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

平成　２９　年　　６　月　１６　日現在

機関番号：　３２６６５
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３００９２

研究課題名（和文）動的システムに対する組込み制御プログラムの信頼性検証に関する研究

研究課題名（英文）A research on verification of embedded control program for dynamic systems

研究代表者
関澤　俊弦（SEKIZAWA, Toshifusa）

日本大学・工学部・准教授

研究者番号：１０５４９３１４

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）：本研究課題は，振舞いに不確実さをもつ組み込み制御システムの信頼性を保証する手法の研究である．自律移動ロボットを具体的な検証対象とする．誤差補正を行ない継続的に動作する振舞いと，位置を確定させる自己位置推定について，信頼性保証技術の一つであるモデル検査を適用し，確率的なモデルの構築と検証が可能であることを示した．また，モデルの有効性を実装に基づき評価している．本研究で得られた成果より，センサの読み取り誤差や外乱を考慮に入れる必要がある組込みシステムに対し，信頼性を保証しシステム設計に反映させることができると考えられる．

研究成果の概要（英文）：This research is a study of a method to ensure the reliability of an embedded control system with uncertainty in behavior. We set an autonomous mobile robot as a concrete verification target. One target behavior is error correction in consideration of disturbances for continuous run. Self-localization method to specify the position of the robot is also a target behavior. Then, we show possibilities of construction of probabilistic models, and verification results. We also evaluate the effectiveness of our models using implementation of an autonomous robot. From the results, our approach can be applied to ensure reliability considering errors and disturbances in design phase.

研究分野：　ソフトウェア工学

キーワード：　確率モデル検査　組込みシステム　自律移動ロボット

１．研究開始当初の背景

本研究の研究開始時には，車載システムなどに代表される組み込み制御システムが普及しつつあり，センサ等を用いてシステムの外部環境の情報を取得するサイバーフィジカルシステム(CPS: Cyber Physical System)が社会において重要な役割を果たすようになっていた．CPS ではセンサ等により外部環境を測定するため，センサの読み取り誤差やノイズなどの外乱によって，システムの振舞いには不確実さが生じる．CPS の研究開発にあたって，不確実さをもつシステムの信頼性を保証する手法が必要とされていた．

情報システムの信頼性保証技術の一つである形式手法は，その使用が国際規格で推奨されるなど，システム開発への適用が広がりつつあった．形式手法の一つであるモデル検査は，研究開始時までにハードウェアを含む様々な情報システムに適用され，システムの信頼性保証に成果を挙げていた．これを実現するモデル検査器が整備されてきたことから，開発現場への適用も進んでいた．しかし，確率的な振舞いなどの不確実さを考慮に入れる必要がある系への適用に関しては，モデルの構築手法や検証手法の研究は十分に成されていなかった．

２．研究の目的

CPS に代表される組み込み制御システムの不確実さを含む振舞いや仕様の信頼性を，形式手法の一つであるモデル検査を用いて検証する手法を本研究課題の目的とする．モデル検査は対象を表わすモデルとシステムが満たすべき仕様を記述した論理式を入力として，網羅的な検証を行なう．モデル検査の適用可能性を調べるためには，不確実さをもつ対象系について，不確実さを考慮に入れた対象のモデル化と検証，および，評価が必要となる．

本研究では，センサを用いて自律的に動作するロボットを CPS の具体的な対象とした．外部環境の情報を得るためにロボットが用いるセンサやシステム外の要因に起因する外乱などによる誤差のために，システムは確率的な不確実さをもつ．また，時間的な性質を考慮に入れることにより，離散系と連続系が混在するシステムへの拡張を調べることも目的とした．

３．研究の方法

自律移動ロボットの振舞いのモデル化と検証の目的に対して，理論的なモデル構築と検証，および，実装したロボットで得られた観測データに基づく評価を行なう．

(1) モデル化

自律移動ロボットの振舞いとして，センサを用いて誤差補正を行ないつつ定められた経路の走行と，センサを用いてロボットの位置を推定する自己位置推定を，モデル化の対象とする．誤差補正は，ロボットの動作に関する不確実さのモデル化であり，自己位置推定は環境に依存する位置の推定に関するモデル化である．モデル化では，モデル検査を用いて検証することが目的であるため，離散化による状態数の有限化や状態数の削減も行なう．

