

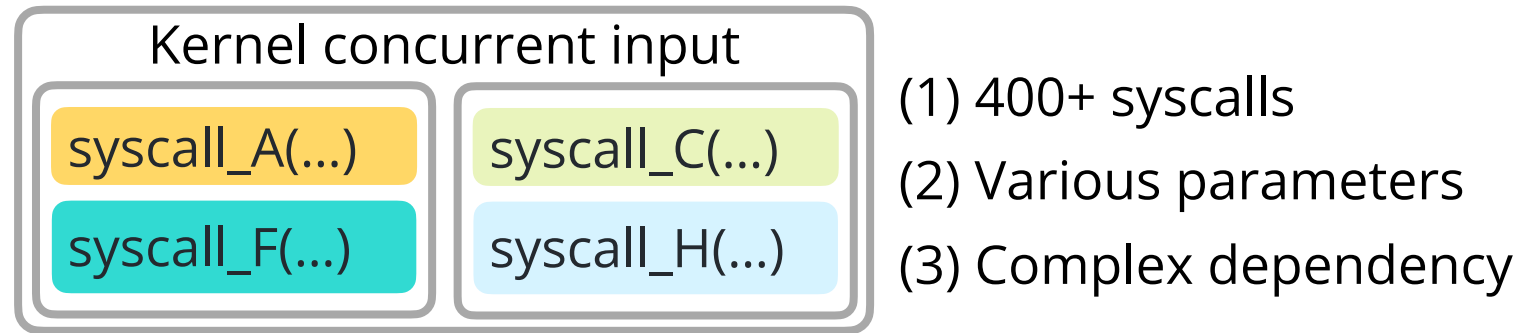
Snowboard: Finding Kernel Concurrency Bugs through Systematic Inter-thread Communication Analysis

Sishuai Gong (Purdue University)
Pedro Fonseca (Purdue University)

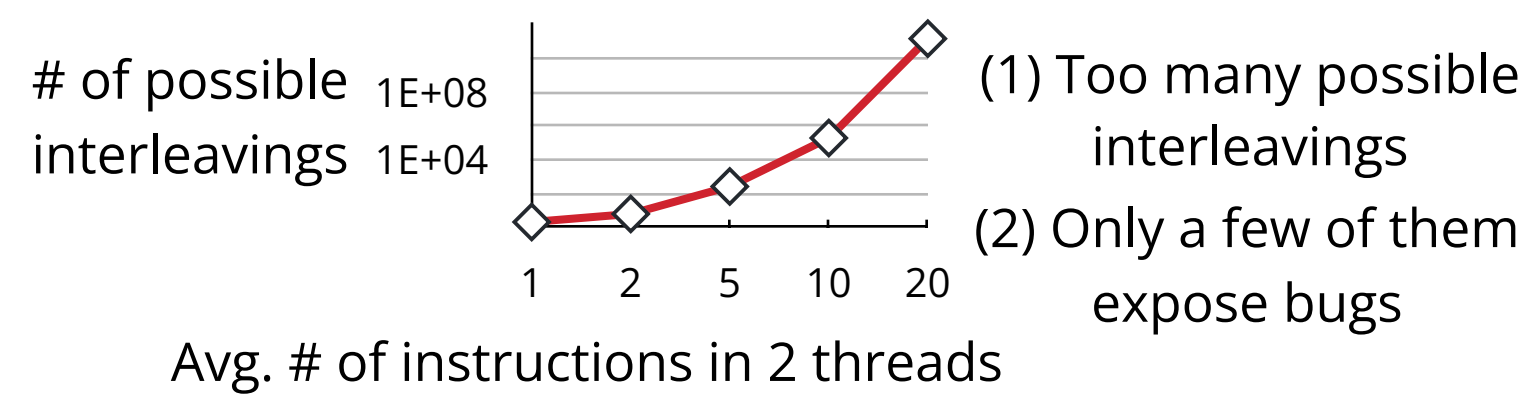
Deniz Altınbüken (Google Research)
Petros Maniatis (Google Research)

