科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月 １３ 日現在

機関番号：１５２０１
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５４００１８

研究課題名（和文）組合せ半群論とその応用

研究課題名（英文）Combinatorial semigroup theory and its applications

研究代表者
庄司　邦孝（Shoji, Kunitaka）

島根大学・総合理工学研究科（研究院）・教授

研究者番号：５００９３６４６

交付決定額（研究期間全体）：（直接経費）　　1,700,000円、（間接経費）　　510,000円

研究成果の概要（和文）：科研課題「組合せ半群論とその応用」に７つの研究項目を掲げた。２３年度－２５年度の研究活動で，研究項目（１），（４），（７）に関しては，十分な成果が得らなかった。他の研究項目については，研究成果を２３年，２４年の国際会議と２４年，２５年と２６年の国内研究集会で発表した。また，２４年，２５年 RIMS kokyurokuに結果を掲載した。科研課題の研究項目(２)について，サザンプトン大 Renshaw 氏と共同研究を始めている。研究項目(３)について，カッセル大 Otto教授と共同研究を継続し，研究項目(５)について，ポルト大Almeida教授と共同研究をしている。

研究成果の概要（英文）：Our research entitled by "Combinatorial semigroup theory and its applications" financially supported by Grant-in-Aid for Scientific Research has been done from 2012 through 2014. We established 7 items of research bjects in the scientific reserach. Concerned with items (1),(4)and(7), there were unsatisfactory results only. The results on the other items than(1),(4)and(7), were announced at 2012, 2013, 2014 international or domestic conferences and published in the journal "RIMS Kokyuroku", 2013, 2014. We continue three joint research works, with Dr. Renshaw (Univ. of Southampton) on item (2), with Prof. Otto (Univ. of Kassel) on item (3), with Prof. Almeida (Univ. of Porto) on item(5).

研究分野：数物系科学

科研費の分科・細目：数学　代数学

キーワード：半群　有限表示　語の問題　アルゴリズム

１．研究開始当初の背景

(1)　群の Burnside 問題の研究の発展させたロシア学派は組合せ半群論を構築した。特に，one-relator 半群の word problem 解法の Adyan アルゴリズムは有用である。一方，rewriting system 理論を用いて，有限表示をもつ半群及び群の word problem を解く研究は Thomas，Otto，Howie，pride，小林，などにより発展している。しかしながら，半群及び群に対する word problem は one-relator 半群の問題をはじめ，依然未解決である。

(2)　２００６年と２００７年に開催して以来，同様な研究集会を毎年開き，本研究に関する研究発表と研究状況の把握に努めて，活発な討論を継続し，形式言語の専門家と形式言語とオートマタに関するアルゴリズム問題について情報交換をし，組合せ半群に関する重要な問題を得た。２０１１年 Lisbon 大学に於ける国際研究会で，本研究のテーマである組合せ半群に関する研究情報を講演・討論を通して得た。協力研究者を含む多くの国際的研究者から多くの情報を交換し，有限表示半群，アルゴリズム論の発展問題について，意見交換ができた。

２．研究の目的

(1)　数学の理論に現れる種々の群（位相空間の基本群，幾何的群，作用素環の群など）の解析・計算は組合せ群論の方法によっている。近年、コード理論，形式言語及び組合せ論を駆使して群の半群としての表現を研究することによって，群の解析・計算に大きな発展をもたらした。基本群の計算プログラム開発上誕生した Automatic 半群，Gromov による双曲群を一般化である word-hyperbolic 半群の研究が盛んに行われている。 この研究の具体的目標は群の解析・計算に関する問題を語の書き換え問題に帰着させ、解決するための基礎理論を開発することである。このような課題の研究は計算代数，アルゴリズム，暗号理論への寄与が期待され，急務である。
期間内の本研究目標を次に挙げる：

(1) 半群及び群に対する word problem に関する語の書き換えアルゴリズムを研究する。
(2) 半群の自由融合積を研究する。
(3) 有限表示半群の small cancellation theory を創る。
(4) 有限表示半群の co-word 問題を研究する。
(5) automatic 半群及び群を一般化する。
(6) word problem を解くためのアルゴリズム問題を暗号のセキリティ問題に応用する

II. 半群及び群に対する word problem の可解性は Turing machine を用いて定義された。しかし，計算プログラム開発と共に，word problem を解くアルゴリズムの複雑性を測るため形式言語と組合せ半群及び群の結び付ける研究が必要となった。本研究課題は形式言語を用いて半群及び群を研究するだけでなく。逆に，word problem を解くための，語の変換，語のコード化，語の rewriting system の手法の研究が形式言語の発展させることができる。さらに，word problem を解くアルゴリズムの複雑性を暗号のセキリティ問題に応用できる。本研究課題の数学と情報科学の境界領域を開拓することを目指している。