(2) 検証

方法(1)で構築したモデルは，ロボットの振舞いを表現している．これらのモデルに対して，ロボットが満たすべき仕様をモデル検査器を用いて検証する．誤差補正については継続的な動作に対応する安全性，自己位置推定については位置の特定に対応する到達可能などが求められる仕様と考えられる．

(3) 実装に基づく評価

方法(1)および方法(2)において，理論的なモデル構築では，不確実さを表現することは可能であるが，その妥当性を判定することは難しい．モデル化の妥当性と適用可能性を調べるにあたり，確率分布やシステム外の要因に起因する外乱の事例が必要となる．本研究では，自律移動ロボットを実装し，センサの測定データや座標等の観測データから確率分布を得ることにより，モデル化の妥当性や有効性を調べる方法を取る．自律移動ロボットの実装として，制御システムをプログラムを可能な LEGO Mindstorms を用いて誤差補正を行ないつつ走行する自律移動ロボットを実装した．実装においては LEGO Mindstorms 用の Java 言語である LeJOS を用いた．このロボットは赤外線センサやアクチュエータを備えており，CPS の具体例として扱うことが可能である．た，走行の際には，センサの誤差や走行面からの外乱などにより，確率的な振舞いを示す．従って，簡易なロボットではあるが，CPS の具体例として扱うことが可能となる．図１に誤差補正を行ないつつ動作する自律移動ロボットの動作例を示す．

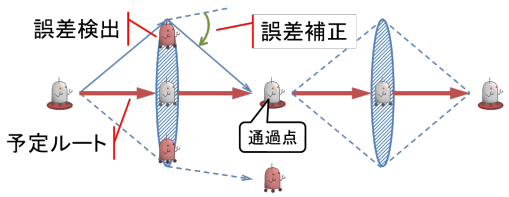

図 1: 誤差補正による自律走行

４．研究成果

(1)確率的な動作のモデル化

自律移動ロボットの動作にはゆらぎが生じることから，動作中の座標は確率的となる．この確率的な振舞いを，マルコフ決定過程(MDP: Markov Decision Process)を用いてモデルを構築した．このモデルでは，ロボットの確率的な振舞いを表わすプロセスと外乱を表わすプロセスで対象系を表現することにより，外的要因から影響を受けるロボットの振舞いをモデル化できることを示した．

はじめに，ボットの動作を表わすプロセスについて記す．ロボットは等速運動をしてい

と仮定することにより，移動に要する時間は単位時間とみなした．MDP では計算時間を単位とするため，この仮定により時間的性質を除去した．ロボットは移動動作に伴う誤差により座標にゆらぎが生じるため，ロボットが取り得る座標は確率分布で表現される．座標を MDP の状態とするとき，確率分布を素直にモデル化すると状態数が無限となる．この問題に対して，ロボットの到達座標を区間として区切る区間分割の手法を適用することにより，状態数を有限とした．具体的には，ロボットが通過を目指す中心座標からの距離に応じて区間を分割した．これは一定の区間の座標を商状態として扱うことによる簡約であり，状態数を有限とすると共に，区間数に応じて状態数を削減することができる．次に，区間の間の遷移確率を定めることにより，ロボットの確率的な振舞いを表現した．図 2 に区間分割と区間の間の遷移確率の関係を示す．ロボットの継続的な動作を表現するために，区間分割された同様の区間が連続して現われるとしてモデル化を行なった．これは，ロボットが等速移動を行ないながら，一定の距離毎に誤差の補正動作を行なう振舞いに相当する．

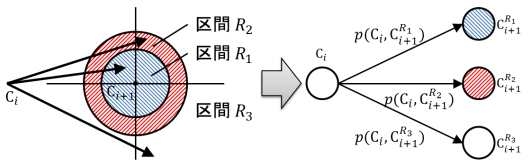

図 2: 区間分割と状態の関係

外乱を表わすプロセスは，ロボットのプロセスと同期して，遷移確率を変化させる．様々な外乱の扱いが考えられるが，外乱はランダムではなく，連続して影響を及ぼすと考えられることから，境界値をもつランダムウォークとしてモデル化した．このモデル化により，横滑りなどの連続した外乱を表現することを可能とした．

