the Navier-Stokes equations*, Adv. Math., **157** (2001) 22–35.
[19] Konieczny, P., Yoneda, T., *On dispersive effect of the Coriolis force for the stationary Navier-Stokes equations*, J. Differential Equations, **250** (2011) 3859–3873.
[20] Kozono, H., Yamazaki, M., *Semilinear heat equations and the Navier-Stokes equation with distributions in new function spaces as initial data*, Comm. Partial Differential Equations, **19** (1994) 959–1014.
[21] Lei, Z., Lin, F., *Global mild solutions of Navier-Stokes equations*, Comm. Pure Appl. Math., **64** (2011) 1297–1304.
[22] Lemari'e-Rieusset, P. G., "*Recent developments in the Navier-Stokes problem*", Chapman & Hall/CRC Res. Notes Math., vol. 431 Chapman & Hall/CRC, Boca Raton, 2002. xiv+395 pp.
[23] Masaki, S., Segata, J., *On the well-posedness of the generalized Korteweg-de Vries equation in scale-critical $\hat{L}^r$-space*, Anal. PDE, **9** (2016) 699–725.
[24] Matsui, T., Nakasato, R., Ogawa, T., *Singular limit for the magnetohydrodynamics of the damped wave type in the critical Fourier–Sobolev space*, J. Differential Equations, **271** (2021) 414–446.
[25] Miyakawa, T., *Hardy spaces of solenoidal vector fields, with applications to the Navier-Stokes equations*, Kyushu J. Math., **50** (1996) 1–64.
[26] Miyakawa, T., *Application of Hardy space techniques to the time-decay problem for incompressible Navier-Stokes flows in R^n*, Funkcial. Ekvac., **41** (1998) 383–434.
[27] Nakasato, R., *Global well-posedness for the incompressible Hall-magnetohydrodynamic system in critical Fourier–Besov spaces*, J. Evol. Equ., **22** (2022) 35 pp.
[28] Nakasato, R., *Global well-posedness for the Hall-magnetohydrodynamic system with quantum effects in a critical L^p framework*, https://dx.doi.org/10.2139/ssrn.4412954.
[29] Nakasato, R., *Analyticity and asymptotic behavior of solutions to the Navier-Stokes equations in an end-point scaling critical framework*, preprint.
[30] Okabe, T., Tsutsui, Y., *Navier-Stokes flow in the weighted Hardy space with applications to time decay problem*, J. Differential Equations, **261** (2016) 1712–1755.
[31] Oliver, M., Titi, Edriss S., *Remark on the rate of decay of higher order derivatives for solutions to the Navier-Stokes equations in $\mathbf{R}^n$*, J. Funct. Anal., **172** (2000) 1–18.
[32] Song, Z., Xu, J., *Global existence and analyticity of L^p solutions to the compressible fluid model of Korteweg type*, J. Differential Equations, **370** (2023) 101–139.
[33] Tsutsui, Y., *An application of weighted Hardy spaces to the Navier-Stokes equations*, J. Funct. Anal., **266** (2014) 1395–1420.
[34] Wang, B., *Ill-posedness for the Navier-Stokes equations in critical Besov spaces $\dot{B}^{-1}_{\infty,q}$*, Adv. Math., **268** (2015) 350–372.
[35] Yoneda, T., *Ill-posedness of the 3D-Navier-Stokes equations in a generalized Besov space near* BMO^{-1}, J. Funct. Anal., **258** (2010) 3376–3387.

FIXED POINT AND CONVERGENCE THEOREMS FOR MAPPINGS DETERMINED BY SEVERAL PARAMETERS

TOSHIHARU KAWASAKI

Abstract. In this paper, we introduce the following: Fixed point theorrm, mean convergence theorem, and weak convergence theorem for widely more generalized mappings in Hilbert spaces; Fixed point theorems in metric spaces; Acute point and skew-acute point in Banach spaces; Acute point theorem and skew-acute point theorem; Mean convergence theorems by using acute point and skew-acute point; Weak convergence theorems by using acute point and skew-acute point; Generalized acute point and generalized skew-acute point in Banach spaces; Generalized acute point theorem and generalized skew-acute point theorem; Mean convergence theorems by using generalized acute point and generalized skew-acute point; Weak convergence theorems by using generalized acute point and generalized skew-acute point.

1. Introduction

Let H be a real Hilbert space and let C be a nonempty subset of H. A mapping T from C into H is said to be generalized hybrid [24] if there exist $\alpha, \beta \in \mathbb{R}$ such that

$$\alpha\|Tx - Ty\|^2 + (1-\alpha)\|x - Ty\|^2 \leq \beta\|Tx - y\|^2 + (1-\beta)\|x - y\|^2$$

for any $x, y \in C$. Such a mapping is said to be (α, β)-generalized hybrid. The class of all generalized hybrid mappings is a new class of nonlinear mappings including nonexpansive mappings, nonspreading mappings [26] and hybrid mappings [28]. A mapping T from C into H is said to be nonexpansive if

$$\|Tx - Ty\| \leq \|x - y\|$$

for any $x, y \in C$; nonspreading if

$$2\|Tx - Ty\|^2 \leq \|Tx - y\|^2 + \|Ty - x\|^2$$

for any $x, y \in C$; hybrid if

$$3\|Tx - Ty\|^2 \leq \|x - y\|^2 + \|Tx - y\|^2 + \|Ty - x\|^2$$

for any $x, y \in C$. Any nonexpansive mapping is $(1, 0)$-generalized hybrid; any nonspreading mapping is $(2, 1)$-generalized hybrid; any hybrid mapping is $\left(\frac{3}{2}, \frac{1}{2}\right)$-generalized hybrid.

Motivated these mappings, in [21] Kawasaki and Takahashi introduced a new very wider class of mappings, called widely more generalized hybrid mappings,

2010 *Mathematics Subject Classification.* 47H10.

Key words and phrases. Fixef point theorem, Mean convergence theorem, Weak convergence theorem, Acute point, Skew-acute point, Generalized acute point, Generalized skew-acute point, Generalized pseudocontraction, Hilbert space, Banach space.

than the class of all generalized hybrid mappings. A mapping T from C into H is widely more generalized hybrid if there exist $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta \in \mathbb{R}$ such that

$$\begin{aligned}
&\alpha\|Tx - Ty\|^2 + \beta\|x - Ty\|^2 + \gamma\|Tx - y\|^2 + \delta\|x - y\|^2 \\
&\quad +\varepsilon\|x - Tx\|^2 + \zeta\|y - Ty\|^2 + \eta\|(x - Tx) - (y - Ty)\|^2 \\
&\leq 0
\end{aligned}$$

for any $x, y \in C$. Such a mapping is said to be $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid. This class includes the class of all generalized hybrid mappings and also the class of all k-pseudocontractions [3] for $k \in [0, 1]$. A mapping T from C into H is called a k-pseudocontraction if

$$\|Tx - Ty\|^2 \leq \|x - y\|^2 + k\|(x - Tx) - (y - Ty)\|^2$$

for any $x, y \in C$. Any (α, β)-generalized hybrid mapping is $(\alpha, 1 - \alpha, -\beta, \beta - 1, 0, 0, 0)$-widely more generalized hybrid; any k-pseudocontraction is $(1, 0, 0, -1, 0, 0, -k)$-widely more generalized hybrid. Furthermore, they proved some fixed point theorems [7–12, 20–23] and some mean convergence theorems [7, 8, 20–22].

There are some studies on Banach space related to these results. In [30] Takahashi, Wong and Yao introduced the generalized nonspreading mapping and the skew-generalized nonspreading mapping in a Banach space. Let E be a smooth Banach space and let C be a nonempty subset of E. A mapping T from C into E is said to be generalized nonspreading if there exist $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in \mathbb{R}$ such that

$$\begin{aligned}
&\alpha\phi(Tx, Ty) + \beta\phi(x, Ty) + \gamma\phi(Tx, y) + \delta\phi(x, y) \\
&\quad \leq \varepsilon(\phi(Ty, Tx) - \phi(Ty, x)) + \zeta(\phi(y, Tx) - \phi(y, x))
\end{aligned}$$

for any $x, y \in C$, where J is the duality mapping on E and

$$\phi(u, v) \stackrel{\text{def}}{=} \|u\|^2 - 2\langle u, Jv\rangle + \|v\|^2.$$

Such a mapping is said to be $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta)$-generalized nonspreading. A mapping T from C into E is said to be skew-generalized nonspreading if there exist $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in \mathbb{R}$ such that

$$\begin{aligned}
&\alpha\phi(Tx, Ty) + \beta\phi(x, Ty) + \gamma\phi(Tx, y) + \delta\phi(x, y) \\
&\quad \leq \varepsilon(\phi(Ty, Tx) - \phi(y, Tx)) + \zeta(\phi(Ty, x) - \phi(y, x))
\end{aligned}$$

for any $x, y \in C$. Such a mapping is said to be $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta)$-skew-generalized nonspreading. These classes include the class of generalized hybrid mappings in a Hilbert space, however, it does not include the class of widely more generalized hybrid mappings.

Motivated these results, we introduced a new class of mappings [13–15, 17] on Banach space corresponding to the class of all widely more generalized hybrid mappings on Hilbert space. Let E be a smooth Banach space and let C be a nonempty subset of E. A mapping T from C into E is called a generalized pseudocontraction if there exist $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2 \in \mathbb{R}$ such that

$$\begin{aligned}
&\alpha_1\phi(Tx, Ty) + \alpha_2\phi(Ty, Tx) + \beta_1\phi(x, Ty) + \beta_2\phi(Ty, x) \\
&\quad +\gamma_1\phi(Tx, y) + \gamma_2\phi(y, Tx) + \delta_1\phi(x, y) + \delta_2\phi(y, x) \\
&\quad +\varepsilon_1\phi(Tx, x) + \varepsilon_2\phi(x, Tx) + \zeta_1\phi(y, Ty) + \zeta_2\phi(Ty, y) \\
&\leq 0
\end{aligned}$$

for any $x, y \in C$. Such a mapping is called an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction.

On the other hand, in [29] Takahashi and Takeuchi introduced a concept of attractive point in a Hilbert space. Let H be a real Hilbert space, let C be a nonempty subset of H, and let T be a mapping from C into H. $x \in H$ is called an attractive point of T if

$$\|x - Ty\| \leq \|x - y\|$$

for any $y \in C$. Let

$$A(T) = \{x \in H \mid \|x - Ty\| \leq \|x - y\| \text{ for any } y \in C\}.$$

Furthermore, they proved that a mean convergence theorem of Baillon's type [2] for generalized hybrid mappings without convexity of C.

In [30] Takahashi, Wong and Yao introduced some extensions of attractive point and proved some attractive point theorems on Banach spaces. $x \in E$ is an attractive point of T if

$$\phi(x, Ty) \leq \phi(x, y)$$

for any $y \in C$; $x \in E$ is a skew-attractive point of T if

$$\phi(Ty, x) \leq \phi(y, x)$$

for any $y \in C$. Let

$$\begin{aligned} A(T) &= \{x \in E \mid \phi(x, Ty) \leq \phi(x, y) \text{ for any } y \in C\}; \\ B(T) &= \{x \in E \mid \phi(Ty, x) \leq \phi(y, x) \text{ for any } y \in C\}. \end{aligned}$$

In [1] Atsushiba, Iemoto, Kubota and Takeuchi introduced a concept of acute point as an extension of attractive point in a Hilbert space. Let H be a real Hilbert space, let C be a nonempty subset of H and let T be a mapping from C into H and $k \in [0, 1]$. $x \in H$ is called a k-acute point of T if

$$\|x - Ty\|^2 \leq \|x - y\|^2 + k\|y - Ty\|^2$$

for any $y \in C$. Let

$$\mathscr{A}_k(T) = \{x \in H \mid \|x - Ty\|^2 \leq \|x - y\|^2 + k\|y - Ty\|^2 \text{ for any } y \in C\}.$$

Furthermore, using a concept of acute point, they proved convergence theorems without convexity of C.

In this paper, we introduce the following:

(1) Fixed point theorrm, mean convergence theorem, and weak convergence theorem for widely more generalized mappings in Hilbert spaces;
(2) Fixed point theorems in metric spaces;
(3) Acute point and skew-acute point in Banach spaces;
(4) Acute point theorem and skew-acute point theorem;
(5) Mean convergence theorems by using acute point and skew-acute point;
(6) Weak convergence theorems by using acute point and skew-acute point;
(7) Generalized acute point and generalized skew-acute point in Banach spaces;
(8) Generalized acute point theorem and generalized skew-acute point theorem;
(9) Mean convergence theorems by using generalized acute point and generalized skew-acute point;
(10) Weak convergence theorems by using generalized acute point and generalized skew-acute point.

2. Fixed point theorems in Hilbert spaces [21]

Let H be a real Hilbert space and let C be a nonempty subset of H. A mapping T from C into H is said to be widely more generalized hybrid if there exist $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta \in \mathbb{R}$ such that

$$\begin{aligned}&\alpha\|Tx - Ty\|^2 + \beta\|x - Ty\|^2 + \gamma\|Tx - y\|^2 + \delta\|x - y\|^2 \\ &\quad + \varepsilon\|x - Tx\|^2 + \zeta\|y - Ty\|^2 + \eta\|(x - Tx) - (y - Ty)\|^2 \\ &\leq 0\end{aligned}$$

for any $x, y \in C$. Such a mapping T is called an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping. We first prove a fixed point theorem for widely more generalized hybrid mappings in Hilbert spaces.

Lemma 2.1. *Let H be a real Hilbert space, let C and D be non-empty subsets of H, let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping from C into D, and $\lambda \in [0, 1]$ Then T is an $(\alpha, (1-\lambda)\beta + \lambda\gamma, \lambda\beta + (1-\lambda)\gamma, \delta, (1-\lambda)\varepsilon + \lambda\zeta, \lambda\varepsilon + (1-\lambda)\zeta, \eta)$-widely more generalized hybrid mapping from C into D.*

Theorem 2.1. *Let H be a real Hilbert space, let C be a non-empty, closed, and convex subset of H, and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping from C into itself. Suppose that there exists $\lambda \in [0, 1]$ such that*

(1) $\alpha + \beta + \gamma + \delta \geq 0$;

(2) $(1-\lambda)\varepsilon + \lambda\zeta + \eta \geq 0$;

(3) $\alpha + (1-\lambda)(\beta + \zeta) + \lambda(\gamma + \varepsilon) + \eta > 0$.

Then T has a fixed point if and only if there exists $z \in C$ such that $\{T^n z \mid n = 0, 1, \ldots\}$ is bounded. In particular, a fixed point of T is unique in the case of $\alpha + \beta + \gamma + \delta > 0$.

By Theorem 2.1 the following are derived.

Theorem 2.2 (The Banach contraction principle)**.** *Let H be a real Hilbert space and let T be a contractive mapping from H into H, that is, there exists a real number α with $\alpha \in (0, 1)$ such that*

$$\|Tx - Ty\| \leq \alpha\|x - y\|$$

for any $x, y \in H$. Then T has a unique fixed point.

Theorem 2.3 (Kocourek, Takahashi and Yao [24])**.** *Let H be a real Hilbert space, let C be a non-empty, closed, and convex subset of H, and let T be a generalized hybrid mapping from C into itself, that is, there exist real numbers α and β such that*

$$\alpha\|Tx - Ty\|^2 + (1-\alpha)\|x - Ty\|^2 \leq \beta\|Tx - y\|^2 + (1-\beta)\|x - y\|^2$$

for any $x, y \in C$. Then T has a fixed point if and only if there exists $z \in C$ such that $\{T^n z \mid n = 0, 1, \ldots\}$ is bounded.

Theorem 2.4. *Let H be a real Hilbert space, let C be a non-empty, bounded, and closed convex subset of H, and let T be a strongly pseudocontractive mapping from C into itself, that is, there exists a real number k with $k \in [0, 1)$ such that*

$$\|Tx - Ty\|^2 \leq \|x - y\|^2 + k\|(x - Tx) - (y - Ty)\|^2$$

for any $x, y \in H$. Then T has a fixed point if and only if there exists $z \in C$ such that $\{T^n z \mid n = 0, 1, \ldots\}$ is bounded.

3. Mean convergence theorem in Hilbert spaces [21]

In this section, we consider a mean convergence theorem of Baillon's type in Hilbert spaces. We need the following lemmas.

Lemma 3.1. *Let H be a real Hilbert space, let C be a non-empty, closed, and convex subset of H and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping from C into itself. Suppose that T has a fixed point and there exists $\lambda \in [0, 1]$ such that*
(3) $\quad \alpha + (1 - \lambda)(\beta + \zeta) + \lambda(\gamma + \varepsilon) + \eta > 0.$
Then the set of fixed points of T is closed.

Lemma 3.2. *Let H be a real Hilbert space, let C be a non-empty, closed, and convex subset of H and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping from C into itself. Suppose that T has a fixed point and there exists $\lambda \in [0, 1]$ such that*
(1) $\quad \alpha + \beta + \gamma + \delta \geq 0;$
(3) $\quad \alpha + (1 - \lambda)(\beta + \zeta) + \lambda(\gamma + \varepsilon) + \eta > 0.$
Then the set of fixed points of T is convex.

Lemma 3.3. *Let H be a real Hilbert space, let C be a non-empty, closed, and convex subset of H and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping from C into itself. Suppose that T has a fixed point and there exists $\lambda \in [0, 1]$ such that*
(1) $\quad \alpha + \beta + \gamma + \delta \geq 0;$
(2) $\quad (1 - \lambda)\varepsilon + \lambda\zeta + \eta \geq 0;$
(4) $\quad \alpha + \lambda\beta + (1 - \lambda)\gamma > 0.$
Then T is quasi-nonexpansive.

Theorem 3.1. *Let H be a real Hilbert space, let C be a non-empty, closed, and convex subset of H and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping from C into itself. Suppose that T has a fixed point and there exists $\lambda \in [0, 1]$ such*
(1) $\quad \alpha + \beta + \gamma + \delta \geq 0;$
(2) $\quad (1 - \lambda)\varepsilon + \lambda\zeta + \eta \geq 0;$
(3) $\quad \alpha + (1 - \lambda)(\beta + \zeta) + \lambda(\gamma + \varepsilon) + \eta > 0;$
(4) $\quad \alpha + \lambda\beta + (1 - \lambda)\gamma > 0.$
Then for any $x \in C$,

$$S_n x \overset{def}{=} \frac{1}{n} \sum_{k=0}^{n-1} T^k x$$

is weakly convergent to a fixed point p of T, where P is the metric projection of H onto the set of all fixed points of T and $p = \lim_{n\to\infty} PT^n x$.

4. Weak convergence theorem in Hilbert spaces

In this section, we consider a weak convergence theorem in a Hilbert space.

Theorem 4.1. *Let H be a real Hilbert space, let C be a non-empty, closed, and convex subset of H and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta)$-widely more generalized hybrid mapping from C into itself. Suppose that T has a fixed point and there exists $\lambda \in [0, 1]$ such*

(1) $\alpha+\beta+\gamma+\delta \geq 0$;
(2) $(1-\lambda)\varepsilon+\lambda\zeta+\eta \geq 0$;
(3) $\alpha+(1-\lambda)(\beta+\zeta)+\lambda(\gamma+\varepsilon)+\eta > 0$;
(4) $\alpha+\lambda\beta+(1-\lambda)\gamma > 0$.
Let $\{\alpha_n$ *be a sequence of real numbers with* $\alpha_n \in (0,1)$ *and* $\liminf_{n\to\infty} \alpha_n(1-\alpha_n) > 0$. *Then a sequence generated by* $x_1 = x \in C$ *and*

$$x_{n+1} = \alpha_n x_n + (1-\alpha_n)Tx_n$$

for any $n \in \mathbb{N}$ *is weakly convergent to a fixed point* p *of* T*, where* P *is the metric projection of* H *onto the set of all fixed points of* T *and* $p = \lim_{n\to\infty} PT^n x$.

5. Fixed point theorems in metric spaces [10,12]

Let (X,d) be a metric space. A mapping T from X into itself is said to be widely more generalized hybrid if there exist real numbers $\alpha,\beta,\gamma,\delta,\varepsilon$ and ζ such that

$$\begin{aligned}\alpha d(Tx,Ty)^2 + \beta d(x,Ty)^2 + \gamma d(Tx,y)^2 + \delta d(x,y)^2 \\ +\varepsilon d(x,Tx)^2 + \zeta d(y,Ty)^2 \\ \leq 0\end{aligned}$$

for any $x,y \in X$. Such a mapping is called an $(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta)$-widely more generalized hybrid mapping.

Lemma 5.1. *Let* (X,d) *be a metric space, let* T *be an* $(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta)$*-widely more generalized hybrid mapping from* X *into itself, and* $\lambda \in [0,1]$ *Then* T *is an* $(\alpha,(1-\lambda)\beta+\lambda\gamma,\lambda\beta+(1-\lambda)\gamma,\delta,(1-\lambda)\varepsilon+\lambda\zeta,\lambda\varepsilon+(1-\lambda)\zeta)$*-widely more generalized hybrid mapping from* X *into itself.*

Lemma 5.2. *Let* X *be a metric space and let* T *be an* $(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta)$*-widely more generalized hybrid mapping from* X *into itself. Suppose that there exists* $\lambda \in [0,1]$ *such that*
(1) $\alpha+(1-\lambda)\varepsilon+\lambda\zeta+2\min\{\lambda\beta+(1-\lambda)\gamma,0\} \geq 0$;
(2) $\alpha+\delta+\varepsilon+\zeta+4\min\{\lambda\beta+(1-\lambda)\gamma,0\} > 0$.
Then $\{T^n x \mid n \in \mathbb{N}\cup\{0\}\}$ *is a Cauchy sequence for any* $x \in X$.

By Lemma 5.2, we obtain directly the following theorem.

Theorem 5.1. *Let* X *be a complete metric space and let* T *be an* $(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta)$*-widely more generalized hybrid mapping from* X *into itself. Suppose that there exists* $\lambda \in [0,1]$ *such that*
(1) $\alpha+(1-\lambda)\varepsilon+\lambda\zeta+2\min\{\lambda\beta+(1-\lambda)\gamma,0\} \geq 0$;
(2) $\alpha+\delta+\varepsilon+\zeta+4\min\{\lambda\beta+(1-\lambda)\gamma,0\} > 0$.
Then for any $x \in X$ *there exists* $\lim_{n\to\infty} T^n x$.

By Theorem 5.1, we obtain the following theorem.

Theorem 5.2. *Let* X *be a complete metric space and let* T *be an* $(\alpha,\beta,\gamma,\delta,\varepsilon,\zeta)$*-widely more generalized hybrid mapping from* X *into itself. Suppose that therre exists* $\lambda \in [0,1]$ *such that*
(1) $\alpha+(1-\lambda)\varepsilon+\lambda\zeta+2\min\{\lambda\beta+(1-\lambda)\gamma,0\} \geq 0$;
(2) $\alpha+\delta+\varepsilon+\zeta+4\min\{\lambda\beta+(1-\lambda)\gamma,0\} > 0$;
(3) $\alpha+(1-\lambda)(\beta+\zeta)+\lambda(\gamma+\varepsilon) > 0$.
Then T *has a fixed point* u*, where* $u = \lim_{n\to\infty} T^n x$ *for any* $x \in X$*. Additionally, if* $\alpha+\beta+\gamma+\delta > 0$*, then* T *has a unique fixed point.*

We obtain the another type theorem also.

Lemma 5.3. *Let (X, d) be a metric space and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta)$-widely more generalized hybrid mapping from X into itself. Suppose that therre exists $\lambda \in [0, 1]$ such that*
(1) $\alpha + (1-\lambda)\varepsilon + \lambda\zeta + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} > 0.$
Then

$$d(T^2x, Tx) \leq \sqrt{A}d(Tx, x)$$

holds for any $x \in X$, where

$$A = \max\left\{-\frac{\delta + \lambda\varepsilon + (1-\lambda)\zeta + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\}}{\alpha + (1-\lambda)\varepsilon + \lambda\zeta + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\}}, 0\right\}.$$

Lemma 5.4. *Let (X, d) be a metric space and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta)$-widely more generalized hybrid mapping from X into itself. Suppose that therre exists $\lambda \in [0, 1]$ such that*
(1) $\alpha + (1-\lambda)\varepsilon + \lambda\zeta + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} > 0;$
(2) $\alpha + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} > 0.$
Then

$$d(T^3x, Tx) \leq \sqrt{B}d(Tx, x)$$

holds for any $x \in X$, where

$$\begin{aligned} B \quad = \quad & \max\left\{\max\left\{-\frac{(1-\lambda)\varepsilon + \lambda\zeta}{\alpha + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\}}, 0\right\} A^2\right. \\ & + \max\left\{-\frac{(1-\lambda)\beta + \lambda\gamma + 2\min\{\delta, 0\}}{\alpha + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\}}, 0\right\} A \\ & \left. - \frac{\lambda\varepsilon + (1-\lambda)\zeta + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} + 2\min\{\delta, 0\}}{\alpha + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\}}, 0\right\}. \end{aligned}$$

Lemma 5.5. *Let (X, d) be a metric space and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta)$-widely more generalized hybrid mapping from X into itself. Suppose that therre exists $\lambda \in [0, 1]$ such that*
(1) $\alpha + (1-\lambda)\varepsilon + \lambda\zeta + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} > 0;$
(2) $\alpha + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} > 0.$
Then

$$d(T^3x, T^2x) \leq \sqrt{C}d(Tx, x)$$

holds for any $x \in C$, where

$$C \quad = \quad \max\left\{-\frac{\lambda\beta + (1-\lambda)\gamma}{\alpha + (1-\lambda)\varepsilon + \lambda\zeta}, 0\right\} B + \max\left\{-\frac{\delta + \lambda\varepsilon + (1-\lambda)\zeta}{\alpha + (1-\lambda)\varepsilon + \lambda\zeta}, 0\right\} A.$$

By Lemma 5.5, we obtain the following theorem.

Theorem 5.3. *Let (X, d) be a complete metric space and let T be an $(\alpha, \beta, \gamma, \delta, \varepsilon, \zeta)$-widely more generalized hybrid mapping from X into itself. Suppose that therre exists $\lambda \in [0, 1]$ such that*
(1) $\alpha + (1-\lambda)\varepsilon + \lambda\zeta + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} > 0;$
(2) $\alpha + 2\min\{\lambda\beta + (1-\lambda)\gamma, 0\} > 0;$
(3) $C < 1.$
Then T has a fixed point u, where $u = \lim_{n\to\infty} T^n x$ for any $x \in X$. Additionally, if $\alpha + \beta + \gamma + \delta > 0$, then T has a unique fixed point.

6. Fixed point theorems in Banach spaces [13, 17]

Let E be a smooth Banach space and let C be a nonempty subset of E. A mapping T from C into E is called a generalized pseudocontraction if there exist $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2 \in \mathbb{R}$ such that

$$\begin{aligned}
&\alpha_1\phi(Tx,Ty) + \alpha_2\phi(Ty,Tx) + \beta_1\phi(x,Ty) + \beta_2\phi(Ty,x)\\
&\quad +\gamma_1\phi(Tx,y) + \gamma_2\phi(y,Tx) + \delta_1\phi(x,y) + \delta_2\phi(y,x)\\
&\quad +\varepsilon_1\phi(Tx,x) + \varepsilon_2\phi(x,Tx) + \zeta_1\phi(y,Ty) + \zeta_2\phi(Ty,y)\\
&\le 0
\end{aligned}$$

for any $x, y \in C$. Such a mapping is called an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction.

Lemma 6.1. *Let E be a smooth Banach space, let C and D be nonempty subsets of E, let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into D and let $\lambda \in [0,1]$. Then T is a $((1-\lambda)\alpha_1 + \lambda\alpha_2), \lambda\alpha_1 + (1-\lambda)\alpha_2, (1-\lambda)\beta_1 + \lambda\gamma_2, \lambda\gamma_1 + (1-\lambda)\beta_2, (1-\lambda)\gamma_1 + \lambda\beta_2, \lambda\beta_1 + (1-\lambda)\gamma_2, (1-\lambda)\delta_1 + \lambda\delta_2, \lambda\delta_1 + (1-\lambda)\delta_2, (1-\lambda)\varepsilon_1 + \lambda\zeta_2, \lambda\zeta_1 + (1-\lambda)\varepsilon_2, (1-\lambda)\zeta_1 + \lambda\varepsilon_2, \lambda\varepsilon_1 + (1-\lambda)\zeta_2)$-generalized pseudocontraction from C into D.*

Theorem 6.1. *Let E be a strictly convex, reflexive, and smooth Banach space, let C be a nonempty, closed, and convex subset of E, and let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda \in [0,1]$ such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1) + \lambda(\alpha_2+\beta_2+\gamma_2+\delta_2) \ge 0;\\
&\lambda(\alpha_1+\gamma_1) + (1-\lambda)(\alpha_2+\beta_2) \ge 0;\\
&\lambda(\beta_1+\delta_1) + (1-\lambda)(\gamma_2+\delta_2) \ge 0;\\
&(1-\lambda)\varepsilon_1 + \lambda\zeta_2 \ge 0;\\
&\lambda\zeta_1 + (1-\lambda)\varepsilon_2 \ge 0
\end{aligned}$$

and suppose that one of the following holds:
(1) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1) + \lambda(\alpha_2+\gamma_2+\varepsilon_2) > 0$ *and* $\lambda\varepsilon_1 + (1-\lambda)\zeta_2 \ge 0$*;*
(2) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1) + \lambda(\alpha_2+\gamma_2+\varepsilon_2) \ge 0$ *and* $\lambda\varepsilon_1 + (1-\lambda)\zeta_2 > 0$.
Then T has a fixed point if and only if there exists $z \in C$ such that $\{T^n z \mid n \in \mathbb{N}\cup\{0\}\}$ is bounded.

Furthermore, if $(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1) + \lambda(\alpha_2+\beta_2+\gamma_2+\delta_2) > 0$ or $\lambda(\alpha_1+\beta_1+\gamma_1+\delta_1) + (1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2) > 0$, then the fixed point is unique.

Theorem 6.2. *Let E be a strictly convex, reflexive, and smooth Banach space, let C be a nonempty subset of E satisfying $J(C)$ is closed and convex, and let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda \in [0,1]$ such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2) + \lambda(\alpha_1+\beta_1+\gamma_1+\delta_1) \ge 0;\\
&\lambda(\alpha_2+\gamma_2) + (1-\lambda)(\alpha_1+\beta_1) \ge 0;\\
&\lambda(\beta_2+\delta_2) + (1-\lambda)(\gamma_1+\delta_1) \ge 0;\\
&(1-\lambda)\varepsilon_2 + \lambda\zeta_1 \ge 0;\\
&\lambda\zeta_2 + (1-\lambda)\varepsilon_1 \ge 0
\end{aligned}$$

and suppose that one of the following holds:

(1) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1)>0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1\geq 0$*;*
(2) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1)\geq 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1>0$.

Then T has a fixed point if and only if there exists $z\in C$ such that $\{T^nz \mid n\in\mathbb{N}\cup\{0\}\}$ is bounded.

Furthermore, if $(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2)+\lambda(\alpha_1+\beta_1+\gamma_1+\delta_1)>0$ or $\lambda(\alpha_2+\beta_2+\gamma_2+\delta_2)+(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1)>0$, then the fixed point is unique.

7. Acute point and skew-acute point [13]

Let E be a smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E and let $k,\ell\in\mathbb{R}$. $x\in E$ is called a (k,ℓ)-acute point of T if

$$\phi(x,Ty)\leq\phi(x,y)+k\phi(y,Ty)+\ell\phi(Ty,y)$$

for any $y\in C$. $x\in E$ is called a (k,ℓ)-skew-acute point of T if

$$\phi(Ty,x)\leq\phi(y,x)+k\phi(y,Ty)+\ell\phi(Ty,y)$$

for any $y\in C$. Let

$$\begin{aligned}\mathscr{A}_{k,\ell}(T)&=\{x\in E\mid\phi(x,Ty)\leq\phi(x,y)+k\phi(y,Ty)+\ell\phi(Ty,y)\text{ for any }y\in C\};\\ \mathscr{B}_{k,\ell}(T)&=\{x\in E\mid\phi(Ty,x)\leq\phi(y,x)+k\phi(y,Ty)+\ell\phi(Ty,y)\text{ for any }y\in C\}.\end{aligned}$$

It is obvious that

$$\mathscr{A}_{k_1,\ell_1}(T)\subset\mathscr{A}_{k_2,\ell_2}(T),\ \mathscr{B}_{k_1,\ell_1}(T)\subset\mathscr{B}_{k_2,\ell_2}(T)$$

for any $k_1,k_2,\ell_1,\ell_2\in\mathbb{R}$ with $k_1\leq k_2$ and $\ell_1\leq\ell_2$.

The following lemmas are important property characterizing them.

Lemma 7.1. *Let E be a smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E and let $k,\ell\in\mathbb{R}$. Then $\mathscr{A}_{k,\ell}(T)$ is closed and convex.*

Lemma 7.2. *Let E be a smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E and let $k,\ell\in\mathbb{R}$. Then $\mathscr{B}_{k,\ell}(T)$ is closed.*

Lemma 7.3. *Let E be a strictly convex and smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E and let $k,\ell\in\mathbb{R}$. Then the following hold:*

(1) *If $(k,\ell)\in(-\infty,1]\times(-\infty,0]\setminus\{(1,0)\}$, then $C\cap\mathscr{A}_{k,\ell}(T)$ is included in the set of all fixed points of T;*
(2) *If $(k,\ell)\in(-\infty,0]\times(-\infty,1]\setminus\{(0,1)\}$, then $C\cap\mathscr{B}_{k,\ell}(T)$ is included in the set of all fixed points of T.*

8. Acute point theorem and skew-acute point theorem [13, 17]

Theorem 8.1. *Let E be a reflexive and smooth Banach space, let C be a nonempty subset of E, and let T be an $(\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2,\zeta_1,\zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $z\in C$ such that $\{T^nz\mid n\in\mathbb{N}\cup\{0\}\}$ is bounded and suppose that there exists $\lambda\in[0,1]$ such that*

$$\begin{aligned}&(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1)+\lambda(\alpha_2+\beta_2+\gamma_2+\delta_2)\geq 0;\\ &\lambda(\alpha_1+\gamma_1)+(1-\lambda)(\alpha_2+\beta_2)\geq 0;\\ &\lambda(\beta_1+\delta_1)+(1-\lambda)(\gamma_2+\delta_2)\geq 0;\\ &(1-\lambda)\varepsilon_1+\lambda\zeta_2\geq 0;\\ &\lambda\zeta_1+(1-\lambda)\varepsilon_2\geq 0;\end{aligned}$$

$$(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)>0.$$

Then there exists a $\left(-\frac{(1-\lambda)\zeta_1+\lambda\varepsilon_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}, -\frac{\lambda\varepsilon_1+(1-\lambda)\zeta_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}\right)$*-acute point.*

Theorem 8.2. *Let* E *be a strictly convex, reflexive and smooth Banach space, let* C *be a nonempty subset of* E*, and let* T *be an* $(\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2,\zeta_1,\zeta_2)$*-generalized pseudocontraction from* C *into itself. Suppose that there exists* $z\in C$ *such that* $\{T^nz \mid n\in\mathbb{N}\cup\{0\}\}$ *is bounded and suppose that there exists* $\lambda\in[0,1]$ *such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2)+\lambda(\alpha_1+\beta_1+\gamma_1+\delta_1)\geq 0;\\
&\lambda(\alpha_2+\gamma_2)+(1-\lambda)(\alpha_1+\beta_1)\geq 0;\\
&\lambda(\beta_2+\delta_2)+(1-\lambda)(\gamma_1+\delta_1)\geq 0;\\
&(1-\lambda)\varepsilon_2+\lambda\zeta_1\geq 0;\\
&\lambda\zeta_2+(1-\lambda)\varepsilon_1\geq 0;\\
&(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)>0.
\end{aligned}$$

Then there exists a $\left(-\frac{(1-\lambda)\zeta_2+\lambda\varepsilon_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}, -\frac{\lambda\varepsilon_2+(1-\lambda)\zeta_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}\right)$*-skew acute point.*

9. Mean convergence theorems (acute point version) [14]

Theorem 9.1. *Let* E *be a uniformly convex Banach space with a Fréchet differentiable norm, let* C *be a nonempty subset of* E*, and let* T *be an* $(\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2,\zeta_1,\zeta_2)$*-generalized pseudocontraction from* C *into itself. Suppose that there exists* $\lambda\in[0,1]$ *such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1)+\lambda(\alpha_2+\beta_2+\gamma_2+\delta_2)\geq 0;\\
&\lambda(\alpha_1+\gamma_1)+(1-\lambda)(\alpha_2+\beta_2)\geq 0;\\
&\lambda(\beta_1+\delta_1)+(1-\lambda)(\gamma_2+\delta_2)\geq 0;\\
&(1-\lambda)\varepsilon_1+\lambda\zeta_2\geq 0;\\
&\lambda\zeta_1+(1-\lambda)\varepsilon_2\geq 0;\\
&(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)>0,
\end{aligned}$$

and suppose that

$$\mathscr{A}_{-\frac{(1-\lambda)\zeta_1+\lambda\varepsilon_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}, -\frac{\lambda\varepsilon_1+(1-\lambda)\zeta_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}}(T)\subset B(T)\neq\emptyset.$$

Let R *be the sunny generalized nonexpansive retraction of* E *onto* $B(T)$*. Then for any* $x\in C$*,*

$$S_nx\overset{def}{=}\frac{1}{n}\sum_{k=0}^{n-1}T^kx$$

is weakly convergent to an element

$$q\in\mathscr{A}_{-\frac{(1-\lambda)\zeta_1+\lambda\varepsilon_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}, -\frac{\lambda\varepsilon_1+(1-\lambda)\zeta_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}}(T),$$

where $q=\lim_{n\to\infty}RT^nx$*.*

Additionally, if C *is closed and convex and one of the following holds:*

(1) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2)>0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2\geq 0$*;*

(2) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2)\geq 0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2>0$*,*

then q is a fixed point of T.

Theorem 9.2. *Let E be a strictly convex and reflexive Banach space with Kadec-Klee property and a uniformly Fréchet differentiable norm, let C be a nonempty subset of E, and let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda \in [0,1]$ such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2)+\lambda(\alpha_1+\beta_1+\gamma_1+\delta_1) \geq 0;\\
&\lambda(\alpha_2+\gamma_2)+(1-\lambda)(\alpha_1+\beta_1) \geq 0;\\
&\lambda(\beta_2+\delta_2)+(1-\lambda)(\gamma_1+\delta_1) \geq 0;\\
&(1-\lambda)\varepsilon_2+\lambda\zeta_1 \geq 0;\\
&\lambda\zeta_2+(1-\lambda)\varepsilon_1 \geq 0;\\
&(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1) > 0,
\end{aligned}$$

suppose that

$$\mathscr{B}_{-\frac{\lambda\varepsilon_2+(1-\lambda)\zeta_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)},-\frac{(1-\lambda)\zeta_2+\lambda\varepsilon_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}}(T) \subset A(T) \neq \emptyset$$

and suppose that J^{-1} is weakly sequentially continuous. Let R^* be the sunny generalized nonexpansive retraction of E^* onto $J(A(T))$. Then for any $x \in C$,

$$S_n x \stackrel{def}{=} J^{-1}\left(\frac{1}{n}\sum_{k=0}^{n-1} JT^k x\right)$$

is weakly convergent to an element

$$q \in \mathscr{B}_{-\frac{\lambda\varepsilon_2+(1-\lambda)\zeta_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)},-\frac{(1-\lambda)\zeta_2+\lambda\varepsilon_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}}(T),$$

where $q = \lim_{n\to\infty} J^{-1}R^*JT^n x$.

Additionally, if $J(C)$ is closed and convexx and one of the following holds:

(1) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1) > 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1 \geq 0$*;*

(2) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1) \geq 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1 > 0$*,*

then q is a fixed point of T.

10. Weak convergence theorems (acute point version) [15]

Theorem 10.1. *Let E be a uniformly convex Banach space with a uniformly Fréchet differentiable norm, let C be a nonempty convex subset of E, and let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda \in [0,1]$ such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1)+\lambda(\alpha_2+\beta_2+\gamma_2+\delta_2) \geq 0;\\
&\lambda(\alpha_1+\gamma_1)+(1-\lambda)(\alpha_2+\beta_2) \geq 0;\\
&\lambda(\beta_1+\delta_1)+(1-\lambda)(\gamma_2+\delta_2) \geq 0;\\
&(1-\lambda)\varepsilon_1+\lambda\zeta_2 \geq 0;\\
&\lambda\zeta_1+(1-\lambda)\varepsilon_2 \geq 0;\\
&(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2) > 0,
\end{aligned}$$

and suppose that

$$\mathscr{A}_{-\frac{(1-\lambda)\zeta_1+\lambda\varepsilon_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)},-\frac{\lambda\varepsilon_1+(1-\lambda)\zeta_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}}(T) \subset B(T) \neq \emptyset.$$

Let R be the sunny generalized nonexpansive retraction of E onto $B(T)$ and let $\{\alpha_n\}$ be a sequence of real numbers with $\alpha_n \in (0,1)$ and $\liminf_{n\to\infty} \alpha_n(1-\alpha_n) > 0$. Then a sequence $\{x_n\}$ generated by $x_1 = x \in C$ and

$$x_{n+1} = \alpha_n x_n + (1-\alpha_n)Tx_n$$

for any $n \in \mathbb{N}$ is weakly convergent to an element

$$q \in \mathscr{A}_{-\frac{(1-\lambda)\zeta_1+\lambda\varepsilon_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)},-\frac{\lambda\varepsilon_1+(1-\lambda)\zeta_2}{(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}}(T),$$

where $q = \lim_{n\to\infty} Rx_n$.

Additionally, if C is closed and one of the following holds:

(1) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2) > 0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2 \geq 0$*;*

(2) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2) \geq 0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2 > 0$*,*

then q is a fixed point of T.

Theorem 10.2. *Let E be a uniformly convex Banach space with a uniformly Fréchet differentiable norm, let C be a nonempty subset of E satisfying $J(C)$ is convex, and let T be an $(\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2,\zeta_1,\zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda \in [0,1]$ such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2)+\lambda(\alpha_1+\beta_1+\gamma_1+\delta_1) \geq 0;\\
&\lambda(\alpha_2+\gamma_2)+(1-\lambda)(\alpha_1+\beta_1) \geq 0;\\
&\lambda(\beta_2+\delta_2)+(1-\lambda)(\gamma_1+\delta_1) \geq 0;\\
&(1-\lambda)\varepsilon_2+\lambda\zeta_1 \geq 0;\\
&\lambda\zeta_2+(1-\lambda)\varepsilon_1 \geq 0;\\
&(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1) > 0,
\end{aligned}$$

suppose that

$$\mathscr{B}_{-\frac{\lambda\varepsilon_2+(1-\lambda)\zeta_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)},-\frac{(1-\lambda)\zeta_2+\lambda\varepsilon_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}}(T) \subset A(T) \neq \emptyset$$

and suppose that J^{-1} is weakly sequentially continuous. Let R^* be the sunny generalized nonexpansive retraction of E^* onto $J(A(T))$ and let $\{\alpha_n\}$ be a sequence of real numbers with $\alpha_n \in (0,1)$ and $\liminf_{n\to\infty} \alpha_n(1-\alpha_n) > 0$. Then a sequence $\{x_n\}$ generated by $x_1 = x \in C$ and

$$x_{n+1} = J^{-1}(\alpha_n Jx_n + (1-\alpha_n)JTx_n)$$

for any $n \in \mathbb{N}$ is weakly convergent to an element

$$q \in \mathscr{B}_{-\frac{\lambda\varepsilon_2+(1-\lambda)\zeta_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)},-\frac{(1-\lambda)\zeta_2+\lambda\varepsilon_1}{(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}}(T),$$

where $q = \lim_{n\to\infty} J^{-1}R^*Jx_n$.

Additionally, if $J(C)$ is closed and one of the following holds:

(1) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1) > 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1 \geq 0$*;*

(2) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1) \geq 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1 > 0$*,*

then q is a fixed point of T.

11. Generalized acute point and generalized skew-acute point [16]

Let E be a smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E, and let $k, \ell, s \in \mathbb{R}$. $x \in E$ is called a (k,ℓ,s)-generalized acute point of T if

$$s(\phi(x,Ty)-\phi(x,y)) \leq k\phi(y,Ty)+\ell\phi(Ty,y)$$

for any $y \in C$. $x \in E$ is called a (k, ℓ, s)-generalized skew-acute point of T if

$$s(\phi(Ty, x) - \phi(y, x)) \leq k\phi(y, Ty) + \ell\phi(Ty, y)$$

for any $y \in C$. Let

$$\begin{aligned}\mathscr{A}_{k,\ell,s}(T) &= \{x \in E \mid s(\phi(x, Ty) - \phi(x, y)) \leq k\phi(y, Ty) + \ell\phi(Ty, y) \text{ for any } y \in C\};\\ \mathscr{B}_{k,\ell,s}(T) &= \{x \in E \mid s(\phi(Ty, x) - \phi(y, x)) \leq k\phi(y, Ty) + \ell\phi(Ty, y) \text{ for any } y \in C\}.\end{aligned}$$

It is obvious that

$$\mathscr{A}_{k_1,\ell_1,s_1}(T) \subset \mathscr{A}_{k_2,\ell_2,s_2}(T),\ \mathscr{B}_{k_1,\ell_1,s_2}(T) \subset \mathscr{B}_{k_2,\ell_2,s_2}(T)$$

for any $k_1, k_2, \ell_1, \ell_2 \in \mathbb{R}$ and for any $s_1, s_2 \in (0, \infty)$ with $\frac{k_1}{s_1} \leq \frac{k_2}{s_2}$ and $\frac{\ell_1}{s_1} \leq \frac{\ell_2}{s_2}$;

$$\mathscr{A}_{k_1,\ell_1,s_1}(T) \supset \mathscr{A}_{k_2,\ell_2,s_2}(T),\ \mathscr{B}_{k_1,\ell_1,s_2}(T) \supset \mathscr{B}_{k_2,\ell_2,s_2}(T)$$

for any $k_1, k_2, \ell_1, \ell_2 \in \mathbb{R}$ and for any $s_1, s_2 \in (-\infty, 0)$ with $\frac{k_1}{s_1} \leq \frac{k_2}{s_2}$ and $\frac{\ell_1}{s_1} \leq \frac{\ell_2}{s_2}$. Furthermore

$$\mathscr{A}_{k,\ell,0}(T) = \mathscr{B}_{k,\ell,0}(T) = E$$

for any $(k, \ell) \in [0, \infty) \times [0, \infty)$;

$$\mathscr{A}_{k,\ell,0}(T) = \mathscr{B}_{k,\ell,0}(T) = \emptyset$$

for any $(k, \ell) \in (-\infty, 0] \times (-\infty, 0] \setminus \{(0, 0)\}$; otherwise,

$$\mathscr{A}_{k,\ell,0}(T) = E \text{ or } \emptyset,\ \mathscr{B}_{k,\ell,0}(T) = E \text{ or } \emptyset;$$

however, it is generally unknown which case holds.

The following lemmas are important property characterizing them.

