Alex Hubers
CSC:341 Spring 2024

HW #1

Due: February 06, 2022

Learning Outcomes Completion of this assignment will contribute to your ability to fulfill the following learning outcomes:
1-1: Represent a problem using a regular model of computation.

Instructions. You are allowed to collaborate with others, however you should write up solutions independently. Copying an answer from another source (e.g. the Web) or from another student may yield few or zero points. Write solutions neatly and legibly, or type your solutions in LaTeX. Be sure to number each problem, and indicate a final solution (if relevant). Answers to problems should include justification (show your work).

Acknowledgments. Problems from this homework come from published sources. The specific sources are withheld due to the nature of this assignment.

Academic Honesty. Include the following information at the top of your submission, along with your name.

- Written sources used: (Include textbook(s), complete citations for web or other written sources. Write *none* if no sources used)
- Help obtained: (Include names of anyone other than the instructor.)

Rubric. Problems will be graded on a 4-point *EMBN rubric*. Graded answers will be assigned an appropriate letter descriptor (below) and provided some justification of this assignment. Points will be awarded in the range associated with each descriptor.

- **E (Excellent)**. 4 pts. Complete understanding of the material is evident; exhibits no errors and can serve as an exemplar solution for the course.
- **M (Meets Expectation)**. $[3, 4)$ pts. Complete understanding of the material is evident, but exhibits some minor errors that warrant revision.
- **B (Below Expectation)**. $[1, 3)$ pts. Limited understanding of the material is evident; exhibits many minor errors or one or more major errors that necessitate revision.
- **N (Not Completed)**. 0 pts. Not completed to a degree where understanding is evident.

Protocols

Specification

A powerful application of finite automata is the specification and verification of protocols. In this problem, we'll examine a protocol between a client and a conference management server (CMS) such as HotCRP. A client to this system may be an author editing a paper for a review. That same client might also be a reviewer editing reviews for papers submitted to the conference. Such a system segregates the two roles so that authors cannot edit reviews of other papers they are in competition with.

The client may issue the following commands to the server:

- Connect
- Change role to author
- Change role to reviewer
- Edit paper
- Edit review
- Disconnect

A valid session between the client and CMS adheres to the following rules.

1. The client must connect to the server before performing any other action.
2. Once connected, the client is initially given the author role.
3. While connected, the client can switch their role between author and reviewer. (Presumably, the client needs to have proper rights to switch roles, but that is not captured in this protocol.)
4. As an author, the client can edit papers but not reviews
5. As a reviewer, the client can edit reviews but not papers.
6. The client cannot connect to the server if it is already connected.
7. The client must disconnect from the server to end the session.

Note that in a single session, the client may connect and disconnect multiple times. However, every valid session ends with the client disconnected from the CMS.

Exercises

#1 (4 pts)

Specify a language, L, that captures valid sessions between the client and the server. L should be specified in set-theoretic terms without appeal to a machine, and you should clearly define its alphabet Σ.

#2 (4 pts)

Give a deterministic finite automata, D, that recognizes L in terms of a state diagram. You may either use a library to build this in your LaTeX/Markdown source, e.g., TikZ for LaTeX, or embed a picture of the diagram made in a third party tool or drawn by-hand. In your state diagram, you make take the shortcut that any transition from a state that is not drawn implicitly goes to an additional "dead" state.

#3 (4 pts)

Prove that the DFA D recognizes L. To do this:

- Assign a property to each state of D that captures the essence of what that state means, for example, the "disconnected" state.
- Perform an exhaustive case analysis on each state q of D, arguing that each of q's transitions is valid and preserves the property of q according to the rules of the protocol.

#4 (4 pts)

Give an implementation of the protocol in a real-world programming language of your choice. If your code is handwritten, use indentation and provide numbering so it is easy to follow. If typing your code in LaTeX, please use the verbatim environment or a package such as algorithmic. DO NOT type an algorithm in a simple word processing document (word, docs, etc).

```
def protocol(curr-state, command):
        if curr-state = (author or reviewer) && command = disconnect
                return dead-state
        if curr-state = author
            if  command = edit-paper
                    return author
            else if command = change-role
                return reviewer
        if curr-state = reviewer
            if command = edit-review
                return reviewer
            else if command = change-role
                return author
        if curr-state = start and command = connect
                return author
        else
                return dead-state
```

#5 (4 pts)

Finally, based on your experiences developing D and your "real-world" implementation of the protocol, describe the pros and cons of first using a finite automata to model a protocol before going to implementation. More broadly, consider the problem description an *informal specification* and the DFA you constructed a *formal specification*. Does the formal specification aid the software implementation? Why might you want one over the other? Be open-minded about the benefits you consider not just in terms of correctness but also productivity.

(This question will be graded on a S/Ns scale. Full credit will be given to any honest reply.)