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 １３ 日現在

機関番号：１２５０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１１５４

研究課題名（和文）ベクトル加算系における到達可能性問題の決定可能性の形式化

研究課題名（英文）Formalization of the decidability of the reachability problem for vector addition systems

研究代表者

山本　光晴（Yamamoto, Mitsuharu）

千葉大学・大学院理学研究院・教授

研究者番号：００２９１２９５

交付決定額（研究期間全体）：（直接経費）　　1,900,000円

研究成果の概要（和文）：ベクトル加算系およびそれと等価な状態遷移系における到達可能性問題周辺のいくつかの問題について形式化を完成させた。具体的には、ペトリネットの有界性問題および停止性問題に関する形式化、状態付きベクトル加算系からベクトル加算系への到達可能性を保存する変換の形式化である。ベクトル加算系における到達可能性問題の決定可能性については形式化の完成を見なかったが、この問題に対する様々な証明手法を調査し、形式化に有望な手法に関する知見を得た。

研究成果の学術的意義や社会的意義
定理証明支援系を用いた形式化によって、機械的に検査された正しい証明が得られるだけでなく、一旦完了した証明に対する試行錯誤や適切な抽象化の検討がしやすくなる。本研究の成果の一部である状態付きベクトル加算系からベクトル加算系への変換の形式化においても、適切な抽象化を行うことで元の証明に用いられていた変換が改良された。
また、形式化の過程で構築・蓄積された技術やノウハウは、後に別の定理を形式的に証明する際の道具として生かされる。上記の変換の形式化においてもベクトルの回転に関するライブラリが整備された。

研究成果の概要（英文）：We have formalized several problems around reachability for vector addition systems or their equivalent state transition systems. Concretely, boundedness and termination for Petri nets, and reachability-preserving transformation from a vector addition system with states to a vector addition system are formalized. Although formalization of the decidability of the reachability problem for vector addition systems could not be completed, some insight into promising approach to formalization is obtained by investigating several methods for proving the decidability.

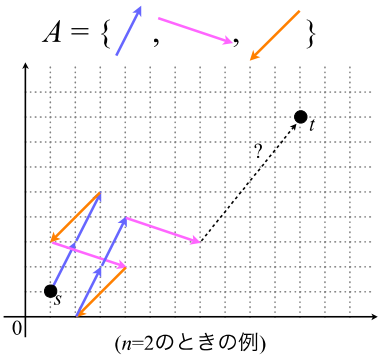
研究分野：情報数理学

キーワード：定理証明支援系　形式化　ベクトル加算系

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

(1) ベクトル加算系(VAS)とペトリネット、到達可能性問題



(*n*=2のときの例)

n を正整数とし、*A* を整数上の *n* 次元ベクトルを要素とする有限集合とする。いま、非負整数上の *n* 次元ベクトルによって位置を表すこととし、先の集合 *A* の要素をその変位ベクトルとして捕える。非負整数上の *n* 次元ベクトル *s* と *t* が与えられたとき、*s* に *A* の要素を重複を許して有限回加えていき、途中でどの成分も負になることなく *t* に辿り着くことが可能かを判定する問題を考える。
この問題はベクトル加算系(VAS, Vector Addition System)の到達可能性問題と呼ばれる。一見単純に思えるが、実は「途中でどの成分も負にならない」という条件がポイントとなっており、この条件によってある種の制御の表現が可能となって、かつ問題が複雑になる。実際に VAS は並行、化学、生物、ビジネスプロセスのモデル化に広範囲に用いられるペトリネットという系と等価であることが知られている。また、到達可能性問題は他の多くの問題がこの問題に帰着されるという点で、最も基本的かつ重要な問題となっている。
VAS の到達可能性問題が決定可能か、すなわち、プログラムで有限時間内に判定可能かどうかは暫く未解決であったが、1981 年に肯定的に解決された。その後も 1990 年初頭にかけてその証明が改良されていたが、それらは複雑な分解操作を伴うものであった。しかし、2011 年になってその複雑な分解操作を用いない形の新しい証明がなされ、その後さらにその証明の簡略化がなされた[1]。

