科学研究費助成事業　　研究成果報告書

平成　２６　年　　４　月　２３　日現在

機関番号：　１３３０２
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５０００４１

研究課題名（和文）論理式肥大に伴う活性のモデル検査の非効率化の改善

研究課題名（英文）Improvement of liveness model checking performance degraded by obese formulas

研究代表者
緒方　和博（OGATA, KAZUHIRO）

北陸先端科学技術大学院大学・情報科学研究科・准教授

研究者番号：３０２７２９９１

交付決定額（研究期間全体）：（直接経費）　　3,900,000円、（間接経費）　　1,170,000円

研究成果の概要（和文）：公平性のもとでの活性のモデル検査対象の論理式は"公平性 ⇒ 活性"の形をとる。この論理式はBuchiオートマトンへ変換される。この変換は論理式の大きさに対しべき乗の計算と空間を必要とするため、公平性が大きくなるとBuchiオートマトンへの変換が実質不可能になり、モデル検査自体もできなくなる。本研究では、"公平性 ⇒ 準公平性"を満たし、公平性より小さな論理式である準公平性を探し、"準公平性 ⇒ 活性"をモデル検査することで公平性のもとでのモデル検査を可能とする方法を提案する。すなわち、"公平性 ⇒ 活性"の代わりに、"公平性 ⇒ 準公平性" と"準公平性 ⇒ 活性"をモデル検査することである。

研究成果の概要（英文）：Model checking a liveness property lprop under a fairness assumption fair, the formula is in the form "fair => lprop". The formula is transformed into a Buchi automaton. The transformation requires an exponential time and space of the size of the formula. If the formula becomes large, it becomes (almost) impossible to transform the formula into a Buchi automaton and then to model check the formula. The research proposes a way of making the model checking feasible by model checking "fair => qfair" and "qfair => lprop" for some formula qfair such that the size of qfair is (much) smaller than that of fair.

研究分野：　計算機科学

科研費の分科・細目：　ソフトウェア

キーワード：　モデル検査　活性　公平性　準公平性　分割統治　公平性の理解　反例　Maude

１．研究開始当初の背景

安心安全な計算機システム構築のための科学技術１つが形式手法である。形式手法を使いこなすには数学や論理学の素養を必要とし、一般の技術者にとっては敷居が高かった。その敷居を下げることに成功した技術革新は「モデル検査」である。

計算機システムの数学モデル(状態機械)を記述し､満たすべき要求(性質) を(時相)論理式で記述しさえすれば、モデル検査器は、計算機システムが性質を満たすか否かを自動で調べる。理論的には状態機械の状態数が有限であればモデル検査可能であるが、使用できるメモリ量や時間を考慮すると状態数は十分に小さくする必要がある。しかし、実用規模の計算機システム、特にソフトウェアに対応する状態機械の状態数は非常に大きく、典型的には無限である。このためモデル検査を効果的に利用できなくなるといった問題が起こる：「状態爆発問題」。この問題を回避するため状態機械の抽象化に関する研究が盛んに行われている。健全な抽象化により、状態数の多い(無限の)状態機械から､状態数の十分に小さい抽象状態機械を生成し、抽象状態機械に対しモデル検査を適用することで、元の状態機械がある性質を満たすことの検証を行える。

状態機械に加え、性質を記述する論理式もモデル検査の効率に大きく影響する。計算機システムの性質は大きく２種類に分類できる。「安全性」と「活性」である。安全性は、危険な状態には決して陥らないことを、活性は、目的は必ず達成できることを表すことができる。性質を安全性に限れば、十分に短い論理式で記述可能である。しかし、活性を扱うと長い論理式を記述する必要が出てくる。というのは、活性の検証には「公平性」を仮定する必要があるからである。

