行政院國家科學委員會專題研究計畫　期中進度報告

無限狀態系統之自動驗證(1/3)

計畫類別：個別型計畫
計畫編號：NSC91-2213-E-002-073-
執行期間：91年08月01日至92年07月31日
執行單位：國立臺灣大學電機工程學系暨研究所

計畫主持人：顏嗣鈞

計畫參與人員：林春成、陳姿樺、彭孟池

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 92年5月29日

附件一

行政院國家科學委員會補助專題研究計畫 □ 成果報告 ■期中進度報告

無限狀態系統之自動驗證(1/3)

計畫類別：■ 個別型計畫　　□ 整合型計畫

計畫編號：NSC　91-2213-E-002-073

執行期間：　91 年 8 月 1 日 至　92 年 7 月 31 日

計畫主持人：顏嗣鈞 教授

共同主持人：

計畫參與人員：林春成、陳姿樺、彭孟池

成果報告類型(依經費核定清單規定繳交)：■精簡報告　□完整報告

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、列管計畫及下列情形者外，得立即公開查詢

□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立台灣大學電機工程系

中　華　民　國　92　年　7　月　25　日

行政院國家科學委員會專題研究計畫執行進度報告

無限狀態系統之自動驗證(1/3)

計畫編號：NSC 91-2213-E-002-073
執行期限：91 年 8 月 1 日至 94 年 7 月 31 日(全程)
(第一年: 91 年 8 月 1 日至 92 年 7 月 31 日)

主持人：顏嗣鈞 台大電機系
計畫參與人員： 林春成、陳姿樺、彭孟池 台大電機系

一、中文摘要

本研究的主要目的在探討即時系統驗證之相關問題。我們探討具有未知變數(unknown timing parameters)之時間自動機(timed automata)的抵達解答空間(reachability solution space)問題。一般而言，該問題為不可解的。我們定義三類有限制之具參數時間自動機，並詳細分析其抵達解答空間問題。該三類分別為「上限」(upper-bound)、「下限」(lower-bound)、「雙分」(bipartite) 時間自動機。我們詳細分析以上問題的複雜度，並將結果應用至「具狀態之時間向量加法系統」(timing parameter vector addition systems with states) 。

關鍵詞：時間自動機、時態邏輯、即時系統驗證。

Abstract

We investigate the problem of characterizing the solution spaces for timed automata augmented by unknown timing parameters (called *timing parameter automata* (TPA)). The main contribution of this work is that we identify three non-trivial subclasses of TPAs, namely, *upper-bound, lower-bound* and *bipartite* TPAs, and analyze how hard it is to characterize the solution space. As it turns out, we are able to give complexity bounds for the sizes of the minimal (resp., maximal) elements which completely characterize the upward-closed (resp., downward-closed) solution spaces of upper-bound (resp., lower-bound) TPAs. For bipartite TPAs, it is shown that their

solution spaces are not semilinear in general. We also extend our analysis to TPAs equipped with counters without zero-test capabilities.

Key words: Timed automata, temporal logic, real-time verification.

二、計畫目標與規劃

Timed automata have been a popular model in the research of formal description and verification of real-time systems. In real-world applications, systems are usually described with unknown parameters to be analyzed. Here we use the term *timing parameters* to refer to those parameters which are compared with clocks in either timed automata or parametric TCTL formulae. A timed automaton extended with unknown timing parameters is called a *timing parameter automaton* (TPA). A *valuation* of unknown parameters making the goal state reachable in a TPA is called a *solution*. In this research, we are mainly concerned with the following problem:

- The ***reachability solution characterization (RSC)} problem***: Given a real-time system *A* and a reachability predicate ç, formulate a representation for the solution space of *A* with respect to ç.

It has been shown that the emptiness problem are compared with unknown parameters in TPAs. Knowing such a limitation, a line of subsequent research has been focused on the solution characterization problem for a number of restricted versions of TPAs. The positive results obtained in the last few years have all been focused on unknown timing parameters in the specification of logic formulae. But in practice, it is more likely that engineers will use unknown parameters in the system behaviour descriptions. Moreover, engineers will be more interested at knowing the condition for solution parameters valuations than at knowing whether there exists a solution parameter valuation. In this work, we identify three subclasses of TPAs and investigate the complexity issue of their timing parameter characterization problems. The three subclasses are called *upper-bound TPAs*, *lower-bound TPAs*, and *bipartite TPAs*.

