論文の内容の要旨

論文題目　Studies on Verification by Search
on Infinite Systems and Its Optimization

(無限状態システム上の探索による検証と
その最適化に関する研究)

氏名　　山本光晴

背景および全体の概要 (第１章)

グラフの探索問題は到達可能性、最短路問題、データフロー解析、有限状態オートマトンなど、様々な解析の基礎となっている。グラフの探索問題の実用的な応用として、モデル検査が挙げられる。これはシステムが仕様を満たしていることを検証する手法である。モデル検査は高度に自動化された手法で、早い段階で設計の誤りを検出できるなどの特徴を備えており、これまでハードウェア検証などの分野で成功をおさめてきた。

モデル検査をグラフの探索問題の応用として捕えると、いくつかの問題が浮かびあがってくる。まず、モデル検査は状態空間の網羅的探索を基本としているため、そのままでは無限の状態空間を扱うことができない。よって、無限の空間を有限に落とすための抽象化が必要である。また、有限の空間に制限したとしても、巨大な空間を網羅的に探索するのは現実的ではない。そのため、探索範囲を縮小するための最適化が必要である。最後に、モデル検査の検証結果をより信頼できるものにするために、上記の抽象化や最適化は何らかの手段で正当性が保証されているべきである。

本論文では、モデル検査をグラフの探索問題の応用として考えた場合の上記の問題点について論じる。すなわち、無限空間の抽象化および有限の範囲での最適化を、正当性を保証した上で行うことを目的とする。さらに、これをモデル検査以外のより広い範囲に適用することについても述べる。

モデル検査における無限の状態空間の抽象化は、抽象モデル検査として研究されてきた。これについて、抽象モデル検査アルゴリズムのあるクラスを含むようなアルゴリズムの定式化、および時間を含むシステムの解析の２点から考察する。１つ目については、到達可能性検査の拡張として抽象到達可能性検査アルゴリズムを定式化し、これが抽象モデル検査アルゴリズムのあるクラスを含むことを示す。また、抽象到達可能性検査が抽象モデル検査以外の具体的なアルゴリズムも含んでいることを示す。２つ目については、時間オートマトンと時間ペトリネットの拡張となる時間付き多重集合書き換え系を導入し、その性質について述べる。

有限の範囲での最適化については、最短路問題の最適化として知られる A* アルゴリズムを上記の抽象到達可能性検査に適用する。次にこれを無限状態システムの例である、時間を扱うシステムに応用する。抽象的なアルゴリズムの上で正当性を議論したり、最適化アルゴリズムを定義したりすることにより、様々な具体アルゴリズムに対する最適化および正当性証明を一様な方法で得ることが可能となる。実際に、実時間システムの代表例である時間オートマトンの拡張である線形プライス付き時間オートマトンの最小コスト問題に対し、上記の最適化を適用する。

正当性の保証は証明検証系を利用することによって行う。検証の対象となるアルゴリズムは抽象グラフ探索と呼ばれ、最短路問題やデータフロー解析などのグラフ上の問題を含んでいる。このアルゴリズムについて、実際に証明検証系 HOL の上で基本的な探索アルゴリズムおよび最適化アルゴリズムの検証を行う。この際、基本アルゴリズムと最適化アルゴリズムの検証を全く独立に行うのではなく、前者の検証に用いた証明を後者の検証に用いることが可能であることを示し、これを利用して労力の軽減を計る。

抽象グラフ探索アルゴリズムの形式化 (第 3 章)

到達可能性、最短路問題、データフロー解析、有限状態オートマトンなど、グラフ探索の種々の問題を包括する体系である抽象グラフ探索について述べ、その正当性の形式的証明を証明検証系 HOL を用いて行う。抽象グラフ探索は玉井による定式化をもとにしたものであり、グラフの辺に束上の単調関数が割り当てられたときに、グラフの点に対する束の要素の割り当てで、ある性質を満たすものを反復アルゴリズムによって求めるものであ

る。証明検証系上で検証を行うことにより、オリジナルの証明で暗黙のうちに置かれていた条件や、緩和しても証明が可能な条件を明確化する。さらに、抽象グラフ探索に対して最適化手法の一つである A* アルゴリズムを適用し、それについても証明検証系で形式的証明を行う。抽象グラフ探索に対する証明とその A* に対する証明は独立に行うのではなく、双方のアルゴリズムを結びつける定理を証明し、それを通して前者の証明を後者の証明に利用することによって、形式的証明の労力の軽減を計る。これは、基本アルゴリズムに関する証明から最適化アルゴリズムに関する証明を得る事例研究として位置付けられる。

