Modelización Formal y Verificación Automática de Sistemas de Tiempo-Real.

Alfredo Olivero[+*], Adriana Gaudiani[*] y Gabriela Maidana[+*]

[+]Depto de Computación. Universidad de Buenos Aires.
[*]Instituto de Ciencias. Universidad Nacional de Gral. Sarmiento
e-mail: alfredo@dc.uba.ar

Resumen

Los sistemas de tiempo-real son sistemas en los cuales el tiempo juega un rol fundamental. Ejemplos de estos sistemas son los controles automáticos de navegación de aviones, los protocolos de comunicación, los procesos industriales automatizados, cajeros automáticos, controladores de radar, etc. El carácter crítico, en más de un sentido, de esta clase de sistemas ha evidenciado la necesidad de proveer métodos formales para su especificación y posterior verificación. Además, su creciente complejidad y tamaño justifica el desarrollo de herramientas que ayuden a su concepción y que automaticen su verificación.

El objetivo de este proyecto está vinculado al desarrollo de herramientas para la verificación automática de sistemas de tiempo-real. Utilizaremos como marco de nuestro trabajo la herramienta KRONOS [BDMOTY98] (en la que uno de los autores ha trabajado desde 1992) estudiando métodos que permitan ampliar sus funcionalidades y mejorando algorítmicamente las técnicas utilizadas hasta el presente.

Área temática: Teoría.
Palabras clave: Sistemas de tiempo-real. Modelización y verificación formal. Herramientas de verificación automática.

Presentación general

Los sistemas de tiempo-real son sistemas en los cuales el tiempo juega un rol fundamental.

Ejemplos de estos sistemas son los controles automáticos de navegación de aviones, los protocolos de comunicación, los procesos industriales automatizados, cajeros automáticos, controladores de radar, etc.

El carácter crítico, en más de un sentido, de esta clase de sistemas ha evidenciado la necesidad de proveer métodos formales para su especificación y posterior verificación.

La creciente complejidad y tamaño de los sistemas tiempo-real con los que nos encontramos a diario justifica el desarrollo de herramientas que ayuden a su concepción y que automaticen su verificación.

Una importante parte de la actividad científica en esta área se ha volcado en el diseño, prototipado e implementación de herramientas con dicha finalidad, como [JO94, HH94, ORS92] entre muchas otras.

Un ejemplo de tales herramientas es el verificador automático de propiedades temporales KRONOS [DOTY96,BDMOTY98] desarrollado en el laboratorio Verimag de Grenoble, Francia.

En el área de sistemas de tiempo-real, un énfasis especial está puesto en la especificación y en los métodos de análisis que puedan ser tratados por herramientas automáticas o semi-automáticas, y en hacer esas herramientas más poderosas, extensibles a grandes sistemas, convenientes y naturales en su uso e inmersas en un marco común que permita un fácil acceso a una amplia gama de enfoques y formalismos.

Típicamente los lenguajes propuestos para la especificación del comportamiento de un sistema de tiempo-real son álgebras de procesos tiempo-real y autómatas extendidos con variables reales.

Los lenguajes de requisitos son lógicas temporales que puedan expresar cambios continuos en el tiempo.

La verificación algorítmica de sistemas con un número finito de estados está basada clásicamente en el método denominado *model checking*. Los algoritmos de model checking determinan los estados que satisfacen una fórmula temporal por un análisis del espacio de estados considerado como un grafo. La

mayor limitación práctica de los algoritmos de model checking está vinculada al tamaño del grafo de estados. Un enfoque para controlar esa "explosión del número de estados" reside en la representación *simbólica* (en vez de *enumerativa*) de los conjuntos de estados. El enfoque simbólico del model checking (implementado en la herramienta KRONOS desarrollada en VERIMAG) evita la construcción explícita del modelo que crece en forma exponencial.
El núcleo del presente proyecto es el desarrollo de herramientas para la verificación automática de sistemas de tiempo-real. Estará basado en la herramienta KRONOS, en la cual el autor ha trabajado durante tres años en la Unidad Mixta de Investigación VERIMAG.