三、計畫分析與討論

Intuitively, what makes upper-bound (resp. lower-bound) TPAs easier to analyze, in comparison with their general counterparts, lies in the fact that for each of such TPAs, the solution space is *upward-closed* (resp. downward-closed). It is well known that an upward-closed set (resp., downward-closed set) is completely characterized by its *minima*l (resp., maximal) elements, which always form a finite set although the set might not be effectively computable in general. We are able to give a complexity bound for the sizes of the minimal elements for a given upper-bound TPA. Our analysis is carried out using a strategy in which a sufficient and necessary condition was derived under which the set of minimal elements of an upward-closed set is guaranteed to be effectively computable. Taking advantage of certain properties offered by timed automata, we are able to yield complexity bounds for the sizes of the minimal elements for the upward-closed sets associated with upper-bound TPAs, allowing us to characterize their solution spaces. This in turn answers the RSC problem for upper-bound TPAs. We are also able to extend our analysis to the model of upper-bound *timing parameter vector addition systems with states (TPVASSs)*, each of which can be viewed as a TPA equipped with counters without zero-test capabilities.

We feel that the method developed in this paper for analyzing upward-closed sets is interesting in its own right. Our technique refines the strategy of Valk and Jantzen (which deals with computing the minimal elements of upward-closed sets) in the following sense. Although the approach proposed in Valk and Jantzen is powerful for showing decidability for a variety of problems in a unified framework, the lack of information regarding the nature of the underlying system makes the calculation of the size of the associated upward-closed infeasible. Our study shows that if a key step in the algorithm of Valk and Jantzen meets certain conditions, then the sizes of the minimal elements can be deduced. It would be interesting to seek additional applications of our technique.

四、計畫成果自評

Given a TPA, the set of all solutions forms the so-called solution space. With respect to a given pair of A and goal predicate ç, the problem of finding a proper characterization for the solution space of A with respect to ç arises naturally in many real-world applications. Such a problem is called the *Reachability Solution Characterization (RSC)* problem. It is not surprising that, in general, a simple characterization of solution spaces for TPAs is unlikely, since the emptiness problem (i.e., the problem of deciding whether thesolution space is empty) is undecidable. In the following, we define subclasses of TPAs whose solution spaces have simpler characterizations.

We have studied in detail the sizes of the minimal (maximal, resp.) elements of upward-closed (downward-closed, resp.) solution spaces associated with upper-bound (lower-bound, resp.) TPAs. Aside from the results themselves, for upper-bound TPAs our analysis also suggests a strategy which, in a sense, supplements the unified approach of Valk and Jantzen for reasoning about upward-closed sets. We feel that our new approach for upward-closed sets is interesting in its own right, and deserves further investigation. We were also able to extend our analysis to upper-bound TPVASSs, i.e., TPAs equipped with counters without zero-test capabilities. Results concerning lower-bound and bipartite TPAs were also derived in this paper. A line of future research for upper-bound TPAs (and TPVASSs) is to explore the possibility of manipulating and characterizing the computations and the solution spaces in a symbolic fashion. One way to do this, perhaps, is to take a closer look at data structures designed explicitly for upward-closed sets, such as the so-called *sharing trees*. Finding how tight our complexity bounds for upper-bound and lower-bound TPAs are remains a question to be answered.

五、參考文獻

[1] R. Alur, C. Courcoubetis, D.L. Dill. Model-Checking in Dense Real-Time, Information and Computation 104(1), 2-34, 1990.

[2] R. Alur, D.L. Dill, D. Automata for Modeling Real-Time Systems, in Proc. 17th ICALP, LNCS 443, pp.~332--335, 1990.

[3] G. Delzanno, J.-F. Raskin. Symbolic representation of Upward-closed Sets, in Proc. TACAS 2000, LNCS 1785, pp. 426-440, 2000.

[4] E.A. Emerson, R. Trefler. Parametric Quantitative Temporal Reasoning, in Proc. IEEE LICS, pp. 336--343, July 1999.

[5] T. Hune, J. Romijn, M. Stoekinga, F. Vaandrager. Linear Parametric Model Checking of Timed Automata, in Proc. TACAS 2001, Italy, April, 2001, LNCS 2031, pp. 189-203.

[6] R. Valk, M. Jantzen. The Residue of Vector Sets with Applications to Decidability in Petri Nets, Acta Informatica, 21, 643-674, 1985.

[7] F. Wang. Parametric Timing Analysis for Real-Time Systems, Information and Computation, 130(2), 131-150, 1996. Also in Proc. 10th IEEE LICS, 1995.

[8] F. Wang, H.-C. Yen. Parametric Optimization of Open Real-Time Systems, Paris, July 2001, in Proc. SAS 2001, LNCS 2126, pp. 299-318.