(2) 定理証明支援系による形式化

定理証明支援系とは、命題とその証明の記述を人間が行うことを支援し、その証明が正しいことを検査する計算機上のシステムである。部分的に自動証明を行う機能を含むこともあるが、証明の大部分については人間が対話的に記述することを想定している。命題は計算機が理解できるような人工的・形式的言語で記述しなければならないが、それ故に自然言語にあるような曖昧さによる誤解が生じる余地がない。定理証明支援系自体は人間が作る計算機プログラムであるため、バグが入り込む余地はゼロではないが、通常は証明の正しさを検査する部分が(定理証明支援系の実装全体から比較すれば)小規模に実装され、検証された証明の正しさを保証する部分には極力バグが入らないように設計されている。
記号的に厳密に定義された形式的言語を用いて命題を記述し、やはり記号的に厳密に定義された論理体系のもとでその証明を行うことを形式化と呼ぶ。形式化された命題や証明のもとでは意味や直感は記号から切り離され、定理として認められるかどうかは厳密な記号操作のみによって定められる。ここでは本来の意味からするとやや狭い意味にはなるが、定理証明支援系を用いて、機械によって検査された証明を構成することを単に形式化と呼ぶことにする。
定理証明支援系技術の発展に伴い、最近では数百ページにも及ぶような数学の定理の証明を定理証明支援系を用いて形式化することも現実的になっている。著名な例として以下のものが挙げられる。

- 地図の塗り分けに関する 4 色定理の形式的証明[2]
- 群に関する奇数位数定理 (Feit-Thompson Theorem)[3]
- 3 次元球の充填問題に関するケプラー予想の証明[4]

２．研究の目的

本研究の目的は、ベクトル加算系における到達可能性問題の決定可能性を、定理証明支援系を用いて形式化することである。形式化の一般的な利点として、機械的に検査された正しい証明が得られる、一旦完了した証明に対する試行錯誤や適切な抽象化の検討がしやすい、正しさが保証されたプログラムが証明からのプログラム抽出によって得られる、といったものがあるが、それらにも増して、形式化の過程を通して以下に述べる「研究課題の核心をなす学術的『問い』」に答えたい。
本研究課題の核心をなす学術的「問い」は、上記研究開始当初の背景(1)で述べた「ベクトル加算系における到達可能性問題の決定可能性証明」を、上記研究開始当初の背景(2)で述べた「定理証明支援系で形式化」する際に、どのような数学的道具や抽象化、データ構造や定理証明支援系の機構が必要になるか、である。一般に、既に非形式的な証明が存在する場合でも、その証明を形式化するのは単に記号化する単純作業では全くない。例えば前述のケプラー予想の証明について言えば、査読者が「99%正しいと確信する」とした非形式的な証明について、その著者自身

が主導して形式化を完成させるのに 21 名の共同研究者と 11 年の歳月を要した(当初は 20 年かかると見積られていた)。
非形式的な証明において単に「明らか」「可能」と述べられている部分に関して、形式的な証明ではどう「明らか」か、具体的にどのようにすれば「可能」なのかについて明確に述べなければならない。形式的証明が不必要に複雑にならないように、「明らか」な部分は「明らか」に見えるように示すべきで、そのためには定理証明支援系の適切な支援が必要となり、場合によっては新たな機構を追加することとなる。どう「可能」なのかを具体的操作として示す際には、プログラムを記述することが多く、適切なデータ構造とその上の操作が必要となる。このような過程で構築・蓄積された技術やノウハウは、後に別の定理を形式的に証明する際の道具として生かされる。
ベクトル加算系やペトリネットにおける到達可能性問題の決定可能性は、他のシステムにおける様々な性質の決定可能性を帰着させる先としてよく使用される。この意味でも、本性質について形式的な証明が得られる意義は大きい。例えば文献[7]では、同一の挙動を示すモバイルデバイスの集合体として構成されるセンサーネットワークの形式的モデルであるポピュレーション・プロトコルについて、与えられたプロトコルがデバイスの集合体の任意の初期状況から始めて必ず合意に至る(well-specified)か、与えられたプロトコルが与えられた述語を計算するかという 2 種類の判定問題を、いずれもペトリネットの到達可能性問題に帰着させ、それらの決定可能性を示している。

