7. 文部科学省委託事業関連

7-1 「数学・数理科学と諸科学・産業との協働によるイノベーション創出のための研究促進プログラム（略称：数学協働プログラム)）（中核機関：統計数理研究所，H24～28 年度）

①数学協働プログラムワークショップ「大自由度分子系における化学反応機序の理解と制御」

開催日時：2015/10/31 ～ 2015/11/01

開催場所：北海道大学理学部 3 号館 202 号室

運営責任者：北海道大学電子科学研究所附属社会創造数学研究センターデータ数理分野

（センター専任教員）寺本　央　准教授

北海道大学電子科学研究所附属社会創造数学研究センターデータ数理分野

（センター長）小松崎　民樹　教授

採択番号：2015W02

該当する重点テーマ：ビッグデータ、複雑な現象やシステム等の構造の解明

キーワード：力学系理論 、関数解析 、応用特異点論 、確率微分方程式 、準古典解析 、量子化学

プログラム

(Day 1)

13:00-13:10 小松崎民樹・寺本　央（北海道大学電子科学研究所）ワークショップ開催の趣旨説明

13:10-13:40 佐藤　譲（北海道大学電子科学研究所）Random strange attractors and stochastic chaos

13:45-14:15 河合信之輔（静岡大学理学部化学科）大自由度系を効率よく記述する確率微分方程式と隠された自由度の抽出法

14:20-14:50 中野直人（北海道大学さきがけ専任研究員　確率微分方程式）TBA

15:00-15:30 寺本　央（北海道大学電子科学研究所）特異点論を用いた非断熱交差の安定性と分岐の解析

15:35-16:05 武次徹也（北海道大学理学部化学科）量子化学における反応経路モデルと経路分岐

16:15-16:45 千葉逸人（九州大学マスフォアインダストリ研究所）A generalized spectral theory based on a Gelfand triplet

16:50-17:20 安池智一（放送大学教養学部）環境と相互作用する分子のダイナミクス ー 電子共鳴状態，電子集団運動，ランダム力学

17:25-17:55 山口義幸（京都大学情報学研究科数理工学専攻）古典平均場系の特殊性と応用可能性

18:00-18:30 高橋博樹（慶應義塾大学理工学部数理科学科）Escape rate for non hyperbolic one-dimensional maps

ポスター発表

(Day 2)

09:00-10:00 高塚和夫（東京大学教養学部）分子科学の諸問題（基調講演）

10:10-10:40 小嶋泉（京都大学）量子と古典 --ミクロマクロ双対性の視点から-

10:45-11:15 藤井幹也（東京大学大学院工学系研究科化学システム工学専攻）ホッピング周期軌道による非断熱系の半古典量子化
11:20-11:50 斉木吉隆（一橋大学大学院商学研究科）双曲性が崩れた状況における不安定周期軌道展開の試み
13:25-13:55 國府寛司（京都大学大学院理学研究科）Morse decomposition of regulatory networks via determining nodes
14:00-14:30 小西哲郎（中部大学工学部共通教育科）整数化された保測写像：統計性と対称性
14:35-15:05 戸田幹人（奈良女子大学研究院自然科学系物理領域）大自由度力学系の特徴抽出
15:10-15;40 柳尾朋洋（早稲田大学基幹理工学部）高分子鎖の周期的なひねり運動から生じる幾何学的な宙返り効果
15:55-16:25 荒井迅（北海道大学理学部数学科）エノン写像のモノドロミー
16:30-17:00 首藤啓（首都大学東京理工学研究科物理学専攻）非可積分系のトンネル効果

まとめと自由討論
参加者数：数学・数理科学：14、 諸科学：13
当日の論点
① 非線形ランダム力学系の現象論の構築に向けて
② Liouville（Langevin, Schrodinger）方程式をいくつかの物理量で張られる空間に射影することで得られる一般化ランジュバン方程式の解析法
③ 時系列データから確率微分方程式、一般化ランジュバン方程式の抽出法
④ 断熱ポテンシャル面上の経路の分岐、断熱ポテンシャル面間の交差の構造とその分岐
⑤ 量子共鳴状態を記述するための一般化スペクトル理論とその量子化学への応用
⑥ 長距離相互作用系における緩和の理論とその量子化学への応用
⑦ 非双曲系におけるエスケープ率
⑧ 高次元結び目理論、余次元１の多様体のトポロジーの化学反応速度論への応用可能性
⑨ ミクロマクロ双対性の視点からの量子古典対応
⑩ 周期軌道展開(古典、量子)の非双曲系、非断熱系への拡張
⑪ 大自由度力学系の理解およびその時系列解析の手法
⑫ 高分子鎖の周期的なひねり運動から生じる幾何学的な宙返り効果
⑬ 複素力学系と非可積分系のトンネル効果の理解

