1. InstrumentReturn (call instruction?)vs instrumentBranch
2. If you find a `Predicate(line=3, column=5, pred\_type="BranchTrue")`
3. in the log, then you have observed it as True,
4. further it also means you've observed is complement:
5. `Predicate(line=3, column=5, pred\_type="BranchFalse")` as False.
6. What about -? (branch, return
7. Dict[Predicate, ObservationStatus]

What is the predicate type?

Do we need to filter the predicates?(apply sampling algo, geometric distribution?) No

Where does sampling process happen? Instrumentation? During run time dynamic analysis.

Do we need to cast to branch instruction?

Why input0.cbi.jsonl

For each input? Do we need to run cbi for all inputs to get P?

P==0 63 there are 63 runs p==0 occurrences nothing to do with fail/sucess

Single run? Predicates true/false/both collectobservations

2.1 1

2.2 1

2.3 1

2.4 1

3.1 2

3.2 2

4 3

rm -rf fuzz\_output\_test3 **&&** mkdir fuzz\_output\_test3

timeout 1 fuzzer ./test3 fuzz\_input fuzz\_output\_test3 10

cbi ./test3 ./fuzz\_output\_test3

opt -load ../build/CBIInstrumentPass.so –CBIInstrumentPass test2.ll

rm -rf fuzz\_output\_test2 **&&** mkdir fuzz\_output\_test2

timeout 1 fuzzer ./test2 fuzz\_input fuzz\_output\_test2 10

cbi ./test2 ./fuzz\_output\_test2

return value of Callinst how to determine the return value? 20:24

branch true/false of BranchInst

BrachInst VS cmpInst