Problem and Key Idea

1. Massive concurrent input space

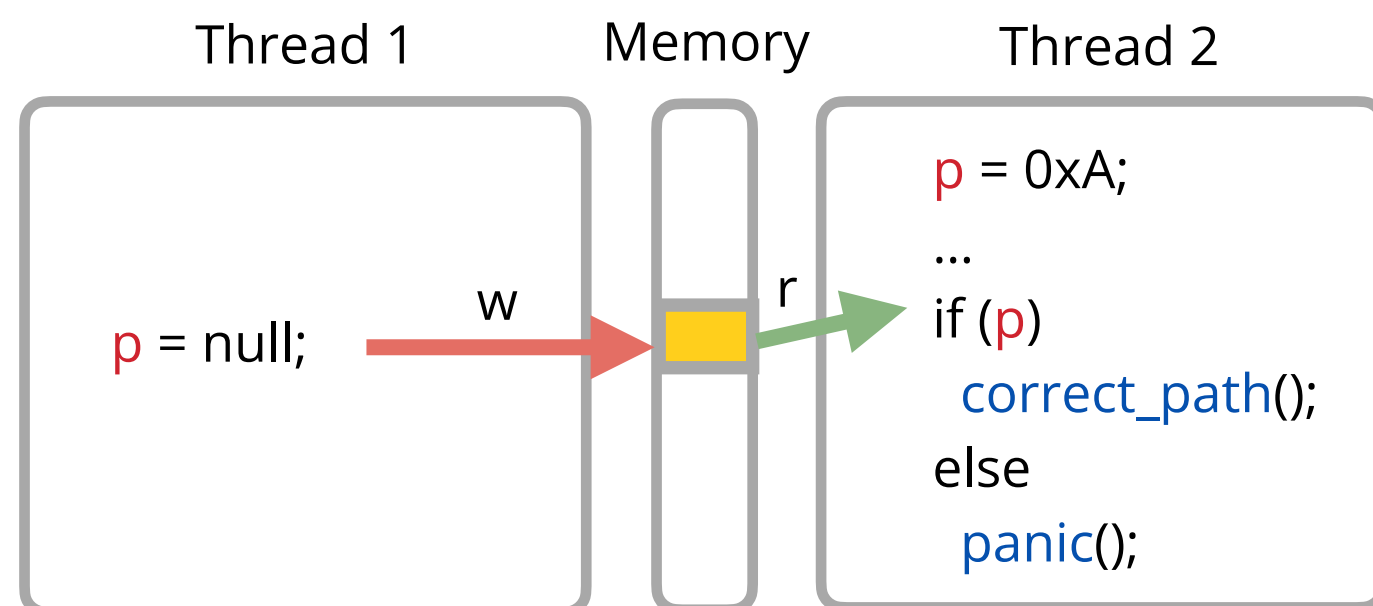


2. Extensive interleaving space



Potential Memory Communication (PMC)

