公開

研 究 終 了 報 告 書

「近似的数理モデルによる CPS の動的安全機構」

研究期間： 2020 年 11 月～2023 年 3 月
研 究 者： 和賀 正樹

1. 研究のねらい

近年、自動運転車やロボットを始めとする物理情報システム(CPS)の実用化が進んでいる。CPS では事故が人命に関わるなど重大な影響を及ぼす恐れがあるため、高い信頼性が要求される。そのため CPS の開発において、開発者の経験に強く依存する職人芸的なテストではなく、システマティックに品質を保証する、安全機構(Safe CPS)が重要である。

従来の Safe CPS は、形式検証に代表される Safe CPS 1.0 と、要求仕様の充足度合いを元にした探索的テストに代表される Safe CPS 2.0 に大別される。Safe CPS 1.0 は数学的証明によって安全性の明確な根拠（安心）を与えられる一方で、システムの厳密な挙動を数理モデルで記述する必要がある点に実用上の課題がある。また、Safe CPS 2.0 はモデル構築が不要で実用性が高い一方、安全性の明確な根拠を与えられない点に課題がある。

本研究では安全性の明確な根拠(安心)と実用的安全確保の両立に課題がある Safe CPS 1.0 と Safe CPS 2.0 の短所を補いつつ利点を享受する(Safe CPS 3.0)ことを目指す。Safe CPS 3.0 では、Safe CPS 1.0 における数理モデルの証明を近似数理モデルに適用しつつ、Safe CPS 2.0 におけるシステマティックな実動作の解析手法と融合させることで、安心と実用的安全の両立を図る。システムや外界の近似的数理モデルの構築は、人手で構築することも可能であるが、観測データを用いることで構築・精緻化することを主眼に置いている。

ACT-X の期間内では、Safe CPS 3.0 の中でも特にオートマトン学習による近似数理モデルの動的な生成と、モデル検査等の形式的な解析手法の組み合わせに主眼を置く。具体的には、研究提案時には以下の 3 つの研究項目を計画していた。

研究項目 1: オートマトン学習を用いた CPS の数理最適化による探索的テストの、連続的時間概念への拡張
研究項目 2: オートマトン学習を用いた、CPS の製品群に対する数理最適化による探索的テスト
研究項目 3: オートマトン学習を用いた、強化学習の実行時防護。

2. 研究成果

（1）概要

オートマトン学習を用いた探索的テストであるブラックボックス検査において、これまでシステムの挙動を近似するために Mealy 機械などの、時間を暗黙的かつ離散的に扱うオートマトンが用いられてきた。 研究項目 1 において、まず従来のオートマトンを連続時間概念に拡張した時間オ

ートマトンの収束保証付きの能動的な学習アルゴリズムの提案を行った。本手法について、理論の構築や証明・実装・実験評価を行い、形式検証に関するトップ国際会議 CAV 2023 に論文が採択された。

また時間オートマトンによって明示的に扱えるようになった時間の概念の他にも、物理的な位置のような連続的な状態やノイズ等による確率的なシステムの挙動も CPS のモデリングにおいて非常に重要であることが判明した。以上の調査・検討を踏まえ、CPS のブラックボックス検査に適した、ハイブリッドオートマトンの学習手法の構築及び確率的システムに対する確率的ブラックボックス検査の構築を行い、国際会議論文投稿に向けて論文執筆やより詳細な性能評価を行っている。

研究項目 2 においては、前述のブラックボックス検査を通して学習された近似オートマトンを、他の類似したシステムのテストに再利用することで、 CPS の製品群に対するブラックボックス検査を効率化する手法を構築した。本手法では、類似したシステムを近似するオートマトンから重要な入力を抽出し、これを再利用することで探索を効率化させる。本手法について複数ベンチマークを用いた予備実験の結果、入力列の抽出に用いたシステムとテスト対象のシステム間の類似度などに影響されるものの、探索的テストの効率化を行える場合があることが判明した。現在国際会議論文投稿に向けて、本手法のより詳細な評価や改良に取り組んでいる。

研究項目 3 において、ホワイトボックス的なアプローチによって強化学習の探索を安全にする手法である実行時防護を、オートマトン学習と組み合わせることでブラックボックスなシステムに対しても適用可能に拡張した。強化学習の適用対象となるシステムは多くの場合内部構造の不明なブラックボックスシステムだが、本手法によって実行時防護の適用範囲を広げることができた。

