

Lab 0: Preparation Lab
15-424/15-624/15-824 Logical Foundations of Cyber-Physical Systems
TA: Katherine Cordwell (kcordwel@cs.cmu.edu)

Due Date: Thursday, September 5th, 11:59PM, worth 10 points

NO late days: it is essential that you get everything running correctly as soon as possible.

Lab Resources: <https://lfcps.org/course/lfcps19/lab0.zip>

1 Installation

KeYmaera X is a theorem prover that you will use for every lab assignment in this course. KeYmaera X works best when it uses Mathematica as a powerful back-end arithmetic solver, as opposed to the free Z3 solver which is installed automatically. Since you will be using KeYmaera X a lot, we expect you to set it up with Mathematica.

For your convenience, we provide instructions on installing Mathematica and running KeYmaera X from your own computer. However, if you are unable to do this, the lab assignments can be completed using KeYmaera X from any CMU cluster with Mathematica installed. After installing Mathematica, installing KeYmaera X should be straightforward.

Unless you have a very underpowered machine, we suggest you install KeYmaera X locally.

Step 0: Update Java To run KeYmaera X, you will need a version of Java after 8u131 and before version 11. You could use, for example, Java 8u221 (the latest version of Java 8). To check your version of Java, run this from the command line:

```
$ java -version
```

Step 1: Install Mathematica, download KeYmaera X, and run KeYmaera X We provide instructions for three settings: CMU Mac Clusters, CMU Linux Clusters, and local installation.

Option 1: Run KeYmaera X from a CMU Mac Cluster

Check that Mathematica is installed and has an active license by opening it from the command line:

```
$ mathematica
```

Follow on-screen directions (if any), until the Mathematica welcome screen appears, and then exit. This only needs to be done the first time you use Mathematica.

Next, download and open KeYmaera X: <https://www.ls.cs.cmu.edu/KeYmaeraX/keymaerax.jar>

Once downloaded, you may also open this file via the terminal with this command:

```
$ java -jar keymaerax.jar
```

Skip to Step 2.

Option 2: Run KeYmaera X from a CMU Linux Cluster

Check that Mathematica is installed and has an active license by opening it from the command line:

```
[user@unix1 ~]$ mathematica
```

Follow on-screen directions (if any), until the Mathematica welcome screen appears, and then exit. This only needs to be done the first time you use Mathematica.

Then run the following from the command line to download and run KeYmaera X:

```
[user@unix1 ~]$ wget https://www.ls.cs.cmu.edu/KeYmaeraX/keymaerax.jar
[user@unix1 ~]$ java -jar keymaerax.jar
```

Skip to Step 2.

Option 3: Run KeYmaera X from your personal computer.

First, download the latest CMU student version of Mathematica version from here:

<https://www.cmu.edu/computing/software/all/mathematica/index.html>

At the point of writing, this should get you Mathematica version **12.0**.

The installation file is **large**, so the download will take some time.

Follow the detailed installation instructions in the **README** file to install Mathematica and retrieve a license key from the Wolfram website.

Before proceeding, activate Mathematica by launching Mathematica and entering the license key that you obtained by following the instructions in the README file included with Mathematica.

Is Mathematica Installed?

To check that Mathematica is installed, open a new notebook, typing in “1 + 1”, and hit SHIFT + ENTER. You should see some reasonable output!

If you have the correct paths set up (see <https://pages.uoregon.edu/noeckel/Mathematica.html>, e.g.), you can also open and run Mathematica from the command line:

- Open a terminal and run the `math` command. You should get a prompt like “In[1]:=”. Type `1=1` and hit enter. You should see some reasonable output :-). If you see some message about license information, follow the directions in the **README** file that came with Mathematica.
- If you do not know how to open a terminal window, Google “<your operating system> open terminal”. Google will give you some instructions right on the search page.

Next, download KeYmaera X: <https://www.ls.cs.cmu.edu/KeYmaeraX/keymaerax.jar>

Open `keymaerax.jar` or run `java -jar keymaerax.jar` from the command line in the folder where the file downloaded. Double-clicking on `keymaerax.jar` may not work:

- If you are on a Mac, open the folder containing `keymaerax.jar` in Finder, and then right-click on `keymaerax.jar` and select **Open**
- If you are on a Windows machine, try running `java -jar keymaerax.jar` from the command line if double-click does not work.
- If you are on a Linux machine, run `java -jar keymaerax.jar` if double-clicking does not seem to have any effect. You may also need to set the executable bit by running `chmod +x keymaerax.jar`.

You may safely ignore any Java security warnings.

Step 2: Access the KeYmaera X Web User Interface You should have run `java -jar keymaerax.jar` or otherwise launched KeYmaera X. When doing so, you should have seen a loading screen with a progress bar. After a few moments, a web browser window should automatically open the KeYmaera X web-based user interface. If this does not happen, open a web browser and go to <http://127.0.0.1:8090/>.

Is KeYmaera X Running?

KeYmaera X runs in the background. To check if KeYmaera X is running, simply access the web page <http://127.0.0.1:8090> from your web-browser.