Lemma 11.1. *Let E be a smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E and let $k, \ell, s \in \mathbb{R}$. Then $\mathscr{A}_{k,\ell,s}(T)$ is closed and convex.*

Lemma 11.2. *Let E be a smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E and let $k, \ell, s \in \mathbb{R}$. Then $\mathscr{B}_{k,\ell,s}(T)$ is closed.*

Lemma 11.3. *Let E be a strictly convex and smooth Banach space, let C be a nonempty subset of E, let T be a mapping from C into E, and let $k, \ell, s \in \mathbb{R}$. Then the following hold:*

(1) *If $(k, \ell) \in (-\infty, s] \times (-\infty, 0] \setminus \{(s, 0)\}$, then $C \cap \mathscr{A}_{k,\ell,s}(T)$ is a subset of the set of all fixed points of T;*

(2) *If $(k, \ell) \in (-\infty, 0] \times (-\infty, s] \setminus \{(0, s)\}$, then $C \cap \mathscr{B}_{k,\ell,s}(T)$ is a subset of the set of all fixed points of T.*

12. Generalized acute point theorem and generalized skew-acute point thorem [16]

Theorem 12.1. *Let E be a reflexive and smooth Banach space, let C be a nonempty subset of E, and let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $z \in C$ such that $\{T^n z \mid n \in \mathbb{N} \cup \{0\}\}$ is bounded and suppose that there exists $\lambda \in [0, 1]$ such that*

$$\begin{aligned}&(1 - \lambda)(\alpha_1 + \beta_1 + \gamma_1 + \delta_1) + \lambda(\alpha_2 + \beta_2 + \gamma_2 + \delta_2) \geq 0;\\ &\lambda(\alpha_1 + \gamma_1) + (1 - \lambda)(\alpha_2 + \beta_2) \geq 0;\\ &\lambda(\beta_1 + \delta_1) + (1 - \lambda)(\gamma_2 + \delta_2) \geq 0;\end{aligned}$$

$$(1-\lambda)\varepsilon_1 + \lambda\zeta_2 \geq 0;$$
$$\lambda\zeta_1 + (1-\lambda)\varepsilon_2 \geq 0.$$

Then there exists a $(-((1-\lambda)\zeta_1+\lambda\varepsilon_2), -(\lambda\varepsilon_1+(1-\lambda)\zeta_2), (1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2))$*-generalized acute point.*

By Theorem 12.1 we can proove Theorem 6.1.

Theorem 12.2. *Let E be a strictly convex, reflexive, and smooth Banach space, let C be a nonempty subset of E, and let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $z \in C$ such that $\{T^n z \mid n \in \mathbb{N} \cup \{0\}\}$ is bounded and suppose that there exists $\lambda \in [0,1]$ such that*

$$(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2) + \lambda(\alpha_1+\beta_1+\gamma_1+\delta_1) \geq 0;$$
$$\lambda(\alpha_2+\gamma_2) + (1-\lambda)(\alpha_1+\beta_1) \geq 0;$$
$$\lambda(\beta_2+\delta_2) + (1-\lambda)(\gamma_1+\delta_1) \geq 0;$$
$$(1-\lambda)\varepsilon_2 + \lambda\zeta_1 \geq 0;$$
$$\lambda\zeta_2 + (1-\lambda)\varepsilon_1 \geq 0.$$

Then there exists a $(-(\lambda\varepsilon_2+(1-\lambda)\zeta_1), -((1-\lambda)\zeta_2+\lambda\varepsilon_1), (1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1))$*-generalized skew-acute point.*

By Theorem 12.2 we can proove Theorem 6.2.

13. Mean convergence theorems (generalized acute point version) [18]

Theorem 13.1. *Let E be a uniformly convex Banach space with a Fréchet differentiable norm, let C be a nonempty subset of E, and let T be an $(\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_2, \delta_1, \delta_2, \varepsilon_1, \varepsilon_2, \zeta_1, \zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda \in [0,1]$ such that*

$$(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1) + \lambda(\alpha_2+\beta_2+\gamma_2+\delta_2) \geq 0;$$
$$\lambda(\alpha_1+\gamma_1) + (1-\lambda)(\alpha_2+\beta_2) \geq 0;$$
$$\lambda(\beta_1+\delta_1) + (1-\lambda)(\gamma_2+\delta_2) \geq 0;$$
$$(1-\lambda)\varepsilon_1 + \lambda\zeta_2 \geq 0;$$
$$\lambda\zeta_1 + (1-\lambda)\varepsilon_2 \geq 0,$$

and suppose that

$$\mathscr{A}_{-((1-\lambda)\zeta_1+\lambda\varepsilon_2), -(\lambda\varepsilon_1+(1-\lambda)\zeta_2), (1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}(T) \subset B(T) \neq \emptyset.$$

Let R be the sunny generalized nonexpansive retraction of E onto $B(T)$. Then for any $x \in C$,

$$S_n x \stackrel{def}{=} \frac{1}{n}\sum_{k=0}^{n-1} T^k x$$

is weakly convergent to an element

$$q \in \mathscr{A}_{-((1-\lambda)\zeta_1+\lambda\varepsilon_2), -(\lambda\varepsilon_1+(1-\lambda)\zeta_2), (1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}(T),$$

where $q = \lim_{n\to\infty} RT^n x$.

Additionally, if C is closed and convex and one of the following holds:

(1) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2)>0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2\geq 0$*;*
(2) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2)\geq 0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2>0$*,*
then q is a fixed point of T.

Theorem 13.2. *Let E be a strictly convex and reflexive Banach space with Kadec-Klee property and a uniformly Fréchet differentiable norm, let C be a nonempty subset of E, and let T be an $(\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2,\zeta_1,\zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda\in[0,1]$ such that*

$$\begin{aligned}&(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2)+\lambda(\alpha_1+\beta_1+\gamma_1+\delta_1)\geq 0;\\&\lambda(\alpha_2+\gamma_2)+(1-\lambda)(\alpha_1+\beta_1)\geq 0;\\&\lambda(\beta_2+\delta_2)+(1-\lambda)(\gamma_1+\delta_1)\geq 0;\\&(1-\lambda)\varepsilon_2+\lambda\zeta_1\geq 0;\\&\lambda\zeta_2+(1-\lambda)\varepsilon_1\geq 0,\end{aligned}$$

suppose that

$$\mathscr{B}_{-(\lambda\varepsilon_2+(1-\lambda)\zeta_1),-((1-\lambda)\zeta_2+\lambda\varepsilon_1),(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}(T)\subset A(T)\neq\emptyset$$

and suppose that J^{-1} is weakly sequentially continuous. Let R^* be the sunny generalized nonexpansive retraction of E^* onto $J(A(T))$. Then for any $x\in C$,

$$S_nx\overset{def}{=}J^{-1}\left(\frac{1}{n}\sum_{k=0}^{n-1}JT^kx\right)$$

is weakly convergent to an element

$$q\in\mathscr{B}_{-(\lambda\varepsilon_2+(1-\lambda)\zeta_1),-((1-\lambda)\zeta_2+\lambda\varepsilon_1),(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}(T),$$

where $q=\lim_{n\to\infty}J^{-1}R^*JT^nx$.

Additionally, if $J(C)$ is closed and convexx and one of the following holds:
(1) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1)>0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1\geq 0$*;*
(2) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1)\geq 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1>0$*,*
then q is a fixed point of T.

14. Weak convergence theorems (generalized acute point version) [19]

Theorem 14.1. *Let E be a uniformly convex Banach space with a uniformly Fréchet differentiable norm, let C be a nonempty convex subset of E, and let T be an $(\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2,\zeta_1,\zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda\in[0,1]$ such that*

$$\begin{aligned}&(1-\lambda)(\alpha_1+\beta_1+\gamma_1+\delta_1)+\lambda(\alpha_2+\beta_2+\gamma_2+\delta_2)\geq 0;\\&\lambda(\alpha_1+\gamma_1)+(1-\lambda)(\alpha_2+\beta_2)\geq 0;\\&\lambda(\beta_1+\delta_1)+(1-\lambda)(\gamma_2+\delta_2)\geq 0;\\&(1-\lambda)\varepsilon_1+\lambda\zeta_2\geq 0;\\&\lambda\zeta_1+(1-\lambda)\varepsilon_2\geq 0,\end{aligned}$$

and suppose that

$$\mathscr{A}_{-((1-\lambda)\zeta_1+\lambda\varepsilon_2),-(\lambda\varepsilon_1+(1-\lambda)\zeta_2),(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}(T)\subset B(T)\neq\emptyset.$$

Let R be the sunny generalized nonexpansive retraction of E onto $B(T)$ and let $\{\alpha_n\}$ be a sequence of real numbers with $\alpha_n \in (0,1)$ and $\liminf_{n\to\infty} \alpha_n(1-\alpha_n) > 0$. Then a sequence $\{x_n\}$ generated by $x_1 = x \in C$ and

$$x_{n+1} = \alpha_n x_n + (1-\alpha_n)Tx_n$$

for any $n \in \mathbb{N}$ is weakly convergent to an element

$$q \in \mathscr{A}_{-((1-\lambda)\zeta_1+\lambda\varepsilon_2),-(\lambda\varepsilon_1+(1-\lambda)\zeta_2),(1-\lambda)(\alpha_1+\beta_1)+\lambda(\alpha_2+\gamma_2)}(T),$$

where $q = \lim_{n\to\infty} Rx_n$.

Additionally, if C is closed and one of the following holds:
(1) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2) > 0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2 \geq 0$*;*
(2) $(1-\lambda)(\alpha_1+\beta_1+\zeta_1)+\lambda(\alpha_2+\gamma_2+\varepsilon_2) \geq 0$ *and* $\lambda\varepsilon_1+(1-\lambda)\zeta_2 > 0$*,*
then q is a fixed point of T.

Theorem 14.2. *Let E be a uniformly convex Banach space with a uniformly Fréchet differentiable norm, let C be a nonempty subset of E satisfying $J(C)$ is convex, and let T be an $(\alpha_1,\alpha_2,\beta_1,\beta_2,\gamma_1,\gamma_2,\delta_1,\delta_2,\varepsilon_1,\varepsilon_2,\zeta_1,\zeta_2)$-generalized pseudocontraction from C into itself. Suppose that there exists $\lambda \in [0,1]$ such that*

$$\begin{aligned}
&(1-\lambda)(\alpha_2+\beta_2+\gamma_2+\delta_2)+\lambda(\alpha_1+\beta_1+\gamma_1+\delta_1) \geq 0;\\
&\lambda(\alpha_2+\gamma_2)+(1-\lambda)(\alpha_1+\beta_1) \geq 0;\\
&\lambda(\beta_2+\delta_2)+(1-\lambda)(\gamma_1+\delta_1) \geq 0;\\
&(1-\lambda)\varepsilon_2+\lambda\zeta_1 \geq 0;\\
&\lambda\zeta_2+(1-\lambda)\varepsilon_1 \geq 0,
\end{aligned}$$

suppose that

$$\mathscr{B}_{-(\lambda\varepsilon_2+(1-\lambda)\zeta_1),-((1-\lambda)\zeta_2+\lambda\varepsilon_1),(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}(T) \subset A(T) \neq \emptyset$$

and suppose that J^{-1} is weakly sequentially continuous. Let R^* be the sunny generalized nonexpansive retraction of E^* onto $J(A(T))$ and let $\{\alpha_n\}$ be a sequence of real numbers with $\alpha_n \in (0,1)$ and $\liminf_{n\to\infty} \alpha_n(1-\alpha_n) > 0$. Then a sequence $\{x_n\}$ generated by $x_1 = x \in C$ and

$$x_{n+1} = J^{-1}(\alpha_n Jx_n + (1-\alpha_n)JTx_n)$$

for any $n \in \mathbb{N}$ is weakly convergent to an element

$$q \in \mathscr{B}_{-(\lambda\varepsilon_2+(1-\lambda)\zeta_1),-((1-\lambda)\zeta_2+\lambda\varepsilon_1),(1-\lambda)(\alpha_2+\beta_2)+\lambda(\alpha_1+\gamma_1)}(T),$$

where $q = \lim_{n\to\infty} J^{-1}R^*Jx_n$.

Additionally, if $J(C)$ is closed and one of the following holds:
(1) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1) > 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1 \geq 0$*;*
(2) $(1-\lambda)(\alpha_2+\beta_2+\zeta_2)+\lambda(\alpha_1+\gamma_1+\varepsilon_1) \geq 0$ *and* $\lambda\varepsilon_2+(1-\lambda)\zeta_1 > 0$*,*
then q is a fixed point of T.

References

[1] S. Atsushiba, S. Iemoto, R. Kubota, and Y. Takeuchi, *Convergence theorems for some classes of nonlinear mappings in Hilbert spaces*, Linear and Nonlinear Analysis **2** (2016), 125–153.

[2] J.-B. Baillon, *Un théorème de type ergodique pour les contractions non linéaires dans un espace de Hilbert*, Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences. Séries A et B **280** (1975), 1511–1514.

[3] F. E. Browder and W. V. Petryshyn, *Construction of fixed points of nonlinear mappings in Hilbert space*, Journal of Mathematical Analysis and Applications **20** (1967), 197–228.

[4] D. Butnariu, A. N. Iusem, and E. Resmerita, *Total convexity for powers of the norm in uniformly convex Banach spaces*, Journal of Convex Analysis **7** (2000), 319–334.

[5] I. Ciorănescu, *Geometry of Banach Spaces, Duality Mappings and Nonlinear Problems*, Mathematics and its applications, vol. 62, Kluwer Academic Publishers, Dordrecht, 1990.

[6] T. Ibaraki and W. Takahashi, *A new projection and convergence theorems for the projections in Banach spaces*, J. Approx. Theory **149** (2007), 1–14.

[7] T. Kawasaki, *An extension of existence and mean approximation of fixed points of generalized hybrid non-self mappings in Hilbert spaces*, preprint.

[8] ———, *Fixed points theorems and mean convergence theorems for generalized hybrid self mappings and non-self mappings in Hilbert spaces*, Pacific Journal of Optimization **12** (2016), 133–150.

[9] ———, *Fixed point theorem for widely more generalized hybrid demicontinuous mappings in Hilbert spaces*, Proceedings of Nonlinear Analysis and Convex Analysis, Yokohama Publishers, Yokohama, to appear.

[10] ———, *Fixed point theorems for widely more generalized hybrid mappings in metric spaces, Banach spaces and Hilbert spaces*, Journal of Nonlinear and Convex Analysis **19** (2018), 1675–1683.

[11] ———, *On convergence of orbits to a fixed point for widely more generalized hybrid mappings*, Nihonkai Mathematical Journal **27** (2016), 89–97.

[12] ———, *Fixed point theorems for widely more generalized hybrid mappings in a metric space, a Banach space and a Hilbert space*, Proceedings of Nonlinear Analysis and Convex Analysis, Yokohama Publishers, Yokohama, to appear.

[13] ———, *Fixed point and acute point theorems for new mappings in a Banach space*, Journal of Mathematics **2019** (2019), 12 pages.

[14] ———, *Mean convergence theorems for new mappings in a Banach space*, Journal of Nonlinear and Variational Analysis **3** (2019), 61–78.

[15] ———, *Weak convergence theorems for new mappings in a Banach space*, Linear and Nonlinear Analysis **5** (2019), 147–171.

[16] ———, *Generalized acute point theorems for generalized pseudocontractions in a Banach space*, Linear and Nonlinear Analysis **6** (2020), 73–90.

[17] ———, *Fixed point and acute point theorems for generalized pseudocontractions in a Banach space*, Journal of Nonlinear and Convex Analysis **22** (2021), 1057–1075.

[18] ———, *Mean convergence theorems to generalized acute points for generalized pseudocontractions*, Advances in the Theory of Nonlinear Analysis and its Application **7** (2023), 387–404.

[19] ———, *Weak convergence theorems to generalized acute points for generalized pseudocontractions*, Advances in the Theory of Nonlinear Analysis and its Application, to appear.

[20] T. Kawasaki and T. Kobayashi, *Existence and mean approximation of fixed points of generalized hybrid non-self mappings in Hilbert spaces*, Scientiae Mathematicae Japonicae **77 (Online Version: e-2014)** (2014), 13–26 (Online Version: 29–42).

[21] T. Kawasaki and W. Takahashi, *Existence and mean approximation of fixed points of generalized hybrid mappings in Hilbert spaces*, Journal of Nonlinear and Convex Analysis **14** (2013), 71–87.

[22] ———, *Fixed point and nonlinear ergodic theorems for widely more generalized hybrid mappings in Hilbert spaces and applications*, Proceedings of Nonlinear Analysis and Convex Analysis, Yokohama Publishers, Yokohama, to appear.

[23] ———, *Fixed point theorems for generalized hybrid demicontinuous mappings in Hilbert spaces*, Linear and Nonlinear Analysis **1** (2015), 125–138.

[24] P. Kocourek, W. Takahashi, and J.-C. Yao, *Fixed point theorems and weak convergence theorems for generalized hybrid mappings in Hilbert spaces*, Taiwanese Journal of Mathematics **14** (2010), 2497–2511.

[25] F. Kohsaka and W. Takahashi, *Generalized nonexpansive retractions and a proximal-type algorithm in Banach spaces*, Journal of Nonlinear and Convex Analysis **8** (2007), 197–209.

[26] ———, *Fixed point theorems for a class of nonlinear mappings related to maximal monotone operators in Banach spaces*, Archiv der Mathematik **91** (2008), 166–177.

[27] W. Takahashi, *Nonlinear Functional Analysis*, Yokohama Publishers, Yokohama, 2000.

[28] ———, *Fixed point theorems for new nonlinear mappings in a Hilbert space*, Journal of Nonlinear and Convex Analysis **11** (2010), 79–88.

[29] W. Takahashi and Y. Takeuchi, *Nonlinear ergodic theorem without convexity for generalized hybrid mappings in a Hilbert space*, Journal of Nonlinear and Convex Analysis **12** (2011), 399–406.

[30] W. Takahashi, N.-C. Wong, and J.-C. Yao, *Attractive point and mean convergence theorems for new generalized nonspreading mappings in Banach spaces*, Infinite Products of Operators and Their Applications (S. Reich and A. J. Zaslavski, eds.), Contemporary Mathematics, vol. 636, American Mathematical Society, Providence, 2015, pp. 225–248.

[31] H. K. Xu, *Inequalities in Banach spaces with applications*, Nonlinear Anal **16** (1981), 1127–1138.

Faculty of Engineering, Tamagawa University, Tokyo 194–8610, Japan; Faculty of Science, Chiba University, Chiba 263–8522, Japan

Email address: toshiharu.kawasaki@nifty.ne.jp

-HOMOMORPHISMS BETWEEN GROUPOID C-ALGEBRAS

FUYUTA KOMURA

Abstract. 本稿ではエタール亜群から構成される C*環 (亜群 C*環) を扱う．本分野の主な流れとして「亜群 C*環の性質をエタール亜群の言葉で特徴づける」というものがあるが，本稿では亜群 C*環上の準同型がエタール亜群の言葉で記述するための十分条件を与える．系として，亜群 C*環のとある自己同型群について構造定理を与える．

0. Introduction

作用素環論は関数解析の一分野であり，主に無限次元の非可換な代数を扱う分野である．作用素環は扱う位相によって von Neumann 環と C*環に大別されるが，本稿では C*環を扱う．C*環とは大雑把に言えば involution と完備なノルムを持つ $\mathbb{C}$ 代数である．例えば，行列環 $M_n(\mathbb{C})$Hilbert 空間, H 上の有界線形作用素のなす C*環 $B(H)$, コンパクト空間 X の上の複素連続関数環 $C(X)$ は C*環の例である．この他の具体例を自在に構成することは非自明な問題となるが，現在では様々な C*環の構成方法が知られている．数多くの C*環を構成する方法として，エタール亜群を用いる方法がある．エタール亜群から構成される C*環 (亜群 C*環) の研究は Renault[12] によって始められ，現在でも様々な研究者によって亜群 C*環の研究が行われている．例えば，[13] では亜群 C*環からエタール亜群を再構成する，という類の結果が得られている．他には，亜群 C*環の単純性については [2]，核型性については [1] などで研究されている．

本稿で紹介する結果について概説する．[13] の帰結として，2 つのエタール亜群 G_1, G_2 に対し，その亜群 C*環が同型であるならば G_1 と G_2 が同型であるという定理が得られる (正確な主張は [13, Proposition 4.13] を参照せよ)．様々な C*環が亜群 C*環として実現されるため，この結果は C*環の幅広いトピックに応用されている．例えば，力学系から構成される C*環や半群から構成される C*環の理論では必須とも言える結果である． このように [13] は重要な結果であるが，[9] では [13] の一般化として亜群 C*環の同型とは限らない準同型写像を扱った．すなわち，[13] の結果の肝は C*環の同型写像からエタール亜群の同型写像を構成することであるが，この手続きが C*環の同型と

Center for Advanced Intelligence Project, RIKEN, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan
Phone: +81-45-566-1641+42706
Fax: +81-45-566-1642
E-mail address: fuyuta.k@keio.jp.

2010 *Mathematics Subject Classification.* 20M18, 22A22, 46L05.

は限らない準同型写像に対しても可能であることを [9] で示した．この応用として，亜群 C*環のとある自己同型群がエタール亜群の自己同型群と 1-cocycle の群で記述できることを示した．特に，亜群 C*環への群作用であって不動点環が十分大きいものは，本質的に可換群作用であることが本結果から分かる．

本稿の構成について述べる．まず，エタール亜群や亜群 C*環について定義と基本的な性質を述べる．その後，筆者の結果 [9] の背景と，主定理の概要を述べる．最後に，主定理の応用と今後の展望について述べる．

Acknowledgement. 本研究は JST CREST Grant Number JPMJCR1913 と RIKEN Special Postdoctoral Researcher Program の助成を受けたものです．

1. 準備

本節では C*環とエタール亜群の定義と例を紹介し，エタール亜群から C*環を構成する方法について述べる．C*環論を含む作用素環論については [15] や [4] などを，エタール亜群と亜群 C*環については [12], [14], [11] を参照せよ．

1.1. C*環の定義と例.

C*環の定義と例を紹介する．詳細は [15] や [4] を参照せよ．

大雑把に言えば，C*環とは積と involution を備えた複素 Banach 空間 A で，諸般の条件をみたすもののことである．本稿では正確な定義を与える代わりに，具体例を紹介する．

Example 1.1.1. X を局所コンパクトハウスドルフ空間とする．$C(X)$ を X 上の複素数値連続関数全体からなる集合とする．$f \in C(X)$ が無限遠で消えるとは，任意の $\varepsilon > 0$ に対し

$$\{x \in X | f(x)| \geq \varepsilon\}$$

がコンパクト集合になることとする．このとき，$C_0(X)$ を X 上の無限遠で消える連続関数全体からなる集合とすると，$C_0(X)$ は C*環となる．実際，$C_0(X)$ は各点での演算によって $\mathbb{C}$ ベクトル空間と積の構造を持つ．また，$C_0(X)$ の involution は各点での複素共役によって定まる．$f \in C_0(X)$ のノルムは $\|f\| := \sup_{x \in X}|f(x)|$ と定められる．以上の構造によって，$C_0(X)$ は C*環となる．$C_0(X)$ の積が可換であることに注意せよ．また，任意の可換 C*環が $C_0(X)$ の形として得られることが Gelfand-Naimark の定理として知られている．

Example 1.1.2. H を複素 Hilbert 空間とする．有界線形作用素全体からなる集合 $B(H)$ は C*環となる．実際，各点での演算によって $B(H)$ は $\mathbb{C}$ ベクトル空間となる．また，写像の合成によって $B(H)$ の積が定まる．$B(H)$ の involution は有界線形作用素の adjoint によって定まる．また，$T \in B(H)$ のノルムは $\|T\| := \sup_{\|x\| \leq 1}\|Tx\|$ である．以上の構造によって $B(H)$ は C*環となる．$H = \mathbb{C}^n$ の場合は，$B(H)$ は n 次正方行列からなる環 $M_n(\mathbb{C})$ と同型になる．また，全ての C*環が $B(H)$ の部分環として実現できることが Gelfand-Naimark の定理として知られている．

理論的には $B(H)$ の部分環を考えることで全ての C*環が構成できるが，この方法で自由自在に C*環を構成することは困難である．そのため，C*環論の研究では様々な C*環の構成法が考えられ，その研究が行われてきた．本稿ではエタール亜群から C*環を構成する方法について説明し，エタール亜群と C*環の関係について概説する．

1.2. **エタール亜群の定義と例．** エタール亜群の定義と例を紹介する．詳しくは [12], [14], [11] を参照せよ．

亜群は群をある意味で拡張した概念である．亜群は一般に単位元を複数個持ち，部分的にのみ定義された積を持つという点で群を拡張した概念である．端的には，亜群とは「全ての射が可逆であるような小圏」と定義される．本稿では亜群について以下の記法を用いる．

Definition 1.2.1. 亜群 G は以下の 4 つ組 $(G, G^{(0)}, d.r)$ からなる．

(1) 単位元からなる集合 $G^{(0)} \subset G$,
(2) domain map と range map $d, r\colon G \to G^{(0)}$,
(3) $d(\alpha) = r(\beta)$ となる $\alpha, \beta \in G$ に対し，その積 $\alpha\beta \in G$,
(4) $\alpha \in G$ に対し，その逆元 $\alpha^{-1} \in G$．ただし，逆元は $\alpha^{-1}\alpha = d(\alpha)$, $\alpha\alpha^{-1} = r(\alpha)$ を満たす．

$G^{(0)}$ を G の unit space と呼ぶ．

Definition 1.2.2. G を亜群とする．積と逆元を取る写像が連続となる位相を G が備えている時，G を位相亜群と呼ぶ．また，$d\colon G \to G^{(0)}$ が局所同相写像となるとき，位相亜群 G をエタール亜群と呼ぶ．ただし，d が局所同相写像であるとは，d が開写像であって，各 $\alpha \in G$ に対しある α の開近傍 $U \subset G$ が存在し $d|_U$ が像への同相写像となることである．この場合，r も局所同相写像になることが $r(\alpha) = d(\alpha^{-1})$ という公式と逆元を取る写像が同相であることから分かる．

エタール亜群は位相亜群と離散群を含む概念である．

Example 1.2.3. $G = G^{(0)}$ を満たすエタール亜群は，位相空間と等価な概念である (この場合，積や逆元は自明となる)．また，$G^{(0)}$ が 1 点集合となるエタール亜群は，離散群と等価な概念である．

より一般に，離散群の位相空間への作用からエタール亜群を構成することができる．

Example 1.2.4. Γ を離散群，X を位相空間とし，$\tau\colon \Gamma \curvearrowright X$ を作用とする．また，

$$\Gamma \ltimes_\tau X := \{(y, s, x) \in X \times \Gamma X \mid y = \tau_s(x)\}$$

と置くこのとき，$\Gamma \ltimes_\tau X$ は以下のようなエタール亜群の構造を持つ．まず，unit space は $(\Gamma \ltimes_\tau X)^{(0)} := X$ と定められる．ここで，単射

$$X \ni x \mapsto (x, e, x) \in \Gamma \ltimes_\tau X$$

によって X を $\Gamma \ltimes_\tau X$ の部分集合と同一視している．domain map と range map をそれぞれ $(y, s, x) \in \Gamma \ltimes_\tau X$ に対し．

$$d((y, s, x)) = x, r((y, s, x)) = y$$

と定める．積と逆元はそれぞれ

$$(z,s,y)(y,t,x)=(z,st,x),\ \ (y,t,x)^{-1}=(x,t^{-1},y)$$

によって定められる．これらの構造によって $\Gamma\ltimes_\tau X$ は亜群となり，直積位相の相対位相によって $\Gamma\ltimes_\tau X$ はエタール亜群となる．

上の例では群作用からエタール亜群を構成した．より一般に，逆半群の作用からエタール亜群を構成することができる．逆に，全てのエタール亜群は逆半群の作用から得られる．これらの結果については [11] や [5] を参照せよ．

本稿では，エタール亜群と言ったら局所コンパクトハウスドルフであることを仮定する．この仮定は，エタール亜群上の連続関数が豊富に存在することを保証するために要請される (実際に，本分野では Urysohn の補題や Tietze の拡張定理などが数多く使用される)．一方，ハウスドルフ性は若干強い仮定であり，実際にハウスドルフ性を満たさないエタール亜群は自然に現れる．ハウスドルフでないエタール亜群の取り扱いについては，[11] や [6] を参照せよ．

1.3. **亜群 C*環の定義．** 本節ではエタール亜群から構成される C*環 (亜群 C*環) の定義について説明する．群環と同様に，亜群 C*環も convolution algebra を用いて定義される．以下，その概略を説明する．

G を局所コンパクトハウスドルフなエタール亜群とする．$C_c(G)$ を G 上のコンパクトサポートを持つ複素連続関数全体からなる集合とする．このとき，$C_c(G)$ は各点での演算によってベクトル空間となる．$f,g\in C_c(G)$ に対し，convolution $f*g\in C_c(G)$ と involution $f^*\in C_c(G)$ をそれぞれ

$$f*g(\gamma):=\sum_{\alpha\beta=\gamma}f(\alpha)g(\beta),\ \ f^*(\gamma):=\overline{f(\gamma^{-1})}$$

と定める (ただし，$\gamma\in G$ である)．$f*g$ が実際に $C_c(G)$ の元として定まることは若干非自明であるが，エタール亜群の性質を用いて証明することができる ([14] などを参照せよ)．

このようにして，$C_c(G)$ は*-algebra(involution を備えた $\mathbb{C}$ 代数) となる．あとは $C_c(G)$ を適当なノルムで完備化することで C*環が得られるが，ノルムの選び方は一般には一意ではない．主に用いられるノルムは reduced norm と universal norm の 2 種類であり，他のノルムについては存在性も含めて非自明な対象である．以下，reduced norm と universal norm について説明する．

まず，G の reduced norm について説明する．$x\in G^{(0)}$ に対し $G_x:=d^{-1}(\{x\})$ と置く．このとき，d が局所同相写像であることから，G_x は離散集合になることがわかる．$\ell^2(G_x)$ を

$$\ell^2(G_x):=\left\{\xi\colon G_x\to\mathbb{C}\ \middle|\ \sum_{\alpha\in G_x}|\xi(\alpha)|^2<\infty\right\}$$

と定める．この時，$\ell^2(G_x)$ は Hilbert 空間となる．本稿では $\ell^2(G_x)$ の内積を $\xi,\eta\in\ell^2(G_x)$ に対し

$$\langle\xi|\eta\rangle:=\sum_{\alpha\in G_x}\overline{\xi(\alpha)}\eta(\alpha)$$

と書く (内積が右線形であることに注意せよ)．$f \in C_c(G)$ に対し，$\lambda_x(f)\colon \ell^2(G_x) \to \ell^2(G_x)$ を

$$\lambda_x(f)(\delta_\beta) := \sum_{\alpha \in G_{r(\beta)}} f(\alpha)\delta_{\alpha\beta}$$

によって定める (ここで，$\delta_\beta \in \ell^2(G_x)$ は β で 1, その他で 0 となる関数である)．記号の乱用となはるが，一般の $\xi \in \ell^2(G_x)$ に対しては $\lambda_x(f)\xi = f * \xi$ となることに注意せよ．$\lambda_x(f)$ は有界線形作用素になることがわかるため，写像 $\lambda_x\colon C_c(G) \to B(\ell^2(G_x))$ が得られる．さらに，λ_x は*を保つ準同型写像になることもわかる．

ここで，$C_c(G)$ の reduced norm を次のように定める．

Definition 1.3.1. $f \in C_c(G)$ に対し，f の reduced norm を

$$\|f\|_r := \sup_{x \in G^{(0)}} \|\lambda_x(f)\|$$

と定める．ただし，右辺に現れるノルムは $B(\ell^2(G_x))$ の作用素ノルムである．$C_c(G)$ の reduced norm による完備化を $C_r^*(G)$ と書き，被約亜群 C*環 (reduced groupoid C*-algebra) と呼ぶ．

$\|f\|_r < \infty$ を示すためには若干の議論が必要である．例えば [3, Lemma 5.6.12] を参照せよ．

次に，universal norm について説明する．

Definition 1.3.2. $f \in C_c(G)$ に対し，f の universal norm を

$$\|f\|_u := \sup_\pi \|\pi(f)\|$$

と定める (ただし，右辺の sup は全ての*-表現 $\pi\colon C_c(G) \to B(H)$ に対し考えている)．$C_c(G)$ の universal norm による完備化を $C^*(G)$ と書き，普遍亜群 C*環 (universal groupoid C*-algebra) と呼ぶ．

reduced norm の場合と同様に，universal norm が well-defined であることも非自明である．[3, Lemma 5.6.12] の下部にある説明を参照せよ．

定義から $\|f\|_r \leq \|f\|_u$ が任意の $f \in C_c(G)$ に対して成り立つ．従って，$C_c(G)$ 上の恒等写像は $q\colon C^*(G) \to C_r^*(G)$ という*-準同型写像に拡張される．q が全射であることは C*環の一般論から従うが，一般に単射ではない．G が従順という性質を持つとき，q が単射であることが従う ([3, Corollary 5.6.17] を参照せよ)．逆は成り立たず，q の単射性は G の従順性を導くとは限らない．このようなエタール亜群 G の例については [16] を参照せよ．また，G の従順性と $C^*(G)$, $C_r^*(G)$ の核型性という性質が同値である ([3, Theorem 5.6.18] を参照せよ)．

本節の最後に，$G^{(0)}$ から定まる $C^*(G)$ と $C_r^*(G)$ の可換部分環について説明する．$G^{(0)} \subset G$ は [14, Lemma 8.4.2] より開集合であるため (実際には [14, Lemma 8.3.2] より閉でもある)，自然な包含写像 $C_c(G^{(0)}) \subset C_c(G)$ が得られる．この包含写像は $C_0(G^{(0)}) \subset C_r^*(G)$, $C_0(G^{(0)}) \subset C^*(G)$ に拡張される ([14, Corollary 9.3.4] を参照せよ)．

2. 主定理

前節ではエタール亜群 G から 2 種類の C*環 $C^*(G)$, $C_r^*(G)$ を構成した．$C^*(G)$ や $C_r^*(G)$ の C*環としての性質とエタール亜群 G の性質との関係を調べることが，本分野における基本的な問題意識である．本節では，亜群 C*環上の*-準同型がエタール亜群の言葉で捉えられるための条件について検討する．具体的には，亜群 C*環上の*-準同型が unit space 上の連続関数環を保つならば，その*-準同型はエタール亜群の言葉で記述できるという筆者の結果 [9] について説明する．

2.1. 亜群 C*環上の*-準同型の構成． まず，亜群 C*環上の*-準同型がエタール亜群のどのような概念から構成されるか説明する．最初に不変閉集合から*-準同型を構成する方法について説明し，次に cocycle と亜群の準同型から*-準同型を構成する方法について説明する．引き続き，エタール亜群は局所コンパクトハウスドルフであることを仮定する．

Definition 2.1.1. G をエタール亜群とする．$F \subset G^{(0)}$ が不変であるとは，任意の $\alpha \in G$ に対し $d(\alpha) \in F$ ならば $r(\alpha) \in F$ が成り立つこととする．このとき，$G_F := d^{-1}(F)$ と書く．

$F \subset G^{(0)}$ を不変な閉集合とする．このとき，G_F は G の閉部分亜群となる．$G_F^{(0)} = F$ となることに注意せよ．

不変な閉集合は，以下のように全射*-準同型を誘導する．

Proposition 2.1.2 ([14, Proposition 10.3.2])**.** $F \subset G^{(0)}$ を不変な閉集合とする．このとき，

$$\mathrm{res}\colon C_c(G) \ni f \mapsto f|_{G_F} \in C_c(G_F)$$

は*-準同型となる．また，この写像は全射*-準同型 $\mathrm{res}\colon C_r^*(G) \to C_r^*(G_F)$ を誘導する．

次に，エタール亜群の cocycle と準同型から誘導される*-準同型について説明する．

Definition 2.1.3. G をエタール亜群とし，$\mathbb{T}$ を円周群とする．連続な準同型 $c\colon G \to \mathbb{T}$ を，G 上の cocycle と呼ぶ．また，G 上の cocycle 全体からなる集合を $Z(G)$ と書く．$Z(G)$ は各点での演算によって可換群となる．

Proposition 2.1.4 (cf. [8, Proposition 3.13])**.** G と H をエタール亜群とする．$\Phi\colon G \to H$ を局所同相な連続準同型とし，$c \in Z(G)$ とする．また，Φ が $G^{(0)}$ 上で単射であったと仮定する．さらに，$\varphi_{c,\Phi}\colon C_c(G) \to C_c(H)$ を

$$\varphi_{c,\Phi}(f)(\delta) := \sum_{\alpha \in \Phi^{-1}(\{\delta\})} c(\alpha) f(\alpha)$$

と定める (ただし，$f \in C_c(G)$, $\delta \in H$ である)．この時，$\varphi_{c,\Phi}\colon C_c(G) \to C_c(H)$ は*-準同型となる．

Remark 2.1.5. 上述の $\varphi_{c,\Phi}$ が $C_r^*(G)$ 上の*-準同型に拡張できるとは限らない．実際，G を非従順な離散群 (例えば，階数が 2 以上の自由群など)，H を

自明群とした時には $\varphi_{c,\Phi}$ が*-準同型 $\varphi_{c,\Phi}\colon C_r^*(G)\to C_r^*(H)$ に拡張されることはない．これは，非従順群の被約群 C*環が 1 次元表現を持たないという事実から分かる ([3, Theorem 2.6.8] を参照せよ)．一方，$\varphi_{c,\Phi}$ を universal 亜群 C*環上の*-準同型 $\varphi_{c,\Phi}\colon C^*(G)\to C^*(H)$ に拡張することは universal norm の性質よりいつでも可能である．

以上より，$C_r^*(G)$ 全体に定義できるかどうか注意が必要ではあるが，不変な閉集合，cocycle と亜群の準同型から*-準同型を作ることができた．次節では，このようにして得られる*-準同型の特徴づけを主定理として紹介する．

2.2. **主定理．** 前節では，不変な閉集合，cocycle と亜群の準同型から*-準同型を構成する手続きを確認した．本節では，このようにして得られる*-準同型の特徴づけを主定理として紹介する．

まず，主定理に用いられる概念を定義する．引き続き，エタール亜群は局所コンパクトハウスドルフ空間であることを仮定する．

Definition 2.2.1. G をエタール亜群とする．G が effective であるとは, $G^{(0)}=\mathrm{Iso}(G)^\circ$ が成り立つこととする．ただし，

$$\mathrm{Iso}(G):=\{\alpha\in G\mid d(\alpha)=r(\alpha)\}$$

であり，$\mathrm{Iso}(G)^\circ$ は $\mathrm{Iso}(G)$ の内部を表す．

$G^{(0)}\subset\mathrm{Iso}(G)^\circ$ は任意のエタール亜群 G に対して成り立つため，反対側の包含 $G^{(0)}\supset\mathrm{Iso}(G)^\circ$ が effective 性の本質的な仮定である．

Example 2.2.2. 自明でない離散群 Γ は effective ではない．また，$G=G^{(0)}$ となるエタール亜群 (i.e. 局所コンパクト空間) は effective である．一般に，局所コンパクト空間 X への離散群作用 $\tau\colon\Gamma\curvearrowright X$ に対し，τ が位相的に自由であるならば，$\Gamma\ltimes_\tau X$ は effective である．ここで，$\tau\colon\Gamma\curvearrowright X$ が位相的に自由であるとは，安定化群

$$\Gamma_x:=\{s\in\Gamma\mid\tau_s(x)=x\}$$

が自明となるような $x\in X$ が X で稠密になることである．また，Γ が可算であると仮定する．このとき，$\Gamma\ltimes_\tau X$ が effective であるならば $\tau\colon\Gamma\curvearrowright X$ は位相的に自由である．これは Baire のカテゴリー定理から容易に従う．

直感的に言えば，effective なエタール亜群は離散群からかけ離れたエタール亜群である．effectiveness を仮定することで離散群由来の困難を排除することができるため，effectiveness は亜群 C*環の研究においてしばしば用いられる仮定である．

先の $\tau\colon\Gamma\curvearrowright X$ に付随する例と同様に，多くの具体例においてエタール亜群の安定化群はほとんど自明となる．実際，エタール亜群の effectiveness について次のことが知られている．

Proposition 2.2.3 ([13, Proposition 3.6])**.** G をエタール亜群とする．$x\in G^{(0)}$ に対し，

$$G(x):=\{\alpha\in G\mid d(\alpha)=r(\alpha)=x\}$$

と置く．このとき，$G(x)=\{x\}$ となる $x\in G^{(0)}$ が $G^{(0)}$ で稠密であるならば，G は effective である．また，G が第二可算であるならば，逆も成り立つ．

本稿の主定理について述べる．G と H をエタール亜群とし，H を effective とする．まず，エタール亜群 G に対し被約亜群 C*環 $C_r^*(G)$ とその可換部分環 $C_0(G^{(0)})$ が構成されることに注意せよ．次の主定理は，$C_0(G^{(0)})$ を $C_0(H^{(0)})$ に移すような*-準同型が Proposition 2.1.2 と Proposition 2.1.4 の*-準同型の合成として得られることを主張する．

Theorem 2.2.4 ([9, Theorem 2.1.1])**.** G と H をエタール亜群とし，H が effective であると仮定する．また，*-準同型 $\varphi\colon C_r^*(G) \to C_r^*(H)$ に対し，$\varphi(C_0(G^{(0)}))$ が $C_0(H^{(0)})$ にイデアルとして含まれていたとする．このとき，不変な閉集合 $F \subset G^{(0)}$, cocycle $c \in Z(G_F)$, 局所同相な準同型写像 $\Phi\colon G_F \to H$ が存在し，

$$\varphi(f) = \varphi_{c,\Phi} \circ \mathrm{res}(f)$$

が任意の $f \in C_c(G)$ に対し成り立つ．ここで，res と $\varphi_{c,\Phi}$ はそれぞれ Proposition 2.1.2 と Proposition 2.1.4 に現れる*-準同型である．

Proof. 証明の概略について述べる．まず，$F \subset G^{(0)}$ の構成であるが，

$$\ker \varphi \cap C_0(G^{(0)}) = C_0(G^{(0)} \setminus F)$$

を満たす閉集合 $F \subset G^{(0)}$ として構成される．このような F の存在は，可換 C*環 $C_0(X)$ のイデアルが X の閉集合と 1 対 1 に対応することから従う．また，直接計算から $F \subset G^{(0)}$ が不変であることも分かる．

$\Phi\colon G_F \to H$ の構成が最も非自明である．亜群 C*環の構造からエタール亜群の構造を再構成する技術は [13] で整備されているため，[13] の技術を用いることが重要となる．一方，[13] では主に effective なエタール亜群が扱われているが，G や G_F は effective とは限らないため，実際には [13] に現れる技術を改良したものが必要となる．詳細は [9, Theorem 2.1.1] の証明を参照せよ．

最後に $c \in Z(G_F)$ であるが，これは φ と $\varphi_{1,\Phi} \circ \mathrm{res}$ を比較することで構成される (ただし，$1 \in Z(G_F)$ を定数 cocycle とした)． □

上述の証明でも述べたように，G に effective 性を課していない点に本定理の技術的な新規性がある．また，H の effective 性を外すことは不可能である．実際，群 C*環の間の*-準同型を群の言葉のみで記述することは一般に不可能である ($G = \mathbb{Z}/2\mathbb{Z}$, $H = \mathbb{Z}/3\mathbb{Z}$ の場合などを考えよ)．

2.3. 応用．

本節では前節の主定理 Theorem 2.2.4 の応用について述べる．特に，亜群 C*環上の自己同型写像に対し Theorem 2.2.4 を応用する．

まず，記号を用意する．

Definition 2.3.1. A を C*環とし，$B \subset A$ を部分 C*環とする．$\mathrm{Aut}(A)$ を A の自己同型全体からなる群とする．また，$\mathrm{Aut}(A)$ の部分群をそれぞれ

$$\mathrm{Aut}(A; B) := \{\varphi \in \mathrm{Aut}(A) \mid \varphi(B) = B\},$$
$$\mathrm{Aut}_B(A) := \{\varphi \in \mathrm{Aut}(A) \mid \text{全ての } b \in B \text{ に対し } \varphi(b) = b\}$$

と定める．

$\mathrm{Aut}_B(A)$ が $\mathrm{Aut}(A; B)$ の正規部分群であることに注意せよ．$A = C_r^*(G)$, $B = C_0(G^{(0)})$ とし，Theorem 2.2.4 を応用することで次の系が得られる．

Corollary 2.3.2 ([10, Proposition 5.7], [9, Corollary 2.2.2, Corollary 2.2.6]). G を effective なエタール亜群とする．このとき，

$$\Psi\colon \operatorname{Aut}(G) \ltimes Z(G) \ni (\Phi, c) \mapsto \varphi_{c,\Phi} \in \operatorname{Aut}(C_r^*(G); C_0(G^{(0)})$$

は群としての同型写像である．ここで，$\operatorname{Aut}(G) \ltimes Z(G)$ は自然な作用 $\operatorname{Aut}(G) \curvearrowright Z(G)$ に関する半直積群である．また，$\Psi(Z(G)) = \operatorname{Aut}_{C_0(G^{(0)})}(C_r^*(G))$ が成り立つ．従って，Ψ は $Z(G)$ と $\operatorname{Aut}_{C_0(G^{(0)})}(C_r^*(G))$ の間の同型写像を誘導する．

Proof. 証明の概略を述べる．まず，Ψ が well-defined であり，群準同型であることと単射性が直接計算から分かる．Ψ の全射性が非自明であるが，これは Theorem 2.2.4 から直ちに従う．ここで，同型写像については対応する不変集合 F が $G^{(0)}$ となり $G_F = G$ となることに注意せよ．

後半の主張は，「$\Phi \in \operatorname{Aut}(G)$ が $\Phi|_{G^{(0)}}$ を満たすならば $\Phi = \mathrm{id}_G$ となる」という主張から従う．詳しくは [9, Corollary 2.2.6] を参照せよ． □

Remark 2.3.3. Corollary 2.3.2 について補足をする．[10, Proposition 5.7] では $\operatorname{Aut}(G) \ltimes Z(G)$ と $\operatorname{Aut}(C_r^*(G); C_0(G^{(0)})$ の同型が，G が第二可算である場合に示されていた．[9, Corollary 2.2.2] では G が第二可算とは限らない場合にもこの同型が正しいことを証明した．$Z(G)$ と $\operatorname{Aut}_{C_0(G^{(0)})}(C_r^*(G))$ が同型であることは [9, Corollary 2.2.6] で得られた結果である．[9, Corollary 2.2.6] では topologically principal という effective より強い性質を G に仮定しているが，実際には effective で十分である [7].

2.4. **今後の展望.** 今後の展望について述べる．Corollary 2.3.2 において，群の同型

$$\operatorname{Aut}(G) \ltimes Z(G) \simeq \operatorname{Aut}(C_r^*(G); C_0(G^{(0)})$$

が得られた．一般に C*環の自己同型群を計算することは困難であるため，この同型は C*環の自己同型群の研究に貴重な手がかりを与えると考えられる．そこで，上の同型を用いて $\operatorname{Aut}(C_r^*(G); C_0(G^{(0)})$ の具体的な計算や群としての構造を調べることが喫緊の課題であると筆者は考えている．

References

[1] C. Anantharaman-Delaroche and J. Renault. *Amenable Groupoids*. Monographie de l'Enseignement mathématique. L'Enseignement Mathématique, 2000.

[2] J. Brown, L. O. Clark, C. Farthing, and A. Sims. Simplicity of algebras associated to étale groupoids. *Semigroup Forum*, **88**(2):433–452, 2014.

[3] N. P. Brown and N. Ozawa. *C*-algebras and Finite-dimensional Approximations*. Graduate studies in mathematics. American Mathematical Soc., 2008.

[4] K.R. Davidson. *C*-Algebras by Example*. Fields Institute for Research in Mathematical Sciences Toronto: Fields Institute monographs. American Mathematical Society, 1996.

[5] R. Exel. Inverse semigroups and combinatorial C*-algebras. *Bulletin of the Brazilian Mathematical Society, New Series*, 39, 04 2007.

[6] R. Exel. Non-Hausdorff étale groupoids. *Proceedings of the American Mathematical Society*, **139**(3):897–907, 2011.

[7] F. Komura. in preparation.

[8] F. Komura. Quotients of étale groupoids and the abelianizations of groupoid C*-algebras. *Journal of the Australian Mathematical Society*, 111(1):56–75, 2021.

[9] F. Komura. *-homomorphisms between groupoid C*-algebras. arXiv:2302.10405, 2023.

[10] H. Matui. Homology and topological full groups of étale groupoids on totally disconnected spaces. *Proceedings of the London Mathematical Society*, 104(1):27–56, 08 2011.

[11] A. Paterson. *Groupoids, Inverse Semigroups, and their Operator Algebras*. Progress in Mathematics. Birkhäuser Boston, 2012.

[12] J. Renault. *A Groupoid Approach to C*-Algebras*. Lecture Notes in Mathematics. Springer-Verlag, 1980.

