様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １２ 日現在

機関番号：１２１０１
研究種目：若手研究
研究期間：2020～2023
課題番号：２０Ｋ１４３０２

研究課題名（和文）整環上の格子圏におけるAuslander-Reiten理論の研究

研究課題名（英文）Auslander-Reiten theory for the lattice category of ordes

研究代表者
宮本　賢伍（Miyamoto, Kengo）

茨城大学・理工学研究科（工学野）・助教

研究者番号：９０８４５８０１

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：数学的な成果と工学的な成果を以下に述べる．数学的な成果として，(1) 完備離散付値環上の対称整環の（安定）AR箙の構造論に関するもの (2) 有限次元代数のτ傾有限による分類に関するもの (3) その他（連分数のq変形，有限群の一様分解に関するもの）がある．工学的な成果として，(4) カードベース暗号におけるシャッフルプロトコルの提案と実装およびパズルへの応用に関するもの (5) グラフのテキスト検索を応用とするグラフ線形表示の提案である．

研究成果の学術的意義や社会的意義
代数の表現論の大きな目標は代数の加群圏の解明にある．これは現代の言葉ではAR箙の構造を決定することや部分圏を分類することとなる．体上の有限次元代数のAR箙の構造と異なり，係数環の次元を上げればそれ上の代数のAR箙の構造論はまだまだ未開の分野である．今回は完備離散付値環の非特異孤立点とは限らないような対称整環の（安定）AR箙の形状に関する制限を与えたものである．部分圏の分類に関しては，（台）τ傾加群と呼ばれるものが（有限関手）ねじれ部分圏の分類を与え，これが有限となるケースは基本的であるため，様々な代数のクラスに対してτ傾有限な代数を完全に分類することは重要である．

研究成果の概要（英文）：Mathematical and engineering results are described below. Mathematical results include (1) the structure of (stable) AR quivers of symmetric orders over a complete discrete valued ring (2) the classification of finite dimensional algebras by τ-tilting finite, and (3) others (q-deformed continued fractions, uniform decomposition of finite groups). Engineering results include (4) a proposal and implementation of a shuffling protocol for card-based cryptography and its application to puzzles, and (5) a proposal for a graph linear notation with an application to text search on graphs.

研究分野：多元環の表現論，カードベース暗号

キーワード：安定AR箙　Heller格子　τ傾有限代数　カードベース暗号　グラフ自己同型シャッフル　一様群分解　q-連分数　グラフ線形表示

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属します。

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景
以下にそれぞれの研究に対する大まかな背景を述べる.

(1) 代数の表現論の共通の目標は「代数の加群圏または導来圏の構造を理解すること」である. そのための主な研究として, 単純または直既約加群の分類, 部分圏の分類が行われている. 係数環が体である整環(=有限次元代数)の場合は有限生成加群圏を理解することが目標であり, 係数環が完備離散付値環であるときは, 加群圏すべてを理解することは困難であるため加群圏の充満部分圏である格子圏を考察することになる. 特に直既約加群の分類は基本的な問題であり, 現代の用語では AR 箙とよばれる有向グラフを与えることになる. Drozd の古典的な結果により, 直既約加群が分類 できる代数は原始的に限られているため, より一般な代数になるほど AR 箙の一部だけを決定することが表現論における現実の目標である.整環の Auslander-Reiten 理論は「孤立特異点」と呼ばれる場合(例えば係数環が体の場合)には十分な発展があり AR 箙の計算例も多く与えられてるが, 非孤立特異点の場合の AR 箙の構造論はほとんど与えられていなかった. つまり, 係数環が体の場合は理論のみならず, 加群圏の AR 箙の具体的な構造論を与えるといった問題が多く解決されているが, 係数環の次元を 1 つあげて(完備な)離散付値環とすれば, AR 箙の構造が途端に複雑になり一般には全てを記述することはできない. 例えば, 体上の一変数剰余多項式環は Jordan 細胞によってパラメトライズできるが, 完備離散付値環上にすれば無限表現型となり統率がとれない状況であった. AR 箙の決定には概分裂完全列の計算を要するが, 係数環の次元が上がれば, 概分裂完全列を計算する具体的な手法が整備されていなかった. この不具合に対して, 研究代表者を含む共同研究において概分裂完全列の構成法を具体的に記述した. この構成法を用いることで, これまでほとんど進展のなかった非孤立特異点の AR 箙の具体的な構造論を与えることが可能となった.
また, 河田氏による群環の先行研究によれば, 群環の Heller 格子を終域にもつ AR 列を完備離散付値環の剰余体に係数拡大した完全列は, 剰余体上のある AR 列と完全列の直和になることが知られている. この性質は, 一変数剰余多項式環の場合に研究代表者らによって同じ性質を持つことがわかっている. これは, 完備離散付値環上の AR 箙から, 剰余体上の AR 箙が復元できることを述べており, このように係数環が異なる次元をもつ代数の AR 箙間の関係を明らかにできる可能性を示唆している.