３．研究の方法

本研究における形式化には、定理証明支援系として Coq[5]を、またその上の証明言語である SSReflect[6]と数学ライブラリ MathComp を用いる。これらは前述の 4 色問題の形式化の際に作られた道具やライブラリを整理して作成されたものであり、同じく前述の群の奇数位数定理の形式化の際にも用いられた。研究代表者自身の以前の研究でも使用している
研究体制は、研究代表者と、研究協力者としての研究室の大学院生で構成される。研究代表者と既存の非形式的証明を精査して形式化のための全体の設計を決め、自身も形式化を進める。適切なレベルの部分問題を大学院生自身に形式化してもらい、折に触れて浮かび上がった問題点について大学院生と議論する。この形式は我々の以前の研究であるペトリネットにおける被覆性問題の決定可能性の形式化でも採ったものである。

４．研究成果

(1) ペトリネットの有界性に関する性質の形式化

まず、ベクトル加算系と等価な状態遷移系であるペトリネットについて、我々の以前の研究である被覆性問題の決定可能性の形式化を拡張する形で、有界性に関する性質をいくつか形式化した。具体的には、有界性の複数の定義の間の同値性、有界性の決定可能性、有界であるときの到達可能性の決定可能性である。
初期マーキング付きペトリネットにおける有界性は、次のような同値な特徴付けが可能である。

- 初期マーキングから到達可能な任意のマーキングを上から押さえるマーキングが存在する
- 初期マーキングから到達可能な任意のマーキングにおける各プレースのトークン数を上から押さえる自然数が存在する
- 初期マーキングから到達可能なマーキング全体の集合が有限である

1 番目は有界であるという概念を直接的に表現したもの、2 番目はプレース有界性と呼ばれる、有界性を一般化した概念に拡張しやすいもの、3 番目はペトリネットに限らない、一般的な状態遷移系に関しても適用可能なものである。これらの特徴付けおよび実際に同値であることを定理証明支援系を用いて形式化した。
有界性の決定可能性は我々の以前の研究である被覆性問題の決定可能性の形式化と同様、Karp-Miller 木を構成し、その木の中に無限大を表すωが存在するかどうかで判定できることを形式化した。有界性判定の健全性証明に被覆性判定の完全性を用い、有界性判定の完全性証明に被覆性判定の健全性を用いるという関係になっている。なお、このときに用いた有界性の特徴付けは上記の 2 番目のもので、プレース有界性の判定もできるように一般化してある。
有界であるときに限定した場合の到達可能性の決定可能性は一般の場合と比較すれば非常に簡単な問題である。これは、研究協力者の大学院生に、形式化に使用している定理証明支援系 Coq および証明言語である SSReflect、数学ライブラリ MathComp に習熟してもらうことをねらいとしたものであったが、後に述べるように、一般の場合との関連があることが分かった。

(2) ペトリネットの停止性の決定可能性の形式化

次に、上記のペトリネットの有界性に関する各種性質の形式化を拡張する形で、停止性に関する性質をいくつか形式化した。具体的には、停止性を持つならば有界性も持つこと、停止性が決定可能であることである。
初期マーキング付きペトリネットが停止性を持つとは、その初期マーキングから始まる無限の遷移列が存在しない、すなわち、どのように遷移し続けたとしてもいずれ遷移できなくなることである。この停止性について、やはり被覆性問題の決定可能性の形式化の際に構築した Karp-Miller 木を構築し、その木の中にωも先祖に同じマーキングのある葉もないかをチェックすることで、判定が可能であることを形式化した。証明の方針は停止性を持つペトリネットが構成する可達木と、対応する Karp-Miller 木とが同型になることを示すというものである。前者は初期マーキングのみから構成されるのに対し、後者は履歴に関する情報が必要となるため、帰納法で証明する前に履歴に関する一般化が必要となった。

(3) 状態付きベクトル加算系からベクトル加算系への変換の形式化

上記のペトリネット以外にも、ベクトル加算系と等価な状態遷移系として状態付きベクトル加算系(VASS, Vector Addition System with States)が知られている。我々は、状態付きベクトル加算系の到達可能性問題を、状態なしのベクトル加算系の到達可能性問題に還元させる方法の形式化を完成させた。これにより、ベクトル加算系の到達可能性の決定可能性を、状態付きベクトル加算系にも適用させることが可能となる。
変換方法は VASS の初出論文[8]で述べられている手法に基づいている。到達可能性を保存する変換に求められる性質を抽象化することにより、もとの変換を改良したものを得ることに成功し、またそれが最良であることも形式化した。一般に形式化においては、元の証明の議論を一般化・抽象化することにより、形式化の労力が削減され、また元の問題へのより深い理解が得られる。本結果もそのような例となっている。

