

CONCORDIA UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE
AND SOFTWARE ENGINEERING

SOEN 331-S:
Formal Methods for Software Engineering

Course Outline - Fall 2021

Dr. Constantinos Constantinides, P.Eng.

September 3, 2021

Contents

1	General information	3
2	Office hours	3
3	Course description and learning objectives	3
4	Tutorials	4
5	Graduate attributes	5
6	Material and important dates	6
6.1	Bibliography and references	6
6.2	Resources	7
7	Assessment	7
7.1	Policy	7
7.2	Organization	7
7.3	Submitting coursework	7
7.4	Receiving assessed coursework	8
7.5	Disputes of grades	8
8	Communication	8
9	Rights and responsibilities	8
10	Services and policies	9

1 General information

Course: SOEN 331: Formal Methods for Software Engineering.
Section S, Fall 2021.

Instructor: **Dr. Constantinos Constantinides, P.Eng.**
(constantinos.constantinides@concordia.ca)

Office hours: Tuesday, Thursday 10:15 - 11:30, or by appointment. ON-LINE.

Lectures and location: Tuesday, Thursday 08:45 - 10:00, MB 3.430 SGW.

Tutorials: SA: Friday 14:15 - 16:05, MB 2.285 SGW.
Tutor: TBA.

SB: Friday 12:15 - 14:05, MB 2.285 SGW .
Tutor: TBA.

Course website: <http://users.encs.concordia.ca/~cc/soen331>

Lectures and tutorials will be held on-site. Please respect all pandemic-related rules that have been announced by the University.

2 Office hours

I will have office hours on-line, using a zoom channel the credentials of which I will send to the class at the beginning of the term. This will be on a first-come-first-served basis and I will maintain a waiting room for the channel so that meetings will be one-on-one. If you wish to see me as a group, then the first person to join the channel can give me the rest of the names and I will allow everybody in. Additionally, you can email me for a zoom appointment if this time is not convenient to you.

3 Course description and learning objectives

Prerequisite: COMP 232, 249. This course covers the following topics: property-based (axiomatic and algebraic) formalisms and model-based (abstract and visual) formalisms; axiomatic formalisms with temporal logic, assertions and contracts; algebraic formalisms through algebraic specifications;

abstract formalisms through the Z and Object-Z specification languages; visual formalisms through automata (finite state machines and extended finite state machines). Lectures: three hours per week. Tutorial: two hours per week. (Source: Undergraduate Calendar).

There are two major components to the course: *Model-Based Specifications* and *Property-Based Specifications*. Model-Based Specifications are divided into *Visual* and *Abstract*. Under Visual Model-Based Specifications, we will cover Extended Finite State Machines (also referred to as UML State Diagrams). Under Abstract Model-Based Specifications we will cover two specification languages: The Z specification and one of its object-oriented variants, Object-Z. Property-Based Specifications are divided into *Axiomatic* and *Algebraic*. Under Axiomatic Property-Based Specifications we will cover Assertions and Contracts, and Temporal Logic which is an extension to Propositional Logic, where the propositions are qualified in terms of time. Under Algebraic Property-Based Specifications we will cover Algebraic Specifications. Both Model-Based and Property-Based Specifications build on the fundamentals concepts of Logic and Discrete Structures, some of which were covered in COMP 232. In the course I have chosen to provide lecture notes with a relatively complete discussion of the fundamentals for the sake of cohesion of the material. During lectures I will select important topics and focus on what is new.

4 Tutorials

Tutorials start on the second week of term, and they are designed to reinforce the material covered during the lectures with examples and exercises. Tutorials are also designed to be highly interactive and we strongly recommend that you attend them. Though attendance to tutorials is not mandatory for assessment, please do not attend a tutorial session for which you are not registered.

5 Graduate attributes

Graduate attributes are skills that have been identified by the Canadian Engineering Accreditation Board (CEAB) and the Canadian Information Processing Society (CIPS) as being central to the formation of engineers, computer scientists and information technology professionals. As such, the accreditation criteria for our programs dictate that graduate attributes are taught and evaluated as part of the courses. This particular course aims at teaching and evaluating three graduate attributes. The following is a description of these attributes, along with a description of how these attributes will be incorporated in the course.

Attribute 1: Knowledge-base for engineering Property-oriented (axiomatic and algebraic) formalisms and model-based (abstract and visual) formalisms. Axiomatic formalisms with temporal logic, assertions and contracts. Algebraic formalisms through algebraic specifications. Abstract formalisms through the Z and Object-Z specification languages. Visual formalisms through automata (extended finite state machines). Assessed through examinations and coursework.

Attribute 2: Problem analysis Specify and validate requirements formally through temporal logic. Develop implementation specifications using assertions (method preconditions and postconditions and class invariants) and contract programming. Develop formalisms via algebraic specifications to match system requirements. Specify requirements formally in Z and Object-Z and mapping them to implementation. Assessed through examinations and coursework.

Attribute 5: Use of Engineering tools Use of programming languages and software tools for assertion checking and verification. Built-in support for contract programming vs. third-party provision. Assessed through coursework.

