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(2/3)

計畫類別：個別型計畫
計畫編號：NSC92-2213-E-002-018-
執行期間：92年08月01日至93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：彭柏源、　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　93年5月31日

行政院國家科學委員會專題研究計劃成果報告

無限狀態系統之自動驗證(2/3)

計畫編號: 92-2213-E-002-018

執行期間:92 年 8 月 1 日至 93 年 7 月 31 日

計畫主持人: 顏嗣鈞 教授 國立台灣大學電機工程系

計劃參與人員: 彭柏源、 陳姿樺、 彭孟池

一、摘要

本年度之研究計畫中、我們研究「參數時間自動機」(timing parameter automata, TPA)之「解答空間問題」(the solution space problem) 。 一般而言，此問題為不可解。我們探討三類可解之情形: upper-bound TPA 、 lower-bound TPA 、 bipartite TPA 。我們並發展新的驗證技術來解決以上三類參數時間自動機之解答空間問題，並分析其複雜度。

關鍵字：時間自動機，時間參數

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 spaces. 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.

Keyword: *timed automata, timing parameter*

二、計畫緣由與目的

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 TPA *A* and a goal predicate η, formulate a representation for the solution space of *A* with respect to η.

By `formulating a representation' we mean finding a proper characterization for the solution space so as to allow queries arisen frequently in verification (such as emptiness, membership, etc) to be answered effectively.

三、計畫方法

It has been shown that the emptiness problem (i.e., the problem of deciding whether there exists a parameter valuation under which the associated timed language is nonempty) becomes undecidable when three or more clocks are compared with unknown parameters in TPAs. Knowing such a limitation, a line of subsequent research has been focused on the RSC problem for a number of restricted versions of TPAs. These 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 design engineers will use unknown parameters in the system behaviour descriptions. Moreover, design engineers will be more interested in knowing the condition for solution parameters valuations than in knowing whether there exists a solution parameter valuation. In this work, we identify three subclasses of TPAs and investigate the complexity issue of their RSC problems. The three subclasses are called *upper-bound TPAs, lower-bound TPAs,* and *bipartite TPAs.* In our setting, unknown parameters range over the set of natural numbers. A previous work shows that unknown parameters of integer values can be used for modelling, for instance, the maximal number of retransmissions in the Bounded Retransmission Protocol (BRP), which is a data link protocol used by Philips.

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 *minimal* (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 in a way similar to a strategy proposed in the literature (by Valk and Jantzen), 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. (Note, however, the work by Valk and Jantzen reveals no complexity bounds for the sizes of the minimal elements.) Taking advantage of certain properties offered by timed automata, we are able to refine Valk and Jantzen's approach 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.

Given an upper-bound TPA and an η, we are able to show that RSC(A, η) is upward-closed. Using the basic theory of timed automata, we can take advantage of certain properties of timed automata to derive complexity bounds for computing min(RSC(A, η)).

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. Once the sizes of minimal elements become available, finding all such elements can be done by exhaustive search using the region graph technique, although it would clearly be interesting to develop smarter (and more efficient) algorithms. Some complexity results are also derived for lower-bound TPAs. For bipartite TPAs, we are able to show that their solution spaces are not semilinear in general, in spite of the fact that the emptiness problem is decidable. We feel that the method developed in this work for analyzing upward-closed sets is interesting in its own right. Our strategy provides a refinement over the approach proposed in Valk and Jantzen in the sense that the sizes of the minimal elements can now be deduced, provided that certain conditions are met. It would be interesting to seek additional applications of our technique.

四、結論與未來展望

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. 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. 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] P. Abdulla, A. Annichini, and A.

Bouajjani, Symbolic Verification of Lossy Channel Systems: Application to the Bounded Retransmission Protocol, in Proc. TACAS'99, LNCS 1579, pp.208--222, 1999.

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

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

[4] R. Alur, K. Etessami, S. La Torre, and D. Peled, Parametric Temporal Logic for Model Measuring, in Proc. 26th ICALP, LNCS 1644, pp. 169-178, 1999.

[5] R. Alur, T. Henzinger, M. Vardi, Parametric Real-Time Reasoning, in Proc. 25th ACM STOC, pp.~592--601, 1993.

[6] A. Annichini, E. Asarin, and A. Bouajjani, Symbolic Techniques for Parametric Reasoning about Counter and Clock Systems, in Proc. 12th CAV, LNCS 1855, pp 419-449, 2000.

[7] P. Bouyer, Untameable Timed Automata!, in Proc. STACS 2003}, LNCS 2607, pp. 620-631, 2003.

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

[9] J. Hopcroft, and J. Pansiot, On the Reachability Problem for 5-Dimensional Vector Addition Systems, Theoret. Comput. Sci., 8, 135-159, 1979.

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

[11] C. Rackoff, The Covering and Boundedness Problems for Vector Addition Systems, {\em Theoret. Comput. Sci.}, 6, 223-231, 1978.

[12] L. Rosier, and H. Yen, A Multiparameter Analysis of the Boundedness Problem for Vector Addition Systems, J. Comput. System Sci., 32, 105-135, 1986.

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

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

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