

**Curso:** Verificación de Sistemas Críticos

**Docente:** Pedro R. D'Argenio

## Resumen

Diariamente interactuamos con decenas de sistemas informáticos ocultos dentro de la electrónica de consumo (como la TV, los reproductores de CD, video o DVD), en los medios de comunicación, en los medios de transporte (como los aviones, automóviles, trenes) y sus respectivos controles de tráfico, plantas industriales, equipos médicos, etc. Muchas de las actividades que desempeñan estos sistemas son críticas: una respuesta incorrecta o tardía puede tener consecuencias irreparables que van desde la pérdida del capital invertido hasta la pérdida de vidas humanas.

En esta materia se enseñarán diversas técnicas que permiten analizar la correctitud de diseños de sistemas críticos de manera completamente automática. Nos concentraremos en los fundamentos teóricos y uso de las herramientas que hoy se utilizan en el contexto de la industria (como Spin, SMV, y Uppaal). Por otra parte, abordaremos también temas actualmente bajo investigación.

## Contenido

1. Introducción
  - Objetivo de la validación formal de sistemas
  - Revisión del ciclo de vida del software
  - Técnicas de validación
  - Ejemplos
  - Autómatas como modelo de especificación
  - Composición de autómatas
2. Verificación de Lógicas Temporales Lineales (LTL)
  - Sintaxis y semántica de LTL
  - Propiedades
  - Especificación de propiedades usando LTL
  - Cómo verificar propiedades LTL
  - Aplicación usando SPIN
3. Verificación de Lógicas Temporales de Bifurcación (CTL)
  - Sintaxis y semántica de CTL
  - Especificación de propiedades usando CTL
  - Cómo verificar propiedades CTL
  - Fairness
  - Aplicación usando nuSMV
4. Otras lógicas
  - La lógica CTL\*
  - El cálculo-mu
  - Expresividad comparativa
  - Cómo verificar propiedades en el cálculo-mu alternante

5. Verificación de Sistemas Temporizados
  - Descripción simbólica mediante autómatas temporizados
  - Semántica de los autómatas temporizados
  - Sintaxis y semántica de la lógica TCTL
  - Cómo verificar propiedades TCTL
  - Análisis de alcanzabilidad
  - Aplicación usando UPPAAL
6. Verificación de Sistemas Probabilísticos
  - Descripción usando procesos de decisión de Markov
  - Verificación cualitativa
  - Sintaxis y semántica de la lógica PCTL
  - Verificación cuantitativa: Cómo verificar propiedades PCTL
7. Técnicas de Reducción del Espacio de Estados
  - Representación simbólica usando BDDs
  - Estrategias de administración de memoria
  - Reducción de ordenes parciales
  - Reducción a través de equivalencias
  - Técnicas de abstracción

## Dictado y carga horaria

El curso se dictará durante el segundo cuatrimestre. Semanalmente se dictarán 5 horas de teoría más consultas de práctica de acuerdo surjan necesidades. Se estima una carga horaria total de 120 horas.

## Modo de Evaluación

El curso se evaluará mediante tres trabajos prácticos en la modalidad “*take-home*”. Además, cada alumno estará a cargo de preparar una clase (cada uno con tema independiente) la cual también formará parte de la evaluación.

## Bibliografía

- J.-P. Katoen. Concepts, Algorithms and Tools for Model Checking. Arbeitsberichte der Informatik, Friedrich-Alexander-Universitaet Erlangen-Nuernberg, vol. 32 no. 1, Gruner Druck GmbH, 1999.
- E.M. Clarke, O. Grumberg, and D. Peled, Model Checking. MIT press, 1999.
- Michael Huth and Mark Ryan, Logic in Computer Science Modelling and reasoning about systems. Cambridge University Press, 1999.
- B. Berard, M. Bidoit, A. Finkel, F. Laroussinie, A. Petit, L. Petrucci, Ph. Schnoebelen, and P. McKenzie. Systems and Software Verification: Model-Checking Techniques and Tools. Springer-Verlag, 2001.
- Andrea Bianco, Luca de Alfaro: Model Checking of Probabalistic and Nondeterministic Systems. FSTTCS 1995. LNCS 1026, 499-513. Springer 1995.

- Doron Peled: Partial Order Reduction: Model-Checking Using Representatives. MFCS 1996: 93-112
- Doron Peled: Combining Partial Order Reductions with On-the-Fly Model-Checking. Formal Methods in System Design 8(1): 39-64 (1996)
- Anca Browne, Edmund M. Clarke, Somesh Jha, David E. Long, Wilfredo R. Marrero: An Improved Algorithm for the Evaluation of Fixpoint Expressions. Theor. Comput. Sci. 178(1-2): 237-255 (1997)
- Luca de Alfaro: Temporal Logics for the Specification of Performance and Reliability. STACS 1997. LNCS 1200, 165-176. Springer 1997.
- Pedro R. D'Argenio, Bertrand Jeannot, Henrik Ejersbo Jensen, Kim Guldstrand Larsen: Reachability Analysis of Probabilistic Systems by Successive Refinements. PAPM-PROBMIV 2001. LNCS 2165, 39-56. Springer 2001.
- Johan Bengtsson, Wang Yi: Timed Automata: Semantics, Algorithms and Tools. Lectures on Concurrency and Petri Nets 2003. LNCS 3098, 87-124. Springer 2004.
- Christel Baier, Marcus Groesser, Frank Ciesinski: Partial Order Reduction for Probabilistic Systems. QEST 2004, 230-239. IEEE press.
- Pedro R. D'Argenio, Peter Niebert: Partial Order Reduction on Concurrent Probabilistic Programs. QEST 2004, pp. 240-249. IEEE press, 2004.
- Christel Baier, Pedro R. D'Argenio and Marcus Groesser: Partial Order Reduction for Probabilistic Branching Time. QAPL 2005, to appear in ENTCS.