Step 3: Register an Account and Log In to KeYmaera X Enter a username and password and press **Register** then choose Learner’s mode. Accept the license agreement and you will be logged in automatically.

Password Security Note: We take standard security precautions with passwords, such as storing them only as a salted hash and using timing attack-resistant hash comparisons. That being said, we do store the salted hash in the home directory of the machine where you ran keymaerax.jar.

If you do not like this, we recommend using a throwaway username and password, such as “guest” and “guest”.

Step 4: Configure KeYmaera X to use Mathematica

Click **Help** and then **Tool Configuration**.

Set the **Arithmetic Solver** to Mathematica.

If you are running KeYmaera X on your own machine, click **Reset to _ default** (where _ is the name of your operating system) next to each of the input boxes. Then, click **Save Configuration**.

It is possible that you will encounter the error message “*Exception: We’re sorry, an internal safety check was violated, which may point to a bug. The safety check reports requirement failed: Initialized tool expected*” at this stage. If that happens, restart KeYmaera X and repeat the above steps. **Note: CMU clusters use a non-default path for Mathematica. For the clusters, use the following paths:**

- MathKernel: /usr/local/depot/mathematica-11.3/Executables/MathKernel
- JLink (make sure to copy both lines of the path): /usr/local/depot/mathematica-11.3/SystemFiles/Links/JLink/Libraries/Linux-x86-64/libJLinkNativeLibrary.so

We tell you to use Mathematica by default because it usually works better than Z3. However, Z3 may also work better once in a while. You can return to this page and select Z3 later if you wish to experiment with it.

Updating KeYmaera X

KeYmaera X is constantly being updated. The current version status is displayed on the footer of any page. Currently, you should see the text **KeYmaera X version 4.7.1 (latest release)** on the footer of any page in the KeYmaera X web UI. Sometimes you will see an update text like:

(version _ is now available from keymaerax.org)

This indicates that your version of KeYmaera X is out of date. Delete your current keymaerax.jar and download the latest release of KeYmaera X from <https://www.ls.cs.cmu.edu/KeYmaeraX/keymaerax.jar>. You do not need to make a new account.

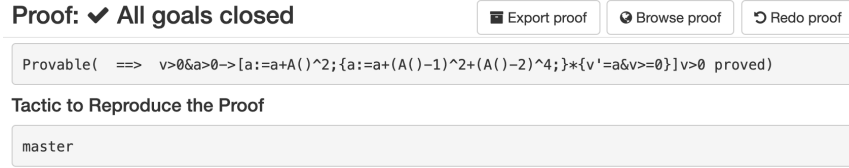




Figure 1: Proof Result dialog for a successful proof.

2 Getting Started with KeYmaera X

Here are a couple of exercises so that you can start getting familiar with KeYmaera X. Download the template files for this lab from: <https://lfcps.org/course/lfcps19/lab0.zip> For subsequent labs, a link to the lab resources will be included at the start of the file. Remember to download and use these for the labs! This lab also contains basic instructions for downloading the `.kx` files that you will use when submitting proofs for the lab assignments. Refer back to this lab if you forget how to export this files in future labs, and take note of the **warnings in bold**.

- **Exercise 1: Prove a property using KeYmaera X and Mathematica.** Load `lab0.kx` (included in `lab0.zip`) into KeYmaera X:
 - Click on `Models` in the menu bar at the top of the page.
 - Click `New Model` and enter a model name (anything will do; e.g., Lab 0 Part 1).
 - Click `Select File` and locate the `lab0.kx` file.
 - Click `Save`.
 - The new model should appear in the list of models. Click the  button in the `Actions` column to start a new proof for this model.
 - Click `▶ Auto`. Wait while the automatic proof search procedure executes. This took a second or two on the TA's machine.
 - Soon a dialog should appear indicating that the procedure succeeded (see Figure 1). From here you can download your work by pressing `Export proof`, which will give you the `.kx` file for your proof. **You need to submit `.kx` files for every KeYmaera X proof that you have done for this course.**
 - If you forget to export the proof when you finish the proof, the same functionality is also available from the `Proofs` screen by clicking the  button next to your proof. **For grading purposes, your `.kx` files should contain exactly one model and one proof.** If you have multiple proofs for a model, make sure to download only the proof that you want to submit from the `Proofs` screen.
 - If for some reason your `.kx` file will not download, see Appendix A for another way to submit assignments in case of emergency. However, that method is harder to grade, so please only do it when absolutely necessary.
 - If the proof automation finishes but the proof is not done yet (i.e. the Proof Result dialog does not appear), this probably means Mathematica is not configured correctly. Make sure Steps 1 through 4 were completed correctly.
- **Exercise 2: Finding counterexamples with KeYmaera X.** Think of the formula $\forall x(x > 0 \wedge x < 1)$, i.e., for all real numbers x , x is greater than 0 and x is smaller than 1. Is this formula valid? If not, why? Can you find a counterexample? Counterexamples are assignments of variables that falsify

the formula, and therefore the existence of a counterexample implies the formula is false. KeYmaera X prefers to check whether formulas are true, so it won't try to find a counterexample unless we ask for it explicitly.

