

CS 5382: Topics in Software Development

Writing Verifiably Correct Programs

Spring 2010

CRN: 24955

Lecture: TR 4:30-5:50 pm in CS 322

Website: <http://www.cs.utep.edu/cheon/cs5382>

Instructor: Yoonsik Cheon (x-8028, ycheon@utep.edu); office hours: TR 3:00-4:00 pm in CS 202B

Prerequisite: None

Description

The following course description is excerpted from the Graduate Course Catalog: “The study of the production of high-quality software systems. Topics may include process improvement models, deductive and inductive program synthesis, clean-room programming, and software project management. May be repeated for credit when topic varies.”

The goals of this course are (1) to learn *Cleanroom methods* of software development and (2) to learn basic concepts of formal methods by studying several formal specification languages. Cleanroom methods are a lightweight or semi-formal approach to software development, originally developed by IBM. The “Cleanroom” name was taken from the electronics industry, where a physical clean room exists to prevent introduction of defects during hardware fabrication, and the method reflects the same emphasis on defect prevention rather than defect removal. Special methods are used at each stage of the software development to avoid errors. The key component is the use of specification and verification, where verification means proving, mathematically, that a program agrees with its specification. The beauty of the approach is that one can tune the level of formality, e.g., from mathematical formulae to informal natural language descriptions.

Topics:

- Cleanroom methods
- Basic concepts of formal methods
- Formal specification languages
- Pre and post assertions
- Formal verification

Learning Objectives

- [Level 3: *Synthesis and evaluation*] Adapt the Cleanroom approach to other programming languages and constructs.
- [Level 3] Combine or integrate the Cleanroom approach with other formal specification techniques.
- [Level 2: *Application and analysis*] Using a common formal specification language, formulate the specification of a simple software system and demonstrate the benefits from a quality perspective.
- [Level 2] Create and evaluate pre- and post-assertions for a variety of situations ranging from simple through complex.
- [Level 2] Apply verification techniques to code with low complexity.
- [Level 2] Refine specifications of low complexity into executable code.
- [Level 1: *Knowledge and comprehension*] Explain main steps of the Cleanroom process.
- [Level 1] Explain the potential benefits and drawbacks of using formal specification languages.
- [Level 1] Translate into natural language a software requirement specification written in a commonly used formal specification language.

Textbook

The textbook—Allan M. Staveland, *Toward Zero-Defect Programming*, Addison Wesley, 1999—is available at the UTEP bookstore, and you are expected to acquire a copy for your use in this course, as reading assignments will be taken from the textbook. Additional supplementary readings will be available from the course website.

Examinations

There will be two mid-term exams but no final exam. The mid-term exams will take place during the regular class session and will be 80 minutes in length.

Assignments

There will be two kinds of assignments: in-class presentation and written homework assignments. Students are expected to read and present some research papers related to the Cleanroom approach or formal methods in general. The number of presentations will be one or two depending on the class size. The suggested list of papers is found from the course website; the list is tentative, as the course topics will be decided upon during the first few course meeting. There will be occasional written homework or programming assignments. All assignments shall be done individually unless otherwise specified, and no late submission will be accepted

Projects

You should do a small semester-long class project. The purpose of this project is to apply the ideas and skills learned from the course to your thesis or dissertation research. Sample project topics will be suggested by the instructor, but you may choose your own project topics; your topics must be approved by the instructor. You are expected to write a project proposal, submit a final project report, and present the project result in class.

Grading

Your grade is independent of anyone else's grade; that is, we do not grade on a curve. Everyone can get an A in this course. The purpose of grading is not to rank you, but to uphold a standard of quality and to give you feedback. The final letter grade will be based on a combination of assignments, project, exams, and class participation. The approximate percentages are as follows:

Assignment:	20%
Project:	40%
Exam:	40%

There are also up to 5% bonus points for lecture attendance and class participation. To earn this, you must arrive at lecture on time and participate in class discussion in a constructive and prepared manner, e.g., by asking or answering questions that demonstrate that you have read and attempted to understand the material.

The nominal percentage-score-to-letter-grade conversion is as follows:

90% or higher:	A
80-89%:	B
70-79%:	C
60-69%:	D
below 60%:	F

I reserve the right to adjust these criteria downward, e.g., so that 88% or higher represents an A, based on overall class performance. The criteria will not be adjusted upward, however.

Attendance

Lecture attendance is not mandatory but is recommended. You should understand that your success in the course will improve greatly by attending class regularly. It is your responsibility to keep up to date with notes, assignments and projects.

Standards of Conduct

You are expected to conduct yourself in a professional and courteous manner, as prescribed by the UTEP Standards of Conduct. Graded work (assignments, projects, exams) is to be completed independently and should be unmistakably your own work, although you may discuss your work with others in a general way. You may not represent as your own work material that is transcribed or copied from another source, including persons, books, or Web pages. Instructors are required to—and will—report academic dishonesty and any other violation of the Standards of Conduct to the Dean of Students.

Disabilities

If you feel that you may have a disability that requires accommodation, contact the Disabled Student Services Office at 747-5184, go to Room 106E Union, or email dss@utep.edu.

Schedule

The following table shows a planned schedule for the course. The schedule is subject to change, and an up-to-date schedule will be available from the course website.

	Dates	Topics	Readings	Assignments
Week 1	Jan. 19	Introduction	Chapter 1	
	Jan. 21	Cleanroom Method		
Week 2	Jan. 26	States and Functions	Sec 2.1-2.4	
	Jan. 28	Intended Functions	Sec 2.5-2.7	
Week 3	Feb. 2	Verification	Sec 3.1-3.5	Homework 1
	Feb. 4	Trace Tables	Sec 3.5-3.7	
Week 4	Feb. 9	Verification of Iterations	Sec 4.1-4.2	
	Feb. 11	Verification of Iterations	Sec 4.3-4.5	
Week 5	Feb. 16	Programming with Intended Functions	Sec 5.1-5.3	
	Feb. 18	Group Work	Sec 5.4-5.5	Homework 2
Week 6	Feb. 23	Verification Review	Sec 6.1-6.3	
	Feb. 25	Exam 1		
Week 7	Mar. 2	Definite Iteration	Sec 7.1-7.3	
	Mar. 4	Definite Iteration	Sec 7.4-7.7	
Week 8	Mar. 9	Data Abstraction	Sec 8.1-8.3	
	Mar. 11	Object-Oriented Programs	Sec 8.4	Homework 3
Week 9	Mar. 15-19	Spring break –University closed		
Week 10	Mar. 23	Recursion	Sections 9.1-9.3	
	Mar. 25	Introduction to Formal Methods	Handout	
Week 11	Mar. 30	Exam 2		
	Apr. 1	Project Proposal Presentation		Project proposal
Week 12	Apr. 6	Formal BSL: JML	Handout	
	Apr. 8	JML		
Week 13	Apr. 13	Tabular Notation	Handout	
	Apr. 15	OCL	Handout	
Week 14	Apr. 20	Formal Specification Language: VDM-SL	Handout	
	Apr. 22	Z	Handout	
Week 15	Apr. 27	Process Algebra: CCS and CSP	Handout	
	Apr. 29	CCS and CSP		
Week 16	May 4 & 6	Project Presentation		Project report

Important Dates

January 18: Martin Luther King, Jr. day (university closed)
 January 19: Class begins
 February 3: Census day
 March 4: Exam 1
 March 15-19: Spring break (no classes)
 March 31: Cesar Chavez day (no class)
 April 2: Course drop deadline & Good Friday (no class)
 April 8: Exam 2
 May 7: Dead day