Snagle: A lightweight sparse conditional null pointer and unreachable code analysis

Gang Fan, Charles Zhang

香港科技大學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

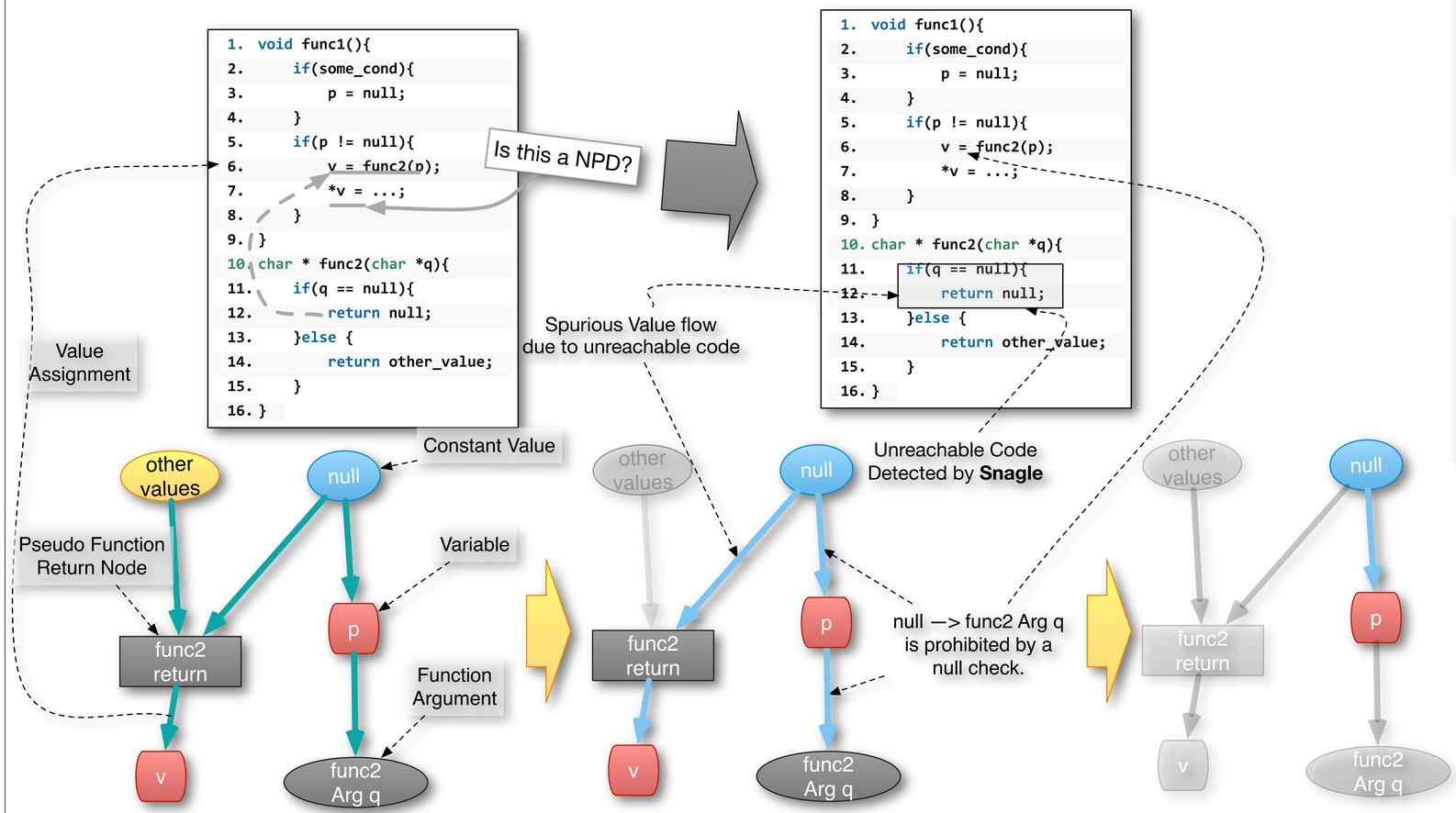
THE DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
計算機科學及工程學系

