Introduction to the Coq Package

1 Structure of Our Coq Package

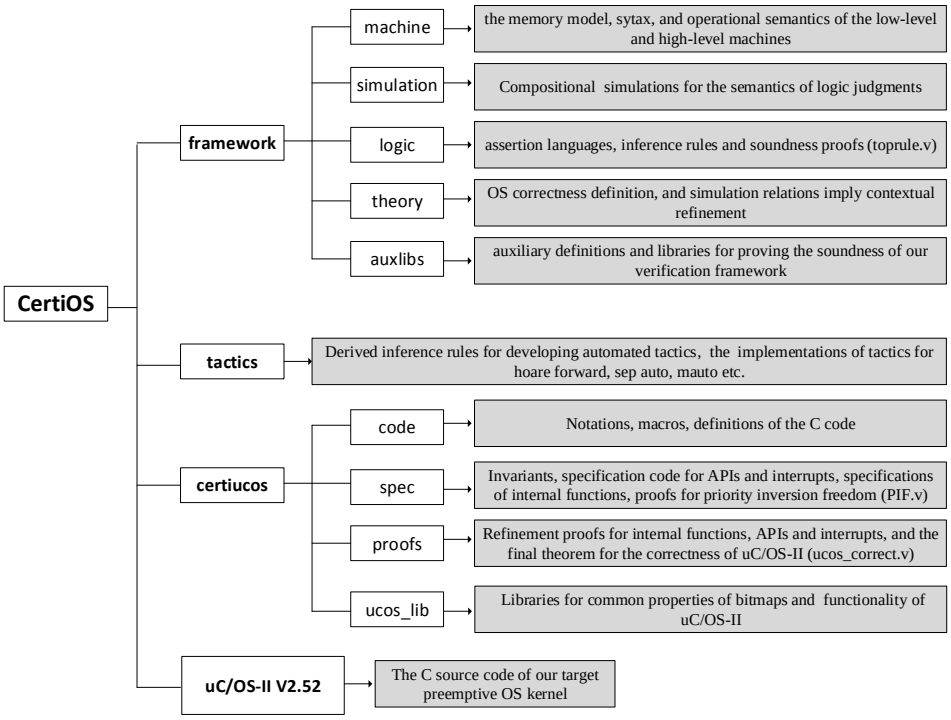

Fig. 1. Structure of Our Coq Package

As shown in Fig.1, the entire package consists of three main components: the verification framework (framework), automated tactics (tactics) and certified μC/OS-II (certiucos). The "framework" directory contains the formalizations for the low-level and high-level machines, meta-theories for our refinement-based program logic and soundness proofs. The "tactics" directory contains some derived inference rules and automated tactics we developed for improving the productivity. The above two directories corresponds to the contents in Sections 3 and 4 of our submitted paper. The "certiucos" directory is used for verifying

μC/OS-II (corresponding to Section 6) and the priority inversion freedom for mutexes in μC/OS-II (corresponding to Section 5).

2 Coq Version

Our coq package is compiled with the current stable Coq Version 8.4pl6, which can be downloaded from `http://coq.inria.fr`

3 Compilation Instructions

Please unzip the package first, then type the following instructions to compile the entire package:

```
cd CertiOS
make
```

If you only want to compile the soundness theorem of the verification framework, please type the following instructions:

```
cd CertiOS
make framework/logic/toprule.vo
```

If you want to compile the correctness theorem for uC/OS-II, please type the following instructions:

```
cd CertiOS
make certiucos/proofs/ucos_correct.vo
```

NOTE: It will take around 16 hours to finish the entire compilation on a machine with 3.6GHz cpu and 32G memory. The compilation of the verification framework takes around half an hour, and the certified μC/OS-II takes around 16 hours. A machine with a good cpu and large memory is highly recommended. You can use the command "sh pg xxx.v" to play with our code in emacs.