様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ４ 日現在

機関番号：１７１０２
研究種目：挑戦的萌芽研究
研究期間：2013～2014
課題番号：２５６１００３４

研究課題名（和文）離散構造体の計算理論に関する形式的証明と自動検証

研究課題名（英文）Toward a formal proofs and automated verifications of discrete mathematics

研究代表者
溝口　佳寛（Mizoguchi, Yoshihiro）

九州大学・マス・フォア・インダストリ研究所・准教授

研究者番号：８０２０９７８３

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）：組合せ数学，論理と計算に関するセミナー等を中心に離散構造体に関する数学の形式化として，有限オートマトン，スティッカー系，ファジー・データベースの定式化を行った．研究集会「高信頼な理論と実装のための定理証明および定理証明器」では数学，計算機科学，産業界の各方面から，国内外合わせて約80名の参加者が集い，形式証明に関する結果の理解と今後の展開への道筋を共有することが出来た．また，同時期に公開された400年来の難問であったケプラー予想の形式証明については，解説記事を速報すると同時に，数学教育現場に携わる先生方等への今後の数学の形式化についての傾向と展開について広報した．

研究成果の概要（英文）：Our main results include a formalization of finite automata, sticker system and Fuzzy database as a formal specification of mathematics of discrete objects. A successful international workshop about "Theorem proving and provers for reliable theory and implementations" were held with over 80 participants including engineers in companies and researchers of computer science and mathematics. The famous unsolved problem for more than 400 years ago, Kepler conjecture was solved by Thomas Hales using formalized proofs last year. We publicized their result with introductions. Further, we appealed the importance and future view of the formalization of mathematics especially to students and teachers who are going to study mathematics in future.

研究分野：理論計算機科学

キーワード：数理論理学　数学の形式化　検証可能証明　ソフトウェア検証　離散数学　計算理論

１．研究開始当初の背景

近年の計算機能力の向上と証明支援系ソフトウェアの発展により，プログラムの形式仕様記述とその検証においては，証明支援系を利用した自動検証が実用的にも利用されて来ていた．特に，証券取引，交通網，航空宇宙工学，マイクロプロセッサなどプログラムの誤りにより多大な損失が生じるシステムに形式手法は活用されていた．また，論理的・数学的な考察そのものにも計算機が利用され,数学理論の証明検証においての計算機の利用が課題となっていた．計算機を利用した証明で広く知られているものとして平面地図塗り分け問題である「四色問題」がある．1976 年に Appel と Haken らによって計算機を利用して解決された．しかし，その計算プログラムに誤りがないのかは簡単に人で検証できるものではなく，2004 年に Gonthier (INRIA,マイクロソフト研究所)は，定理証明支援系 Coq とその拡張 Ssreflect(Small Scale Reflection Extension)を用いて,プログラムと証明を計算機で検証可能な形で与えた．Coq はフランスの INRIA 研究所で開発された証明支援言語で，型付きラムダ計算言語の一種で，プログラムとその正当性を自動検証可能な形で記述するための言語である．実社会においては，例えば周辺機器との通信プロトコルの実装やハードウェア制御等のプログラムを誤りなく実現するために利用されていた．プログラムの自動検証支援系では，Coq 以外にも，Isabelle(英国,ケンブリッジ大学)や Agda(スウェーデン,Chalmers 工科大学)などが，また，数学定理の検証系では，Mizar(ポーランド，Bialystok 大学)などの開発が進められていた．そして，数学定理の検証可能証明(形式化)が注目されて来ており，2004 年の四色定理の後，2012 年に群論の奇数位数定理の検証可能証明が Gonthier らにより完成されていた．このような背景の中，離散数学における構成的な証明の形式化の重要性に着目し本研究を開始した．

２．研究の目的

本研究は離散構造体の変換による計算理論をグラフ変換，セルオートマトン，言語理論の一般化として定式化するものである．特に，関係計算を用いて形式的な自動検証可能な証明を与えながら理論を構築する．離散構造物の変換(変形)による計算理論の構築は，それそのものでも数学的対象として興味深いが，全く新しい仕組みの計算機の実現へのヒントを与える可能性もある．研究代表者の研究背景である「圏論」「関係計算理論」「オートマトン理論」を基盤に「グラフ」「セル」という離散構造体を利用した計算を一般化し離散構造体の変換による計算理論を形式的証明とともに研究対象として構築することを目的とした．