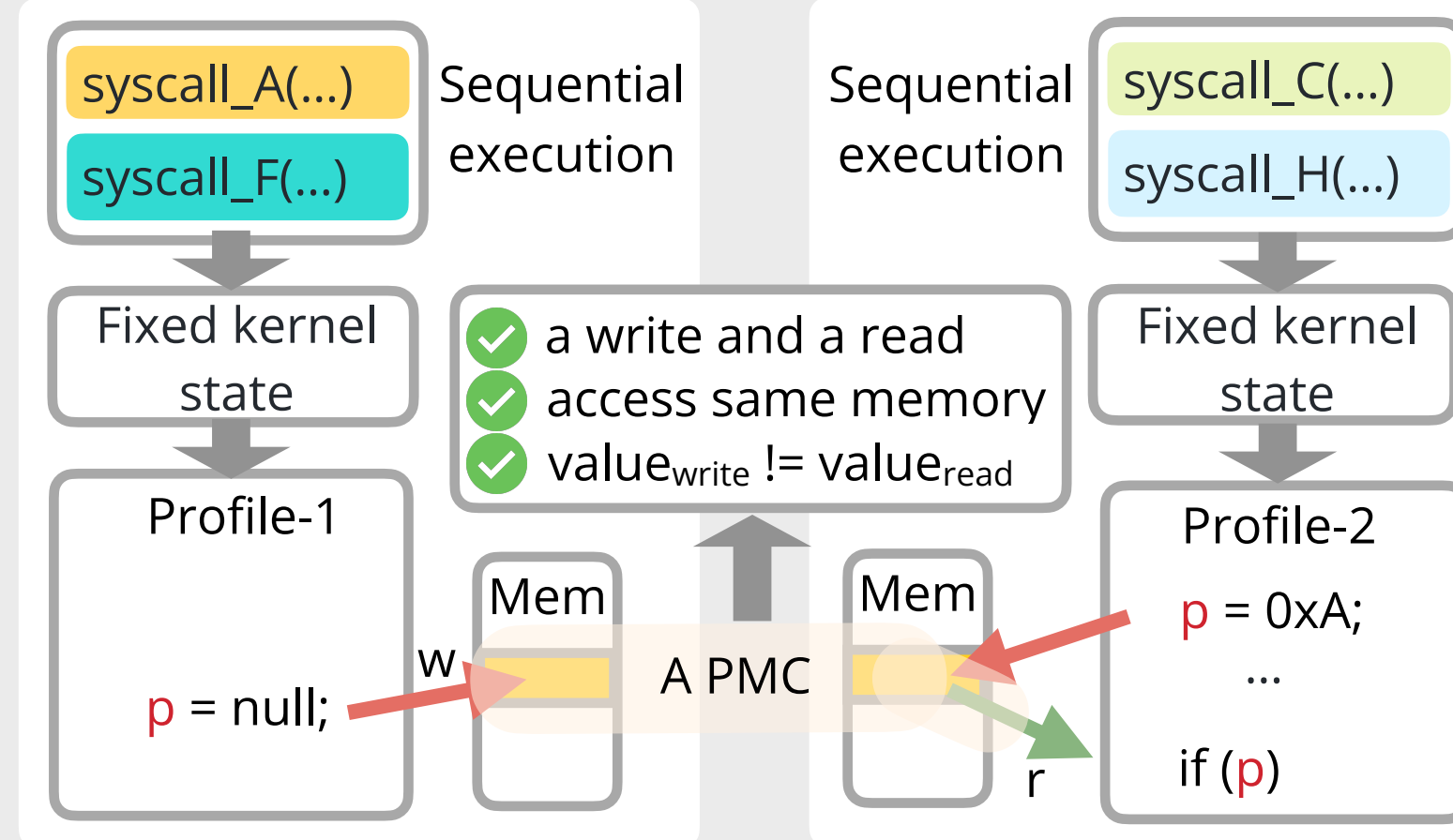
Testing PMCs reveals concurrency bugs



Pair of write and read accesses to shared resources by different write and read values