6 Material and important dates

Material will be made available on the course website. This includes lecture notes (accompanied by pre-recorded lecture sessions from previous offerings of the course) and tutorial notes. A tentative schedule is as shown below:

7 September : First lecture.

17 September : First tutorial.

30 September : Assignment 1 posted.

14 October : Assignment 1 due. Assignment 2 posted.

28 October : Assignment 2 due. Assignment 3 posted.

11 November : Assignment 3 due. Assignment 4 posted.

25 November : Assignment 4 due.

26 November : Last tutorial.

30 November : Last lecture.

TBA : Final examination.

The date for the final examination will be scheduled and announced by the University.

6.1 Bibliography and references

1. V. S. Alagar and K. Periyasamy, *Specification of Software Systems*, 2nd. ed., Springer, 2011.
2. M. Fisher, *An Introduction to Practical Formal Methods Using Temporal Logic*, Wiley, 2011.
3. J. M. Spivey, *The Z Notation: A Reference Manual*, 2nd. ed.:
cse.buffalo.edu/LRG/CSE705/Papers/Z-Ref-Manual.pdf
4. G. Smith, *The Object-Z Specification Language*:
citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.2294&rep=rep1&type=pdf

6.2 Resources

1. MiKTeX (L^AT_EX for Windows): www.miktex.org/
2. MacTeX (L^AT_EX for Mac OS): www.tug.org/mactex/
3. Texmaker (cross-platform L^AT_EX editor): www.xmlmath.net/texmaker/
4. TeXnicCenter (integrated L^AT_EX environment for Windows): www.texniccenter.org/
5. A simple guide to LaTeX - Step by Step: www.latex-tutorial.com/
6. ShareLaTeX: An on-line, collaborative LaTeX editor: www.sharelatex.com/
7. Wikipedia, LaTeX symbols: en.wikipedia.org/wiki/Wikipedia:LaTeX_symbols

7 Assessment

7.1 Policy

The course will be assessed as follows: $4 \times \text{assignments (15\%)} + \text{final exam (40\%)} = 100\%$.

7.2 Organization

For your coursework assignments you will work in teams. Detailed instructions on the organization of each assignment will be included with each announcement.

The final examination will be in a multiple-choice format and it will cover the entire material. You are responsible for everything covered or assigned as additional reading during lectures and tutorials.

Please note that if due to the ongoing pandemic the final examination cannot be held on-site (as currently planned), then the examination will be replaced by a project.

7.3 Submitting coursework

You team leader must submit all coursework electronically on behalf of the team. Please make sure you include all names and id's of team members. The electronic submission system is available at <https://fis.encs.concordia.ca/eas/>

7.4 Receiving assessed coursework

Once your coursework is assessed, our teaching Assistants will send an email to the leader of your team with a detailed marking report for each assignment.

7.5 Disputes of grades

If you wish to dispute a mark you have received in an assignment, please do not contact our Teaching Assistants. Instead, your team leader should email me within three business days of this being returned to you. Describe in detail why you think more credit should be given, comparing your solution to the one we will make available to you on the course website. We will review your concern and give you a response. Our response will be final, i.e. we will not iterate over this.

8 Communication

All announcements will be made through the course website. If you wish to contact me via email, please include the course number and section in the subject line and make sure you sign your message with your complete name and Concordia id.

9 Rights and responsibilities

The most common offense under the Academic Code of Conduct is plagiarism which the Code defines as “the presentation of the work of another person as one’s own or without proper acknowledgement.” This could be material copied word for word from books, journals, internet sites, professor’s course notes, etc. It could be material that is paraphrased but closely resembles the original source. It could be the work of a fellow student, for example, an answer on a quiz, data for a lab report, a paper or assignment completed by another student. It might be a paper purchased through one of the many available sources. Plagiarism does not refer to words alone - it can also refer to copying images, graphs, tables, and ideas. “Presentation” is not limited to written work. It also includes oral presentations, computer assignments and artistic works. Finally, if you translate the work of another person into French or English and do not cite the source, this is also plagiarism. In Simple Words: Do not copy, paraphrase or translate anything from anywhere without saying where you obtained it!

(Source: The Academic Integrity Website:

<http://provost.concordia.ca/academicintegrity/plagiarism/>)

In the case where we have reasonable to grounds to suspect a plagiarism offense, we will submit an Incident Report to the Dean per item 17.10.3.25 of the Academic Integrity and the Academic Code of Conduct (<https://www.concordia.ca/academics/undergraduate/calendar/current/17-10.html>). In the interim, and until there is a final outcome of any proceedings under this Code, there will be a pending notation in your transcript.

10 Services and policies

- Counselling and Psychological Services: <http://www.concordia.ca/offices/cdev.html/>
- Concordia Library Citation and Style Guides:
<http://library.concordia.ca/help/howto/citations.html>
- Student Advocacy Office: <http://www.concordia.ca/offices/advocacy.html>
- New Student Program: <http://newstudent.concordia.ca/>
- Centre for Gender Advocacy: <http://genderadvocacy.org/about-us/the-centre/>
- Accessibility services:
<http://www.concordia.ca/students/accessibility.html>
- Student Success Centre: <http://www.concordia.ca/students/success.html>
- Academic Integrity: <http://www.concordia.ca/students/academic-integrity.html>
- Financial Aid and Awards Office: <http://www.concordia.ca/offices/faao.html>
- Health Services: <http://www.concordia.ca/students/health.html>
- Official Policies: <http://www.concordia.ca/about/policies.html>