[13] J. Renault. Cartan subalgebras in C*-algebras. *Irish Math. Soc. Bull.*, **61**:29–63, 2008.

[14] A. Sims. Hausdorff étale groupoids and their C*-algebras. *Operator Algebras and Dynamics: Groupoids, Crossed Products, and Rokhlin Dimension*, 2020.

[15] M. Takesaki. *Theory of Operator Algebras I*. Encyclopaedia of Mathematical Sciences. Springer Berlin Heidelberg, 2001.

[16] R. Willett. A non-amenable groupoid whose maximal and reduced C^*-algebras are the same. *Münster J. Math.*, **8**(1):241–252, 2015.

Pearcey系に対するWKB解のBorel和の接続公式について

内田 匠風　(日本大学 理工学部)*

1 はじめに

Voros [26] により創始された完全WKB解析は, 主に2階のSchrödinger型の常微分方程式に対する解の大域的な性質を解明するのに極めて有効な手法であることが知られている [16, 23]. 最近では, クラスター代数や位相的漸化式と量子曲線の理論との関連も見出されている [13, 14].

[2] では, 2階のSchrödinger型の常微分方程式に対するVoros接続公式 [26] が, 超局所解析の視点から証明されている. 証明手法について少し述べる. まず, 解析的なポテンシャルを持つ2階のSchrödinger型の常微分方程式を, 単純変わり点近傍で, 大きなパラメータ付きのAiry方程式に形式的に変換する. この変換に現れる形式級数は, 超局所微分作用素を用いることで正当化することができる. 次に, 大きなパラメータ付きのAiry方程式に対するWKB解のBorel変換は, Gaussの超幾何函数で書けることを証明する. そして, Gaussの超幾何函数の接続公式を用いることにより, Vorosの接続公式を証明する.

[2] の証明で使われたGaussの超幾何函数のパラメータは, Schwarzのリスト [24] に含まれている. すなわち, Airy方程式に対するWKB解のBorel変換は, 3次の代数函数を用いて表すことができる. この視点を応用することで, Airy方程式に対するVorosの接続公式を, Gaussの超幾何函数を用いず代数函数を用いて, 導出することができる [5].

[18] では, 2次元Garnier系およびその合流型方程式系の特殊解が議論されている. 特に, $LH(5)$ はAiry方程式を2変数に拡張した系に相当する. この系は, Pearcey系と呼ばれる線型偏微分方程式系と等価である. Pearcey系に対する完全WKB解析は, 廣瀬 [9, 10, 11] 及び本多-河合-竹井 [12] により集中的に研究されている. 特に, [9, 10, 11] では, Pearcey系およびその接方程式系に対するStokes曲面 (曲線), 接続公式などが考察されている. また, Pearcery系は独立変数の1つを固定すると, Berk-Nevins-Roberts [7] によって研究された3階の線型常微分方程式 (BNR方程式) となる.

本講演では, Pearcey系に対するWKB解のBorel変換が, 4次の代数函数の一次結合として明示的に書けることを述べる. その帰結として, Pearcey系に対するWKB解はresurgent [8] であることを述べる. また, 代数函数の解析接続を考えることで, Pearcey系に対するWKB解のVoros型の接続公式が得られることを述べる.

2 Pearcey系のWKB解

本節では, Pearcey系に対するWKB解の構成について説明する. η は大きなパラメータとし, 次の振動積分を考える:

$$u = \int \exp\left(\eta(t^4 + x_2t^2 + x_1t)\right) dt. \tag{1}$$

この積分は, 大きなパラメータ付きのPearcey積分と呼ばれている [10, 22]. ただし, 積分路は被積分函数が遠方で急減少するような複素平面上の路を取る. Pearcey積分は,

---

* 〒274-8501 千葉県船橋市習志野台7-24-1
e-mail: uchida.shofu@nihon-u.ac.jp
本研究は, 青木貴史氏 (近畿大学) 及び鈴木貴雄氏 (近畿大学) との共同研究に基づく.

大きなパラメータ付きの Airy 積分

$$\int \exp\left(\eta(t^3+xt)\right) dt$$

の自然な拡張と見做すことができる [18]. Pearcey 積分は, 次の線型偏微分方程式系を満たす [1, 10]:

$$\begin{aligned} Q_1 u &= (4\partial_1^3 + 2\eta^2 x_2 \partial_1 + \eta^3 x_1)u = 0, \\ Q_2 u &= (\eta\partial_2 - \partial_1^2)u = 0. \end{aligned} \tag{2}$$

ただし, $\partial_i = \partial/\partial x_i$ $(i=1,2)$ とする. この線型偏微分方程式系は, 次の線型偏微分方程式系と等価である [18].

$$\begin{aligned} P_1\psi &= (4\partial_1\partial_2 + 2\eta x_2\partial_1 + \eta^2 x_1)\psi, \\ P_2\psi &= (4\partial_2^2 + \eta x_1\partial_1 + 2\eta x_2\partial_2 + \eta)\psi, \\ P_3\psi &= (\eta\partial_2 - \partial_1^2)\psi. \end{aligned} \tag{3}$$

実際,

$$\begin{aligned} P_1 &= \eta^{-1}\left(Q_1 + 4\partial_1 Q_2\right), \\ P_2 &= \eta^{-2}\partial_1 Q_1 + \left(4\eta^{-2}Q_2 + 8\eta^{-2}\partial_1^2 + 2x_2\right) Q_2, \\ Q_1 &= \eta P_1 - 4\partial_1 P_3 \end{aligned}$$

が成り立つ. 注意として, $P_2 = \eta^{-1}\partial_1 P_1 + 2\left(2\eta^{-1}\partial_2 + x_2\right) P_3$ が成り立つ.

線型偏微分方程式系 (2) の WKB 解の接続問題は, 廣瀬 [9, 10, 11] および本多-河合-竹井 [12] によって集中的に研究されている. しかし, 我々は [9, 10, 11] や [12] とは少し違った観点から考える. 具体的には, η を大きなパラメータではなく, (複素) 独立変数として考える. このとき, 線型偏微分方程式系 (3) は subholonomic [15] であり, Pearcey 積分は (2) だけでなく,

$$Q_3 u = (3x_1\partial_1 + 2x_2\partial_2 - 4\eta\partial_\eta - 1)u = 0$$

も満たす. この方程式は, Pearcey 積分の擬斉次性より得られる. そこで, 方程式

$$P_4\psi = (3x_1\partial_1 + 2x_2\partial_2 - 4\eta\partial_\eta - 1)\psi = 0 \qquad (Q_3\psi = 0).$$

と線型偏微分方程式系 (3) とを合わせた線型偏微分方程式系

$$P_k\psi = 0 \quad (k = 1,2,3,4) \tag{4}$$

を考える. この線型偏微分方程式系 (4) は, D-加群の理論を用いると, 次のように定式化することができる. D は変数 (x_1, x_2, η) で定義される Weyl 代数とし, I は P_k $(k = 1,2,3,4)$ で生成される D の左イデアルとする. また, M は I で定義される左 D-加群とする. すなわち,

$$M = D/I$$

とする. グレブナー基底のアルゴリズム [20, 21] を適用することにより, 次が証明できる:

Lemma 1 ([5, 6])**.** 左 D-加群 M は, *rank* 3 の *holonomic* 系である.

次に, M の WKB 解を構成する. 線型偏微分方程式系 (4) の未知函数 u に対して,

$$S^{(1)} = \partial_1 u/u, \quad S^{(2)} = \partial_2 u/u$$

とおく. このとき, $S^{(1)}, S^{(2)}$ は, $Q_k u = 0$ $(k = 1, 2)$ より, 次の非線型偏微分方程式系を満たす:

$$\begin{cases} 4\left(S^{(1)}\right)^3 + 2\eta^2 x_2 S^{(1)} + \eta^3 x_1 + 12 S^{(1)} \partial_1 S^{(1)} + 4\partial_1^2 S^{(1)} = 0, \\ \eta S^{(2)} - \partial_1 S^{(1)} - \left(S^{(1)}\right)^2 = 0. \end{cases}$$

この非線型偏微分方程式系の形式解を,

$$S^{(i)} = S^{(i)}(x_1, x_2, \eta) = \sum_{j \geq -1} S_j^{(i)}(x_1, x_2)\, \eta^{-j} \qquad (i = 1, 2)$$

という形を仮定して求める. すると, $S^{(1)}$ の leading term $S_{-1}^{(1)} = \zeta$ は 3 次方程式

$$4\zeta^3 + 2x_2\zeta + x_1 = 0 \tag{5}$$

を満たし, また, $S_j^{(1)}$ $(j \geq 0)$ および $S_j^{(2)}$ $(j \geq -1)$ は, 次の漸化式を満たすことがわかる:

$$\begin{cases} S_0^{(1)} = -\dfrac{1}{2}\partial_1 \log\left(6(S_{-1}^{(1)})^2 + x_2\right), \\ S_j^{(1)} = -\dfrac{2}{6(S_{-1}^{(1)})^2 + x_2}\left(\displaystyle\sum_{\substack{j_1+j_2+j_3=j-2 \\ -1 \leq j_1, j_2, j_3 < j}} S_{j_1}^{(1)} S_{j_2}^{(1)} S_{j_3}^{(1)} \right. \\ \qquad\qquad \left. +3 \displaystyle\sum_{\substack{j_1+j_2=j-2 \\ -1 \leq j_1, j_2 < j}} S_{j_1}^{(1)} \partial_1 S_{j_2}^{(1)} + \partial_1^2 S_{j-2}^{(1)} \right) \quad (j \geq 1), \end{cases} \tag{6}$$

$$\begin{cases} S_{-1}^{(2)} = \left(S_{-1}^{(1)}\right)^2, \\ S_j^{(2)} = \displaystyle\sum_{m=0}^{j+1} S_{m-1}^{(1)} S_{j-m}^{(1)} + \partial_1 S_{j-1}^{(1)} \quad (j \geq 0). \end{cases} \tag{7}$$

したがって, 漸化式 (6), (7) 及び (5) を用いることにより, 形式級数

$$S^{(i),\ell} = S^{(i),\ell}(x_1, x_2, \eta) = \sum_{j \geq -1} S_j^{(i),\ell}(x_1, x_2)\, \eta^{-j} \qquad (i = 1, 2)$$

を構成することができる. ただし, $S_{-1}^{(1),\ell} = \zeta_\ell$ $(\ell = 1, 2, 3)$ とし, ζ_ℓ $(\ell = 1, 2, 3)$ は 3 次方程式 $4\zeta^3 + 2x_2\zeta + x_1 = 0$ の根とする.

Lemma 2 ([1, 10])**.** 1-形式 $\omega^{(\ell)} = S^{(1),\ell} dx_1 + S^{(2),\ell} dx_2$ は閉形式である.

[1, 10] では形式解

$$\psi = \eta^{-1/2} \exp\left(\int_{(a_1, a_2)}^{(x_1, x_2)} \omega\right) \tag{8}$$

を WKB 解と呼んでいる. ここで, $(a_1, a_2) \in \mathbb{C}^2$ は適当に固定された点である. しかし, 上の WKB 解の構成では, 擬斉次性の方程式

$$P_4\psi = (3x_1\partial_1 + 2x_2\partial_2 - 4\eta\partial_\eta - 1)\psi = 0$$

を用いていない. 擬斉次性を仮定すると, 次が証明できる.

Lemma 3 ([5, 6])**.** $\omega_j^{(\ell)}$ は $\omega^{(\ell)}$ の η^{-j} $(j = -1, 0, 1, 2, \ldots)$ に関する係数とする．このとき, M の *WKB* 解 ψ_ℓ が $P_4\psi_\ell = 0$ を満たすことと

$$\int \omega_0^{(\ell)} = -\frac{1}{2}\log\left(6\left(S_{-1}^{(1),\ell}\right)^2 + x_2\right) + C \tag{9}$$

$$\int \omega_j^{(\ell)} = -\frac{1}{4j}\left(3x_1S_j^{(1),\ell} + 2x_2S_j^{(2),\ell}\right) \quad (j \geq -1, j \neq 0). \tag{10}$$

が成り立つことは必要十分である．ここで, C は任意定数であり,

$$\int \omega^{(\ell)} = \sum_{j\geq -1} \eta^{-j} \int \omega_j^{(\ell)}$$

である．

したがって, 我々は Lemma 3 において, $C = 0$ としたものを M の WKB 解と呼ぶ. M の WKB 解 ψ_ℓ $(\ell = 1, 2, 3)$ の明示的な表示は次で与えられる:

$$\psi_\ell = \frac{\exp\left(\frac{\eta}{4}\left(3x_1S_{-1}^{(1),\ell} + 2x_2S_{-1}^{(2),\ell}\right)\right)}{\left(\eta\left(6\left(S_{-1}^{(1),\ell}\right)^2 + x_2\right)\right)^{1/2}} \exp\left(-\sum_{j\geq 1}\frac{\eta^{-j}}{4j}\left(3x_1S_j^{(1),\ell} + 2x_2S_j^{(2),\ell}\right)\right). \tag{11}$$

3 変わり点と Stokes 集合

本節では, M の Stokes 集合が 6 次の代数函数を用いて書けることを説明する．M に対する変わり点および Stokes 曲面の定義は, [1, 10] で与えられている．まず, M に対する変わり点について紹介する．

Definition 4. $\ell, k \in \{1, 2, 3\}$ は $\ell \neq k$ を満たすとする．点 $\tau = (\tau_1, \tau_2) \in \mathbb{C}^2$ が M の type (ℓ, k) の変わり点であるとは,

$$\omega_{-1}^{(\ell)}(\tau) = \omega_{-1}^{(k)}(\tau)$$

が成り立つことである．

すべての type の変わり点の集合を T と表す．この T を M の変わり点集合と呼ぶ. 定義より, T は 3 次式 $4\zeta^3 + 2x_2\zeta + x_1$ の (ζ に関する) 判別式の零点集合と等しいことがわかる [1, 10]:

$$T = \{(x_1, x_2) \in \mathbb{C}^2 \mid 27x_1^2 + 8x_2^3 = 0\}.$$

次に, Stokes 集合を定義する．

Definition 5. 点 $\tau = (\tau_1, \tau_2) \neq (0, 0)$ は type (ℓ, k) の変わり点とする．点 τ を通る Stokes 曲面とは, 次の式で定義される曲面である:

$$\mathcal{S}_\tau = \left\{x = (x_1, x_2) \in \mathbb{C}^2 \;\middle|\; \operatorname{Im}\int_\tau^x \left(\omega_{-1}^{(\ell)} - \omega_{-1}^{(k)}\right) = 0\right\}.$$

曲面 $\mathcal{S}_\tau$ を type (ℓ, k) の Stokes 曲面という．また, すべての type の変わり点 $\tau \in T$ に関する $\mathcal{S}_\tau$ の和集合を M の Stokes 集合といい, $\mathcal{S}$ と表す. Lemma 3 を用いることにより, 次を証明することができる．

Theorem 6 ([6])**.** 次の 6 次方程式によって定義される代数函数を F とする：

$$16F^6+32x_2\left(27x_1^2-x_2^3\right)F^4+16x_2^2\left(27x_1^2-x_2^3\right)^2F^2+x_1^2\left(27x_1^2+8x_2^3\right)^3=0.$$

このとき,

$$\mathcal{S}=\{(x_1,x_2)\in\mathbb{C}^2\,|\,\mathrm{Im}\,F(x_1,x_2)=0\,\}.$$

特に, $\mathcal{S}$ は $\mathbb{C}^2$ の部分集合として, 半代数的集合である.

この定理により, 6 次の代数函数を用いて M の Stokes 集合を描くことができる. 注意として, 一般的な仮定の下で, $\mathcal{S}$ は半代数的集合であることが示されている [11, 17] .

4 WKB 解の Borel 変換と代数函数

本節では, M の WKB 解の Borel 変換が代数函数の 1 次結合で書けることを説明する. M の WKB 解 ψ_ℓ は, η で展開すると次のように書ける:

$$\psi_\ell=\exp\left(\eta\varpi_\ell\right)\sum_{j=0}^{\infty}\eta^{-j-\frac{1}{2}}f_{j,\ell}\left(x_1,x_2\right)\qquad(\ell=1,2,3).$$

ただし,

$$\varpi_\ell=\frac{1}{4}\left(3x_1S_{-1}^{(1),\ell}+2x_2S_{-1}^{(2),\ell}\right),$$

$$f_{0,\ell}\left(x_1,x_2\right)=\left(6(S_{-1}^{(1),\ell})^2+x_2\right)^{-\frac{1}{2}}$$

とする. M の WKB 解の Borel 変換を $\psi_{\ell,B}$ と表す:

$$\psi_{\ell,B}=\sum_{j=0}^{\infty}\frac{f_{j,\ell}\left(x_1,x_2\right)}{\Gamma(j+1/2)}\left(y+\varpi_\ell\right)^{j-1/2}.$$

変数 (x_1,x_2,y) で定義される Weyl 代数を D_B とし, $P_{k,B}$ $(k=1,2,3,4)$ で生成される D_B の左イデアルを I_B とする. ここで, $P_{k,B}$ $(k=1,2,3,4)$ は P_k の Borel 変換とする:

$$\begin{aligned}
P_{1,B}&=4\partial_1\partial_2+2x_2\partial_1\partial_y+x_1\partial_y^2,\\
P_{2,B}&=4\partial_2^2+x_1\partial_1\partial_y+2x_2\partial_2\partial_y+\partial_y,\\
P_{3,B}&=\partial_2\partial_y-\partial_1^2,\\
P_{4,B}&=3x_1\partial_1+2x_2\partial_2+4y\partial_y+3.
\end{aligned}$$

I_B で定義される左 D_B-加群 を M_B とする. すなわち, $M_B=D_B/I_B$ とする.

Lemma 7 ([5, 6])**.** 左 D_B-加群 M_B は, *rank* 3 の *holonomic* 系である.

Remark 8. J は Q_k $(k=1,2,3)$ で生成される D の左イデアルとし, N は J で定義される左 D-加群とする. また, J_B は $Q_{k,B}$ $(k=1,2,3)$ で生成される D_B の左イデアルとし, N_B は J_B で定義される左 D_B-加群とする. このとき, N は rank 3 の holonomic 系であるが, N_B は rank 6 の holonomic 系となる. すなわち, N_B には 3 次元分の余剰な解が存在する. J の monomial order $\eta\succ x_1\succ x_2$ に対するグレブナー基底 $\boldsymbol{G}=\{G_1,G_2,G_3,G_4\}$ は

$$\begin{aligned}
G_1&=\eta(4\partial_1\partial_2+2\eta x_2\partial_1+\eta^2x_1),\\
G_2&=\eta^2(4\partial_2^2+\eta x_1\partial_1+2\eta x_2\partial_2+\eta),\\
G_3&=\eta\partial_2-\partial_1^2,\\
G_4&=3x_1\partial_1+2x_2\partial_2-4\eta\partial_\eta-1
\end{aligned}$$

で与えられる．G_k $(k=1,2,3,4)$ を適当に η の冪で割ることにより，P_k $(k=1,2,3,4)$ が得られる．

M の WKB 解の Borel 変換は $u_\ell := -\varpi_\ell$ に特異点を持ち，$u=u_\ell$ $(\ell=1,2,3)$ は，次の 3 次方程式を満たす:

$$256u^3 - 128x_2u^2 + 16x_2(9x_1^2 + x_2^3)^2 u - x_1^2(27x_1^2 + 4x_2^3) = 0.$$

したがって，M の Stokes 集合 $\mathcal{S}$ は，上の方程式の根を用いて次のように書ける:

$$\mathcal{S} = \bigcup_{j \neq k} \left\{ (x_1, x_2) \in \mathbb{C}^2 \mid \operatorname{Im}(u_j - u_k) = 0 \right\}.$$

M_B の singular locus は，グレブナー基底の理論 [21] を用いることにより，

$$\{(x_1, x_2, y) \in \mathbb{C}^3 \mid 256u^3 - 128x_2u^2 + 16x_2(9x_1^2 + x_2^3)^2 u - x_1^2(27x_1^2 + 4x_2^3) = 0\}$$

と書ける．これは，$z^4 + x_2z^2 + x_1z + y$ の (z に関する) 判別式の零点集合と一致する．

Pearcey 積分の議論に戻る．Pearcey 積分 (1) は，変数変換 $y = -(z^4 + x_2z^2 + x_1z)$ を施すことにより，Laplace 積分の形に書き換えることができる:

$$\int \exp(-\eta y) g\,(x_1, x_2, y)\, dy. \tag{12}$$

ただし，

$$g\,(x_1, x_2, y) = - \left. \frac{1}{4z^3 + 2x_2z + x_1} \right|_{z = z(x_1, x_2, y)}$$

とし，$z = z(x_1, x_2, y)$ は方程式 $z^4 + x_2z^2 + x_1z + y = 0$ の根とする．Laplace 積分 (12) は WKB 解の Borel 和の形に似ていることより，M に対する WKB 解の Borel 変換 $\psi_{\ell,B}$ は g を用いて表すことができると期待される [1]．[12, 25] では，x_2 が固定されているとき，(12) は (4) の WKB 解の Borel 和に対応することが示されている．

Lemma 9 ([5, 6])**.** *函数 g は次の方程式により定義される代数函数とする:*

$$\begin{aligned}(4x_1^2x_2(36y - x_2^2) + 16y(x_2^2 - 4y)^2 - 27x_1^4)\, g^4 \\ + 2(-8x_2y + 2x_2^3 + 9x_1^2)\, g^2 - 8x_1g + 1 = 0.\end{aligned} \tag{13}$$

このとき，g は M_B の解である．

4 次方程式 (13) は 4 つの根 g_k $(k=1,2,3,4)$ を持ち，これらは $g_1 + g_2 + g_3 + g_4 = 0$ を満たす．

Theorem 10 ([5, 6])**.** *WKB 解の Borel 変換 $\psi_{\ell,B}$ $(\ell = 1,2,3)$ は，(13) で定まる代数函数の一次結合で書ける．特に，$\psi_{\ell,B}$ は代数函数であり，ψ_ℓ は resurgent（Borel 総和可能）である．*

5 接続公式

本節では, M の WKB 解の Borel 変換が代数函数の一次結合で明示的に表すことができることを説明する. その後, 接続公式について説明する. M の WKB 解の Borel 変換は, 擬斉次性の方程式 $P_{4,B}\psi_{\ell,B} = 0$ を満たすので,

$$\psi_{\ell,B}\left(\lambda^3 x_1, \lambda^2 x_2, \lambda^4 y\right) = \lambda^{-3}\psi_{\ell,B}\left(x_1, x_2, y\right) \qquad (\lambda \neq 0)$$

が成り立つ. したがって, $x_1 \neq 0$ のとき,

$$\psi_{\ell,B}\left(1, \frac{x_2}{x_1^{2/3}}, \frac{y}{x_1^{4/3}}\right) = x_1\psi_{\ell,B}\left(x_1, x_2, y\right).$$

が成り立つ. よって, 新しい変数 s, t を導入する:

$$(s,t) = \left(\frac{y}{x_1^{4/3}}, \frac{x_2}{x_1^{2/3}}\right).$$

$p_\ell = \dfrac{3}{4^{4/3}}e^{\frac{2\pi i}{3}\ell}$ $(\ell = 1,2,3)$ とおく. $x_1\psi_{\ell,B}\big|_{t=0}$ を点 $s = p_\ell$ で展開すると,

$$\begin{aligned} x_1\psi_{\ell,B}\big|_{t=0} = &-\frac{2^{1/6}}{\sqrt{3\pi}}e^{-\frac{2\pi i}{3}\ell}\left(s-p_\ell\right)^{-1/2} \\ &\times\left(1 - \frac{7}{9\cdot 2^{1/3}}e^{-\frac{2\pi i}{3}\ell}\left(s-p_\ell\right) + \frac{385}{486\cdot 2^{2/3}}e^{\frac{2\pi i}{3}\ell}\left(s-p_\ell\right)^2 + O\left(\left(s-p_\ell\right)^3\right)\right) \end{aligned}$$

を得る. ただし, $s - p_\ell$ の branch は, $s \in \mathbb{C}\setminus\{p_\ell\}$ $(\ell = 1,2,3)$ に対して

$$-\pi < \arg\left(s - p_\ell\right) \leq \pi$$

として選ぶ.

一方, (13) で定義される代数函数 g は, Lemma 9 より $\psi_{\ell,B}$ と同様な擬斉次性を持つことがわかる. したがって, $x_1 g\left(x_1, x_2, y\right)$ は変数 (s,t) の函数と見做すことができ, それを $h(s,t)$ と表すことにする. 簡単な計算により, $h = h(s,t)$ は次の 4 次方程式を満たすことがわかる:

$$(256s^3 - 128s^2t^2 + 16st(t^3+9) - 4t^3 - 27)h^4 + \left(4t^3 - 16st + 18\right)h^2 - 8h + 1 = 0. \tag{14}$$

原点近傍における代数函数 h の branch h_j $(j = 1,2,3,4)$ を次のように定める:

$$\begin{aligned} h_1(s,t) &= \frac{1}{3} + \frac{4}{9}e^{-\frac{2\pi i}{3}}s + \frac{2}{9}e^{\frac{2\pi i}{3}}t + \cdots, \\ h_2(s,t) &= \frac{1}{3} + \frac{4}{9}e^{\frac{2\pi i}{3}}s + \frac{2}{9}e^{-\frac{2\pi i}{3}}t + \cdots, \\ h_3(s,t) &= \frac{1}{3} + \frac{4}{9}s + \frac{2}{9}t + \cdots, \\ h_4(s,t) &= -1 - 2st - 4s^3 + \cdots. \end{aligned} \tag{15}$$

代数函数 h の $t=0$ への制限を考えると, $h(s,0)$ は点 $s=p_\ell$ $(\ell=1,2,3)$ に特異点を持つことがわかる. 代数函数 h を点 $s=p_\ell$ で Puiseux 展開することにより, $s=p_\ell$ 近傍における代数函数 h の branch $h_j^{(\ell)}(s,0)$ $(j=1,2,3,4;\ell=1,2,3)$ を次のように定める:

$$\begin{aligned}
h_1^{(\ell)}(s,0) &= \frac{1}{2^{5/6}\sqrt{3}}e^{-\frac{2\pi i}{3}\ell}(p_\ell-s)^{-1/2}+O(1),\\
h_2^{(\ell)}(s,0) &= -\frac{1}{2^{5/6}\sqrt{3}}e^{-\frac{2\pi i}{3}\ell}(p_\ell-s)^{-1/2}+O(1),\\
h_3^{(\ell)}(s,0) &= \frac{4+i\sqrt{2}}{18}+O(p_\ell-s),\\
h_4^{(\ell)}(s,0) &= \frac{4-i\sqrt{2}}{18}+O(p_\ell-s).
\end{aligned}\tag{16}$$

ただし, $p_\ell-s$ の branch は, $s\in\mathbb{C}\setminus\{p_\ell\}$ $(\ell=1,2,3)$ に対して

$$-\pi<\arg(p_\ell-s)\leq\pi$$

として選ぶ. 次の補題は, これらの branch がどのように対応しているかを主張するものである.

Lemma 11 ([6])**.** 次が成り立つ:

$$\begin{aligned}
h_1(s,0) &= h_4^{(3)}(s,0)=h_2^{(1)}(s,0)=h_3^{(2)}(s,0),\\
h_2(s,0) &= h_3^{(3)}(s,0)=h_4^{(1)}(s,0)=h_2^{(2)}(s,0),\\
h_3(s,0) &= h_1^{(3)}(s,0)=h_3^{(1)}(s,0)=h_4^{(2)}(s,0),\\
h_4(s,0) &= h_2^{(3)}(s,0)=h_1^{(1)}(s,0)=h_1^{(2)}(s,0).
\end{aligned}\tag{17}$$

ただし, $s\in\Sigma_1\cup\Sigma_2\cup\Sigma_3$ とし,

$$\begin{aligned}
\Sigma_1 &= \{e^{2\pi i/3}\sigma \mid 0<\sigma<p_3\},\\
\Sigma_2 &= \{e^{4\pi i/3}\sigma \mid 0<\sigma<p_3\},\\
\Sigma_3 &= \{\sigma \mid 0<\sigma<p_3\}
\end{aligned}$$

とする.

$g_j=h_j/x_1$ $(j=1,2,3,4)$, $g_j^{(\ell)}=h_j^{(\ell)}/x_1$ $(j=1,2,3,4;\ell=1,2,3)$ とおく. $|x_2|$ が十分に小さいとき, Lemma 11 より

$$\begin{aligned}
g_1 &= g_4^{(3)}=g_2^{(1)}=g_3^{(2)},\\
g_2 &= g_3^{(3)}=g_4^{(1)}=g_2^{(2)},\\
g_3 &= g_1^{(3)}=g_3^{(1)}=g_4^{(2)},\\
g_4 &= g_2^{(3)}=g_1^{(1)}=g_1^{(2)}
\end{aligned}\tag{18}$$

が成り立つ.

Theorem 12 ([6])**.** $|x_2|$ は十分に小さいと仮定する. このとき, *WKB* 解の *Borel* 変換 $\psi_{\ell,B}$ は, 次のような形で書くことができる:

$$\psi_{\ell,B}=\frac{i}{\sqrt{\pi}}(-1)^{\ell-1}(g_\ell-g_4)\quad(\ell=1,2,3).\tag{19}$$

Theorem 12 を用いることにより, M に対する WKB 解の (Borel 和の) 接続公式が得られる [6]. 具体例については講演中に紹介する. x_2 を 0 でない定数 c に制限すると, BNR 方程式 [7] と呼ばれる常微分方程式

$$(4\partial_x^3 + 2c\partial_x + x)\psi = 0$$

が得られる. この常微分方程式の WKB 解は resurgent (Borel 総和可能) であり, Pearcey 系の場合と同様な主張を得ることができる.

References

[1] 青木貴史, ホロノミー系の完全 WKB 解析に向けて, 数理解析研究所講究録, **1433** (2005), 1–8.

[2] Aoki, T., Kawai, T. and Takei,Y., The Bender-Wu analysis and the Voros theory, Special Functions, ICM-90 Satellite Conference Proceedings, Springer, 1991, 1–29.

[3] Aoki, T., Kawai, T. and Takei, Y., New turning points in the exact WKB analysis for higher order ordinary differental equations, Analyse algébrique des perturbations singulières, I, Méthodes résurgentes, Hermann, (1994), 69–84.

[4] Aoki, T., Kawai, T., Koike, T., Takei, Y., On the exact WKB analysis of operators admitting infinitely many phases, Adv. in Math., **181** (2004), 165–189.

[5] Aoki, T., Suzuki, T. and Uchida, S., An elementary proof of the Voros connection formula for WKB solutions to the Airy equation with a large parameter, to appear in RIMS Kôkyûroku Bessatsu.

[6] Aoki, T., Suzuki, T. and Uchida, S., The Borel transform of the WKB solution to the Pearcey system, submitted, arXiv:2205.02988.

[7] Berk, H. L., Nevins, W. M. and Roberts, K. V., New Stokes' line in WKB theory, J. Math. Phys., **23** (1982), 988–1002.

[8] Ecalle, J., Cinq applications des fonctions résurgentes, Prepublication d'Orsay, **84** (1984).

[9] Hirose, S., Exact WKB analysis for a holonomic system satisfied by the Pearcey integral (in Japanese), Master's thesis, Kyoto University.

[10] Hirose, S., On the Stokes geometry for the Pearcey system and the (1,4) hypergeometric system, RIMS Kôkyûroku Bessatsu, **B40** (2013), 243–292.

[11] Hirose, S., Exact WKB analysis of a differential system satisfied by an oscillatory integral related to a simple singularity of type A, to appear in RIMS Kôkyûroku Bessatsu.

[12] Honda, N., Kawai, T. and Takei, Y., Virtual Turning Points, SpringerBriefs in Mathematical Physics (2015).

[13] Iwaki, K., Koike, T. and Takei, Y.-M., Voros coefficients for the hypergeometric differential equations and Eynard-Orantin's topological recursion: Part II: For confluent family of hypergeometric equations, Journal of Integrable Systems, **4** (2019), 1–46.

[14] Iwaki, K. and Nakanishi, T., Exact WKB analysis and cluster algebras, J. Phys. A: Math. Theor., **47** (2014).

[15] Kashiwara, M., On the holonomic systems of linear differential equations, II, Inventiones mathematicae, **49** (2) (1978), 121–135.

[16] Kawai, T. and Takei, Y., Algebraic Analysis of Singular Perturbation Theory, American Mathematical Society (2005).

[17] Lando, S. K., Geometry of the Stokes sets of families of functions of one variable, J. Math. Sci., **83** (4) (1997), 534–538.

[18] Okamoto, K. and Kimura, H., On particular solutions of the Garnier systems and the hypergeometric functions of several variables, Quart. J. Math., **37** (1986), 61–80.

[19] Olver, F. W. J. et al., NIST Handbook of Mathematical Functions, Cambridge University Press (2010).

[20] Oaku, T., Computation of the characteristic variety and the singular locus of a system of differential equations with polynomial coefficients, Japan J. Indust. Appl. Math., **11** (1994), 485–497.

[21] 大阿久俊則, グレブナ基底と線型偏微分方程式系 (計算代数解析入門), 上智大学数学講究録, **38** (1994); WEB 公開用改訂版, (2014).

[22] Pearcey, T., The structure of an electromagnetic field in the neighbourhood of a cusp of a caustic, Phil. Mag., **37** (1946), 311–317.

[23] 佐藤幹夫, 青木貴史, 河合隆裕, 竹井義次, 特異摂動の代数解析, 数理解析研究所講究録, **750** (1991), 43–51.

[24] Schwarz, H. A., Ueber diejenigen Fälle in welchen die Gaussische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt, Journal für die reine und angewandte Mathematik, **75** (1873), 292–335.

[25] Takei, Y., Integral representation for ordinary differential equations of Laplace type and exact WKB analysis (Exact steepest descent method), RIMS Kôkyûroku, **1168** (2000), 80–92.

[26] Voros, A., The return of the quartic oscillator – The complex WKB method, Ann. Inst. Henri Poincaré, **39** (1983), 211–338.

不定値グラスマン多様体上のコホモロジーの同型について

関口英子 (東京大学大学院数理科学研究科)

1. 序

本稿の主役は，$k \leq p+q$ に対して定まる不定値グラスマン多様体 $X = Gr_k^+(\mathbb{C}^{p,q})$ 上の $\overline{\partial}$ コホモロジーである．X は非コンパクトであり，このコホモロジー空間は無限次元の Frechét 空間となる．

ここで用いた記号を説明する．いま，$\mathbb{C}^{p,q}$ を符号 (p,q) の不定値計量

$$(z,z) = |z_1|^2 + \cdots |z_p|^2 - |z_{p+1}|^2 - \cdots - |z_{p+q}|^2$$

を備えた $p+q$ 次元の複素ベクトル空間とし，不定値グラスマン多様体 $X = Gr_k^+(\mathbb{C}^{p,q})$ を

$$Gr_k^+(\mathbb{C}^{p,q}) = \{\mathbb{C}^{p,q} \text{ の maximally positive な } k \text{ 次元部分空間}\}.$$

と定める．X はグラスマン多様体 $Gr_k(\mathbb{C}^{p+q}) = \{\mathbb{C}^{p+q}$ の k 次元部分空間$\}$ における開集合として複素多様体の構造をもつ．さらに，

$$\begin{aligned} &X \text{ はコンパクト} &&\iff q = 0 \text{ または } k \in \{0, p+q\} \\ &X \text{ はシュタイン多様体} &&\iff p = k \end{aligned}$$

となるので，X は，一般には，非コンパクトかつ非シュタイン複素多様体である．単純リー群である不定値ユニタリ群

$$G := SU(p,q) = \{g \in SL(p+q, \mathbb{C}) : \overline{{}^t g}\, I_{p,q}\, g = I_{p,q}\}$$

は不定値グラスマン多様体 $X = Gr_k^+(\mathbb{C}^{p,q})$ に双正則かつ推移的に作用する．X は G の等質空間として

$$Gr_k^+(\mathbb{C}^{p,q}) \simeq G/L_k$$

第 63 回実函数論・函数解析学合同シンポジウム，2024 年 9 月 9 日 (月)–11 日 (水), 東京大学駒場キャンパス・数理科学研究科棟・大講義室，
代表者: 伊藤健一，佐々木格，鈴木智成.

と表される．ここで，L_k は次の式で定義される G の部分群である．

$$L_k = \begin{cases} S(U(k)\times U(p-k,q)) & (0\le k\le p), \\ S(U(p,k-p)\times U(p+q-k)) & (p\le k\le p+q). \end{cases}$$

$k\neq 0, p+q$ のとき，X 上の G 同変な正則直線束は $\lambda\in\mathbb{Z}$ で分類される．すなわち，固定部分群 L_k の一次元表現 $\mathbb{C}_\lambda$ を

$$\det{}^\lambda \boxtimes \mathbf{1}\colon L_k \ni (A,B)\mapsto (\det A)^\lambda \in \mathbb{C}^\times.$$

と定め，$\mathcal{L}_\lambda$ を同伴束

$$\mathcal{L}_\lambda := G\times_{L_k}\mathbb{C}_\lambda \to G/L_k \simeq Gr_k^+(\mathbb{C}^{p,q})$$

として定義するのである．$X = Gr_k^+(\mathbb{C}^{p,q})$ の複素多様体としての標準直線束 K_X はこの記法で $\mathcal{L}_{p+q}$ と表される．

さて，$q=0$ の場合は G はコンパクト群 $SU(p)$ となり，古典的な Borel–Weil–Bott の定理により，

$$H^i_{\bar\partial}(X,\mathcal{L}_\lambda) = \begin{cases} F^G((\lambda-p-q)\omega_k) & i = k(p-k) \\ 0 & i\neq k(p-k) \end{cases} \tag{1.1}$$

となる．ここで $F^G(\ell\omega_k)$ は $\ell\omega_k = \ell\,(\underbrace{1,\dots,1}_{k},\underbrace{0,\dots,0}_{p+q-k})$ を最高ウェイトとする G の既約表現である．これは有限次元表現であり，その次元は $\prod_{i=1}^{k}\prod_{j=1}^{p+q-k}(\ell+i+j-1)$ となる．

以下では，$1\le p,q$ かつ $0\le k\le \min(p,q)$ とし，$X = Gr_k^+(\mathbb{C}^{p,q})$ と $Y := Gr_{p+q-k}^+(\mathbb{C}^{p,q})$ という 2 つの複素多様体を同時に考える．$\lambda,\mu\in\mathbb{Z}$ に対して，2 つの G 同変な正則直線束を考えよう:

$$\begin{array}{ccccccc} G\times_{L_k}\mathbb{C}_\lambda & \simeq & \mathcal{L}_\lambda & & \mathcal{L}_\mu & \simeq & G\times_{L_{p+q-k}}\mathbb{C}_\mu \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ X := G/L_k & \simeq & Gr_k^+(\mathbb{C}^{p,q}) & & Gr_{p+q-k}^+(\mathbb{C}^{p,q}) & \simeq & G/L_{p+q-k} =: Y \end{array}$$

$p,q\ge 1$ なので，$G = SU(p,q)$ は非コンパクトであり，(1.1) の類似として得られる無限次元の表現は，パラメータが代数的表現論でいうところの good range ([14]) ならば，一般論 (Zuckerman, Speh–Vogan, Beilinson–Bernstein 他) により，かなり良く理解されている．一般論から得られる事実を命題として整理しておく．

命題 1. $\lambda, \mu \geq p+q$，$x := k(p-k)$，$y := k(q-k)$ とおく.

(1) $H^i_{\overline{\partial}}(X, \mathcal{L}_\lambda) = \begin{cases} 0 & i \neq x, \\ SU(p,q) \text{ の表現として既約} & i = x. \end{cases}$

(2) $H^j_{\overline{\partial}}(Y, \mathcal{L}_\mu) = \begin{cases} 0 & i \neq y, \\ SU(p,q) \text{ の表現として既約} & i = y. \end{cases}$

(3) (1), (2) の 0 でない cohomology は $SU(p,q)$ の表現として，互いに同値ではない.

パラメータが good range の範囲では，コンパクト リー群の Borel–Weil–Bott 定理の無限次元版として想像しやすい形の類似が成り立っているといえる．ところが，パラメータが good range から外れると G がコンパクトの場合 ($p=0$ または $q=0$) の有限次元のコホモロジー空間と G が非コンパクトの場合 ($p, q \geq 1$) の無限次元のコホモロジー空間とでは大きな差異が出る．すなわち，G がコンパクトの場合 ($q=0$) の (1.1) では $\lambda \geq p+q$ の仮定を外して，例えば $\lambda = p+q-1$ とすると全ての次数のコホモロジーが消滅してしまうが，G が非コンパクトの場合の命題 1 で λ, $\mu \geq p+q$ の仮定を緩めても x 次 (あるいは y 次) のコホモロジーはすぐには消滅しない．さらに，$(\lambda, \nu) = (p,q)$ という特異パラメータにおいては，以下の不思議な現象が生じる.

定理 2 (Twistor 変換)**.** $0 \leq k \leq \min(p,q)$ とする.
このとき，2 つの Fréchet 空間 $H^{k(p-k)}_{\overline{\partial}}(X, \mathcal{L}_p)$ と $H^{k(q-k)}_{\overline{\partial}}(Y, \mathcal{L}_q)$ との間に '自然な' 位相同型写像が存在する．さらに，この位相同型写像は $G = SU(p,q)$ の自然な作用の絡作用素となっている:

$$H^{k(p-k)}_{\overline{\partial}}(X, \mathcal{L}_p) \xrightarrow[\Psi]{\sim} H^{k(q-k)}_{\overline{\partial}}(Y, \mathcal{L}_q).$$

2. 軌道法からの観点

この節と次節では，Kirillov–Kostant–Duflo–Vogan の軌道法の観点から定理 2 の意味を考察する.

一般に，G をリー群とし,

$$\widehat{G} := \{G \text{ の既約ユニタリ表現の同値類からなる集合}\}$$

とおく．$\widehat{G}$ は G の**ユニタリ双対**と呼ばれる.

一方，$\mathfrak{g}$ を G のリー代数とし，随伴表現 $\mathrm{Ad}\colon G \to GL(\mathfrak{g})$ の反傾表現を $\mathrm{Ad}^*\colon G \to GL(\mathfrak{g}^*)$ とする．このとき，$\mathfrak{g}^*/\mathrm{Ad}^*(G)$ は**余随伴軌道**の集合を表す．

Kirillov の軌道法は，1 つの有限次元表現に付随した余随伴軌道の空間 $\mathfrak{g}^*/\mathrm{Ad}^*(G)$ が，すべての既約ユニタリ表現のなす集合と深い関係があるというものである．

$$\mathfrak{g}^*/\mathrm{Ad}^*(G) \fallingdotseq \widehat{G} \tag{2.1}$$

G が単連結冪零リー群ならば (2.1) は自然な全単射である (Kirillov, 1962; 藤原 [2])．一方，G が $SU(p,q)$ のような単純リー群の場合は，ユニタリ双対 $\widehat{G}$ は完全には分類されていないが，少なくとも (2.1) の左辺に適当な整数条件を付け加えた程度では，functorial な全単射が得られないことは長年にわたって，多くの専門家によって指摘されてきた．例えば，補系列表現は軌道法の枠組みに入れるのが特に難しいと認識されている．[1] このような側面を含めて，軌道法はユニタリ双対 $\widehat{G}$ の全貌の理解を助ける方向に深化を続けている．

さて，(2.1) という対応が (部分的にでも) 存在するとすれば，その余随伴軌道 $\mathcal{O}_\lambda = \mathrm{Ad}^*(G)\lambda$ に対して，G のある既約ユニタリ表現 π_λ が対応することになる．一方，余随伴軌道 $\mathcal{O}_\lambda$ には Kostant–Kirillov–Souriau のシンプレクティック形式によりシンプレクティック多様体の構造が入り，G の余随伴作用はハミルトン的になる．従って $\mathcal{O}_\lambda \rightsquigarrow \pi_\lambda$ はシンプレクティック多様体の**幾何的量子化**と見なされる．

模式的に書くとすれば，

$$\mathcal{O}_\lambda = \mathrm{Ad}^*(G)\lambda \mapsto \pi_\lambda := Q(\mathcal{O}_\lambda)$$

によって幾何的量子化

$$Q\colon \mathfrak{g}^*/\mathrm{Ad}^*(G) \dashrightarrow \widehat{G}$$

が $\mathfrak{g}^*/\mathrm{Ad}^*(G)$ の適当な部分集合上で定義されると期待するのである．

[1]最近，ローレンツ群のすべての補系列表現を幾何的量子化によって構成し，軌道法 (2.1) に付加データを与えることで，軌道法の新しい解釈と深化を与えるという結果も得られている ([3])．

3. 余随伴軌道の幾何的量子化

G が半単純リー群のときは Killing form を使って，リー代数 $\mathfrak{g}$ とその双対 $\mathfrak{g}^*$ を同一視することができる．$\mathfrak{g}^* \leftrightarrow \mathfrak{g}$, $\lambda \leftrightarrow H_\lambda$ と対応しているとき，余随伴軌道 $\mathcal{O}_\lambda = \mathrm{Ad}^*(g)\lambda$ に対して

$$\mathcal{O}_\lambda \text{ が楕円軌道} \iff \mathrm{ad}(H_\lambda) \in \mathrm{End}(\mathfrak{g}_{\mathbb{C}}) \text{ は対角化可能で，}$$
$$\text{すべての固有値が純虚数.}$$

と定義すると，λ が適当な整数条件と positivity をみたすとき，

$$\text{楕円型余随伴軌道} \qquad \mathcal{O}_\lambda = \mathrm{Ad}^*(G)\lambda = G/G_\lambda \subset \mathfrak{g}^*.$$

の幾何的量子化 $\pi_\lambda := Q(\mathcal{O}_\lambda)$ は

$$\begin{array}{ccl} \mathcal{O}_\lambda & \rightsquigarrow & \text{正則直線束 } \mathcal{L}_\lambda = G \underset{G_\lambda}{\times} \mathbb{C}_\lambda \to \mathcal{O}_\lambda \\ & \underset{\text{Okamoto, Schmid}}{\rightsquigarrow} & \text{Fréchet 表現 } G \curvearrowright H^*_{\bar\partial}(\mathcal{O}_\lambda, \mathcal{L}_\lambda), \\ & \underset{\text{Vogan, Wallach}}{\rightsquigarrow} & \text{ユニタリ表現 } \pi_\lambda \text{ of } G \end{array}$$

として得られる (詳しくは [5] の解説参照).

例 1. G がコンパクトのときは $\pi_\lambda = Q(\mathcal{O}_\lambda)$ は既約有限次元表現の Borel–Weil–Bott の構成法である．

例 2. 任意の Harish-Chandra 離散系列表現は λ が regular かつ strongly elliptic ($\Leftrightarrow$ G_λ compact トーラス) のときの $\pi_\lambda = Q(\mathcal{O}_\lambda)$ として構成される．

そこで $\pi_\lambda = Q(\mathcal{O}_\lambda)$ が '自然' に定まる楕円軌道 $\mathcal{O}_\lambda$ の全体を $[\mathfrak{g}^*_{\mathrm{ell}}]$ とおき，次の問題を考える．

問 1. 幾何的量子化 Q は $[\mathfrak{g}^*_{\mathrm{ell}}]$ 上で単射か?

