

科学研究費補助金研究成果報告書

平成23年 5月 17日現在

機関番号：11401

研究種目：基盤研究 (C)

研究期間：2008～2010

課題番号：20540055

研究課題名 (和文) 数学構造とアルゴリズム

研究課題名 (英文) Mathematical structures and algorithm

研究代表者

山村 明弘 (AKIHIRO YAMAMURA)

秋田大学・工学資源学研究科・教授

研究者番号：30358866

研究成果の概要 (和文) : 数学構造として、いくつかの代数系についてその構造を考察し、語の問題などのアルゴリズム問題について調べた。特に可換な逆半群の逆半群のクラスにおける融合積に関する語の問題について考察した。また、ある種の恒等式を満たす完全正則半群の代数構造を明確にした。特に完全単純半群の場合における Rees 行列半群に表現を決定した。このことから恒等式をみたす完全正則半群の variety について知見を得た。そして、群論における Krull-Schmidt 定理に相当する結果を orthocryptogroup に対して得た。また、立方体表面におけるラテン方陣のようなデザインを考察し、それを数独パズルに応用し、解法プログラム及び問題作成プログラムを構成した。

研究成果の概要 (英文) : We study the structures of some algebraic systems as mathematical structure and examine algorithmic problems such as the word problem. In particular, we study the word problem of amalgamated free products of commutative inverse semigroups in the class of inverse semigroups. In addition, we clarify the algebraic structure of completely regular semigroups satisfying a certain equation. In particular, we completely characterize Rees matrix semigroup representations of completely simple semigroups. Then we obtain some results on varieties of completely regular semigroups satisfying the equation. We also obtain a theorem for orthocryptogroups similar to the Krull-Schmidt theorem in group theory. On the other hand, we examine designs like Latin squares on the surface of squares and applied to construct a Sudoku-type puzzle.

交付決定額

(金額単位：円)

	直接経費	間接経費	合 計
2008年度	1,400,000	420,000	1,820,000
2009年度	500,000	150,000	650,000
2010年度	500,000	150,000	650,000
年度			
年度			
総 計	2,400,000	720,000	3,120,000

研究分野：代数学

科研費の分科・細目：数学・代数学

キーワード：半群、アルゴリズム

1. 研究開始当初の背景

チャーチの提唱により、計算可能性の問題は計算機のモデル化には依存しないことが知られているが、具体的なアルゴリズム問題の計算量はデータ構造に依存するので、それを十分に把握する事は実現されていない。しかしアルゴリズムに関する効率性の問題は実用の観点からも重要な課題である。数学構造上のアルゴリズムを現実的な問題に適用する際には、プログラムとして具現化される。

一般的に、プログラム＝データ構造＋アルゴリズムと考えることが多い。数学構造に関連するアルゴリズムには理論的な興味とともに、実システムへの応用も多い。例えば、セキュリティの要素技術である暗号については、数学構造にその安全性が依存しており、アルゴリズムの性質（計算量、メモリ量）を理解する事はセキュリティシステムにおいて重要である。したがって、数学構造のアルゴリズムと暗号理論との関連性を調べる事は理論的な興味だけでなく、数学構造の研究を実社会に応用していく点においても重要であった。

無限群のアルゴリズム問題として、語の問題が重要である。群表示におけるアルゴリズム問題としては Novikov と Boone による群の語の問題の否定的解決により、一般的には語の問題を解くアルゴリズムは存在しないことが知られている。一方で表示された群が特別な性質、特に幾何学的構造を持つような特殊な場合には効率的なアルゴリズムが存在する。M.Gromov が導入した語双曲幾何的な群については 1 次の多項式時間のアルゴリズムが、Epstein 等が導入したオートマテ

ィック構造を持つ群には 2 次の多項式時間のアルゴリズムが存在する。

これらの例からも示唆されるように幾何学的な性質はアルゴリズムにおける探索空間を縮小させることにより効率を高めることに役立つ。このことから、群と半群における幾何学的性質（語双曲幾何性やオートマティック性）とアルゴリズムの関連性を調べることは極めて重要な研究課題となっており、国内外で活発に研究が進んでいる。また、群の自然な拡張である逆半群についてのアルゴリズムに関して今までに研究がそれほどなされていない。また、群の自然な拡張である逆半群の語の問題は一般的には非決定的であるが、群論において決定的なアルゴリズムが存在する問題についても、逆半群では非決定になることも多い。例えば、有限群の融合積の語の問題は決定的であるが、逆半群では非決定的である。このように群と逆半群ではアルゴリズム問題において異なる様相を呈しており、逆半群におけるアルゴリズム問題については未解決問題が多く残されていた。