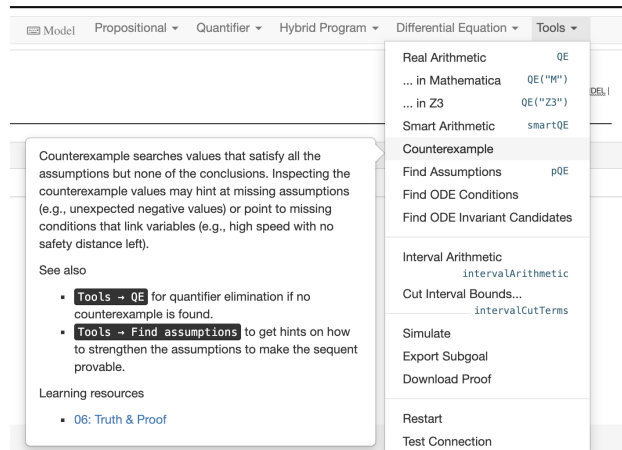


Figure 2: Dropdown menu from `Tools ▾`.

- Create a new model from `lab0-forall.kyx` in KeYmaera X. Start a new proof for the model.
 - Explore the interface. Select the whole formula by hovering the mouse over the $\forall x$.
 - To find a counterexample, click `Tools ▾` and select `Counterexample`. A window should pop up with a counterexample. Make sure that the counterexample that KeYmaera X found is indeed a counterexample.
 - Write the generated counterexample in `lab0.txt`.
- **Exercise 3: Write a formula yourself.** Create a new file called `lab0-transitivity.kyx`. Using KeYmaera X's syntax from the cheatsheet¹ and the `lab0-forall.kyx` example, write down the following formula that expresses transitivity of $>$ for the real numbers.

$$\forall x (\forall y (\forall z ((x > y \wedge y > z) \rightarrow x > z)))$$

A template file is included with the code handout for this assignment in `lab0-transitivity.kyx`. After filling out the template with your answer, load your new `lab0-transitivity.kyx` file into KeYmaera X and make sure that it parses correctly. Complete the proof as you did in Exercise 1 with `▶ Auto` and generate the corresponding `.kyx` file.

- **Exercise 4: Semantics for First-Order Logic.** For each of the formulas below, write in `lab0.txt` whether the formula is unsatisfiable, (just) satisfiable, or valid, and briefly explain why. If you wish, check your work in KeYmaera X using the features you just learned.

1. $\exists y xy = 1$
2. $\forall x \exists y xy = 1$

¹<http://keymaerax.org/KeYmaeraX-sheet.pdf>

3 Submission Instructions

We will use Autolab (<https://autolab.andrew.cmu.edu/courses/15424-f19/>) for all submissions in this course. When submitting a lab assignment, you will receive a *preliminary* binary grade (0/1). If you receive a score of 0, it means there was some error in your submission – a missing file, a file that KeYmaera X could not parse, etc. If you receive a score of 1, then your submission is in valid form. The Autolab binary score indicates whether your submission is valid and *does not* necessarily indicate your final grade on the lab! Your final submission for Lab 0 should be in the form of **a single .zip file** containing these 3 files:

lab0.kyx – The proved archive for the model lab0.kyx distributed with this lab. This contains the model and proof from Exercise 1.

lab0-transitivity.kyx – The proved archive for your answer and proof for Exercise 3.

lab0.txt – A text file containing answers to the written questions (Exercises 2 and 4).

At the top of each of your .kyx files, create a comment that says how long the tactic for your proof takes to run and whether the proof closes. The template is already included in the .kyx files distributed with this assignment. For example:

```
/**
 * Running time (in minutes, estimate): 2 mins
 * Proved? (Y/N): Y
 * KeYmaera X Version: 4.7.1
 * ...more comments here...
 */
```

This comment block should be included in all .kyx files you submit in this course. Please do not include any personally identifiable information in your submission. This way it is easier for us to grade anonymously and reduce implicit grading bias. Autolab already knows who you are so there is no need to say so in your submission.

4 Installation FAQ

We know this is new software, and all new software has bugs. We want you to be able to spend as much of your time as possible focusing on the assignment instead of dealing with bugs, so please reach out to us when something seems broken and we will respond as quickly as possible. Finally, please ask for help from your TAs during installation! You may also share tips on installing and upgrading KeYmaera X with (and ask for help from) your fellow students. (However, remember that sharing the specifics of lab solutions with other students does violate the academic integrity policies of the course.)

A Database Extraction

Submitting your archive should work fine, but in case of bugs, here is an alternate, older method. Please only use this if the prior method does not work because this is harder to grade. Every proof you do in KeYmaera X, including all your intermediate scratch work, is stored in an SQLite database, which is located in a subdirectory of your home directory: `.keymaerax/keymaerax.sqlite` Submit this file in case of emergency. Do not forget to submit any other files that are not .kyx files: those are not stored in the database. Autolab will tell you that your submission is bad because this is not the intended submission format, but we will have your file on our Autolab and be able to grade it.