抽象到達可能性 (第 4 章)

無限状態システムの検証に用いられる抽象モデル検査アルゴリズムのあるクラスを表現可能な抽象到達可能性検査を導入し、その正当性を証明する。抽象到達可能性検査アルゴリズムは Emerson らによって種々の抽象モデル検査アルゴリズムを表現するために導入された Covering Graph Construction をもとにしたもので、状態間に順序関係を持つようなラベル付き遷移系の上の反復アルゴリズムとして定義される。抽象到達可能性検査はいくつかのパラメータを含んでおり、これらを具体化することによって様々な具体アルゴリズムを得ることができる。実際に、前章の抽象グラフ探索が抽象到達可能性検査の具体化によって表現できることを示し、さらに抽象到達可能性検査に関する性質を利用して、抽象グラフ探索によって求められた解の正当性を示す。最後に、抽象到達可能性検査の上で A* の考え方を利用した抽象 A* アルゴリズムを定義し、その正当性を証明する。最適化アルゴリズムの定義やその正当性証明が抽象アルゴリズムのレベルで行われているため、様々な具体アルゴリズムの上でその A* 版とその正当性証明を統一的な方法で得ることが可能となる。

時間を扱うシステム (第 5 章)

無限状態システムの例として、時間を扱うシステムに関して述べる。時間を扱うシステムでは、一般に状態に時間を表す非負実数を含むため、状態空間が無限になってしまう。そのため、それらに関する解析には抽象化が不可欠である。

前半では、前章の抽象到達可能性検査およびその A* 版の具体的応用例として、線形プライス付き時間オートマトンの最小コスト問題の例を挙げる。線形プライス付き時間オートマトンは、時間オートマトンにおける離散的遷移と連続的遷移の両方にコストを割り当てたものである。連続的遷移の場合は経過時間に比例したコストがかかるため、「線形プ

ライス付き」と呼ばれる。この最小コスト問題はコスト付きリージョンやコスト付きゾーンの上の反復アルゴリズムによって解かれるが、この反復アルゴリズムは抽象到達可能性検査を具体化したもので表すことができる。さらに、A* を適用する場合に必要な補助的情報は通常の最短路問題で求めることができるため、線形プライス付き時間オートマトンの最小コスト問題についてその A* 版を考えることができる。この A* 版の正当性は、前章の抽象 A* アルゴリズムの正当性により自動的に得られる。

後半では時間を扱うシステムとして、多重集合書き換えに時間の概念を付加した時間付き多重集合書き換え系を導入する。有限集合 S に対し、

$$\{a_1{:}t_1, \ldots, a_n{:}t_n\} \quad a_i \in S,\ t_i \text{ は非負実数 } (i = 1, \ldots, n)$$

という形の有限多重集合を時間付き多重集合と呼ぶ。時間付き多重集合書き換え系は、以下のような書き換え規則

$$\begin{aligned} &a_1{:}s_1, \ldots, a_n{:}s_n \to b_1{:}t_1, \ldots, b_m{:}t_m \text{ if } \mathcal{C} \\ &\quad (a_i, b_j \in S,\ s_i, t_j \text{ は非負実数かクロック変数,} \\ &\quad \mathcal{C} \text{ はクロック変数と整数との比較からなる論理積)} \end{aligned}$$

の有限集合と不変制約の有限集合からなる書き換え系であり、書き換え規則による書き換えと、時間経過による書き換えの 2 種類の書き換えが行われる。これは時間オートマトンと時間ペトリネットという、2 種類のよく知られている時間を扱うシステムの拡張となっている。この時間付き多重集合書き換え系に対し、ペトリネットに関する性質から自然に導入される性質である、到達可能性、有界性、被覆性について、それぞれが決定可能であるかどうかを考察する。一般に、不変制約を含む場合はいずれも決定不能であり、このことは 2 カウンタ機械の停止性問題の決定不能性を利用して示す。一方、不変制約を含まない場合については、到達可能性は決定不能、有界性と被覆性は決定可能である。決定可能なものに関しては、時間オートマトンや時間ペトリネットの解析に用いられるリージョン、ゾーン、Karp-Miller 木などを組み合わせることによって、その解析方法を示す。さらに、対角線制約と呼ばれる制約を付加した場合、不変制約を含んでいても決定可能となるような部分クラスについて考察を行う。