(2) 先述のように, 加群圏の全てを扱える代数は原始的に限られている. そこで, 特に性質の良い部分圏を抽出して分類することで大まかに構造論を決定しようとする研究がなされてきた. 現代では 「ねじれ部分圏」を分類する研究が広く展開されている. 近年では足立, 伊山, Reiten によって導入された「台τ傾加群」によって関手的有限なねじれ部分圏が分類されているので, ねじれ部分圏の分 類には「台τ傾加群全体」がどのような構造をしているかを調べることに帰着されるといっていい. 台τ傾加群には変異と呼ばれる, 直既約因子を一つ取り替えて新しい台τ傾加群を作る圏論的操作がある が, このとき,「台τ傾加群が有限個しか存在しない」クラスは重要であり, この場合は「ねじれ部分圏」 は完全に分類される.

(3) 秘密計算とは, 大雑把にいえば n 人の各プレイヤーがブール関数にそれぞれ入力を行ったときに, 他のプレイヤーに入力の情報を知られることなく関数の値を得る計算手法である. 秘密計算の概念は 1980 年台に Yao によって定式化され, 現在では暗号理論における重要なトピックのひとつである. 秘密計算の分野の一つとして, デッキと呼ばれる物理的カード組を用いて秘密計算を実現することを目的としているのがカードベース暗号と呼ばれる分野である. カードベース暗号では, 各プレイヤーが入力をカード列として符号化し伏せた状態で提出した後, それらに対して並び替え, シャッフル, ターンを施すことで入力情報を秘匿し, 最後にカード列を全てめくることで出力を決定する. カードベース暗号の特徴は, カードを並べて実際にプロトコルを手操作で実現できることであり, プロトコルの正当性や安全性を直感的に理解できることである. そのため, 教育的効果が期待されており, 実際にいくつかの大学においてカードベース暗号を教材として用いた事例がある. カードベース暗号プロトコルの操作の中で最も重要なものがシャッフルである. シャッフルとは, ある確率分布に従って置換を選択し, その置換に従ってカード列を並び替える操作であるが, カードベース暗号プロトコルではこの確率的操作によってプロトコルの安全性を実現する. 多様なシャッフルの中でも特に基本的かつ重要なものに, ランダムカット, ランダム二等分割カット, パイルスクランブルシャッフルがある. 実際, 多くのカードベース暗号プロトコルはこれらの 3 種類のシャッフルを用いて実現されている. カードベース暗号では, シャッフル実行の実際のプロトコルや必要なカード枚数, シャッフル回数を抑える研究が専ら行われている.

２．研究の目的

先にも述べたように，代数の表現論の共通の目標は「代数の加群圏または導来圏の構造を理解すること」である．係数環が体である整環(=有限次元代数)の場合は有限生成加群圏の構造論を与えることが目標であり，係数環が完備離散付値環であるときは，加群圏すべてを理解することは困難であるため加群圏の充満部分圏である格子圏を考察することになる．この目標を達成するための流れとして，おおきく 2 つの考え方がある．

(1)直既約加群の分類 加群を構成する最小単位である直既約加群の分類は基本的な問題であり，現代の用語では，Auslander, Reiten によって導入された AR 箙とよばれる有向グラフを与えることになる．直既約加群が分類できる代数は原始的に限られているため，より一般な代数になるほど AR 箙の一部だけを決定することが表現論における現実の目標である．整環のなかで「孤立特異点」と呼ばれる場合(例えば係 数環が体の場合)には十分な発展があり AR 箙の計算例も多く与えられているが，非孤立特異点の場合の AR 箙の構造論はほとんど与えられていない．また，Heller 格子を切り口に，異なる次元をもつ係数環上の代数の間の AR 箙の間の関係を明確化することで，その構造論の解明にも大きな貢献をすることになる．そこで，研究目標として以下を挙げる．
【研究課題 1】 非孤立特異点である整環の AR 箙の構造論を組み合わせ論的に具体的に与えよ．また，Heller 格子を終域にもつ AR 列を係数拡大した完全列の性質を調べよ．