研究項目外の内容についても、例えば事前定義された近似数理モデルを用いた CPS の動的安全機構などにも取り組んだ。

（2）詳細

研究項目 1: オートマトン学習を用いた CPS の探索的テストの、連続的時間概念への拡張

オートマトン学習を用いた探索的テストであるブラックボックス検査において、これまでシステムの挙動を近似するために Mealy 機械などの、時間を暗黙的かつ離散的に扱うオートマトンが用いられてきた。 ブラックボックス検査を CPS へ適用する際には、時間及び入出力値を離散化する必要があり、システムの近似が非常に粗くなってしまうという問題がある。また、応答時間や収束時間などの時間に関係する性質をテストする際には、時間の概念を陽に扱う数理モデルを用いる必要がある。

研究項目 1 におけるねらいは、ブラックボックス検査において CPS の挙動をより忠実に近似できる数理モデルを用いることで、より幅広いシステムや仕様を扱えるようにする点にある。また、実システムと近い近似数理モデルを得られるため、探索的テストの精度向上も見込まれた。物理

情報システムにおいては特に応答時間や収束時間など、時間に関係する性質が重要となるため、従来のオートマトンを連続時間概念に拡張した「時間オートマトン」を用いたブラックボックス検査を構築することが当初の目標であった。

研究期間内に時間オートマトンの学習手法について調査・検討を行ったところ、従来の学習手法には収束性などの課題があることが判明した。本問題を回避しつつ幅広いクラスの時間オートマトンの学習すべく、決定的時間オートマトンに対して収束保証付きの能動的な学習アルゴリズムを構築した。本手法について、理論の構築や証明・実装・実験評価を行い、形式検証に関するトップ国際会議 CAV 2023 に論文が採択された。

また、各種 CPS について調査・検討をする上で、時間オートマトンによって明示的に扱うことのできるように拡張された「時間」の概念の他にも、物理的な位置のような「連続的な状態」やノイズ等による「確率的なシステムの振る舞い」も CPS のモデリングにおいて非常に重要であることが判明した。以上の調査・検討を踏まえ、 CPS のブラックボックス検査に適した、ハイブリッドオートマトンの学習手法の構築及び確率的システムに対する確率的ブラックボックス検査の提案を行った。これらの成果は現在予備実験を終え、国際会議論文投稿に向けて論文執筆や詳細な性能評価を行っている。

研究項目 2: オートマトン学習を用いた、CPS の製品群に対する探索的テスト

前述の通りブラックボックス検査においてはオートマトン学習とその形式検証を組み合わせることでシステムの探索的テストを行う。 研究項目 2 におけるねらいは、ブラックボックス検査において学習されたオートマトンを再利用することで、複数の類似した製品群のテストを効率化することすることにある。

本研究項目では類似したシステムを近似したオートマトンから抽出した入力列を用いることで、ブラックボックス検査における探索を効率化させる手法を提案した。本方式について複数ベンチマークを用いた予備実験の結果、探索的テストの効率化を行える場合があることが判明した。国際会議論文投稿に向けて本手法のより詳細な評価や改良を現在行っている。

研究項目 3: オートマトン学習を用いた、強化学習の実行時防護

システムモデルと形式検証を組み合わせた実行時防護を用いることで、強化学習を安全にすることができることが（Alshiekh et al., AAAI'18）にて示された。（Alshiekh et al., AAAI'18）の手法は強化学習の学習時に安全なアクションのみを探索できるようにする一方、システムモデルを要求するためブラックボックスシステムに適用できないという課題がある。研究項目 3 におけるねらいは、強化学習の実行時防護とオートマトン学習を組み合わせることで、実行時防護の適用範囲をブラックボックスシステムへ拡大することにある。

本研究項目の成果として、オートマトン学習を用いた強化学習の実行時防護手法である「動的実行時防護」を提案した。動的実行時防護の概要は以下のようである。

1. 強化学習の探索において観察される環境への入出力の関係を元に環境の様子を近似する Mealy 機械を随時学習する。
2. 近似して得られた Mealy 機械から実行時防護機構を構築する。
3. 強化学習の探索時に前述の実行時防護機構を用いる。

動的実行時防護を用いることで、強化学習の学習時に近似して得られた Mealy 機械において安全と見なされるアクションのみを探索することができる。これらのアクションは必ずしも安全とは限らないが、一度観測された危険なアクションは必ず防ぐことができ、危険な探索を減少させられることが期待できる。実際複数のベンチマークを用いて実験的に評価を行い、通常の強化学習と比べて危険な探索を大幅に減少させられることが判明した。本手法について、枠組みの提案・理論的な性質の証明・実装・実験評価を行い、形式検証に関する国際会議 ATVA 2022 に論文が採択され、発表を行った。