Motivation

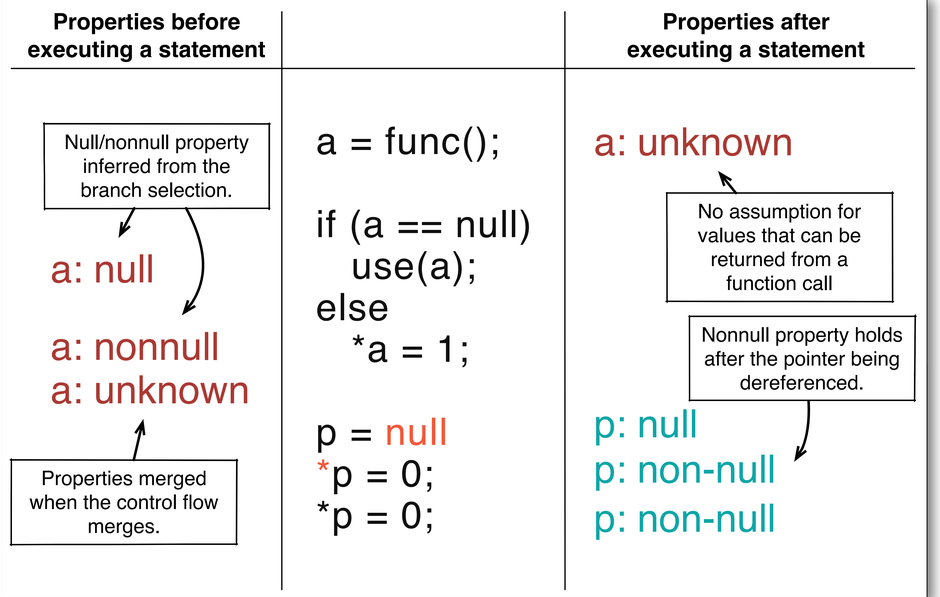
- Path sensitive bug detection tools can be very **precise** but highly **expensive**.
- Expensive algorithms waste too much time on **easy cases.**
- Many bug candidates could be easily pruned with **less precise but more efficient** algorithms.
- We propose an algorithm named **Snagle** that is efficient and powerful enough to prune most candidates in practice.

Iterative VS Worklist(Snagle)

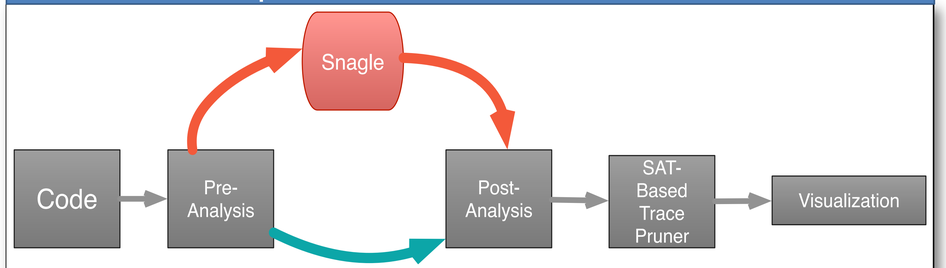
- Two methods for combining NCA and NFA:
- **Iterating NCA and NFA until a fixed point is reached.**
  - Easy to implement
  - Any status changes lead to a whole program re-computation.
  - Inefficient if a value flow can be terminated earlier.
- **Using worklists (Snagle)**
  - Only do re-computation for parts that are changed.
  - Fast termination if a value flow is guarded by a check.



Null Check Analysis (NCA)



Implementation and Evaluation



Project	Instruction Count	Without Snagle(s)	With Snagle(s)	Speedup
ELFedit	3961	30.90	0.56	**55.2✕**
Pbzip2	3648	1.06	0.86	**1.2✕**
Memcached	16239	847.00	53.00	**16.0✕**
Lighttpd	41018	281.60	25.80	**10.9✕**
Tar	86303	>3600.00(Timeout)	22.14	**>162.6✕**
Transmission	121638	654.80	25.15	**26.0✕**

Contact Me!

Email: gfan@cse.ust.hk

Web: www.cse.ust.hk/~gfan