(2)部分圏の分類
現代では 「ねじれ部分圏」を分類する研究が広く展開されている．近年では足立，伊山，Reiten によって導入された「台τ傾加群」によって関手的有限なねじれ部分圏が分類されているので，ねじれ部分圏の分類には「台τ傾加群全体」がどのような構造をしているかを調べることに帰着されるといっていい．台τ傾加群には変異と呼ばれる，直既約因子を一つ取り替えて新しい台τ傾加群を作る圏論的操作があるが，このとき，「台τ傾加群が有限個しか存在しない」クラスは重要であり，この場合は「ねじれ部分圏」 は完全に分類される．そこで，2 つめの研究目標として以下を挙げる．
【研究課題 2】 与えられた代数やクラスにおける台τ傾加群の構造論や有限性を組み合わせ論的に具体的に与えよ．

カードベース暗号プロトコルは，入力情報を表すカード列に物理 的操作を施し，出力情報を表すカード列に変換するものである.物理的操作の中でも，安全性を達成するために最も重要な操作がシャッフルであり，これはある確率分布に従って置換を選択し，その置換に従ってカード列を並び替える操作である．代表的なシャッフルにランダムカット (RC)，ランダム二等分割カット (RBC)，パイルランダムカット(PRC)，パイルスクランブルシャッフル (PSS)がある．
一方で，シャッフルの中には実現方法が知られていないものも多く，シャッフルの実現方法を示すことは重要な研究課題である．特に，n 次対称群 Sn の部分群 G に対して，カード列に G の一様ランダムな元を作用させるようなシャッフル(一様閉シャッフル)は重要かつ比較的簡単なシャッフルであるが，このようなシャッフルでさえ実現することは決して自明ではない．そこで，当該分野におけるモチベーションは，基本的なシャッフルを用いて複雑な一様閉シャッフルを実現することである．
【研究課題 3】 群 G に対する一様閉シャッフルを実現するための枠組みを構築せよ．

３．研究の方法

【課題１について】
まず，Kronecker 代数の場合に，Heller 格子の決定及び，それを含む AR 箙の構造を完全に決定する．その際，Heller 格子を終域にもつ AR 列を剰余体まで係数拡大してその様子を観察する．その後，Kronecker 代数の Heller 格子をもつ AR 箙の構造論を完全に決定する． その際， Webb の手法を踏襲する． これは AR 列（より正確には安定 AR 箙の連結成分）上に劣加法関数を適切に定義できるか，という問題に帰着する方法である．ここで問題となるのは，連結成分が AR 転移τで非周期ならば， 先行研究で用いていた「連結成分のτ軌道上にある格子の階数の平均をとる」関数を用いることが出来ない点である．そこで，本研究では「非射影直既約因子の数」という代表者が定義した新たな関数を用いることで Webb の手法を踏襲することを可能にした．
また， 河田氏が群環の場合に行った考察が対称整環のケースで適切に適用できないかを検証する．今回，先行研究で新たに整備した AR 列の計算手法を Ext 群の言葉で理解することで Heller 格子を終域にもつ AR 列を係数拡大したものが，AR 列と分裂完全列の直和となるかどうかの鍵を握っている．直既約加群が簡単に構成できる Brauer グラフ代数の場合に多くの計算を実行する

ことで，実例を多く生み出し，状況を整理することで研究を遂行する．

【課題 2 について】
Skowronski によって，様々なクラスの有限次元対称代数の表現型による森田同値類もしくは導来同値類による分類がまとめられている．そこで，対称代数に着目してτ傾有限性を調べることとする．τ傾有限（あるいは無限）であることを調べるには,イデアル商や冪等元によるカットを適切に取る他，対称代数の場合はそのカルタン行列に着目し，それの導来同値類すべてのカルタン行列の成分を持ってきたときに，それに上限があれば有限であることを示すことができる．これが対称代数に着目する大きな理由である．
また，対称代数ではないクラスについては，有限表現型とτ傾有限が同値となるようなクラスとして「単連結代数」がある．従って，単連結代数のτ傾有限性を調べるには，表現型を調べればよいことになる．表現型を調べる方法は（決して簡単ではないが）τ傾有限であることを調べるより手法が多い．本研究ではこれを深化させることを目指す．単連結代数のテンソルは再び単連結代数となるため，表現型の決定がτ傾有限性の決定につながる．そこで，単連結代数のテンソル代数で有限表現型となるものを箙と関係式で表示するとどうなるかを与えることで完全な分類を与える．先行研究により，弱誠実なものに関しては箙と関係式が与えられているが，本研究では弱誠実であるかどうかに無関係に分類を与える．

