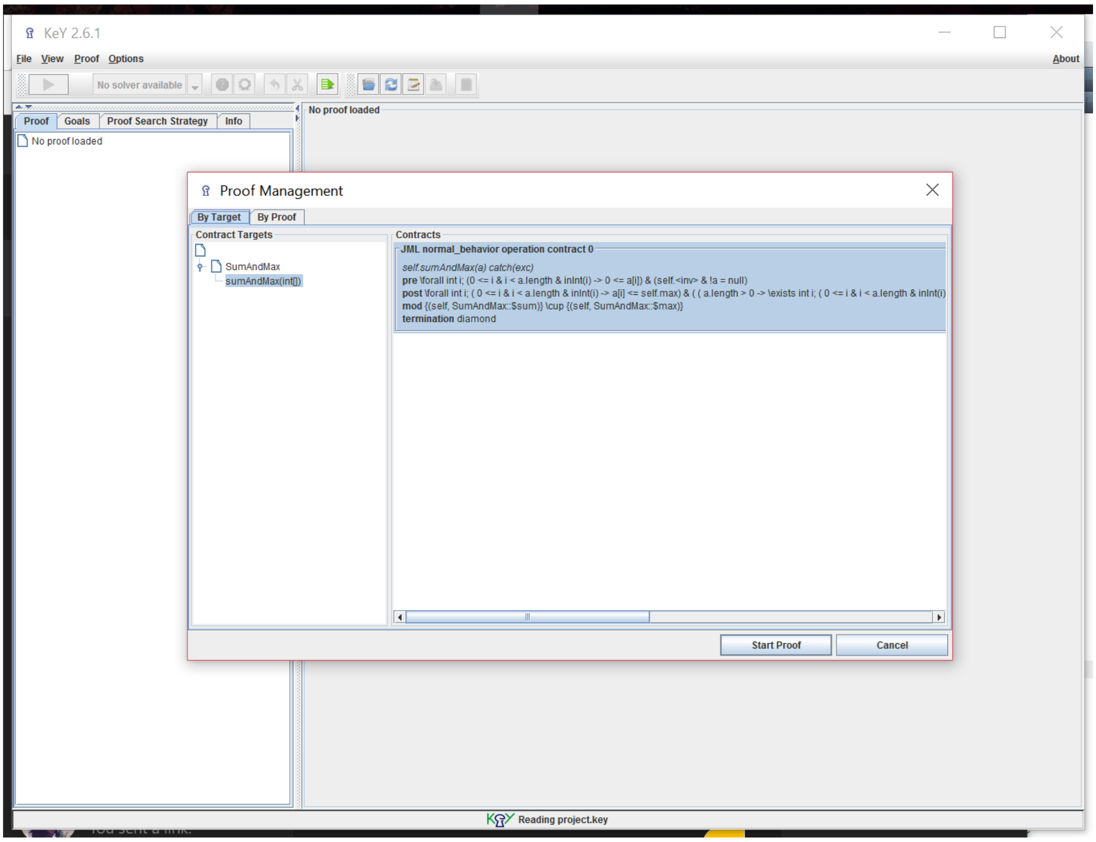
SaDS HW 3

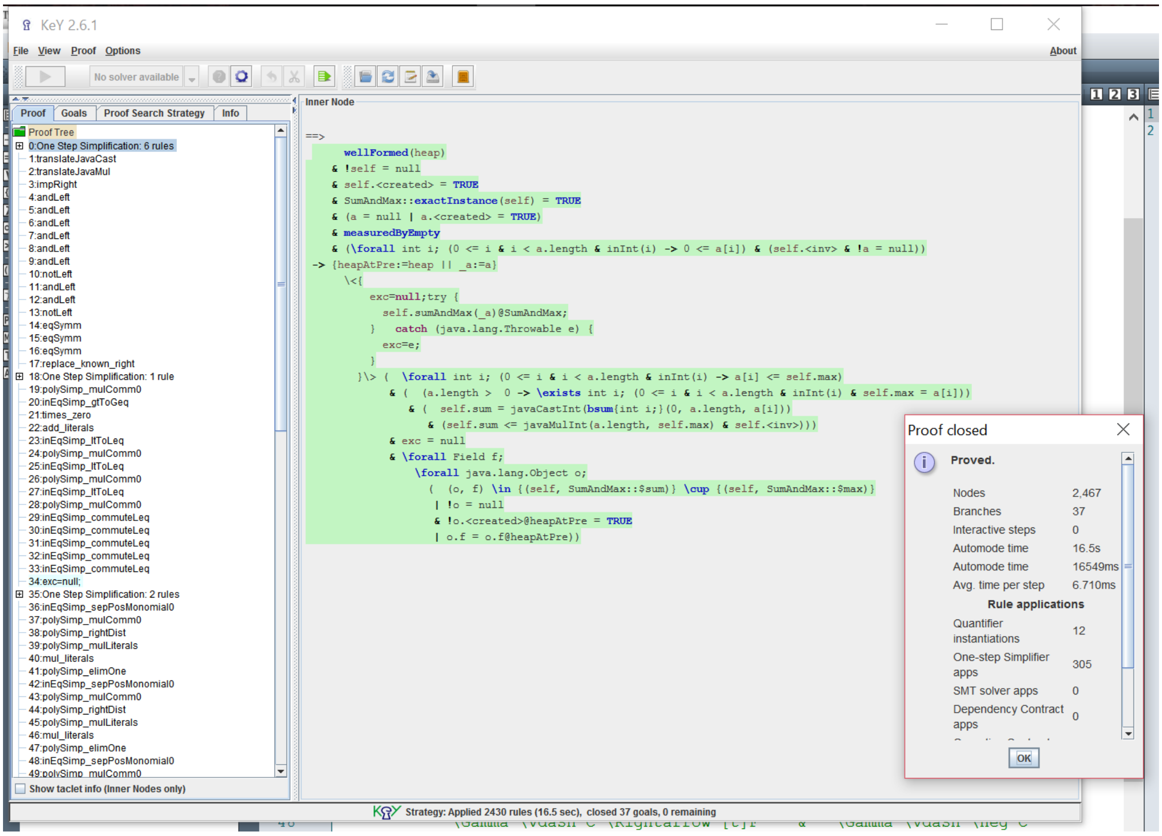
Inti Mendoza

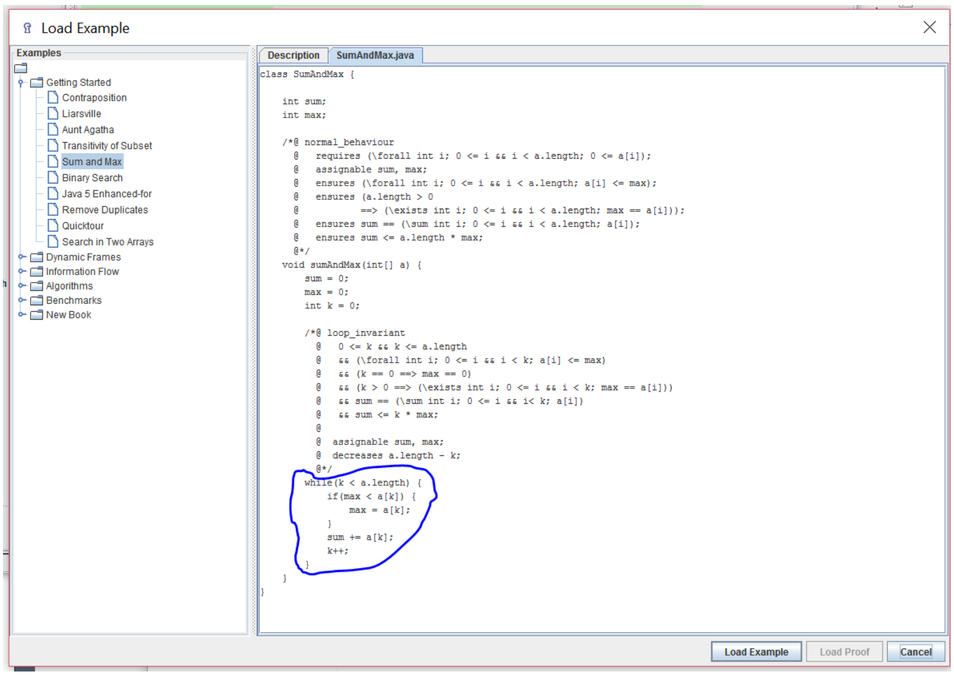
Problem 4.1

- Factorial
  - Precondition $P(n)$ is $n \geq 0$
  - Postcondition $Q(n, x)$ is $n \leq x$
  - Loop invariant I is $product = (factor - 1)!$
  - Termination orderings is given by $(n - 1)!n$
- revertImmutable
  - Precondition $P(x)$ is $x \neq \emptyset$
  - Postcondition $Q(x, rev)$ is $|x| = |rev|$
  - Loop invariant I is $|rest| = |x| - |rev|$
  - Termination ordering is given by $rest = \emptyset$

Problem 4.2







Problem 4.3

- Proof for soundness of **if**

From lecture notes, C is assumed to be pure. Hence, when used in **if**, every possible outcome has to be true - defined in every state. **if** produces two cases. When $C == true$ and $C == false$.

In the rule for **if** :

$$\frac{\Gamma \vdash C \Rightarrow [t]F \quad \Gamma \vdash \neg C \Rightarrow [t']F}{\Gamma \vdash [\textbf{if } (C)\{t\} \textbf{ else } \{t'\}]F}$$

C is allowed two states - the states possible by definition of **if** and is defined in both of them.

$\therefore$ **if** is sound.

- Proof for soundness of **while**

  From lecture notes, C is assumed to be pure. Hence, when used in **while**, every possible outcome has to be true - defined in every state. **while** has the loop invariant attribute.

  In the rule for **if** :

  $$\frac{\Gamma \vdash I \quad \Gamma * \vdash (I \wedge C) \Rightarrow [t]I \quad \Gamma \vdash (I \wedge \neq C) \Rightarrow F}{\Gamma \vdash [\textbf{while} C\{t\}]F}$$

  The loop invariant is defined as true before and after **while** starts for whatever C.

  $\therefore$ **while** is sound.