上に掲げた本研究目標の
第一目標を達成するためには rewriting system を整備し，overlappping する word の subword として出現する piece を分類することが課題である。実際，Ivanov，Margolis，Meakin 半群及び群に対する word problem は半群の small cancellation theory を用いて，one-relator 逆半群 の word problem は群の menbership problem と同値であることを示した。この成果は形式言語のコード理論は overlap している word の性質を利用して，有限表示半群の元の Cayley グラフを与えることで word problem を解くアルゴリズムの存在を示唆している。さらに，無限群論，幾何的群論の道具として応用されることが期待できる。また，代数計算のアルゴリズム問題を解決するために，半群論とオートマタ理論が発展を共有できる意味で意義がある。半群 の word problem を解くためには
第二目標である半群の自由融合積の研究が不可欠である。実際，one-relator group の word problem を解法は群の自由融合積上の word problem に置き換え，解かれている。one-relator semigroup の word problem を解くためには，融合基の研究成果を用いて半群の自由融合積の理論をつくる。第三目標について，small cancellation theory は 30 年前 Von Kampen に始められた方法で，有限表示半群及び群の word problem を解くための基本的道具である。今後，rewriting system 理論を絡ませ，発展させることが自然な研究方向であると確信している。第四目標について，申請者は有限階数の自由半群 X*から S 上への準同形写像 ϕ をもつ有限表示半群 S に対して，S の各元 s に対して，$\phi(w)=s$ を満たす w の集合が正則言語であるとき， S は剰余的有限であることを示した。これを発展させて $\phi(w)=s$ を満たす w の集合が context-free 言語である半群 S を研究し，vertually free 群の一般化を目指す。さらに，S の語の問題を解明する。第五目標について，位相空間の基本群の計算を目的とし、「automatic 群」の概念が文字の集

合 X とオートマトンで受理される自由半群 X^{*} の中で rational な形式言語をなす語で書かれる関係で定義された Automatic 群は重要な性質 fellow traveller をもつ。 性質 fellow traveller をもつ半群及び hyperbolic 半群を研究する予定である。第六目標では組合せ群論及び半群論の成果を暗号のセキュリティ問題に応用する。
以上の目標を達成することで，ロシア学派が構築した半群論と群論を統一的に扱う方法を発展させ，組合せ半群論を確立できる。さらに，暗号のセキュリティ問題に応用することで社会に貢献できる。

III. 群の Burnside 問題は組合せ半群の理論，リー代数の理論を構築しながら，ロシア学派 Novikov, Adian, Zemanov, Ivanov などによって，解決した。その過程で，
Adian (参照[1])は word problem の解くための"語のコード化", "語の変換アルゴリズム "など種々の方法を創出し, 弟子と共同研究で word problem に関する多くの成果を上げた。実際，piece(２つの語の overlapping している部分)をコード化し，書き換えを行い，ある条件下で，word problem が可解か，否かを判定してきた。この研究成果は莫大なものである。彼らの成果の検証は不可欠であり，申請者は既に検証を始めている。特に，Water(参照[2]) による one-relator が２つの word の長さの一方が他方の２乗より小さいときの one-relator 半群の word problem 解法の Adyan アルゴリズムを解析した。一方，rewriting system 理論を用いて，有限表示をもつ半群及び群の word problem を解く研究は Thomas, Otto，Howie，pride，小林，などにより，研究成果が上がっている。しかしながら，半群及び群に対する word problem は one-relator 半群の問題をはじめ，依然未解決である。一方，幾何的群論の研究は活発で，その成果は組合せ群論及び組合せ半群論を発展を促進している。実際，Gromov は双曲群を Cayley グラフ上の語の距離を用いて定義し，その性質を明らかにしたが，Gilman は，形式言語を用いて word-hyperbolic 半群を定義し，問題を提起している。一方，automatic 群は 幾何学者の Thurston，Epstein，が位相空間の基本群を計算するプログラムを開発する中で，発見された概念であり，automatic 性は combing 性, quasi-convex 性 などに拡張され，発展している。Burside 問題を研究した Olshanski(参照[5])，Ivanov は群の一般 small cancellation theory を巧みに用いて，Burnside 群，有限表示をもつ群に関する結果を次々と発表し，群の一般 small cancellation theory を重要性を示した。最近，McCammond は Burnside 半群の一般 small cancellation theory を開発し，顕著な結果を得た。さらに，McCammond はカテゴリー CAT(0) を用いて無限群論の代数的側面と幾何的側面を融合させながら組合せ半群論を構築した。また，Shpilrain は組合せ群論及び半群論の成果を暗号のセキリティ問題に応用した。

(2) 本研究は，半群及び群の有限表示から代数構造を組合せ的方法で，代数的側面と幾何的側面を結び付け，総合的な研究を目指すものである。

３．研究の方法

本研究を効果的に進めるため，以下の研究項目を設定した。

(1) word problem の解法のため small cancellation theory を開発する。半群の word problem を解法のために，piece (relator である２つの word u，v の overlapping している部分) を分類し，piece の集合がコード化できる relator を分類する。この成果を small cancellation theory の構築に生かす。この際，Burnside 半群の McCammond の一般 small cancellation theory と比較検討する。

(2) 半群，群の融合問題に対する解法アルゴリズムを開発する。基本群など，有限表示をもつ群の研究成果は，ほとんど，自由融合積で表せる群に限られると言っても過言ではない。半群及び群の自由融合積に関する研究と共に自由融合積の幾何的な側面を研究をする。