問 1 を正確に述べるためには,「ρ シフト」といった正規化を幾何的量子化においてどのように取り込むかを決めなければならないが，上の問の答えは一般には No である．例えば G がコンパクト群のときの自明な 1 次元表現は，旗多様体でも退化した旗多様体でも自明な直線束の切断の空間に自然に実現される (Liouville の定理)．このような,「ほぼ自明な」反例が問 1 には起こり得るが，それに起因する「やや非自

明な」ケースとして，より一般に，コンパクトなファイバーをもつ G が作用する複素解析的なファイブレーション

$$\begin{tikzcd}
\mathcal{O}_\lambda \arrow[dr] & & \mathcal{O}_\mu \arrow[dl] \\
& Z &
\end{tikzcd}$$

に付随するコホモロジーのスペクトル列が退化することによって生じる同型 $Q(\mathcal{O}_\lambda) \simeq Q(\mathcal{O}_\mu)$ も存在する．このように広い意味でコンパクト群の Borel–Weil–Bott の定理に帰着できる G 同型を “elementary な同型” ということにする．そこで問 1 を精密化して

問 2. 幾何的量子化 Q は (“elementary な同型” を除くと) $[\mathfrak{g}^*_{\mathrm{ell}}]$ 上，単射になるか？

という問題を考える．代数的表現論の結果を用いることで，問 2 はパラメータが good range に入っていれば肯定的であることが分かる ([10, Thm. 4.1])．従って問 2 に否定的な場合が存在するとすれば，λ, μ が good range に属さない特異なパラメータの場合になる．

定理 2 の主張をこの文脈で解釈すると，自然な量子化写像 Q は “elementary な同型” ではないのに単射にはならないことが実際にあり得る，すなわち，問 2 の反例があることが分かる．

この様子を見てみよう．冒頭で定義した不定値グラスマン多様体 $Gr_k^+(\mathbb{C}^{p,q})$ は $G = SU(p,q)$ の余随伴軌道と同一視するために，次のような対角行列 E_k をとる:

$$E_k := \sqrt{-1}\,\mathrm{diag}(\underbrace{1,\ldots,1}_{k},\underbrace{0,\ldots,0}_{p+q-k}) - \frac{\sqrt{-1}k}{p+q} I_{p+q} \in \mathfrak{g}.$$

このとき $\mathrm{ad}(E_k) \in \mathrm{End}(\mathfrak{g})$ は半単純でその固有値はすべて純虚数となる．従って，$\lambda, \mu > 0$ とするとき，随伴軌道

$$\begin{aligned}
\mathcal{O}_\lambda &:= \mathrm{Ad}(G)(\lambda E_k) \qquad \subset \mathfrak{g} \\
\mathcal{O}_\mu &:= \mathrm{Ad}(G)(\mu E_{p+q-k}) \subset \mathfrak{g}
\end{aligned}$$

はいずれも (楕円型) 随伴軌道であり，固定部分群がそれぞれ L_k, L_{p+q-k} と一致することから，$\mathcal{O}_\lambda$ は $Gr_k^+(\mathbb{C}^{p,q})$ と $\mathcal{O}_\mu$ は $Gr_{p+q-k}^+(\mathbb{C}^{p,q})$ と同型

となる．定理 2 は適当な正整数の組 (λ, μ) を選んだとき，$\mathcal{O}_\lambda$ と $\mathcal{O}_\mu$ の幾何的量子化である 2 つのユニタリ表現の間に，

$$Q(\mathcal{O}_\lambda) \simeq Q(\mathcal{O}_\mu)$$

というユニタリ同値が成り立つことを主張しているのである．

一方，$p \neq q$ ならば $\mathcal{O}_\lambda$ と $\mathcal{O}_\mu$ は双正則ではない．さらに強く，コンパクトなファイバーをもつ複素解析的な G ファイブレーション

$$\begin{tikzcd} \mathcal{O}_\lambda \arrow[dr] & & \mathcal{O}_\mu \arrow[dl] \\ & Z & \end{tikzcd}$$

も存在しない，すなわち，G 同型 $Q(\mathcal{O}_\lambda) \simeq Q(\mathcal{O}_\mu)$ は 'elementary な同型' ではない (λ と μ は good range ではないことに注意する)．このようにして，定理 2 は問 2 に否定的な例を与えているのである．

4. 定理 2 の証明のスケッチ

定理 2 の証明のアイディアを述べる．定理 2 の同型は抽象的な同型ではなく (一般化された) Penrose 変換を組み合わせて幾何的に説明することができる．鍵になるのは，(一般化された) Penrose 変換である ([1, 8])．

以下では，X と Y という 2 つの複素多様体のコホモロジー空間上に実現された G 加群

$$H^*_{\bar\partial}(X, \mathcal{L}_\lambda) \text{ と } H^*_{\bar\partial}(Y, \mathcal{L}_\mu),$$

を比較する．X と Y には直接の射はないが，3 つの複素多様体 X', Ω, Y' を準備し，次の G 複素多様体のファイブレーションを考える:

$$\begin{tikzcd} & {}^\exists X' \arrow[dl, "\alpha"'] \arrow[dr, "u"] & & {}^\exists Y' \arrow[dl, "v"'] \arrow[dr, "\beta"] & \\ X & & {}^\exists\Omega & & Y \end{tikzcd}$$

この図式で，左端の X におけるコホモロジーと右端の Y におけるコホモロジーを真ん中の Ω に持ってくると，同じ微分方程式の大域解になるという方針で定理 2 を示す．

(X' と Y' は後述するがそれぞれ (X,Ω), (Ω,Y) に対する Chern fibration になっており，さらに ファイバー α と β は非コンパクトかつ可縮，u と v はコンパクトなファイバーとなる.)

この方針に現れた記号について，まず真ん中の Ω から説明する．$M(q,p;\mathbb{C})$ を $q\times p$ 次の複素行列からなる空間とし，有界対称領域 Ω を

$$\Omega := \{Z\in M(q,p;\mathbb{C}) : I_q - ZZ^* \gg 0\}$$

と定める．Ω は $G=SU(p,q)$ に付随するエルミート対称空間 G/K と表せることに注意しよう.

自然数 $k\in\{0,1,2,\ldots,\min(p,q)\}$ に対して, $(\mathcal{M}_k)$ により，以下の $k+1$ 斉次の小行列式型の偏微分方程式系を表すものとする:

$$(\mathcal{M}_k) \qquad \det\left(\frac{\partial}{\partial z_{ij}}\right)_{\substack{i\in I\\ j\in J}} F(Z)=0 \qquad Z=(z_{ij})_{\substack{i\in I\\ j\in J}}$$

ここで I と J は

$$I\subset\{1,2,\ldots,q\},\quad J\subset\{1,2,\ldots,p\},\quad \sharp I=\sharp J=k+1$$

をみたす部分集合を表し，$\frac{\partial}{\partial z_{ij}}$ は holomorphic な微分作用素である．

Ω 上の大域解の空間を

$$\mathcal{S}ol(\Omega,\mathcal{M}_k)\equiv\mathcal{S}ol(\mathcal{M}_k) := \{F(Z)\in\mathcal{O}(\Omega) : F \text{ は } (\mathcal{M}_k) \text{ の解}\}.$$

と定める．

例 **3** ($p=4$, $q=3$ の場合): $G=SU(4,3)$)．

$$\frac{\partial}{\partial Z}=\begin{pmatrix} \frac{\partial}{\partial z_{11}} & \frac{\partial}{\partial z_{12}} & \frac{\partial}{\partial z_{13}} & \frac{\partial}{\partial z_{14}} \\ \frac{\partial}{\partial z_{21}} & \frac{\partial}{\partial z_{22}} & \frac{\partial}{\partial z_{23}} & \frac{\partial}{\partial z_{24}} \\ \frac{\partial}{\partial z_{31}} & \frac{\partial}{\partial z_{32}} & \frac{\partial}{\partial z_{33}} & \frac{\partial}{\partial z_{34}} \end{pmatrix}\equiv\begin{pmatrix} \partial_{11} & \partial_{12} & \partial_{13} & \partial_{14} \\ \partial_{21} & \partial_{22} & \partial_{23} & \partial_{24} \\ \partial_{31} & \partial_{32} & \partial_{33} & \partial_{34} \end{pmatrix}$$

1) $k=0$ の場合. 微分方程式 $(\mathcal{M}_k)$ は 1 次の微分作用素で定義され，$\mathcal{S}ol(\Omega,\mathcal{M}_k)$ は Ω 上の定数関数のみからなる 1 次元空間となる．

2) $k=1$ の場合．微分方程式 $(\mathcal{M}_k)$ は 2 次の微分作用素で定義され，$\mathcal{S}ol(\Omega, \mathcal{M}_2)$ は多重調和函数の空間となる．

3) $k=2$ の場合．微分方程式 $(\mathcal{M}_k)$ は 3 次の微分作用素で定義され，次の形の微分方程式の系となる:

$$\det\begin{pmatrix}\partial_{11} & \partial_{12} & \partial_{13}\\ \partial_{21} & \partial_{22} & \partial_{23}\\ \partial_{31} & \partial_{32} & \partial_{33}\end{pmatrix}F=\det\begin{pmatrix}\partial_{11} & \partial_{12} & \partial_{14}\\ \partial_{21} & \partial_{22} & \partial_{24}\\ \partial_{31} & \partial_{32} & \partial_{34}\end{pmatrix}F=\det\begin{pmatrix}\partial_{11} & \partial_{13} & \partial_{14}\\ \partial_{21} & \partial_{23} & \partial_{24}\\ \partial_{31} & \partial_{33} & \partial_{34}\end{pmatrix}F=\det\begin{pmatrix}\partial_{12} & \partial_{13} & \partial_{14}\\ \partial_{22} & \partial_{23} & \partial_{24}\\ \partial_{32} & \partial_{33} & \partial_{34}\end{pmatrix}F=0.$$

これに付随した "3 階の偏微分方程式系で定義された多変数の青本–Gelfand 超幾何方程式をさらに一般化した方程式の解の次元の挙動" については [7] や落合–Zunderiya [6] の研究がある．

4) $k\geq 3$ の場合．$(\mathcal{M}_k)=\emptyset$.

一般の設定に戻る．X のコンパクト部分多様体 $C_X = Gr_k(\mathbb{C}^p)$ を左移動して得られるコンパクト部分多様体の族 (サイクル空間)

$$\{g\cdot C_X : g\in G\}$$

は Ω によってパラメトライズされる．同様に，Y のコンパクト部分多様体 $C_Y = Gr_{q-k}(\mathbb{C}^q)$ を左移動して得られる Y のコンパクト部分多様体の族 (サイクル空間)

$$\{g\cdot C_Y : g\in G\}$$

も同じ空間 Ω によってパラメトライズされる．

X 上のコホモロジーを $g\cdot C_X$ 上で積分することによって得られる写像を $\mathcal{R}_k$ と表す．すなわち，$\mathcal{R}_k$ は

$$\mathcal{R}_k\colon H^{k(p-k)}_{\overline{\partial}}(X,\mathcal{L}_p) \longrightarrow C^\infty(\Omega)$$

という写像である．同様に

$$\mathcal{R}_{p+q-k}\colon H^{k(q-k)}_{\overline{\partial}}(Y,\mathcal{L}_q) \longrightarrow C^\infty(\Omega)$$

という写像が定まる．

定理 3 ([8, 9])**.** $\mathcal{R}_k$ と $\mathcal{R}_{p+q-k}$ はそれぞれ Fréchet 空間における G の表現の位相 G 同型を与える．

$$\mathcal{R}_k\colon H^{k(p-k)}_{\overline{\partial}}(X,\mathcal{L}_p) \xrightarrow{\sim} \mathcal{S}ol(\Omega,\mathcal{M}_k),$$
$$\mathcal{R}_{p+q-k}\colon H^{k(q-k)}_{\overline{\partial}}(Y,\mathcal{L}_q) \xrightarrow{\sim} \mathcal{S}ol(\Omega,\mathcal{M}_k).$$

定理 2 の設定に戻る．最初の X, Y, Ω は今まで説明した空間，X' と Y' はここで初出の空間である．

$$\begin{aligned}
X :=& \{\mathbb{C}^{p,q} \text{ の maximally positive な } k \text{ 次元部分空間}\},\\
Y :=& \{\mathbb{C}^{p,q} \text{ の maximally positive な } (p+q-k) \text{ 次元部分空間}\},\\
\Omega :=& \{\text{maximally positive } p \text{ 次元部分空間}\},\\
&\simeq X \text{ のサイクル空間}\\
&\simeq Y \text{ のサイクル空間}\\
X' :=& \{X \text{ と } \Omega \text{ の incidence relations}\},\\
=& \{V \subset W : V \in X,\ W \in \Omega\},\\
Y' :=& \{Y \text{ と } \Omega \text{ の incidence relations}\},\\
=& \{W \subset U : U \in Y,\ W \in \Omega\}
\end{aligned}$$

とおく．ここで Ω が X のサイクル空間であると同時に Y のサイクル空間でもあることが重要である．すなわち，図式

$$\begin{tikzcd}
& {}^{\exists}X' \arrow[dl, "\alpha"'] \arrow[dr, "u"] & & {}^{\exists}Y' \arrow[dl, "v"'] \arrow[dr, "\beta"] & \\
X & & {}^{\exists}\Omega & & Y
\end{tikzcd}$$

が自然な形で得られる．このことが X と Y のコホモロジー空間をつなげる鍵となる．すなわち，左端の X 上のコホモロジーと右端 Y 上のコホモロジーからそれぞれ出発し，真ん中の空間 Ω での微分方程式で同型になることから定理 2 の証明が完成する．

References

[1] M. Eastwood, R. Penrose, R. O. Wells, Jr., *Cohomology and massless fields*, Comm. Math. Phys., **78** (1981), 305–351.

[2] H. Fujiwara, 指数型可解リー群のユニタリ表現 — 軌道の方法, 数学の杜 **1**, 数学書房, 2010.

[3] J. Hilgert, T. Kobayashi, J. Möllers, *Minimal representations via Bessel operators*, J. Math. Soc. Japan **66** (2014), no.2, 349–414.

[4] T. Kobayashi, Singular Unitary Representations and Discrete Series for Indefinite Stiefel Manifolds $U(p,q;\mathbb{F})/U(p-m,q;\mathbb{F})$, Mem. Amer. Math. Soc., **462**, vi+106 pp., 1992.

[5] T. Kobayashi, *Harmonic analysis on homogeneous spaces of reductive type and representation theory*, Sugaku, **46** (1994), 124–143; Math. Soc. Japan English translation, Sugaku Exposition, Amer. Math. Soc. (1998), **183** 1 – 31.

[6] H. Ochiai, U. Zunderiya, *A generalized hypergeometric system*, J. Math. Sci. Univ. Tokyo **20** (2013), 285–315.

[7] H. Sekiguchi, *Combinatorial formula of the dimension of global solutions to a generalized hypergeometric system* $\widetilde{\mathcal{M}}_{3,2}(\nu)$, Japan. J. Math. (N.S.) **27** (2001), no. 2, 311–326.

[8] H. Sekiguchi, *The Penrose transform* $Sp(n,\mathbb{R})$ *and singular unitary representations*, J. Math. Soc. Japan, **54** (2002), 215–253.

[9] H. Sekiguchi, *Penrose transform for indefinite Grassmann manifolds*, Internat. J. Math. **22** (2011), 47–65.

[10] H. Sekiguchi, *Radon–Penrose transform between symmetric spaces*, Contemp. Math. **598**, Amer. Math. Soc., 2013, 239–256. A special volume in honour of S. Helgason.

[11] H. Sekiguchi, *Elliptic coadjoint orbits of holomorphic type*, J. Lie Theory **33** (2023) 717–722.

[12] H. Sekiguchi, *Holomorphic Laplacian on the Lie ball and the Penrose transform*, accepted for publication in Indagationes Mathematicae, Available online April 20th, 2024.

[13] H. Sekiguchi, *Twistor transform for indefinite Grassmannian manifolds*, preprint.

[14] D. Vogan, Jr., *Unitarizability of certain series of representations*, Ann. of Math., **120**, 141–187, (1984).

「不定値グラスマン多様体上のコホモロジーの同型について」の正誤表

- 4 節　式 $(\mathcal{M}_k)$

(誤) $\det\left(\dfrac{\partial}{\partial z_{ij}}\right)_{\substack{i\in I\\ j\in J}} F(Z) = 0 \qquad Z = (z_{ij})_{\substack{i\in I\\ j\in J}}$

(正) $\det\left(\dfrac{\partial}{\partial z_{ij}}\right)_{\substack{i\in I\\ j\in J}} F(Z) = 0 \qquad Z = (z_{ij})_{\substack{1\le i\le q\\ 1\le j\le p}}$

非対称鍵共有法の数学的特徴付けと応用について

神保 洸貴 *

August 23, 2024

1 はじめに

暗号とは，2 人の通信者間でのメッセージのやり取りを，盗聴者が存在する通信路上で秘密裏にやり取りするための技術であり，暗号を用いた通信を暗号通信と呼ばれる．暗号通信は大きく分けて，暗号化と復号という 2 つの処理より構成され，暗号化とは，送信者がメッセージを，盗聴者に読まれない何らかの形に変換する処理のことであり，復号とは変換されたメッセージを元のメッセージに戻す処理のことである．この暗号化と復号をそれぞれ送信者と受信者が実行するためには，暗号鍵と復号鍵と呼ばれる特別な情報を，それぞれが暗号通信を行う前に保持している必要がある．２者間で暗号鍵，復号鍵を事前に共有するための技術の一つとして，公開鍵共有がある．公開鍵共有とは，ある集合の１つの要素を，盗聴者が存在する通信路を用いて，２者間で秘密裏に生成する技術であり，これを用いて生成された要素が，共有秘密鍵と呼ばれ暗号鍵，復号鍵として用いられる．

公開鍵共有の代表的なアルゴリズムとして，Diffie と Hellman らによって 1976 年に考案された Diffie-Hellman 鍵共有法 (D-H)[4] と呼ばれるものがあり，考案から 50 年近く経った現在でも，実社会の暗号通信の重要な基礎基盤技術として用いられている．しかし，実社会で重要な役割を担っている D-H であるが，その計算効率の悪さが問題視されることがある．一般に，D-H をはじめとする鍵共有法では，鍵共有の安全性と，共有秘密鍵のビット長等のパラメータには正比例の関係性があり，高い安全性を確保するためには，長い鍵長の共有秘密鍵が共有される必要がある．しかし一方で，長い共有秘密鍵を生成するためには，2 人の通信者ともに，より大きな計算資源が必要になる．計算機科学の発展とともに，悪意あるユーザーの用いる計算機の性能が向上している昨今，安全基準となる共有秘密鍵の長さも過去と比べて長くなっており，このことが高速な暗号通信を阻害する，もしくは，そもそも安全基準を満たさない共有秘密鍵を用いるユーザーも増加していることが報告されている [2]．このような状況は，D-H 以外の鍵共有法にも同様に当てはまる．

本稿では，上記の公開鍵共有の抱える実用上の問題の一部を，Accardi らによって考案された”強非対称な鍵共有”フレームワーク [1] を用いて解決することを試みた研究 [6] を紹介する．”強非対称な鍵共有”とは，公開鍵共有の一つのクラスであり，従来と異なる点は，２人の通信者が異なる計算規則に従って共有秘密鍵の生成を行うことであり，この特徴を鍵共有の”非対称性”と呼んでいる．この”非対称”な鍵共有を用いることで，２者のうち一方の計算資源が乏しい通信環境

*東京理科大学 創域理工学部

下で鍵共有の計算速度を向上させられることが示されている．本稿では，計算効率の向上と非対称な鍵共有の数学的構造の関連を議論することを主な目的とする．

本稿の構成は以下の通りである．2 章では，暗号通信の数学的枠組みと，暗号通信の安全性についてを説明することで，公開鍵共有の暗号通信における位置付けを明確にする．3 章では，公開鍵共有の数学的な枠組みと，安全性が一般的にどのように計られるかを説明する．4 章では，強非対称な鍵共有フレームワークの数理やこのフレームワークによってもたらされる性質を数理的に表現し，この性質と強非対称な鍵共有アルゴリズムの関連を，非対称な鍵共有アルゴリズムの数学的構造に着目して考察する．

2　暗号とは

2.1　暗号系

暗号系とは (1) を満たす以下の 5 つの (有限) 集合より構成される 5 つ組 $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ のことである．

- $\mathcal{M}$: 平文空間と呼ばれる． $\mathcal{M}$ の要素を平文と呼ぶ．
- $\mathcal{C}$: 暗号文空間と呼ばれる． $\mathcal{C}$ の要素を暗号文と呼ぶ．
- $\mathcal{K}$: 鍵空間と呼ばれる．$\mathcal{K}$ の要素を鍵と呼ぶ．
- $\mathcal{E} := \{E_k : \mathcal{M} \to \mathcal{C} \mid k \in \mathcal{K}\}$ とし， $\mathcal{E}$ の要素を暗号化関数と呼ぶ．
- $\mathcal{D} := \{D_k : \mathcal{C} \to \mathcal{M} \mid k \in \mathcal{K}\}$ とし， $\mathcal{D}$ の要素を復号関数と呼ぶ．
- $$\forall e \in \mathcal{K}, \exists d \in \mathcal{K}, \text{s.t.}, \forall p \in \mathcal{M}, D_d(E_e(p)) = p \tag{1}$$
  ただし，$E_e \in \mathcal{E}$，$D_d \in \mathcal{D}$． また， (1) を満たす $e \in \mathcal{K}$ を暗号鍵とよび，$d \in \mathcal{K}$ を復号鍵と呼ぶ．

以上の $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ において，ある暗号鍵 $e \in \mathcal{K}$ と復号鍵 $d \in \mathcal{D}$ を用いて，任意のメッセージを暗号化および復号可能な暗号プロトコルを図 1 のようにして構成できる．また，暗号鍵 e を通信路に公開する暗号系を公開鍵暗号，公開しないものを共通 (秘密) 鍵暗号と呼ぶ．暗号通信プロトコルを構成する上で重要なこと

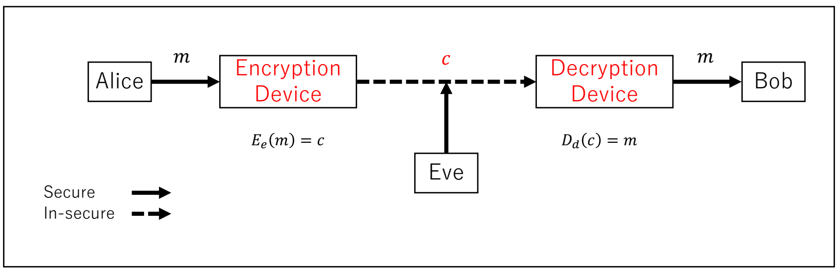


Figure 1: 暗号通信

は，二人の通信者 (Alice: メッセージの送信者， Bob: メッセージ受信者) 間で，Alice の送信する暗号文 $c = E_e(p) \in \mathcal{C}$ より， 平文 $p \in \mathcal{M}$ の”情報が漏れない”ようにプロトコルを設計することである．すなわち， 暗号文 c が送信される通信路上に， 盗聴者 Eve が存在することを仮定し， 盗聴者が Alice の送った暗号文 c に平文 p の”情報がどれほど含まれているか”によって， 暗号プロトコルが安全であるか否かが判断される．

一般に，ある通信系の持つ情報の量は，シャノンエントロピー [?] と呼ばれる尺度で測られる．以下の章 2.2 にて， Eve が獲得する，暗号文 c が含む平文 p の”情報の量”を，シャノンエントロピーを用いて定義する．

2.2　暗号通信の安全性

準備 (情報量)

ある通信系のシャノンエントロピー，あるいは情報量は，”確率”をもとに定義される．標本空間を X とし，離散かつ有限な集合とすると，$X = \{x_1, x_2, \dots, x_n\}$ のように表せる．このとき，各根元事象 x_i の生起確率を $p(x_i)$ と表し，以下が成り立つとする．

$$\forall i \in \{1, \dots, n\}, p(x_i) \geq 0, \sum_{i=1}^{n} p(x_i) = 1$$

以降では，取り扱う標本空間はすべて離散かつ有限であるとする．また，上記の離散確率分布 $p = (p(x_1), \dots, p(x_n))$ に対して以下のように，各事象とその生起確率を横に並べた系を完全事象系と呼ぶ (本稿では，標本空間と対応する完全事象系を同じシンボルで表す)．

$$X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ p(x_1) & p(x_2) & \cdots & p(x_n) \end{pmatrix}$$

完全事象系 X に対して以下のように定義された $S(X)$ を X のシャノンエントロピー (単にエントロピーと呼ばれることが多い) と呼ぶ．

$$S(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i)$$

ここで各 i に対して，$-\log p(x_i)$ は自己情報量と呼ばれ，x_i が持つ”曖昧さ”を表す．この”曖昧さ”あるいは”不確かさ”をもって，情報の量 (情報量) は定義され，例えば $p(x_i)$ の値が小さければ小さいほど x_i の曖昧さは高くなり，すなわち x_i の持つ情報量は大きいとみなされる．$S(X)$ は各事象がどのくらいの曖昧さを持つかを $p(x_i)$ で平均したものであり，系 X の持つ情報量とみなす．明らかに $S(X) \geq 0$ であり，すべての x_i が等確率，つまりすべての i に対して $p(x_i) = 1/n$ のとき，$S(X)$ は最大値 $\log n$ をとる．

また, 2 つの完全事象系 $X = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ p(x_1) & p(x_2) & \cdots & p(x_n) \end{pmatrix}$ と $Y = \begin{pmatrix} y_1 & y_2 & \cdots & y_m \\ p(y_1) & p(y_2) & \cdots & p(y_m) \end{pmatrix}$ に対して $(p(y_i) \geq 0 \ (\forall i), \sum_{i=1}^{m} p(y_i) = 1$ とする)，複合事象系 $X \times Y$ を考える．事象 (x_i, y_j) の生起確率を $p(x_i, y_j)$ で表し，$\forall i \in \{1, \dots, nm\}, p(x_i, y_j) \geq 0, \sum_{i=1}^{nm} p(x_i, y_j) = 1$ とする．また，x_i と y_j が独立な事象であれば $p(x_i, y_j) = p(x_i)p(y_j)$ とする．複合事象系のエントロピー $S(X \times Y)$ も同様に，以下のように定義される．

$$S(X \times Y) = -\sum_{i=1}^{nm} p(x_i, y_j) \log p(x_i, y_j)$$

また，複合事象系 $X \times Y$ に対して，根元事象 x_i を得たもとでの条件付き確率 $p(y_j \mid x_i)$ を $p(y_j \mid x_i) = p(x_i, y_j)/p(x_i)$ と定義し，x_i を得た元での Y の条件付きエントロピー $S(Y \mid x_i)$ を次のように定義する．

$$S(Y \mid x_i) = -\sum_{i=1}^{m} p(y_j \mid x_i) \log p(y_j \mid x_i)$$

これを用いて，系 X を得たもとでの Y の条件付きエントロピー $S(Y \mid X)$ を次のように定義する．

$$S(Y \mid X) = \sum_{i=1}^{n} p(x_i) S(Y \mid x_i)$$

この量は，根元事象 x_i を得たもとでの Y の情報量を $p(x_i)$ で平均したものである．すなわち，系 X を知ったもとで系 Y に残っている情報量を表す．最後に，系 X と Y の相互エントロピー (相互情報量) と呼ばれる量を定義する．相互情報量は $I(X, Y)$ と書き，系 Y の情報を得たとき系 X の情報量の減少量を表している．すなわち，$I(X, Y)$ は次のように定義される．

$$I(X, Y) = S(X) - S(X \mid Y)$$

系 Y の情報を得ることで系 X の情報量が減少するとはすなわち，系 Y の情報を得ることで解消した系 X の曖昧さの量であり，系 X について系 Y から獲得できた情報量とも解釈することができる．また，$S(X, Y) = S(X) + S(Y \mid X) = S(Y) + S(X \mid Y)$ が成り立つことより，次が成り立つ．

$$\begin{aligned} I(X, Y) &= S(X) - S(X \mid Y) \\ &= S(X) + S(Y) - S(X, Y) \\ &= S(Y) - S(Y \mid X) = I(Y, X) \end{aligned}$$

暗号通信の安全性

上で述べたように，暗号通信プロトコルの安全性は，暗号文を盗聴可能 (Alice が送信する暗号文 $c = E_e(p)$ を獲得できる) な Eve が通信路に存在することを仮定し，Eve がどのくらいの平文の情報量を得ることができるかで定義される．安全な暗号系とは何かを定義するために，以下の状況設定を行う．Alice と Bob は暗号通信を始める前に，(1) を満たす暗号鍵 e と復号鍵 d をそれぞれ選ぶ．簡単のため，以降では (1) を満たす e, d を同一の記号で $k = e = d$ のように表す．つまり，鍵空間 $\mathcal{K}$ の要素数を l とすると，以下が成り立っているとする．

$$\forall i \in \{1, \ldots, l\}, \forall m \in \mathcal{M}, D_{k_i}(E_{k_i}(m)) = m \tag{2}$$

Alice と Bob は，まず (2) を満たす鍵 k_i を，ある確率 $p(k_i)$ で選ぶ．次に，Alice は送信したいメッセージ $m_j \in \mathcal{M}$ を，k_i に依存せずに確率 $p(m_j)$ で選び，暗号文 $c_h = E_{k_i}(m_j)$ を Bob に送信する．ただし，$\mathcal{M}$ の中に，$p(m_j) = 0$ となるような m_j は含まれていないとする．盗聴者 Eve は，上のステップで Alice が送信した暗号文 c_h を得ることができ，さらに完全事象系 $\mathcal{M}$ と $\mathcal{K}$，暗号化関数，復号関数の集合 $\mathcal{E}, \mathcal{D}$ も知っているとする．Eve は Alice と Bob の選んだ k_i と Alice が暗号化した m_j のみを知らない．暗号文空間 $\mathcal{C}$ の要素数 を s とすると，Eve は任意の $h \in \{1, \ldots, s\}$ に対して，$E_k(m) = c_h$ を満たすすべての $(m, k) \in \mathcal{M} \times \mathcal{K}$，すなわち集合 $S_h = \{(m_j, k_i) \in \mathcal{M} \times \mathcal{K} \mid E_{k_i}(m_j) = c_h\}$ を考えることで，暗号文 c_h が生起する確率 $p(c_h)$ を $p(c_h) = \sum_{(m_j, k_i) \in S_h} p(m_j) p(k_i)$ により計算することが

できる．また，任意の暗号文 $c_h \in \mathcal{C}$ に対する上記 S_h を用いて，平文 m_j を任意に固定することで，暗号文 c_h を得たもとで平文 m_j を得る条件付き確率 $p(m_j \mid c_h)$ も $p(m_j \mid c_h) = (\sum_{k_i,(m_j,k_i)\in S_h} p(m_j)p(k_i)/p(c_h)$ と計算することができる．

Eve は得た暗号文 c_h より Alice の送った平文の情報を得たいが，$\mathcal{M}$ よりどの平文が暗号化されたかを知らない．よって，Eve はすべての $j \in \{1,\dots,n\}$ に対して $p(m_j \mid c_h)$ を計算し，平文の確率分布 $(p(m_1),\dots,p(m_n))$ と比較することで，どの平文が送られたか，何らかの推測を行う (例えば，ある j に対して $p(m_j \mid c_h) = 1$ であれば，Eve は平文 m_j を復元することができる)．

ここでもし，すべての $h \in \{1,\dots,t\}$, $j \in \{1,\dots,n\}$ に対して $p(m_j \mid c_h) = p(m_j)$ が成り立っていれば，m_j の暗号化の過程で，平文の確率分布が変化しないことを意味し，この場合 Eve は平文を平文の確率分布のみに従って推測することになる．すなわちこの条件を満たす暗号系では，任意の暗号文に，平文の情報が一切含まれていないことを意味している．実際，完全事象系 $\mathcal{M},\mathcal{C}$ に対して，明らかに $S(\mathcal{M}) = S(\mathcal{M} \mid \mathcal{C})$ が成り立つことから，Eve が系 $\mathcal{C}$ より得られる系 $\mathcal{M}$ の情報量，すなわち相互エントロピー $I(\mathcal{M},\mathcal{C})$ は 0 となる．

逆に $I(\mathcal{M},\mathcal{C}) = 0$ が成り立っているとき，複合事象系 $\mathcal{M}\times\mathcal{C}$ において (m_j, c_h) の生起確率を $p(m_j, c_h)$ と表記すると，$I(\mathcal{M},\mathcal{C})$ が以下の式でかけることから:

$$I(\mathcal{M},\mathcal{C}) = \sum_{j=1}^{n}\sum_{h=1}^{t} p(m_j, c_h) \log \frac{p(m_j, c_h)}{p(m_j)p(c_h)}$$

$I(\mathcal{M},\mathcal{C}) = 0 \iff \forall j,h, p(m_j,c_h) = p(m_j)p(c_h) \iff \forall j,h, p(m_j \mid c_h) = p(m_j)$ となる．

以上の，$I(\mathcal{M},\mathcal{C}) = 0$ を満たす暗号系は，Shannon [**?**] により，以下のように定義された．

定義 1 (完全秘匿性 [8])**.** 与えられた暗号系が，すべての暗号文 $c_h \in \mathcal{C}$, すべての平文 $m \in \mathcal{M}$ に対して，

$$p(m_j \mid c_h) = p(m_j) \tag{3}$$

を満たすとき，この暗号系は完全守秘性を持つと呼ばれる．

(3) を満たす暗号系のクラスは，空ではない．実際，以下の例に記述する Vernam の使い捨て暗号は，完全守秘性を持つことが， [8] において Shannon によって示されている．

例 1 (Vernam 暗号)**.** *Vernam* 暗号 $C_{Ver} = (\mathcal{M},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$ は次のように構成される．

- $\mathcal{M},\mathcal{C},\mathcal{K} = \mathbb{Z}_2^n = \{0,1\}^n$
- $\mathcal{K}$ について，全部で 2^n 個の根元事象が存在し，それぞれの生起確率は $\frac{1}{2^n}$ とする．$\mathcal{M}$ も同様に，全部で 2^n 個の根元事象が存在するが，それぞれの生起確率はどのような分布に従っていても良い．
- $\mathcal{E} = \{E_k : \mathcal{M} \to \mathcal{C} \mid (E_k(m))_i \equiv m_i + k_i \pmod 2, k \in \mathcal{K}, i \in \{1,\dots,n\}\}$
- $\mathcal{D} = \{D_k : \mathcal{C} \to \mathcal{M} \mid (D_k(c))_i \equiv c_i + k_i \pmod 2, k \in \mathcal{K}, i \in \{1,\dots,n\}\}$

C_{ver} は完全秘匿性を満たす．すべての暗号文 $c_h \in \mathcal{C}$ と平文 $m_j \in \mathcal{M}$ に対して，ベイズの定理より，上と同様に定義された条件付き確率 $p(m_j \mid c_h) = (\sum_{k_i,(m_j,k_i)\in S_h} p(m_j)p(k_i))/p(m_j)$ を用いて，$p(m_j \mid c_h)$ は次のように表せる．

$$p(m_j \mid c_h) = \frac{p(c_h \mid m_j)p(m_j)}{p(c_h)}$$

ここで，$\mathcal{E}$ の定義より，異なる $k \in \mathcal{K}$ に対して，$E_k(m_j)$ は異なる暗号文を生成する．よって，$E_k(m_j) = c_j$ を満たす $k \in \mathcal{K}$ がただ一つ存在し，$p(c_h \mid m_j)$ はその鍵の生起確率 $1/2^n$ に等しい．また，上で述べたように，$p(c_h) = \sum_{(m_j,k_i)\in S_h} p(m_j)p(k_i)$ であり，ここでも同様に鍵の一意性を用いて，

$$p(c_h) = \sum_{(m_j,k_i)\in S_h} p(m_j)p(k_i) = \frac{1}{2^n}\sum_{m_j\in\mathcal{M}} p(m_j) = \frac{1}{2^n}$$

となる．結局，

$$p(m_j \mid c_h) = \frac{p(c_h \mid m_j)p(m_j)}{p(c_h)} = \frac{\frac{1}{2^n}p(m_j)}{\frac{1}{2^n}} = p(m_j)$$

となる．

上で述べたように，完全秘匿性を持つ暗号系において，暗号文の中に平文の情報が一切含まれていないのであるから，攻撃者 Eve は暗号文に対していかなる解析をしようとも，Alice が送った平文を復元することができない．このことから，実社会では Vernam 暗号を含む，完全秘匿性を持つ暗号系が暗号通信で大きな役割を担っているかと考えられるかもしれないが，これらの暗号系が用いられることはほとんどない．上の例を見るとわかるように，Vernam 暗号を用いて暗号通信を実現するためには，Alice と Bob 間で事前に鍵 k を鍵空間 $\mathcal{K}$ より一様に選び共有する必要がある．同様に，一般の暗号系についても，すべての暗号文，平文に対して (2) が成立するためには，鍵空間の大きさが平文空間の大きさ以上かつ各鍵の生起確率が $1/|\mathcal{K}|$ であることが必要条件であり (証明は省略する [9, 10]．また $|\cdot|$ は集合の要素数を表す．)，鍵を事前に Alice・Bob 間で共有する必要があるのは同じである．鍵 k を共有するためには，安全な通信路，すなわち Eve が存在しない通信路を確保する必要があり，このような通信路とは具体的に Alice と Bob が密室にて鍵 k がプリントされた紙を手渡する，などであり物理的な接触を伴う．工学的な視点から見て，完全秘匿性を持つ暗号通信を実現するためには，運用コストが大きいことから，非常に限られた用途でしか用いられていない．

3 公開鍵共有 (鍵共有)

完全秘匿性を持つ暗号通信は，運用コストの観点から，ほとんど実社会で用いられることはない．一般に，以下で説明する公開鍵共有 (鍵共有) という技術を用いて，Alice と Bob 間で共通の鍵 $k \in \mathcal{K}$ を生成し，AES などの秘密鍵暗号方式を用いてメッセージの暗号化が行われる．AES は後に説明する，計算量的安全性と呼ばれる概念に基づいて設計された暗号であり，簡単に説明すると，暗号化関数等のある関数の逆像を求めることに非常に大きな計算時間がかかることを利用した概念であり，上で説明した完全秘匿性より弱い概念である．AES の説明は本稿では省略する．

3.1 公開鍵共有の一般的な枠組み

- X_A, X_B: 有限集合で，それぞれ Alice，Bob の秘密鍵空間と呼ぶ．X_A, X_B の要素をそれぞれ Alice，Bob の秘密鍵と呼ぶ．
- Y: 有限集合で，公開鍵空間と呼ぶ．Y の要素を公開鍵と呼ぶ．
- $\mathcal{K}$: 有限集合で，暗号系で定義したものと同様に鍵空間と呼ぶ．

- $F_A = \{f_i^A : X_A \times T^i \mid i = 1, 3, \ldots, 2l-1\}$: 関数の集合で，$F_A$ の要素を (i 番目の)Alice の公開鍵生成関数と呼ぶ.

- $F_B = \{f_j^B : X_A \times T^j \mid j = 2, 4, \ldots, 2l-2\}$: 関数の集合で，$F_B$ の要素を (j 番目の)Bob の公開鍵生成関数と呼ぶ.

- $n = 2l-1$ とする． $g_A : X_A \times T^n \to \mathcal{K}, g_B : X_B \times T^n \to \mathcal{K}$ をそれぞれ Alice，Bob の拠有鍵生成関数と呼ぶ.

  任意の $x_A \in X_A$, $x_B \in X_B$ に対して，以下の 4 が成り立つとき， 4つ組 (g_A, F_A, g_B, F_B) を公開鍵共有あるいは単に鍵共有と呼ぶ.

$$g_A(x_A, t_1, t_2, \ldots, t_n) = g_B(x_B, t_1, t_2, \ldots, t_n) \tag{4}$$

  ただし $i = 1, 3, \ldots, n$ に対して $t_i = f_i^A(x_A, t_1, t_2, \ldots, t_{i-1})$,$j = 2, 4, \ldots, n-1$ に対して $t_j = f_j^B(x_B, t_1, t_2, \ldots, t_{j-1})$ とする.

公開鍵共有 (g_A, F_A, g_B, F_B) を実装するにあたって，Alice は上記 $t_1, t_3, \ldots, t_n$ を生成し，暗号通信の場合と同様に，これらを Eve の存在する通信路を介して Bob に送信する．Bob は $t_2, t_4, \ldots, t_{n-1}$ を生成し，同じ通信路を用いて Alice に送信する．x_A，x_B はそれぞれ秘密裏に保管し，通信路上に公開しない．Alice と Bob は $t_1, t_2, \ldots, t_n$ を保持している (Eve も同様に保持している) ので，それぞれ $g_A(x_A, t_1, t_2, \ldots, t_n)$，$g_B(x_B, t_1, t_2, \ldots, t_n)$ を計算することができる．これらの計算結果は (4) より同一であり，この値を共有秘密鍵あるいは Secret Shared Key (SSK) と呼ぶ.

公開鍵共有の安全性は，暗号系の安全性と同様に，公開されている情報 (すなわち公開鍵) にどれほど SSK の情報が含まれているかによって測ることができる．つまり $I(\mathcal{K}, Y^n)$ の値が 0 に近いほど，Eve は公開鍵から獲得できる SSK の情報が少なくなる．しかし $I(\mathcal{K}, Y^n) = 0$ を達成する公開鍵共有は現在までに知られていない．上記 g_A，g_B による計算結果にある一定の誤差を許し，十分小さな $\epsilon > 0$ に対して $I(\mathcal{K}, Y^n) \leq \epsilon$ と，緩められた条件を達成する鍵共有方式は存在し，BB84 方式 [3] をもとにした量子鍵配送や Maurer の衛星通信 [7] を用いた方式などが代表的である．しかしこれらの鍵共有方式は，運用コストの観点より，インターネットなどの高速かつ運用の容易性が求められる通信環境で用いることは想定されていない．一般的には，以下の例にある Diffie-Hellman 鍵共有法 (D-H) [4] などの，計算量的安全性に従う鍵共有が用いられる.

例 2. **ステップ 0** 初めに，*Alice* と *Bob* は以下のパラメータを設定する.
p : 大きな素数
$\mathbb{Z}/p\mathbb{Z} := \mathbb{Z}_p$: p より構成される有限体
$g \in \mathbb{Z}_p$: $\mathbb{Z}_p \setminus \{0\}$ の生成元

Step A1 *Alice* は $x_A \in \mathbb{Z}_{p-1}$ を一様ランダムに選び，それを秘密裏に保管する．その後公開鍵 y_A を次のように計算する.

$$y_A := g^{x_A} \in \mathbb{Z}_p.$$

Step B2 *Bob* は $x_B \in \mathbb{Z}_{p-1}$ を一様ランダムに選び，それを秘密裏に保管する．その後，公開鍵 y_B を次のように計算する.

$$y_B := g^{x_B} \in \mathbb{Z}_p.$$

Step A2 *Alice* は *Bob* の公開鍵 y_B と秘密鍵 x_A を使用して，以下の κ_A を計算する．

$$\kappa_A := {y_B}^{x_A} = (g^{x_B})^{x_A} = g^{x_B x_A} \in \mathbb{Z}_p.$$

Step B2 *Bob* は *Alice* の公開鍵 y_A と秘密鍵 x_B を使用して，以下の κ_B とを計算する．

$$\kappa_B := {y_A}^{x_B} = (g^{x_A})^{x_B} = g^{x_A x_B} \in \mathbb{Z}_p.$$

すべての $x, y \in \mathbb{Z}_{p-1}$ および $g \in \mathbb{Z}_p$ に対して，$g^{xy} = g^{yx}$ が成り立つため，*Alice* と *Bob* は同じ値 $\kappa = \kappa_A = \kappa_B \in \mathbb{Z}_p$ を持ち，この κ を共通鍵暗号の暗号化および復号化の鍵として使用する．*D-H* の安全性は，有限体における離散対数問題（*DLP*）を解くことの困難さに基づいている．*DLP* とは与えられた $b = a^x \in \mathbb{Z}_p$ および $\mathbb{Z}_p \setminus \{0\}$ の原始元 a に対して，$x \in \mathbb{Z}_{p-1}$ を計算する問題であり，効率的に解く方法は未だ見つかっていない．効率的に問題を解くとは簡単に，$n = \log_2 p$ に対して，ある多項式 p が存在して，高々$p(n)$ 回の処理で問題の解を見つけることであり，単に多項式時間で解ける，などと言われることが多い．問題を効率的に解く，解けないことの定式化は以降で述べる．

3.2 計算量的安全性

以下で説明する一方向性関数は，計算量的安全性に関する重要な要素の一つである．一方向性関数を説明する前に，まずは確率変数の表記や確率的多項式時間アルゴリズムなどの基礎的な概念を説明する．

確率変数について

確率論における確率変数は，確率空間から可測空間への可測関数として定義される．具体的には，確率空間 $(\Omega, \mathcal{F}, P)$ と可測空間 $(\mathbb{R}, \mathcal{B})$ が与えられたとき，確率変数 X は関数 $X : \Omega \to \mathbb{R}$ であり，任意のボレル集合 $B \in \mathcal{B}$ に対して，集合 $\{\omega \in \Omega \mid X(\omega) \in B\} \in \mathcal{F}$ が成り立つ．しかし，本稿では，[5] および多くの暗号理論関連の文献と同様に，確率変数および確率を可測空間，確率空間，標本空間を定義することなく取り扱う．具体的には，確率変数 X は集合 S から値を取り，S の各要素に割り当てられる確率 P は 0 から 1 までの実数である．例えば，$S = \{a, b\}$ とし，a が S から選ばれる確率を $P[X = a] = \frac{1}{3}$，b が選ばれる確率を $P[X = b] = \frac{2}{3}$ と表す．特に，確率変数が U_S と表される場合，集合 S 上で一様分布に従うとする．例えば，$S = \{a, b, c, d\}$ であれば，すべての $x \in S$ に対して，

$$P[U_S = x] = \frac{1}{4}$$

確率的 (非決定的) アルゴリズム

アルゴリズムとは，ある問題の解放を与えるための有限個の処理の集まりのことであり，入力に対し，何らかの出力を行う．決定的アルゴリズムとは，与えられた入力に対して，必ず同じ結果を返すアルゴリズムであり，例えばある決定的アルゴリズム M に対して，取り得る入力の集合を S，出力の集合を T とすると，各 $x \in S$ に対して，ある決まった値 $y \in T$ を必ず返す．すなわち決定的アルゴリズムは関数 $M : S \to T$ として考えてよい．

これに対して，確率的アルゴリズムとは，入力に対する出力が，アルゴリズム内部で生成される乱数 (コイントス) によって決定されるものである．すなわち確率的アルゴリズム M' は，入力の集合を S，出力の集合を T とすると，二変数関数 $M' : S \times \{0, 1\}^m \to T$ として考えることができる．ただし $\{0, 1\}^m$ は M' の

内部で行われる有限回のコイントスを表す．一般的に，M' 内部で行われるコイントスは，M' に対する入力とは取り扱わず，$x \in S$ に対して $M'(x)$ のようにして M' の出力を表記する．また，コイントス $r \in \{0,1\}^m$ によって，出力が変わるので，$M'(x)$ を確率変数 $M'(x) : \{0,1\}^m \to T$ と考えることができ，$M'(x)$ が $y \in T$ をとる確率を：$P[M'(x) = y] = \sum_{r \in \{0,1\}^m, M'(x,r)=y} \frac{1}{2^m}$ のように定義することができる．

以上，アルゴリズムに対して，与えられた問題が解けるか否かだけでなく，解くのに要する時間を考慮することが重要である．計算時間は，一般に入力の大きさ (ビット数) に対する演算回数などで定義され，単調増加関数 $T : \mathbb{N} \to \mathbb{N}$ で表される．T が多項式時間とは，ある $c > 0$，ある自然数 n_0 が存在して，すべての $n \geq n_0$ に対して $T(n) \leq n^c$ となることを言い，M が多項式時間アルゴリズムであるとは，M の計算時間が多項式時間であることを言う．

一方向性関数と計算量的安全性

以上の用語や表記を用いて，一方向性関数は以下のように定義される．また以降では，$|\cdot|_B$ は入力された集合の要素数のビット長を示し，非整数の結果を扱うために天井関数を使用することに注意する．例えば，$S = \{a, b, c, d\}$ の場合，S の要素数は 4 であり，$|S|_B = \lceil \log_2 4 \rceil = 2$ である．同様に，9 個の要素を持つ集合 T の場合，T の要素数は 9 であり，$|T|_B = \lceil \log_2 9 \rceil = 4$ である．

定義 2. 集合 S と S' に対する関数 $f : S \to S'$ が以下 *2* つの条件を満たすとき，f は一方向性関数と呼ばれる．

1. 任意の $x \in S$ に対して，決定的多項式時間アルゴリズム A が存在して $A(x) = f(x)$ を満たす．

2. 任意の確率的多項式時間アルゴリズム A' および任意の正の多項式 p に対して，ある自然数 n_0 が存在し，$|T|_B = n \geq n_0$ を満たす任意の $T \subseteq S$ に対して，以下が成り立つ．

$$P[A'(f(U_T)) \in f^{-1}(f(U_T))] < \frac{1}{p(n)} \tag{5}$$

2 つ目の条件は，多項式時間という制約のもとでは，任意の入力 $x \in S$ に対して $f(x)$ の逆像を求めることができる確率が非常に低いことを表している．また，この定義よりある $m < n_0$ について次のことが言える．同じ関数 $f : S \to S'$ に対して，$|T|_B \leq m$ を満たす任意の部分集合 $T \subset S$ に対し，関数 f を T に制限したもの，すなわち $f : T \to S'$ は一方向性の性質を持たない．すなわち，ある確率的多項式時間アルゴリズム A''，正の多項式 p'，および整数 $m < n_0$ が存在し，$|T|_B \leq m$ を満たす任意の部分集合 $T \subset S$ に対して，次が成り立つ．

$$\Pr[A''(f(U_T)) \in f^{-1}(f(U_T))] \geq \frac{1}{p'(m)} \tag{6}$$

注意 1. 一方向性関数の定義は上の通りだが，この定義を満たすと示されている関数は現在までのところ存在しない．つまり，一方向性関数であると考えられている関数は，単に一方向性の *2* つ目の条件を満たすと仮定されているだけである．すなわち，例 *2* の有限体上の指数関数などの関数は，*2* つ目の条件における ”任意の確率的多項式時間アルゴリズム A'”というフレーズを，”任意の**既知の**確率的多項式時間アルゴリズム A'”と読み替えたもとで，条件を満たす．

また，一方向性を持つという仮定が事実であったとしても，その関数を用いた暗号アルゴリズムが計算量的に攻撃不可であるとは限らない．というのもこれまで発表された，鍵共有をはじめとする計算量的安全性を持つと考えられている暗号アルゴリズムにおいて，暗号アルゴリズムを破る問題が，安全性の基礎として用いる一方向性関数の逆像を求める問題に帰着できることは示されているものの，その逆の証明はされていない．一般に言われている計算量的安全性を持つ暗号アルゴリズムとは，用いる一方向性関数に対する逆像を求める効率的なアルゴリズムが見つかっていない，かつ，逆像を求める以外に暗号アルゴリズムを破る効率的な攻撃方法が見つかっていないものを指す.