２．研究の目的

モデル検査の効率は状態機械と(性質を記述した)論理式の大きさに大きく依存する。前者による非効率化(状態爆発問題)は、状態機械の抽象化により解決の兆しが見え始めている。しかし、後者による非効率化はあまり注目されていない。安全性は活性より基本的かつ重要であることと、性質を安全性に限れば簡潔な論理式で表現可能であるためであると考えられる。しかし、活性を考慮すると、後者による非効率化は無視できなくなる。理由は公平性を論理式の一部に埋め込む必要があり、これによりモデル検査対象の論理式が肥大化するからである。本研究課題ではこの問題の解決方法を提案する。

３．研究の方法

モデル検査器として代数仕様言語 OBJ の流れをくむ Maude の LTL モデル検査器を用いる。Maude は、並行・分散システムの汎用の形式化のための論理的基礎である rewriting logic を背景に持ち、これまでに幾種もの並行・分散システムが記述された実績を持つ。また、OBJ の流れをくむため並行・分散システム内で使うリストや待ち行列等のデータ構造を素直に記述することもできる。このような表現力の豊かさに加え、Maude の LTL モデル検査器の性能（処理速度）は、モデル検査に特化して開発された Spin と同等であるとの報告もある。この表現力ならびに性能の高さが Maude の LTL モデル検査器を本研究課題で用いる理由である。

公平性により論理式が肥大化しモデル検査不能にあるいは効率良くモデル検査できなくなる活性を効率良くモデル検査するための方法を、具体的な事例をとおして、考案する。具体的な事例は、Suzuki-Kasami 分散相互排除プロトコル(SKDMEP)と通信プロトコル Alternating Bit Protocol (ABP)である。

SKDMEP は、ネットワークで接続されたノード間の相互排除のためのプロトコルである。ノードは共有メモリを有しておらず、情報のやり取りはメッセージの送受信のみで行われる。送受信される情報のひとつは privilege と呼ばれるものである。privilege はシステム内にひとつだけ存在し、あるノードに所有されているか、あるノードに送信中でネットワーク内にいるかのいずれかである。privilege を有しているノードのみ際どい領域に入ることを許される。privilege を有していないノードが際どい領域に入りたい場合、その他のノードに request メッセージを送信し、privilege メッセージが送られてくるまで際どい領域に入るのを待つ。privilege を有しているノードは、どのノードがどの順番で際どい領域に入るのを待っているかを保持する待ち行列を管理する。privilege を有するノードが際どい領域を出るときに、待ち行列を更新し、待ち行列の先頭のノードに、待ち行列の残りの情報を privilege メッセージとして送る。

ABP は、信頼性のないチャネルをとおして送信者ノードから受信者ノードにパケットを過不足なく送るためのプロトコルである。信頼性がないとは、チャネル内のデータは欠落するかもしれないし、複製されるかもしれないということである。ただし、順番が入れ替わることはないし、データの一部分のみ書き換わることはないとする。送信者はビット sbit と次に送信したいパケット pac を持ち、受信者はビット rbit を受信したパケットを格納するリスト buf を持つ。送信者から受信者に<sbit,pac>を送るチャネル(データチャネル)と、受信者から送信者に rbit を送るチャネル(アックチャネル)の２つを用いる。送

信者はデータチャネルに<sbit,pac>を繰返し入れ、受信者はアックチャネルに rbit を繰返し入れる。受信者がデータチャネルから<b,p>を取り出すと、b と rbit を比較し、p を buf に格納するか捨てるかを決める。格納する場合、rbit を反転する。送信者がアックチャネルから b を取り出すと、b と sbit を比較し、現時点の pac が受信者に届いたかどうかを判定する。届いたと判定した場合、sbit を反転するとともに pac を次のパケットに更新する。

