Non-race concurrency bug detection through order-sensitive critical sections

Non-Race & Order-sensitive critical section

- A pair of critical section that can lead to non-deterministic shared memory state depending on the order in which they execute.

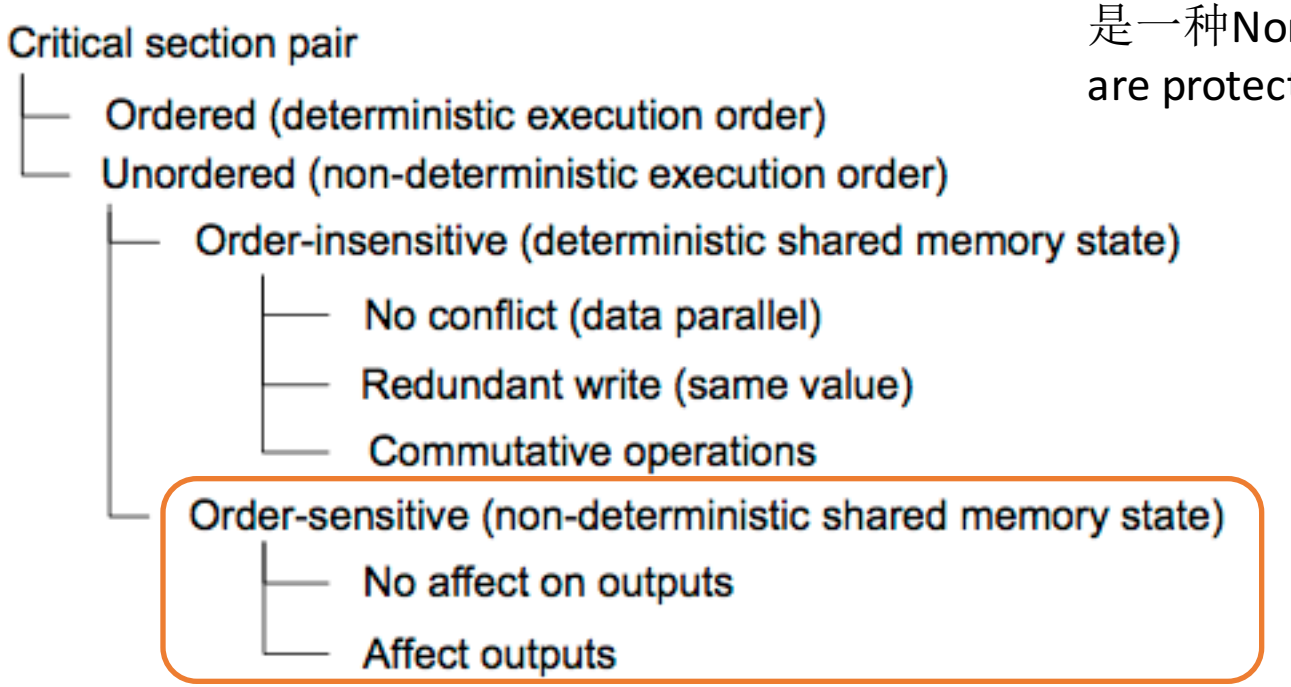
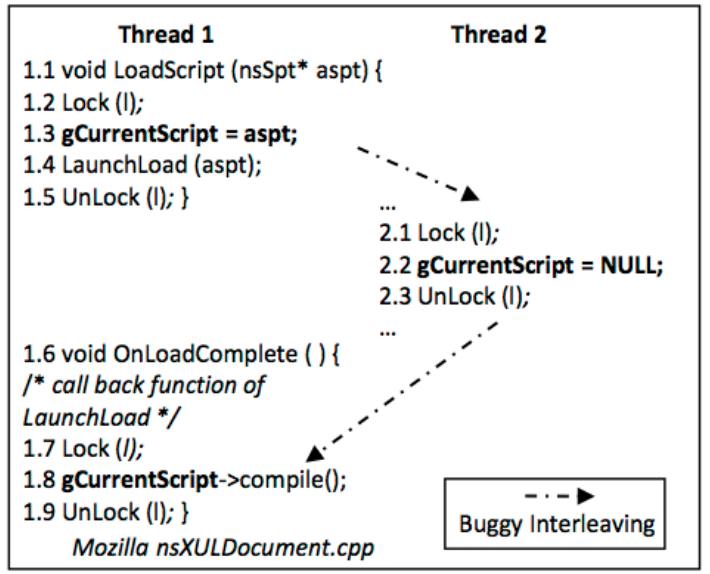


Figure 2: Types of critical section pairs.

是一种Non-race bug，因为memory access at same location are protected by mutex, 所以并没有存在data-race



(c) Order-sensitive critical section pair. Non-race atomicity violation bug (Mozilla-1) [11].

How to detect OSCS

- Filter our ordered and order-insensitive critical sections.