4　強非対称公開鍵共有アルゴリズムとその性質

この章では，本項の主題である強非対称鍵共有アルゴリズムと，その性質についてを議論する．

4.1　強非対称鍵共有フレームワーク

強非対称鍵共有フレームワークとは，Accardi ら [1] によって考案された鍵共有の枠組みの一つであり，英名で Strongly Asymmetric Public Key Agreement と書かれる．以後，強非対称鍵共有フレームワークを，英名の頭文字をとり SAPKA と表記する．SAPKA は，以下のようにある半群から半群への関数とその合成によって記述される．

SAPKA の鍵共有プロセス

まず，Alice と Bob は二つの半群 $\mathcal{S}$ と $\mathcal{S}'$ を準備し，これらは公開する．次に以下の条件を満たす関数 $x_1, x_3 : \mathcal{S}' \to \mathcal{S}'$ および $x_2, x_4 : \mathcal{S} \to \mathcal{S}'$ を選ぶ.

定義 3. すべての $y \in \mathcal{S}$ に対して：

$$x_1 \circ x_2(y) = x_3 \circ x_4(y) \in \mathcal{S}' \tag{7}$$

ここで，$\circ$ は二つの関数の合成を表す．この条件を満たす x_1, x_2, x_3, x_4 を**互換性がある**と呼ぶ.

これらの 4 つの関数は Bob の秘密鍵であり，さらに Bob は彼の秘密鍵に属する逆関数を持つ関数 $N_1 : \mathcal{S}' \to \mathcal{S}'$ を追加で選ぶ．これら 5 つの関数 x_1, x_2, x_3, x_4 および N_1 は一方向性関数の条件 (1) を満たすとする．SAPKA の鍵共有プロセスは以下のように記述される．

Step 1(Bob) Bob は彼の公開鍵 $y_{B,1}, y_{B,2}$ をそれぞれ次の関数として構成し，

$$y_{B,1} := N_1^{-1} \circ x_4,$$

$$y_{B,2} := x_1 \circ x_2$$

これを Alice に送る．

Step 1(Alice) Alice は秘密鍵 x_A を $\mathcal{S}$ から選び，次のように公開鍵 y_A を計算する．

$$y_A := y_{B,1}(x_A) = N_1^{-1} \circ x_4(x_A)$$

これを Bob に送る．

Step 2(Alice) Alice は次の κ_A を計算する．

$$\kappa_A := y_{B,2}(x_A) = x_1 \circ x_2(x_A)$$

Step 2(Bob) Bob は次の κ_B とを計算する．

$$\kappa_B := x_3 \circ N_1(y_A) = x_3 \circ N_1 \circ N_1^{-1} \circ x_4(x_A) = x_3 \circ x_4(x_A)$$

関数を送信するとは，Alice が $\mathcal{S}$ あるいは $\mathcal{S}'$ のすべての要素に対してその関数を計算するための十分な，何らかの値を公開することを意味する．例えば，$f(x) = a^{bx}$ と定義される $f : \mathbb{Z}_{n-1} \to \mathbb{Z}_n$ を送信したい場合，$a^b \in \mathbb{Z}_n$ を送信すれば，受信者はすべての $x \in \mathbb{Z}_{n-1}$ に対して $f(x)$ を計算することができる．

$\mathcal{M}_{\mathcal{S}'}$ を $\mathcal{S}'$ から $\mathcal{S}'$ へのすべての関数の集合，$\mathcal{M}_{\mathcal{S}}$ を $\mathcal{S}$ から $\mathcal{S}'$ へのすべての関数の集合とする．また，$\hat{\mathcal{M}_{\mathcal{S}'}}$ を $\mathcal{M}_{\mathcal{S}'}$ の部分集合であり，すべての可逆関数からなる集合とする．SAPKA は (3) を満たす関数により特徴付けられるため，以下のような表記を用いる．

定義 4. x_1, x_2, x_3, x_4 が互換性 (7) を持つような $(x_1, x_2, x_3, x_4, N_1) \in \mathcal{M}_{\mathcal{S}'} \times \mathcal{M}_{\mathcal{S}} \times \mathcal{M}_{\mathcal{S}'} \times \mathcal{M}_{\mathcal{S}} \times \hat{\mathcal{M}_{\mathcal{S}'}}$ 全体の集合を C_{SAPKA} と書く．また，このクラスに属する鍵共有を *SAPKA* アルゴリズムと呼ぶ.

4.2 SAPKA の持つ性質

4.1 章にて説明した SAPKA の大きな特徴は，Alice と Bob で生成する秘密鍵，公開鍵の集合が異なり，それに伴い，両者の公開鍵・SSK の生成規則が異なることである．"強非対称" とは，鍵共有のプロセスにおけるこの性質のことを指す．D-H をはじめとする従来の鍵共有アルゴリズムは一方で，両者の秘密鍵，公開鍵集合及び鍵生成規則が同一なものがほとんどである．"強非対" な鍵共有アルゴリズムと対比して，これらのアルゴリズムは "対称的な" 鍵共有と呼ぶ.

また，SAPKA を構成する 5 つの関数に課されている条件は (3) と N_1 が逆写像を持つことのみであり，非常に大きな鍵共有のクラスであることが考えられる．実際，いくつかの対照的な鍵共有は，C_{SAPKA} に含まれる．以下で，例として対照的な鍵共有である D-H が，C_{SAPKA} の要素であることを示す.

定理 1. *D-H* 鍵共有法は，C_{SAPKA} に含まれる．

Proof. 例 2 と同様に，大きな素数 p，有限体 $\mathbb{Z}_p$，生成元 g は公開情報とする．3.1 章の表記を用いると，次のように定義される $f_1^A : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$, $f_1^B : \mathbb{Z}_{p-1} \to \mathbb{Z}_p$, $g_A : \mathbb{Z}_{p-1} \times \mathbb{Z}_p \to \mathbb{Z}_p$，$g_B : \mathbb{Z}_{p-1} \times \mathbb{Z}_p \to \mathbb{Z}_p$ を用いて，D-H は (g_A, f_1^A, g_B, f_1^B) と表せる．

$$f_1^A(x) = f_1^B(x) = g^x \qquad ; \qquad g_A(x, y) = g_B(x, y) = y^x$$

任意の $x_A, x_B \in \mathbb{Z}_{p-1}$ に対して，同一の公開鍵 $t_1 = f_1^A(x_A)$，$t_2 = f_1^B(x_A)$ 及び共有秘密鍵 $g_A(x_A, t_2)(= g_B(x_B, t_1))$ を生成できるような $(x_1, x_2, x_3, x_4, N_1) \in C_{SAPKA}$ が存在することを示す．SAPKA における $\mathcal{S}, \mathcal{S}'$ を $\mathcal{S} = \mathbb{Z}_p, \mathcal{S}' = \mathbb{Z}_p \setminus \{0\}$ とし，5 つの関数を以下のように定義する．

$$x_1 := id_{\mathcal{S}} \qquad , \qquad N_1 := id_{\mathcal{S}'}$$

$$y \in \mathcal{S} \mapsto x_2(y) := (g^{x_B})^y \in \mathcal{S}' \qquad , \qquad y \in \mathcal{S}' \mapsto x_3(y) := y^{x_B} \in \mathcal{S}'$$

$$y \in \mathcal{S} \mapsto x_4(y) := g^y \in \mathcal{S}'$$

すると，x_A に対して $y_{B,1}(x_A) = N_1 \circ x_4(x_A) = g^{x_A} = t_1$，$y_{B,2}(x_A) = x_1 \circ x_2(x_A) = g^{x_A x_B} = g_A(x_A, t_2)$．$x_B$ に対して，$x_1 \circ x_2(1) = g^{x_B} = t_2$，$x_3 \circ N_1^{-1}(t_1) = g^{x_A x_B} = g_B(x_B, t_1)$ となる． □

以上のように，ある対称な鍵共有は C_{SAPKA} の要素であることがわかった．しかし，C_{SAPKA} の要素であるからといって，SAPKA の性質である"Alice・Bob 両者の計算規則が異なる"という性質を本質的に持っているわけではない．上の定理において，$y_{B,1}$ は事前に共有されている g をもとに構成されており，つまり Bob は $y_{B,1}$ を送信しなくとも Alice は公開鍵 g^{x_A} を計算することができる．また，関数 $y_{B,2}$ の送信のため Bob は g^{x_B} を計算することが十分であるが，これは Alice の公開鍵と同一の関数を計算していることを意味する．SSK も同様に Alice・Bob は同一の計算を行っている．

もし対称な鍵共有を，SAPKA を用いて両者が異なる計算規則に従うように改良を行うことができれば，公開鍵・SSK の計算の際，Alice，Bob 間で各鍵生成に必要な計算ステップ数に差異を持たせられる場合がある．このとき，Alice，Bob が用いるデバイスの性能 (単位時間あたりに計算可能なステップ数とし，それぞれ $E_A, E_B \in \mathbb{R}^+$ と表す) によっては，鍵共有に必要な計算時間 (両者で SSK を生成し終わるまでの時間) を短縮することができる．以下でこれを示す．以下では便宜的にすべての鍵共有アルゴリズムの集合を C_{PKA} とする．また，任意の鍵共有アルゴリズム $A \in C_{PKA}$ に対して，Alice と Bob の計算ステップ数を SSK 長 N に関して単調増加関数 $S_A, S_B : C_{PKA} \times \mathbb{N} \to \mathbb{N}$ で表す．D-H をはじめとする対称な鍵共有では，以下が成り立つ：

$$S_A(A, N) = S_B(A, N), \tag{8}$$

このような鍵共有を $A_{A=B} \in C_{PKA}$ と表す．一方で，次のような条件を満たす鍵共有を $A_{A<B} \in C_{PKA}$ と表すことにする．

$$S_A(A_{A<B}, N) < S_A(A_{A=B}, N) \tag{9}$$

$$S_B(A_{A<B}, N) > S_B(A_{A=B}, N) \tag{10}$$

以上の表記を用いて，次の定理を証明する．

定理 2. 鍵共有 $A_{A=B}$ を改良し，新しい鍵共有 $A_{A<B} \in C_{PKA}$ を得たとする．このとき，$A_{A<B}$ の鍵共有に必要な計算時間が $A_{A=B}$ の鍵共有に必要な計算時間を下回るような，通信環境 (E_A, E_B)*(ただし* $E_A < E_B$*)* が存在する．

Proof. $A_{A=B}$ において，$E_A < E_B$ であるとき Alice と Bob 両者が SSK 生成を終える時間は以下のように表される．

$$T_0 := \frac{S_A(A_{A=B}, N)}{E_A} \tag{11}$$

改良後の $A_{A<B}$ において Alice と Bob の SSK 計算時間はそれぞれ $T_{1,A} := \frac{S_A(A_{A<B}, N)}{E_A}$ および $T_{1,B} := \frac{S_B(A_{A<B}, N)}{E_B}$ であり，総計算時間 T_1 はこれらの最大値として表される：$T_1 = \max\{T_{1,A}, T_{1,B}\}$．このとき，$T_1 < T_0$ となる (E_A, E_B) となる条件は以下のように求められる．

- $T_{1,B} < T_{1,A}$ の場合，(9) が成り立つため，任意の $E_A, E_B (E_A < E_B)$ に対して明らかに $T_1 < T_0$ である．

- $T_{1,A} < T_{1,B}$ の場合，$T_{1,B} < T_0$ となることが十分条件である．これは (11) より，以下が同値であり：

$$\frac{S_B(A_{A<B}, N)}{S_A(A_{A=B}, N)} = \frac{S_B(A_{A<B}, N)}{S_B(A_{A=B}, N)} < \frac{E_B}{E_A} \tag{12}$$

  E_B が十分に大きければこれは達成できる．

□

4.3 計算量非対称な SAPKA サブクラス

もし (10) が成り立っていない場合，$T_1 < T_0$ は自明なため，定理 2 を満たすために本質的な条件は (9) であると言える．ただし (9) を満たすように鍵共有アルゴリズムを改良できたとしても，Alice の公開鍵に対する攻撃が容易になってしまっては，実用性の観点で意味がない．従って，我々の目標は，(9) が成り立っていても，Alice の公開鍵に対する攻撃が，Bob のそれに対する攻撃と同等な難しさを持つ SAPKA サブクラスを構成することである．この性質を，**計算量非対称性**と呼ぶ．

C_{SAPKA} には，そもそも攻撃が容易 (Alice の公開鍵，Bob の公開鍵のいずれからも SSK を多項式時間で求めることが可能) な鍵共有が含まれているので，まずは以下のように任意の一方向性関数を用いて，このような鍵共有を除外する必要がある．例えば，$\mathcal{S} = \mathcal{S}' = \mathbb{Z}_p$ とし，$y \in \mathcal{S}$ に対して $x_1(y) = x_3(y) := x_B y \in \mathcal{S}$，$x_2 = x_4 := id_{\mathcal{S}}$，および $y \in \mathcal{S}$ に対して $N_1(y) := n_B y \in \mathcal{S}$ と定義する．ここで $x_B, n_B \in \mathcal{S}$ は Bob の秘密鍵とする．このとき $(x_1, x_2, x_3, x_4, N_1) \in C_{SAPKA}$ は多項式時間で破られる．なぜなら，関数 $y_{B,1}$ と $y_{B,2}$ を Alice が正しく計算するために，Bob は x_B と n_B を送信する必要があるためである．

一方向性関数を用いた SAPKA サブクラス

[6] では，任意の一方向性関数 $f : \mathcal{S} \to \mathcal{S}'$ および $x'_1 = x'_2 \circ x'_3$ を満たす $x'_1, x'_2, x'_3 : \mathcal{S} \to \mathcal{S}$ を用いた SAPKA サブクラスが構築されている．このサブクラスでは，f によって Bob の公開鍵 $y_{B,1}$ および $y_{B,2}$ から秘密鍵を簡単に導出できないように定義されている．具体的に Bob は以下の公開鍵を構築する：

$$y_{B,1} := N_1^{-1} \circ x_4 = f \circ x'_3 \tag{13}$$

$$y_{B,2} := x_1 \circ x_2 = f \circ x'_1 \tag{14}$$

このとき，Bob が SSK を計算するためには，関数 $x_3 \circ N_1$ が以下を満たす必要がある．

$$\begin{aligned} x_3 \circ N_1 \circ y_{B,1} &= x_3 \circ N_1 \circ f \circ x'_3 \\ &= f \circ x'_2 \circ x'_3 \end{aligned} \tag{15}$$

$y_{B,1}$，$y_{B,2}$，および $x_3 \circ N_1$ が条件 (13) から (15) を満たす $(x_1, x_2, x_3, x_4, N_1) \in C_{SAPKA}$ の集合を，安全性が一方向性関数 $f : \mathcal{S} \to \mathcal{S}'$ をもとにしていることを強調するために $C_{f,\mathcal{S},\mathcal{S}'}$ と表す．

計算量非対称性を持つ SAPKA アルゴリズム

$C_{f,\mathcal{S},\mathcal{S}'}$ の中に計算量非対称性を持つ鍵共有アルゴリズムが存在することを，具体例を挙げることで示す．この鍵共有アルゴリズムは，[6] で提案されたものであり，定理 1 の D-H の SAPKA 表現に対して，有限体上の指数関数を行列を用いたものに変更し，N_1 を恒等写像でないものとすることで，本質的に非対称な構造 (Alice と Bob で計算規則が異なる) を持たせたものである．また，このアルゴリズムは，Schur-Exponentiation と呼ばれる演算を用いていることから，Schur-Exponentiation based Diffie-Hellman(SEDH) と呼ばれる．以下に SEDH の構成を示す．

準備

$d \in \mathbb{N}^* := \mathbb{N} \setminus \{0\}$ とし，p を大きな素数とする．全ての要素が $\mathbb{Z}_p$ にある d 次元正方行列の集合を $\mathcal{M}(d, \mathbb{Z}_p)$ とする．$\mathbb{Z}_p^d$ は，$\mathbb{Z}_p$ 上の d 次元ベクトル空間で，$\mathbb{Z}_p$ の d 組の順序対より構成される．特に指定がない限り，ベクトル $\boldsymbol{u} \in \mathbb{Z}_p^d$ の"座標"は，標準基底での座標を指す．二項演算 $\odot : \mathbb{Z}_p^d \times \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ を次のように定義する：

$$\boldsymbol{v} \odot \boldsymbol{u} := \begin{pmatrix} \boldsymbol{v}_1 \circ \boldsymbol{u}_1 \\ \vdots \\ \boldsymbol{v}_d \circ \boldsymbol{u}_d \end{pmatrix}$$

ここで，$\circ$ は座標ごとの乗算を表す．このとき，$\mathbb{Z}_p^d$ は $\odot$ に関して乗法半群となり，次のベクトルを単位元とする：

$$1 := \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

以下で表される $\mathbb{Z}_p^d$ の部分集合：

$$\hat{\mathbb{Z}}_p^d := \{\boldsymbol{u} := (u_1, \ldots, u_d) \in \mathbb{Z}_p^d \colon u_j \in \mathbb{Z}_p^* := \mathbb{Z}_p \setminus \{0\},\ j \in \{1, \ldots, d\}\} \subset \mathbb{Z}_p^d$$

は $\odot$ に関して群をなす．以下に Schur-Exponentiation の定義を記述する．

定義 5. スカラー $c \in \mathbb{Z}_p$ による行列 $M \in M(d, \mathbb{Z}_p)$ の *Schur-Exponentiation* は次のように定義される：

$$(c^{\circ M})_{i,j} := c^{M_{i,j}} \qquad ; \qquad i, j \in \{1, \cdots, d\}$$

同様に，ベクトル $c \in \mathbb{Z}_p$ によるベクトル $\boldsymbol{v} \in \mathbb{Z}_p^d$ の *Schur-Exponentiation* は次のように定義される：

$$(c^{\circ \boldsymbol{v}})_i := c^{\boldsymbol{v}_i} \qquad ; \qquad i \in \{1, \cdots, d\}$$

最後に，ベクトルによる行列の *Schur-Exponentiation* は次のように定義されるベクトルである：

$$(y^{\circ M})_i := \prod_{l \in \{1, \ldots, d\}} (y)_l^{(M)_{i,l}} \quad , \quad i \in \{1, \ldots, d\}$$

ここで，$c^{\circ M} \in M(d, \mathbb{Z}_p)$ および $c^{\circ \boldsymbol{v}} \in \hat{\mathbb{Z}}_p^d$ である．また，両方の操作に同じ記号 $\circ$ を使用しているが，各場合においてどの操作が関与しているかは文脈から明らかであることに注意する．

SEDH アルゴリズムでは，Alice と Bob は半群 $\mathcal{S} := (\mathbb{Z}_{p-1}^d, +)$ および $\mathcal{S}' := (\mathbb{Z}_p^d, \odot)$ を選び，これらは公開される．さらに,，Alice と Bob は $\mathcal{Z}_p^*$ の生成元 g を選び，これも公開する．Bob は，N_B が $M(d, \mathbb{Z}_{p-1})$ 内で逆行列を持つような，$M(d, \mathbb{Z}_{p-1})$ の 2 つの行列 x_B と N_B を生成する．これらは，公開せず Bob が秘密裏に持つ．これらを用いて Bob は，次のように $\mathbb{Z}_{p-1}^d$ から $\hat{\mathbb{Z}}_p^d$ への関数 x_2, x_4 および $\hat{\mathbb{Z}}_p^d$ から $\hat{\mathbb{Z}}_p^d$ への関数 x_1, x_3, N_1 を構築する．

$$x_1 := id_{\hat{\mathbb{Z}}_p^d}$$

$$y \in \mathbb{Z}_{p-1}^d \mapsto x_2(y) := g^{\circ x_B y} \in \hat{\mathbb{Z}}_p^d \quad , \quad x_2(y)_i := \prod_{l \in \{1,\dots,d\}} (g^{\circ x_B})_{i,l}^{(y)_l} \in \mathbb{Z}_p^*$$

$$y \in \hat{\mathbb{Z}}_p^d \mapsto x_3(y) := y^{\circ x_B} \in \hat{\mathbb{Z}}_p^d \quad , \quad x_3(y)_i := \prod_{l \in \{1,\dots,d\}} (y)_l^{(x_B)_{i,l}} \in \mathbb{Z}_p^*$$

$$y \in \mathbb{Z}_{p-1}^d \mapsto x_4(y) := g^{\circ y} \in \hat{\mathbb{Z}}_p^d$$

$$y \in \hat{\mathbb{Z}}_p^d \mapsto N_1(y) := y^{\circ N_B^{-1}} \in \hat{\mathbb{Z}}_p^d \quad , \quad N_1(y)_i := \prod_{l \in \{1,\dots,d\}} (y)_l^{(N_B^{-1})_{i,l}} \in \mathbb{Z}_p^*$$

x_1, x_2, x_3, x_4 は定義 3 の意味で互換性があることに注意する．実際,

$$x_1 \circ x_2(y) = g^{\circ x_B y} = x_3 \circ x_4(y) = x_3(g^{\circ y}) = (g^{\circ y})^{\circ x_B} = (g^{\circ x_B y}) \tag{16}$$

ここで，最後の等号は次のことから成り立つ．

$$((g^{\circ y})^{\circ x_B})_i = \prod_{l \in \{1,\dots,d\}} (g^{\circ y})_l^{(x_B)_{i,l}} = \prod_{l \in \{1,\dots,d\}} (g^{y_l})^{(x_B)_{i,l}} = \prod_{l \in \{1,\dots,d\}} (g^{(x_B)_{i,l} y_l})$$

$$= g^{\sum_{l \in \{1,\dots,d\}} (x_B)_{i,l} y_l} = (g^{x_B y})_i$$

4.4 Key agreement of SE-DH

Step 1(Bob) Bob は以下の $y_{B,1}$ と $y_{B,2}$ を構築し，Alice に送る．

$$\begin{aligned} y_{B,1}(y)_i &:= N_1^{-1} \circ x_4(y)_i \\ &= \prod_{l \in \{1,\dots,d\}} (g^{\circ y})_l^{(N_B)_{i,l}} \\ &= \prod_{l \in \{1,\dots,d\}} (g^{\circ N_B})_{i,l}^{(y)_l} \end{aligned} \tag{17}$$

$$\begin{aligned} y_{B,2}(y)_i &:= x_1 \circ x_2(y)_i \\ &= \prod_{l \in \{1,\dots,d\}} (g^{\circ x_B})_{i,l}^{(y)_l} \end{aligned} \tag{18}$$

ここで $i \in \{1,\ldots,d\}$ とする．また，$y_{B,1}$ は，以下のように構成される $\mathbb{Z}_{p-1}^d$ から $\hat{\mathbb{Z}}_p^d$ への写像であるとみなすこともできる．

$$
\begin{aligned}
y \in \mathbb{Z}_{p-1}^d \mapsto y_{B,1}(y) &= N_1^{-1} \circ x_4(y) \\
&= N_1^{-1}(g^{\circ y}) \\
&= (g^y)^{\circ N_B} \\
&= g^{\circ N_B y} \in \hat{\mathbb{Z}}_p^d
\end{aligned}
$$

同様に $y_{B,2}$ も以下のように表せる．

$$
y \in \mathbb{Z}_{p-1}^d \mapsto y_{B,2}(y) = g^{\circ x_B y} \in \hat{\mathbb{Z}}_p^d
$$

Bob が $y_{B,1}$ と $y_{B,2}$ を Alice に送るということは，上記のように，Bob が $y_{B,1}$ と $y_{B,2}$ を計算するために必要な何らかの値を送信することを意味する．この場合，これは $g^{\circ N_B}, g^{\circ x_B} \in M(d, \mathbb{Z}_p)$ の行列を送ることに相当する．

Step 1(Alice) Alice は x_A を $\mathbb{Z}_{p-1}^d$ から任意に選び，自身の秘密鍵とする．次に Alice は，Bob の公開鍵の一つである $y_{B,1}$ と自分の秘密鍵 x_A を用いて，次のように自身の公開鍵 y_A を計算する（$i \in \{1,\ldots,d\}$）．

$$
\begin{aligned}
(y_A)_i := y_{B,1}(x_A)_i &= N_1^{-1} \circ x_4(x_A)_i \\
&= \prod_{l \in \{1,\ldots,d\}} (g^{\circ N_B})_{i,l}^{(x_A)_l} \\
&= (g^{\circ N_B x_A})_i
\end{aligned} \tag{19}
$$

Step 2(Alice) Alice は，Bob のもう一つの公開鍵 $y_{B,2}$ と，秘密鍵 x_A を用いて，次のように κ_A で表される自身の SSK を計算する（$i \in \{1,\ldots,d\}$）．

$$
\begin{aligned}
(\kappa_A)_i := y_{B,2}(x_A)_i &= x_1 \circ x_2(x_A)_i \\
&= \prod_{l \in \{1,\ldots,d\}} (g^{\circ x_B})_{i,l}^{(x_A)_l} \\
&= (g^{\circ x_B x_A})_i
\end{aligned} \tag{20}
$$

Step 2(Bob) Bob は，y_A を使用して κ_B で表される，自身の SSK を計算する（$i \in \{1,\ldots,d\}$）．

$$
\begin{aligned}
(\kappa_B)_i := x_3 \circ N_1(y_A)_i &= x_3 \circ N_1 \circ N_1^{-1} \circ x_4(x_A)_i \\
&= x_3 \circ N_1(g^{\circ N_B x_A})_i \\
&= \prod_{l \in \{1,\ldots,d\}} (g^{\circ N_B x_A})_l^{(x_B N_B^{-1})_{i,l}} \\
&= g^{\sum_{l \in \{1,\ldots,d\}} (N_B x_A)_l (x_B N_B^{-1})_{i,l}} \\
&= g^{(x_B N_B^{-1} N_B x_A)_i} \\
&= g^{(x_B x_A)_i} = (g^{\circ x_B x_A})_i
\end{aligned} \tag{21}
$$

今 (16) が成り立つことより,$\kappa_A = \kappa_B$ が成立する．

注意 2. 関数 $x'_1, x'_2, x'_3 : \mathcal{S} \to \mathcal{S}$ をそれぞれ $x_1(y) = x_B y$, $x'_2(y) = x_B N_B^{-1}$, $x'_3(y) = N_B y$ $(y \in \mathcal{S})$ と定義すると，$x'_1 = x'_2 \circ x'_3$ が成り立つ (この $\circ$ は関数の合成を表す). $f : \mathcal{S} \to \mathcal{S}'$ を $f(x) = g^{\circ x}$ $(x \in \mathcal{S})$ と定義すると，これは例 2 の有限体上の指数関数を独立かつ同時に d 回行う計算であるため，DLP の難しさを仮定した際は，この f は一方向性関数である．また，Bob の公開鍵 $y_{B,1}$ と $y_{B,2}$ は以上の関数を用いて，それぞれ (13) と (14) の右辺の形で表現することができる．また，$x_3 \circ N_1$ は (15) を満たしているので，$SEDH$ は $C_{f,\mathcal{S},\mathcal{S}'}$ の要素である．

また，以上の構成より次の結果が得られることに注意する．

補題 1. 以下の g, f, y_A と x_A は上で定義したものであるとする．$x_E \in \mathcal{S}$ に対して，$N_1^{-1} \circ x_4(x_E) = y_A$ が成り立つならば，$x_E = x_A$ である．

Proof. 今，$g \in \mathbb{Z}_p^*$ は生成元なので f は全単射である．従って，$y_A = N_1^{-1} \circ x_4(x_E) = f \circ x'_3(x_E)$ に対して，$x := x'_3(x_E)$ は $f(x) = y_A$ を満たすただ一つの f への入力となる．また，$x'_3(y) = N_B y$ であり，N_B は $M(d, \mathbb{Z}_{p-1})$ 上で正則なので，x_E は $x = x'_3(x_E)$ を満たすただ一つの x'_3 への入力である．$y_A = f \circ x'_3(x_A)$ でもあるので $x_E = x_A$ である． □

4.5 SEDH の計算量非対称性

SEDH の計算量非対称性について議論する．この場合の"計算的非対称性"とは，もし x_A が Bob の秘密鍵が選ばれる集合よりもはるかに小さい集合から選ばれたとしても，Alice の秘密鍵 x_A の安全性が Bob の秘密鍵（すなわち $x_B \in \mathcal{M}(d, \mathbb{Z}_n)$ および $N_B \in \mathcal{M}(d, \mathbb{Z}_n)$）と同等のレベルであることを意味する．これを証明するために，次の記法と Eve に関するいくつかの条件設定を導入する．ただし，以下の n_0 は (5) を満たす自然数であるとする．これを証明するために，次の記法と Eve に関するいくつかの条件設定を導入する．f を注意 2 で定義したものとし，以下の n_0 は (5) を満たす自然数であるとする．

(a) まず，$f : \mathcal{S} \to \mathcal{S}'$ は一方向性関数であるとし，g が $\mathbb{Z}_p^*$ の生成元であることより全単射である．これは，$|\mathcal{S}|_B = n' \geq n_0$ であり，任意の $a \in \mathcal{S}$ に対して $f(a)$ を計算することが多項式時間で可能であることを意味する．しかし，与えられた $f(a) \in \mathcal{S}'$ に対して，$a = f^{-1}(f(a)) \subset G_1$ を見つけることは多項式時間制約内では実現不可能である．具体的には，任意の確率的多項式時間アルゴリズム A' と任意の正の多項式 p に対して，以下が成立する．

$$\Pr[A'(f(U_{\mathcal{S}})) = f^{-1}(f(U_{\mathcal{S}}))] < \frac{1}{p(n')} \tag{22}$$

(b) ある整数 $m < n_0$ に対して，任意の部分集合 $H \subset \mathcal{S}$ で $|\mathcal{S}|_B \leq m$ を満たすものに制限された f は上述のように一方向性ではない．今，任意の $g \in \mathbb{Z}_p^*$ に対して，$T_g = \{g^{\circ x} \mid x \in \mathbb{Z}_{2^m}^d, g \in \mathbb{Z}_p^*\}$ とすると，$|T_g|_B = m$ を満たす．全ての $g \in \mathbb{Z}_p^*$ に対して，$f : T_g \to \mathcal{S}'$ が一方向性関数ではないことを次のように定式化できる．すなわち，確率的多項式時間アルゴリズム A'' と正の多項式 p' が存在し，以下が成立する．

$$\Pr[A''(f(U_{T_g})) = f^{-1}(f(U_{T_g}))] \geq \frac{1}{p'(m)} \tag{23}$$

今 m と $d \in \mathbb{N} \setminus \{1\}$ の間に以下の多項式関係が成立しているとし，Alice の秘密鍵 x_A は公開値 $g \in \mathbb{Z}_p^*$ に対して，T_g から選ばれるとする．このとき，次の結果が得られる．

定理 3. *SEDH* において *Eve* が上記の (a) および (b) の制限を受けているとき，*Eve* が y_A から x_A を得るための計算量は，一方向性関数 f を破るのと同等である．

この定理の証明は非常に長いため [6] に詳細は任せる．以下に証明のアイデアの方針のみ記載する．証明は，Eve が y_A から x_A を見つける問題を多項式時間で解けるとしたとき，この問題を解くアルゴリズムを利用して f の逆像を求めることができる，つまり f が一方向性を持つという仮定に矛盾が生じることを示すことで，定理が示される．

以下は，x_A を y_A より導出する難しさに関する考察であり，上の定理の証明とはならないものの，直感的な理解を助けるためのものである．

考察 1.

1. 今 $\mathcal{S}'$ は $\odot$ の下で群である．したがって，任意の $j \in \{1, \ldots, d\}$ および $\boldsymbol{a}, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_{j-1}, \boldsymbol{b}_{j+1}, \ldots, \boldsymbol{b}_d \in \mathcal{S}'$ に対して，$\boldsymbol{a} = \boldsymbol{b}_1 \odot \cdots \odot \boldsymbol{b}_{j-1} \odot \boldsymbol{b}_j \odot \boldsymbol{b}_{j+1} \odot \cdots \odot \boldsymbol{b}_d$ を満たす一意の $\boldsymbol{b}_j$ が存在する．言い換えれば、与えられた $\boldsymbol{a} \in \hat{\mathbb{Z}}_p^d$ に対して，ある $j \in \{1, \ldots, d\}$ 以外のすべての i で $\boldsymbol{b}_i$ が任意に選ばれても，$\boldsymbol{a} = \boldsymbol{b}_1 \odot \cdots \odot \boldsymbol{b}_d$ を満たす $\boldsymbol{b}_j$ が常に存在する．

2. *Alice* の秘密鍵 x_A を $x_A = (\alpha_1, \ldots, \alpha_d) \in \mathcal{S}$ と表し，*Bob* の秘密鍵 N_B を $N_B = (\boldsymbol{n}_1, \boldsymbol{n}_2, \ldots, \boldsymbol{n}_d)$ と列ベクトル $\boldsymbol{n}_i \in \mathcal{S}$ を並べたもので表し，集合 $S_{g^{\circ \boldsymbol{n}_i}}$ を $S_{g^{\circ \boldsymbol{n}_i}} := \{g^{\circ k \boldsymbol{n}_i} \mid k \in \{1, \ldots, 2^m\}\}$ と定義する（すべての $i \in \{1, \ldots, d\}$ について）．任意の $j \in \{1, \ldots, d\}$ を固定すると，*1.* の議論から，任意の $\boldsymbol{b}_i \in S_{g^{\circ \boldsymbol{n}_i}}$ $(i \neq j)$ に対して $\boldsymbol{b}_j \in \mathcal{S}'$（必ずしも $S_{g^{\circ \boldsymbol{n}_j}}$ に属するわけではない）が存在し，以下を満たす：

$$y_A = \boldsymbol{b}_1 \odot \boldsymbol{b}_2 \odot \cdots \odot \boldsymbol{b}_d \tag{24}$$

ここから先は一般性を失うことなく $j = d$ とする．この議論により，任意の $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{d-1}) \in S_{g^{\circ \boldsymbol{n}_1}} \times \cdots \times S_{g^{\circ \boldsymbol{n}_{d-1}}}$ が (24) の解候補となり得ると考えることができる．

3. 今すべての $g^{\circ \boldsymbol{n}_i}$ が公開されていることより，$\boldsymbol{a}_i = g^{\circ \alpha_i \boldsymbol{n}_i}$ とすると，もし *Eve* が y_A から x_A を効率的に導出できるならば，すべての $\boldsymbol{a}_i$ を簡単に計算できる．逆に，*Eve* が次の集合から $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{d-1})$ を効率的に見つけることができるならば：

$$S := \{(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{d-1}) \in S_{g^{\circ \boldsymbol{n}_1}} \times \cdots \times S_{g^{\circ \boldsymbol{n}_{d-1}}}\}$$

これを用いて $\boldsymbol{a}_d$ を $\boldsymbol{a}_d = \boldsymbol{a}_{d-1}^{-1} \odot \cdots \boldsymbol{a}_1^{-1} \odot y_A$ と計算する．状況設定 **(b)** より，*Eve* はすべての $i \in \{1 \ldots, d\}$ について $\log_{g^{\circ \boldsymbol{n}_i}} \boldsymbol{a}_i$ *(*$= \log_{g^{\circ \boldsymbol{n}_i}} g^{\circ \alpha_i \boldsymbol{n}_i} = \alpha_i$*)* を (23) の右辺以上の確率で多項式時間で計算できる．これは，y_A から x_A を見つける問題が S から $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{d-1})$ を見つける問題と同等であることを意味する *(*本来ならば，**(b)** の確率的多項式時間アルゴリズム A'' を有限個用いて，すべての α_i を求めることができる確率がある多項式分の *1* 以上であることを示さないといけないが，煩雑なため省略する*)*.

このとき注目すべきは，すべての i について，*Eve* は *Alice* によって計算された $g^{\circ \alpha_i \boldsymbol{n}_i}$ の値を知らないという点である．従って *Eve* は x_A を求めるために $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{d-1})$ を S より探し当てなければならない．今 S の任意の $(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{d-1})$ が $(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_{d-1})$ の候補であり，もし *Alice* が T_g から x_A を均一に選ぶならば，*Eve* にとって，各 $\boldsymbol{a}_i$ は $S_{g^{\circ \boldsymbol{n}_i}}$ 上で一様に分布しているように見える．公開情報以外に x_A に関する手がかりを何も持たないのであれば，*Eve* は S 上での全探索を実行し *1* つの解を見つけることが必要であるが，集合 S の大きさは $2^{m(d-1)}$ 上であり，たとえ m が小さく選ばれても，d を任意に大きくすることで全探索の実行時間を任意に大きくすることができる *(*$n' = md$ などとすれば良い*)*.

References

[1] Luigi Accardi, Satoshi Iriyama, Massimo Regoli, and Masanori Ohya. Strongly asymmetric public key agreement algorithms. In Technical Report ISEC2011-20; IEICE: Tokyo, Japan, pages 115–121, 2011.

[2] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect forward secrecy: How diffie-hellman fails in practice. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15, page 5–17, New York, NY, USA, 2015. Association for Computing Machinery.

[3] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science, 560:7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[4] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6):644–654, 1976.

[5] Oded Goldreich. Foundations of cryptography. ii: Basic applications. 2, 05 2004.

[6] Satoshi Iriyama, Koki Jimbo, and Massimo Regoli. New subclass framework and concrete examples of strongly asymmetric public key agreement. Applied Sciences, 11(12), 2021.

[7] U.M. Maurer. Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory, 39(3):733–742, 1993.

[8] C. E. Shannon. Communication theory of secrecy systems. The Bell System Technical Journal, 28(4):656–715, 1949.

[9] Douglas R Stinson. Cryptography: theory and practice. Chapman and Hall/CRC, 2005.

[10] Wade Trappe. Introduction to cryptography with coding theory. Pearson Education India, 2006.

Bilinear oscillatory Fourier multipliers *

至田　直人†

1　導入

1.1　線形の場合について

まず，線形のフーリエ乗法作用素について考える．$\mathbb{R}^n$ 上の有界な関数 θ に対して，フーリエ乗法作用素 $\theta(D)$ は

$$\theta(D)f(x) = \frac{1}{(2\pi)^n}\int_{\mathbb{R}^n} e^{ix\cdot\xi}\theta(\xi)\widehat{f}(\xi)\,d\xi, \quad x\in\mathbb{R}^n,$$

と定義される線形作用素である．ただし，f は $\mathbb{R}^n$ 上のシュワルツの急減少関数，$\widehat{f}$ はそのフーリエ変換を表わす．θ のことをマルチプライヤーと表わす．

X および Y は（擬）ノルム $\|\cdot\|_X$ および $\|\cdot\|_Y$ をそれぞれ備えた $\mathbb{R}^n$ 上の関数空間とする．フーリエ乗法作用素 $\theta(D)$ が $X\to Y$ 有界であるとは，ある $C>0$ が存在して，

$$\big\|\theta(D)f\big\|_Y \le C\|f\|_X, \quad f\in\mathcal{S}\cap X,$$

が成立することをあらわす．ここで，$\mathcal{S}=\mathcal{S}(\mathbb{R}^n)$ は $\mathbb{R}^n$ 上のシュワルツの急減少関数全体をあらわす．本稿では，ルベーグ空間 L^p，ハーディー空間 H^p および有界平均振動関数全体の成す空間 BMO 上での有界性について考える．

ハーディー空間 $H^p=H^p(\mathbb{R}^n)$ とは，$0<p\le\infty$ に対して，

$$H^p(\mathbb{R}^n) = \Big\{ f\in\mathcal{S}'(\mathbb{R}^n) \ : \ \|f\|_{H^p} = \Big\| \sup_{t>0}\big|t^{-n}\phi(t^{-1}\cdot)*f\big| \Big\|_{L^p} < \infty \Big\}$$

と定義される関数空間である．ただし，$\phi\in\mathcal{S}(\mathbb{R}^n)$ は $\int_{\mathbb{R}^n}\phi(x)dx \ne 0$ を満たす．ハーディー空間の定義は ϕ の取り方に依存しない．また，$1<p\le\infty$ の場合は，$H^p=L^p$ であり，$p=1$ の場合は $H^1\hookrightarrow L^1$ であることが知られている．

有界平均振動関数全体の成す空間 $BMO=BMO(\mathbb{R}^n)$ は

$$BMO(\mathbb{R}^n) = \Big\{ f\in L^1_{loc}(\mathbb{R}^n) \ : \ \|f\|_{BMO} = \sup_Q \frac{1}{|Q|}\int_Q |f(x)-f_Q|\,dx < \infty \Big\}$$

と定義される関数空間である．ここで，$\sup_Q$ は軸に平行な辺をもつ $\mathbb{R}^n$ の立方体 Q 全体についての上限を表わし，f_Q は立方体 Q 上の積分平均，すなわち，$f_Q=|Q|^{-1}\int_Q f$ であ

---

*本講演は，宮地晶彦氏（東京女子大），冨田直人氏（大阪大），加藤睦也氏（岐阜大）との共同研究に基づく．

†名古屋大学多元数理科学研究科

る．$L^\infty(\mathbb{R}^n) \subset BMO(\mathbb{R}^n)$ であることが知られている．これらの関数空間の詳細については，例えば，Stein [13, Chapters III and IV] をみよ．

さて，$s > 0$ とし，以下の形のマルチプライヤーを考える：

$$\theta(\xi) = e^{i|\xi|^s}(1 + |\xi|^2)^{m/2}.$$

この形のマルチプライヤーに対応するフーリエ乗法作用素に対する有界性について，以下のことが知られている．

Theorem A (Sjölin [12], Miyachi [7]). $n \geq 1$, $s \neq 1$, $1 \leq p \leq \infty$, $m \in \mathbb{R}$ とし，$\sigma(\xi) = (1 + |\xi|^2)^{m/2}$ とおく．このとき，フーリエ乗法作用素 $e^{i|D|^s}\sigma(D)$ が $H^p \to H^p$ 有界であるための必要十分条件は

$$m \leq -ns\Big|\frac{1}{p} - \frac{1}{2}\Big| \tag{1.1}$$

である．ただし，$p = \infty$ の場合は H^p を BMO に置き換える．

本稿では，この Theorem A の双線形の場合への拡張を考える．

Remark 1.1. $s = 1$ の場合には，(1.1) の条件を

$$m \leq -(n-1)\Big|\frac{1}{p} - \frac{1}{2}\Big|$$

に置き換えて，Theorem A と同じ主張が成立することが知られている．ただし，$n \geq 2$ である．$s = 1$ の場合の結果については，例えば，Miyachi [6]，Seeger–Sogge–Stein [14] などを参照されたい．

1.2 双線形の場合について

次に，双線形の場合について考える．$\mathbb{R}^n \times \mathbb{R}^n$ 上の有界な関数 $\sigma = \sigma(\xi, \eta)$ に対して，双線形フーリエ乗法作用素 T_σ は

$$T_\sigma(f, g)(x) = \frac{1}{(2\pi)^{2n}} \int_{\mathbb{R}^{2n}} e^{ix\cdot(\xi+\eta)}\sigma(\xi, \eta)\widehat{f}(\xi)\widehat{g}(\eta)\, d\xi d\eta, \quad x \in \mathbb{R}^n,$$

と定義される双線形作用素である．ただし，f および g は $\mathbb{R}^n$ 上のシュワルツの急減少関数とし，$\widehat{f}$ および $\widehat{g}$ はそのフーリエ変換をそれぞれ表わす．

X, Y および Z は（擬）ノルム $\|\cdot\|_X$，$\|\cdot\|_Y$ および $\|\cdot\|_Z$ をもつ $\mathbb{R}^n$ 上の関数空間とする．T_σ が $X \times Y \to Z$ 有界であるとは，ある $C > 0$ が存在して，

$$\big\|T_\sigma(f, g)\big\|_Z \leq C\|f\|_X\|g\|_Y, \quad f \in \mathcal{S} \cap X, \ \ g \in \mathcal{S} \cap Y,$$

が成立することを表わす．

本稿では，$s > 0$ として，

$$e^{i|\xi|^s}e^{i|\eta|^s}\sigma(\xi, \eta)$$

といった形の双線形のマルチプライヤーを考える．対応する双線形フーリエ乗法作用素を T^s_σ と表わす．すなわち，T^s_σ を

$$T^s_\sigma(f, g)(x) = \frac{1}{(2\pi)^{2n}} \int_{\mathbb{R}^{2n}} e^{ix\cdot(\xi+\eta)}e^{i|\xi|^s}e^{i|\eta|^s}\sigma(\xi, \eta)\widehat{f}(\xi)\widehat{g}(\eta)\, d\xi d\eta, \quad x \in \mathbb{R}^n$$

と定義する．ここで，σ は次で定義されるクラスに属しているものを考える．

Definition 1.2. $m \in \mathbb{R}$ にとする．$\sigma = \sigma(\xi, \eta) \in S^m_{1,0}(\mathbb{R}^{2n})$ ですべての $\alpha, \beta \in (\mathbb{N}_0)^n = \{0, 1, 2, \dots, \}^n$ に対して，

$$\left|\partial_\xi^\alpha \partial_\eta^\beta \sigma(\xi, \eta)\right| \le C_{\alpha,\beta}(1 + |\xi| + |\eta|)^{m-|\alpha|-|\beta|}$$

を満たすもの全体を $S^m_{1,0}(\mathbb{R}^{2n})$ と定義する．

さて，以下では $s \neq 1$ の場合を考えよう．最近，Bergfeldt–Rodoríguez-López–Rule–Staubach [1] では，以下のことが示された．

Theorem B ([1, Theorem 1.4])**.** $n \ge 1$, $s \neq 1$ とし，$1 \le p, q \le \infty$, $1/r = 1/p + 1/q$ とする．このとき，

$$m = -ns\Big(\Big|\frac{1}{p} - \frac{1}{2}\Big| + \Big|\frac{1}{q} - \frac{1}{2}\Big|\Big) \tag{1.2}$$

ならば，すべての $\sigma \in S^m_{1,0}(\mathbb{R}^{2n})$ に対して，双線形フーリエ乗法作用素 T^s_σ は $H^p \times H^q \to L^r$ 有界である．ただし，$p = q = r = \infty$ ならば，$L^\infty \times L^\infty \to BMO$ 有界である．

