

# Assignment 4

March 21, 2018

## $k$ -induction

In class and notes,<sup>1</sup> we discussed  $k$ -induction as a technique for proving validity of a Hoare triple. You are to implement the  $k$ -induction algorithm using the Z3 SMT solver.

Your implementation should take a Hoare triple:

$$\{\phi\} \text{ while } b \text{ do } P_{body} \{\psi\}$$

Given a value  $k \geq 1$ , your implementation should perform  $k$ -induction, returning “success” if  $k$ -induction succeeds, and “failure” otherwise.

*Your implementation can take the program as two formulas,  $b$  and  $\text{enc}(P_{body})$ .* So you do not have to parse the program and encode automatically for this assignment.

- It is highly recommend that you use the Python API of the Z3 SMT solver ([github.com/Z3Prover/z3](https://github.com/Z3Prover/z3)). Z3 has other language bindings, but Python is the easiest to prototype with and will make you most productive.
- You are expected to **exhaustively comment your code** and describe what parts of  $k$ -induction you are implementing.
- You should encode three non-trivial Hoare triples. All examples you provide should be valid Hoare triples. One of the Hoare triples should require  $k \geq 2$  for the induction to succeed. Explain the programs you provide. For the example where  $k \geq 2$  is required, explain why  $k = 1$  is insufficient. It is OK for your examples to be hard-coded.
- Provide a valid Hoare triple for which  $k$ -induction cannot prove correctness for any value of  $k$ . Argue why that is the case.
- Note: In the notes, we encoded sequential composition with an existential quantifier. The quantifiers are not needed when checking validity, as is done in  $k$ -induction, so you do not need them.

---

<sup>1</sup><https://github.com/barghouthi/cs704/blob/master/notes/transRelEnc.pdf>