研究の現状と課題（既にできていること、できていないことの切り分け）
① 非線形ランダム力学系の現象論
近年、化学反応動力学においても孤立分子系における化学反応とその溶媒中での反応との違いに注目が集まっている。孤立分子系における化学反応はSchrödinger方程式、または、Newton方程式により記述できるのだが、溶媒中での反応においてはそれに加えて分子の周囲の溶媒からうける揺動の効果を考慮する必要がある。そのような外部から系に加わる揺動の効果をランダムな雑音として理想化したものがランダム力学系であり、すでに溶媒中におけるタンパク質の折り畳みのシミュレーション等に幅広く用いられている。そのようなシミュレーションにより多くの現象が再現されているが、一方で、その動力学の現象論的な理解はあまり進んでいるとは言えない。例えば、系の温

度等のパラメータを変化させたときに系の動力学が質的に変化するようにみえる、自励力学系における分岐現象のようなものがみられる場合があるが、ランダム力学系における分岐とは何か？ということに対する最終的な答えは得られていない。また、ランダム力学系を含む非自励力学系を理解するため、自励力学系の概念が非自励力学系に拡張されてきているが、

・自励力学系と違い非自励力学系は対象が広すぎるのでその中でどのような力学系に的を絞るのがよいのか(その中でも歪積力学系等の比較的扱いやすいクラスもあるが)わからない。

・自励力学系の概念の拡張の仕方も一通りではなく、どのような拡張を考えればよいのか数学的な観点だけからは明らかではない場合もある。 これらの問題には数学だけで答えを出すのは難しいが、自然現象を通して現れるランダム力学系を解析することにより、

・どのようなクラスの非自励力学系(ランダム力学系)を考察の対象とすればよいのか？

・自励力学系における種々の概念の内、どの概念がランダム力学系の理解においても有用であるのか？

・自励力学系における概念のランダム力学系への自然な拡張が一通りではない場合にどの拡張が有意義であるのか？

という問題を解きながら、非線形ランダム力学系の現象論を構築していく必要がある。本ワークショップでは、佐藤らに非線形ランダム力学系の現象論の構築に向けての現状と展望に関して講演していただいた。自励力学系におけるLyapunov指数の非自励力学系への自然な拡張であるDichotomy spectrumとそれによるランダム力学系の分岐の特徴づけに関する活発な議論がなされた。

Dichotomy spectrumは数学的にはきれいな性質を持っているが、その具体的な計算は難しくあまり具体的な系には適用されてこなかった。今回、佐藤らによりその具体的な例への応用がなされたことにより、そのDichotomy spectrumのsupの正負によりランダム力学系の分岐を特徴づける可能性が示されたとともに、臨界点を持つ写像の場合にはそのinfが常に負の無限大になってしまうためinfの方はそのような写像力学系に対してはあまり有用な情報をもたらさないであろうことが解明された。このような可能性及び問題点は具体的な応用がないとあまり認識されない問題であり、今後もこのような具体的な応用を通じて、何が非自励力学系の理解に有用な概念であるのか、という選別が行われ、非線形ランダム力学系の現象論の構築、および、それによるランダム力学系の理解が進んで行くことが期待されている。

既に出来ている事：

・いくつかの系のランダム力学系によるモデル化およびその系における現象の再現

・歪積力学系などの非自励力学系への種々の自励力学系の概念の拡張可能性の議論

できていないこと：

・自励力学系のようにランダム力学系として考察すべき自然な力学系のクラスを考える。

・一つの自励力学系の概念に対して、いくつかの自然なランダム力学系への拡張が考えられるとき、どの拡張がランダム力学系の理解にとって有用なのかを考える。

・以上のことを通して、ランダム力学系のどの部分が自励力学系の自然な拡張として理解されるかを明らかにし、その上でランダム力学系と自励力学系の質的な違いを明らかにすること。

② Liouville（Langevin, Schrödinger）方程式をいくつかの物理量で張られる空間に射影することで得られる一般化ランジュバン方程式の解析法

一般化ランジュバン方程式は大自由度のLiouville（Langevin, Schrödinger）方程式を少数自由度で張られる空間に射影することで得られる方程式であり、形式的には少数自由度だけで閉じた形になるため、複雑な系の動力学を解明するための有力な方法論である。この一般化ランジュバン方程式の歴史は古く、古くは森、久保ら[2]に始まり川崎の非線形Langevin方程式[3]において形式的には完成され、ガラスなどの遅い緩和を扱うため系の背後にある分布関数も時間発展する状況を記述するため、時間依存射影演算子法等に拡張されてきている。本ワークショップでは、河合らにそのレビュー、解析法および与えられた時系列から一般化ランジュバン方程式を構築するための試みの報告がなされた。一般化ランジュバン方程式は、”ノイズ”項と”記憶”項と呼ばれる二つの項からなる[4]。”それらを厳密に計算することは縮約する前の方程式を解く以上に困難であるため様々な近似が考えられてきた。比較的よく用いられる近似としては、・”ノイズ”項、”記憶”項は縮約された自由度に依存しない[5]。・”記憶”項をFourier変換(Laplace変換)したものは有理関数とする[6]。この時、記憶項は有限個の指数関数の重ね合わせとして記述される。という二つの近似であり、以上の近似の下、時系列からそれらの”ノイズ”項と”記憶”項およびその背後にあるいくつかの減衰モードを抽出するための方法論が議論された。 今後、上の二つの前提条件を緩和していくことが、より複雑な系の動力学を理解するうえで重要になるのではないかと期待される。

