

氏 名 Ezequiel Gustavo Castellano

学位(専攻分野) 博士(情報学)

学位記番号 総研大甲第 2160 号

学位授与の日付 2020 年 3 月 24 日

学位授与の要件 複合科学研究科 情報学専攻
学位規則第6条第1項該当

学位論文題目 Minimising Makespan of Discrete Controllers: A Qualitative
Approach

論文審査委員 主 査 准教授 吉岡 信和

教授 中島 震

助教 加藤 弘之

准教授 鄭 顕志

早稲田大学 理工学術院

准教授 石川 冬樹

国立情報学研究所 アーキテクチャ科学研究系

准教授 Nicolas D'IPPOLITO

Universidad de Buenos Aires

(Form 3)

Summary of Doctoral Thesis

Name in full Ezequiel Gustavo Castellano

Title Minimising Makespan of Discrete Controllers: A Qualitative Approach

The problem of automatically synthesising event-based solutions from environment models and qualitative goal specifications has been widely studied. In these problems, the environment and the goals are specified by using a formal language. The environment is typically modelled as a state machine whose actions are partitioned into controllable and uncontrollable actions. The controller synthesis problem is to automatically produce a solution, i.e., a controller, that by only disabling controllable actions guarantees the satisfaction of the goals. In particular, we focus on reachability and safety goals which are of interest to supervisory control theory, conformant and contingent planning.

Qualitative control problems are boolean in the sense that a controller satisfies a set of goals, or it does not. When a qualitative control problem has a solution, we say it is realisable. Realisable control problems may allow for several possible solutions. Different solutions may differ in the strategy which they apply to satisfy the goals. Typically, based on the arrival of monitored actions, the strategies implemented by controllers decide which and when to start activities. For instance, regarding end-to-end makespan, a controller that starts several activities concurrently instead of executing them sequentially can be, intuitively, considered as a better strategy, no matter which the durations of the activities are. Unfortunately, qualitative synthesis procedures are, so far, oblivious to such considerations. The controller produced is one of the many alternatives and users cannot specify their preferences; e.g., lower-makespan controller. Thus, it is desired to have the ability to express preferences and automatically compute a solution from a set of possible solutions to a control problem accordingly.

Synthesis and planning techniques that allow expressing preferences exist, such as those regarding performance or reliability. Such quality attributes are modelled by introducing a quantitative aspect to the system specification, which imposes a preference order on the controllers that satisfy the qualitative part of the specification. However, from a practical perspective, these approaches require modelling quality attributes quantitatively, whereas in many cases, such detailed representation is not available, possible, or desired.

The main objective is to present a formal approach to reason about preferences qualitatively, restricting attention to makespan of discrete event-based controllers for safety and reachability goals. We aim to provide a framework in which time is

reasoned symbolically, which relieves the user from providing concrete quantitative measures. In particular, we study the scenario in which durations of individual activities are not known up-front. Our hypothesis is that it is possible to i) define a qualitative framework to compare controllers qualitatively regarding their makespan, ii) specify preferences in control problems qualitatively, and iii) produce controllers that reflect those preferences.

In our approach, the specification of the control problem is given as labelled transition systems and linear temporal logic formulas. We define lower-makespan as our preference and introduce a formal framework to qualitatively reason about makespan of discrete event-based controllers for safety and reachability goals. To reason qualitatively about makespan of controllers, we introduce a symbolic time metric derived from parametric timed automata (PTA) semantics. This metric requires modelling sub-tasks of the problem which take time as activities. However, no quantitative information about the duration of the activities is required. Then, we define a mechanism to compare makespan of controllers under unknown durations of activities and event contingencies produced by uncontrollable behaviour. Such a comparison is made through exhaustive analysis by using a symbolic computation over the parameters of a PTA and Satisfiability Modulo Theories (SMT) solving. The parameters of the PTA represent the uncertain duration of the activities. Then, we define makespan-minimising controllers by using the symbolic comparison and we introduce an algorithm that produces a makespan-minimising controller qualitatively. The algorithm is implemented in the MTSA tool and evaluated in case studies. The evaluation consists of comparing the output produced by our algorithm against the standard synthesis algorithm of the tool.

The main contribution of this work is building a framework to symbolically compare makespan of controllers for safety and reachability goals. The results of the comparison establish a dominance relation between controllers. Moreover, we provide a qualitative definition of makespan-minimising controllers, which are controllers that cannot be dominated by any other controller. We also present a sound algorithm to produce a makespan-minimising controller. In addition, we perform experiments to compare the controllers generated by our algorithm against the ones produced by the standard synthesis algorithm that is implemented in MTSA. The experiment validates that our algorithm removes those transitions that lead to sequential execution from a universal controller. By removing those transitions, we can generate controllers that perform better than the ones produced by standard qualitative synthesis algorithms of MTSA. The current implementation can produce makespan-minimising controllers for small to medium size problems, but it does not scale up to large size problems.

博士論文審査結果

Name in Full
氏名 Ezequiel Gustavo Castellano

Title
論文題目 Minimising Makespan of Discrete Controllers: A Qualitative Approach

本論文は、与えられた環境・要求モデルから、正しさが保証された動作仕様を自動生成するコントローラ合成アルゴリズムに関して行った出願者の研究内容をまとめたものである。従来のコントローラ合成アルゴリズムは主に時相論理式で記述される機能要求の保証のみを扱い、機能要求を満たす様々なソリューションの中からある1つのもののみを出力するのにとどまっており、多くの実システム開発で重要視される品質要求を扱うことができなかった。これらの問題に対し、作業完了時間(メイクスパン)最小化に着目し、より短いメイクスパンとなるコントローラを定性比較によって得るためのコントローラ合成アルゴリズムを見出すことが本研究の目的である。

論文は10章から構成される。第1章では研究の背景と目的、第2章では例題、第3章では背景技術となる Labelled Transition System(LTS)、時相論理式、LTS コントローラ合成、Parametric Timed Automata(PTA)、Satisfiability Modulo Theories(SMT)ソルバ等について紹介している。

続いて、第4章では、提案するコントローラ合成手法の全体像を説明している。第5章では、シンボリックな時間概念を導入したコントローラ合成問題の定式化を示している。従来の LTS 形式の環境モデルに対し時間経過を伴うアクティビティを導入し、アクティビティを含むコントローラ合成問題を定式化している。第6章では、メイクスパンの観点からコントローラを比較する比較フレームワークについて説明している。PTA をベースにアクティビティを伴う LTS の時間セマンティクスを示し、SMT ソルバを用いてシンボリックな表現上でコントローラをメイクスパンの観点から定性的に比較する手法を説明している。第7章では、第6章で紹介した比較フレームワークを用いてより短いメイクスパンとなるコントローラを合成する手法を説明している。

第8章では提案したコントローラ合成手法の実装概要と評価を説明している。評価には、コントローラ合成分野で用いられる4つのベンチマークを用い、従来のアルゴリズムと比較し、同等もしくは短いメイクスパンのコントローラが生成されることを示した。

第9章では関連研究についてまとめ、第10章では本論文の貢献、限界と今後の展望を提示した。

なお、研究成果として、出願者は主著でトップレベル査読付き国際会議1篇その他の発表を行っている。

以上を要するに、本論文はソフトウェア動作仕様の保証を伴う自動合成を可能にするコントローラ合成に関する課題として、機能的な要求のみならずメイクスパンに関する品質要求を保証するコントローラ合成手法を提案し、その有効性を示したものである。以上の理由により、審査委員会は、本論文が学位の授与に値すると判断した。