Máster en Ingeniería de Sistemas e Informática
62639 - Verificación asistida por computador de sistemas concurrentes

Guía docente para el curso 2010 - 2011

Curso: 1, Semestre: 0, Créditos: 4.0

Información básica

Profesores

- **Fernando García Vallés** gvalles@unizar.es

- **José Manuel Colom Piazuelo** jm@unizar.es

Recomendaciones para cursar esta asignatura

José Manuel Colom

Co-responsable del curso. jm@unizar.es
Centro Politécnico Superior, Edif. Ada Byron, despacho 1.15
Tutorías: Previo acuerdo con el profesor mediante solicitud por correo electrónico

Fernando García Vallés

Co-responsable del curso. gvalles@unizar.es
Centro Politécnico Superior, edif. Ada Byron, despacho 2.19
Tutorías:

Actividades y fechas clave de la asignatura

Se planificarán con los estudiantes el primer día de clase.

Inicio

Resultados de aprendizaje que definen la asignatura

El estudiante, para superar esta asignatura, deberá demostrar los siguientes resultados...

1:
Es capaz de aplicar las técnicas de verificación formal dentro del ciclo de vida del sistema y sobre todo en etapas tempranas de la fase de diseño.

2:
Es capaz de, a partir de una especificación general del sistema, abstraer dicho sistema reteniendo los aspectos relevantes para el proceso de verificación posterior. A partir de ahí debe identificar las propiedades a verificar con una expresión rigurosa de las mismas, y construir el modelo de comportamiento del sistema.

3:
Es capaz de diseñar la estrategia de verificación adecuada a las características del sistema y la propiedad de que se trate, para posteriormente explotar los resultados de la verificación.

Introducción

Breve presentación de la asignatura

La asignatura consta de 4 créditos ECTS o 100 horas de trabajo del alumno. El Máster en Ingeniería de Sistemas e Informática tiene un bloque de asignaturas que forma al alumno en sistemas concurrentes. Dentro de ese bloque, esta asignatura aborda dos de los problemas fundamentales de este tipo de sistemas: (1) la representación y manejo eficientes del espacio de estados de sistemas concurrentes que resultan de dimensiones enormes (*state explosion problem*); y (2) la identificación eficiente de las anomalías que pueden aparecer en el funcionamiento de estos sistemas debidas a la propia concurrencia (*computer aided verification*). La aproximación adoptada es lo suficientemente general como para abordar el estudio de sistemas especificados mediante redes de Petri, autómatas o álgebras de procesos.

Contexto y competencias

Sentido, contexto, relevancia y objetivos generales de la asignatura

La asignatura y sus resultados previstos responden a los siguientes planteamientos y objetivos:

El primer objetivo es que el estudiante conozca los conceptos relacionados con la verificación formal de sistemas concurrentes y distribuidos. Estos conceptos relacionados con la concurrencia deben ser percibidos con el suficiente grado de abstracción como para identificarlos en dominios diferentes a la informática. Entre ellos se incluyen el concepto de especificación formal, modelo de sistema, propiedades de buen comportamiento, verificación formal.

El segundo objetivo que se persigue es que el estudiante conozca las herramientas y formalismos para realizar las tareas de verificación formal. Entre los elementos a considerar están: modelos y formalismos, lógicas temporales para expresión de propiedades, y algoritmos de verificación viables (basados en teoría de autómatas y algoritmos de “model checking”).

Contexto y sentido de la asignatura en la titulación

Esta asignatura aporta, dentro del bloque de Sistemas de Eventos Discretos, y para los Sistemas de Eventos Discretos, los conceptos, métodos y herramientas para la realización de la fase de verificación de la especificación del sistema con relación al modelo que representa el diseño del mismo.

Al superar la asignatura, el estudiante será más competente para...

1:
Dado un sistema en el que exista concurrencia y sea necesario verificar la corrección de su comportamiento:

1. Abstraer el sistema para construir un modelo que represente todos y solo aquellos detalles relevantes para demostrar su correcto comportamiento

2. Especificar formalmente las propiedades de buen comportamiento a verificar
3. Construir el modelo del sistema para la verificación de propiedades

2:
Dado un modelo formal y la especificación formal de las propiedades a verificar:

1. Diseñar la estrategia de verificación y selección de los métodos más adecuados al tipo de modelo y propiedad a verificar.
2. Aplicar la estrategia de verificación diseñada utilizando las herramientas que la tecnología en cada momento ofrezca
3. Interpretar los resultados de la verificación en términos del sistema, y en su caso, explotando contraejemplos obtenidos

