Chris Cargile - February 7, 2014 CSCI658 - Testing and Maintenance

HOMEWORK ASSIGNMENT: CHAPTER 8

Question 8.1:
Finite state verification falls between basic flow analysis and formal verification in power and cost, but it also often designed to provide results that are tantamount to formal proofs of program properties. Are these two statements contradictory? If not, how can a technique that is less powerful than formal verification produce results that are tantamount to formal proofs?

Response:
While formal proofs of program properties would generally be more costly to produce to human-intensive labor they require, more than any other technique for verifying program properties, as a technique is it generally not the optimal choice for a variety of reasons. Due to the notion that formal proofs may be neither pragmatic nor adaptable or valid amidst changing conditions a program is designed to run against, more flexible techniques may be more suitable – aside from the lessened computation strain imposed by other, less intensive techniques to verifying properties.

On the other hand, basic flow analysis may be too simplistic a technique to produce a report that affords much confidence as to predictability of non-failure when the program is run against 'in-the-wild' conditions. A technique that verifies program properties, confronting conditions at an appropriate level of abstraction, which may well be beyond the level of control effected by program logic itself – such as verifiability concerns resulting from the JVM/compiler – may be the most reasonable and optimal compromise during the technique selection process. Whereas a mathematical proof may be sufficient to ensure there exists a means for two processes to coexist, in parallel, without affecting one another in theory, a non-formal proof afforded by finite state verification may additionally guarantee outcomes tailored to the environmental conditions affecting a program's executions, so may be superior and less resource-hungry, simultaneously. Therefore, it is not contradictory to assert the circumspect claim above.

Question: 8.4:
A property like 'if the button is presed, then eventually the elevator will come" is classified as a liveness property but 'if the button is pressed, then elevator will arrive <=30sec.' is technically a safety property, as opposed to a liveness property. Why is that?

Response:
The immediately apparent answer is that in accordance with the author's definitions and descriptions of liveness and safety properties, the existence of a 'finite' approximation as to the elevator's expectancy to arrive confirms the type of property to be a safety property. More technically, there is likely some justification that ties finite state verification. This question has challenged me to further explore the nature of finite state verification to aid me in gaining a fuller comprehension of its applicability and means for achieving it in practice.