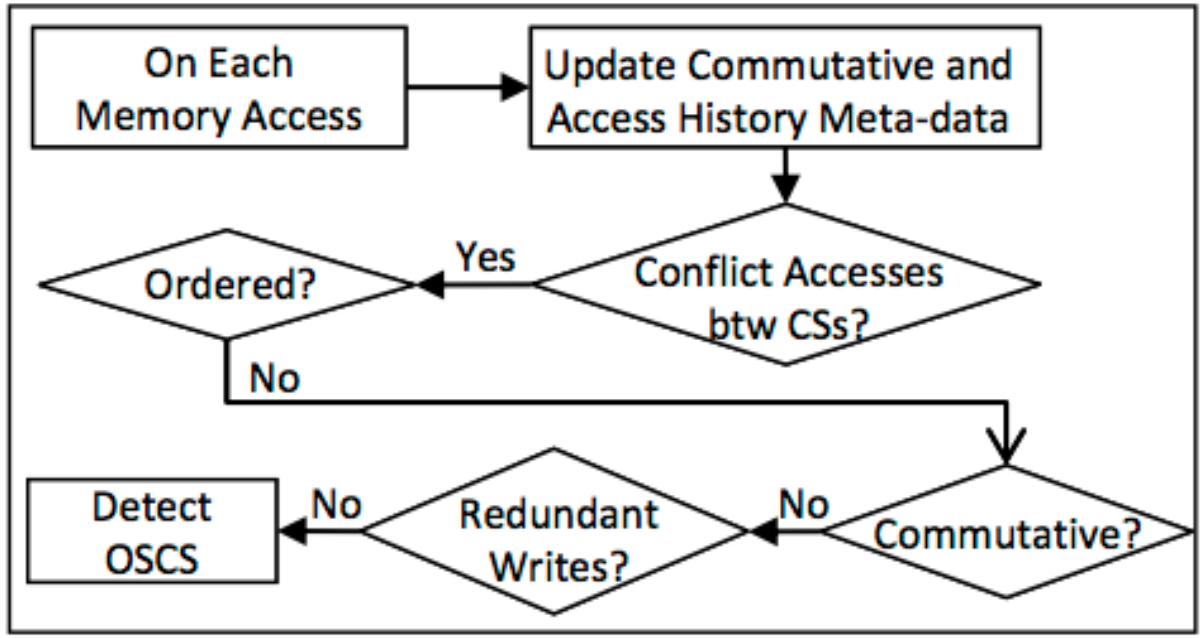
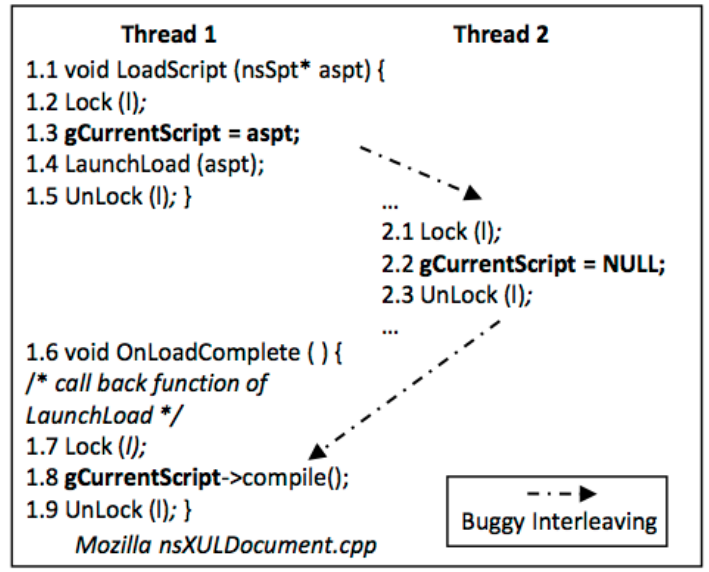


Figure 6: OSCS operations on every memory access.

Commutative operation is determined by read-write sequence



(c) Order-sensitive critical section pair. Non-race atomicity violation bug (Mozilla-1) [11].

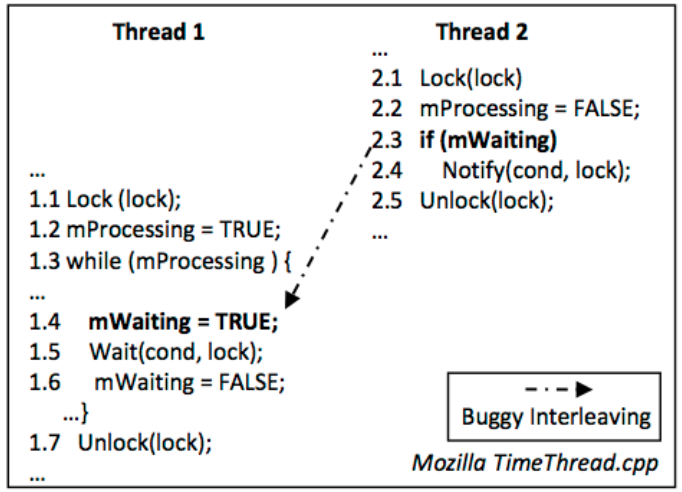


Figure 4: An ordering violation bug example (KB3) [24].

Evaluation

- Concurrency bugs
  - Atomicity violation
  - Ordering violation
  - Multi-variable bugs
- False positive
- False negative

Synchronization

- Ordering synchronization operations
  - Barrier
  - Wait-signal pair
- Mutex synchronization
  - Mutex
  - semaphore