４．研究成果

SKDMEP が満たすべき活性のひとつは無排斥性と呼ばれるもので、どのノードも際どい領域に入りたい場合必ず有限時間内に入ることができる、というものである。want(i)と crit(i)で、それぞれ、ノード i が際どい領域に入りたいことを表明する状態と際どい領域に入っている状態を表すとする。すると、ノード i に関する無排斥性 lofree(i)は、want(i) ↦ crit(i) (□(want(i) ⇒ ◇crit(i))と等価) で表現できる。lofree で、lofree(1) ∧ lofree(2) ∧ lofree(3)を表すとする。また fair でノード数 3 の場合の公平性(状態遷移に関する弱公平性)を表すとする。すると、モデル検査の対象となる論理式は fair ⇒ lofree となる。SKDMEP は、各ノードごとに 13 の状態遷移を持つ状態遷移機械としてモデル化する。公平性を表す論理式の大きさ(長さ)は状態遷移数に依存する。状態遷移 t の弱公平性は、(◇□enabled(t)) ⇒ (□◇applied(t))で表現される。ここで、enabled(t)は、t が実行可能であることを、applied(t)は、t が実行されたことを表す。fair は、このような論理式を 13 個連言(∧)でつないだ論理式であり、活性 lofree そのものより巨大である。このため、Buchi オートマトンへの変換に手間を要し、fair ⇒ lofree のモデル検査は数日経過しても終了しない。提案方法は、fait と lofree を取り持つ中間の qfair を探し、fair ⇒ lofree をモデル検査する代わりに、fair ⇒ qfair と qfair ⇒ lofree をモデル検査する。fair ⇒ qfair と qfair ⇒ lofree のモデル検査により反例が見つからない場合、fair ⇒ lofree のモデル検査でも反例は見つからないことになる。この事例では、fair ⇒ qfair と qfair ⇒ lofree のモデル検査は 2 分程度で終了し、反例はないとの結論を得ることができる。これにより、各状態遷移の弱公平性を仮定すると、ノード数 3 の場合、SKDMEP は無排斥性を満たすと結論づけることができる。数日経過しても終了しないモデル検査を 2 分程度で終了できるようになり、提案方法の有効性を示している。提案方法は、fair ⇒ lofree を fair ⇒ qfair と qfair ⇒ lofree に分割することでモデル検査を効率良く行うことができるようにするため、「分割統治法による活性のモデル検査法」と呼ぶ。

ABP が満たすべき活性のひとつは通信進捗性を呼ばれるもので j 番目のパケットは受信側に必ず有限時間内に到達する、というものである。これを pcp(j)で表現することにする。pcp(j)のモデル検査には、公平性 fair に加え、ある種の不公平性 afair も必要とする。afair には、データチャネルの組<b,p>は複製され続けることはないといったり、欠落され続けることはないといったりするものを含む。たとえば、j-1 番目のパケットを含む組がデータチャネル内で永遠に複製され続けるとすれば、j 番目のパケットが受信側に到達することがないからでる。各チャネルの容量を 5、送信するパケット数を 10 にすると、fair ∧ afair ⇒ pcp(10)のモデル検査には約 40 時間必要とする。一方、 分割統治法による活性のモデル検査法を用いると、モデル検査に必要となる時間は約 15 秒となる。本事例により、提案方法は、公平性のみならず不公平性も仮定する活性のモデル検査に対しても有効であることを示している。

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　3 件）

１．Kazuhiro Ogata and Min Zhang: A Divide & Conquer Approach to Model Checking of Liveness Properties, Proceedings of the 37th Annual International Computer Software & Applications Conference (37th COMPSAC), IEEE Computer Society Press, pp.648-657 (2013)(査読有).

２．Kazuhiro Ogata: Model Checking Liveness Properties under Fairness & Anti-fairness Assumptions, Proceedings of the 20th Asia-Pacific Software Engineering Conference (20th APSEC), IEEE, pp.565-570 (2013) (査読有).

３．Kazuhiro Ogata and Phan Thi Thanh Huyen: Specification and Model Checking of the Chandy and Lamport Distributed Snapshot Algorithm in Rewriting Logic, Proceedings of the 14th International Conference on Formal Engineering Methods (14th ICFEM), LNCS 7635, Springer, pp. 87-102 (2012) (査読有).

〔学会発表〕（計　0 件）

〔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
緒方　和博（OGATA KAZUHIRO）
北陸先端科学技術大学院大学
・情報科学研究科・准教授
研究者番号：30272991

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：