指数 $m = -ns(|1/p - 1/2| + |1/q - 1/2|)$ がシャープなものであるかどうかについて，彼らは次のことを示している（[1, Section 3.2]）．

Theorem C. $n \ge 1$, $s \neq 1$ とし，$1 \le p, q \le 2$ または $2 \le p, q \le \infty$, $1/r = 1/p + 1/q$ とする．このとき，すべての $\sigma \in S^m_{1,0}(\mathbb{R}^{2n})$ に対して，双線形フーリエ乗法作用素 T^s_σ が $H^p \times H^q \to L^r$ 有界（ただし，$p = q = r = \infty$ ならば，$L^\infty \times L^\infty \to BMO$ 有界）であるならば，

$$m \le -ns\Big(\Big|\frac{1}{p} - \frac{1}{2}\Big| + \Big|\frac{1}{q} - \frac{1}{2}\Big|\Big)$$

である．

本稿の目的は，$1 \le p < 2 < q \le \infty$ または $1 \le q < 2 < p \le \infty$ の場合に，彼らの結果を改良することである．

主結果を述べるために，$m_s(p, q)$ を以下のように定義する：
$0 < s < 1$ のとき，

$$m_s(p,q) = \begin{cases} -ns\big(|\frac{1}{p} - \frac{1}{2}| + |\frac{1}{q} - \frac{1}{2}|\big) & \text{for } (1/p, 1/q) \in \mathrm{I} \cup \mathrm{II}, \\ -ns(1-s)\big|\frac{1}{p} - \frac{1}{2}\big| - ns\big|\frac{1}{q} - \frac{1}{2}\big| & \text{for } (1/p, 1/q) \in \mathrm{III} \cup \mathrm{VI}, \\ -ns\big|\frac{1}{p} - \frac{1}{2}\big| - ns(1-s)\big|\frac{1}{q} - \frac{1}{2}\big| & \text{for } (1/p, 1/q) \in \mathrm{IV} \cup \mathrm{V}. \end{cases}$$

$s > 1$ のとき，

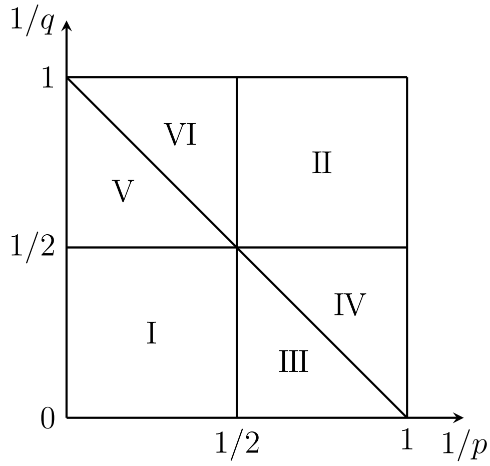
$$m_s(p,q) = \begin{cases} -ns\big(|\frac{1}{p} - \frac{1}{2}| + |\frac{1}{q} - \frac{1}{2}|\big) & \text{for } (1/p, 1/q) \in \mathrm{I} \cup \mathrm{II}, \\ -ns\big|\frac{1}{q} - \frac{1}{2}\big| & \text{for } (1/p, 1/q) \in \mathrm{III} \cup \mathrm{VI}, \\ -ns\big|\frac{1}{p} - \frac{1}{2}\big| & \text{for } (1/p, 1/q) \in \mathrm{IV} \cup \mathrm{V}. \end{cases}$$

ただし，$\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{V}, \mathrm{VI}$ は以下で定義される範囲を表す．

$$\begin{aligned} \mathrm{I} &= \{0 \le 1/p, 1/q \le 1/2\}, \\ \mathrm{II} &= \{1/2 \le 1/p, 1/q \le 1\}, \end{aligned}$$

$$
\begin{aligned}
\mathrm{III} &= \{0 \le 1/q \le 1/2 \le 1/p \le 1,\ \ 1/p + 1/q \le 1\},\\
\mathrm{IV} &= \{0 \le 1/q \le 1/2 \le 1/p \le 1,\ \ 1/p + 1/q \ge 1\},\\
\mathrm{V} &= \{0 \le 1/p \le 1/2 \le 1/q \le 1,\ \ 1/p + 1/q \le 1\},\\
\mathrm{VI} &= \{0 \le 1/p \le 1/2 \le 1/q \le 1,\ \ 1/p + 1/q \ge 1\}.
\end{aligned}
$$

$\mathrm{I}\cup\mathrm{II}\cup\mathrm{III}\cup\mathrm{IV}\cup\mathrm{V}\cup\mathrm{VI} = \{0 \le 1/p, 1/q \le 1\}$ である．また，各範囲は以下の図のように割り当てられたものである．



本稿の主結果は以下の通りである．

Theorem 1.3 ([5, Theorem 1.3])**.** $n \ge 1$, $1 \le p, q \le \infty$, $1/r = 1/p + 1/q$ とし，$0 < s < 1$ または $s > 1$ とする．このとき，

$$m = m_s(p, q)$$

ならば，すべての $\sigma \in S^m_{1,0}(\mathbb{R}^{2n})$ に対して，双線形フーリエ乗法作用素 T^s_σ は $H^p \times H^q \to L^r$ 有界である．ただし，$p = q = r = \infty$ ならば，$L^\infty \times L^\infty \to BMO$ 有界である．

まず，$(1/p, 1/q) \in \mathrm{I} \cup \mathrm{II}$ の場合は，

$$m_s(p, q) = -ns\Big|\frac{1}{p} - \frac{1}{2}\Big| - ns\Big|\frac{1}{q} - \frac{1}{2}\Big|$$

であり，上記の Theorem B で述べた Bergfeldt, Rodríguez-López, Rule, Staubach らの結果 [1] と同じ主張である．ところが，$(1/p, 1/q) \in \mathrm{III} \cup \mathrm{IV} \cup \mathrm{V} \cup \mathrm{VI}$ の場合は，$1/p = 1/2$ あるいは $1/q = 1/2$ の場合を除いて，

$$m_s(p, q) > -ns\Big|\frac{1}{p} - \frac{1}{2}\Big| - -ns\Big|\frac{1}{q} - \frac{1}{2}\Big|$$

である．ゆえに，Theorem 1.3 は Theorem B の改良となっていることがわかる．

さらに，我々が与えた指数 $m = m_s(p, q)$ は，ある範囲においてはシャープなものになっている．本稿の 2 つ目の主結果は以下のとおりである．

Theorem 1.4 ([5, Theorem 1.4])**.** $n \ge 1$, $(1/p, 1/q) \in \mathrm{I} \cup \mathrm{II} \cup \mathrm{IV} \cup \mathrm{VI}$, $1/r = 1/p + 1/q$, $m \in \mathbb{R}$ とし，$0 < s < 1$ または $1 < s < \infty$ とする．このとき，すべての $\sigma \in S^m_{1,0}(\mathbb{R}^{2n})$ に対して，双線形フーリエ乗法作用素 T^s_σ が $H^p \times H^q \to L^r$ 有界である（ただし，$p = q = r = \infty$ のときは，$L^\infty \times L^\infty \to BMO$ 有界）であるならば，$m \le m_s(p, q)$ である．

この定理から，$(1/p,1/q)\in \mathrm{I}\cup\mathrm{II}\cup\mathrm{IV}\cup\mathrm{VI}$ の場合には $m=m_s(p,q)$ はシャープな指数になっていることがわかる．$(1/p,1/q)\in \mathrm{I}\cup\mathrm{II}$ の場合は Bergfeldt, Rodríguez-López, Rule, Staubach の主張と同じものであるが，[5] では異なる証明を与えている．$(1/p,1/q)\in \mathrm{III}\cup\mathrm{V}$ の場合に $m_s(p,q)$ がシャープな指数かどうかについては現在のところ不明なままである．

Remark 1.5. $s=1$ の場合に対する双線形フーリエ乗法作用素 T_σ^1 の有界性に関する研究は Grafakos–Peloso [2] からはじまり, その後，Rodríguez-López, Rule, Staubach らの一連の研究 [9, 10, 11] によって進展が与えられている．ごく最近，彼らの結果はさらに改良できることが Kato–Miyachi–Tomita [4] において明らかになっている．本稿の研究は [4] に刺激を受けて始めたものであるが，本稿の主題は $s\neq 1$ の場合であるから，結果の詳細を述べることについては省略する．

2 証明の準備

この節では，証明に使う記号や補題を準備する．

2.1 関数空間について

局所ハーディー空間 $h^1=h^1(\mathbb{R}^n)$ とは

$$h^1(\mathbb{R}^n)=\left\{f\in\mathcal{S}'(\mathbb{R}^n)\ :\ \|f\|_{h^1}=\left\|\sup_{0<t<1}\left|t^{-n}\phi(t^{-1}\cdot)*f\right|\right\|_{L^1}<\infty\right\}$$

と定義される関数空間である．ここで，$\phi\in\mathcal{S}(\mathbb{R}^n)$ で，$\int\phi\neq 0$ を満たす．局所ハーディー空間は Goldberg [3] により定義された関数空間である．局所ハーディー空間の定義は ϕ の取り方によらないことが知られている．また，$H^1\hookrightarrow h^1\hookrightarrow L^1$ であることが知られている．局所ハーディー空間 h^1 に属する関数は以下を満たすアトムと呼ばれる関数に分解される（[3]）：

$$\operatorname{supp} a\subset\{|y-\bar{y}|\le r\},\quad \|a\|_{L^\infty}\le r^{-n}. \tag{2.1}$$

さらに，$r<1$ の場合は

$$\int_{\mathbb{R}^n}a(x)\,dx=0 \tag{2.2}$$

を満たすとする．(2.1) を $r\ge 1$ として満たすアトム f は (2.1) を $r=1$ として満たすアトムの線形結合で表わすことができることが知られている．このことの詳細については，例えば，Miyachi-Tomita [8] を参照．$r<1$ に対して，(2.1) と (2.2) を満たすアトム f を h^1-*atom of first kind* という．また，(2.1) を $r=1$ として満たすものを h^1-*atom of second kind* と呼ぶ（モーメント条件は課さない）．これらの 2 種類のアトムをまとめて h^1-アトムと呼ぶ．任意の $h^1(\mathbb{R}^n)$ の関数は h^1-アトムの列 $\{a_j\}_j$ を用いて分解できることが知られている．

2.2 補題

$\theta \in \mathcal{S}(\mathbb{R}^n)$ は $\operatorname{supp}\theta \subset \{|\xi| \le 2\}$ を満たすものとする．

$\varphi \in C_0^\infty(\mathbb{R}^n)$ は $\operatorname{supp}\varphi \subset \{|\xi| \le 2\}$ であり，$|\xi| \le 1$ ならば $\varphi(\xi) = 1$ であるとし，$\zeta = 1 - \varphi$ と定める．$\zeta \in C^\infty(\mathbb{R}^n)$ であり，$|\xi| \le 1$ ならば $\zeta(\xi) = 0$ であり，$|\xi| \ge 2$ ならば $\zeta(\xi) = 1$ である．

次の線形のフーリエ乗法作用素に対するいくつかの評価が重要な役割を果たす：

$$S_j f(x) = \Big(e^{i|\xi|^s}\,\zeta(\xi)\theta(2^{-j}\xi)\,\widehat{f}(\xi)\Big)^\vee(x), \quad Tf(x) = \Big(e^{i|\xi|^s}\,\varphi(\xi)\widehat{f}(\xi)\Big)^\vee(x).$$

ただし，$j \in \mathbb{N}_0$ であり，$\vee$ はフーリエ逆変換

$$(g)^\vee(x) = \frac{1}{(2\pi)^n}\int_{\mathbb{R}^n} e^{i\xi\cdot x} g(\xi)\,d\xi$$

を表わす．これらは積分核の表示を用いることで，以下のようにも表わすことができる：

$$S_j f(x) = K_j * f(x), \qquad K_j(x) = \Big(e^{i|\xi|^s}\,\zeta(\xi)\theta(2^{-j}\xi)\Big)^\vee(x),$$
$$Tf(x) = L * f(x), \qquad L(x) = \Big(e^{i|\xi|^s}\,\theta(\xi)\Big)^\vee(x).$$

積分核 K_j について，以下が成立する（[5, Corollary 3.2]）．

Lemma 2.1 ([5, Corollary 3.2]). *(1)* $0 < s < 1$ のとき．$N > 0$ とする．ある $c > 0$ が存在して，

$$\big|K_j(x)\big| \le c \times \begin{cases} |x|^{-\frac{n}{2}-\frac{n}{2(1-s)}}, & \textit{if } |x| \le 1, \\ |x|^{-N}, & \textit{if } |x| > 1, \end{cases}$$

がすべての $j \in \mathbb{N}_0$ について成立する．

(2) $s > 1$ のとき．$N > 0$ とする．ある $c > 0$ が存在して，

$$\big|K_j(x)\big| \le c \times \begin{cases} \big(1+|x|\big)^{-\frac{n}{2}+\frac{n}{2(s-1)}}, & \textit{if } |x| \le s8^{s-1}\,2^{j(s-1)}, \\ |x|^{-N}, & \textit{if } |x| > s8^{s-1}\,2^{j(s-1)}, \end{cases}$$

がすべての $j \in \mathbb{N}_0$ について成立する．

これらの評価は，$\operatorname{supp}\psi \subset \{2^{-1} \le |\xi| \le 2\}$ を満たす $\psi \in C_0^\infty(\mathbb{R}^n)$ に対して，

$$\big(e^{i|\xi|^s}\psi(2^{-j}\xi)\big)^\vee(x)$$

に対する挙動を調べることにより導かれる．詳細については [5, Proposition 3.1] を参照されたい．

Lemma 2.1 を用いることにより，S_j に対する以下の評価が得られる．

Lemma 2.2 ([5, Lemma 4.1]). $0 < s < 1$ または $s > 1$ とし，$1 \le p \le \infty$ とする．このとき，$c > 0$ が存在して，

$$\|S_j f\|_{L^p(\mathbb{R}^n)} \le c\,(2^j)^{sn|\frac{1}{p}-\frac{1}{2}|}\|f\|_{L^p(\mathbb{R}^n)}$$

がすべての $j \in \mathbb{N}_0$ について成り立つ．

Lemma 2.3 ([5, Lemma 4.2 (2)]). $0<s<1$ または $1<s<\infty$ とし，f は原点中心，半径 r の球に台をもつ h^1-アトムであると仮定する．このとき，$A \geq 2r$ であり，N は

$$\begin{cases} 0 \leq N < \frac{n}{2(1-s)}, & \textit{if } 0<s<1, \\ 0 \leq N < \infty, & \textit{if } 1<s<\infty, \end{cases}$$

を満たすならば,

$$\left\| S_j f(x) \right\|_{L^2(A \leq |x| \leq 2A)} \leq c\,(2^j)^{\frac{n}{2}} \left(2^{j(1-s)} A\right)^{-N}$$

がすべての $j \in \mathbb{N}_0$ に対して成立する．ここで，定数 $c>0$ は $n,\ s,\ N,\ \theta$ にのみ依存する．

次の補題は $s<1$ の場合にのみ成立するものである．

Lemma 2.4 ([5, Lemma 4.4]). $0<s<1$ とする．このとき，$c=c(n,s,\theta)>0$ が存在して，以下が成立する．

(1) f が原点中心，半径 $r \leq 1$ の球に台をもつ h^1-アトムであるならば,

$$\left\| S_j f(x) \right\|_{L^1(|x| \geq 2)} \leq c, \quad j \in \mathbb{N}_0,$$

が成り立つ．

(2) $0<A \leq 10$ に対して,

$$\left\| S_j f(x) \right\|_{L^2(|x| \leq A)} \leq c A^{\frac{n(1-s)}{2}} \|f\|_{L^\infty(\mathbb{R}^n)}, \quad j \in \mathbb{N}_0,$$

が成り立つ．

最後の補題は $s>1$ の場合に成立するものである．

Lemma 2.5 ([5, Lemma 4.5]). $s>1$ とする．このとき，$j \in \mathbb{N}_0,\ A \geq 2^{j(s-1)}$ ならば

$$\left\| S_j f(x) \right\|_{L^2(|x| \leq A)} \leq c A^{\frac{n}{2}} \|f\|_{L^\infty(\mathbb{R}^n)},$$

が成り立つ．ここで，$c>0$ は n,s,θ にのみ依存する定数である．

3 証明の概略

本節では Theorem 1.3 の証明の概略を述べる．証明のアイデアは，$H^1 \times L^\infty \to L^1$ 有界性を改良することである．具体的には，以下を証明した．

Proposition 3.1 ([5, Theorem 5.1]).

$$m = \begin{cases} -\frac{sn}{2} - \frac{s(1-s)n}{2}, & \textit{if } 0<s<1, \\ -\frac{sn}{2}, & \textit{if } 1<s<\infty. \end{cases}$$

とする．このとき，$\sigma \in S^m_{1,0}(\mathbb{R}^{2n})$ ならば，双線形フーリエ乗法作用素 T^s_σ は $h^1 \times L^\infty \to L^1$ 有界である．

実際に，Proposition 3.1 が証明されれば，Theorem B と補間することにより，Theorem 1.3 が得られる．

本稿では，簡単のために，$0 < s < 1$,

$$m < -\frac{ns}{2} - \frac{ns(1-s)}{2} \tag{3.1}$$

の場合についての証明を与える．$s > 1$ の場合や $m = -\frac{ns}{2} - \frac{ns(1-s)}{2}$ の場合については [5] を参照してほしい．

それでは，実際に (3.1) の場合に対する Proposition3.1 の証明について述べる．

まず，Littlewood–Paley の 2 進分解および Fourier 級数展開を用いることで，以下の形をしているマルチプライヤーに対して，$h^1 \times L^\infty \to L^1$ 有界性を示せばよいことがわかる：

$$\begin{aligned}
\widetilde{\sigma}_0(\xi,\eta) &= c_0\theta_1(\xi)\,\theta_2(\eta),\\
\widetilde{\sigma}(\xi,\eta) &= \sum_{j\in\mathbb{N}} c_j\,\theta_1(2^{-j}\xi)\,\theta_2(2^{-j}\eta).
\end{aligned}$$

ただし，$\{c_j\}_{j\in\mathbb{N}_0}$ は複素数の列で $|c_j| \lesssim 2^{jm}$ を満たすものであり，$\theta_1, \theta_2 \in C_0^\infty(\mathbb{R}^n)$ は $\operatorname{supp}\theta_1, \operatorname{supp}\theta_2 \subset \{|\xi| \le 2\}$ を満たすものである．

以下では，マルチプライヤー $\widetilde{\sigma}$ についてのみ考える．具体的に $T^s_{\widetilde{\sigma}}$ を書き下すと

$$T^s_{\widetilde{\sigma}}(f,g)(x) = \sum_{j\in\mathbb{N}} c_j \left(e^{i|D|^s}\theta_1(2^{-j}D)f(x)\right)\left(e^{i|D|^s}\theta_2(2^{-j}D)g(x)\right)$$

と表わせる．さらに，関数 φ および ζ を用いて，$T^s_{\widetilde{\sigma}}$ を以下のように分割する．

$$\begin{aligned}
T^s_{\widetilde{\sigma}}(f,g)(x) = \sum_{j\in\mathbb{N}} c_j \Big\{ & T^1_j f(x) T^2_j g(x) + S^1_j f(x) T^2_j g(x)\\
&+ T^1_j f(x) S^2_j g(x) + S^1_j f(x) S^2_j g(x) \Big\}.
\end{aligned}$$

ただし，

$$T^\ell_j f(x) = \left(e^{i|\xi|^s}\varphi(\xi)\theta_\ell(2^{-j}\xi)\widehat{f}(\xi)\right)^\vee(x), \quad S^\ell_j f(x) = \left(e^{i|\xi|^s}\zeta(\xi)\theta_\ell(2^{-j}\xi)\widehat{f}(\xi)\right)^\vee, \quad \ell = 1,2,$$

とおいた．そして，$|c_j| \lesssim 2^{jm}$ であるから，$h^1 \times L^\infty \to L^1$ 有界性を得るには，

$$\sum_{j\in\mathbb{N}} 2^{jm}\big\|U^1_j f\, V^2_j g\big\|_{L^1} \lesssim \|f\|_{h^1}\|g\|_{L^\infty}, \quad U, V \in \{S, T\}$$

を示せば十分である．さらに，h^1 のアトム分解から，

$$\sum_{j\in\mathbb{N}} 2^{jm}\big\|U^1_j f\, V^2_j g\big\|_{L^1} \lesssim \|g\|_{L^\infty}, \quad U, V \in \{S, T\} \tag{3.2}$$

が全ての h^1-アトム f について一様に成立することを示せば十分である．平行移動不変性により，h^1-アトム f は原点中心，半径 r の球に台をもつ場合を考えれば十分である．

$U = T$ または $V = T$ の場合の証明は本稿では省略する．これらの場合の評価については，[5] を参照してほしい．

以下，$(U,V) = (S,S)$ の場合のみを考える．

まず，(3.2) の左辺の L^1 ノルムを以下の 3 つに分ける．

$$\big\|\cdots\big\|_{L^1(\mathbb{R}^n)} = \big\|\cdots\big\|_{L^1(|x|\le 2r)} + \big\|\cdots\big\|_{L^1(2r\le|x|\le 4)} + \big\|\cdots\big\|_{L^1(|x|\ge 4)}$$

3.1 $L^1(|x| \le 2r)$ の評価

コーシー・シュワルツの不等式と，Lemma 2.2 より，

$$\begin{aligned}\left\|S_j^1 f\, S_j^2 g\right\|_{L^1(|x|\le 2r)} &\le r^{\frac{n}{2}} \left\|S_j^1 f\right\|_{L^2(\mathbb{R}^n)} \left\|S_j^2 g\right\|_{L^\infty(\mathbb{R}^n)} \\ &\lesssim r^{\frac{n}{2}} \|f\|_{L^2(\mathbb{R}^n)} 2^{\frac{ns}{2}} \|g\|_{L^\infty(\mathbb{R}^n)} \lesssim 2^{\frac{ns}{2}} \|g\|_{L^\infty(\mathbb{R}^n)}.\end{aligned}$$

ここで，最後の不等式において f が h^1-アトムであることを用いた．ゆえに，$m = -ns/2 - ns(1-s)/2 < -ns/2$ より，

$$\sum_{j\in\mathbb{N}} 2^{jm} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(|x|\le 2r)} \lesssim \|g\|_{L^\infty}$$

を得る．

3.2 $L^1(|x| \ge 4)$ の評価

ヘルダーの不等式と Lemma 2.4 (1), Lemma 2.2 より，

$$\left\|S_j^1 f\, S_j^2 g\right\|_{L^1(|x|\ge 4)} \le \left\|S_j^1 f\right\|_{L^1(|x|\ge 4)} \left\|S_j^2 g\right\|_{L^\infty(\mathbb{R}^n)} \lesssim 2^{\frac{ns}{2}} \|g\|_{L^\infty(\mathbb{R}^n)}.$$

ゆえに，前節と同様にして，

$$\sum_{j\in\mathbb{N}} 2^{jm} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(|x|\ge 4)} \lesssim \|g\|_{L^\infty}$$

を得る．

3.3 $L^1(2r \le |x| \le 4)$ の評価

以下では，2 つ目の項に対する評価

$$\sum_{j\in\mathbb{N}} 2^{jm} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2r\le|x|\le 4)} \lesssim \|g\|_{L^\infty}$$

を考える．

さて，以下のようにして左辺の $L^1(2r \le |x| \le 4)$ ノルムを更に細かく分割する：

$$\sum_{j\in\mathbb{N}} 2^{jm} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2r\le|x|\le 4)} = \sum_{j\in\mathbb{N}} 2^{jm} \sum_{k\in\mathbb{N}, 2^k r\le 4} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2^k r\le|x|\le 2^{k+1} r)}$$

右辺の L^1 ノルムについて，以下の評価が示される：$0 \le N < \frac{n}{2(1-s)}$ とする．このとき，すべての $k \in \mathbb{N}$, $2^k r \le 4$，に対して，

$$\begin{aligned}\left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2^k r\le|x|\le 2^{k+1} r)} &\lesssim 2^{j\left(\frac{n}{2} - \frac{(1-s)^2 n}{2}\right)} \left(2^{j(1-s)} 2^k r\right)^{-N + \frac{(1-s)n}{2}} \\ &= \left(2^j\right)^{\frac{ns}{2} - \frac{ns(1-s)}{2}} \left(2^{j(1-s)} 2^k r\right)^{-N + \frac{(1-s)n}{2}}\end{aligned}$$

が成り立つ．これは，コーシー・シュワルツの不等式，Lemma 2.3 と Lemma 2.4 (2) から従う．よって，特に，$N=0$ として，この不等式を用いると

$$\begin{aligned}\sum_{\substack{k\in\mathbb{N},2^k r\le 4\\ 2^{j(1-s)}2^k r\le 1}} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2^k r\le|x|\le 2^{k+1}r)} &\lesssim \left(2^j\right)^{\frac{ns}{2}-\frac{ns(1-s)}{2}} \sum_{\substack{k\in\mathbb{N},2^k r\le 4\\ 2^{j(1-s)}2^k r\le 1}} \left(2^{j(1-s)}2^k r\right)^{\frac{(1-s)n}{2}}\\ &\lesssim \left(2^j\right)^{\frac{ns}{2}+\frac{ns(1-s)}{2}}\end{aligned}$$

を得る．ここで，最後の不等式では $1-s>0$ であることを用いた．

一方で，N を $\frac{(1-s)n}{2}<N<\frac{n}{2(1-s)}$ を満たすように選べば（$0<s<1$ の場合は，常にこのような選び方ができる），

$$\begin{aligned}\sum_{\substack{k\in\mathbb{N},2^k r\le 4\\ 2^{j(1-s)}2^k r> 1}} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2^k r\le|x|\le 2^{k+1}r)} &\lesssim \left(2^j\right)^{\frac{ns}{2}-\frac{ns(1-s)}{2}} \sum_{\substack{k\in\mathbb{N},2^k r\le 4\\ 2^{j(1-s)}2^k r> 1}} \left(2^{j(1-s)}2^k r\right)^{-N+\frac{(1-s)n}{2}}\\ &\lesssim \left(2^j\right)^{\frac{ns}{2}+\frac{ns(1-s)}{2}}\end{aligned}$$

を得る．これらの評価をまとめて，

$$\begin{aligned}&\sum_{j\in\mathbb{N}} 2^{jm} \sum_{k\in\mathbb{N},2^k r\le 4} \left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2^k r\le|x|\le 2^{k+1}r)}\\ &\le \sum_{j\in\mathbb{N}} 2^{jm}\Bigg(\sum_{\substack{k\in\mathbb{N},2^k r\le 4\\ 2^{j(1-s)}2^k r\le 1}} + \sum_{\substack{k\in\mathbb{N},2^k r\le 4\\ 2^{j(1-s)}2^k r> 1}}\Bigg)\left\|S_j^1 f\, S_j^2 g\right\|_{L^1(2^k r\le|x|\le 2^{k+1}r)}\\ &\lesssim \sum_{j\in\mathbb{N}} \left(2^j\right)^{m+\frac{ns}{2}+\frac{ns(1-s)}{2}}\\ &\lesssim 1\end{aligned}$$

を得る．最後の不等式で $m<-\frac{ns}{2}-\frac{ns(1-s)}{2}$ であることを用いた．

Remark 3.2. ここまでの証明の中ではアトム f のモーメント条件

$$\int_{\mathbb{R}^n} f(x)\,dx = 0$$

を用いていない．この条件は $m=-\frac{ns}{2}-\frac{ns(1-s)}{2}$ のときの証明の中で用いる．詳しくは [5] を参照してほしい．

Remark 3.3. 実際には，不等式 $\lesssim$ において，S_j^1 および S_j^2 の定義にあらわれる関数 θ_1, θ_2 の依存性について注意して評価を考えなければならない．しかし，簡単のために，このことについては省略して記述した．

参考文献

[1] A. Bergfeldt, S. Rodríguez-López, D. Rule, and W. Staubach, Multilinear oscillatory integrals and estimates for coupled systems of dispersive PDEs, Trans. Amer. Math. Soc. **376** (2023), 7555–7601.

[2] L. Grafakos and M. M. Peloso, Bilinear Fourier integral operators, J. Pseudo-Differ. Oper. Appl. **1** (2010), 161–182.

[3] D. Goldberg, A local version of real Hardy spaces, Duke Math. J. **46** (1979), 27–42.

[4] T. Kato, A. Miyachi, and N. Tomita, Estimates for some bilinear wave operators, Rev. Mat. Iberoam. **40** (2024), no. 4, 1571–1608.

[5] T. Kato, A. Miyachi, N. Shida, and N. Tomita, Bilinear oscillatory Fourier multipliers, available at arXiv:2404.10488.

[6] A. Miyachi, On some estimates for the wave equation in L^p and H^p, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **27** (1980), no. 2, 331–354.

[7] A. Miyachi, On some singular Fourier multipliers, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), 267–315.

[8] A. Miyachi and N. Tomita, Calderón-Vaillancourt–type theorem for bilinear operators, Indiana Univ. Math. J. **62** (2013), 1165–1201.

[9] S. Rodríguez-López and W. Staubach, Estimates for rough Fourier integral and pseudodifferential operators and applications to the boundedness of multilinear operators, J. Funct. Anal. **10** (2013), 2356–2385.

[10] S. Rodríguez-López, D. Rule and W. Staubach, A Seeger-Sogge-Stein theorem for bilinear Fourier integral operators, Adv. Math. **264** (2014), 1–54.

[11] S. Rodríguez-López, D. Rule, and W. Staubach, On the boundedness of certain bilinear oscillatory integral operators, Trans. Amer. Math. Soc. **367** (2015), 6971–6995.

[12] P. Sjölin, An H^p inequality for strongly singular integrals, Math. Z. **165** (1979), 231–238.

[13] E.M. Stein, *Harmonic Analysis, Real-variable Methods, Orthogonality, and Oscillatory Integrals*, Princeton University Press, Princeton, New Jersey, 1993.

[14] A. Seeger, C. D. Sogge, and E. M. Stein, Regularity properties of Fourier integral operators, Ann. of Math. (2) **134** (1991), no. 2, 231–251.

The distance from a projection to nilpotents[*] [†]

森 迪也[‡] (東大数理/理研 iTHEMS)

概 要

階数 $m \in \{1, 2, \ldots, n\}$ の $n \times n$ 直交射影行列と $n \times n$ ベキ零行列全体の距離は $(2\cos\frac{\pi}{\frac{n}{m}+2})^{-1}$ である．

1 はじめに

この講演は泉正己氏（京都大）との共同研究 [8] に基づく[1]．本稿全体を通じ，n を（固定された）正の整数とする．ベクトル $h = \begin{pmatrix} h_1 \\ h_2 \\ \vdots \\ h_n \end{pmatrix} \in \mathbb{C}^n$ に対し，$\|h\| = \sqrt{|h_1|^2 + |h_2|^2 + \cdots + |h_n|^2}$ と定める．複素 $n \times n$ 行列全体を $\mathcal{M}_n$ と表す．$A \in \mathcal{M}_n$ に対し，$\|A\| \coloneqq \sup_{h \in \mathbb{C}^n,\, \|h\| \leq 1} \|Ah\|$ と定める．$a_1, a_2, \ldots, a_n \in \mathbb{C}$ に対し，第 (i, i) 成分が a_i $(1 \leq i \leq n)$ である $n \times n$ 対角行列を $\mathrm{Diag}\,(a_1, a_2, \ldots, a_n)$ と表す．$n \times n$ ベキ零行列全体を $\mathcal{N}_n$ と表す．

次が本講演における主定理である．

定理 1 ([8])．$1 \leq m \leq n$ とする．$P_m \coloneqq \mathrm{Diag}\,(\underbrace{1, 1, \ldots, 1}_{m \text{ 個}}, \underbrace{0, 0, \ldots, 0}_{n-m \text{ 個}})$ に対し

$$\inf_{N \in \mathcal{N}_n} \|P_m - N\| = \left(2\cos\frac{\pi}{\frac{n}{m}+2}\right)^{-1}$$

が成り立つ．

3 節・4 節において,（定理 7 を例外として）ほぼ自己完結な形でこの証明を与えたい．論文 [8] にはより一般的な結果が書かれているが，それについては 5 節で説明する．

2 背景

定理 1 への動機を説明しよう[2].（可分）複素 Hilbert 空間 H, K に対し，H から K への有界線形作用素全体を $\mathcal{B}(H, K)$ と表す．$A \in \mathcal{B}(H, K)$ に対し，

$$\|A\|\,(= \|A\|_{\mathcal{B}(H,K)}) \coloneqq \sup_{h \in H,\, \|h\| \leq 1} \|Ah\|$$

[*]2024 年度 実函数論・函数解析学合同シンポジウム 講演集原稿

[†]講演者は科研費（課題番号 22K13934）による助成を受けている．

[‡]mmori@ms.u-tokyo.ac.jp

[1]が，行列の場合を主として扱うため，[8] より議論を簡略化した箇所や，逆に議論を丁寧に書いた箇所が多々ある．

[2]本節の内容の一部は [11] と重複している．説明がやや粗い部分があるがご容赦いただきたい．続く 3 節・4 節では行列の場合しか考えない．

と定めると，$\mathcal{B}(H,K)$ はノルム $\|\cdot\|$ について Banach 空間をなす．このノルムは距離 $d(A,B) := \|A-B\|$ $(A,B \in \mathcal{B}(H,K))$ を定め，この距離から $\mathcal{B}(H,K)$ の位相（ノルム位相）が定まる．$A \in \mathcal{B}(H,K)$ に対し，$\langle A^*k, h\rangle = \langle k, Ah\rangle$ $(h \in H,\, k \in K)$ なる $A^* \in \mathcal{B}(K,H)$ が唯一つ存在し，$\|A^*\|_{\mathcal{B}(K,H)} = \|A\|_{\mathcal{B}(H,K)}$, $\|A^*A\|_{\mathcal{B}(H,H)} = \|A\|^2_{\mathcal{B}(H,K)}$ が成り立つ．

以下，主として $H = K$ の場合を考える．$\mathcal{B}(H,H)$ を $\mathcal{B}(H)$ と表す．$\mathcal{B}(H)$ は合成を積として Banach 環をなす（$\|AB\| \le \|A\|\|B\|$ が成り立つ）．$\mathcal{B}(H)$ の単位元は H 上の恒等作用素である．これを $I_{\mathcal{B}(H)}$ あるいは I と表すことにする．$n = \dim H < \infty$ のとき，H から $\mathbb{C}^n$ への（線形等距離）同型写像をひとつとれば，通常の方法により，$\mathcal{B}(H)$ は $n \times n$ 複素行列全体のなす空間 $\mathcal{M}_n$ と同一視される．このような同一視について，前節で定めた行列のノルムは本節で定めた作用素のノルムと一致する．

作用素 $N \in \mathcal{B}(H)$ に対し，ある正の整数 k が存在して $N^k = 0$ が成り立つとき，N は**ベキ零**（nilpotent）であるという．$\mathcal{B}(H)$ のベキ零な元全体の集合を $\mathcal{N}(H)$ と表す．$A \in \mathcal{B}(H)$ に対し，A と $\mathcal{N}(H)$ の距離 $\inf\limits_{N \in \mathcal{N}(H)} \|A - N\|$ を $\nu(A)$ と表すことにする．線形代数で学ぶように，$N \in \mathcal{M}_n$ がベキ零であることは $N^n = 0$ であることと同値である．したがって，$n \times n$ ベキ零行列の全体 $\mathcal{N}_n$ は $\mathcal{M}_n$ の閉集合である．これよりとくに，$A \in \mathcal{M}_n$ に対し，$\nu(A) = 0$ であることは $A \in \mathcal{N}_n$ であることと同値である．

いっぽう，$\dim H = \infty$ の場合は，ベキ零作用素全体の集合は閉集合ではない．作用素 $A \in \mathcal{B}(H)$ に対し，スペクトル $\{\lambda \in \mathbb{C} \mid \lambda I - A$ は可逆でない $\}$ を $\sigma(A)$ で表す．$A \in \mathcal{B}(H)$ のスペクトル $\sigma(A)$ が一点集合 $\{0\}$ であるとき，A は**準ベキ零**（quasinilpotent）であるという．Gelfand のスペクトル半径公式[3]から，A が準ベキ零であることは $\|A^k\|^{1/k} \to 0$ $(k \to \infty)$ となることと同値である．とくに，ベキ零作用素は準ベキ零である．

作用素論に関する Paul Halmos の有名な 10 の問題 [5] の第 7 問は，任意の準ベキ零作用素は $\mathcal{N}(H)$ の閉包に属すか，という問題である．この問題は肯定的に解かれており，より強い以下の定理が知られている．

定理 2 (Apostol, Foiaș, Voiculescu [1])**.** $A \in \mathcal{B}(H)$ が $\mathcal{N}(H)$ の閉包に属する（すなわち $\nu(A) = 0$ となる）ためには次の 3 条件が成り立つことが必要十分である．

1. A のスペクトルは 0 を含み，連結である．
2. A の本質的スペクトル[4]は 0 を含み，連結である．
3. $\lambda \in \mathbb{C}$ に対し，$\lambda I - A$ が semi-Fredholm ならば $\lambda I - A$ の Fredholm index は 0 である[5]．

ベキ零作用素への理解を（「外側」から）もっと深めるために，ν の具体的な値をさらに調べよう，と考えることは自然な発想であろう．ところが，それはどうやら易しくないらしく，ν の具体的な値が知られている作用素は，ν がゼロの場合（上記）を除き，H が有限次元でも無限次元でもかなり限定的である．ν の値に関し知られているいくつかの事実を以下に述べる．

- 任意の $A, B \in \mathcal{B}(H)$ と $\lambda \in \mathbb{C}$ に対し，$\nu(\lambda A) = |\lambda|\nu(A)$，$\nu(A) = \nu(A^*)$, $|\nu(A) - \nu(B)| \le \|A - B\|$ である（定義より明らか）．

---

[3] $A \in \mathcal{B}(H)$ ならば，$\sup\{|\lambda| \mid \lambda \in \sigma(A)\} = \lim\limits_{k\to\infty} \|A^k\|^{1/k}$ である．この値を**スペクトル半径**という．

[4] $A \in \mathcal{B}(H)$ が Fredholm であるとは，A の像が閉で，$\dim\ker A < \infty$ かつ $\dim\ker A^* < \infty$ であることを意味する．A の**本質的スペクトル**とは，$\lambda I - A$ が Fredholm でない $\lambda \in \mathbb{C}$ の全体を表す．

[5] これはつまり次を意味する．$\lambda \in \mathbb{C}$ に対し，$\lambda I - A$ の像が閉で，$\dim\ker(\lambda I - A) < \infty$ あるいは $\dim\ker(\lambda I - A)^* < \infty$ であるならば，$\dim\ker(\lambda I - A) = \dim\ker(\lambda I - A)^*$ である．

- $U \in \mathcal{B}(H)$ が等距離作用素（$U^*U = I$）ならば，$\nu(U) = 1$ である．（$\nu(U) \le 1$ は明らか．$N \in \mathcal{N}(H)$ ならば，$h \in \ker N (\neq \{0\})$ に対し $\|(U-N)h\| = \|Uh\| = \|h\|$ となるため，$\nu(U) \ge 1$ である．）

- （Apostol–Salinas [2, Theorem 3.5]）任意の $A \in \mathcal{B}(H)$ に対し，$\nu(A)$ は A のスペクトル半径以下である．

$P \in \mathcal{B}(H)$ が**射影**（projection）であるとは，$P = P^2 = P^*$ であることを指す．$\mathcal{B}(H)$ の射影全体の集合を $\mathcal{P}(H)$ と表す．また，$\mathcal{M}_n$ の射影全体の集合を $\mathcal{P}_n$ と表し，$\mathcal{P}_n$ の元で階数が m であるもの全体を $\mathcal{P}_{n,m}$ と表す．$P_m = \mathrm{Diag}\,(\underbrace{1,1,\ldots,1}_{m\text{ 個}},\underbrace{0,0,\ldots,0}_{n-m\text{ 個}}) \in \mathcal{P}_{n,m}$ である．また，$P \in \mathcal{P}_{n,m}$ ならば，あるユニタリ行列 $U \in \mathcal{M}_n$ が存在して $UPU^* = P_m$ となることにも注意．よって，任意の $P \in \mathcal{P}_{n,m}$ に対し $\nu(P) = \nu(P_m)$ である．射影は基本的な作用素であるが，射影の場合に限っても ν の完全な理解は以前まで得られていなかった．先行研究をまとめてみよう．

- 射影に対する ν の値の評価を与えた最も古い研究はおそらく [6] である．この論文で著者の Hedlund は，零でない射影全体の集合と $\mathcal{N}(H)$ の距離について "the determination of the precise value (中略) seems difficult, even if H is finite-dimensional" と述べている．

- （Herrero [7, Corollary 9]）$\dim H = \infty$ のとき，$P \in \mathcal{P}(H) \setminus \{0\}$ の核が無限次元なら $\nu(P) = 1/2$, 有限次元なら $\nu(P) = 1$ である．

- （MacDonald [9, Theorem 1]）$P \in \mathcal{P}_{n,1}$ ならば，$\nu(P) = (2\cos\frac{\pi}{n+2})^{-1}$ である．

- （Cramer [4, Theorem 3.6]）$n \ge 2$, $P \in \mathcal{P}_{n,n-1}$ ならば，$\nu(P) = (2\cos\frac{\pi}{\frac{n}{n-1}+2})^{-1}$ である．

MacDonald [9] は，任意の $P \in \mathcal{P}_n \setminus \{0\}$ に対し $\nu(P) \ge (2\cos\frac{\pi}{n+2})^{-1}$ が成り立つと予想した．講演者は MacDonald の予想に証明を与えた [10, 11]．Cramer [4, Conjecture 5.1] は $m \in \{1,2,\ldots,n\}$, $P \in \mathcal{P}_{n,m}$ ならば $\nu(P) = (2\cos\frac{\pi}{\frac{n}{m}+2})^{-1}$ であると予想した．定理 1 はこの予想を証明した結果に他ならない．

3 準備

主定理について考えるための準備として，行列に関するいくつかの事実を述べよう．読者の面倒を避けるため，証明もかんたんにつけることにしたい．

行列 $A \in \mathcal{M}_n$ に対し，そのトレースを $\mathrm{tr}\,A$，行列式を $\det A$，階数を $\mathrm{rank}\,A$ と表す．A のスペクトル $\sigma(A)$ は A の固有値全体，すなわち固有多項式の根全体の集合に他ならない．また，$A = (a_{ij})_{1\le i,j\le n}$ に対し $A^* = (\overline{a_{ji}})_{1\le i,j\le n}$ である．A がエルミート行列（$A = A^*$）のとき，$\sigma(A) \subset \mathbb{R}$ が成り立つ．エルミート行列 A の固有値がすべて 0 以上であるとき，A は**正**であるという．エルミート行列 A, B に対し，$B - A$ が正であるとき，$A \le B$ と書く．この条件は，任意の $h \in \mathbb{C}^n$ に対し $\langle Ah, h\rangle \le \langle Bh, h\rangle$ となることと同値である．したがって，$\le$ は半順序関係となる．また，可逆行列 $X \in \mathcal{M}_n$ に対し

$$A \le B \iff X^*AX \le X^*BX \tag{1}$$

であることもわかる．エルミート行列 A, B に対し，$B - A$ が正かつ可逆であるとき，$A < B$ と書くことにする．

一般に，行列 X に対し，X^*X, XX^* は正である．また，正行列のノルムは最大固有値に等しい．ゆえに

$$\begin{aligned} &\|X\| \le 1 \iff \|X^*X\| \le 1 \iff X^*X \le I \\ \iff &\|X^*\| \le 1 \iff \|XX^*\| \le 1 \iff XX^* \le I \end{aligned} \tag{2}$$

が成り立つ．

エルミート行列 $A \in \mathcal{M}_n$ の固有値が（重複度を込めて）$\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$ であるとき，あるユニタリ行列 $U \in \mathcal{M}_n$ が存在して，$A = U\mathrm{Diag}\,(\lambda_1, \lambda_2, \ldots, \lambda_n)U^*$ が成り立つ．関数 $f\colon \sigma(A) \to \mathbb{C}$ に対し，$f(A) = U\mathrm{Diag}\,(f(\lambda_1), f(\lambda_2), \cdots f(\lambda_n))U^*$ と定める[6]（**functional calculus**）．f の像が $\mathbb{R}$, $[0,\infty)$, $\{z \in \mathbb{C} \mid |z| = 1\}$ に含まれるとき，$f(A)$ はそれぞれエルミート，正，ユニタリとなることに注意しておく．$0 \le A$，$f(t) = t^{1/2}$ のとき，$f(A) = A^{1/2}$ を A の（正の）**平方根**という．

次の 2 つの定理はどちらも有名である．

定理 3. $A, B \in \mathcal{M}_n$ とする．このとき，AB の固有多項式は BA の固有多項式と一致する．

証明．A が可逆のときは $BA = A^{-1}(AB)A$ より明らか．一般の場合，十分小さい任意の実数 $\varepsilon > 0$ に対し，$A + \varepsilon I$ は可逆なので $\det(xI - (A + \varepsilon I)B) = \det(xI - B(A + \varepsilon I))$ が成り立つ．$\varepsilon \to 0$ という極限[7]を考えれば $\det(xI - AB) = \det(xI - BA)$ であることがわかる． □

定理 4. エルミート行列 $A, B \in \mathcal{M}_n$ が正・可逆であるとする．このとき，$A \le B$ と $B^{-1} \le A^{-1}$ は同値である．

証明．$A \le B \overset{(1)}{\iff} B^{-1/2}AB^{-1/2} \le I \overset{(2)}{\iff} A^{1/2}B^{-1}A^{1/2} \le I \overset{(1)}{\iff} B^{-1} \le A^{-1}.$ □

行列解析の理論において基本的な **min-max 定理**を思い出そう．

定理 5 (min-max 定理)**.** $A \in \mathcal{M}_n$ をエルミート行列，$1 \le k \le n$ とする．このとき，A の（重複度を込め）k 番目に大きい固有値 λ_k について次が成り立つ．

$$\begin{aligned} \lambda_k &= \max\{\min\{\langle Ah, h\rangle \mid h \in V, \|h\| = 1\} \mid V \text{ は } \mathbb{C}^n \text{ の } k \text{ 次元部分空間}\} \\ &= \min\{\max\{\langle Ah, h\rangle \mid h \in V, \|h\| = 1\} \mid V \text{ は } \mathbb{C}^n \text{ の } n-k+1 \text{ 次元部分空間}\}. \end{aligned}$$

証明．ひとつめの等号を示す．ふたつめの等号の証明も同様である．A をユニタリ行列により対角化することで，$A = \mathrm{Diag}\,(\lambda_1, \lambda_2, \ldots, \lambda_n)$ の場合に帰着できる．

（$\ge$ の証明）k 番目より前の成分がすべてゼロであるベクトル全体 $W \subset \mathbb{C}^n$ の次元は $n-k+1$ である．よって，$V \subset \mathbb{C}^n$ を k 次元部分空間とすると，$V \cap W \ne \{0\}$ である．ノルム 1 のベクトル $h \in V \cap W$ をとれば，$h \in W$ より $\langle Ah, h\rangle \le \lambda_k$ が従う．

（$\le$ の証明）k 番目より後の成分がすべてゼロであるベクトルの全体を $V \subset \mathbb{C}^n$ とおけば，$\min\{\langle Ah, h\rangle \mid h \in V, \|h\| = 1\} = \lambda_k$ が成り立つ． □

補題 1. エルミート行列 $X, Y \in \mathcal{M}_n$ が $X \le Y$ を満たすと仮定する．関数 $f\colon \sigma(X) \cup \sigma(Y) \to \mathbb{R}$ が単調減少なら，$\mathrm{tr}\,(f(X)) \ge \mathrm{tr}\,(f(Y))$ である．もしさらに f が単射で $X \ne Y$ なら $\mathrm{tr}\,(f(X)) > \mathrm{tr}\,(f(Y))$ である．

[6] これはこのような条件を満たすユニタリ U の取り方によらずに定まる．
[7] 多項式を $x \in \mathbb{C}$ の関数とみなし，各 $x \in \mathbb{C}$ に対する極限を考える．