既にできていること：

”ノイズ”項、”記憶”項は縮約された自由度に依存しない、”記憶”項をFourier変換(Laplace変換)したものは有理関数とする、という理想化の下で、縮約された自由度の他いくつかの自由度を付け加えることにより記憶なしのランジュバン方程式に変形すること。

できていないこと：

二つの理想化を緩和しより一般的な系に適用可能な方法論を作ること。揺動散逸定理が破れているような非平衡系において、物理的に自然な力のノイズ項と散逸項に分解するための方法論を確立すること。

⑨ミクロマクロ双対性の視点からの量子古典対応

既にできていること：

化学ポテンシャルの概念を（ガロア理論的に）自然に導き出す数学的機構はAHKT 理 論（荒木・Haag・Kastler・竹崎）という形で既に出来上がっている。（ただし、その物理化学的意味や解釈の課題は放置されて来たので、その部分に関する考察を今回加えた。）

できていないこと：

「数理〇〇学」という領域を「分離」することにもろてを挙げて賛成というわけではないが，「数理論理学」，「数理言語学」，「数理物理学」，「数理生物学」等々， という名前を聞くのに対して，寡聞にして「数理化学」は聞いたことがない。「数学協働プログラム」という企画が何を目指すかに依ることだが，単に個別の研究課題に即した化学と数学との共同研究，というだけの協力に終わらせることなく，化学の基礎概念とその構成に関係する議論から始めて，「数理化学」の構築を目指すかなり長期の展望に向けたactivityがあれば，種々の異なるアプローチを統一的に理解する

ことによって理論展開が促進されるのではないか？そのために重要なのは，「数理〇〇学」という名前の本質を，数学との連携によって理論の概念構成に基いた柔軟な方法論の活用を重視するところに置くべきで，「厳密さ追求の自己目的化」ということには決して陥らないよう，絶えず注意を払うことが必要だと思う。

⑩周期軌道展開(古典、量子)の非双曲系、非断熱系への拡張

既にできていること：周期起動展開を用いて量子準位を考えることは量子論黎明期から考えられていて，前期量子論におけるボーアによる水素原子内電子の量子化にまで遡る．その後，トーラス量子化などを経てカオス系における量子準位の周期軌道展開がGutzwillerによって確立されるに至り，量子古典対応を考察する半古典力学として知られている．一方，非断熱系ダイナミクスの古典対応としてはホッピング軌道や平均場上の軌道を用いることが多かったが，これら古典的軌道は概念の導入に恣意的な部分が多く，妥当性は当然のこと，周期軌道展開によって量子準位を考察できるのか不明であった．このような状況のもと，近年藤井らによってホッピング軌道の半古典的導出[FUJII1]，および非断熱量子準位のホッピング周期軌道展開が行われ[FUJII2]，ホッピング軌道が非断熱量子現象の適切な古典的対応物であることが示された．本研究会でも藤井からホッピング軌道の導出およびホッピング周期軌道展開の発表があった．

できていないこと：

藤井らの研究は1自由度に限られており，その多自由度への拡張は全くできておらず今後の課題である．特に，２自由度以上の系で現れるコニカル・インターセクションは光反応から光電変換デバイスにいたるまで多くの化学的現象を決定的に左右する重要なものである．本研究会で寺本らによってコニカル・インターセクションがあるクラスに分類できることが示され，多自由度非断熱系における周期軌道展開やトーラス量子化と寺本らの分類がどのような接点をもつのかは今後の興味深い課題の１つである．本研究会で藤井が紹介したホッピング軌道は確率的にポテンシャルスイッチをおこす力学系としても解釈できる．歴史的に力学系の研究は非常に盛んに行われてきているものの，非断熱動力学・ホッピング軌道の力学系的理解は皆無といってよい．これはホッピング軌道の恣意性ゆえ，力学系研究者にとってホッピング軌道が興味の対象外であったためと思われる．しかし，ホッピング軌道の半古典的導出が確立した[FUJII1]現在においては，非断熱動力学・ホッピング軌道の力学系的理解(例えば，複数の断熱面間で不変多様体同士はどのように非断熱相互作用し得るか？)は，化学者と物理学者が協働してとりくむ課題だと考えられる．その他にも，高塚教授から指摘があったように，非断熱遷移は量子カオスと深い関係があることが知られている．さらに，M. Berryらが精力的に研究したように量子カオスは周期軌道展開の跡公式を通じて素数定理と関係があることも知られている．そのため，非断熱遷移と素数定理にも何か関係があることは十分考えられるが，そのような視点での研究は行われていない．本研究会で藤井が紹介したホッピング周期軌道による周期軌道展開では，ホッピング周期軌道に対して素因数分解を導入したのが本質的であり，まさに自然数の素因数分解との類似性を思わせる．このような状況のもと非断熱遷移と素数定理の関係を考察していくことは，分子の動力学に存在するかもしれない数学的実在をみつけることであり化学者と数学者が協働で，探求していくべき課題である．