研究項目外の研究・取り組み

研究開始時点では明確に研究項目として盛り込んでいなかったが、ACT-X 期間中に以下のような近似数理モデルを用いた、CPS の動的安全機構に関する研究成果を挙げた。

本研究の目標とする近似数理モデルを用いた CPS の動的安全機構の応用範囲を広げるべく、事前定義された近似数理モデルを用いた CPS の動的安全機構にも取り組んだ。ソフトウェアを用いて CPS をモニタリングする際には、サンプリングにより時間・観測値の離散化が避けられないが、ネットワーク越しのモニタリングの場合には時間の離散化の間隔が長くなり離散化による影響を受けることが考えられる。本研究ではハイブリッドオートマトンとして与えられた近似数理モデルを用いて柔軟に観測値を補間するモニタリング手法を提案した。本研究成果は物理情報システムに関する主要国際会議 ICCPS'21 に採択され、発表を行った。また、本論文の拡張版が、ACM の論文誌 Transactions on Cyber-Physical Systems の Special Issues for Best Papers of ICCPS 2021 において採択・出版された。本研究成果は、オートマトン学習との組合せという観点では、例えば研究項目 1 で取り組んだハイブリッドオートマトンの学習手法と組み合わせることが期待される。

本研究課題で取り組むブラックボックス検査をより複雑で現実的なシステムに適用する際の効率化にも取り組んだ。ブラックボックス検査を複雑な CPS に適用する場合、システムの実行の所要時間が大きいことが考えられるため、システムの実行回数を減らす効率化を行った。より具体的には、オートマトン学習によって得られた Mealy 機械をテスト対象の仕様のみではなく、テスト対象の仕様を適切に強化した仕様に対してもモデル検査を適用することで、より効率的に近似 Mealy 機械を精緻化することに成功した。本研究成果は実行時検証に関する主要国際会議 RV'21 に採択され、発表を行った。また本研究成果を取り込んだ、ブラックボックス検査による CPS のテストツール FalCAuN を用いて、同様のツールのコンペティッションである ARCH-COMP の falsification track に 2021 年及び 2022 年に参加した。

3. 今後の展開

本研究の直近(2023 年度前半見込み)の展開は、研究期間内の未出版の成果を論文化及び出版し、プロトタイプツールを公開することである。特に時間オートマトンやハイブリッドオートマトンの学習は従来のオートマトンの学習と比べて難易度が大幅に高いことが研究コミュニティにおいて知られており、システム同定など本研究の目的であった Safe CPS 3.0 の幅を超えた後続研究も十分に期待できる。

本研究の短期的(1,2 年以内程度)な展開として、本研究の研究項目 1 の方向性をより押しすすめ、Safe CPS 3.0 において実際のシステムをより正確に近似できるオートマトンを用いることで実効性を高めることが挙げられる。また、2021 年と 2022 年に参加した ARCH-COMP における CPS の探索的テストツールの friendly competition に引き続き参加することで、実効性の向上を対外的にアピールする。また Safe CPS に関連する共同研究を通じて ACT-X 研究の成果を実用的に発展させ、実際の CPS 開発に用いることが本研究の中期的展開(5 年程度)として挙げられる。さらにこれらの成果を元により一般的に適用可能なツール展開を行うことも、より長期的な展開として挙げられる。

4. 自己評価

研究目的の達成状況

全体として研究目的を概ね達成したと評価する。本研究の研究の目的は「近似的オートマトンの学習と数学的証明による、CPS の探索的テストと実行時防護の実用的発展」であった。実行時防護について、研究項目 3 での成果である動的実行時防護によって、実行時防護をより現実的な問題設定においても適用可能にしたという点で、実用的に発展させたといえる。

CPS の探索的テストについて、前述の通り研究項目 1 では当初見込んでいた時間オートマトンを用いたブラックボックス検査の提案には至らなかった一方、確率的システムに対するブラックボックス検査の構築し実装・評価した。確率的な挙動も CPS において重要ではあるが従来のブラックボックス検査が対象としていなかった対象であり、CPS の探索的テストを実用的に発展させたといえる。また時間オートマトンについて、ブラックボックス検査より更に基礎的な課題であるオートマトン学習アルゴリズム自体に課題を発見し取り組んだという点で、より裾野の広い基盤技術に取り組んだと言える。

研究の進め方

研究実施体制について、研究統括の和賀に加えて大学院生 1 名がリサーチアシスタントとして、実験データの収集・解析や実験用プログラムの実装などを行う体制で研究を実施した。これは研究開始時の計画通りの研究実施体制である。

