Introduction to Software Analysis

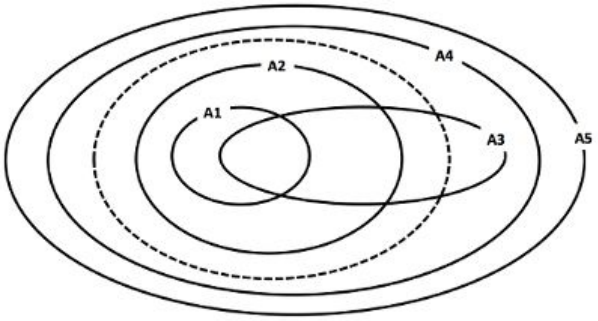
Question 1. Static vs. Dynamic Analysis

a. State one advantage of static analysis over dynamic analysis.

b. State one advantage of dynamic analysis over static analysis.

Question 2. We may classify each program as either safe or unsafe. For instance, we may say that a program is safe if it does not dereference a null pointer in any execution, and unsafe if there exists an execution in which it will dereference a null pointer.

A software analysis is considered sound if whenever it reports a program as safe, the program is indeed safe. However, due to the undecidability of software analysis, a sound analysis may reject some safe programs. A sound analysis A is more precise than a sound analysis B if whenever analysis B accepts a program, analysis A also accepts that program.



Consider the above figure. Inside of the dotted (---) oval lies the set of all safe programs, and the outside of the oval denotes the set of all unsafe programs. The inside of each solid oval, labeled A1 through A5, denotes the set of programs accepted by the corresponding analysis (e.g., these are five different null dereference checking analyses). Each analysis rejects all programs outside its corresponding oval.

Which of these five analyses are sound? List the sound analyses ordered by precision, i.e A6 > A7 > A8 indicates that A6, A7, and A8 are all sound, and A6 is more precise than A7, which is more precise than A8.