(4) ベクトル加算系の到達可能性証明に関する調査・検討

ベクトル加算系における到達可能性問題の決定可能性については形式化の完成を見なかったが、研究期間中にこの問題に対する様々な証明手法を調査し、形式化に適したものを検討して、いくつかの知見を得た。以下では 3 種類の証明手法について、形式化を目的とする観点で比較する。

① 到達可能・不能な場合のそれぞれに停止する半アルゴリズムを組み合わせる方法

この方法は文献[1]によるもので、到達可能な場合にのみ停止する半アルゴリズムと、到達不能な場合にのみ停止する半アルゴリズムとを並行実行し、一方が停止した時点で全体を停止させるものである。前者の半アルゴリズムは可達木を構築していくことで素朴に構成でき、後者は到達不能である場合にプレスバーガー算術式で表される不変条件が存在し、プレスバーガー算術式が列挙可能かつ不変条件であることが確認可能であることから構成できる。これは従来用いられてきた複雑な分解操作を用いない手法で、本研究課題の開始時点で形式化の対象として考えていたものである。
本研究で使用している定理証明支援系 Coq は直観主義論理を基盤としているため、排中律は一般には成立しない。このような環境で相補的な半アルゴリズムを並行実行した場合の全体の停止性を議論する方法を検討したが、適切な方法を見出すことができなかった。一旦この手法については中断し、他の方法を検討することとした。

② 有界なベクトル加算系の到達可能性問題に還元する方法

2020 年にオンラインで開催された国際会議 LICS/ICALP での Jérôme Leroux 氏による招待講演[9]において、一般のベクトル加算系の到達可能性問題が、有界なベクトル加算系の到達可能性問題に対数領域還元可能であるという内容が発表された。後者の有界な場合に限った決定可能性や判定アルゴリズムは、一般の場合と比較して格段に易しい。この還元は前年度に同氏らが LICS で発表した、VASS の到達可能性の計算量に関する論文[10]中の定理の応用となっている。
有界なベクトル加算系への還元によって決定可能性を示すという方法は、本研究課題の開始時点では知られていなかった新しい手法である。還元先である有界なベクトル加算系の到達可能性問題の決定可能性については、それと等価である有界なペトリネットに関して、上述の通り本研究課題で形式化を行っているため、その成果を利用できるのではないかと考えた。
手法を詳細に検討していくと、従来用いられてきた複雑な分解操作を基礎としていることが分かった。次の項目で述べる方法でもこの分解操作は用いられており、そちらの方がより直接的な

証明となるため、先に後者の方の形式化を進めることとした。有界なベクトル加算系の到達可能性問題への還元については、次の項目で述べる方法での分解操作の形式化が完成した後に、その成果を利用して計算量の議論や到達可能性の決定可能性の別証明として形式化する方が有効であると考えられる。

③ Kosaraju の到達可能性アルゴリズムの実装 KReach による方法

2020 年の国際会議 TACAS において、関数型プログラミング言語 Haskell 上に実装された、VASS の到達可能性検査プログラム Kreach が発表された[11]。これは 1982 年に発表された Kosaraju の到達可能性アルゴリズムの初の実装と考えられている。この方法は複雑な分解操作と伴うものではあるが、関数型プログラミング言語の上の実装が与えられたことで、これを参考にして、やはり関数型プログラミング言語を基盤としている証明検証系 Coq の上に実装することが本研究課題当初考えていたよりも現実的なものとなった。
KReach では分解操作の他に、部分問題として θ_1 と呼ばれる整数計画問題と、θ_2 と呼ばれる被覆性問題の解を用いている。後者の被覆性問題については我々の従来研究である Karp-Miller 木の形式化を利用できる。前者の整数計画問題については KReach では外部 SMT ソルバーに解かせているため、Coq 上での形式化においては独自の実装が必要である。まず整数解については、形式化に使用している数学ライブラリ MathComp にすでに存在している補題を拡張することで一般解を求めることが可能であり、実際に形式化してプルリクエスト[12]を提出している。θ_1 で求めるべきなのは実は整数解ではなく自然数解の一般解なのであるが、これについては整数解の一般解を変形して求められることが[13,14]によって主張されている。ただし、形式化を進めていく途中でこれの証明に誤りと思われるものが発見されたため、修正して形式化を進めている。自然数解の一般解を求める方法が形式化されれば、VAS の到達可能性問題だけでなく、それと密接に関連する半線形集合の理論の形式化にも貢献できることが期待される。