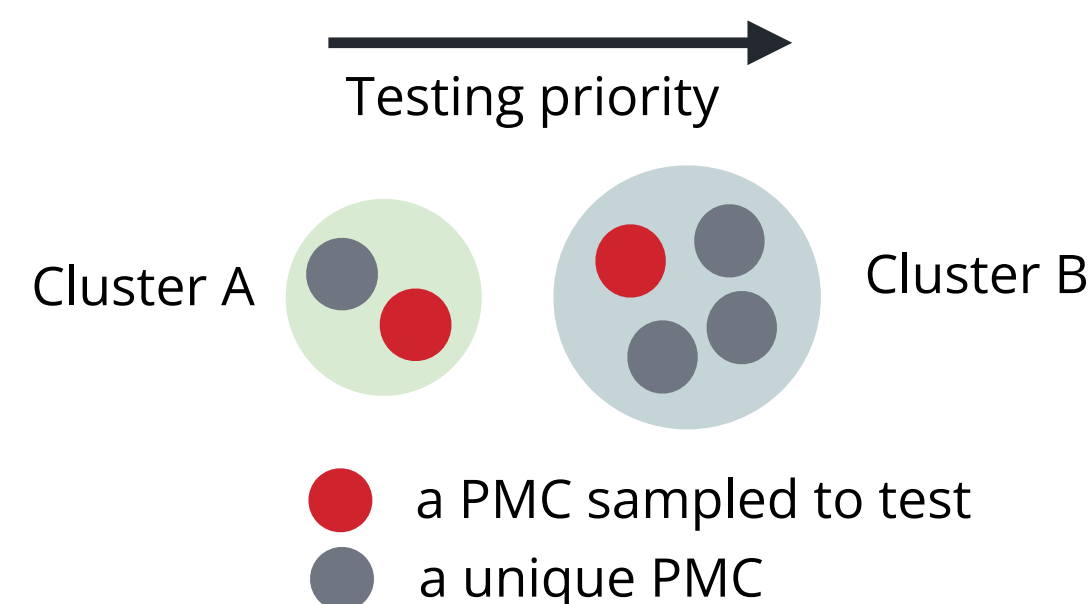
Approach

1. Find PMCs



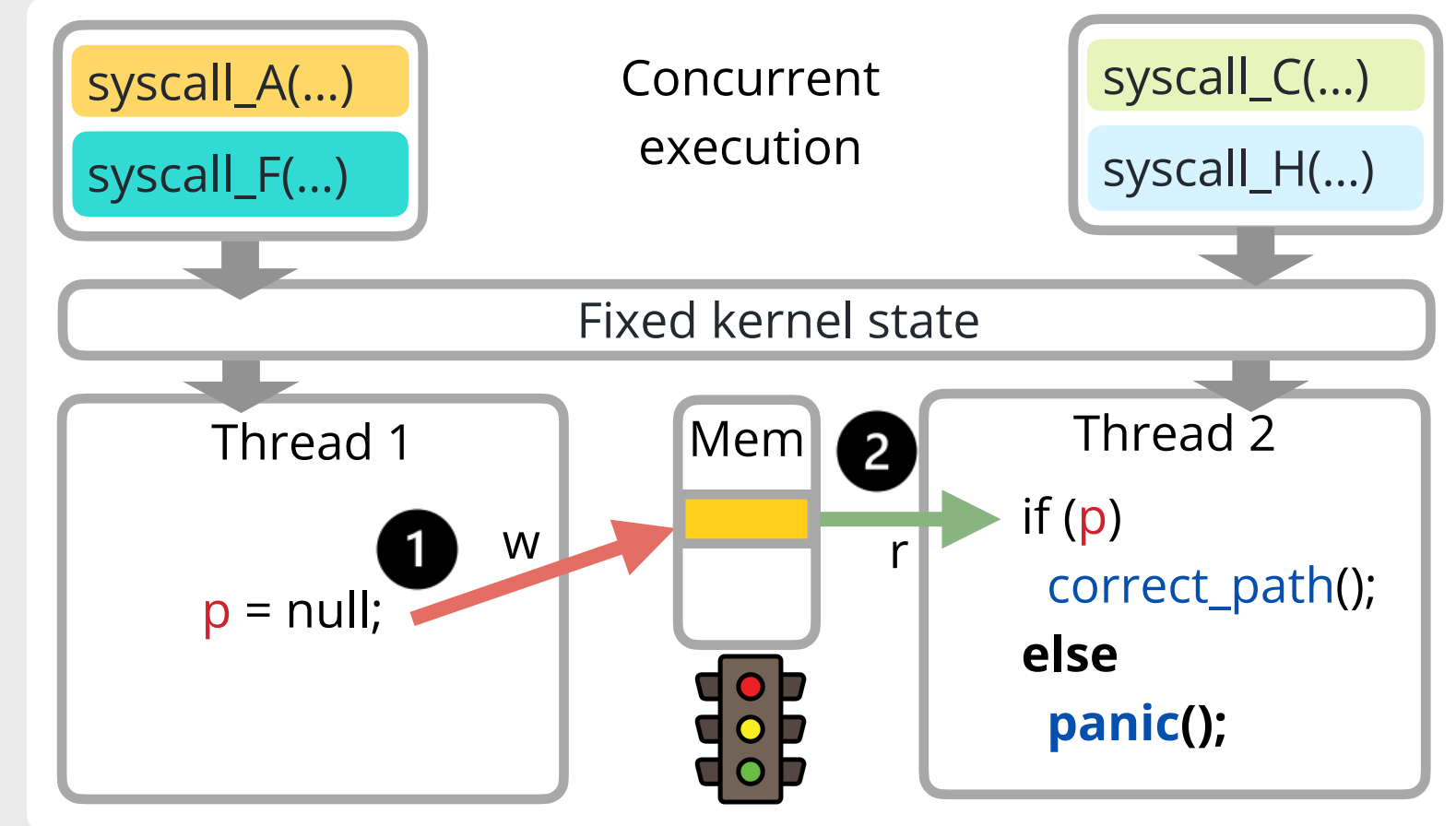
2. Prioritize PMCs

- 1 Cluster similar PMCs
- 2 Prioritize smaller clusters
- 3 Sample a PMC from each cluster

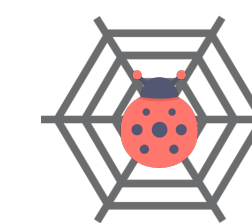



Approach (cond.)

3. Test PMCs



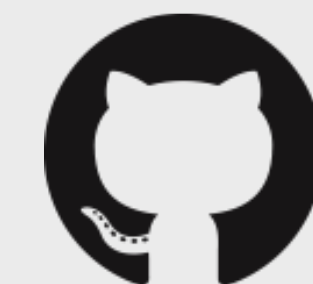
Impact



Effective in finding new kernel concurrency bugs hat 

- had serious impact (e.g., panics)
- existed for years (e.g., 10 years)

Artifact



<https://github.com/rssys/snowboard>