CS 643 Formal Verification of Software Syllabus

The syllabus below describes a recent offering of the course, but it may not be completely up to date. For current details about this course, please contact the course coordinator. Course coordinators are listed on the course listing for undergraduate courses and graduate courses.

Text Books

Required

Daniel Jackson , *Software Abstractions: Logic, Language, and Analysis* , 2012

Recommended

Michael Huth and Mark Ryan , *Logic in Computer Science: Modelling and Reasoning about Systems* , 2004

Week-by-Week Schedule

Week	Topics Covered	Reading	Assignments
1	Course overview; review of sets, relations, functions.	ch 1	
2	Introduction to Alloy specifications.	ch 2	small exercises (appendix of textbook)
3	Modeling and analysis using Alloy.	ch 2 and 3	small exercises
4	More modeling and analysis using Alloy.	ch 3	small exercises
5	Dynamic models.	ch 4	airport or other project
6	More on dynamic models in Alloy.	ch 5	
7	Alloy case study.	ch 6	model project
8	Design by contract. Basics of specification, verification, and weakest preconditions	lect notes	
9	More verification and weakest preconditions	lect notes	
10	Verification using Alloy vs verification by proof. Abstraction and predicate abtraction		final project
11	Overview of UML/OCL and connections with Alloy. Introduction to JML and ESC/Java.	ESC/Java tutorial	
12	Subclassing and behavioral subtyping; modifies, and invariants in JML	lect notes	
13	Final project presentations and discussion		
14	Final project presentations and discussion		