[FUJII1] Mikiya Fujii, ″Quantum and semiclassical theories for nonadiabatic transitions based on overlap integrals related to fast degrees of freedom″, J. Chem. Phys. 135, 114102-1 - 114102-14 (2011)

[FUJII2] Mikiya Fujii and Koichi Yamashita,"Semiclassical quantization of nonadiabatic systems with hopping periodic orbits", ", J. Chem. Phys. 142,074104-1 -074104-10 (2015)

注釈および引用文献

[1] 例えば、自励力学系のアトラクターの非自励力学系への拡張として、forward attractor, pullback attractor等の種々の自然な拡張が考えられる。この場合、forward attractorは力学系の時間発展に対して不変ではないが、pullback attractorは力学系の時間発展に対して不変である、等の違いがあり数学的にはpullback attractorの方が扱いやすいということはあるかもしれない(Rasmussenら、Attractivity and Bifurcation for Nonautonomous Dynamical Systems, Springer(2007), Kloedenら、Nonautonomous Dynamical Systems, American Mathematical Society (2011)))。

[2] 森ら、Progr. Theoret. Phys. (Kyoto) 33, 423 (1965)).、久保ら、in Tokyo Lectures in theoretical Physics, edited by R. Kubo (W. A. Benjamin, Inc., New York, 1966), part I, p. 1.; R. Kubo, Rept. Progr. Phys. 29, 255 (1966)).

[3] 川崎ら、J. Phys. A: Math. Nucl. Gen. 6, 1289 (1973))

[4] ここで”　”としているのは、[一般化ランジュバン方程式を非平衡系に拡張した際に、この”ノイズ”と”記憶”項と物理的に解釈できるかに関して必ずしも明らかではないからである。一般化ランジュバン方程式においては、常に”ノイズ”項と”記憶”項の間に揺動散逸定理が成立するように、”ノイズ”項と”記憶”項が形式的に分解されるが、一方で、非平衡系においては原田・佐々等式に示されるようにノイズと記憶の項の揺動散逸定理が破れる、ということがわかっているからである(原田ら、Phys. Rev. Lett. 95, 130602 (2005))。この問題を解決するため林らによるノイズ項と記憶項の新しい分解の試み（林ら、Phys. Rev. E 71, 020102 (R),(2005))もある。

[5] タンパク質の折り畳み等において、遷移状態が縮約した自由度の空間で広く分布する場合には、”記憶”項の縮約した自由度依存性が重要になるのではないかという指摘がある(Plotkinら、Phys. Rev. Lett. 80, 5015 (1998))。特にタンパク質の場合には、ほどけた変性状態と折りたたまれた天然構造の間で水和構造等も劇的に変化するので、”記憶”項の座標依存性が重要になるのではないかと期待される。[6] 森の連分数展開(森ら、Progr. Theor. Phys. 34, 399 (1965))を有限次までで打ち切ったものに相当し、その場合に”記憶”項は有限個の指数関数の重ね合わせとして記述される。この連分数展開がどのぐらい広いクラスの解析関数に対して収束するのかに関しては、決定的な答えはないが(Bakerら、Pade Approximants, ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS, GAMBRIDGE (1994))、例えば連分数展開を有限次まで打ち切ったものは高々有理関数で複素平面上1価関数なので、ベキ的減衰を生むbranch cutを持つような解析関数等に対してはその連分数展開は元の関数に通常の意味では収束し得ない。しかしながら、いくつかのbranch cutを持つ特定の解析関数に対する連分数展開の収束性を議論した論文は存在し、それによると　1．与えられた複素関数に対してそのbranch cutは一通りには定まらないが、capacity（定義は先のBakerらの定義を参照のこと)が最小になるようなbranch cutが選ばれ、２．そのbranch cutに沿って連分数展開の極が並ぶ、 というような収束性を示すようであり、 このような場合には”記憶”項のベキ的な振る舞いは上のように選ばれたbranch cut上に並ぶ極に対応する指数関数の和として近似されると期待される。この他、解析関数が真正特異点、自然境界等の非孤立特異点を持つ場合、を含む非有理型関数に対する連分数展開の収束性の議論はあまりなく、この方面の発展がより

