

Problems:

- 1. path coverage guarantee
- 2. sensitive analysis guarantee

Constraints:

- 1. language extensibility
- 2. performance (minimize the instrumentation)



- 1. get the block-level CFG of a function, encode each CFG node as a block ID
- 2. the CFG is language-independent, satisfying the constraint 1.
- 3. apply the instrumentation algorithm on the CFG to compute PCG guidance, satisfying the constraint 2.
- 1. define a language-independent IR to retain the necessary information for SAG, satisfying the constraint 1.
- 2. extend the block-level CFG to instruction (or statement)-level CFG: each node represents a statement in IR
- 3. Def-Use computation on the use of each CMP and SWITCH node of the CFG: get the definition statement for each branch variables as SAG
 - 4. merge SAG and PCGG, satisfying the constraint 2.