3:
Seleccionar métodos y herramientas que le permitan realizar el análisis ayudándole con la explosión combinatoria del espacio de estados debido a la concurrencia

Importancia de los resultados de aprendizaje que se obtienen en la asignatura:

Los sistemas concurrentes y distribuidos son cada vez más utilizados en soluciones de ingeniería de dominios muy diversos. Su complejidad, junto con el cúmulo de comportamientos contraintuitivos hacen que cada vez más la verificación de la corrección de estos sistemas en etapas tempranas de su diseño se convierta en un elemento estratégico para llegar antes al mercado y con niveles de calidad del producto final superiores. Los conceptos y técnicas están hoy en día bien comprendidos, aunque queda un cierto camino por recorrer en cuanto a su despliegue. Adicionalmente, tratar con espacios de estados de dimensiones enormes da lugar a técnicas de representación y manipulación de información no convencionales que pueden ser un beneficio complementario de esta asignatura.

Evaluación

Actividades de evaluación

El estudiante deberá demostrar que ha alcanzado los resultados de aprendizaje previstos mediante las siguientes actividades de evaluacion

1:
Lectura y exposición oral de uno o más artículos que definan el estado del arte en alguno de los temas involucrados en la materia. Los artículos, serán seleccionados por los profesores. Cada exposición oral tendrá una duración de unos 30 minutos a la que asistirá el resto de alumnos y el profesor involucrado en el tema, que será quien la evalúe. Estas exposiciones quedan fuera del horario establecido para clases magistrales. Se presentará por escrito un resumen de la exposición y defensa realizados.

2:
Realización en laboratorio de dos prácticas guiadas por alguno de los profesores. En ellas se aprenderá a utilizar diversas herramientas computacionales para la verificación de sistemas concurrentes mediante técnicas de model checking.

Actividades y recursos

Presentación metodológica general

El proceso de aprendizaje que se ha diseñado para esta asignatura se basa en lo siguiente:

1. Clase magistral participativa donde se expondrán los contenidos fundamentales del curso.
2. Prácticas de aula (problemas y casos prácticos) para que los alumnos adquieran habilidades y asienten conceptos presentados en la clase magistral.
3. Trabajo personal sobre ejercicios prácticos propuestos al alumno adaptados al tipo de sistemas de interés para el estudiante.
4. Prácticas de laboratorio.

Actividades de aprendizaje programadas (Se incluye programa)

El programa que se ofrece al estudiante para ayudarle a lograr los resultados previstos comprende las siguientes actividades...

1:
Temas a presentar en el curso.

1. Conceptos de especificación, diseño y verificación.
2. Técnicas de verificación y ciclo de vida del sistema
3. Bases tecnológicas para la construcción de herramientas software de verificación. Diagramas de Decisiones Binarias Ordenadas y Reducidas (ROBDD) y herramientas.
4. Modelos de concurrencia. Ejemplos de modelado procedentes de diversos dominios de aplicación: programación, Wokflow Management Systems, manufactura, etc.
5. Técnicas para la construcción del espacio de estado de sistemas concurrentes
6. Lógica temporal como herramienta de especificación. Propiedades a verificar.
7. Técnicas de verificación basadas en Model Checking.
8. Ejemplos de verificación de diseños industriales.

2:
Prácticas a realizar

1. Familiarización con el uso del entorno de verificación SMV
2. Modelado, especificación y verificación de un sistema con la ayuda de SMV

3:
Bibliografía básica del curso con la que el estudiante deberá estar familiarizado

- *M.R.A. Huth and M.D. Ryan. Logic in Computer Science. Modelling and reasoning about systems. Cambridge University Press, Cambridge, 2000.*
- *E.M.Clarke, O. Grumberg and D.A. Peled. Model Checking. The MIT Press, Massachusetts, USA, 1999.*
- *R.P. Kurshan. Computer-Aided Verification of Coordinating Processes: The Automata-Theoretic Approach. Princeton University Press, 1994.*
- *C. Girault and R. Valk (Eds). Petri Nets for Systems Engineering. A Guide to Modeling, Verification, and Applications. Springer Verlag, Berlin, 2002.*

Planificación y calendario

Calendario de sesiones presenciales y presentación de trabajos

Se planificará con los estudiantes matriculados en el curso.

Referencias bibliográficas de la bibliografía recomendada