証明. $X \leq Y$ と min-max 定理より，X の（重複度を込めた）k 番目に大きい固有値は Y の k 番目に大きい固有値以下である．よって，$f(X)$ の k 番目に小さい固有値は $f(Y)$ の k 番目に小さい固有値以上である．トレースは固有値の総和であるから，$\mathrm{tr}\,(f(X)) \geq \mathrm{tr}\,(f(Y))$ が成り立つ．
$X \leq Y$ かつ $X \neq Y$ なら，$\mathrm{tr}\,(Y-X) > 0$ であるため，ある $k \in \{1, 2, \ldots, n\}$ について X の k 番目に大きい固有値は Y の k 番目に大きい固有値より真に小さい．これより後半も示せる．　□

次の **interlacing inequality** とよばれる不等式 (3) は，min-max 定理の系として得られる．

定理 6. $A, B \in \mathcal{M}_n$ をエルミート行列，$A \leq B$, $\mathrm{rank}\,(B-A) \leq 1$ とする．A の固有値を（重複度を込めて）$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$，$B$ の固有値を $\beta_1 \geq \beta_2 \geq \cdots \geq \beta_n$ とおく．このとき，不等式

$$\beta_1 \geq \alpha_1 \geq \beta_2 \geq \alpha_2 \geq \cdots \geq \beta_n \geq \alpha_n \tag{3}$$

が成り立つ．

次の事実もよく知られている．これは interlacing inequality と関係が深い．

補題 2. k を正の整数とする．

$$\alpha'_1 \geq \alpha_1 \geq \alpha'_2 \geq \alpha_2 \geq \cdots \geq \alpha_{k-1} \geq \alpha'_k$$

を実数とする．エルミート行列 $A \in \mathcal{M}_{k-1}$ の固有値が $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_{k-1}$ のとき，固有値が $\alpha'_1 \geq \alpha'_2 \geq \cdots \geq \alpha'_k$ であるエルミート行列 $A' \in \mathcal{M}_k$ であって，A' の左上の $(k-1) \times (k-1)$ 成分が A と一致するものが存在する．

証明. $UAU^* = \mathrm{Diag}\,(\alpha_1, \alpha_2, \ldots, \alpha_{k-1}) =: D$ となるユニタリ行列 $U \in \mathcal{M}_{k-1}$ をとる．$h_1, h_2, \ldots, h_k \in \mathbb{R}$ に対し，$h = (h_1, h_2, \ldots, h_{k-1})$ とおき，行列 $\begin{pmatrix} D & h^* \\ h & h_k \end{pmatrix}$ について考える．この固有値は

$$\begin{pmatrix} U^* & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} UAU^* & h^* \\ h & h_k \end{pmatrix} \begin{pmatrix} U & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} A & (hU)^* \\ hU & h_k \end{pmatrix}$$

の固有値に一致する．したがって，条件を満たす A' の存在をいうためには，$\begin{pmatrix} D & h^* \\ h & h_k \end{pmatrix}$ の固有値が $\alpha'_1 \geq \alpha'_2 \geq \cdots \geq \alpha'_k$ となるような $h_1, h_2, \ldots, h_k \in \mathbb{R}$ を見つければよい．$\alpha_1 > \alpha_2 > \cdots > \alpha_{k-1}$ である場合に示せれば，他の場合も容易に示せる．したがって，$\alpha_1 > \alpha_2 > \cdots > \alpha_{k-1}$ の場合を考えよう．$p \in \{1, 2, \ldots, k-1\}$ に対し

$$h_p = \sqrt{\frac{-\displaystyle\prod_{q=1}^{k}(\alpha_p - \alpha'_q)}{\displaystyle\prod_{q \in \{1,2,\ldots,k-1\} \setminus \{p\}} (\alpha_p - \alpha_q)}}$$

と定める（根号の中身は 0 以上の実数となることに注意）．そして，

$$h_k = (\alpha'_1 + \alpha'_2 + \cdots + \alpha'_k) - (\alpha_1 + \alpha_2 + \cdots + \alpha_{k-1})$$

と定める．ふたつの k 次多項式

$$\det\left(xI - \begin{pmatrix} D & h^* \\ h & h_k \end{pmatrix}\right), \quad \prod_{l=1}^{k}(x - \alpha'_l)$$

の差を $f(x)$ とおく．すると，f は高々 $k-2$ 次の多項式であり，また $f(\alpha_1)=f(\alpha_2)=\cdots=f(\alpha_{k-1})=0$ となることが確かめられるため，$f=0$ である．ゆえに

$$\det\left(xI-\begin{pmatrix} D & h^* \\ h & h_k \end{pmatrix}\right)=\prod_{l=1}^{k}(x-\alpha'_l)$$

であり，望み通り $\begin{pmatrix} D & h^* \\ h & h_k \end{pmatrix}$ の固有値が $\alpha'_1 \geq \alpha'_2 \geq \cdots \geq \alpha'_k$ となる． □

さいごにもうひとつ簡単な補題を用意しておく．

補題 3. エルミート行列 $X, Y \in \mathcal{M}_n$ が $X < Y$ を満たすと仮定する．$E \in \mathcal{M}_n$ を階数 1 の射影とする．このとき，$\max\{t \in \mathbb{R} \mid X \leq Y - tE\}$ が存在し，それを t_0 とおくと $\operatorname{rank}(Y - t_0E - X) = n-1$ が成り立つ．また，$t < t_0$ に対し $X < Y - tE$ である．

証明. $X=0$ と仮定しても一般性を失わない．このとき $0 < Y$ となる．$Y - tE = Y^{1/2}(I - tY^{-1/2}EY^{-1/2})Y^{1/2}$ だから，$I - tY^{-1/2}EY^{-1/2}$ について考えればよい．$Y^{-1/2}EY^{-1/2}$ は正・階数 1 の行列である．$tY^{-1/2}EY^{-1/2}$ が射影となる t を t_0 とおけば（つまり $t_0 = \|Y^{-1/2}EY^{-1/2}\|^{-1}$ とおけば），それは $I - tY^{-1/2}EY^{-1/2}$ が正となる最大の t に一致する．$I - t_0Y^{-1/2}EY^{-1/2}$ は階数 $n-1$ の射影であり，したがって $\operatorname{rank}(Y - t_0E) = \operatorname{rank}(Y^{1/2}(I - t_0Y^{-1/2}EY^{-1/2})Y^{1/2}) = n-1$ となる．$t < t_0$ に対し $0 < Y - tE$ であることも容易に確かめられる． □

4 Cramer の予想の証明

狭義上三角，つまり $\begin{pmatrix} 0 & * & \cdots & * \\ 0 & 0 & \ddots & \vdots \\ \vdots & \vdots & \ddots & * \\ 0 & 0 & \cdots & 0 \end{pmatrix}$ という形である $n \times n$ 行列の全体を $\mathcal{T}_n$ と表す．前節までに引き続き，$0 \leq m \leq n$ に対し，P_m で対角行列 $\operatorname{Diag}(\underbrace{1,1,\ldots,1}_{m\text{ 個}},\underbrace{0,0,\ldots,0}_{n-m\text{ 個}})$ を表す．射影 $P \in \mathcal{M}_n$ に対し，$P^\perp \coloneqq I - P$ と定めると，$P^\perp$ も射影となる．ν の値を調べるにあたり，Arveson の距離公式 [3] の一種として知られる次の定理が重要である．証明を知りたい方は [11] を参照されたい．

定理 7 ([13, Lemma], [12, Theorem 1])**.** $A = (a_{ij})_{1\leq i,j\leq n} \in \mathcal{M}_n$ とする．このとき，最小値 $\min\limits_{T\in\mathcal{T}_n}\|A - T\|$ が存在し，それは $\max\limits_{1\leq k\leq n}\|P_{k-1}^\perp AP_k\|$ に等しい．

$N \in \mathcal{M}_n$ がベキ零であるためには，あるユニタリ行列 U について $UNU^* \in \mathcal{T}_n$ となることが必要十分である[8]．したがって，$n\times n$ ユニタリ行列全体を $\mathcal{U}_n$ と表せば，$\mathcal{N}_n = \{U^*TU \mid U \in \mathcal{U}_n, T \in \mathcal{T}_n\}$ が成り立つ．ゆえに，任意の $A \in \mathcal{M}_n$ に対し

$$\nu(A) = \inf_{T\in\mathcal{T}_n, U\in\mathcal{U}_n}\|A - U^*TU\| = \inf_{T\in\mathcal{T}_n, U\in\mathcal{U}_n}\|UAU^* - T\| \overset{\text{定理 7}}{=} \inf_{U\in\mathcal{U}_n}\max_{1\leq k\leq n}\|P_{k-1}^\perp UAU^*P_k\|$$

となる．ここで，$A = P_m$, $1 \leq m \leq n$ の場合を考える．$\{UP_mU^* \mid U \in \mathcal{U}_n\} = \mathcal{P}_{n,m}$ であるから，

$$\nu(P_m) = \inf_{P\in\mathcal{P}_{n,m}}\max_{1\leq k\leq n}\|P_{k-1}^\perp PP_k\|$$

[8] ユニタリ行列による上三角化（Schur triangulation）を考えよ．

が成り立つ．ゆえに，$P \in \mathcal{P}_{n,m}$ に対し $\displaystyle\max_{1\le k\le n} \|P_{k-1}^{\perp} P P_k\|$ を考えることが重要となる．

以下，$P \in \mathcal{P}_{n,m}$ を固定して考える．一般に，行列 X, Y に対し

$$\|XY\|^2 = \|(XY)^*(XY)\| = \|Y^*X^*XY\| = \|((X^*X)^{1/2}Y)^*((X^*X)^{1/2}Y)\| = \|(X^*X)^{1/2}Y\|^2$$

だから $\|XY\| = \|(X^*X)^{1/2}Y\|$ が成り立つ．同様に $\|XY\| = \|X(YY^*)^{1/2}\|$ である．これより，

$$\|P_{k-1}^{\perp}PP_k\| = \|(P_{k-1}^{\perp}P)\cdot(PP_k)\| = \|(PP_{k-1}^{\perp}P)^{1/2}\cdot(PP_k)\| = \|(PP_{k-1}^{\perp}P)^{1/2}\cdot(PP_kP)^{1/2}\|$$

である．よって，$A_k = PP_kP$ $(k \in \{0,1,\ldots,n\})$ と定めると，$\|P_{k-1}^{\perp}PP_k\| = \|(P-A_{k-1})^{1/2}A_k^{1/2}\|$ となる．$A_k - A_{k-1} = P(P_k - P_{k-1})P$ であるから，$0 = A_0 \le A_1 \le \cdots \le A_n = P$, $\mathrm{rank}\,(A_k - A_{k-1}) \le 1$ である．

注意 1. $I - A_{k-1} = P^{\perp} + (P - A_{k-1})$ より，$(I - A_{k-1})^{1/2} = P^{\perp} + (P - A_{k-1})^{1/2}$ である．また，$A_k = PP_kP$ より $P^{\perp}A_k^{1/2} = 0$ である．以上より，$(P - A_{k-1})^{1/2}A_k^{1/2} = (I - A_{k-1})^{1/2}A_k^{1/2}$ であることがわかる．したがって，$\|P_{k-1}^{\perp}PP_k\| = \|(I - A_{k-1})^{1/2}A_k^{1/2}\|$ である．

$\theta \coloneqq \pi(\frac{n}{m}+2)^{-1}$ とおく．各 $1 \le k \le n$ に対し $(2\cos\theta)^{-1}$ と $\|P_{k-1}^{\perp}PP_k\| = \|(I-A_{k-1})^{1/2}A_k^{1/2}\|$ とを比較したい．ここで唐突だが，$[0, \pi - 2\theta]$ から $[0,1]$ への単調増大な全単射

$$t \mapsto \frac{1}{2\cos\theta}\cdot\frac{\sin t}{\sin(t+\theta)}$$

を考える．この逆関数を用いた functional calculus により，$0 \le B_k \le (\pi - 2\theta)P$ および

$$A_k = \frac{1}{2\cos\theta}\cdot\frac{\sin B_k}{\sin(B_k + \theta I)} \tag{4}$$

を満たす $B_k \in \mathcal{M}_n$ が唯一つとれる[9][10]．このとき，$B_0 = 0$, $B_n = (\pi - 2\theta)P$ である．また，$A_0 \le A_1 \le \cdots \le A_n$ より

$$\frac{\sin B_0}{\sin(B_0+\theta I)} \le \frac{\sin B_1}{\sin(B_1+\theta I)} \le \cdots \le \frac{\sin B_n}{\sin(B_n+\theta I)}$$

である．次の命題が重要である．

命題 1. 各 $k \in \{1,2,\ldots,n\}$ に対し，

$$\|(I - A_{k-1})^{1/2}A_k^{1/2}\| \le (2\cos\theta)^{-1} \iff \mathrm{tr}\,(B_k - B_{k-1}) \le \theta,$$

$$\|(I - A_{k-1})^{1/2}A_k^{1/2}\| < (2\cos\theta)^{-1} \iff \mathrm{tr}\,(B_k - B_{k-1}) < \theta$$

が成り立つ．

まずこれを用いて $\nu(P_m) = (2\cos\theta)^{-1}$ を導こう．

$\nu(P_m) \ge (2\cos\theta)^{-1}$ の証明．

$$(\max_{1\le k\le n}\|P_{k-1}^{\perp}PP_k\| =)\ \max_{1\le k\le n}\|(I - A_{k-1})^{1/2}A_k^{1/2}\| < (2\cos\theta)^{-1}$$

を仮定する．命題 1 より，各 k に対し $\mathrm{tr}\,(B_k - B_{k-1}) < \theta$ となる．したがって，$\mathrm{tr}\,(B_n - B_0) < n\theta$ である．$B_0 = 0$, $B_n = (\pi - 2\theta)P$ より，$(\pi - 2\theta)m < n\theta$，つまり $\theta > \pi(\frac{n}{m}+2)^{-1}$ となり，矛盾が得られた． □

[9]右辺の分母の $\sin(B_k + \theta I)$ は可逆で，$\sin B_k$ と $\sin(B_k + \theta I)$ は交換可能なので，分数のように表しても問題は起きない．見やすさのため，このような表記を今後多用する．

[10]この式のような変形が証明のポイントとなる．このようにするとうまくいく理由はいまひとつわかっていない．

$\nu(P_m) \leq (2\cos\theta)^{-1}$ の証明. 次の条件を満たす実数 $\beta_{kl} \in [0, \pi - 2\theta]$ ($1 \leq k \leq n$, $1 \leq l \leq k$) を（なんでもよいので）固定しておく.

(a) 任意の $k \in \{1, 2, \ldots, n\}$ に対し $\displaystyle\sum_{l=1}^{k} \beta_{kl} = k\theta$ である.

(b) 任意の $k \in \{1, 2, \ldots, n\}$ に対し

$$\beta_{k,1} \geq \beta_{k-1,1} \geq \beta_{k,2} \geq \beta_{k-1,2} \geq \cdots \geq \beta_{k-1,k-1} \geq \beta_{k,k}$$

である.

(c) $l \leq m$ ならば $\beta_{nl} = \pi - 2\theta$, $l > m$ ならば $\beta_{nl} = 0$ である.

たとえば,

$$\beta_{kl} = \max\{\min\{\pi - 2\theta, k\theta - (l-1)(\pi - 2\theta)\}, 0\}$$

とすれば条件を満たすことがかんたんに確かめられる.

$$\alpha_{kl} = \frac{1}{2\cos\theta} \cdot \frac{\sin\beta_{kl}}{\sin(\beta_{kl} + \theta)} \in [0, 1]$$

とおく. 関数 $t \mapsto \sin t / \sin(t + \theta)$ は $[0, \pi - 2\theta]$ で単調なので, (b) より各 $k \in \{1, 2, \ldots, n\}$ に対し

$$\alpha_{k,1} \geq \alpha_{k-1,1} \geq \alpha_{k,2} \geq \alpha_{k-1,2} \geq \cdots \geq \alpha_{k-1,k-1} \geq \alpha_{k,k}$$

となる. ゆえに, 補題 2 を繰り返し用いることで, エルミート行列 $Q \in \mathcal{M}_n$ であって, 各 k に対し Q の左上 $k \times k$ 成分のなす小行列の固有値が $\alpha_{k1} \geq \alpha_{k2} \geq \cdots \geq \alpha_{kk}$ となるようなものがとれる. (c) より, $Q \in \mathcal{P}_{n,m}$ である. $A_k = QP_kQ$ とおく. 定理 3 より, $A_k = (P_kQ)^*(P_kQ)$ と $(P_kQ)(P_kQ)^* = P_kQP_k$ の固有値は（重複度を込めて）一致する. よって, A_k の固有値は $\alpha_{k1}, \alpha_{k2}, \ldots, \alpha_{kk}, \underbrace{0, 0, \ldots, 0}_{n-k\text{ 個}}$ である. $0 \leq B_k \leq (\pi - 2\theta)Q$ および (4) を満たす $B_k \in \mathcal{M}_n$ をとると, その固有値は $\beta_{k1}, \beta_{k2}, \ldots, \beta_{kk}, \underbrace{0, 0, \ldots, 0}_{n-k\text{ 個}}$ である. したがって, (a) より $\mathrm{tr}\,(B_k - B_{k-1}) = \theta$ が $k \in \{1, 2, \ldots, n\}$ に対し成り立つ. ゆえに, 命題 1 を $P = Q$ に適用すれば, 各 $k \in \{1, 2, \ldots, n\}$ に対し $\|P_{k-1}^{\perp} QP_k\| = (2\cos\theta)^{-1}$ であることがわかる. $\square$

以下, 命題 1 の証明を行う. まず補題を 3 つ準備する. $\varphi \coloneqq \theta/2$ とおく.

補題 4. エルミート行列 $B, B' \in \mathcal{M}_n$ が $0 \leq B \leq (\pi - 2\theta)I$, $0 \leq B' \leq (\pi - 2\theta)I$ を満たすとする. このとき,

$$\frac{\sin B}{\sin(B + \theta I)} \leq \frac{\sin B'}{\sin(B' + \theta I)} \iff \cot(B + \varphi I) \geq \cot(B' + \varphi I)$$

である[11]. また,

$$\mathrm{rank}\left(\frac{\sin B}{\sin(B + \theta I)} - \frac{\sin B'}{\sin(B' + \theta I)}\right) = \mathrm{rank}\,(\cot(B + \varphi I) - \cot(B' + \varphi I))$$

が成り立つ.

[11] $\cot t = \cos t / \sin t = 1/\tan t$ は cotangent を表す.

証明．公式 $\sin(\alpha\pm\beta)=\sin\alpha\cos\beta\pm\cos\alpha\sin\beta$ を交換可能なエルミート行列に適用して，

$$\begin{aligned}\sin(B+\varphi I\pm\varphi I)&=\sin(B+\varphi I)\cos(\varphi I)\pm\cos(B+\varphi I)\sin(\varphi I)\\&=\cos\varphi\sin(B+\varphi I)\pm\sin\varphi\cos(B+\varphi I)\end{aligned}$$

を得る[12]．ゆえに，

$$\frac{\sin B}{\sin(B+\theta I)}=\frac{\cos\varphi\sin(B+\varphi I)-\sin\varphi\cos(B+\varphi I)}{\cos\varphi\sin(B+\varphi I)+\sin\varphi\cos(B+\varphi I)}=\frac{2I}{I+\tan\varphi\cot(B+\varphi I)}-I$$

が成り立つ．同様に，

$$\frac{\sin B'}{\sin(B'+\theta I)}=\frac{2I}{I+\tan\varphi\cot(B'+\varphi I)}-I$$

となる．ゆえに，

$$\frac{\sin B}{\sin(B+\theta I)}\leq\frac{\sin B'}{\sin(B'+\theta I)}$$

は

$$\frac{2I}{I+\tan\varphi\cot(B+\varphi I)}\leq\frac{2I}{I+\tan\varphi\cot(B'+\varphi I)}$$

と同値である．定理 4 より，これはさらに $\cot(B+\varphi I)\geq\cot(B'+\varphi I)$ と同値である．

可逆行列に対する等式 $X^{-1}-Y^{-1}=X^{-1}(Y-X)Y^{-1}$ より，階数に関する等式も得られる． □

補題 5. エルミート行列 $B,B'\in\mathcal{M}_n$ が $0\leq B\leq(\pi-2\theta)I$, $0\leq B'\leq(\pi-2\theta)I$ を満たすとする．

$$A=\frac{1}{2\cos\theta}\cdot\frac{\sin B}{\sin(B+\theta I)},\quad A'=\frac{1}{2\cos\theta}\cdot\frac{\sin B'}{\sin(B'+\theta I)}$$

とおく．このとき，

$$\|(I-A)^{1/2}(A')^{1/2}\|\leq(2\cos\theta)^{-1}\iff\cot(B'+\varphi I)\geq\cot(B+3\varphi I),\tag{5}$$

$$\|(I-A)^{1/2}(A')^{1/2}\|<(2\cos\theta)^{-1}\iff\cot(B'+\varphi I)>\cot(B+3\varphi I)\tag{6}$$

が成り立つ．

証明．$\sin B+\sin(B+2\theta I)=2\sin(B+\theta I)\cos(\theta I)=2\cos\theta\sin(B+\theta I)$ より，

$$I-\frac{1}{2\cos\theta}\cdot\frac{\sin B}{\sin(B+\theta I)}=\frac{1}{2\cos\theta}\cdot\frac{\sin(B+2\theta I)}{\sin(B+\theta I)}$$

となる．ゆえに，

$$\|(I-A)^{1/2}(A')^{1/2}\|\leq(2\cos\theta)^{-1}\iff\left\|\left(\frac{\sin(B+2\theta I)}{\sin(B+\theta I)}\right)^{1/2}\left(\frac{\sin B'}{\sin(B'+\theta I)}\right)^{1/2}\right\|\leq1$$

が成り立つ．また，補題 4 の証明と同様の計算から，$S=\tan\varphi\cot(B+3\varphi I)$, $T=\tan\varphi\cot(B'+\varphi I)$ に対し

$$\frac{\sin(B+2\theta I)}{\sin(B+\theta I)}=\frac{I+\tan\varphi\cot(B+3\varphi I)}{I-\tan\varphi\cot(B+3\varphi I)}=\frac{I+S}{I-S}$$

および

$$\frac{\sin B'}{\sin(B'+\theta I)}=\frac{I-\tan\varphi\cot(B'+\varphi I)}{I+\tan\varphi\cot(B'+\varphi I)}=\frac{I-T}{I+T}$$

[12]交換可能なエルミート行列の組は，あるユニタリ行列により同時に対角化できるため，このような式が成立する．

が成り立つ[13].

$$
\begin{aligned}
\left\|\left(\frac{I+S}{I-S}\right)^{1/2}\left(\frac{I-T}{I+T}\right)^{1/2}\right\| \le 1 &\overset{(2)}{\iff} \left(\frac{I-T}{I+T}\right)^{1/2}\left(\frac{I+S}{I-S}\right)\left(\frac{I-T}{I+T}\right)^{1/2} \le I \\
&\overset{(1)}{\iff} (I-T)^{1/2}\left(\frac{2I}{I-S}-I\right)(I-T)^{1/2} \le I+T \\
&\iff 2(I-T)^{1/2}(I-S)^{-1}(I-T)^{1/2} \le 2I \\
&\iff (I-T)^{1/2}(I-S)^{-1}(I-T)^{1/2} \le I \\
&\overset{(2)}{\iff} (I-S)^{-1/2}(I-T)(I-S)^{-1/2} \le I \\
&\overset{(1)}{\iff} I-T \le I-S \\
&\iff \cot(B'+\varphi I) \ge \cot(B+3\varphi I)
\end{aligned}
$$

であるから，(5) が示された．同様の同値変形より (6) も得られる． □

補題 6. エルミート行列 $B \in \mathcal{M}_n$ が $0 \le B \le (\pi - 2\theta)I$ を満たすとする．$E \in \mathcal{M}_n$ を階数 1 の射影とする．$\max\{t \in \mathbb{R} \mid \cot(B+\varphi I) - tE \ge \cot(B+3\varphi I)\}$ を t_0 とおくとき，

$$\mathrm{tr}\left(\mathrm{arccot}(\cot(B+\varphi I) - t_0 E) - (B+\varphi I)\right) = \theta$$

が成り立つ[14]．また，実数 t に対し

$$\cot(B+\varphi I) - tE > \cot(B+3\varphi I) \iff \mathrm{tr}\left(\mathrm{arccot}(\cot(B+\varphi I) - tE) - (B+\varphi I)\right) < \theta$$

である．

証明．$C = \cot(B+\varphi I) - t_0 E$, $D = \mathrm{arccot}\, C$ とおく．補題 3 より，$\mathrm{rank}\,(C - \cot(B+3\varphi I)) = n-1$ が成り立つ．$\cot(B+\varphi I)$ の固有値を $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$，$C = \cot(B+\varphi I) - t_0 E$ の固有値を $\lambda'_1 \ge \lambda'_2 \ge \cdots \ge \lambda'_n$ とおくとき，interlacing inequality より，

$$\lambda_1 \ge \lambda'_1 \ge \lambda_2 \ge \lambda'_2 \ge \cdots \ge \lambda_n \ge \lambda'_n$$

が成り立つ．したがって，

$$0 < \mathrm{arccot}\,\lambda_1 \le \mathrm{arccot}\,\lambda'_1 \le \mathrm{arccot}\,\lambda_2 \le \mathrm{arccot}\,\lambda'_2 \le \cdots \le \mathrm{arccot}\,\lambda_n \le \mathrm{arccot}\,\lambda'_n < \pi$$

を得る．

$$\mathrm{tr}\,(B+\varphi I) = \sum_{k=1}^{n} \mathrm{arccot}\,\lambda_k, \quad \mathrm{tr}\,D = \sum_{k=1}^{n} \mathrm{arccot}\,\lambda'_k$$

であるから，

$$\mathrm{tr}\,(B+\varphi I) \le \mathrm{tr}\,D < \mathrm{tr}\,(B+\varphi I) + \pi \tag{7}$$

が従う．

$$\cot t = i\left(\frac{2}{e^{2it}-1} + 1\right)$$

[13] $-I \le S \le I$, $-I \le T \le I$ である．$I-S$, $I+T$ は可逆だが，$I+S$, $I-T$ は可逆と限らないことに注意．

[14] arccot は $\cot\colon (0,\pi) \to \mathbb{R}$ の逆関数（arccotangent）を表す．

より

$$
\begin{aligned}
t_0E &= \cot(B+\varphi I) - \cot D \\
&= i\left(\frac{2I}{e^{2i(B+\varphi I)}-I}+I\right) - i\left(\frac{2I}{e^{2iD}-I}+I\right) \\
&= 2i((e^{2i(B+\varphi I)}-I)^{-1} - (e^{2iD}-I)^{-1}) \\
&= 2i(e^{2i(B+\varphi I)}-I)^{-1}(e^{2iD}-e^{2i(B+\varphi I)})(e^{2iD}-I)^{-1},
\end{aligned}
$$

ゆえに

$$
1 = \operatorname{rank}(t_0E) = \operatorname{rank}(e^{2iD}-e^{2i(B+\varphi I)}) = \operatorname{rank}(e^{2iD}e^{-2i(B+\varphi I)}-I) \tag{8}
$$

である．同様に，

$$
n-1 = \operatorname{rank}(C-\cot(B+3\varphi I)) = \operatorname{rank}(e^{2iD}-e^{2i(B+3\varphi I)}) = \operatorname{rank}(e^{2iD}e^{-2i(B+\varphi I)}-e^{4i\varphi}I) \tag{9}
$$

である．(8), (9) より，ユニタリ $e^{2iD}e^{-2i(B+\varphi I)}$ の固有値はひとつを除き 1 で，残りのひとつは $e^{4i\varphi}=e^{2i\theta}$ である．$e^{2iD}e^{-2i(B+\varphi I)}$ の行列式を考える[15]ことで，$e^{2i\operatorname{tr}D}e^{-2i\operatorname{tr}(B+\varphi I)}=e^{2i\theta}$ を得る．よって，$2i\operatorname{tr}D-2i\operatorname{tr}(B+\varphi I)=2i\theta+2i\pi l$, つまり $\operatorname{tr}D-\operatorname{tr}(B+\varphi I)=\theta+\pi l$ なる整数 l が存在する．(7) より，$l=0$ である．ゆえに，$\operatorname{tr}D-\operatorname{tr}(B+\varphi I)=\theta$ が従う．これが目標としていた等式に他ならない．

後半は，$\cot\colon(0,\pi)\to\mathbb{R}$ が狭義単調減少な全単射であることと，補題 1，補題 3，および前半より従う． □

命題 1 は補題 4, 5, 6 より直ちに従う（$B=B_{k-1}$, $B'=B_k=\operatorname{arccot}(\cot(B+\varphi I)-tE)-\varphi I$ の場合を考えよ）．

5 von Neumann 環への一般化

$\mathcal{B}(H)$ の $*$ 部分代数（部分ベクトル空間で，$*$ および合成演算について閉じているもの）であって，I を含み，かつ強作用素位相（各点収束位相）で閉であるものを **von Neumann 環**という．von Neumann 環であって，その中心が $\mathbb{C}I$ であるものを**因子環**とよぶ．von Neumann 環におけるほとんどの話題は因子環の場合に帰着される．以下でも因子環の場合に限って考えることにする．

因子環は 5 つのタイプ（型）に分類される．前節で扱った行列環 $\mathcal{M}_n$ は $\mathbf{I}_n$ **型**とよばれる因子環であり，これはもっとも簡単な von Neumann 環であると考えられる．そのほかに次の 4 つのタイプがある．

- $\mathbf{I}_\infty$ **型**環 $\cdots$ 無限次元 Hilbert 空間 H に対する $\mathcal{B}(H)$ がこれにあたる．
- $\mathbf{II}_1$ **型**環 $\cdots$ 無限離散群の左正則表現から構成されるたくさんの例などがある．
- $\mathbf{II}_\infty$ **型**環 $\cdots$ II_1 型環と I_∞ 型環のテンソル積で表される．
- **III 型**環 $\cdots$ ほかと比べかなり扱いが難しい．冨田竹崎理論を用いて調べられる．

[15] 一般に，エルミート行列 X に対し $\det e^{2iX}=e^{2i\operatorname{tr}X}$ であることに注意．

因子環 $\mathcal{A}$ とその元 A に対し，$\mathcal{A}$ に属するベキ零作用素全体と A との距離を $\nu_{\mathcal{A}}(A)$ と表すことにする．射影 $P \in \mathcal{A}$ に対する $\nu_{\mathcal{A}}(P)$ について，先に述べた Herrero の結果および von Neumann 環の一般論から，次がわかる[16]．

定理 8 ([7, Corollary 9], [14, Section 8])**.** $\mathcal{A}$ を I_∞, II_∞, III のいずれかのタイプの因子環とする．$P \in \mathcal{A} \setminus \{0\}$ を射影とする．

- $V^*V = I - P$ かつ $I - P \neq VV^* \leq I - P$ なる $V \in \mathcal{A}$ が存在するならば，$\nu_{\mathcal{A}}(P) = 1/2$ である．
- そうでないならば，$\nu_{\mathcal{A}}(P) = 1$ である．

残されていたのが I_n 型と II_1 型の場合である．これらの環は**有限型**の環とよばれ，特別な性質をもつ．von Neumann 環 $\mathcal{A}$ 上の線形汎関数 $\tau \colon \mathcal{A} \to \mathbb{C}$ が条件

- 任意の $A \in \mathcal{A}$ に対し $\tau(A^*A) \geq 0$,
- 任意の $A, B \in \mathcal{A}$ に対し $\tau(AB) = \tau(BA)$,
- $\tau(I) = 1$

を満たすとき，τ を**トレース状態**という．実は，有限型因子環はトレース状態を唯一つ持ち，またトレース状態を持つ因子環は有限型である．論文 [8] では，有限型因子環について，射影 $P \in \mathcal{A}$ に対する $\nu_{\mathcal{A}}(P)$ を完全に決定した．

定理 9 ([8])**.** $\mathcal{A}$ を因子環，τ を $\mathcal{A}$ 上のトレース状態，$P \in \mathcal{A} \setminus \{0\}$ を射影とする．このとき，

$$\nu_{\mathcal{A}}(P) = \left(2\cos\frac{\tau(P)\pi}{1 + 2\tau(P)}\right)^{-1}$$

が成り立つ．

$\mathcal{A} = \mathcal{M}_n$ のときは $\tau(A) = \mathrm{tr}\, A/n$ であるため，定理 9 は前節の結果の拡張となる．定理 9 を II_1 型環に対し証明するにあたり，$\nu_{\mathcal{A}}(P)$ の上からの評価については前節の結果を応用できる（II_1 型環の中に $\mathcal{M}_n$ のコピーが作れる，という事実を用いる）．下からの評価を得るためには前節と少し違う議論が必要となる．これは，$\mathcal{M}_n$ を考える際に有効な「階数の差が 1 以下である行列の組」を用いる方法などが II_1 型環では使えず，命題 1 にあたる部分がそのままの形では成り立たないためである．そのかわりに,「連続値の階数」の役割を果たす量などをうまく考えることで証明ができる．詳しくは論文 [8] を参照されたい．

参考文献

[1] C. Apostol, C. Foiaș, and D. Voiculescu, On the norm-closure of nilpotents. II. *Rev. Roumaine Math. Pures Appl.* **19** (1974), 549–577.

[2] C. Apostol and N. Salinas, Nilpotent approximations and quasinilpotent operators. *Pacific J. Math.* **61**(1975), no. 2, 327–337.

[3] W. Arveson, Interpolation problems in nest algebras. *J. Funct. Anal.* **20** (1975), no. 3, 208–233.

[16] この話題については，von Neumann 環論において最も難しいとされる III 型環の場合が比較的簡単に調べられる．von Neumann 環における作用素論的な研究では，I_n 型や II_1 型の場合が III 型の場合より難しいということがときどき起こる．

[4] Z. Cramer, The Distance from a Rank $n-1$ Projection to the Nilpotent Operators on $\mathbb{C}^n$. *Canad. Math. Bull.* **64** (2021), no. 1, 54–74.

[5] P.R. Halmos, Ten problems in Hilbert space. *Bull. Amer. Math. Soc.* **76** (1970), no. 5, 887–933.

[6] J.H. Hedlund, Limits of nilpotent and quasinilpotent operators. *Michigan Math. J.* **19** (1972), 249–255.

[7] D.A. Herrero, Normal limits of nilpotent operators. *Indiana Univ. Math. J.* **23** (1973/74/1974), 1097–1108.

[8] M. Izumi and M. Mori, Determination of the distance from a projection to nilpotents. Preprint, arXiv:2406.09234.

[9] G.W. MacDonald, Distance from projections to nilpotents. *Canad. J. Math.* **47** (1995), no. 4, 841–851.

[10] M. Mori, On the distance from a matrix to nilpotents. *Linear Algebra Appl.* **679** (2023), 99–103.

[11] 森 迪也，On the distance from a matrix to nilpotents. 令和 5 年度作用素論・作用素環論研究集会 講演集原稿. $\cdots$ 講演者のウェブサイト（論文一覧のページ下部）から入手可能.

[12] S. Parrott, On a quotient norm and the Sz.-Nagy–Foiaș lifting theorem. *J. Funct. Anal.* **30** (1978), no. 3, 311–328.

[13] S.C. Power, The distance to upper triangular operators. *Math. Proc. Cambridge Philos. Soc.* **88** (1980), no. 2, 327–329.

[14] P. Skoufranis, Normal limits of nilpotent operators in von Neumann algebras. *Integral Equations Operator Theory* **77** (2013), no. 3, 407–439.

冪零リー群の表現と擬対称領域上の核関数

嵐晃一[*]

1　はじめに

リー群のユニタリ表現をその既約分解から理解することは, しばしば有意義な視点をもたらす. 例えばヴェルニュ・ロッシ [VR] によるスカラー型最高ウェイトユニタリ表現の分類における, ワラック集合 [Wa] の導出について, 表現の既約分解の観点から次のように考えてみたい. ヴェルニュ・ロッシは, 有界対称領域を, 上半平面の一般化と考えられる, ジーゲル領域に実現し, 扱っている問題を凸錐上のフーリエ変換を用いて, 凸錐上の関数空間の問題に置き換えた. ジーゲル領域上の, あるアフィン変換の群に関する不変な核関数の中で端点であるもの全体を考えるとき, このフーリエ変換は, これら端点から定義される積分変換の形をしている.

ここで, 考えている核関数が定数倍の関係にないとき, 対応する既約ユニタリ表現が異なるという意味での無重複性が成立していることに着目したい. この事実から, スカラー型最高ウェイトユニタリ表現が何であるかに依らず, 考えているアフィン変換の群への制限による既約分解が常に無重複になる. 本稿では, この例を念頭に置き, このアフィン変換の群 (冪零リー群である) をその部分群に置き換えた場合に, 表現の無重複性が成立するかを問題として扱う. ただし, 対称領域だけでなく, 対称性が僅かに失われた「擬対称領域」と呼ばれるジーゲル領域に一般化して問題を扱う. さらに, 擬対称領域上に実現可能な表現について, その核関数の積分表示により提示する. これにより, 既知のジーゲル領域のベルグマン核の積分表示を, これまでに考えられてきた冪零リー群だけではなく, その部分群の表現とも関係づけるという意味で, より一般的な状況から理解することができる.

また, 表現の無重複性が, 群軌道の幾何学的性質と密接に関連していることが知られている. 本稿では, リー群の可視的作用と余等方的作用に焦点を当て, これらとの関係についても述べる.

*Department of Mathematics, Tokyo Gakugei University, Nukuikita 4-1-1, Koganei,Tokyo 184-8501, Japan

2　不変ヒルベルト部分空間と核関数

複素領域 $\mathcal{D}$ に対して, その上の正則関数全体の成す空間を $\mathcal{O}(\mathcal{D})$ で表し, コンパクト開位相を考えることにより, 線型位相空間とみなす. リー群 G の正則自己同型による滑らかな作用 $G \times \mathcal{D} \ni (g, z) \mapsto g \cdot z \in \mathcal{D}$ が与えられたとき, 連続表現 $(\pi_0, \mathcal{O}(\mathcal{D}))$ が次で定まる:

$$\pi_0(g)f(z) := f(g^{-1} \cdot z) \quad (g \in G, f \in \mathcal{O}(\mathcal{D}), z \in \mathcal{D}).$$

可分なヒルベルト空間 $\mathcal{H}$ 上のリー群 G のユニタリ表現 π を考える.

定義 2.1 ([Sch, §1], [Kob3, Definition 2.1])**.** 表現 π と π_0 の間に単射かつ連続な G-準同型 Φ が存在するとき, ユニタリ表現 π は $\mathcal{O}(\mathcal{D})$ **に実現される**という. このとき, 像 $\Phi(\mathcal{H})$ (または単に $\mathcal{H}$) を $\mathcal{O}(\mathcal{D})$ の G-**不変ヒルベルト部分空間**と呼ぶ. さらに π が既約であるとき, 既約 G-不変ヒルベルト部分空間という.

リースの表現定理に注意して, 線型位相空間 $\mathcal{O}(\mathcal{D})$ の G-不変ヒルベルト部分空間 $\mathcal{H}$ に対し, 関数 $K_z^{\mathcal{H}} \in \mathcal{O}(\mathcal{D})$ を次で定義する:

$$(f, K_z^{\mathcal{H}})_{\mathcal{H}} = f(z) \quad (f \in \mathcal{O}(\mathcal{D}), z \in \mathcal{D}).$$

$\mathcal{D} \times \mathcal{D}$ 上の関数 $K(z, z')$ で第一成分について正則, 第二成分について反正則, エルミートかつ正定値なものを**核関数**と呼び, それら全体の成す集合を $\Gamma(\mathcal{D})$ で表す. このとき, 核関数 $K^{\mathcal{H}} \in \Gamma(D)$ が $K_z^{\mathcal{H}} = K^{\mathcal{H}}(\cdot, z)$ によって定まる. さらに $\Gamma_G(\mathcal{D}) \subset \Gamma(\mathcal{D})$ を G-不変な核関数全体の成す凸錐とし, 部分集合 $\mathrm{ext}(\Gamma_G(\mathcal{D})) \subset \Gamma_G(\mathcal{D})$ を端点全体の成す集合とする. ここで, 一般に凸錐 Γ が与えられたとき, その元 K が**端点**であるとは, もし $K = K_1 + K_2\,(K_1, K_2 \in \Gamma)$ と表されているならば,

$$K = \lambda_1 K_1 = \lambda_2 K_2 \quad (\lambda_1, \lambda_2 \geq 0)$$

が成り立つことをいう. 次の定理は基本的である.

定理 2.2 ([FT, Proposition 1],[Sch, §8])**.** 凸錐 $\Gamma_G(\mathcal{D})$ (または $\mathrm{ext}(\Gamma_G(\mathcal{D}))$) の要素は $\mathcal{O}(\mathcal{D})$ の G-不変 (または既約 G-不変) ヒルベルト部分空間と一対一に対応する.

次に, 端点とは限らない不変核関数を, 端点の積分で書くことができることについて説明する. ハウスドルフ空間 Λ からの単射な連続写像

$$\Lambda \ni \lambda \mapsto K^{\lambda} \in \mathrm{ext}(\Gamma_G(\mathcal{D}))$$

が $\mathrm{ext}(\Gamma_G(\mathcal{D}))$ の**認容パラメトリゼーション**であるとは,

$$\mathrm{ext}(\Gamma_G(\mathcal{D})) = \{0\} \coprod \coprod_{\lambda \in \Lambda} \mathbb{R}_{>0} K^{\lambda}$$

が成り立ち, 像からの逆写像が普遍的可測であるこという. なお, 後者の条件について, ハウスドルフ空間 Λ が局所コンパクトかつ第二可算であれば十分である. このようなパラメトリゼーションを一つ固定するとき, 次の定理が知られている.

定理 2.3. [FT, Theorem 1] 任意の $K \in \Gamma_G(\mathcal{D})$ に対して, ハウスドルフ空間 Λ 上のラドン測度 m が存在し, 次の式が成り立つ:

$$K(z, z') = \int_\Lambda K^\lambda(z, z')\, dm(\lambda) \quad (z, z' \in \mathcal{D}). \tag{2.1}$$

なお上記の積分の収束について, コンパクト集合上での一様収束を表す.

3 無重複性

群 G のユニタリ表現の無重複性は通常次のように定義される.

定義 3.1. π が**無重複**であるとは, 環

$$\mathrm{End}_G(\mathcal{H}) = \{A \in B(\mathcal{H}) \mid A\pi(g) = \pi(g)A \text{ for all } g \in G\}$$

が可換であることをいう.

定理 3.2 ([FT, Theorem 2])**.** 次の条件は同値である:

(i) $\mathcal{O}(\mathcal{D})$ の任意の 2 つの既約 G-不変ヒルベルト部分空間が G の同値な表現から定義されているとき, それらの像が線型空間として一致し, 誘導された内積が互いに定数倍の関係となる;

(ii) 任意の $K \in \Gamma_G(\mathcal{D})$ に対して, 積分表示 (2.1) を与えるラドン測度 m が一意的に定まる;

(iii) $\mathcal{O}(\mathcal{D})$ に実現される G の任意のユニタリ表現は無重複である.

本稿では, 定理 3.2 の同値条件のうちどれか一つが成り立つとき π_0 は**無重複**であるという. 我々の設定において, 表現の無重複性と群軌道の幾何学的性質との間に強い結びつきがある. ここで $\mathcal{D}$ は複素有界領域に正則同値であると仮定する (以下で解説する内容は, 関係する理論のほんの一部分に過ぎないことに注意されたい). まず $\mathcal{D}$ のベルグマン計量は正則同相群 (リー群の構造を持つ) の作用に関して不変である. このことから, L^2 正則関数全体が成す空間 $H^2(\mathcal{D})$ 上のユニタリ表現が得られる. また, シンプレクティック作用が自然に定義される.

定義 3.3 ([HW])**.** $\mathcal{D}$ の正則同相群の閉部分群の作用が**余等方的**であるとは, 含まれる群軌道が全て余等方的部分多様体となる $\mathcal{D}$ の (空でない) 開部分集合が存在することと定義する.

一方, 可視的作用の理論 [Kob3] は, 余等方的作用とは別の観点から表現の無重複性を扱う.

定義 3.4 ([Kob1]). (1) $\mathcal{D}$ の全実部分多様体 S および G-不変な (空でない) 開集合 $\mathcal{D}' \subset \mathcal{D}$ で, それに含まれる全ての G-軌道が S と交わるようなものが存在するとき, 作用は**準可視的**であると呼ばれる.

(2) さらに, 全ての $x \in S$ に対して $J_x(T_xS) \subset T_x(G \cdot x)$ のとき, 準可視的作用は**可視的**であると呼ばれる. ただし $J_x \in \mathrm{End}(T_x\mathcal{D})$ は複素構造を表す.

(3) また, ある $\mathcal{D}'$ の反正則微分同相写像 σ が存在し, 次が満たされるとき, 準可視的作用は**強可視的**であると呼ばれる:

$$\sigma|_S = \mathrm{Id}_S,$$

σ が $\mathcal{D}'$の各 G-軌道を保存する.

以下, 強可視的というとき, 反正則微分同相写像 σ が対合的であるという条件を追加して考える.

表現の無重複性が, 幾何学的条件だけから導かれることがある. ただし, 筆者の知る限りでは, 以下の結果と本稿の主結果との間に明確な包含関係があるわけではない.

定理 3.5 ([FT, Theorem 3], [HW, Corollary 7.6]). 次が成り立つ.

(1) $\mathcal{D}$ の正則同相群の連結コンパクト部分群について, 作用が余等方的であることと, ヒルベルト空間 $H^2(\mathcal{D})$ 上のユニタリ表現が無重複であることは同値である.

(2) 群 G の $\mathcal{D}$ への作用が強可視的ならば π_0 は無重複である.

本稿の設定と近いものとして, 次の冪零リー群の例を挙げる.

例 3.6 ([Kob2, Theorem 1.10]). G/K をノンコンパクト型エルミート対称空間とするとき, 群 G の極大ユニポテント部分群の G/K への作用は強可視的である.

4 ジーゲル領域と擬対称領域

以下では, 本稿を通し, リー群のリー代数を表す方法として, 対応するドイツ文字を用いる. 複素ベクトル空間 V とその実形 W に対して, ベクトル $v \in V$ の W に関する複素共役を $\overline{v}^W$ で示す. 体を $\mathbb{R}$ に制限することで得られる実ベクトル空間 V を $V_{\mathbb{R}}$ と表す. 一方, 実ベクトル空間または実リー代数 W に対して, その複素化 $W \otimes_{\mathbb{R}} \mathbb{C}$ を $W_{\mathbb{C}}$ と表す. ベクトル $v \in W_{\mathbb{C}}$ の自然な複素共役を単に $\overline{v}$ と書くことがある. また $\xi \in W^*$ と表記した場合, 複素線型性によって $W_{\mathbb{C}}$ 上の線型形式に拡張されたものを表すことがある.

4.1 ジーゲル領域

ジーゲル領域は上半平面の一般化であり, 任意の有界等質領域はジーゲル領域に正則同値である [VGP]. ノンコンパクト型エルミート対称空間はハリシュ・チャンドラ埋め込みにより, 複素有界領域として実現されるため, ジーゲル領域に正則同値である. U, V をそれぞれ有限次元実および複素ベクトル空間 ($\dim U = N$, $\dim_{\mathbb{C}} V = M$), $\Omega \neq \emptyset \subset U$ を直線を含まない開凸錐, $Q : V \times V \to U_{\mathbb{C}}$ をベクトル値エルミート形式で Ω-正, すなわち $Q(v,v) \in \mathrm{cl}(\Omega)\backslash\{0\}$ $(v \in V\backslash\{0\})$ を満たすものとする. このとき, 次で定義される複素領域は**ジーゲル領域**と呼ばれている:

$$\mathcal{S}(\Omega, Q) := \{(z,v) \in U_{\mathbb{C}} \times V \mid \mathrm{Im}\, z - Q(v,v) \in \Omega\}.$$

ルベーグ測度に関する L^2 正則関数全体のなすヒルベルト空間 $L^2_a(\mathcal{S}(\Omega,Q))$ の核関数を $\mathcal{S}(\Omega,Q)$ の**ベルグマン核**という.