複雑な記憶の緩和挙動を理解するために望まれている。

新たに明らかになった課題、今後解決すべきこと

このワークショップでは、大自由度分子系における化学反応機序の理解と制御、というテーマの下、数学、物理、化学でご活躍されている研究者が一同に会して、議論の場を設けた。ランダウ減衰を物理の側から研究している研究者と化学の側から研究している研究者の交流、F1モーターの運動の解析に数学サイドからポーツハミルトン系の議論が使えないか等の提案等、ワークショップ中、数学、物理、化学の研究者の間で活発な議論がなされた。しかしながら、論点も多様であったため、もう少しその議論の前提知識を提供するような入門的講義を議論の前に設けたらよいのではないか、という意見が特に若手研究者の間から出された。今回は会期が２日間と短く、そのような入門的講義を設ける時間的余裕がなかったが、次期開催の際は、そのような入門的な講義を設けることを考えたい。また、本会議ではやや基礎的な話題が多かったが、何人かの参加者からは、そのような基礎的な話題だけではなく、理論と実験を繋ぐような、時系列解析・多変量解析・逆問題等のテーマも取り上げてもよいのではないかという意見もあった。今後、本ワークショップで見出された基礎理論を実験を通じて検証、または、その成果を産業界に役立てていくためには、そのような理論と実験を繋ぐインターフェースを充実させることも必要であると思われる。

②数学協働プログラムワークショップ「情報セキュリティにおける数学的方法とその実践」

■ 研究集会等の名称　情報セキュリティにおける数学的方法とその実践

■ 採択番号　　2016W13

■ 該当する重点テーマ　ビッグデータ、複雑な現象やシステム等の構造の解明 、計測・予測・可視化の数理 、最適化と制御の数理

■ キーワード　暗号理論 、サイバーセキュリティ 、ビッグデータ 、代数幾何 、組合せ論 、力学系 、量子コンピューティング

■ 主催機関

北海道大学大学院理学研究院数学部門

北海道大学電子科学研究所附属社会創造数学研究センター

北海道大学 Global Station for Big Data and Cybersecurity, GI-CoRE

産業技術総合研究所情報技術研究部門

■ 運営責任者

北海道大学大学院理学研究院数学部門　大本 亨教授／電子科学研究所附属社会創造数学研究センター教授兼務

産総研／JSTさきがけ　国立研究開発法人産業技術総合研究所・情報技術研究部門・高機能暗号研究グループ・主任研究員　縫田 光司（現職：東京大学大学院情報理工学系研究科 准教授（2018.4～））

■ 開催日時　　2016/12/19 09:50 ～ 2016/12/21 15:00

■ 開催場所　　北海道大学理学部４号館５階５０１教室

■ 最終プログラム

～情報セキュリティにおける数学的方法とその実践～

Mathematical methods and practice in cryptography, security and bigdata

12月19日（月）

09:50 - 10:00 ご挨拶 大本 亨（北大・理）・縫田光司（産総研／JSTさきがけ）

10:00 - 10:50 縫田光司（産総研／JSTさきがけ）

Cryptography, Information Security, and Mathematics: Recent Advances

11:00 - 11:50 清水佳奈（早稲田大・基幹理工）

準同型暗号による生命情報の秘匿検索

14:00 - 14:50 須賀祐治（（株）インターネットイニシアティブ）

クラウドストレージの外部操作に適した秘密分散方式

15:10 - 16:00 秋山浩一郎（東芝・研究開発センター）

不定方程式の最小解問題に基づく準同型暗号

16:10 - 17:00 山岡雅直（北大・電子研MSC／日立基礎研）

組合せ最適化問題に適した新概念イジングコンピューティング

18:00 - 20:00 懇親会

12月20日（火）

10:00 - 10:50 荒井 迅（北大・理）On topological tools for network analysis

11:00 - 11:50 有村博紀（北大・情報／GSB, GI-CoRE）準同型性暗号と非決定性オートマトンを用いたメモリと時間効率の良い秘匿正規表現照合（笹川裕人, 原田弘毅, Dave duVerle, 佐久間淳, 津田宏治との共同研究）

12:05 - 12:30 辻栄周平, 黒田匡迪（北大・理）A generalization of almost perfect nonlinear functions

14:00 - 14:50 高島克幸（三菱電機・情報技術総合研究所）格子と同種写像に関するアルゴリズムの耐量子暗号への応用

15:10 - 16:00 徳永浩雄（首都大・理工）A remark on Vanishing Component Analysis via (Hyper)graphs

16:10 - 17:00 Relinde Jurrius (Univ. Neuchatel, Switzerland)An introduction to error-correcting codes and some current-day applications

12月21日（水）

09:30 - 10:20 鍛冶静雄（山口大・理／JSTさきがけ）行列の極分解について

10:30 - 11:20 前野俊昭（名城大学・理工）Polynomial expressions of auction functions

12:40 - 13:30 Relinde Jurrius (Univ. Neuchatel, Switzerland)Application of hyperplane arrangements to error-correcting codes

