Project 6 Requirements

Abstract

The objectives, requirements, and relevant information are stated here. Submission of your files is done through the course website.

1 Purpose

The purpose of this project is for you to demonstrate the following:

Capabilities: to produce a basic technical report of professional quality containing:

- Code solutions to Exercises 13.10.1, 13.10.2, and 14.4.1.
- Session transcripts showing proof results
- Explanations as required by each problem
- All source code for each exercise in the appendix

Reproducible Proofs and Documentation: All your datatypes, definitions, theorems, and proofs are contained in HOL theories. All your theories are pretty-printed as stand-alone LaTeX reports.

- Your HOL theories must be built using *Holmake*
- Your pretty-printed HOL theories must reside in a subdirectory called HOLReports and be maintained using *make clean* and *make*

Use of Relevant Tools and Techniques: LaTeX, AUCTeX, emacs, ML, and HOL

Deliverables and Evidence: a pdf of your report with *all source files allowing others to reproduce your report.*

2 Project Requirements

Your report shall have content to reflect Exercises 13.10.1, 13.10.2, and 14.4.1.

2.1 Theorem and Theory Names

Use the following names:

Theorem Names: In all the exercises use the names as suggested.

Theory Names: Use *solutions1Theory* and *conops0SolutionTheory.*

2.2 Report Contents

Front Matter: Title, Author, Date, Abstract, Acknowledgments, and Table of Contents

Chapter 1: Executive Summary

Chapter 2: Exercise 13.10.1 with the following subsections

1. Forward proof of theorem *aclExercise1* as stated in part A of the exercise
2. Use of *PROVE_TAC* only to prove theorem *aclExercise1B* as stated in part B of the exercise
3. A goal-oriented proof using the ACL tactics as stated in part C to prove *aclExercise1C*.

Only one problem statement covering all three sections is needed. Each section must include relevant code and transcripts of definitions and proofs.

Chapter 3: Exercise 13.10.2 with the following subsections

1. Forward proof of theorem *aclExercise2* as stated in part A of the exercise
2. Use of *PROVE_TAC* only to prove theorem *aclExercise2B* as stated in part B of the exercise
3. A goal-oriented proof using the ACL tactics as stated in part C to prove *aclExercise2C*.

Only one problem statement covering all three sections is needed. Each section must include relevant code and transcripts of definitions and proofs.

Chapter 4: Exercise 14.4.1 with the following sections

1. Definition of datatypes for *commands, people, roles, keyPrinc* and *principals*
2. Proof of *OpRuleLaunch_thm*
3. Proof of *OpRuleAbort_thm*
4. Proof of *ApRuleActivate_thm*
5. Proof of *ApRuleStandDown_thm*

Only one problem statement covering all four sections is needed. Each section must include relevant code and transcripts of definitions and proofs.

Appendix A: Contains the source code file *example1Script.sml*.

Appendix B: Contains the source code file *solutions1Script.sml*.

Appendix C: Contains the source code files *conops0SolutionScript.sml*.

2.3 Pretty-Printed Theories in HOLReports

Your pretty-printed theories must include the following theories:

1. *example1Theory*,
2. *solutions1Theory*, and
3. *conops0SolutionTheory*

3 Relevant Information

3.1 Submission Guidelines

Deadline: check course website

Content & format: zipped file of your Project6 subdirectory containing a pdf of your report and all source files allowing complete reproduction of your report. Your Project6 subdirectory will have the following structure and naming conventions:

- You will have 2 subdirectories in Project6:

  HOL: which contains all your source code, e.g., HOL script files, and

  LaTeX: which contains all the files for your project report, e.g., style files, LaTeX files for your report, figures, etc.

- Definitions and proofs of all exercises will be in their corresponding script files
- Your **HOLReports** folder will be *subdirectory of your HOL folder*. Within HOLReports will be the following files:

  Holmakefile: which includes all the paths to theories needed, and specified in a way that does not require third parties to alter path information to compile pretty-printed reports.

  documentation.sml: which contains all commands necessary to pretty print your theory files

  Makefile: which is the script defining *make clean* and *make* commands that remove or build all pretty-printed HOL theory files, respectively.

How submitted: through course website

Other information: you will be allowed an unlimited number of attempts to submit your files up to the deadline. Your grade is based on the last submission.

3.2 Grading Criteria

Project Report					
Deliverable Item	**Problem Statement**	**Relevant Code**	**Definition & Proof Transcripts**	**Code in Appendix**	**Total**
Chapter 1: Executive Summary	4 points for summary	N/A	N/A	N/A	4 points max
Chapter 2: 13.10.1	1	3	3	1	8 points max
Chapter 3: 13.10.2	1	3	3	1	8 points max
Chapter 4: 14.4.1	1	5	5	1	12 points max
Appendix A: *example1 Theory*	N/A	1	N/A	N/A	1 point max
Appendix B: *solutions1 Theory*	N/A	6	N/A	N/A	6 points max
Appendix C: *conops0Solution Theory*	N/A	5	N/A	N/A	5 points max
Report Content Subtotal	7 points max	23 points max	11 points max	3 points max	44 points max
LaTeX folder with all necessary files to reproduce report with no errors					44 points max
				Report Total	88 points max
HOL Script Files and HOLReports Files					
Deliverable Item					**Total**
HOL theories build with *Holmake* error free: 2 points per item					22 points max
Pretty-printed HOL theories in LaTeX compile using *make* error free: 2 points per definition or theorem					22 points max
				HOL Script and HOLReports Files Total	44 points max
				Grand Total	**132 points max**