定理 4.1 ([Gin]). $\mathcal{S}(\Omega,Q)$ のベルグマン核は次の積分表示を持つ:

$$K(z,v,z',v') = \int_{\Omega'} e^{\langle \xi, i(z-\overline{z'}) + 2Q(v,v')\rangle}\, dm_{\mathcal{S}}(\xi). \tag{4.1}$$

ここで

$$\Omega' := \{\lambda \in U^* \mid \langle \lambda, y\rangle > 0 \text{ for all } y \in \mathrm{cl}(\Omega)\backslash\{0\}\}$$

であり $m_{\mathcal{S}}$ はその上のルベーグ測度に同値な測度である.

ここで, 各 $\xi \in \Omega^*$ に対して, 被積分関数

$$e^{\langle \xi, i(z-\overline{z'}) + 2Q(v,v')\rangle}$$

は以下に定義する $\mathcal{S}(\Omega,Q)$ のアフィン変換群 G^V-不変な核関数 (端点) である. そして, 積分表示 (4.1) は G^V のユニタリ表現 $(\pi_0, L^2_a(\mathcal{S}(\Omega,Q)))$ が無重複であることを表している. ここで 各 $x_0 \in U, v_0 \in V$ に対して, 領域 $\mathcal{S}(\Omega,Q)$ のアフィン変換 $n(x_0,v_0) : \mathcal{S}(\Omega,Q) \to \mathcal{S}(\Omega,Q)$ を

$$n(x_0,v_0)(z,v) := (z + x_0 + 2iQ(v,v_0) + iQ(v_0,v_0), v + v_0)$$

で定め, 実部分空間 $W \subset V$ に対して

$$G^W := \{n(x_0,v_0) \mid x_0 \in U, v_0 \in W\}$$

とおいた. リー代数 $\mathfrak{g}^W$ は $U \oplus W$ と自然に同一視される. これにより, 複素化, 双対空間など, 他の関連するベクトル空間も同一視される.

定理 4.1 から自然に生じる疑問として, 次のようなものが挙げられる: (1) π_0 が G^V の表現として無重複であるか, (2) G^V の作用が余等方的であるか, (3) 認容パラメトリゼーションの始域が Ω' とどのような関係にあるか. 一般に, 部分群の無重複性からもとの群の無重複性が得られる (定理 3.2 参照). そのため, 無重複性が成り立つ小さい群について調べることは意義深い. そこで, 本稿では次の問題を考えたい. ただし, 実際の解決は, 4.2 節で導入する擬対称領域に限定して行う.

問 4.2. (1) どのような実部分空間 $W \subset V$ に対して, 群 G^W の連続表現 π_0 が無重複であるか.

(2) またそれを余等方的作用で特徴づけられるか.

(3) 認容パラメトリゼーションをどのようにとれるか.

4.2 擬対称領域

擬対称領域は, ジーゲル領域の対称性条件の一つを落とした領域として定義される [Sat, §5]. この意味で, 擬対称領域は対称領域に準じた領域のクラスに属していると言える. なお, この領域の名称は統一されておらず, 準対称ジーゲル領域などと呼ばれることもある. 以下では, 本稿に適した形で擬対称領域を定義する. 元の定義やその性質等の詳細については, 前述の文献を参照されたい.

まず, 凸錐 $\Omega \subset U$ として対称錐が指定されることから, 実ベクトル空間 U にジョルダン代数の構造が入るという事実について, [Sat, Chapter 1, §6-8] に基づき説明する. 群

$$G(\Omega) := \{g \in GL(U) \mid g\Omega = \Omega\}$$

は, 自然にリー群の構造を持つ. $G(\Omega)$ の作用が推移的であるとき, Ω を**等質錐**と呼ぶ. U の内積 $\langle\cdot,\cdot\rangle_U$ を固定し,

$$\Omega^* := \{x \in U \mid \langle x, y\rangle_U > 0 \text{ for all } y \in \mathrm{cl}(\Omega)\backslash\{0\}\}$$

とおく. U の正規直交基底を用いて $\mathbb{R}^N$ のルベーグ測度の押し出しを考え, それを U 上のルベーグ測度とみなす. $\Omega = \Omega^*$ のとき等質錐 Ω を**対称錐**と呼ぶ. $A \in \mathfrak{gl}(U)$ の $\langle\cdot,\cdot\rangle_U$ に関する随伴を ${}^tA$ で表す. Ω を対称錐とする. このとき $\mathbb{R}$-群 $G(\Omega) \subset G \subset GL(U)$ で, ザリスキー位相に関する連結成分 G^z が, カルタン対合 $g \mapsto {}^tg^{-1}$ を持つ簡約 $\mathbb{R}$-群となるものが存在することが知られている. カルタン対合 $\theta : \mathfrak{g}(\Omega) \ni A \mapsto -{}^tA \in \mathfrak{g}(\Omega)$ に対応する $\mathfrak{g}(\Omega)$ のカルタン分解を

$$\mathfrak{k}_0 := \mathfrak{g}(\Omega)^{\theta}, \quad \mathfrak{p}_0 := \mathfrak{g}(\Omega)^{-\theta}$$

とおく. 基準点 $e \in U$ として次を満たすものをとる:

$$A \in \mathfrak{k}_0 \Leftrightarrow Ae = 0 \quad (A \in \mathfrak{g}(\Omega)). \tag{4.2}$$

$x \in U$ に対して, 線型変換 $T_x \in \mathfrak{p}_0$ で $T_x e = x$ を満たすものが一意的に存在する. 次で定義される演算に関して (U, e) は単位元を持つジョルダン代数である:

$$xy := T_x y \quad (x, y \in U).$$

V 上の複素構造を j で表す. h を V 上のエルミート内積とし, この内積に関する $B \in \mathfrak{gl}(V)$ の随伴を B^* で表す. $\beta : \mathfrak{g}(\Omega) \to \mathfrak{gl}(V)$ をリー代数 $\mathfrak{g}(\Omega)$ の表現で $A \in \mathfrak{g}(\Omega)$ および $x \in U$ に対して次を満たすものとする:

$$\beta(T_{Ax}) = \beta(A)\beta(T_x) + \beta(T_x)\beta(A)^*, \tag{4.3}$$

$$\beta({}^tA) = \beta(A)^*, \tag{4.4}$$

$$\beta(\mathrm{Id}_U) = \frac{1}{2}\mathrm{Id}_V. \tag{4.5}$$

$x \in U$ に対して

$$R_x := \beta(T_x)$$

とおき, ベクトル値エルミート写像 $Q : V \times V \to U_{\mathbb{C}}$ を次で定義する:

$$2h(R_x v, v') = \langle x, Q(v, v')\rangle_U \quad (x \in U, v, v' \in V).$$

ここで, $\langle \cdot, \cdot \rangle_U$ を $\mathbb{C}$-双線型に拡張した. この Q を使ってジーゲル領域 $\mathcal{S}(\Omega, Q)$ が定義されるが, 本稿ではこれを**擬対称領域**と呼ぶ.

5 主結果

実ベクトル空間 V_0 上の対称双線型形式 $b \in \mathrm{Sym}^2(V_0{}^*)$, および部分空間 $W_0 \subset V_0$ に対して,

$$W_0{}^{\perp, b} := \{v \in V_0 \mid b(v, w) = 0 \text{ for all } w \in W_0\}$$

とおく. $x \in U$ に対して $g_x \in \mathrm{Sym}^2(V_{\mathbb{R}}{}^*)$ を次で定義する:

$$g_x(v_1, v_2) := \langle x, \operatorname{Re} Q(v_1, v_2)\rangle_U \quad (v_1, v_2 \in V).$$

実部分空間 $W \subset V$ に対して, 実部分空間 $S \subset V$ を次で定義する:

$$S(:= S(W)) := jW^{\perp, g_e}.$$

ジョルダン代数のスペクトル定理 [FK94, THEOREM III. 1.1] より次が導かれる.

命題 5.1. 集合として

$$\operatorname{Im} Q(S, S) = \{0\} \tag{5.1}$$

のとき次が成り立つ:

$$\langle x, \operatorname{Im} Q(W^{\perp, g_x}, W^{\perp, g_x})\rangle_U = 0 \quad (x \in U).$$

本稿の主定理は次である.

定理 5.2. $\mathcal{S}(\Omega, Q)$ を擬対称領域とする．実部分空間 $W \subset V$ について, 以下は同値である．

(i) G^W の連続表現 π_0 は無重複である;

(ii) G^W のユニタリ表現 $(\pi_0, L^2_a(\mathcal{S}(\Omega, Q)))$ は無重複である;

(iii) 式 (5.1) が成り立つ;

(iv) $\mathcal{S}(\Omega, Q)$ 上の各 G^W-軌道は (ベルグマン計量から定まるシンプレクティック形式に関して) 余等方的部分多様体である．

注意 5.3. (1) (iii) はジーゲル領域の幾何的な制約条件として比較的古くから知られており (例えば [Gin, Proposition 1.3] を参照), 具体的にはジーゲル領域 $\mathcal{S}(\Omega, Q|_{(S\oplus jS)\times(S\oplus jS)})$ が管状領域に正則同値であるという条件になる．

(2) 定理 5.2 の証明について, まず (i) ⇒ (ii) は定理 3.2 から従う．(ii) ⇒ (iii) は G^V の既約ユニタリ表現としての無重複性を用いる (4.1 節を参照)．ここで G^V のユニタリ表現の G^W への制限から定まる既約分解が問題になるが, 群 G^V が冪零リー群であることに注意すると, 余随伴軌道の方法において, コーウィン・グリーンリーフの重複度関数 [CG] を証明に利用できる．

複素部分空間 $P \subset V$ を

$$P := W \cap jW$$

で定義する．$x \in U$ に対して, 複素部分空間 $N_x \subset P$ および実部分空間 $S_x \subset V$ を次のように定義する:

$$N_x := \{q \in P \mid g_x(q, q) = 0\}, \tag{5.2}$$

$$S_x := jW^{\perp, g_x} \cap W. \tag{5.3}$$

$0 \le k \le \dim_{\mathbb{C}} P$ に対して,

$$\Lambda_k := \left\{ x \in U \;\middle|\; \begin{array}{c} g_x|_{P\times P} \text{ は半正定値}, \\ \dim_{\mathbb{C}} N_x = k, \quad N_x \subset \ker(g_x). \end{array} \right\} \tag{5.4}$$

とおき, 相対位相を入れる．次に, これらの直和 $\widetilde{\Lambda} := \coprod_{k=0}^{\dim_{\mathbb{C}} P} \Lambda_k$ に積位相を入れる．式 (5.1) のもと $\mathrm{ext}(\Gamma_{G^W}(\mathcal{S}(\Omega, Q)))$ の認容パラメトリゼーションの始域として

$$\Lambda := \widetilde{\Lambda} \times S^*$$

がとれる．P の複素部分空間 P^x を次で定める:

$$P^x := N_x^{\perp, g_e} \cap P.$$

定理 5.4. 式 (5.1) のもと $x \in \widetilde{\Lambda}$ に対して次が成り立つ.

(1) $S_x \cap jS_x = P \cap \ker(g_x) = N_x$.

(2) 実部分空間 $S^x \subset S_x$ で N_x の補空間となるものを任意に固定するとき $W = P^x \oplus S_x = P \oplus S^x$ が成り立つ.

$x \in \widetilde{\Lambda}$ とする. 定理 5.4(2) より

$$V = P \oplus S^x \oplus jS^x$$

であることに注意して, 複素ベクトル空間 $S^x \oplus jS^x$ への射影の $S \oplus jS$ への制限 $S \oplus jS \to V$ を p^x とかく. $(S \oplus jS, h)$ 上の自己共役作用素 A^x を次で定義する:

$$A^x := 2(p^x)^* R_x p^x.$$

いま $(x, \chi) \in \Lambda$ に対して,

$$\begin{aligned} K^{x,\chi}(z, v, z', v') := &\exp(i\langle x, z - \overline{z'} - 2iQ(v, v')\rangle_U + h(s - \overline{s'}^S, A^x(\overline{s}^S - s'))) \\ &\cdot e^{-i\langle \chi, s - \overline{s'}\rangle} \end{aligned}$$

とおく. ただし $v = q + s, v' = q' + s'$ $(q, q' \in P, s, s' \in S \oplus jS)$ である.

定理 5.5. 式 (5.1) のもと $\Lambda \ni (x, \chi) \mapsto K^{x,\chi} \in \mathrm{ext}(\Gamma_{G^W}(\mathcal{S}(\Omega, Q)))$ が認容パラメトリゼーションを与える.

6 可視的作用

定理 6.1. 群 G^W の $\mathcal{S}(\Omega, Q)$ への作用が強可視的であることと, 実ベクトル空間 W に含まれる V の実形 V_0 が存在して $\operatorname{Im} Q(V_0, V_0) = \{0\}$ が成り立つことは同値である.

この結果は一般のジーゲル領域に対して成立する. したがって定理 5.2 の全ての条件は G^S の $\mathcal{S}(\Omega, Q|_{(S\oplus jS)\times(S\oplus jS)})$ への作用が強可視的であることと同値である. 一方, 定理 5.2 の条件のうちいずれか一つが成り立つならば, 群 G^W の $\mathcal{S}(\Omega, Q)$ への作用は可視的である.

7 主定理 5.2 (iii) $\Rightarrow$ (i) の証明の概略

この節の内容は, 実質的に認容パラメトリゼーションの決定と同じ内容である.

7.1 コヒーレント状態

まず我々の扱う群は冪零リー群であり, 余随伴軌道の方法が使える. 群 G^W の既約ユニタリ表現 $(\pi, \mathcal{H})$ が $\mathcal{O}(\mathcal{S}(\Omega, Q))$ に実現され, キリロフ・ベアナ写像によって $(-\nu) \in (\mathfrak{g}^W)^*$ を通る余随伴軌道に対応すると仮定する. 余随伴作用を Ad^* で表すとき $\mathrm{Ad}^*(G^W)(-\nu)|_U = -\nu|_U$ に注意して, コーウィン・グリーンリーフの重複度関数を使うと, 制限 $\mathrm{Res}^{G^W}_{G\{0\}} \pi$ は一つの既約表現のコピーであることが分かる. この事実により次を満たす $F \in \mathcal{O}(V)$ が存在する:

$$K^{\mathcal{H}}_{(ie,0)}(z, v) = e^{i\langle \nu, z\rangle} F(v) \quad ((z, v) \in \mathcal{S}(\Omega, Q)). \tag{7.1}$$

以下では U の内積 $\langle \cdot, \cdot \rangle_U$ により U と U^* を自然に同一視し, 記号 ν で $\nu|_U \in U^*$ に対応する U のベクトルを表すことがある. $f := K^{\mathcal{H}}_{(ie,0)}$ とおくとき $K^{\mathcal{H}}$ の G^W-不変性より次が導かれる:

$$d\pi_0(a) f = 0 \quad (a = q - ijq, q \in P). \tag{7.2}$$

ここでユニタリ表現 $\pi_0|_{\mathcal{H}}$ を π_0 と省略し, 微分表現 $d\pi_0$ を複素線型性によって $(\mathfrak{g}^W)_{\mathbb{C}}$ の表現に拡張した. $\mathcal{H}$ の射影空間を $\mathbb{P}(\mathcal{H})$ で表し, 接空間 $T_f\mathcal{H}$ および $T_{[f]}\mathbb{P}(\mathcal{H})$ の間の自然な射影 p_f を考える. $T_{[f]}\mathbb{P}(\mathcal{H})$ 上のフビニ・スタディ計量は以下で与えられる：

$$\|dp_f(f_0)\|^2_{FS} = \frac{\|f\|^2_{\mathcal{H}} \|f_0\|^2_{\mathcal{H}} - |(f, f_0)_{\mathcal{H}}|^2}{\|f\|^4_{\mathcal{H}}}. \tag{7.3}$$

ここで 式 (7.2) から

$$d\pi_0(\mathfrak{h}) f \subset \mathbb{C} f \tag{7.4}$$

を満たす複素部分代数 $\mathfrak{h} \subset \mathfrak{g}^W$ を見つけることは容易であり, 式 (7.2) をコヒーレント状態表現の定義条件の類似 ($\mathfrak{h} \oplus \overline{\mathfrak{h}} = (\mathfrak{g}^W)_{\mathbb{C}}$ は課さない) とみなせる [Lis2]. $a := q + ijq\,(q \in P)$ に対して次が成り立つ:

$$\|dp_f(d\pi_0(a) f)\|^2_{FS} = \frac{(d\pi_0([a, \overline{a}]) f, f)_{\mathcal{H}}}{\|f\|^2_{\mathcal{H}}} = -i\langle \nu, [a, \overline{a}]\rangle_U. \tag{7.5}$$

したがって次を得る.

補題 7.1 (c.f. [Lis1, 2. Proposition])**.** $x = \nu \in U$ に対して

$$-i\langle x, [a, \overline{a}]\rangle_U = 8\langle x, Q(q, q)\rangle_U \geq 0. \tag{7.6}$$

$q \in P$ に対して, $\langle \nu, Q(q, q)\rangle_U = 0$ のとき 式 (7.5) が消えることから次が導かれる.

補題 7.2. $x = \nu \in U$ に対して次が成り立つ:

$$N_x \subset \ker(g_x). \tag{7.7}$$

式 (5.1) を仮定する. ジョルダン代数のスペクトル定理を用いることで $[jW]_x \cap [W]_x = [P]_x\,(x \in U)$ が導かれる. ただし $x \in U$ および実部分空間 $V_0 \subset V$ に対して $[V_0]_x := V_0 + \ker(g_x)/\ker(g_x) \subset V/\ker(g_x)$ と置いた. $x = \nu$ のとき, この分解と式 (7.6), (7.7) から定理 5.4(2) の分解が得られ, 式 (7.1) において $F \in \mathcal{O}(S^\nu \oplus jS^\nu)$ と考えられる. 核関数 $K^{\mathcal{H}}$ が端点であることから命題 5.1 をつかって $k(s,s') := e^{-\langle \nu, Q(s-\overline{s'}^\nu, \overline{s}^\nu - s')\rangle} F(s-\overline{s'}^\nu) \in \mathrm{ext}(\Gamma_{S^\nu}(S^\nu \oplus jS^\nu))$ が導かれる. ここで, $x \in \widetilde{\Lambda}$ に対して $s \in S^x \oplus jS^x$ の複素共役 $\overline{s}^{S^x}$ を $\overline{s}^x$ と省略した.

定理 7.3. ある $\chi \in (S^\nu)^*$ が存在し, 次が成り立つ:

$$\begin{aligned} &K^{\mathcal{H}}(z, q+s, z', q'+s') \\ &= \exp(i\langle \nu, z - \overline{z'} - 2iQ(q,q') - 2iQ(s,s') - iQ(s-\overline{s'}^\nu, \overline{s}^\nu - s')\rangle_U) \\ &\quad \cdot e^{-i\langle \chi, s - \overline{s'}^\nu\rangle}. \end{aligned} \tag{7.8}$$

ここで, $q, q' \in P, s, s' \in S^\nu \oplus jS^\nu$ である.

注意 7.4. コヒーレント状態という名称から物理的な背景を想像するかもしれない. ここでは, 式 (7.4) が不確定性原理に関係していることを紹介する. 具体的には, 対称作用素 $A = id\pi_0(q)$ と $B = id\pi_0(jq)$ の状態 $[f_0]$ における不確定性を, それぞれ $\sigma_A([f_0])$ と $\sigma_B([f_0])$ とした場合, 状態 $[f]$ はこれらの積を最小にする候補となる [Nee, XV.3].

7.2 アウスランダー・コスタント理論

定理 7.3 の核関数がどのような既約ユニタリ表現を定めているか, 余随伴軌道と対応を付けたい. 複素解析的な設定であるから, アウスランダー・コスタントによる複素解析的誘導表現の理論 ([AK]) と相性が良い. これは, 実分極環ではなく, 複素分極環を用いて表現を構成する理論である.

$x \in \widetilde{\Lambda}$, $\sigma \in (S_x)^*$ に対して $X_{x,\sigma} \in (\mathfrak{g}^W)^*$ を次で定義する:

$$X_{x,\sigma}(x_0, q_0 + s_0) := -\langle x, x_0\rangle_U + \langle \sigma, s_0\rangle \quad (x_0 \in U, q_0 \in P^x, s_0 \in S_x).$$

複素分極環を

$$\mathfrak{p} := U_{\mathbb{C}} \oplus (S_x)_{\mathbb{C}} \oplus \{q + ijq \mid q \in P^x\} \subset (\mathfrak{g}^W)_{\mathbb{C}}$$

とおく. これらから構成される複素解析的誘導表現を $V_{x,\sigma}$ とおく. $\sigma|_{N_x} = 0$ のとき, 群 G^W の表現 $V_{x,\sigma}$ が $\mathcal{O}(\mathcal{S}(\Omega, Q))$ に実現される. このときの核関数は $q, q' \in P, s, s' \in S^x \oplus jS^x$ に対して

$$\begin{aligned} &L^{x,\sigma}(z, q+s, z', q'+s') \\ &= \exp(i\langle x, z - \overline{z'} - 2iQ(q,q') - 2iQ(s,s') - iQ(s-\overline{s'}^x, \overline{s}^x - s')\rangle_U) \\ &\quad \cdot e^{-i\langle \sigma, s - \overline{s'}^x\rangle} \end{aligned} \tag{7.9}$$

となる．式 (7.8), (7.9) を比較すると $x = \nu$ かつ線型形式 $\sigma \in (S_\nu)^*$ を, 分解 $S_\nu = S^\nu \oplus N_\nu$ において $\chi \in (S^\nu)^*$ のゼロ拡張としたとき, 表現 $(\pi_0, \mathcal{H})$ が余随伴軌道 $G^W X_{x,\sigma}$ に対応することが分かる [Fu]. 最後に, 余随伴軌道を観察することで証明が完成する.

参考文献

[AK] L. Auslander, B. Kostant, Polarization and unitary representations of solvable Lie groups. Appendix by C. C. Moore, Invent. Math. **14**, 255–354 (1971).

[CG] L. Corwin, F. P. Greenleaf, Spectrum and multiplicities for restrictions of unitary representations in nilpotent Lie groups, Pac. J. Math. **135**, 233–267 (1988).

[FK94] J. Faraut, A. Korányi, Analysis on symmetric cones, (Oxford, Clarendon Press, 1994).

[FT] J. Faraut, E. G. F. Thomas, Invariant Hilbert spaces of holomorphic functions, J. Lie Theory **9**, 383–402 (1999).

[Fu] H. Fujiwara, On unitary representations of exponential groups, J. Fac. Sci., Univ. Tokyo, Sect. I A **21**, 465–471 (1974).

[Gin] S. G. Gindikin, Analysis in homogeneous domains, Russ. Math. Surv. **19**, 1–89 (1964).

[HW] A. T. Huckleberry, T. Wurzbacher, Multiplicity-free complex manifolds, Math. Ann. **286**, 261–280 (1990).

[Kob1] T. Kobayashi, Multiplicity-free representations and visible actions on complex manifolds, Publ. Res. Inst. Math. Sci. **41**, 497–549 (2005).

[Kob2] T. Kobayashi, Visible actions on symmetric spaces, Transform. Groups **12**, 671–694 (2007).

[Kob3] T. Kobayashi, Propagation of multiplicity-freeness property for holomorphic vector bundles, in Lie Groups: Structure, Actions, and Representations, ed. by A. Huckleberry et al. Progress in Mathematics, vol. 306 (Birkhäuser, Basel, 2013).

[Lis1] W. Lisiecki, Kaehler coherent state orbits for representations of semisimple Lie groups, Ann. Inst. Henri Poincaré, Phys. Théor. **53**, 245–258 (1990).

[Lis2] W. Lisiecki, Coherent state representations: A survey, Rep. Math. Phys. **35**, 327–358 (1995).

[Nee] K.-H. Neeb, Holomorphy and convexity in Lie theory. de Gruyter Expositions in Mathematics, vol. 28 (Berlin, de Gruyter, 1999).

[Sat] I. Satake, Algebraic structures of symmetric domains, Kano Memorial Lectures, vol. 4 (Tokyo, Iwanami Shoten, Publishers, 1980).

[Sch] L. Schwartz, Sous-espaces d'espaces vectoriels topologiques et noyaux associés. (Noyaux reproduisants.), J. Anal. Math. **13**, 115–256 (1964).

[VGP] É. B. Vinberg, S. G. Gindikin, I. I. Piatetski-Shapiro, Classification and canonical realization of complex bounded homogeneous domains, Trans. Mosc. Math. Soc. **12**, 404–437 (1963).

[VR] M. Vergne, H. Rossi, Analytic continuation of the holomorphic discrete series of a semisimple Lie group, Acta Math. **136**, 1–59 (1976).

[Wa] N. Wallach, The analytic continuation of the discrete series. I, II, Trans. Amer. Math. Soc. **251**, 1–17, 19–37 (1979).

Smoothing estimate for the heat semigroup with a homogeneous weight on Morrey spaces *

波多野 修也 †

記号一覧

- $\partial_t = \dfrac{\partial}{\partial t}$, Laplacian: Δ.
- Lebesgue 測度: $|E|$ $(E \subset \mathbb{R}^n)$.
- 特性関数: $\chi_E(x) \equiv \begin{cases} 1, & x \in E, \\ 0, & x \notin E. \end{cases}$
- ノルム評価において, $A \leq CB$ が成り立つとき, A, B に含まれる関数やその変数に依存しない定数 C は省略して, $A \lesssim B$ と表す. また, $A \lesssim B$ かつ $A \gtrsim B$ のとき, $A \sim B$ と表す.
- 2 種のノルム区間 $X = (X, \|\cdot\|_X)$, $Y = (Y, \|\cdot\|_Y)$ について,

$$\|f\|_Y \lesssim \|f\|_X \quad ({}^\forall f \in X)$$

  が成り立つとき, $X \hookrightarrow Y$ と表す. また, $X \hookrightarrow Y$ かつ $X \hookleftarrow Y$ のとき, $X \cong Y$ と表す.
- $T : X \to Y$: 有界作用素 $\underset{\text{def}}{\iff}$ $\|Tf\|_Y \lesssim \|f\|_X$ $({}^\forall f \in X)$.
- Lebesgue 空間 (p 乗可積分な関数全体): $L^p(\mathbb{R}^n)$.
- $B(x, \rho) \equiv \{y \in \mathbb{R}^n : |x - y| < \rho\}$, $B(\rho) \equiv B(0, \rho) = \{x \in \mathbb{R}^n : |x| < \rho\}$.
- $\boldsymbol{e}_1 \equiv (1, 0, \ldots, 0) \in \mathbb{R}^n$.

1 導入

幂乗型の非線形項を持つ半線形熱方程式

$$\begin{cases} \partial_t u(t,x) - \Delta u(t,x) = |u(t,x)|^{\alpha-1} u(t,x), & (t,x) \in (0,\infty) \times \mathbb{R}^n, \\ u(0,x) = u_0(x), & x \in \mathbb{R}^n \end{cases} \tag{H}$$

---

* 本研究は池田正弘氏 (理化学研究所, 慶應大学) との共同研究によりに基づく

† 中央大学理工学研究科数学専攻, n.hatano,chuo@gmail.com

はよく研究されている．近年では，非線形項にさらに荷重 (homogeneous weight) が付いた以下のような Hardy-Hénon の放物型方程式の研究がよく行われている:

$$\begin{cases}\partial_t u(t,x) - \Delta u(t,x) = |x|^{-\gamma}|u(t,x)|^{\alpha-1}u(t,x), & (t,x)\in(0,\infty)\times\mathbb{R}^n, \\ u(0,x) = u_0(x), & x\in\mathbb{R}^n\end{cases} \tag{HH}$$

ただし，$\alpha > 1$, $\gamma > 0$ とする．

注意 1.1.

(1) Hénon [7] が方程式 (HH) の定常問題を用いて，恒星の回転軌道の研究を行ったことが起源となっている．
(2) Ben Slimene-Tayachi-Weissler [1]: 方程式 (HH) に対する Lebesgue 空間上の大域的な適切性.
(3) Tayachi [11]: 方程式 (HH) に対する Lorentz 空間上の解の無条件一意性.

方程式 (HH) は Duamel の原理により，積分方程式

$$u(t,x) = e^{t\Delta}u_0(x) + \int_0^t e^{(t-\tau)\Delta}[|x|^{-\gamma}|u(\tau,x)|^{\alpha-1}u(\tau,x)]\,\mathrm{d}\tau$$

に帰着される．ここで，$\{e^{t\Delta}\}_{t>0}$ は熱半群 (heat semigroup) のことであり，

$$e^{t\Delta}f(x) \equiv \frac{1}{\sqrt{(4\pi t)^n}}\int_{\mathbb{R}^n}\exp\left(-\frac{|x-y|^2}{4t}\right)f(y)\,\mathrm{d}y, \quad (t,x)\in(0,\infty)\times\mathbb{R}^n$$

と定義される．このとき，Young の不等式により

$$\|e^{t\Delta}f\|_{L^s} \lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)}\|f\|_{L^p} \quad (1\le p\le s<\infty)$$

が示される．

非線形項における写像 $f \mapsto e^{t\Delta}[|\cdot|^{-\gamma}f]$ に対する平滑化効果 (smoothing estimate) の選考結果は以下のように与えられる．

定理 1.2. $1 \le p, s < \infty$ *and* $\gamma > 0$ とし，

$$\frac{n}{s} - \frac{n}{p} \le \gamma < n - \frac{n}{p}$$

と仮定する．このとき，以下の主張が成り立つ:

(1) *Ben Slimene-Tayachi-Weissler* [1]:

$$\|e^{t\Delta}[|\cdot|^{-\gamma}f]\|_{L^s} \lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}}\|f\|_{L^p}.$$

(2) *Tayachi* [11]:

$$\|e^{t\Delta}[|\cdot|^{-\gamma}f]\|_{L^s} \lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}}\|f\|_{L^{p,\infty}}.$$

そこで，本講演では，Morrey 空間を用いた平滑化効果の改良を紹介する．

2 関数空間の導入

この節で, 本研究で得られた主結果の主張や証明を述べるために必要な関数空間を導入する.

2.1 弱 Lebesgue 空間

本研究では, 弱 Lebesgue 空間は主定理の証明で用いる. Lebesgue 積分論における Chebychev の不等式によると,

$$t|\{x \in \mathbb{R}^n : |f(x)| > t\}|^{\frac{1}{p}} \le \left(\int_{\mathbb{R}^n} |f(x)|^p \, \mathrm{d}x \right)^{\frac{1}{p}}, \quad t > 0$$

が成り立つことが知られている. そこで, 左辺の t における上限として定められる擬ノルムを持つ関数空間は, 調和解析において重要な役割を持つ.

定義 2.1 (弱 Lebesgue 空間, cf. [5, Chapter 1])**.** $1 \le p < \infty$ とする. このとき, 弱 Lebesgue 空間 $\mathrm{W}L^p(\mathbb{R}^n)$ 有限な擬ノルム

$$\|f\|_{\mathrm{W}L^p} \equiv \sup_{t>0} t|\{x \in \mathbb{R}^n : |f(x)| > t\}|^{\frac{1}{p}}$$

を持つ可測関数 f 全体である.

弱 Lebesgue 空間に対しては以下の性質が知られている.

注意 2.2.

(1) 擬三角不等式

$$\|f + g\|_{\mathrm{W}L^p} \lesssim \|f\|_{\mathrm{W}L^p} + \|g\|_{\mathrm{W}L^p}$$

が成り立つ. 特に, ノルムの三角不等式の代わりにこのような擬三角不等式が成り立つとき, 擬ノルムと呼ばれており, 完備な擬ノルム空間のことを擬 Banach 空間という.

(2) 特に $p > q$ ならば,

$$\|f\|_{\mathrm{W}L^p} \sim \sup_{0<|E|<\infty} |E|^{\frac{1}{p}-\frac{1}{q}} \left(\int_E |f(x)|^q \, \mathrm{d}x \right)^{\frac{1}{q}}$$

が成り立つ. 従って $p > 1$ のとき, 特に $q = 1$ の場合で右辺をノルムとして採用すれば, $\mathrm{W}L^p(\mathbb{R}^n)$ は Banach 空間となる.

(3) 埋め込み $L^p(\mathbb{R}^n) \hookrightarrow \mathrm{W}L^p(\mathbb{R}^n)$ が成り立つ. さらに, 具体例として $|x|^{-n/p} \in \mathrm{W}L^p(\mathbb{R}^n) \setminus L^p(\mathbb{R}^n)$ が挙げられる.

2.2 Morrey 空間

Morrey 空間とは, 1938 年に Morrey 氏 [8] によって導入された関数空間であり, この空間を用いて 2 階楕円型偏微分方程式の解の滑らかさを調べたことが起源となっている. 特に当時の論文では, 導関数が Morrey 空間に属するときそのような関数は Hölder 連続であるという性質

$$|f(x)-f(y)| \lesssim \|\nabla f\|_{\mathcal{M}_1^p}|x-y|^{1-\frac{n}{p}}$$

が示されている. ここで, Morrey 空間 $\mathcal{M}_q^p(\mathbb{R}^n)$ は以下のように定義される.

定義 2.3 (Morrey 空間, cf. [9, Chapter 1])**.** $1 \le p, q < \infty$ とする. このとき, Morrey 空間 $\mathcal{M}_q^p(\mathbb{R}^n)$ は有限なノルム

$$\|f\|_{\mathcal{M}_q^p} \equiv \sup_{(x,\rho)\in\mathbb{R}^n\times(0,\infty)} \rho^{\frac{n}{p}-\frac{n}{q}} \left(\int_{B(x,\rho)} |f(y)|^q \, \mathrm{d}y\right)^{\frac{1}{q}}$$

を持つ可測関数 f 全体である.

Morrey 空間には以下の基本性質が成り立つ.

注意 2.4.

(1) Morrey 空間は Banach 空間である.

(2) $p < q$ のとき, $\mathcal{M}_q^p(\mathbb{R}^n) = \{0\}$ が成り立つ.

(3) $1 \le q_2 \le q_1 \le p < \infty$ のとき, 埋め込み

$$\mathcal{M}_p^p(\mathbb{R}^n) = L^p(\mathbb{R}^n) \hookrightarrow \mathcal{M}_{q_1}^p(\mathbb{R}^n) \hookrightarrow \mathcal{M}_{q_2}^p(\mathbb{R}^n)$$

が成り立つ.

特に $p > q$ のとき, 埋め込み $\mathrm{W}L^p(\mathbb{R}^n) \hookrightarrow \mathcal{M}_q^p(\mathbb{R}^n)$ が成り立つ. さらに,

$$E = B(1) \cup \bigcup_{j=1}^{\infty} B(10^j \boldsymbol{e}_1, 1)$$

と置けば, 具体例として $\chi_E \in \mathcal{M}_q^p(\mathbb{R}^n) \setminus \mathrm{W}L^p(\mathbb{R}^n)$ が挙げられる.

2.3 局所 Morrey 型空間

主定理の証明の際に鍵となる関数空間として, Morrey 空間に似た関数空間である局所 Morrey 型空間を導入する.

定義 2.5 (局所 Morrey 型空間, cf. [10, Chapter 16])**.** $1 \le p, q < \infty$, $1 \le r \le \infty$ とする. このとき, 局所 Morrey 型空間 $\mathrm{L}\mathcal{M}^p_{q,r}(\mathbb{R}^n)$ を有限なノルム

$$\|f\|_{\mathrm{L}\mathcal{M}^p_{q,r}} \equiv \begin{cases} \left(\displaystyle\int_0^\infty \left[\rho^{\frac{n}{p}-\frac{n}{q}}\left(\int_{B(\rho)}|f(x)|^q\,\mathrm{d}x\right)^{\frac{1}{q}}\right]^\rho \frac{\mathrm{d}\rho}{\rho}\right)^{\frac{1}{r}}, & r<\infty, \\ \displaystyle\sup_{\rho>0}\rho^{\frac{n}{p}-\frac{n}{q}}\left(\int_{B(\rho)}|f(x)|^q\,\mathrm{d}x\right)^{\frac{1}{q}}, & r=\infty \end{cases}$$

を持つ可測関数 f 全体とする.

局所 Morrey 型空間に対する基本性質は以下のとおりである.

注意 2.6.

(1) $r=\infty$ の場合, すなわち, $\mathrm{L}\mathcal{M}^p_{q,\infty}(\mathbb{R}^n)$ は局所 Morrey 空間とも呼ばれ, $\mathrm{L}\mathcal{M}^p_q(\mathbb{R}^n)$ とも書かれる. さらに,

$$\|f\|_{\mathcal{M}^p_q} = \sup_{x\in\mathbb{R}^n}\|f(x-\cdot)\|_{\mathrm{L}\mathcal{M}^p_q}$$

を満たす.

(2) $r<\infty$ のとき,

$$\mathrm{L}\mathcal{M}^p_{q,r}(\mathbb{R}^n) \neq \{0\} \iff p>q$$

が成り立つ.

(3) $q_1 \ge q_2$ のとき, 埋め込み $\mathrm{L}\mathcal{M}^p_{q_1,r}(\mathbb{R}^n) \hookrightarrow \mathrm{L}\mathcal{M}^p_{q_2,r}(\mathbb{R}^n)$ が成り立つ.

(4) $r_1 \le r_2$ のとき, 埋め込み $\mathrm{L}\mathcal{M}^p_{q,r_1}(\mathbb{R}^n) \hookrightarrow \mathrm{L}\mathcal{M}^p_{q,r_2}(\mathbb{R}^n)$ が成り立つ.

(5) Burenkov-Guliyev, [3, page 159]: $\|f\|_{\mathrm{L}\mathcal{M}^p_{q,q}} = \left(n-\dfrac{nq}{p}\right)^{-\frac{1}{q}}\left\||\cdot|^{\frac{n}{p}-\frac{n}{q}}f\right\|_{L^q}$.

この関数空間の重要な点は, 実補間空間という手法が使えることである. 実補間空間は以下のように定義される.

定義 2.7 (cf. [2, Chapter 3])**.** X_0, X_1 を (擬)Banach 空間とする. このとき, パラメータ $\theta \in (0,1)$ と $r \in (0,\infty]$ に対して, 実補間空間 $(X_0,X_1)_{\theta,r}$ 以下の同値なノルム

$$\|f\|_{(X_0,X_1)_{\theta,r}} \equiv \left(\int_0^\infty \left[\rho^{-\theta}K(\rho,f)\right]^r \frac{\mathrm{d}\rho}{\rho}\right)^{\frac{1}{r}} \sim \left(\int_0^\infty \left[\rho^{-\theta}J(\rho,f)\right]^r \frac{\mathrm{d}\rho}{\rho}\right)^{\frac{1}{r}}$$

が有限となる関数 f 全体とする.

実補間空間に対する重要な性質は, 補間定理と呼ばれる以下の定理が重要である.

定理 2.8. X_0, X_1, Y_0, Y_1 を (擬)*Banach* 空間とし, $T: X_0 \to Y_0$ と $T: X_1 \to Y_1$ がともに有界作用素であり,

$$\|Tf\|_{Y_i} \le {}^{\exists}M_i\|f\|_{X_i} \quad (i=0,1)$$

成り立つとする．このとき，パラメータ $\theta \in (0,1)$ と $r \in (0,\infty]$ に対し，$T:(X_0,X_1)_{\theta,r} \to (Y_0,Y_1)_{\theta,r}$ も有界作用素となり，

$$\|Tf\|_{(Y_0,Y_1)_{\theta,r}} \le M_0^{1-\theta} M_1^{\theta} \|f\|_{(X_0,X_1)_{\theta,r}}$$

が成り立つ．

実補間空間の具体的な計算結果は補間定理を用いる際には重要な研究テーマとなっている．特にここでは, 主定理を証明する際に用いた結果をまとめておく．

定理 2.9. $1 \le q \le p_0, p_1 < \infty$, $1 \le r, r_0, r_1 \le \infty$ とし，

$$p_0 \ne p_1, \quad \frac{1}{p} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}$$

と仮定する．このとき, 以下が成り立つ．

(1) $(X,X)_{\theta,r} \cong X$.
(2) $(L^{p_0}(\mathbb{R}^n), L^{p_1}(\mathbb{R}^n))_{\theta,\infty} \cong \mathrm{W}L^p(\mathbb{R}^n)$.
(3) $(\mathrm{W}L^{p_0}(\mathbb{R}^n), \mathrm{W}L^{p_1}(\mathbb{R}^n))_{\theta,p} \cong L^p(\mathbb{R}^n)$.
(4) *Burenkov-Nursultanov,* [4]: $(\mathrm{L}\mathcal{M}^{p_0}_{q,r_0}(\mathbb{R}^n), \mathrm{L}\mathcal{M}^{p_1}_{q,r_1}(\mathbb{R}^n))_{\theta,r} \cong \mathrm{L}\mathcal{M}^{p}_{q,r}(\mathbb{R}^n)$.

この定理の (4) と注意 2.6 (5) から

$$\left(L^q\left(\mathbb{R}^n, |\cdot|^{\frac{n}{p_0}-\frac{n}{q}}\right), L^q\left(\mathbb{R}^n, |\cdot|^{\frac{n}{p_1}-\frac{n}{q}}\right)\right)_{\theta,\infty} \cong \mathrm{L}\mathcal{M}^p_q(\mathbb{R}^n)$$

も成り立つ．ここで, $L^q\left(\mathbb{R}^n, |\cdot|^{\frac{n}{p}-\frac{n}{q}}\right)$ は

$$\|f\|_{L^q\left(|\cdot|^{\frac{n}{p}-\frac{n}{q}}\right)} \equiv \left\| |\cdot|^{\frac{n}{p}-\frac{n}{q}} f \right\|_{L^q}$$

をノルムとする荷重付き Lebesgue 空間である．従って, Lebesgue 空間上の荷重理論に補間理論を組み合わせることは, Morrey 空間に対して有効なアプローチとなると予想している．

3　主結果

主結果は以下のように与えられる．

定理 3.1 (H.-Ikeda, [6])**.** $1 < q \le p < \infty$, $1 < s < \infty$ *and* $\gamma > 0$ とし，

$$\frac{n}{\min(q,s)} - \frac{n}{p} < \gamma < n - \frac{n}{p}$$

と仮定する．このとき，

$$\|e^{t\Delta}[|\cdot|^{-\gamma} f]\|_{L^s} \lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}} \|f\|_{\mathcal{M}^p_q}$$

が成り立つ．

Proof. $q \geq s$ の場合は, 注意 2.4 (3) より, $q < s$ の場合のみ示せば充分である. 以下, $q < s$ と仮定する. 線形作用素 $f \mapsto e^{t\Delta}[|\cdot|^{-\gamma} f]$ の有界性に補間定理を用いる. まず,

$$\gamma = \frac{n}{\tilde{q}} - \frac{n}{\tilde{p}}, \quad 1 \leq \tilde{q} \leq \tilde{s}$$

を満たすパラメータ $\tilde{p}, \tilde{q}, \tilde{s}$ を選べば,

$$\|e^{t\Delta}[|\cdot|^{-\gamma} f]\|_{L^{\tilde{s}}} \lesssim t^{-\frac{n}{2}\left(\frac{1}{\tilde{q}}-\frac{1}{\tilde{s}}\right)} \||\cdot|^{-\gamma} f\|_{L^{\tilde{q}}} \sim t^{-\frac{n}{2}\left(\frac{1}{\tilde{p}}-\frac{1}{\tilde{s}}\right)-\frac{\gamma}{2}} \|f\|_{\mathrm{L}\mathcal{M}^{\tilde{p}}_{\tilde{q},\tilde{q}}}$$

が成り立つ. 定理の仮定より, パラメータ $(\tilde{p}, \tilde{q}, \tilde{s}) = (p_i, q_i, s_i)$ $(i = 0, 1)$ を適切に

$$\frac{n}{q} - \frac{n}{p_0} = \gamma = n - \frac{n}{p_1}, \quad q_0 = q, \quad q_1 = 1$$

を満たすように選び, 補間定理を用いれば,

$$\begin{aligned}
&\|e^{t\Delta}[|\cdot|^{-\gamma} f]\|_{(L^{s_0}, L^{s_1})_{\theta,\infty}} \\
&\lesssim \left(t^{-\frac{n}{2}\left(\frac{1}{p_0}-\frac{1}{s_0}\right)-\frac{\gamma}{2}}\right)^{1-\theta} \left(t^{-\frac{n}{2}\left(\frac{1}{p_1}-\frac{1}{s_1}\right)-\frac{\gamma}{2}}\right)^{\theta} \|f\|_{(\mathrm{L}\mathcal{M}^{p_0}_{q,q}, \mathrm{L}\mathcal{M}^{p_1}_{1,1})_{\theta,\infty}} \\
&\lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}} \|f\|_{(\mathrm{L}\mathcal{M}^{p_0}_{q,q}, \mathrm{L}\mathcal{M}^{p_1}_{q,1})_{\theta,\infty}}
\end{aligned}$$

が成り立つ. よって,

$$\|e^{t\Delta}[|\cdot|^{-\gamma} f]\|_{\mathrm{W}L^s} \lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}} \|f\|_{\mathrm{L}\mathcal{M}^p_q} \leq t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}} \|f\|_{\mathcal{M}^p_q}$$

が得られる. さらに, $s > q$ であることからパラメータ $s_0 > s_1 > q$ を選び, もう一度補間定理を用いれば,

$$\|e^{t\Delta}[|\cdot|^{-\gamma} f]\|_{(\mathrm{W}L^{s_0}, \mathrm{W}L^{s_1})_{\theta,s}} \lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}} \|f\|_{(\mathcal{M}^p_q, \mathcal{M}^p_q)_{\theta,s}}$$

となるから, 結論

$$\|e^{t\Delta}[|\cdot|^{-\gamma} f]\|_{L^s} \lesssim t^{-\frac{n}{2}\left(\frac{1}{p}-\frac{1}{s}\right)-\frac{\gamma}{2}} \|f\|_{\mathcal{M}^p_q}$$

が得られる. □

参考文献

[1] B. Ben Slimene, S. Tayachi and F. B. Weissler, Well-posedness, global existence and large time behavior for Hardy–Hénon parabolic equations, Nonlinear Anal. **152**, 116–148 (2017).

[2] J. Bergh, J and L. Löfström, Interpolation spaces, An introduction. Grundlehren der Mathematischen Wissenschaften, no. 223. Springer-Verlag, Berlin-New York, 1976.

[3] V. I. Burenkov and H. V. Guliyev, Necessary and sufficient conditions for boundedness of the maximal operator in local Morrey-type spaces, Studia Math. **163** (2004), no. 2, 157–176.

[4] V. I. Burenkov and E. D. Nursultanov, Description of interpolation spaces for local Morrey-type spaces, Tr. Mat. Inst. Steklova **269** (2010), 52–63. Proc. Steklov Inst. Math. **269** (2010), no. 1, 46–56.

[5] L. Grafakos, Classical Fourier Analysis, Texts in Mathmatics, Springer, New York, Third edition **249** (2014).

[6] N. Hatano and M. Ikeda, Smoothing estimate for the heat semigroup with a homogeneous weight on Morrey spaces, arXiv:2404.14094.

[7] M. Hénon, Numerical experiments on the stability of spherical stellarsystems, Astron. Astrophys. **24** (1973) 229–238.

[8] C. B. Morrey Jr., On the solutions of quasi–linear elliptic partial differential equations, Trans. Amer. Math. Soc. **43** (1938), no. 1, 126–166.

[9] Y. Sawano, G. Di Fazio and D. Hakim, Introduction and Applications to Integral Operators and PDE's, Volume I, (Chapman & Hall/CRC Monographs and Research Notes in Mathematics).

[10] Y. Sawano, G. Di Fazio and D. I. Hakim, Morrey spaces-introduction and applications to integral operators and PDE's. Vol. II, Monogr. Res. Notes Math. CRC Press, Boca Raton, FL, 2020, xviii+409 pp.

[11] S. Tayachi, Uniqueness and non-uniqueness of solutions for critical Hardy-Hénon parabolic equations, J. Math. Anal. Appl. **488** (2020), no. 1.