【課題 3 について】
任意の有限群は，あるグラフの自己同型群として実現できる．従って，群シャッフルを与えるには，グラフの自己同型と関連付ければよいという発想は自然である．そこで，まずはグラフの自己同型群によるシャッフルを実現することとする．具体的には，グラフを任意に与えたときに，その頂点にカードを配置し，自己同型群から一様ランダムに自己同型射が選ばれた際，その射が引き起こす頂点間の置換でカードをシャッフルする，という動作を実行するプロトコルを作成する．ただし，本研究の目的は，シャッフルの実現に主眼をおいているため，このプロトコルの実現が容易である必要がある．
また，有限群のなかで最も単純なものは巡回群である.従って，まずは巡回群を実現するシャッフルを構成する必要がある．（もちろん，生成元を任意に与えたときにそのシャッフルが容易に実行できるかどうかはまた別の問題である．）巡回群をグラフの自己同型群として実現する方法は容易であるため，初めの問題が解決できれば，巡回群を与えるシャッフルは構成できたことになる．
一方，有限群論により散在型単純群の分類を実行する中で，有限群を部分群の列に分解するという研究がなされてきた．もし，有限群が（一様に）部分群の列に分解できれば，その有限群を実現するシャッフルを実行するには，分解した部分群のシャッフルの連続適用で与えられることとなる．そこで，もし有限群を巡回部分群に一様に分解することができれば，グラフを利用したシャッフルを有限回実行することで全体のシャッフルを実現することになる．
そのような枠組みを定式化する．

４．研究成果

【課題 1 について】
Kronecker 代数の場合に完全に問題を解決することができた．また，多くの対称代数の AR 箙の構造に制約を与えることができた．Heller 格子との関係は．河田氏の手法をそのまま踏襲することで Heller 格子が直既約になるような対象整環では，Heller 格子を終域にもつ AR 列を係数拡大すれば AR 列と分裂完全列の直和に分けることができることを確認した．

【課題 2 について】
単連結代数のテンソル代数の場合には完全な分類を与えることに成功した．また，対称代数の場合には，多項式増大型の対称代数が傾離散であり，導来同値によってτ傾有限性が保存されることを示した．

【課題 3 について】
グラフの自己同型群シャッフルをパイルスクランブルシャッフルのみを用いて実現する手法を与えた．これにより，巡回群のシャッフルも実現できたことになる．より一般にハイパーグラフによるシャッフルも実現することに成功している．
更に，有限群の一様巡回群分解という概念を導入し，「任意の有限群が一様巡回群分解をもつ」ことと「任意の散在型単純群が一様巡回群分解をもつ」ことが同値であることを証明した．

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　6件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 MIMURA Ren、MIYAMOTO Kengo、FUJIYOSHI Akio	４．巻 E107.D
２．論文標題 Graph Linear Notations with Regular Expressions	５．発行年 2024年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 312～319
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2023FCP0006	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kanai Kazuki、Miyamoto Kengo、Nuida Koji、Shinagawa Kazumasa	４．巻 52
２．論文標題 Uniform cyclic group factorizations of finite groups	５．発行年 2023年
３．雑誌名 Communications in Algebra	６．最初と最後の頁 2174～2184
掲載論文のDOI（デジタルオブジェクト識別子） 10.1080/00927872.2023.2285908	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 宮部 恭平, 宮本 賢伍, 藤芳 明生	４．巻 J106-D(09)
２．論文標題 文字列シーケンス最短マッチング問題	５．発行年 2023年
３．雑誌名 電子情報通信学会	６．最初と最後の頁 435〜444
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Miyamoto Kengo	４．巻 227
２．論文標題 On periodic stable Auslander-Reiten components containing Heller lattices over the symmetric Kronecker algebra	５．発行年 2023年
３．雑誌名 Journal of Pure and Applied Algebra	６．最初と最後の頁 107251～107251
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.jpaa.2022.107251	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 SHINAGAWA Kazumasa, MIYAMOTO Kengo	4．巻 E106.A
2．論文標題 Automorphism Shuffles for Graphs and Hypergraphs and Its Applications	5．発行年 2023年
3．雑誌名 IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences	6．最初と最後の頁 306～314
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transfun.2022CIP0020	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Miyamoto Kengo、Shinagawa Kazumasa	4．巻 -
2．論文標題 Graph Automorphism Shuffles from Pile-Scramble Shuffles	5．発行年 2022年
3．雑誌名 New Generation Computing	6．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00354-022-00164-4	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Aihara Takuma、Honma Takahiro、Miyamoto Kengo、Wang Qi	4．巻 -
2．論文標題 Report on the finiteness of silting objects	5．発行年 2021年
3．雑誌名 Proceedings of the Edinburgh Mathematical Society	6．最初と最後の頁 1～17
掲載論文のDOI（デジタルオブジェクト識別子） 10.1017/s0013091521000109	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計16件（うち招待講演　0件／うち国際学会　1件）

