Formal Languages and the Theory of Computation

Topic 0. Course overview

Han, Nguyen Dinh (han.nguyendinh@hust.edu.vn)

Faculty of Mathematics and Informatics
Hanoi University of Science and Technology

Outline

1. Introduction to the course CS3372

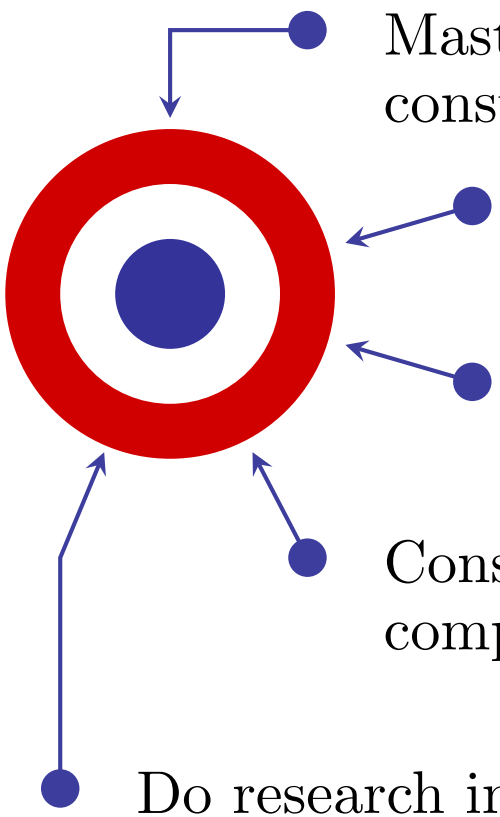
1.1. Course purpose

- This is a required major course in Troy Computer Science Program at HUST. The theoretical part of the course will focus on elements of the theory of computation including: elementary concepts and techniques of automata and formal languages, Turing machines, undecidable and intractable problems

- The practice part of the course gives students chances to study useful computational models and algorithms, and apply them in areas such as complexity and cryptography

1.2. Course objectives

After completing this course, you will be able to:



- Master fundamental concepts and principles constituting the theory of computation
- Develop formal models that represent computing systems
- Analyze and evaluate mathematical models and algorithms of computational systems
- Consult on the design and implementation of computational paradigms
- Do research in a group and work with other team members to build deliverables along the way

1.3. Course content

This course covers key selected topics as foundations of formal languages and the theory of computation including:

- Regular languages and finite automata
- Context-free languages and pushdown automata
- Computation models: Turing machines
- Turing-recognizable and Turing-decidable languages
- Extensions of Turing machines
- Complexity and cryptography

1.4. Learning materials

1. Michael, S. (2012, required) *Introduction to the Theory of Computation*. Third Edition. Cengage Learning

2. Lewis, H.R. and Christos, H.P. (1998) *Elements of the Theory of Computation*. Second Edition. Prentice-Hall

3. Berstel, J., Perrin, D. and Reutenauer, C. (2010) *Codes and Automata*. Cambridge University Press

4. John Talbot and Dominic Welsh (2010) *Complexity and Cryptography: An Introduction*. Cambridge University Press

5. Douglas R. Stinson (2019) *Cryptography Theory and Practice*. Fourth Edition. Taylor & Francis

2. Projects and assignments

Individual project and assignments

1. Quiz
2. Homework
3. Oral presentation

Group project

You are required to work in a group of three to five students. Your group will do a research project in the fields of complexity and cryptography

3. Group project registration

3. Group project registration

In order to register your project, you have to:

1. Define your research problem
2. Propose a name/title for your project
3. Make plans for your research. Your working plan should have five main components: (1) objective, (2) activities/tasks, (3) results, (4) who, and (5) when

The research topics may be: breaking symmetric and asymmetric cryptosystems; establishment and evaluation of post-quantum cryptosystems, blockchain systems, interactive proof systems, etc.

Course overview

Thank you very much for your attention!