(2) 確率的な動作モデルの検証

成果(1)のモデルを用いてロボットの振舞いを検証するために，代表的な確率モデル検査器の一つである PRISM を用いた．検査項目の一つは，ロボットが継続して予定された通過点の近傍を通り続ける確率である．ここで，外乱を考慮に入れない場合と考慮に入れる場合の２つのケースに対して，同じ検査項目を検証することにより，外乱の影響を見ることができる．これにより外乱のモデル化の有効性を示した．理論のみで構築したモデルでは，区間の間の遷移確率を定めることは困難であるが，実装したロボットの実測値から得られた確率分布結果をモデルに適用することにより，成果(1)のモデルがロボットの比較的短い時間における振舞いを表現していることを示した．この結果は，ロボットのフィードバック制御等の設計に応用できると考えられる．一方，ロボットの連続した動作については，モデルとロボットの振舞いの間には乖離が見られた．これは，成果(1)で構築したモデルは，分割した区間の間の遷移確率が変化せずに繰り返し現われるとしているためである．時間経過に伴って動作が安定するロボットを表現するモデルは，成果(1)のモデルで一定とした遷移確率に変化を許すように拡張することで実現できると考えられるが，この観点からのモデル化と検証は今後の課題として残っている．

(3)時間的性質を考慮に入れたモデル化

成果(1)及び成果(2)では，対象系のロボットは等速移動を行なっていると仮定したため，移動に要する時間などの時間的な性質の表現や検証は行なえない．この問題に対して，確率時間オートマトン(PTA: Probabilistic Timed Automaton)を用いて対象系をモデル化することにより，時間的性質も含めたモデルを構築可能であることを示した．PTA によるモデルでは，成果(1)の区間分割の手法に加えて，ロボットの動作に時間を割り当てることにより，確率的な振舞いに加えて時間的な振舞いを併せ持つモデルを構築している．このモデルにより，確率的および時間的性質を考慮に入れたロボットの振舞いもモデル検査の対象となり得ることを示した．このモデルに基づく解析により，システムの設計時に動作時間など時間的制約を保証することが可能になると考えられる．

(4)自己位置推定のモデル化と検証

自律移動ロボットに代表される確率ロボティックスでは，ロボットの位置をセンサ等から得られた情報に基づき，与えられた地図上での位置を推定する自己位置推定は要素技術の一つである．自己位置推定では，成果(1)及び成果(2)で示したロボットの動作そのものの不確実さとは異なり，外部環境に依存した位置を特定する際の不確実さが対象となる．本研究では，自己位置推定方法としてマルコフ位置推定アルゴリズムを採用し，モデル検査の適用可能性を調べるために，確率を排除したモデルをモデル検査器 SPIN 上に構築した．このモデルは，センサの読み取り誤差は排除されているものの，位置に関する不確定性は残したモデルとなっている．ロボットの自己位置推定の可否は地図に依存するため，位置推定の可否をモデル検査の網羅的探索により決定できることを示した．また，自己位置を特定できる場合については，モデル検査から得られる反例を解析することにより，特定に至るまでの経緯を得ることができることを示した．モデル検査においては，状態数が指数的に増加する状態爆発問題が知られているが，本取り組みでは地図の要素数に対するモデルの状態数を調べることにより，モデル検査の適用可能性を示している．この取り組みでは確率は排除されているが，成果(1)および成果(2)のモデルと合成することにより，確率的な動作を含んだ自己位置推定の振舞いを検証する手法となると考えられる．

５．主な発表論文等

〔雑誌論文〕（計１件）

① Kozo Okano, Takeshi Nagaoka, Toshiaki Tanaka, Toshifusa Sekizawa, and Shinji Kusumoto: "Parallel Multiple Counter-Examples Guided Abstraction Loop - Applying to Timed Automaton -," International Journal of Informatics Society (IJIS), Vol. 8, No. 2, pp.103-116, September 2016. 査読あり.