13:40 - 14:30 沼田泰英（信州大・理）計算代数学の数理統計への応用について

■ 参加者数

数学・数理科学：28 諸科学： 産業界：4 その他：

■ 問合せ先　　大本 亨（北海道大学大学院理学研究院数学教室）
ohmoto@math.sci.hokudai.ac.jp
参照URL（北大情報グローバルステーション）https://gi-core.oia.hokudai.ac.jp/gsb/

■ 当日の論点

情報セキュリティ，データサイエンス，IoT分野等において展開されている数学的手法およびその今日的・将来的な課題について紹介し，討議を行った．準同型暗号に関する話題を中心に，第一線の研究者による講演とそれに伴う活発で長めの質疑応答により，求められる数学的課題の本質について理解を深めた．また，暗号理論に限らず，応用が期待される純粋数学の種々の理論や技法に関して，数学者，工学者，学生の間におけるブレインストーミングを通して，現実問題への新しい適用可能性について模索した．

■ 研究の現状と課題（既にできていること、できていないことの切り分け）クラウド上で秘匿性を保持したままデータを解析するために，暗号化と種々の演算操作がある種の可換性をもつような準同型暗号が，現在たいへん注目されている．有力なものは格子暗号であるが，その安全性の根拠となる格子の最小ベクトル探索問題に対する解析手法の発展に伴い，公開鍵サイズの増大が懸念されている．これに対して，代数曲面暗号系（関数体上のデオファントス問題の一種を安全性の根拠とする準同型暗号）が提案され，いくつかの攻撃に対する対処法と鍵サイズの評価について現状の報告がなされた．また，準同型暗号による生命情報分野におけるゲノム配列の秘匿検索技術や，非決定性オートマトンを用いた時間効率のよい秘匿正規表現のマッチング手法など，準同型暗号の具体的実装に関する研究が進められている．このような個々の問題での実装面において，計算量爆発を避ける技法の開発は今後も重要な課題である．暗号理論以外への新しい切り口として，トポロジーや代数幾何の応用についても多数の話題を扱った．すなわち，ホモロジー理論のネットワーク解析への応用，誤り訂正符号のクラウド・ネットワーキング等の応用，グレブナー基底の代数統計への応用（正則勾配法），アフィン群のリー環の表現のコンピュータグラフィクスへの応用について，どのようなタイプの問題が枠組みに乗るか，どのように効率性が高められるか，などに焦点を当てて議論した．

■ 新たに明らかになった課題，今後解決すべきこと

広く利用されている公開鍵暗号であるRSA暗号等は，量子コンピュータが実用化されたならば容易に破られてしまう-すなわち，Shorの量子アルゴリズムによって，素因数分解や離散対数問題さらにアーベル群の隠れ部分群問題等が効率よく解かれてしまうためである．そこで次世代型の暗号技

術においては，耐量子計算性を評価することが最も重要な課題となる．例えば，格子の最小ベクトル問題，不定方程式の最小解問題，楕円曲線間（さらに高種数曲線間）の同種写像の逆計算問題に依拠した暗号技術が有力である．代数曲面暗号や同種写像暗号については，代数曲線のモジュライ空間が持つ豊富な数学的構造を背景にして大いに発展する可能性がある．セキュリティ技術では，近年，クラウドストレージにおける秘密分散方法が広く関心を持たれている．クラウド上のデータ委託においても秘匿性や準同型性および処理速度や安全性が問題となる．排他的論理和のみを用いて構成される秘密分散方法はその意味で極めて有用であり，セキュリティ技術分野における数学の可能性を示唆している．ビッグデータ関連では，イジング・モデルへのマッピングを基に組合せ最適化問題の近似解を求めるローコストで実用的な古典的コンピューティングが提案された．この技術が効果的に扱える問題群の類型化とグラフ埋め込み問題等が数学的な課題として挙げられる．また，純粋数学サイドからは，ヒルベルト基底定理とマッチング手法の融合，超平面配置の組合せ的・代数幾何的不変量の誤り訂正符号理論における利用方法，有限体上の関数の明示的な多項式表示，非線形関数の個数評価について，新しい結果が報告された．これらは純粋数学の有用性を端的に示す萌芽的研究であって，これから発展する余地が十分にある．従来の数学的価値観とは異なり，社会的価値，効率性，安全性，実用性，汎用性など種々のファクターを通して数学概念・理論を見直すことで，新しい数学的関心が掘り起こされ，新しい応用研究が開拓される．この意味で，今回の集会で扱った題材とその方向性は十分に手応えがあったし，本企画に対するアンケートにおける評価もたいへん肯定的であった．