Las actividades a desarrollar en el marco del proyecto comprenden:
- Mejoramiento de los rendimientos de la herramienta KRONOS.
- Ampliación de las funcionalidades con que cuenta la herramienta en la actualidad.
- Estudio de ejemplos, ya sea la extensión de ejemplos existentes o la modelización de nuevos ejemplos.

Objetivos del proyecto

Dentro de este proyecto se destacan dos objetivos generales que son mutuamente dependientes:
- La continuación del desarrollo de la herramienta KRONOS en la cual A. Olivero ha trabajado desde 1992.
- Modelización y posterior verificación de ejemplos que, además, puedan ser utilizados como test de la herramienta mencionada.

Objetivos específicos

Dentro de los objetivos generales descriptos anteriormente, podemos fijar los siguientes objetivos específicos de este proyecto:

Objetivo 1.
Mejoramiento de los rendimientos de la herramienta KRONOS.
El prototipo y las sucesivas versiones de esta herramienta mostraron la factibilidad del enfoque, su flexibilidad y, lo que es más importante, la potencialidad de la misma para ser utilizada a gran escala. Las mejoras planteadas abarcan diversos aspectos: algorítmico, de representación de datos, de utilización de memoria, entre otros, que tendrán como consecuencia una aceleración del proceso de verificación y la posibilidad de tratar ejemplos de mayor tamaño. Algunas de las líneas seguidas son:
- Verificación de sistemas tiempo real utilizando abstraciones.
- Reducción de composiciones de autómatas temporizados
- Mejoras del algoritmo de Model-checking basadas en la estructura del autómata temporizado.

Objetivo 2.
Ampliar los alcances de la herramienta KRONOS:
- La traducción de formalismos de especificación de sistemas de tiempo-real al formato de entrada de la herramienta KRONOS, como ya se ha realizado con el álgebra de procesos ATP [NSY91][Yovine93] y los formalismos T-ARGOS [JMO93][Jourdan94] y ET-LOTOS [DOY94].

Algunos resultados están implementados e integrados a la herramienta KRONOS. Dentro de las diversas líneas planteadas quedan numerosas ideas a desarrollar.

Los objetivos 1 y 2 están vinculados entre sí y se presentan como la continuación del trabajo desarrollado por uno de los autores sobre la herramienta KRONOS.

Objetivo 3.
Modelización y análisis de ejemplos.

Dentro de este objetivo se vislumbran tres posibilidades:

- ampliar la modelización de ejemplos existentes mediante una descripción más detallada, y por lo tanto más realista, y
- modelizar y analizar nuevos ejemplos.

Este último objetivo apunta a complementar los dos anteriores, posibilitando el testeo de la herramienta para detectar sus limitaciones y falencias.

Bibliografía (referente a la herramienta Kronos)

[BDMOTY98]
"KRONOS: A model-checking tool for real-time systems"
M. Bozga, C. Daws, O. Maler, A. Olivero, S. Tripakis y S. Yovine
Computer Aided Verification (CAV 98) Lectures Notes in Computer Science 1427.
Springer Verlag. 1998.

[DOTY 96]
The tool Kronos.
C. Daws, A. Olivero, S. Tripakis y S. Yovine.
Proc. Workshop on Hybrid Systems and autonomous Control. 1996

[DOY 94]
Verifying ET-LOTOS programs with KRONOS
C. Daws, A. Olivero y S. Yovine.
Proc. FORTE'94, 1994.

[Fontana 96]
Una extensión de Kronos para la verificación de sistemas híbridos lineares
Fernando Fontana.
Trabajo de Grado ESLAI, Argentina.

[JMO 93]
Verifying quantitative real-time properties of synchronous programs with Kronos
M. Jourdan, F. Maraninchi y A. Olivero
Fifth Int. Workshop on Computer-Aided Verification, Elounda (Crete), 1993.

[Olivero 94]
Modélisation et Analyse de systèmes temporisés et hybrides
These de Doctorat. Institut National Polytechnique de Grenoble,
Francia 1994.

[Yovine 93]
Méthodes et Outils pour la vérification symbolique des systèmes temporisés
These de Doctorat. Institut National Polytechnique de Grenoble,
Francia 1993.