３．研究の方法と成果

(1) まず初めに，離散構造物の性質を構成的に証明することを意識しながら行った．

(1-1) グラフの隣接行列の固有値，ラプラシアン行列の固有値によるグラフのクラスと特徴付は，計算量は大きいものの全てのグラフに対して均一の単純な方法で計算出来るために，画像の分解，特徴抽出にも利用されている．一方で，第 2 固有値に対する固有ベクトルを用いるグラフ分割は，近似アルゴリズムであるにも関わらず，その近似精度に関する考察は殆ど行われていなかった．まず，グラフのクラスによる近似精度の考察を行い，グラフ分割が成立しないグラフのクラスを与えた．

(1-2) 近年，セルオートマトンはユークリッド平面の格子上だけではなく，双曲平面上の格子上で定義されたもの，有限生成群に対応するケーリーグラフ上で定義されたセルオートマトンなどが考察されている．それらのセルオートマトンの性質，例えば単射性の判定が決定可能であるかなどは，それぞれ個別に，また次元を考慮して考察されている．これらを群上のセルオートマトンとして一般化し群の性質とセルオートマトンの性質を対応づけ，異なる近傍に対する局所遷移関数で定義されたセルオートマトンであっても統一的に取り扱う方法を提案し，セルオートマトン間の結合演算を一般的に定義した．

(1-3) オートマトン理論の形式化はソフトウェア検証において基本的なツールであるばかりか，数学の形式化としては代数構造理論の形式化に繋がる最も基本的な対象である．特に形式化においては，基本的には記号計算による証明となるため，適切な記号体系による対象の表現が重要となる．圏論によるオートマトン理論の抽象化は，抽象一般理論としての側面だけでなく，検証可能な形式化のためにも重要であると考え，その理論の概要を論文にまとめ公表した．

(2) 次に証明支援系 Coq を用いた離散構造体の形式化，および，その性質の形式証明に着手した．

(2-1) 有限オートマトンと分子計算のモデルであるスティッカー系との同等性の証明について国際会議(CANDAR2013)，および，日本数学会において講演を行い研究成果を公表した．また，同時に同講演資料を九州大学レポジトリに公開し，数学理論の形式証明支援系の応用としてのソフトウェア検証技術との関連の広報も行った．

(3) 記号計算による形式証明のための数学理論として，関係計算理論の重要性に気がつき，当初の研究計画にあるグラフ理論の形式化よりも，それを含む関係計算理論の形式化の方を優先するべきと判断し，関係計算理論の形式化へ着手した．

(3-1) 関係計算理論の抽象化であるファジー関係計算を用いたデータベース理論の一般化，および，その制御理論への応用について成果を国際会議(SCIS2014)にて公表した．記号計算により定式化されたデータベースを用いた制御は，制御系への信頼性評価への応用可能性が評価された．

(4) 本萌芽研究においては，研究分野の個別の課題解決のみならず離散数学と理論計算機科学の合同研究集会による研究者間の交流と課題探求を目指した．
(4-1) 組合せ数学セミナーの継続(2013 年度 3 回,2014 年度 2 回)，
(4-2) 論理と計算セミナーの継続(2013 年度,2014 年度各 1 回)，
(4-3)博多ワークショップによる数学ソフトウェアのデモ発表(2013 年度,2014 年度各 1 回)
(4-4) 2014 年度 12 月には国際研究集会「高信頼な理論と実装のための定理証明および定理証明器」を開催した．国内外から 80 名弱の参加者が集まり，数学の形式証明とソフトウェア検証理論のそれぞれの研究の重要性ばかりか，その結びつきそのものの重要性を共有出来たことが大きな成果であった．

(5) 2014 年 8 月に 400 年来の未解決難問であったケプラー予想の形式証明が Thomas Hales らにより完成され公開された．その解説記事を速報すると同時に，数学教育現場に携わる先生方等への今後の数学の形式化についての傾向と展開について広報した．