■ 今後の展開・フォローアップ

北海道大学では，数学・数理科学関連として，理学研究院数学部門のほか，昨年度に発足した電子科学研究所附属社会創造数学研究センター，今年度設立した情報科学研究科Global Station for Big Data and Cybersecurityの３部局がある．今回の研究集会は，これらの部局に加えて産業総合研所の情報技術研究部門の協力のもとに開催された．今後，上記３部局において，数学，数理科学，計算機科学，データサイエンスを研究する教員群が院生を巻き込んだブレインストーミングを通して，新しい応用研究領域を拡げるべく，交流活動を進めることが期待されている．暗号分野においては産総研の協力，さらに広い領域で九大や阪大等の数学・数理科学ネットワークからの協力を仰ぎ、この活動を育てて行きたい．特に，従来の（縦割りの）カリキュラムやキャリア・パスからはみ出して，数学系の若手研究者・院生に新しい応用領域への関心や挑戦する意志を引き起こし，応用系の若手研究者・院生に抽象的な数学概念や理論の有効性を説くことが重要と考える．

7-2 文部科学省委託事業「数学アドバンストイノベーションプラットフォーム (AIMaP: Advanced Innovation powered by Mathematics Platform)」(中核機関:九州大学マス・フォア・インダストリ研究所, H29-33 年度)

①名称　　非ノイマン型計算、理論と応用
採択番号　　2017A019
重点テーマ　　非ノイマン型計算機、特に近年各社が活発に開発しているイジング型計算機等のハードウェアのアプリケーション探索
理論の側からもどのような望ましい専用ハードウェアの模索
キーワード　　イジング型計算機、バイナリーニューラルネット、離散最適化、計算ファイナンス、ブースティング
運営責任者　　北海道大学電子科学研究所附属社会創造数学研究センターデータ数理分野
寺本　央　准教授
開催日時　　2018/03/30
開催場所　　北海道大学電子科学研究所１階会議室

プログラム
9:45 - 10:00　寺本 央（北海道大学）趣旨説明
10:00 - 11:00　竹本享史（日立製作所）非ノイマン型 CMOS アニーリングマシン
11:15 - 12:15　神山直之先生（九州大学）離散最適化とその社会応□
13:30 - 14:30　楠岡成雄先生（東京大学）ファイナンスと数値計算
14:45 - 15:45　畑埜晃平先生（九州大学）ブースティング:最適化の視点に基づくサーベイ
16:00 - 17:00　高前田伸也先生（北海道大学）量子化ニューラルネットワークのためのハードウェアとアルゴリズムの協調設計
意見交換会

参加者数　　数学・数理科学:13 人, 諸科学: 04 人, 産業界: 02 人
当日の論点
①非ノイマン型計算機、特に近年各社が活発に開発しているイジング型計算機等のハードウェアのアプリケーション探索
② 理論の側から望ましい専用ハードウェアの模索
研究の現状と課題（既にできていること、できていないことの切り分け）
研究の現状に関する報告：
・日立のイジング計算機と富士通のデジタルアニーラの現状に関しては、竹本様、神山先生らからご報告があった。
・マトロイド、劣モジュラ関数など離散最適化と相性の良い構造による社会問題のモデル化に関し神山先生よりご報告があった。
・数理ファイナンスの背景知識と現状に関する報告は楠岡先生よりあった。
・種々のブースティングと最近の動向に関しては畑埜先生からご報告があった。
・バイナリーニューラルネットのレビューと近年の取り組みに関するご報告が高前田先生よりあった。
課題：
・イジングモデルよりより広いクラスのモデルを解けるよう計算機を拡張できないか、例えばなぜ隣接スピン間の２体相互作用だけという制約があるのか、等ハードウェアの制約を考慮に入れながらどこまでモデルを一般化しうるのかの検討。
・日立のイジング計算機には画像解析、四色問題等長距離相互作用がないものが向いているのではないかと考えられるが、まだはっきりとしたキラーアプリケーションは見つけられていない。
・イジング計算機で解きやすい問題を狙うのかあるいは NP-hard 等難しい問題を

狙うべきかの見定め。
・Population simulated annealing のように多点スタートでスコアの良い（エネルギーが低い）状態を複製する等の方式がハードウェア実装と相性が良いのかどうかの検討。
・マトロイドは一般に極大を複数持つのだが、どの程度の数の極大を持ちうるのか、その全列挙は可能なのか等の検討。
・日立のイジング計算機は計算ファイナンスで現れる期待値の評価と相性が良いのかの検討。
・現実的には準モンテカルロ法で扱いうる積分計算の次元には上限がある。その上限の改良。
・LPBoost 並みに速い必要計算ステップ数の上限の見積もりを備えたブースティング手法の開発。
・機械学習の半化性能を向上させるために望ましい正則化項の検討。

新たに明らかになった課題、今後解決すべきこと
・日立のイジング計算機で初期条件はランダムに決まっているが、初期条件を工夫することでその性能を改善することができるかどうかの検証。
・日立のイジング計算機で乱数を入れてスピンの状態をその状態から離れた状態へと遷移させることの是非。
・日立のイジング計算機の計算ファイナンスの CVA (or XVA)への適用可能性の吟味。
・Qboost 以外のブースティングを QUBO で定式化可能性の検討。
・イジング計算機の磁場、相互作用係数の対数量子化。