1．発表者名 Kazumasa Shinagawa, Kazuki Kanai, Kengo Miyamoto, Koji Nuida
2．発表標題 How to Covertly and Uniformly Scramble the 15 Puzzle and Rubik's Cube
3．学会等名 12th International Conference on Fun with Algorithms（国際学会）
4．発表年 2023年～2024年

１．発表者名
金井和貴，宮本賢伍，縫田光司，品川和雅

２．発表標題
有限群の一様巡回群分解とそのカードベース暗号への応用

３．学会等名
日本数学会 2024年度年会

４．発表年
2023年～2024年

１．発表者名
品川 和雅，金井 和貴，宮本 賢伍，縫田 光司

２．発表標題
ルービックキューブを秘匿したまま一様ランダムにスクランブルする方法

３．学会等名
2024年 暗号と情報セキュリティシンポジウム（SCIS2024）

４．発表年
2023年～2024年

１．発表者名
宮本賢伍，品川和雅

２．発表標題
無向グラフとハイパーグラフに対するグラフシャッフルプロトコル

３．学会等名
2024年 暗号と情報セキュリティシンポジウム（SCIS2024）

４．発表年
2023年～2024年

１．発表者名
宮本賢伍

２．発表標題
Heller components of symmetric orders with finitely many Heller lattices

３．学会等名
第3回情報数理セミナー

４．発表年
2022年

１．発表者名
三村 廉，宮部 恭平，宮本 賢伍，藤芳 明生

２．発表標題
Graph Linear Notations with Regular Expressions

３．学会等名
数理解析研究所RIMS共同研究(公開型) 「計算機科学の基礎理論とその新潮流」 2022年度 冬のLAシンポジウム

４．発表年
2023年

１．発表者名
宮本 賢伍，王 起

２．発表標題
多項式増大型の対称代数のτ傾有限性

３．学会等名
2023年度 日本数学会 2023年度年会

４．発表年
2023年

１．発表者名
宮本賢伍

２．発表標題
On τ-tilting finiteness of symmetric algebras of polynomial growth

３．学会等名
第27回 代数学若手研究会

４．発表年
2023年

１．発表者名
Kengo Miyamoto

２．発表標題
On τ-tilting finiteness of some certain classes of finite dimensional algebras

３．学会等名
第2回情報数理セミナー

４．発表年
2022年

１．発表者名
宮部 恭平，三村 廉，宮本 賢伍，藤芳 明生

２．発表標題
文字列シーケンスの最短マッチング

３．学会等名
京都大学数理解析研究所RIMS共同研究（公開型） 「情報社会を支える計算機科学の基礎理論」 2021年度 冬のLAシンポジウム

４．発表年
2022年

１．発表者名
Kengo Miyamoto

２．発表標題
Cycle finite algebras with finitely many tau-tilting modules

３．学会等名
Examples of tau-tilting finiteness / infiniteness

４．発表年
2022年

１．発表者名
Kazuki Kanai, Kengo Miyamoto, Kazumasa Shinagawa

２．発表標題
有限群の一様分解とその一様閉シャッフルへの応用

３．学会等名
SCIS 暗号と情報セキュリティシンポジウム 2022

４．発表年
2022年

１．発表者名
Kengo Miyamoto, Kazumasa Shinagawa

２．発表標題
パイルスクランブルシャッフルからのグラフ自己同型シャッフルの構成

３．学会等名
SCIS 暗号と情報セキュリティシンポジウム 2022

４．発表年
2022年

１．発表者名
Kengo Miyamoto

２．発表標題
On τ-tilting finiteness of some certain classes of finite dimensional algebras

３．学会等名
第3回 西西セミナー

４．発表年
2021年

１．発表者名
Kengo Miyamoto

２．発表標題
Finite Heller components for symmetric orders over a complete discrete valuation ring

３．学会等名
情報数理セミナー

４．発表年
2021年

１．発表者名
Kengo Miyamoto, Qi Wang

２．発表標題
On τ-tilting finite tensor product algebras between simply connected algebras

３．学会等名
第53回 環論および表現論シンポジウム

４．発表年
2021年

〔図書〕 計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕 計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関