Detected non-deterministic results when --jobs is not set to 1

Open · 4 tasks

Hi, I have recently been using Infer for an empirical study to detect non-deterministic behaviors in static analyzers. The experiments resulted in discovering some nondeterministic analysis results across multiple runs under various configurations of Infer.

- [ ] The version of Infer I used is `v1.1.0`.
- [ ] The operating system is `ubuntu:20.04` and I am using Docker.
- [ ] I ran Infer on 20 sampling configurations. The base command I used is `infer --compilation-database compile_commands.json` with following checkers on `--annotation-reachability --bufferoverrun --cost --loop-hoisting --pulse`, as well as these options used `--dump-duplicate-symbols --headers --max-nesting --jobs --reactive --scheduler`.
- [ ] I ran Infer on each program-configuration combination 5 times and compared the results across 5 runs for detecting non-deterministic behaviors. The program I used is openssl. And the nondeterministic results are found under the configurations shown below. As observed, these nondeterminism all happen when the `--jobs` option is not set to 1.

dump-duplicate-symbols	headers	max-nesting	jobs	reactive	scheduler
1	1	100	10	0	file
1	0	1	50	0	restart
0	0	100	50	1	callgraph
0	1	5	20	0	callgraph
0	1	1	5	1	callgraph
1	1	10	50	0	file
0	0	100	20	1	file
1	1	10	5	1	restart
1	0	1	20	1	restart
0	0	5	10	0	restart
0	1	10	10	0	file
1	0	5	5	0	file
0	0	10	10	0	callgraph

For example, here are some different results from the running Infer under the same configuration `--headers --max-nesting 1 --jobs 5 --reactive --scheduler callgraph`.

result 1:

```
Found 4354 issues
                                  Issue Type(ISSUED_TYPE_ID): #
                      Integer Overflow L2(INTEGER_OVERFLOW_L2): 1302
                          Buffer Overrun L3(BUFFER_OVERRUN_L3): 1163
                                    Memory Leak(MEMORY_LEAK): 602
                                      Dead Store(DEAD_STORE): 401
              Inferbo Alloc May Be Big(INFERBO_ALLOC_MAY_BE_BIG): 300
                                 Null Dereference(NULL_DEREFERENCE): 145
                          Buffer Overrun L2(BUFFER_OVERRUN_L2): 144
                      Uninitialized Value(UNINITIALIZED_VALUE): 99
                      Integer Overflow L1(INTEGER_OVERFLOW_L1): 92
                          Buffer Overrun L1(BUFFER_OVERRUN_L1): 71
                          Buffer Overrun S2(BUFFER_OVERRUN_S2): 22
                      Nullptr Dereference(NULLPTR_DEREFERENCE): 6
  Expensive Loop Invariant Call(EXPENSIVE_LOOP_INVARIANT_CALL): 4
                     Inferbo Alloc Is Big(INFERBO_ALLOC_IS_BIG): 2
                                Unreachable Code(UNREACHABLE_CODE): 1
```

result 2:

```
Found 4355 issues
                                  Issue Type(ISSUED_TYPE_ID): #
                      Integer Overflow L2(INTEGER_OVERFLOW_L2): 1302
                          Buffer Overrun L3(BUFFER_OVERRUN_L3): 1163
                                    Memory Leak(MEMORY_LEAK): 603
                                      Dead Store(DEAD_STORE): 401
              Inferbo Alloc May Be Big(INFERBO_ALLOC_MAY_BE_BIG): 300
                                 Null Dereference(NULL_DEREFERENCE): 145
                          Buffer Overrun L2(BUFFER_OVERRUN_L2): 144
                      Uninitialized Value(UNINITIALIZED_VALUE): 99
                      Integer Overflow L1(INTEGER_OVERFLOW_L1): 92
                          Buffer Overrun L1(BUFFER_OVERRUN_L1): 71
                          Buffer Overrun S2(BUFFER_OVERRUN_S2): 22
                      Nullptr Dereference(NULLPTR_DEREFERENCE): 6
  Expensive Loop Invariant Call(EXPENSIVE_LOOP_INVARIANT_CALL): 4
                     Inferbo Alloc Is Big(INFERBO_ALLOC_IS_BIG): 2
                                Unreachable Code(UNREACHABLE_CODE): 1
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

Notifications

Unsubscr

You're receiving notifications beca
thread.

result 3:

```
Found 4353 issues
                                Issue Type(ISSUED_TYPE_ID): #
                    Integer Overflow L2(INTEGER_OVERFLOW_L2): 1302
                        Buffer Overrun L3(BUFFER_OVERRUN_L3): 1163
                                Memory Leak(MEMORY_LEAK): 602
                                  Dead Store(DEAD_STORE): 401
            Inferbo Alloc May Be Big(INFERBO_ALLOC_MAY_BE_BIG): 300
                              Null Dereference(NULL_DEREFERENCE): 144
                        Buffer Overrun L2(BUFFER_OVERRUN_L2): 144
                    Uninitialized Value(UNINITIALIZED_VALUE): 99
                    Integer Overflow L1(INTEGER_OVERFLOW_L1): 92
                        Buffer Overrun L1(BUFFER_OVERRUN_L1): 71
                        Buffer Overrun S2(BUFFER_OVERRUN_S2): 22
                    Nullptr Dereference(NULLPTR_DEREFERENCE): 6
  Expensive Loop Invariant Call(EXPENSIVE_LOOP_INVARIANT_CALL): 4
                  Inferbo Alloc Is Big(INFERBO_ALLOC_IS_BIG): 2
                              Unreachable Code(UNREACHABLE_CODE): 1
```

Could you please offer some insights into this issue and suggest ways to mitigate the non-deterministic behavior when running Infer with multiple jobs? Thank you.

Author

Hello Infer team, I'm following up on this issue and would greatly appreciate any insights you could provide. Thank you!

Member

Hi, it is indeed a known issue. Several fixes have landed on master since the 1.1 release (we ought to do one soon), so I would suggest:

- trying master
- disabling biabduction (if not already)
- using the restart scheduler
- code with recursive functions may still exhibit non-determinism.