**Problem and Key Idea**

1. **Massive concurrent input space**
   - 400+ syscalls
   - Various parameters
   - Complex dependency

2. **Extensive interleaving space**
   - Too many possible interleavings
   - Only a few of them expose bugs

**Potential Memory Communication (PMC)**

- Testing PMCs reveals concurrency bugs

**Approach**

1. **Find PMCs**
   - syscall_A(…)
   - syscall_C(…)
   - syscall_F(…)
   - syscall_H(…)

2. **Prioritize PMCs**
   - Cluster similar PMCs
   - Prioritize smaller clusters
   - Sample a PMC from each cluster

**Approach (cond.)**

3. **Test PMCs**
   - syscall_A(…)
   - syscall_C(…)
   - syscall_F(…)
   - syscall_H(…)

**Impact**

Effective in finding new kernel concurrency bugs that:
- Had serious impact (e.g., panics)
- Existed for years (e.g., 10 years)

**Artifact**

https://github.com/rssys/snowboard