〔学会発表〕（計１０件）

① 岡野浩三, 原内聡, 小形真平, 関澤俊弦, 小原岳士: "Java のメソッド等価性判定とその応用," 電子情報通信学会技術研究報告 IEICE-SS2016-65, Vol. 116, No. 512, pp.31-36, March 9, 2017. てんぶす那覇 (沖縄県・那覇市), 査読なし

② 渡辺誠人, 岡野浩三, 関澤俊弦: "ペアワイズ法に基づいた検証項目の生成とモデル検査による組み込みシステムの検証に向けて," IPSJ/SIGSE ウィンターワークショップ・イン・飛騨高山, Jan. 19, 2017. 高山市民文化会館 (岐阜県・高山市), 査読なし

③ 渡邊亮, 岡野浩三, 関澤俊弦: "二次元系における自己位置推定の振舞い検証に向けて," JSSST FOSE2016, ソフトウェア工学の基礎 XXIII, pp. 275-276, Dec. 3, 2016. ことひら温泉 琴参閣 (香川県・仲多度郡 琴平町), 査読なし

④ 小林佳正, 岡野浩三, 関澤俊弦: "移動時間を考慮に入れた自律移動ロボットの確率的な振舞い検証に向けて," JSSST 第23回 ソフトウェア工学の基礎ワークショップ, Dec. 3, 2016. ことひら温泉 琴参閣 (香川県・仲多度郡 琴平町), 査読なし

⑤ 小林佳正, 岡野浩三, 関澤俊弦: "確率時間オートマトンを用いた自律移動ロボットの振舞いのモデル化," 情報処理学会研究報告 Vol. 2016-SE-192, No. 14, June 2016. 東海大学高輪キャンパス (東京都・港区), 査読なし

⑥ 関澤俊弦, 岡野浩三: "一次元系における自己位置推定の振舞い検証に向けて," 電子情報通信学会技術研究報告 SS2015-100, Vol. 115, No. 508, pp.145-150, March 11, 2016. 沖縄県立宮古青少年の家 (沖縄県・宮古島市), 査読なし

⑦ 小林佳正, 岡野浩三, 関澤俊弦: "時間的性質を考慮に入れた自律移動ロボットの誤差検出と振舞い検証に向けて," JSSST 第22回 ソフトウェア工学の基礎ワークショップ, November 27, 2015. ほほえみの宿 滝の湯 (山形県・天童市), 査読なし

⑧ Kozo Okano, Takeshi Nagaoka, Toshiaki Tanaka, Toshifusa Sekizawa, and Shinji Kusumoto: "Parallel Multiple Counter-Examples Guided Abstraction Loop to Timed Automaton," In Proceedings of International Workshop on Informatics 2015, pp. 153-160, September 2015. Hamsphire Hotel (Amsterdam, Netherlands). 査読あり

⑨ Toshifusa Sekizawa, Fumiya Otsuki, Kazuki Ito, and Kozo Okano: "Behavior Verification of Autonomous Robot Vehicle in Consideration of Errors and Disturbances," In Proceedings of COMPSAC 2015 Workshop: The 1st IEEE International Workshop on Dependable Software and Applications, pp. 550-555, July 5, 2015. Tunghai University (Taichung, Taiwan). 査読あり

⑩ 大槻文也, 伊藤和己, 岡野浩三, 関澤俊弦: "自律移動ロボットの誤差検出と振舞い検証に向けて," IPSJ/SIGSE ウィンターワークショップ 2015・イン・宜野湾, pp. 69-70, January 22, 2015. カルチャーリゾート フェストーネ (沖縄県・宜野湾市), 査読なし

６．研究組織

(1)研究代表者

関澤　俊弦（SEKIZAWA Toshifusa）

日本大学・工学部・准教授

研究者番号：10549314

(2)研究分担者

岡野　浩三（OKANO Kozo）

信州大学・学術研究院工学系・准教授

研究者番号： 70252632