今後の展開・フォローアップ　本ワークショップを通じ、日立製作所と数学・数理科学の新たなつながり、理論とハードウェアの専門家とのつながりが生じた。本ワークショップの質疑およびその後の意見交換会にて新たな検討課題も抽出できた。今後の開催は未定だが、本ワークショップで生まれたつながりをもとに非ノイマン型計算機のアプリケーション探索および理論の側から望ましい専用ハードウェアの模索を続けていきたい。

②名称　**反応拡散系と実験の融合**
採択番号　2017A015
重点テーマ　実験により検証可能な数学理論の考察
キーワード　生命科学，反応拡散系，数理モデリング，パターン形成，異分野融合研究
運営責任者　北海道大学大学院理学研究院数学部門　栄　伸一郎　教授／電子科学研究所附属社会創造数学研究センター教授兼務
北海道大学電子科学研究所附属社会創造数学研究センター人間数理分野
長山　雅晴　教授
開催日時　2018/02/21 ～ 2018/02/22
開催場所　石川県金沢市　しいのき迎賓館

プログラム
2月21日（水曜日）
9:55　Opening
10:00～10:40 八杉　徹雄（金沢大学　新学術創成研究機構）分化の波の数理モデル解析と生物学実験による実証
10:40～11:20　田中　吉太郎（北海道大学　理学研究院/CREST）分化の波の数理モデル解析と生物学実験による実証
11:20～11:40　討論時間

昼食
14:00～14:40 傳田　光洋（資生堂リサーチセンター/CREST）表皮バリア機能恒常性維持機構について
14:40～15:20 長山 雅晴（北海道大学 電子科学研究所/CREST）表皮構造の数理モデリング
15:20～15:40 討論時間
休憩
16:00～16:40 李　聖林（広島大学　理学研究科/JSTさきがけ）　非対称細胞分裂における極性形成
16:40～17:20 桑村　雅隆（神戸大学　人間発達環境学研究科）Some properties of a reaction-diffusion system with mass conservation and its perturbed system
17:20～17:40 討論時間
2月22日（木曜日）
10:00～10:40 富樫　英（神戸大学　医学研究科）細胞間接着の親和性と細胞パターン形成
10:40～11:20 村川　秀樹（九州大学　数理学研究院）細胞間接着の親和性と細胞パターン形成：数理的アプローチ
11:20～11:40 討論時間
昼食
14:00～14:40 芳賀　永（北海道大学 先端生命科学研究院）細胞の集団運動と3次元形態形成
14:40～15:20 秋山　正和（北海道大学 電子科学研究所）細胞の集団運動と3次元形態形成”に対する数理的アプローチ
15:20～15:40 討論時間
休憩
16:00～16:40 桧垣　匠（熊本大学 国際先端科学技術研究機構）葉表皮細胞のジグゾーパズル型形態形成
16:40～17:20 三浦　岳（九州大学 大学院医学研究科/CREST）植物細胞壁の湾曲構造形成の理論モデル
17:20～17:40　討論時間
17:40　　Closing

参加者数　　数学・数理科学:27 人, 諸科学: 06 人, 産業界: 01 人

当日の論点

数理科学者と諸分野との融合研究の進展について講演を行ってもらった．その中で、実験研究者と数理科学者が共同研究することの意義や共同研究するに至った経緯、共同研究時の異分野融合研究ならではの困難さについても議論した．

研究の現状と課題（既にできていること、できていないことの切り分け）

今回は現在進んでいる融合研究の現状について講演して頂いた。そのため、数理科学と諸分野（今回は特に生命科学の研究者）の研究者間のコミュニケーションが上手く取れていることが重要であることがより明確になった。また、生命科学者が求めている数理モデリングと数理解析可能な数理モデリングには大きな乖離があることも明確になった。諸分野と数理科学の真の融合研究には、実

験から数理モデリング、数理解析へと繋がるための方法論が必要であると考えられる。現状では、数理モデリングが現象を説明するための道具として、実験の請負仕事になる可能性が高い。

新たに明らかになった課題、今後解決すべきこと

諸分野と数理科学の研究者がコミュニケーションを取るための方法論を確立しないと今後のさらなる融合研究の発展に大きな障壁となる．どのような方法が適切なのか議論していく必要がある．
実験↔現象を説明できる数理モデリング↔縮約化↔数理解析可能な数理モデリング↔数理解析という連携した新しい形の数理と諸分野の融合研究を行う方法論を確立する必要があると思われる．

今後の展開・フォローアップ

今回講演して頂いた融合研究はさらなる発展が大きく見込めるため，今後の研究の進捗状況について研究集会等を開催して報告してもらう予定である．今回は反応拡散系の理論研究と実験研究の融合研究にテーマを絞って開催したが，近年は新しい融合研究が進んでいるので，次回は数理科学の分野を広げて融合研究の進捗状況を把握するための研究会を開催したい．