本解説を数ヶ月で数学セミナー誌へ紹介出来たのも組合せ数学セミナーの継続と蓄積によるもので，それは最初から意図されていたものではなかった．このような予期せぬ結果を導けるインフラとしての研究環境を継続したい．

４．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 4 件）

① K.K.K.R. Perera, Y. Mizoguchi, Bipartition of graphs based on the normalized cut and spectral methods, Part I: Minimum normalized cut, Journal of Math-for-industory, Vol.5, 2013A-8, pp.59-72.
② S.Inokuchi, T.Ito, M.Fujio and Y. Mizoguchi, A formulation of Composition for Cellular Automata on Groups, IEICE Transactions on Information and Systems, Vol.E97-D,No.3,pp.448-454, 2014.
③ Y.Mizoguchi,Theory of Automata, Abstraction and Applications, Mathematis for Industry, Vol.5, pp.337-348, Springer, 2014.
④ Y.Ikeda, F.Fukai, Y.Mizoguchi, A Property of Random Walks on a Cycle Graph, Pacific Journal of Mathematics for Industry, 2015, to appear,

〔学会発表〕（計 8 件）

①Y. Mizoguchi, Mathematical Aspects of Interpolation Technique for Computer Graphics, PNU Mathematics Seminar, Pusan, Sourth Korea, 2013 年 4 月.
②溝口佳寛，数学にコンピュータを使う～数式処理系(Maxima),定理証明支援系(Coq)など～, 2013 年 4 月，第 6 回算数・数学教育研修会・九州数学教育会.
③H.Tanaka, I.Sakashita, S.Inokuchi and Y.Mizoguchi, Formal Proofs for Automata and Sticker Systems, Proc. of 1st International Workshop on Computing and Networking (CANDAR), 563-566, 2013, IEEE Xplore Digital Library, DOI:10.1109/CANDAR.2013.100.
④溝口佳寛,複素数・四元数と図形の回転, 2013 年 12 月，第 4 回算数･数学教育研修会･九州数学教育会.
⑤溝口佳寛,田中久治,坂下一生,井口修一, 有限オートマトンとスティッカー系に関する Coq による形式証明について, 日本数学会年会応用数学講演アブストラクト，pp.59-62，2014 年 3 月.
⑥M.D.Akbar, Y.Mizoguchi, Fuzzy Relational Database Model Using Relational Calculus, Proc. of 7th International Conference on Soft Computing and Intelligent Systems, 4pages, 2014.
⑦溝口佳寛，ケプラー予想の計算機による証明と検証について，2014 年 12 月，九州数学教育会第 4 回算数・数学教育研修会.
⑧溝口佳寛, Coq チュートリアル,ウィンタースクール「数学ソフトウェア・チュートリアル」，2015 年 2 月，九州大学.

〔その他〕
報告書:

①溝口佳寛，脇隼人，平坂貢，谷口哲至，島袋修，博多ワークショップ「組み合わせとその応用」報告書, COE Lceture Note, Vol.48, Kyushu University, 2013.
②Y.Mizoguchi, H.Waki, T.Shibuta, O.Shimabukuro, M.Tagami, H.Kurihara, S.Chiba, Hakata Workshop 2014, Discrete Mathematics and its Applications, MI Lceture Note, Vol.56, Kyushu University, 2014.
③溝口佳寛，J.Garrigue，萩原学，R.Affeldt,高信頼な理論と実装のための定理証明および定理証明器，MI Lecture Note, Vol.61, Kyushu University.

解説記事:
①溝口佳寛,田上真，ケプラー予想の計算機による証明と検証について,数学セミナー誌,2014 年 12 月号，pp.48-54.

ホームページ等
①組合せ数学セミナーHP
http://comb.math.kyushu-u.ac.jp
②論理と計算セミナーHP
http://sakura.imi.kyushu-u.ac.jp/wiki/index.php?Seminar
③研究集会「高信頼な理論と実装のための定理証明および定理証明器」HP
http://imi.kyushu-u.ac.jp/lasm/tpp2014/
④「有限オートマトンとスティッカー系に関する Coq による形式証明について」
http://catalog.lib.kyushu-u.ac.jp/recordID/1430787

６．研究組織
(1)研究代表者
溝口 佳寛（MIZOGUCHI, Yoshihiro）
研究者番号： 80209783