＜参考文献＞

[1] Jérôme Leroux. Vector Addition Systems Reachability Problem (A Simpler Solution). Proceedings of the Alan Turing Centenary Conference, volume 10 of EPiC Series, 214-228 (2012)
[2] Georges Gonthier. Formal proof - the four-color theorem. Notices of the American Mathematical Society, 55(11):1382-1393, 2008.
[3] Georges Gonthier *et al*. A machine-checked proof of the odd order theorem. ITP 2013, LNCS 7998, pages 163-179, 2013.
[4] Thomas C. Hales *et al*. A formal proof of the Kepler conjecture. Forum of Mathematics, Vol. 5, e2, 2017.
[5] The Coq development team. The Coq proof assistant reference manual. πr2 Project, 2017.
[6] Georges Gonthier, Assia Mahboubi, and Enrico Tassi. A small scale reflection extension for the Coq system. Technical Report 6455, Inria Saclay Ile de France, 2015.
[7] Javier Esparza, Pierre Ganty, Jérôme Leroux, Rupak Majumdar: Verification of population protocols. Acta Inf. 54(2): 191-215 (2017)
[8] John Hopcroft and Jean-Jacques Pansiot. On the reachability problem for 5-dimensional vector addition systems. Theoretical Computer Science, Vol. 8, No. 2, pp. 135-159, 1979.
[9] Jérôme Leroux. Invited Talk (LICS/ICALP). https://www.youtube.com/watch?v=4ZHJd2JXBS0, 2020.
[10] Jérôme Leroux and Sylvain Schmitz. Reachability in Vector Addition Systems is Primitive-Recursive in Fixed Dimension. LICS 2019: 1-13.
[11] Alex Dixon and Ranko Lazić. KReach: A Tool for Reachability in Petri Nets. TACAS (1) 2020: 405-412.
[12] Mitsuharu Yamamoto. Add solve_Qint_span to intdiv.v. https://github.com/math-comp/math-comp/pull/1191
[13] Marcus Kracht. A New Proof of a Theorem by Ginsburg and Spanier. manuscript, UCLA, December 2002 (published in The Mathematics of Language).
[14] Marcus Kracht. The Mathematics of Language. Studies in Generative Grammar No. 63, Mouton de Gruyter, Berlin, 2003.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計6件（うち招待講演　0件／うち国際学会　0件）

１．発表者名 脇坂 勝大，山本 光晴
２．発表標題 VASSからVASへの変換のMathCompによる形式化
３．学会等名 日本ソフトウェア科学会第40回大会
４．発表年 2023年

１．発表者名 脇坂 勝大，山本 光晴
２．発表標題 VASSからVASへの変換の形式化
３．学会等名 The 19th Theorem Proving and Provers meeting (TPP 2023)
４．発表年 2023年

１．発表者名 脇坂 勝大，山本 光晴
２．発表標題 Coq/SSReflect/MathCompを用いたVASSからVASへの変換の形式化
３．学会等名 第26回プログラミングおよびプログラミング言語ワークショップ（PPL 2024）
４．発表年 2024年

１．発表者名 稲垣 衛，山本 光晴
２．発表標題 ペトリネットにおける停止性判定の形式化
３．学会等名 The 15th Theorem Proving and Provers meeting (TPP 2019)
４．発表年 2019年

１．発表者名
稲垣 衛，山本 光晴

２．発表標題
ペトリネットにおける有界性判定の形式化

３．学会等名
The 14th Theorem Proving and Provers meeting (TPP 2018)

４．発表年
2018年

１．発表者名
稲垣 衛，山本 光晴

２．発表標題
ペトリネットにおける有界性に関する性質のCoq/SSReflectによる形式化

３．学会等名
第21回プログラミングおよびプログラミング言語ワークショップ (PPL 2019)

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

ペトリネット上のKarp-Miller木に関するCoq/SSReflectによる形式化のリポジトリ
https://bitbucket.org/mituharu/karpmiller

状態付きベクトル加算系からベクトル加算系への変換の形式化のリポジトリ
https://github.com/Wakisaka1205/VASS2VAS-2x

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