研究費執行状況について、総額としては概ね計画通りに研究費を執行した。人件費・謝金については、ほぼ当初の見込み通りの執行であった。一方新型コロナウイルスの感染拡大により、特に 2021 年度の旅費については当初の見込みより減少した。この減少分を主に計算機購入に当てることで、特に深層強化学習を用いる研究項目 3 の遂行などが円滑になった。

研究成果の科学技術及び社会・経済への波及効果

ACT-X における研究の成果は関連分野の研究者から注目・高評価を受けており、科学技術への波及効果は今後の見込みも含めて高いと評価する。例えば研究項目 3 で取り組んだ動的実行時防護については既に後続研究の論文がオーストリアのグラーツ工科大学のグループによって発表されており、今後も同様の学術的発展が見込まれる。また、研究項目 1 で取り組んだ時間オートマトンやハイブリッドオートマトンの学習アルゴリズムについて、出版前ではあるものの関連分野の研究者との informal な議論を通じて問題の難しさや重要性を再確認しており、これらの成果についても出版後に一定の学術的な注目を受け、学術的な波及を与えることが見込まれる。また、今後 ACT-X 研究の成果を実用的に発展させ、実際の CPS 開発に用いることで CPS の利用や開発をより安心・安全にすることで、より迅速な新技術の試行・実用を可能にするという点で社会・経済へも波及することも中・長期的には見込まれる。

5. 主な研究成果リスト

（1）代表的な論文（原著論文）発表

研究期間累積件数：9件

1. Masaki Waga, Étienne André, and Ichiro Hasuo. Model-bounded Monitoring of Hybrid Systems. ACM Transactions on Cyber-Physical Systems. 2022, Volume 6, Issue 4, No. 30, 1-26.
CPS のモニタリングは科学的にも実用的にも注目されているが、実際の挙動が連続時間信号であるのに対し、計算機上ではサンプリングされた離散時間信号しか観測できないという方法論的な困難がある。本論文ではこのサンプリングの不確実性の問題を軽減するために、対象システムに関する近似数理モデルを用いて、離散的なサンプル間の柔軟な補間を行う、model-bounded monitoring という枠組みを提案する。
2. Masaki Waga, Ezequiel Castellano, Sasinee Pruekprasert, Stefan Klikovits, Toru Takisaka, and Ichiro Hasuo. Dynamic Shielding for Reinforcement Learning in Black-Box Environments. Automated Technology for Verification and Analysis. ATVA 2022. 2022, Lecture Notes in Computer Science, vol. 13505. 25-41.
CPS における強化学習の利用には学習時の安全性が保証されていないという課題がある。学習中の危険な挙動を低減するための従来の手法の多くはシステムの事前知識を要求し、その適用範囲は限定的であった。本論文では、強化学習と並行してオートマトン学習によって自動構築された実システムの近似数理モデルを用いることで、事前知識を用いずに学

習時の望ましくない振る舞いを低減する手法を提案する。
3. Junya Shijubo, Masaki Waga, and Kohei Suenaga. Efficient Black-Box Checking via Model Checking with Strengthened Specifications. Runtime Verification. RV 2021. 2021, Lecture Notes in Computer Science, vol. 12974.
ブラックボックス検査を CPS に用いる際には、システムの実行に時間がかかるため、ソフトウェアテストの応用と比べて近似数理モデルと実システムの等価性テストに時間がかかる傾向がある。本論文では、強化された仕様によるモデル検査を用いたブラックボックス検査の拡張を提案する。本拡張により等価性テストの回数が減少し、効率が向上する傾向があることが実験的に示された。

（2）特許出願

研究期間全出願件数：0 件（特許公開前のものも含む）

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）

- Online Quantitative Timed Pattern Matching with Semiring-Valued Weighted Automata. YR-OWLS (Online Worldwide Seminar on Logic and Semantics) 2021, 招待講演.
- Model-Bounded Monitoring of Hybrid Systems. 12th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS 2021) 2021. 口頭発表.
- 完全準同型暗号を用いた秘匿 LTL オンラインモニタリング CSS2021 優秀論文賞（伴野 良太郎氏、 松岡 航太郎氏、 松本 直樹氏、 Bian Song 氏、末永 幸平氏と共同受賞）
- Dynamic Shielding for Reinforcement Learning in Black-Box Environments. International Symposium on Automated Technology for Verification and Analysis (ATVA 2022) 2022. 口頭発表.
- Parametric Timed Pattern Matching. ソフトウェアエンジニアリングシンポジウム 2022 (SES 2022), 2022, 招待講演.