(3) 組合せ半群論の問題を rewriting system 理論の立場から考察する。Book, Otto の著書「rewriting systems」に見られるように, 半群の word problem の判定方法を rewriting system を用いて述べることができる。しかし，relator をなす word のタイプを分類し，より効果的な書き換えができるように，コード理論を利用して，アルゴリズムの作成を実践する。

(4) 有限表示半群 S の relator に現れる word が n より少ない個数の piece の積にならないとき, S は条件 C(n) を満たすという。 条件 C(3) を満たす有限表示半群の word problem は解けることが知られている。条件 C(2) を満たす有限表示半群に対して，relator に現れる word と piece の長さの比を制限する条件 T(q) と word problem の可解性との関連を調べる。 さらに，有限表示半群に対する Cayley 複体に McCammond による 一般化された relator の概念を用いて，幾何的考察を試みる。

(5) 有限生成自由半群 X* から S 上への準同形写像 ϕ をもつ有限表示半群 S に対し

て， $\phi^{-1}(s)$ $(s \in S)$が正則言語であるとき，S は剰余的有限であることを示した。各 $\phi^{-1}(s)$ $(s \in S)$ が context-free 言語となる研究をする。

(6) オートマタによる半群，群の表現を研究する。automatic 群の本質的な性質 fellow traveller property は有限表示をもつ群の生成元%と部分群に関する Tod-Coxceter の方法と Cayley グラフのオートマタによる表現と見なせる。組合せ半群の代数的方法と Cayley グラフの幾何的な性質を調しらべる。

(7) 有限表示半群の Dehn 関数，growth 関数の評価を試みる。word problem のアルゴリズム問題の成果を暗号のセキリティ問題に応用する。

以上の研究計画が進まない場合の対策とより発展した成果を得るための手段として，
国内研究者 山村(秋田大学)，海外研究者 Almeida (Porto 大), Meakin(Nebraska 大), Margolis(Bar-Ilan 大)，Otto(Kassel 大)，Thomas(Lancester),Renshaw(Southampto n 大)と研究打合せを随時行う。

４．研究成果
(1)有限表示半群 S の automaticity を調べ，有限生成自由可換半群 F から S 上への準同形写像 ϕ をもつとき， 条件 $\phi^{-1}(s)$ $(s \in S)$ を満たすとき，S は automatic 半群であるかという問題を論文に掲載した。

(2)有限生成自由半群 X* から S 上への準同形写像 ϕ をもつ one-relator 半群 S=<X/(u, v) > に対して， $\phi^{-1}(s)$ $(s \in S)$が有限集合であるとき，one-relator (u,v) をある条件の下で決定した。この結果を国際研究集会で発表した。

(3)自由 Burnside 半群 B(m,n)は n が３以上ならば各合同類が正則言語となる有限表示をもつ半群である。n=2 の場合，この結果は Brzozoski の問題と同値であることが分かった。自由 Burnside 半群 B(m,2)が各合同類が正則言語となる有限表示をもつかどうかは分かっていない。この結果を研究集会で発表した。

(4) 有限半群を core とする有限半群の自由融合積は常に存在するかどうかを判定するアルゴリズムが存在するかどうかという問題はオートマトンの k-extended word の集合が有界かどうかを判定する問題と同値であることが Otto 教授（Kassel 大）との共同研究で分かった。

(5)有限集合上全変換半群を core とする有限半群の自由融合積は常に存在することを示した。この結果を研究集会で発表した。論文を準備している。

(6)有限生成可換半群 S は有限生成自由可換半群 F から S 上への準同形写像 ϕ をもつ。このとき，$\phi^{-1}(s)$ $(s \in S)$が F の rational 集合であり，ϕを引き起こす合同関係は有限個の relator で表せることが Almeida 教授（Porto 大）との共同研究で分かった。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）
〔雑誌論文〕（計 ３件）
①Kunitaka Shoji, Semigroups presented By regular congruence classes, RIMS Kokyuroku, No.1873, 2014, 12-1

②Kunitaka Shoji, Semigroups presented By finite congruence classes, RIMS Kokyuroku, No.1809, 2012, 169-170

③ Kunitaka Shoji , Automaticity and presentations of semigroups, RIMS Kokyuroku, No.1769, 2011, 1-6

〔学会発表〕（計 ４件）
① 庄司 邦孝, Finite transformation semigroups and amalgamation bases for finite semigroups, 京都大学 数理解析研究所, 2 月 18 日, 2014

②庄司 邦孝, Semigroups presented by congruence classes of regular languages, 京都大学 数理解析研究所, 2 月 18 日, 2013

③Kunitaka Shoji, One relator semigroups presented by finite congruence classes, Uppsala Uiversity, September 1, 2012

④庄司 邦孝, Semigroups presented by finite congruence classes, 京都大学 数理解析研究所, 2 月 22 日, 2012

〔図書〕（計 ０件）

〔産業財産権〕
○出願状況（計 ０件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 ０件）

名称：
発明者：

権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
庄司　邦孝（SHOJI, Kunitaka）
島根大学・大学院総合理工学研究科・教授

研究者番号：50093646

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：