2. 研究の目的

数学構造（群、半群）の理論的研究と、アルゴリズムに影響を与える数学構造とその表現手法について研究する。具体的には群、半群の数学構造に関する構造論とそのアルゴリズムにおける未解決問題を解決することを目的とする。また、数学構造とそのアルゴリズムを応用することも目的の一つとした。そして、最終的には数学構造におけるアルゴリズムに関する統一的な知見を得る事を目

標にした。

数学構造のアルゴリズム問題（語の問題、メンバーシップ問題）として、逆半群の融合積に関する語の問題を否定的に解決（アルゴリズムの非存在性）すること、無限群における幾何学的性質（オートマティック性、語双曲幾何性）と（逆半群による）偏作用の性質を明らかにすること、数学構造に関するアルゴリズムを暗号理論に応用することを目的とした。

これらの目的は、以下のようにまとめることが出来る。

1) 逆半群に関するアルゴリズム問題

2) 無限群における幾何学的性質

3) 数学構造に関するアルゴリズムの暗号理論への応用

3. 研究の方法

逆半群や正則半群の構造は半束、帯、極大部分群、合同類分割などにより明確にされ、逆に、半束、帯、極大部分群、合同類を利用した表現を利用してその構造を記述することが出来る。したがって、正則半群に関する表現と構成理論を利用してデータ構造としての代数系を調査する。そこで得た数学構造を応用する。

4. 研究成果

完全正則半群に関するアルゴリズム問題を考察するため、その構造を研究した。特に恒等式 $((xy)^{-1} = xx^{-1}y^{-1}x^{-1}yy^{-1})$ 及びそれに近い恒等式を満たす完全正則半群についてその構造を明らかにした。まず、この恒等式を満たす完全単純半群の Rees 行列半群表現を完全に決定した。この恒等式を満たす Rees 行列半群のサンドイッチ行列の各成分は、基

礎群の中心に含まれる位数 3 の元でなければならないことが分かった。このことから、この恒等式を満たす完全正則半群の完全単純クラスが決定することによりこれらの恒等式を満たす完全正則半群の variety を明確にした。

さらに normal な部分半群に関する有限性を満足する orthocryptogroup に関して、群論における Krull-Schmidt 定理のように、分解不能な部分半群のつむぎ積に一意的に分解できることを証明し、自明でない normal 部分半群のつむぎ積として定義される completely reducible orthocryptogroup の同値な条件を与えた。これらの結果を論文誌に投稿中である。

一方で、逆半群の融合積の語の問題について研究を進めていたが、まだ解決には至っていない。可換な逆半群（そして Clifford 半群）の（逆半群のクラス内での）融合積の語の問題は肯定的に解決できることが分かっているので、これについて厳密な証明を与える研究を続行しており、近いうちに論文にまとめ投稿する予定である。

また、数学構造とそのアルゴリズムの応用として当初は暗号技術への応用を計画していたが、立方体表面におけるデザイン構造を考察し、それを数独パズル、および、関連する組み合わせパズルに応用した。数独パズルについては解法プログラム及び問題作成プログラムを構成し特許出願を行っている。また、立方体表面上のデザイン構造として、ラテン方陣の一般化が存在するための必要十分条件を明らかにした。これは、上記の立方体表面上の数独パズルの構成に応用できる。

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 0 件)

〔学会発表〕(計 4 件)

- ① 山村明弘, Completely regular semigroups satisfying formula for inverse of a product, 2011/2/21, 計算と言語のアルゴリズムと計算理論, 京都大学数理解析研究所, (京都)
- ② 山村明弘, HNN extensions of inverse semigroups (招待講演), 2009/10/23, Algebra and Logic Related to Computer Science, 京都大学数理解析研究所, (京都)
- ③ Akihiro Yamamura, Word problem of amalgamated free products of commutative inverse semigroups, 2009/8/20, Novi Sad Algebraic Conference, Novi Sad, (Serbia)
- ④ Akihiro Yamamura, Automata theoretic methods in inverse semigroups (招待講演), 2008/11/20, Politecnico di Milano, (Italy)

〔図書〕(計 0 件)

〔産業財産権〕

○出願状況 (計 1 件)

名称: ゲームプログラム及びパズル
発明者: 山村明弘、佐々木悠
権利者: 秋田大学

種類: 特許

番号: 特願 2 0 1 0 - 0 2 4 0 4

出願年月日: H22 年 2 月 1 日

国内外の別: 国内

〔その他〕

ホームページ等

6. 研究組織

(1) 研究代表者

山村 明弘 (AKIHIRO YAMAMURA)
秋田大学・工学資源学研究科・教授
研究者番号: 30358866

(2) 研究分担者

()

研究者番号:

(3) 連携研究者

()

研究者番号: