

Asier Fernández De Lecea Javier Salamero

Memory Dependence Prediction using Store Sets



Memory Dependence Prediction using Store Sets

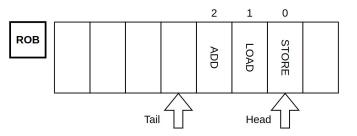
George Z. Chrysos and Joel S. Emer Digital Equipment Corporation Hudson, MA 01749 {chrysos,emer}@vssad.hlo.dec.com



Two types of data dependencies (also known as true dependencies or RAW dependencies):

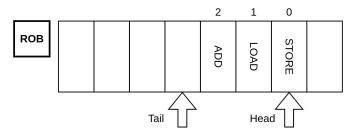
- Register dependencies
 - Can be determined as soon as instructions are decoded
- Memory dependencies:
 - Unknown until addresses are computed (memory disambiguation), a problem in OoO execution schemes





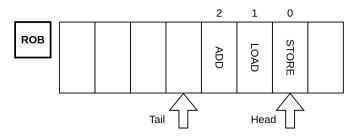
2+IMM] <- R1	# mem[R2	IMM	R2	R1	ST0RE
mem[R4+IMM]	# R3 <-	IMM	R4	R3	LOAD
R3+R3	# R5 <-	R3	R3	R5	ADD

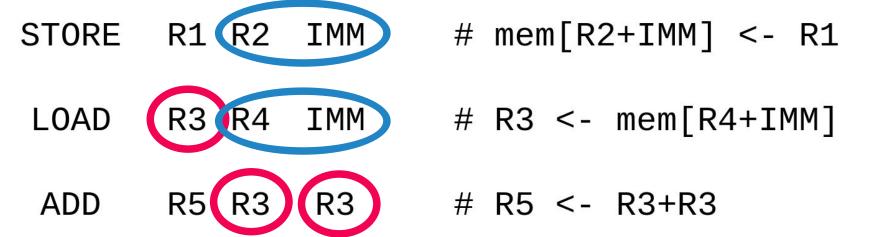




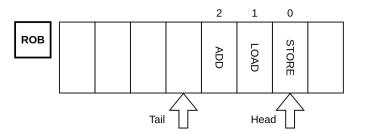




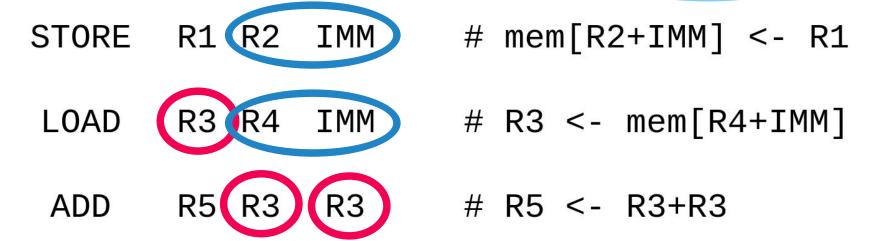




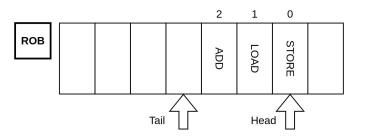




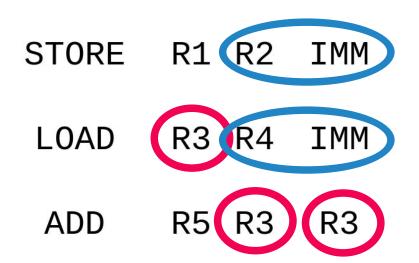
It could be the case that both <u>CALCULATED</u> addresses interfere with each other...



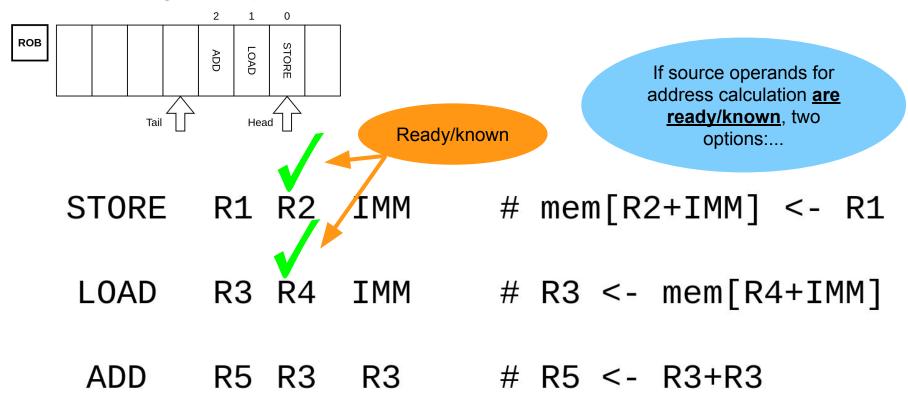




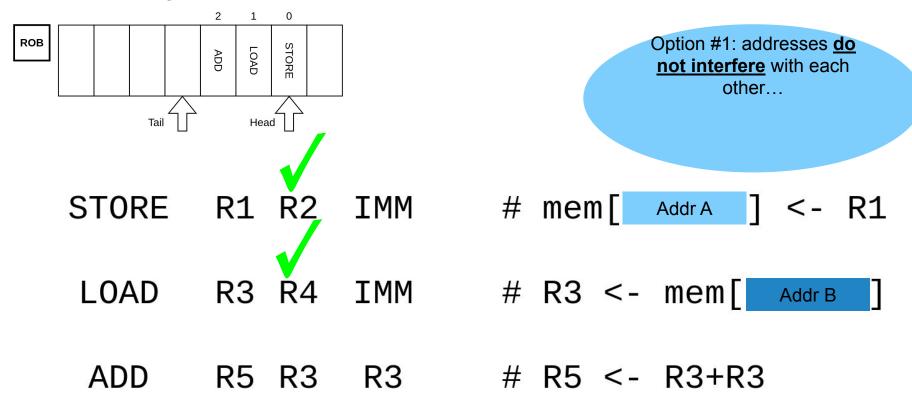
Let's see how that looks...



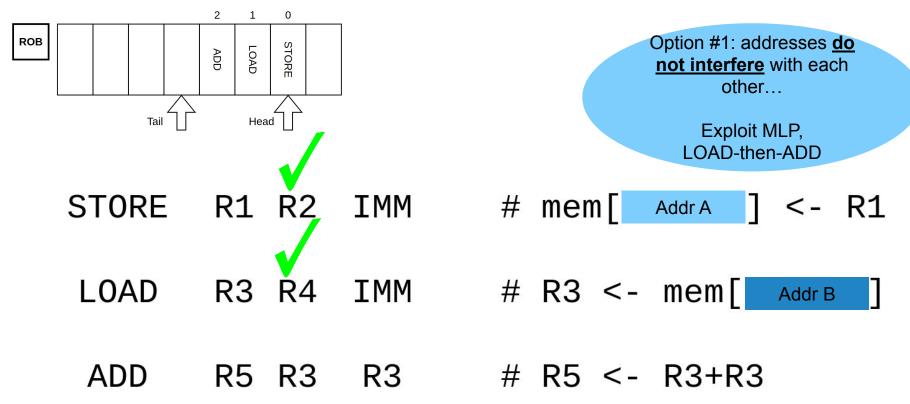




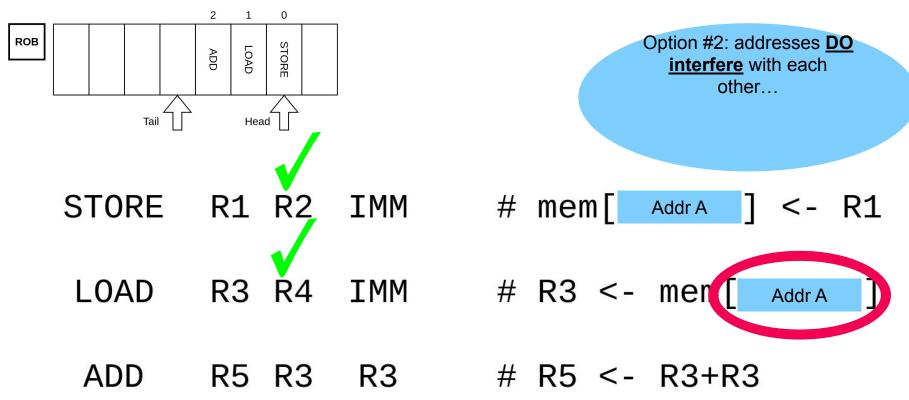




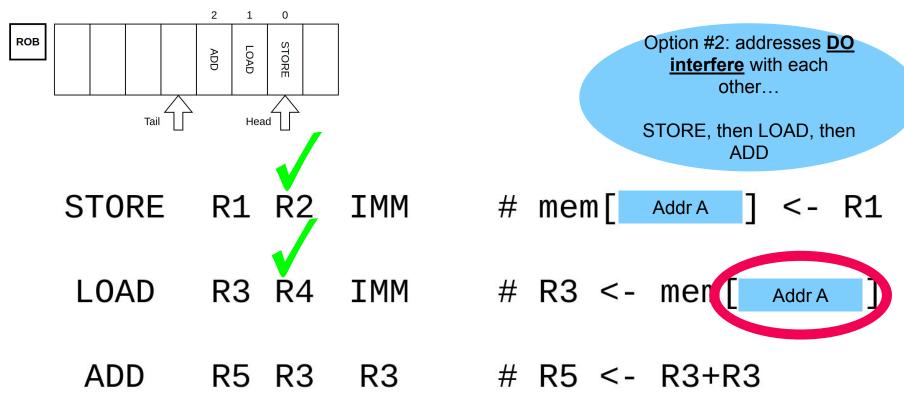




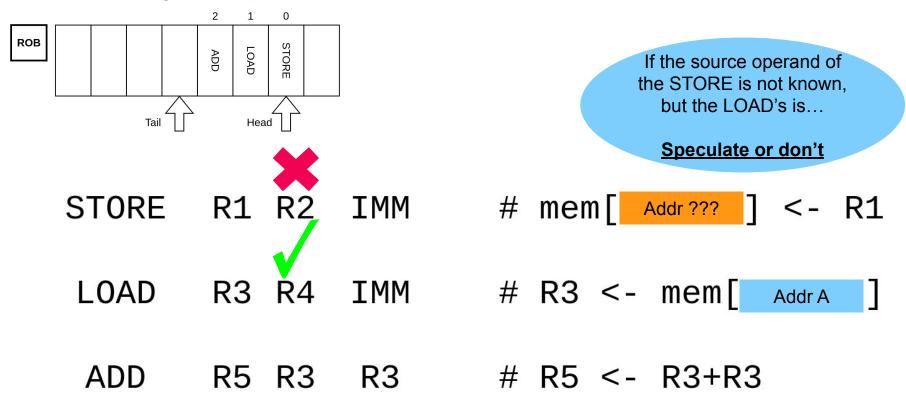




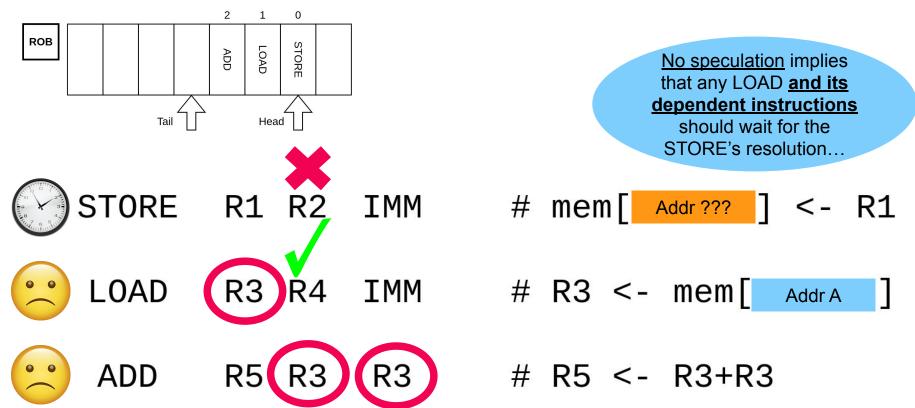




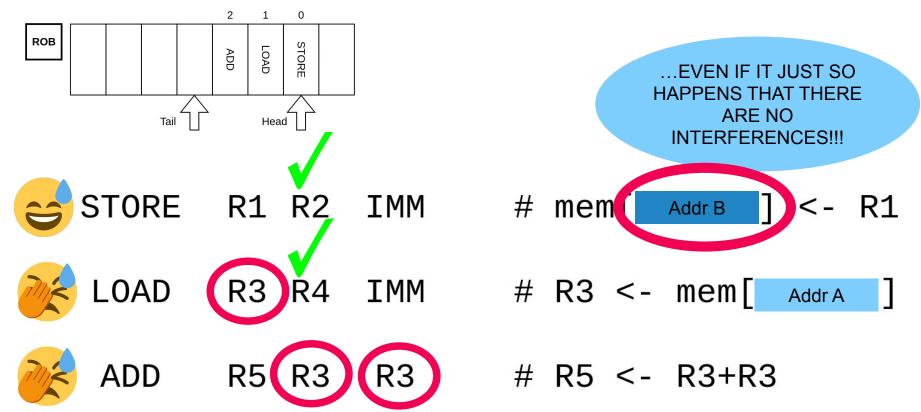




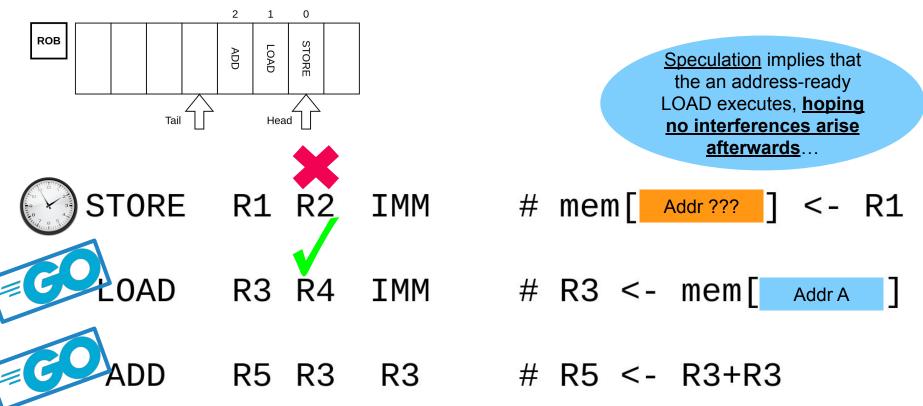




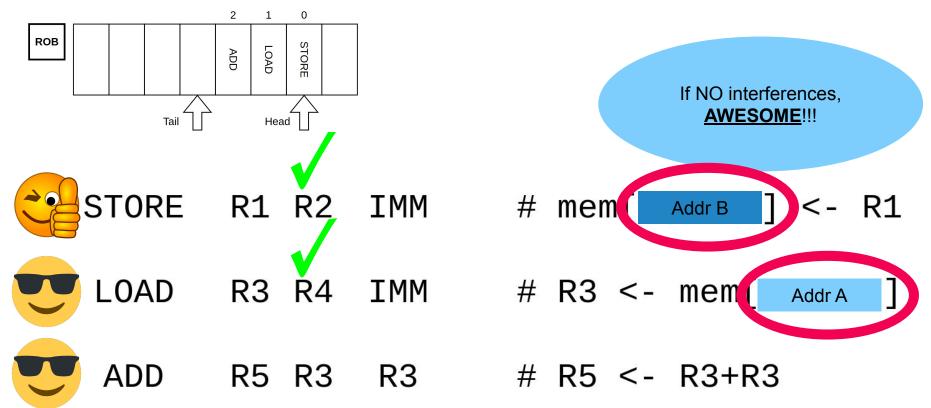




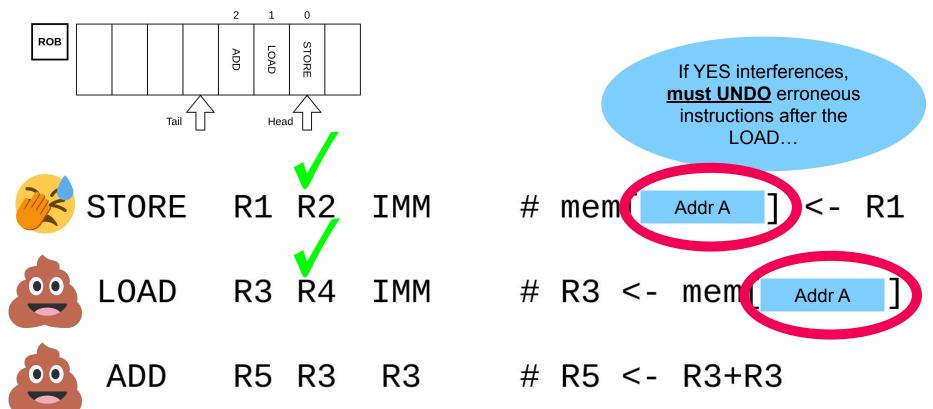














To face the memory disambiguation problem, there are two conventional approaches:

No speculation: blocking a LOAD until all previous STOREs are ready and issued. This creates many false dependencies, but removes memory-order violations.

- For some LOADs, it is not a problem as this added delay is hidden in OoO execution
- Others are in the critical path, and this conservative approach degrades performance



To face the memory disambiguation problem, there are two conventional approaches:

Naive speculation: LOADs always speculate, assuming no dependencies with any previous STOREs and are marked as ready as soon as register dependencies are fulfilled. Thus, there are no false dependencies...

- LOADs can cause memory-order violations and require a re-execution mechanism to produce the correct results
- Better performance than no-speculation scheme



In **Naive Speculation**, re-execution of LOADs after a memory-order violation can be implemented with different strategies, here are two of them:

- Trap the LOAD and squash ALL younger instructions in the pipeline
 - All younger instructions are killed, not only the dependence chain of the LOAD
 - Recovery latency of throwing away all the work done by the discarded instructions can be high



In **Naive Speculation**, re-execution of LOADs after a memory-order violation can be implemented with different strategies, here are two of them:

- Replaying only dependent instructions reduces the penalty, but typically those instructions must remain in the instruction queue (IQ) until the LOAD retires. It has some drawbacks:
 - It fills the IQ with issued instructions waiting until the LOAD commits; if the IQ is full, you cannot extract more ILP
 - Issuing "to-be-replayed" LOADs may delay other useful instructions in the IQ that could issue

Proposal of the paper



This issues reveal the need of memory dependence prediction (MDP), this proposal has the following goals:

- 1. Predict the LOAD instructions that if allowed to execute would cause a memory-order violation
- 2. Delay the execution of these LOADs only as long as is necessary to avoid a such a violation.

If the prediction is accurate, <u>the re-execution of the memory order</u> <u>violating LOADs will be very unlikely</u> and it will not have great impact on performance.



MDP is based on the concept of a store set.

The store set of a LOAD consists of <u>all the STOREs upon which a LOAD has ever depended</u>.

- STOREs identified by PC
- Store set will be used to know which STOREs need to be executed before the LOAD



Simple example with a concrete LOAD:

 Initially its store set is empty, and the LOAD always speculates.

PC Z LOAD r1<- (@A)



Simple example with a concrete LOAD:

- Initially its store set is empty, and the LOAD always speculates.
- 2. If a STORE detects a memory order violation by any LOAD, the STORE is added to the LOAD's set and the LOAD is re-executed.





PC Y



Simple example with a concrete LOAD:

- Initially its store set is empty, and the LOAD always speculates.
- 2. If a STORE detects a memory order violation by any LOAD, the STORE is added to the LOAD's set and the LOAD is re-executed.
- 3. Every time the LOAD is fetched it will be halted in the IQ until all the recently fetched STOREs in the set are issued before it.

PC Y STORE (@A) <- r1

PC Z LOAD r1<- (@A)



STORE SET

PC Y



A STORE could produce a memory dependence:

▷ In multiple LOADS:

```
STORE R1 R2 IMM # mem[R2+IMM] <- R1
LOAD R3 R4 IMM # R3 <- mem[R4+IMM]
LOAD R5 R6 IMM # R5 <- mem[R6+IMM]
```



A STORE could produce a memory dependence:

▷ In multiple LOADS:

STORE	R1 R2	IMM	# mem[Addr A] <- R1
LOAD	R3 R4	IMM	# R3 <- mem[Addr A]
LOAD	R5 R6	IMM	# R5 <- mem[Addr A]



A STORE could produce a memory dependence:

- ▶ Along with other STOREs to the same LOAD address:
 - The LOAD depends on STOREs from different paths

```
R0 R1 PATH2
                               # if R1==R2 PC<-PATH2, else PC<- PC+4
        BEO
       STORE
               R1 R2 IMM
                               # mem[R2+IMM] <- R1
        JUMP
               END IF
                               # PC<-END IF
PATH2
       STORE
                               \# \text{ mem}[R2+IMM] < - R3
               R3 R2
                      IMM
END IF
                               # R5 <- mem[R2+IMM]
        LOAD
               R5 R2
                       IMM
```



A STORE could produce a memory dependence:

- ▷ Along with other STOREs to the same LOAD address:
 - The LOAD depends on STOREs from different paths

```
R0 R1 PATH2
                                   # if R1==R2 PC<-PATH2, else PC<- PC+4
         BE<sub>0</sub>
        STORE
                 R1 R2
                                   \# \text{ mem} [ Addr A ] <- R1
                         IMM
         JUMP
                 END IF
                                   # PC<-END IF
 PATH2
        STORE
                                   \# \text{ mem} [ Addr A ] <- R3
                 R3 R2
                         IMM
END IF
         LOAD
                 R5 R2
                          IMM
                                   \# R5 <- mem AddrA
```



A STORE could produce a memory dependence:

▷ If LOAD depends on multiple STOREs that write in portions of a data word that is read by a single LOAD

```
STORE_BYTE R1 R2 IMM  # mem[R2+IMM] <- R1
STORE_BYTE R3 R4 IMM  # mem[R4+IMM] <- R3
LOAD_HALFW R5 R6 IMM  # R5 <- mem[R6+IMM]
```



A STORE could produce a memory dependence:

▷ If LOAD depends on multiple STOREs that write in portions of a data word that is read by a single LOAD

```
STORE_BYTE R1 R2 IMM  # mem[ Addr A ] <- R1
STORE_BYTE R3 R4 IMM  # mem[ Addr A +1 ] <- R3
LOAD_HALFW R5 R6 IMM  # R5 <- mem[ Addr A ]
```



A STORE could produce a memory dependence:

If WAW hazards are treated as dependencies, a LOAD can depend on a series of STOREs to the same location

```
STORE R1 R2 IMM # mem[R2+IMM] <- R1
STORE R3 R2 IMM # mem[R2+IMM] <- R3
LOAD R5 R2 IMM # R5 <- mem[R2+IMM]
```



A STORE could produce a memory dependence:

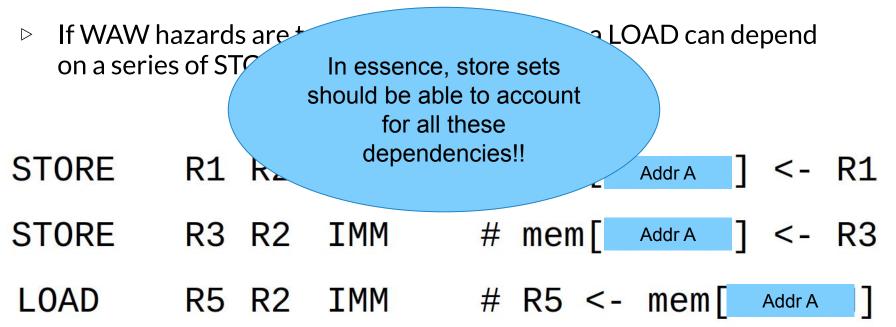
If WAW hazards are treated as dependencies, a LOAD can depend on a series of STOREs to the same location

STORE	R1 R2	IMM	# mem[AddrA] < - R1
STORE	R3 R2	IMM	# mem[AddrA] < - R3
LOAD	R5 R2	IMM	# R5 < - mem[AddrA]

Store Set



A STORE could produce a memory dependence:



Store Set



The concept of MDP with the store set approach is based on two assumptions:

- 1. The historic behavior of memory-order violations is a good approach to avoid future memory-order violations
- It is important to predict dependencies of LOADs where one LOAD is dependent on multiple STOREs or multiple LOADs depend on the same STORE



At the time of publication of the paper, SoA was Alpha 21264, MIPS R10000, HP-PA8000 and Intel Pentium Pro.

Memory-order violations are only relevant in the context of OoO execution. In particular, in processors of sizeable issue width and large instruction windows.



At the time of publication of the paper, SoA was Alpha 21264. MIPS R10000, HP-PA8000 and Intel Pentium Pro.

Memory-order violations are only releveneed execution. In particular, in processors of instruction windows.

Why such disparity (doubling!) of numbers?



At the time of publication of the paper, SoA was Alpha 21264. MIPS

R10000, HP-PA8000 and Intel Pentium Pro.

Memory-order violations are only relever execution. In particular, in processors of instruction windows.

Make the problem of memory-order violations as big as possible and show how good this technique is at mitigating it...?



At the time of publication of the paper, SoA was Alpha 21264. MIPS R10000, HP-PA8000 and Intel Pentium Pro.

Memory-order violations are only releveneed execution. In particular, in processors of instruction windows.

Due considerations also as to the representativeness, realism, feasibility of the model's characteristics...



At the time of publication of the paper, SoA was Alpha 21264. MIPS R10000, HP-PA8000 and Intel Pentium Pro.

Memory-order violations are only relever execution. In particular, in processors of instruction windows.

Also, what CPU model? Gem5? Don't think so...



Other CPU model points:

- Aggressive fetch unit capable of fetching multiple basic blocks in a cycle
- Large McFarling-style choosing branch predictor

CPU Model	
•	128 entry instruction queue
•	128K 2-way set-associative Instruction cache
•	128K 2-way set-associative write-back Data cache
•	8 Instructions maximum issued per cycle
•	4 D-Cache Ports (any combination of loads and stores)
•	8M Direct Mapped, Write-Back Unified Second Level Cache



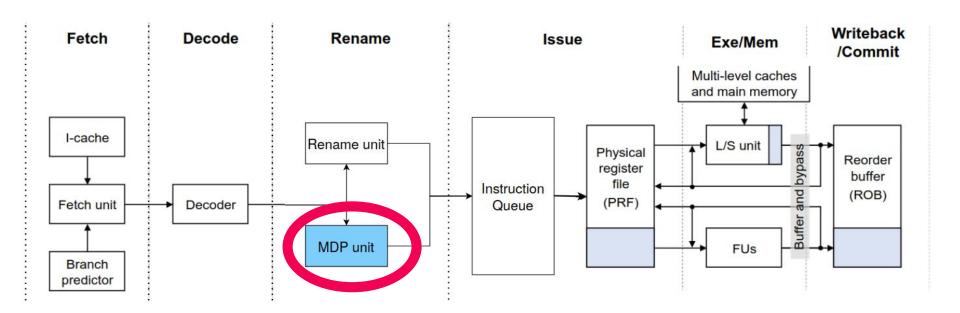
Hardware is limited, having an infinite number of store sets (one per each LOAD with an unlimited number of STOREs in each set) is not feasible.

For a low-cost implementation, we need to relax the structure requirements:

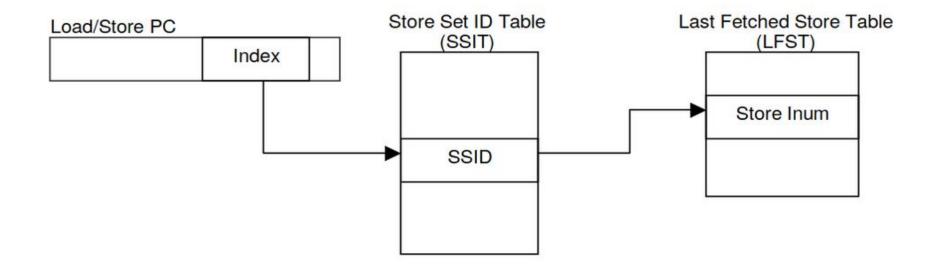
- Limited number of store sets, some LOADs will have to share store sets
- ▷ A STORE's PC will be only in a single set
- Store sets will have a single STORE saved

Where does this go?

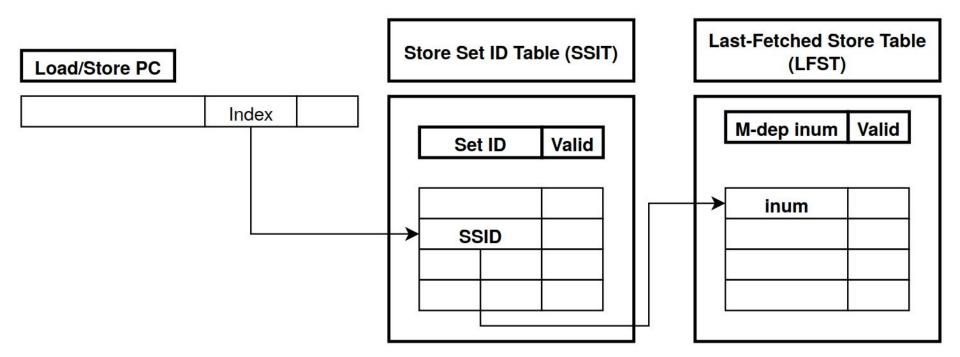










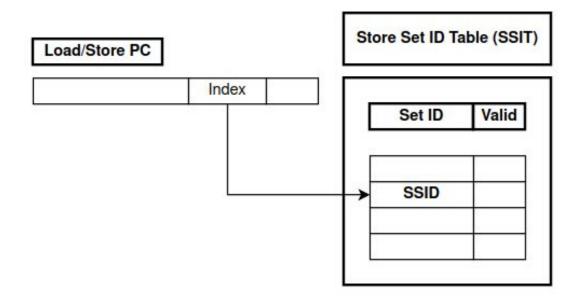




The first table of the proposed solution is the Store Set ID Table (SSIT).

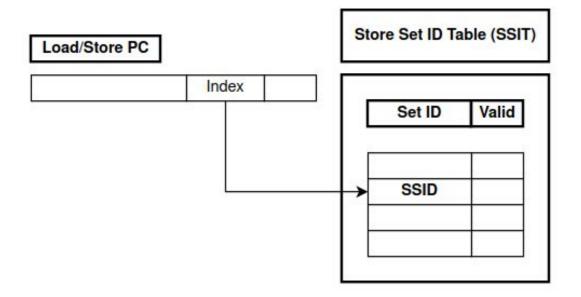
It is indexed by the PC of LOADs/STOREs.

It contains the store set ID to which a LOAD/STORE belongs if it has previously committed a memory-order violation.





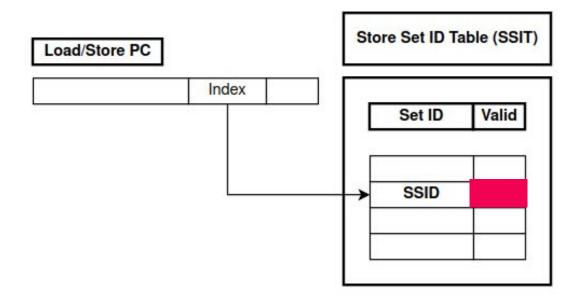
The SSID of a store set is created by XOR-ing the PCs of the first LOAD-STORE pair to commit a memory-order violation.





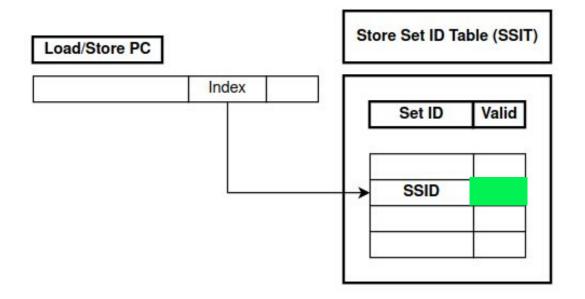
If a LOAD/STORE indexes the SSIT table and finds its entry to be <u>INVALID</u>...

This means that it does not belong to any store set, so there are <u>no memory</u> <u>dependencies</u> to worry about.



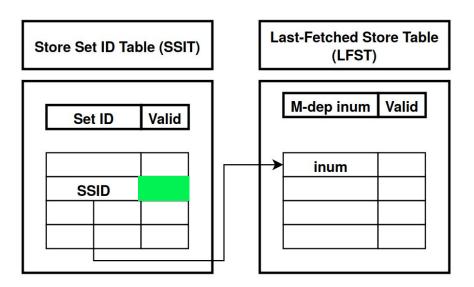


If a LOAD/STORE indexes the SSIT table and finds its entry to be <u>VALID</u>...





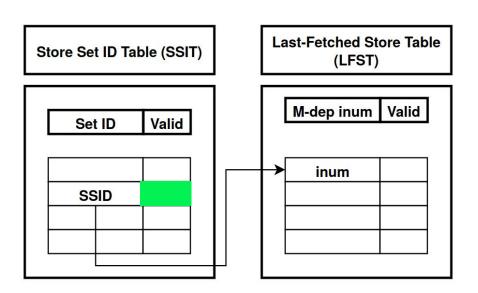
The next table that the paper introduces is the Last-Fetched STORE Table (LFST).





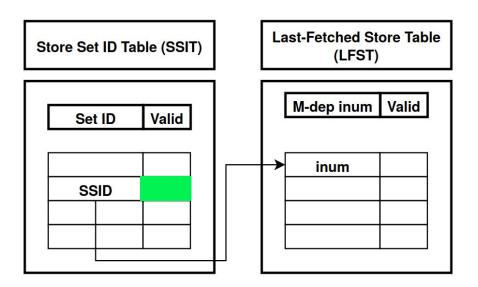
It is indexed by the SSID of a LOAD/STORE that is in a valid STORE Set.

It contains information about the last STORE that was fetched, i.e. which STORE operation is to be waited-for next by the LOAD/STORE instruction.





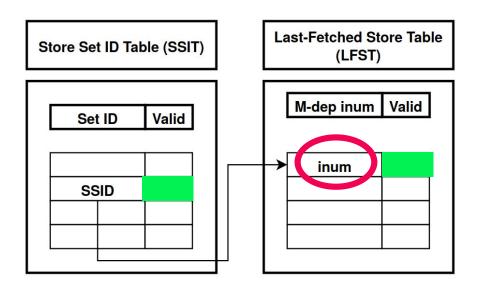
In particular, the LFST contains a unique identifier (we assume ROB ID) of the last STORE to have been fetched.





If the LFST entry is <u>VALID</u>...

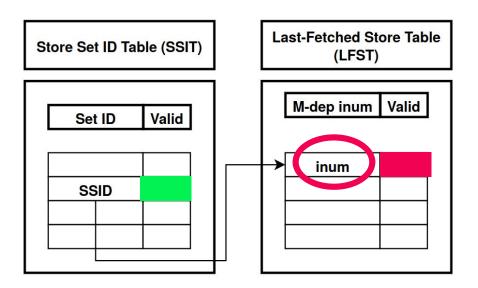
This means that the memory dependence must be respected (needing a wake-up operation), and thus the LOAD/STORE instruction indexing the SSIT will have to wait for the last STORE "inum" to finish.





If the LFST entry is **INVALID**...

This means that there is <u>no</u> memory dependence to be respected, and thus the LOAD/STORE instruction indexing the SSIT is free to go.

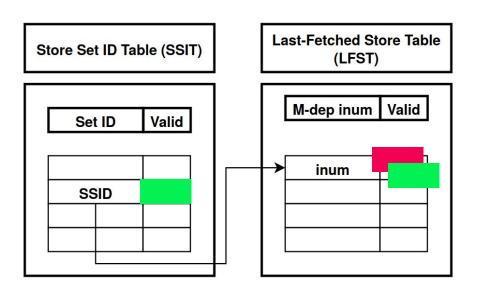




In the case of STORE instructions, they replace the existing "inum" with their own (regardless of whether it was valid or invalid), so that the next instruction waits for the...

...Last-Fetched...

...STORE instruction!



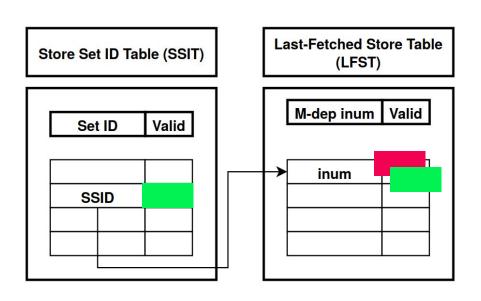


In the case of STORE instructions, they replace the existing "inum" with their own (regardless of whether it was valid or invalid), so that the next instruction waits for the...

...Last-Fetched...

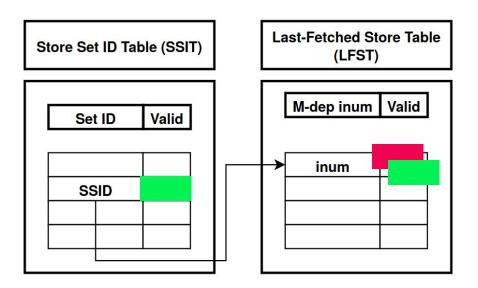
...STORE instruction!

(don't forget to validate the LFST entry too...)

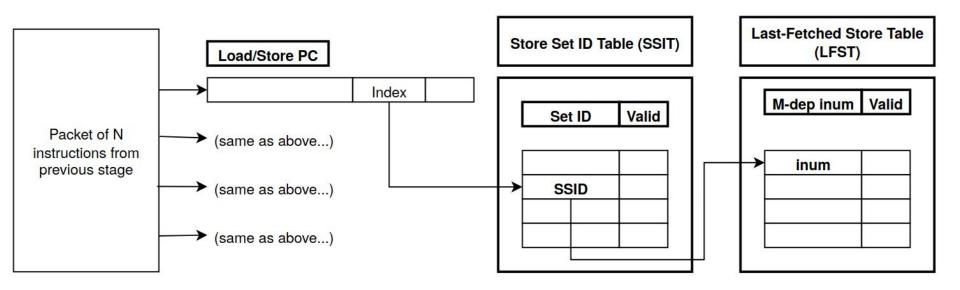




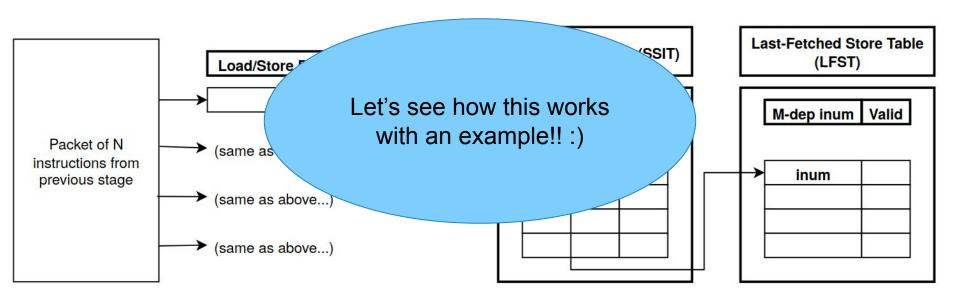
Later, in the IQ, M-dependencies will need the same wake-up logic as with R-dependencies, but now with this "inum" business...

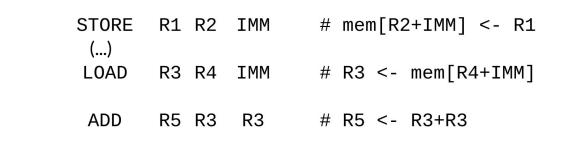


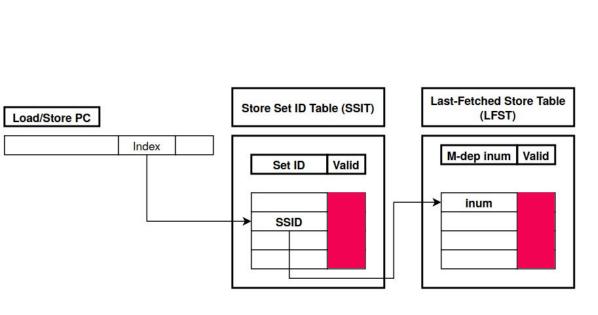


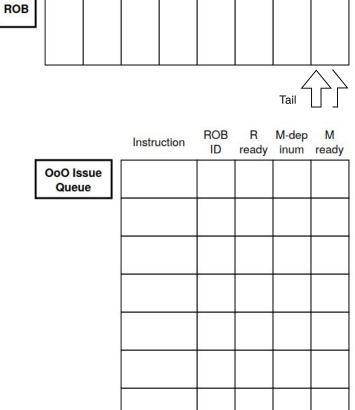


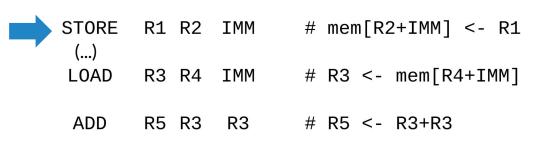


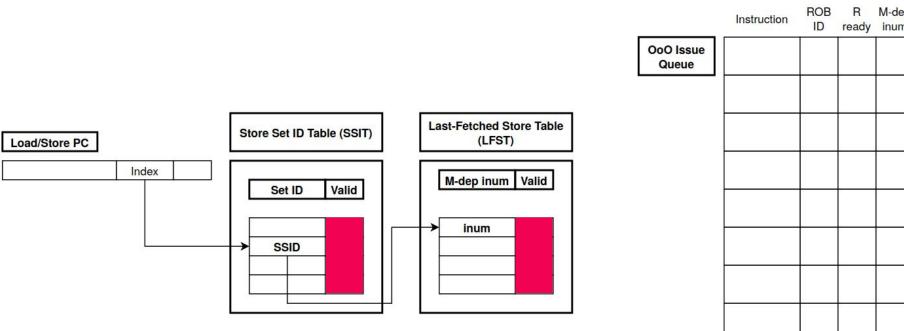


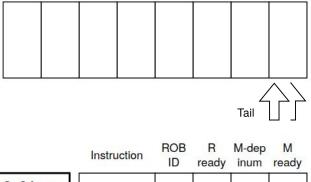


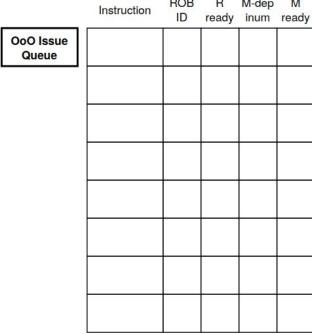


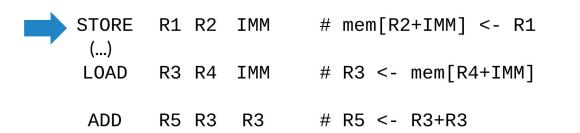


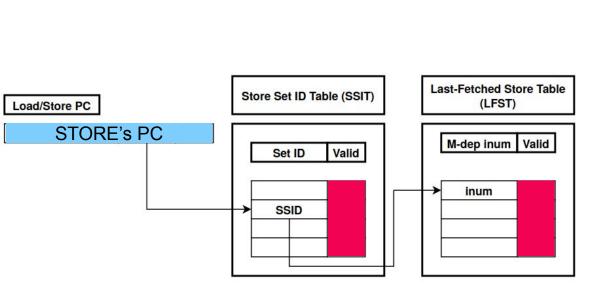


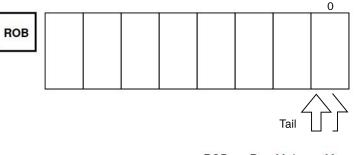


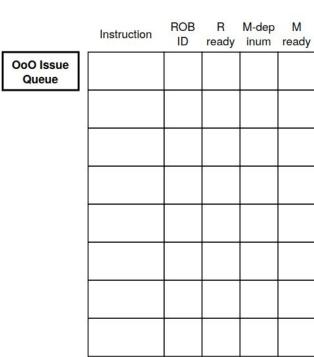


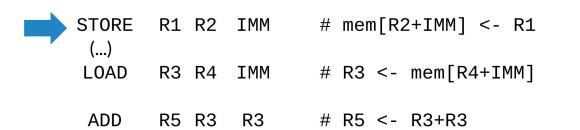


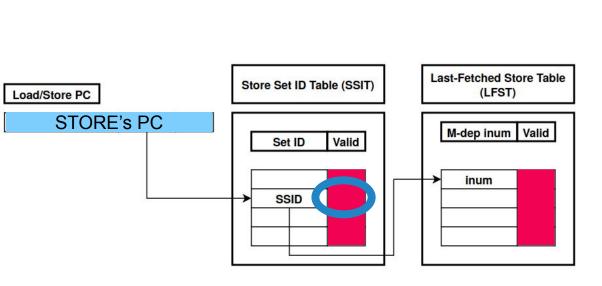


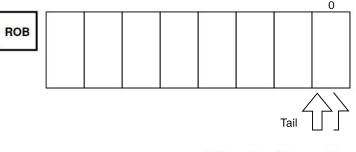


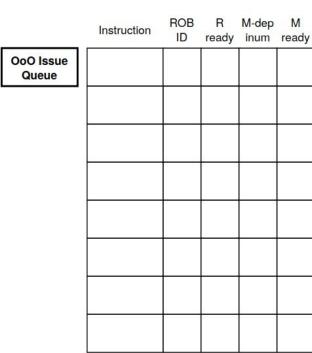


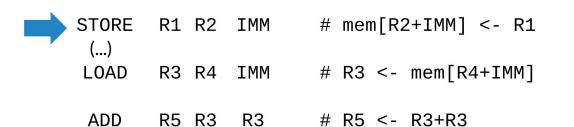


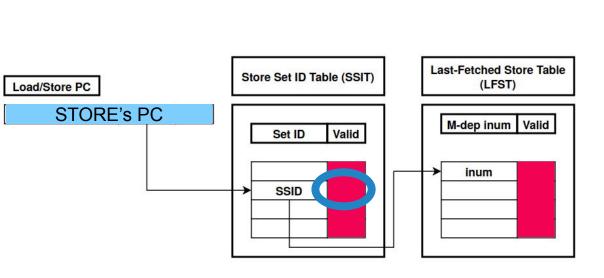


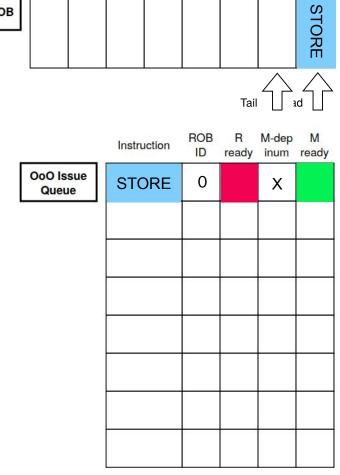


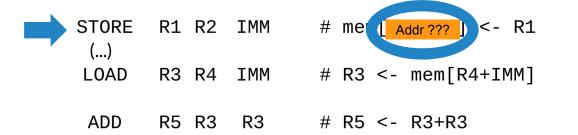


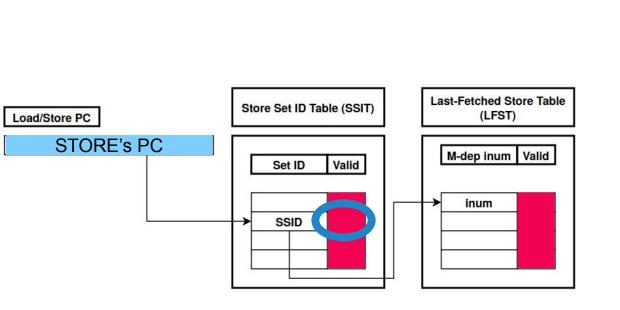


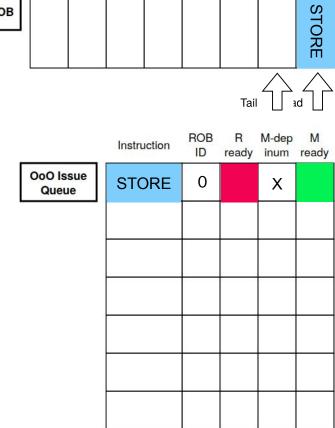


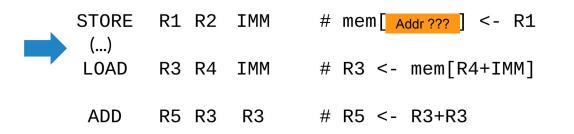


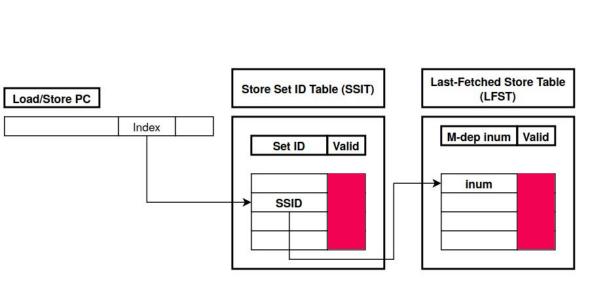


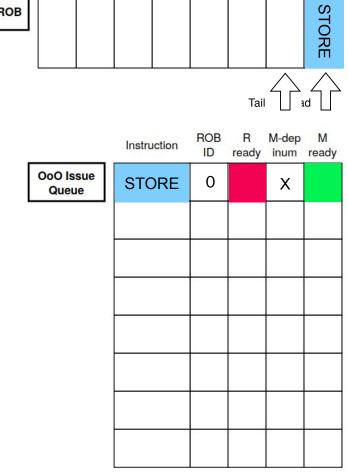


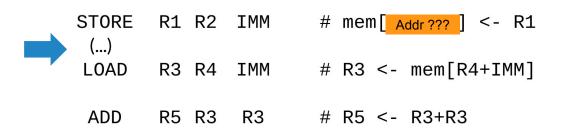


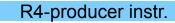


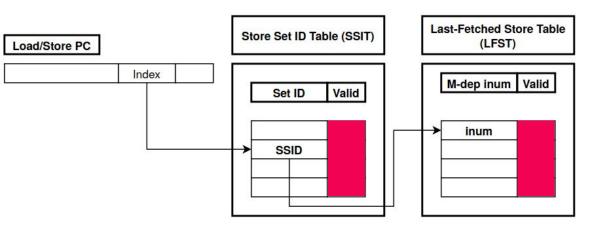


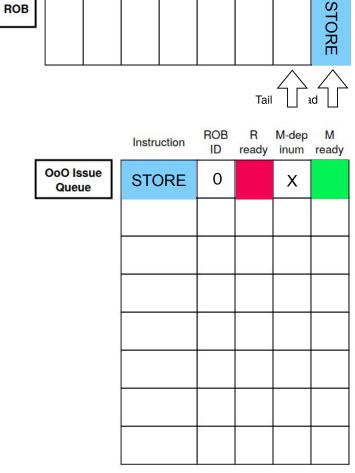


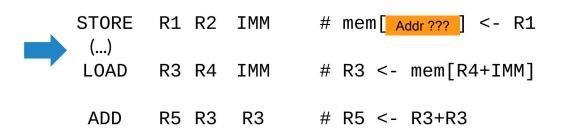




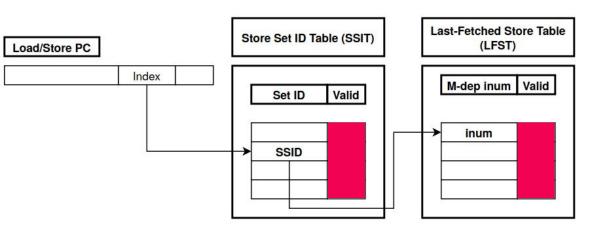


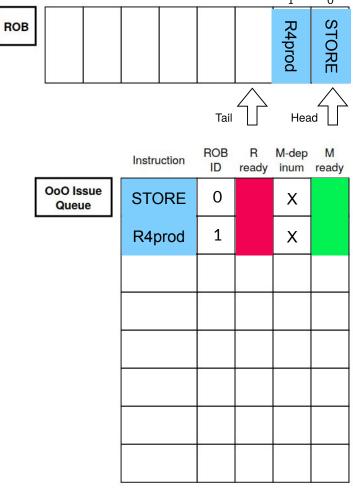


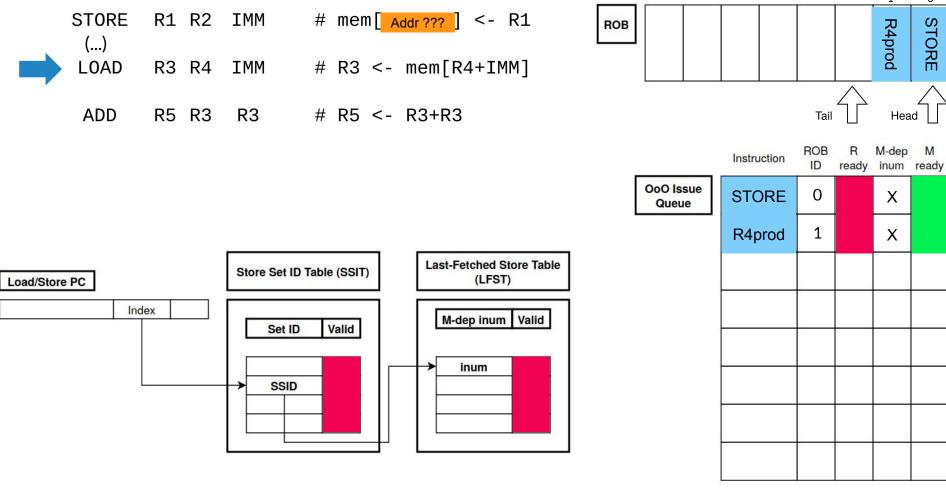


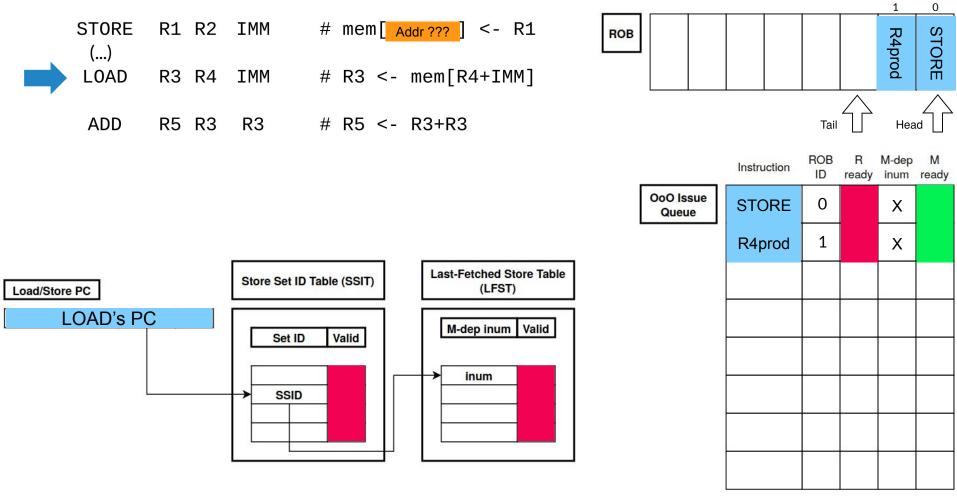


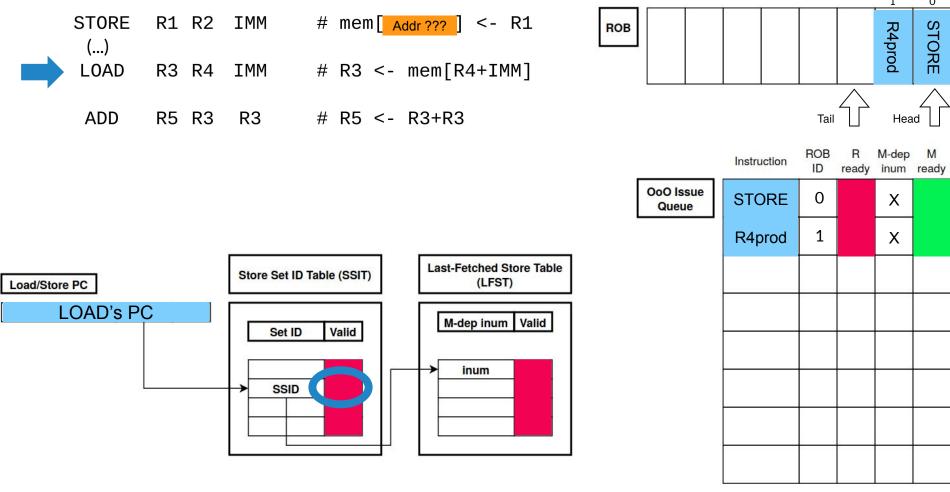
R4-producer instr.

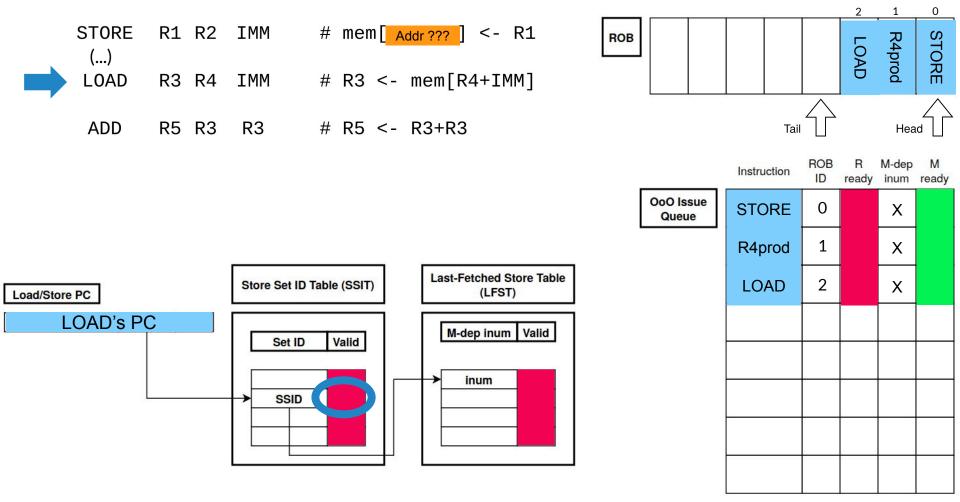


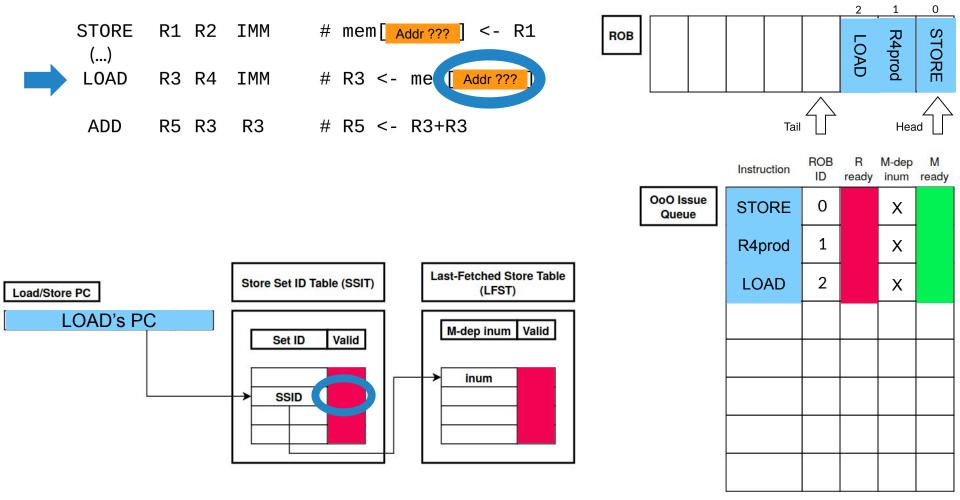


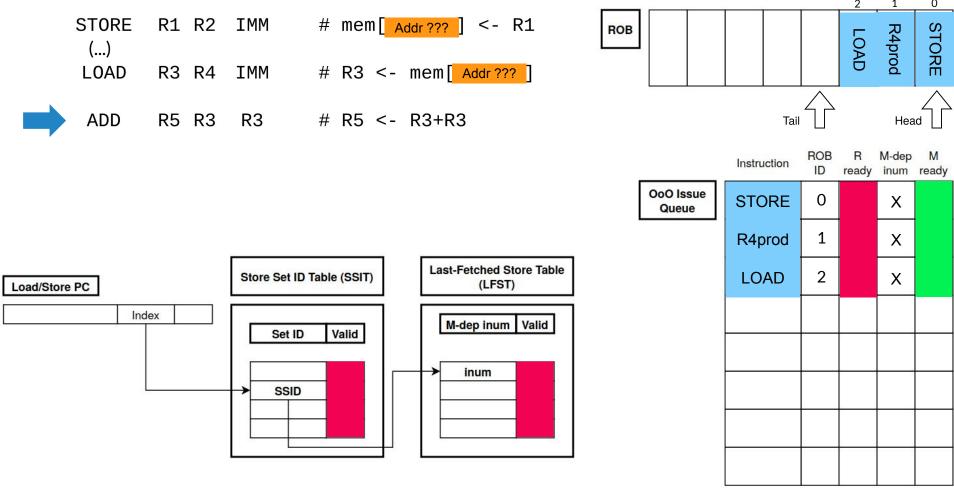


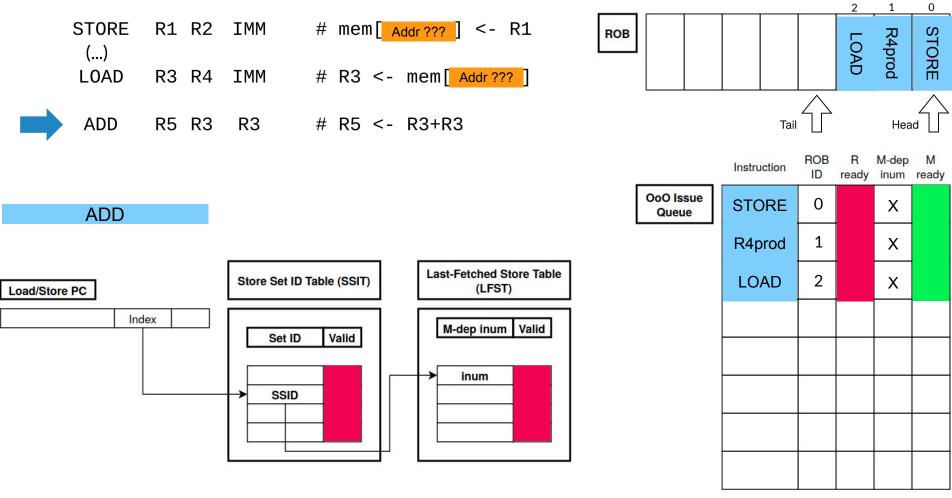


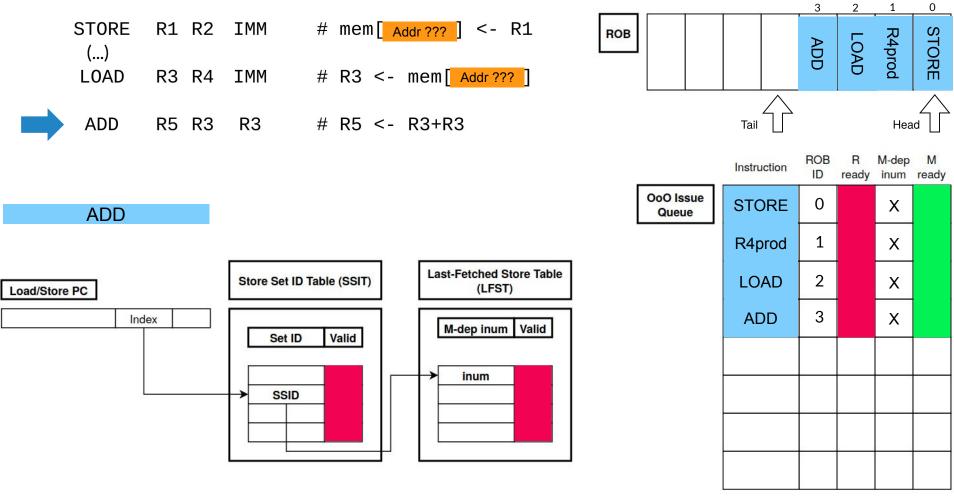


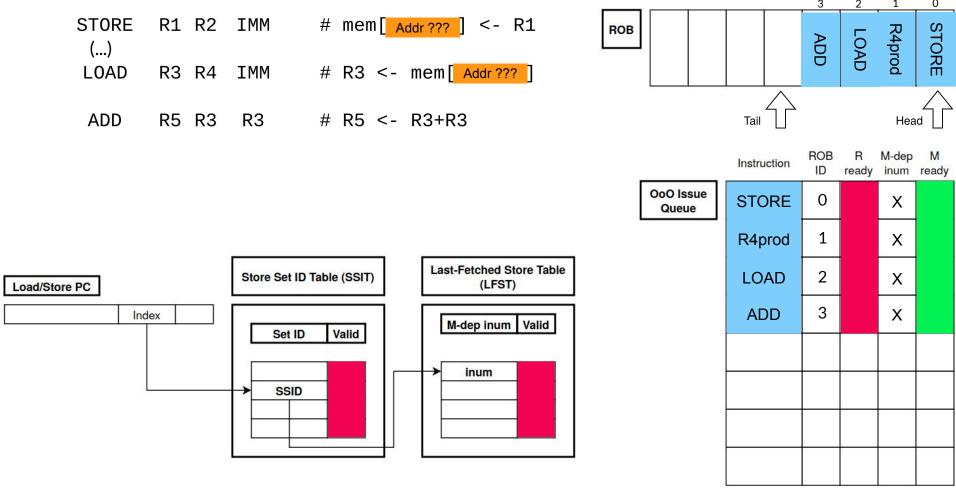


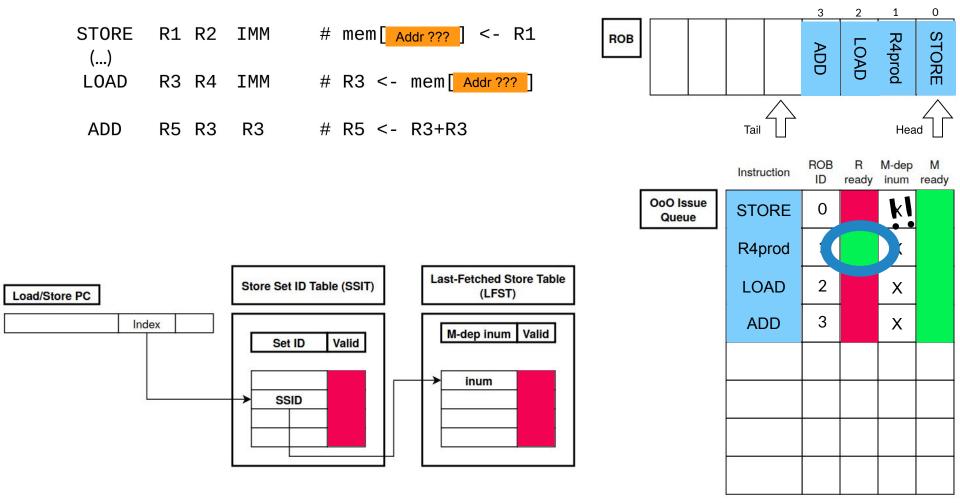


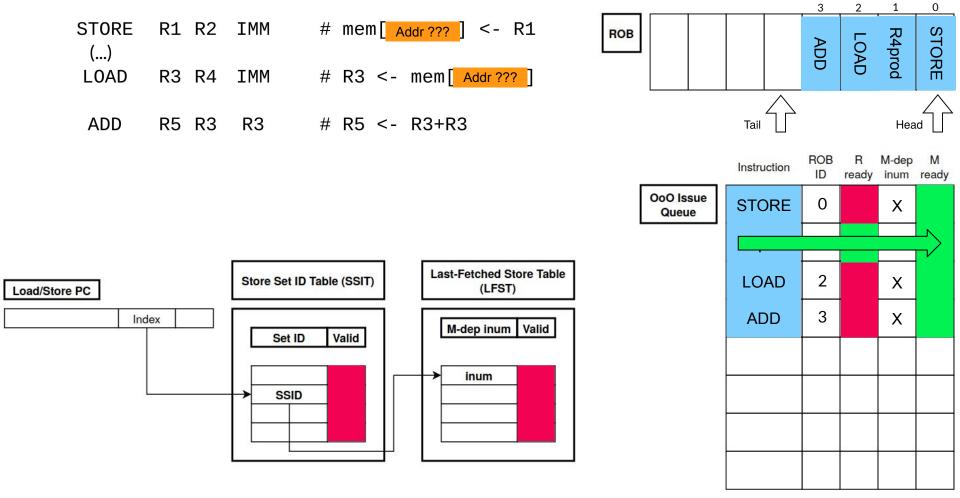


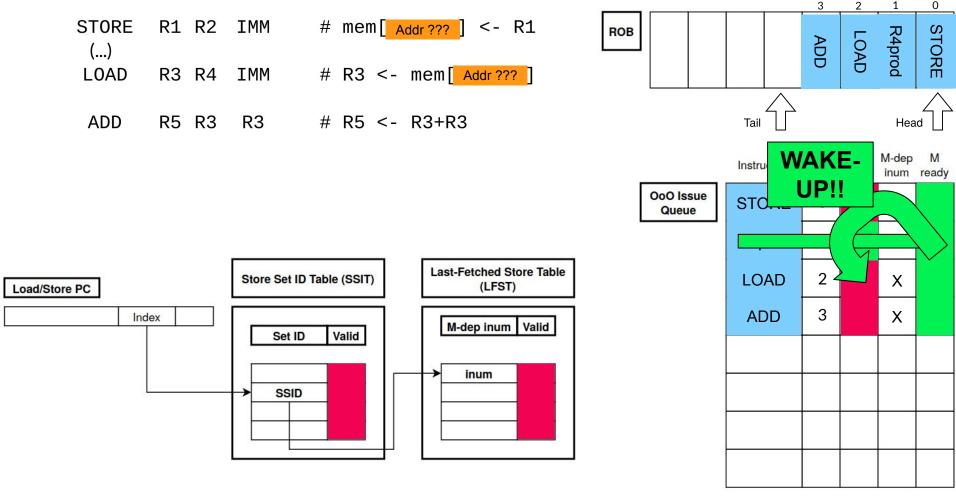


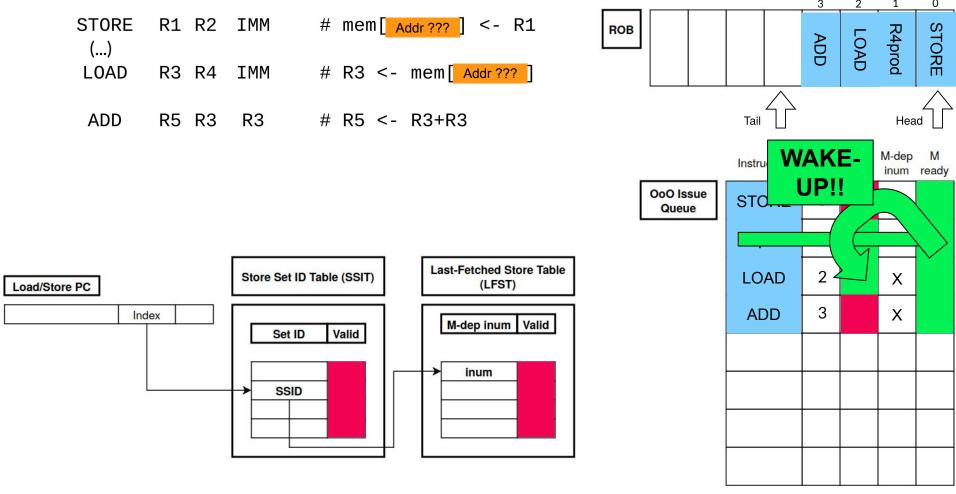


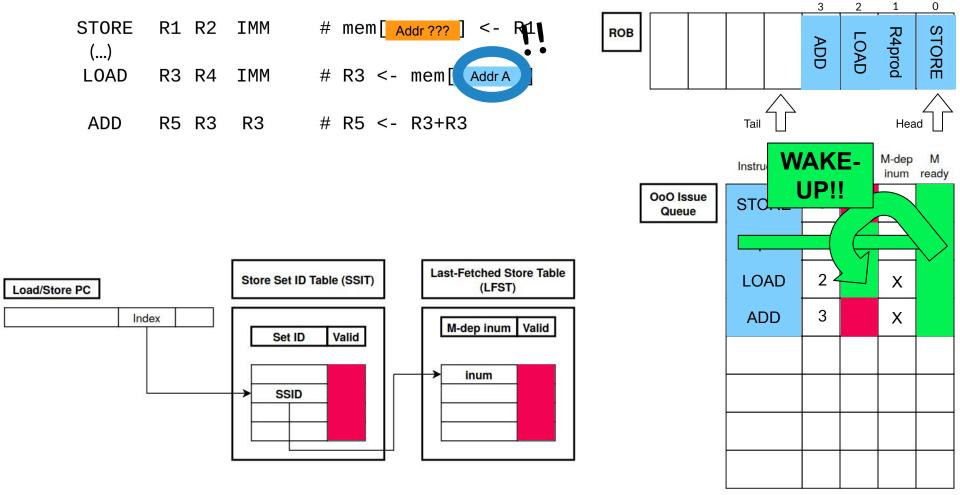


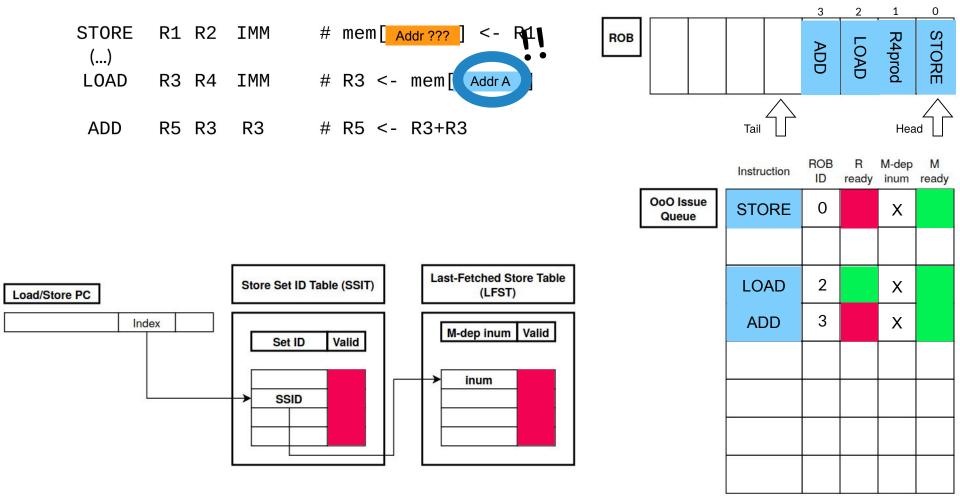


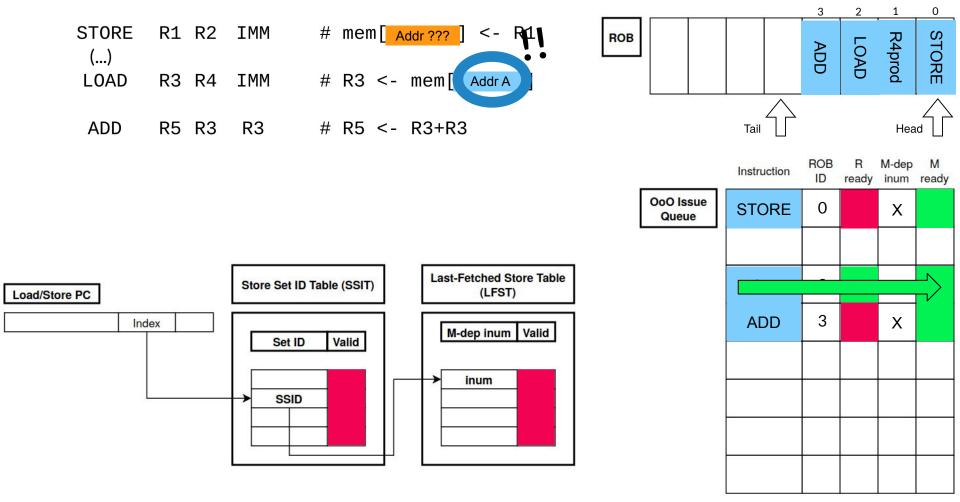


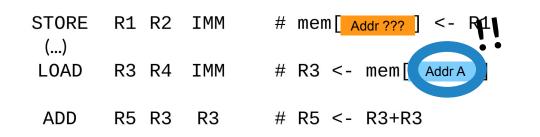


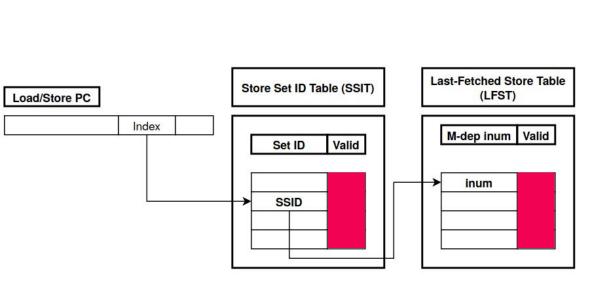


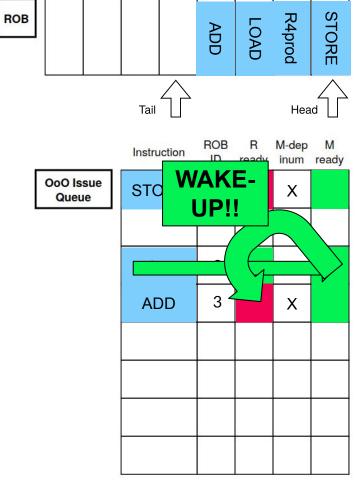


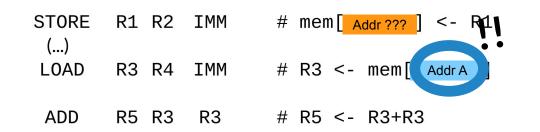


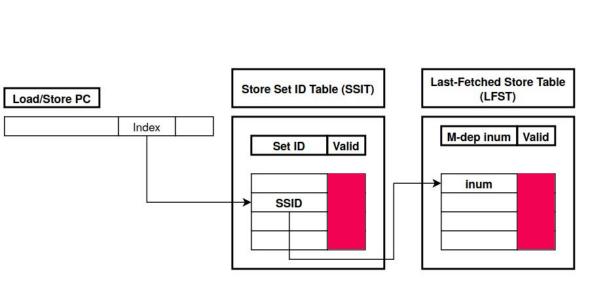


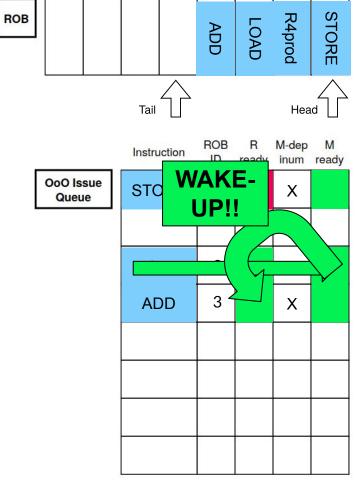


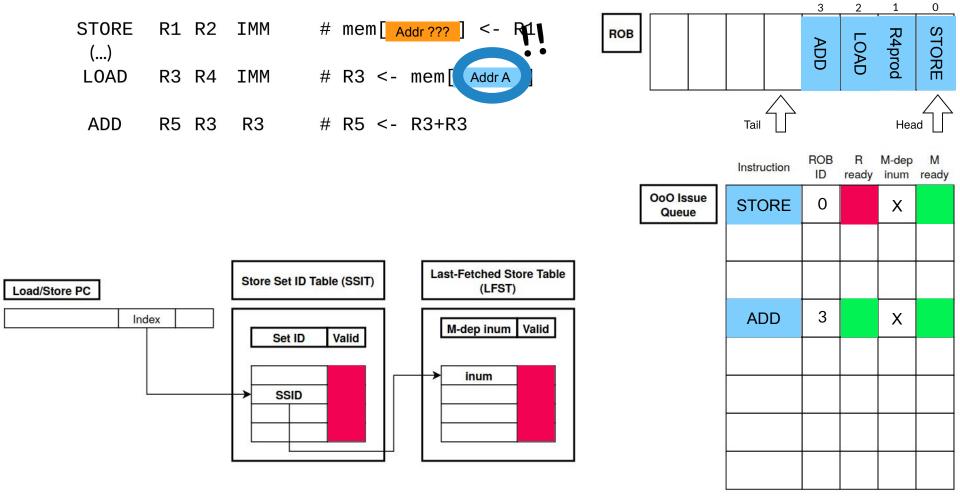


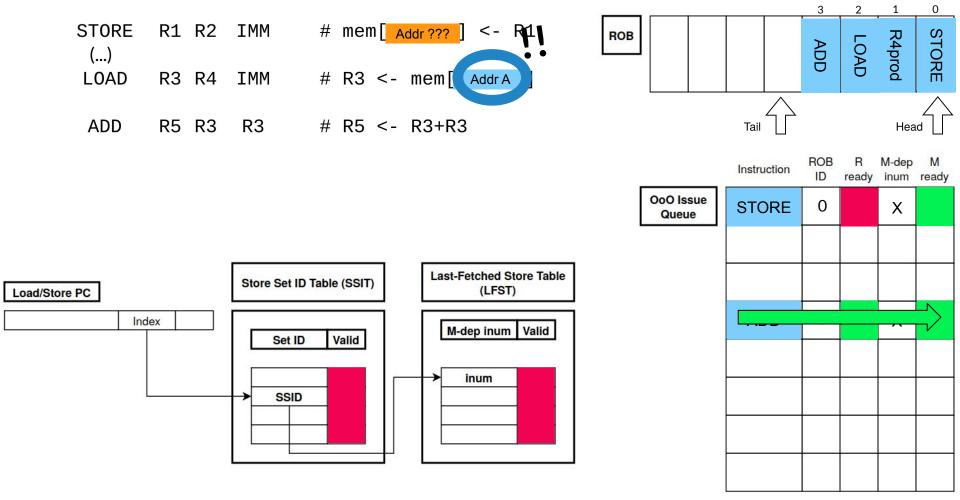


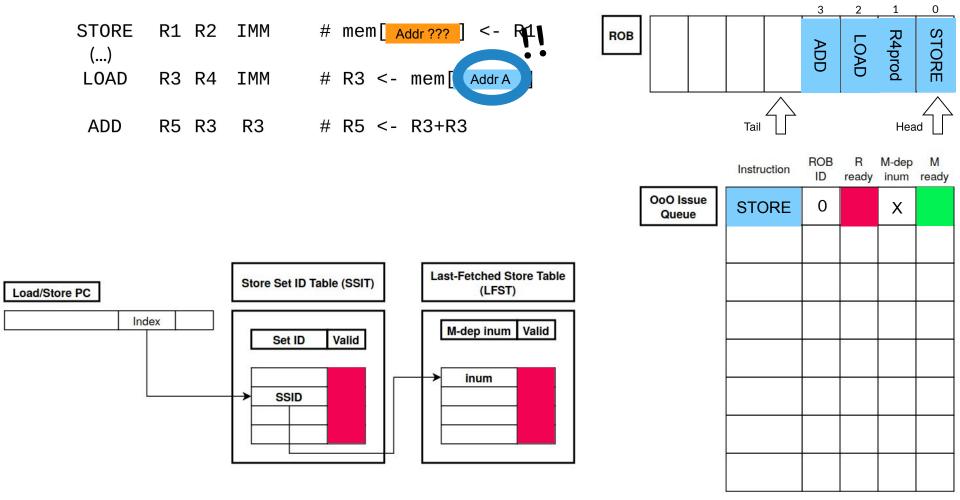


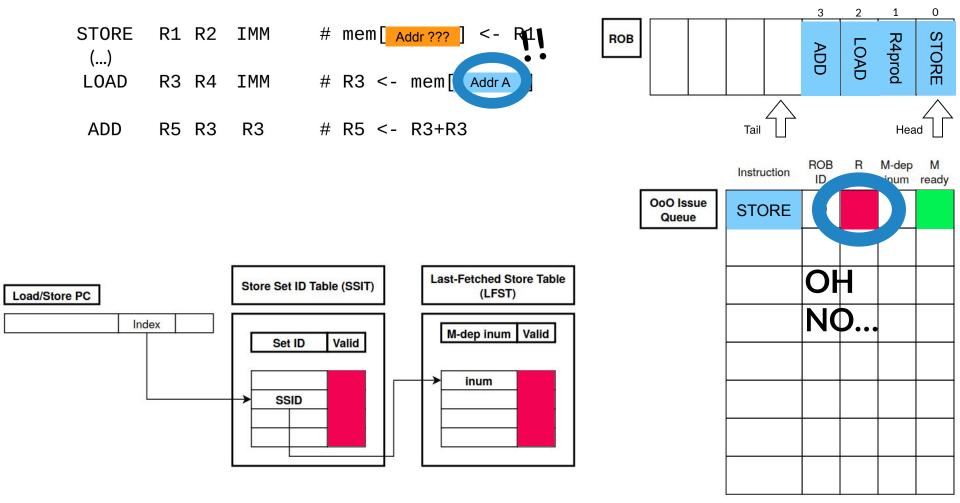


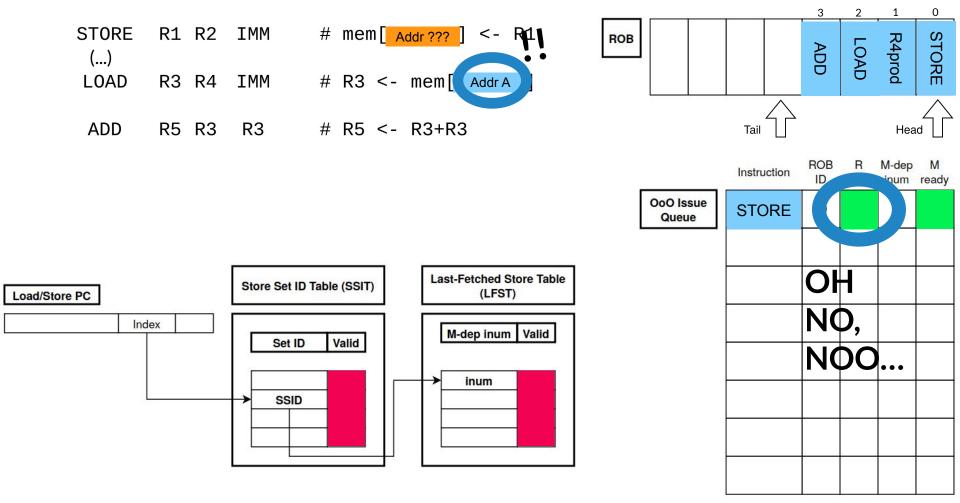


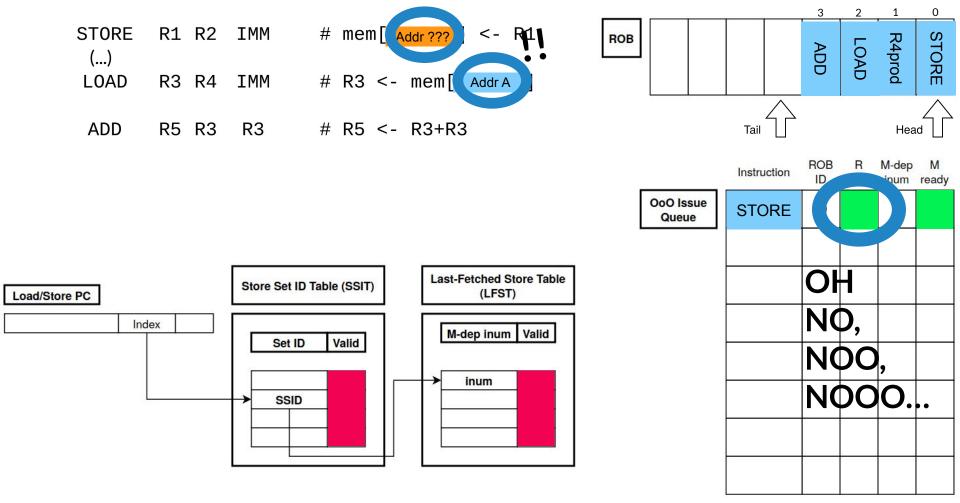


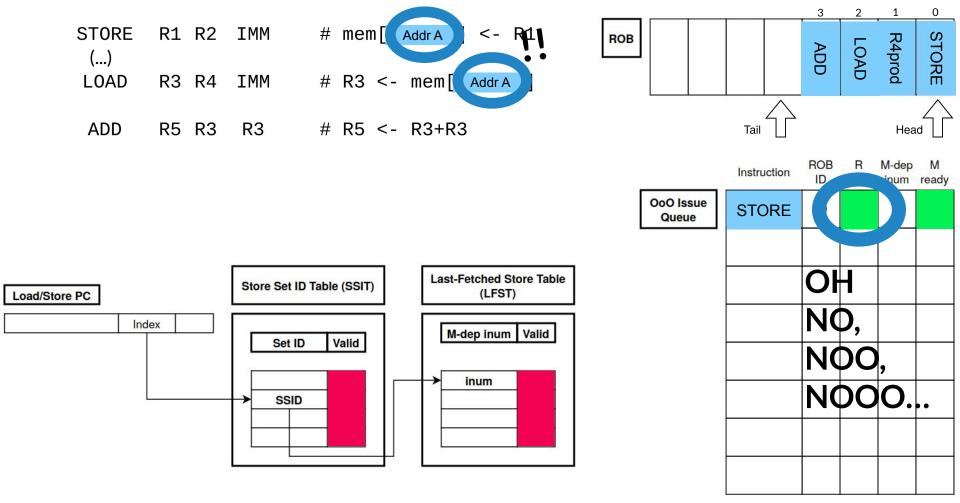




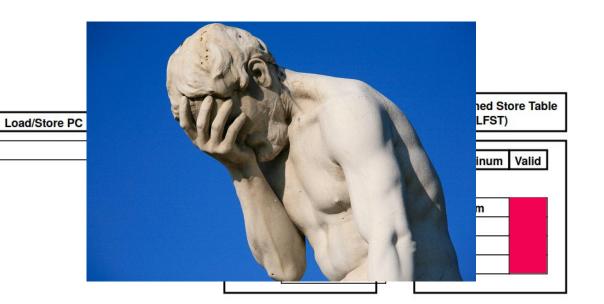


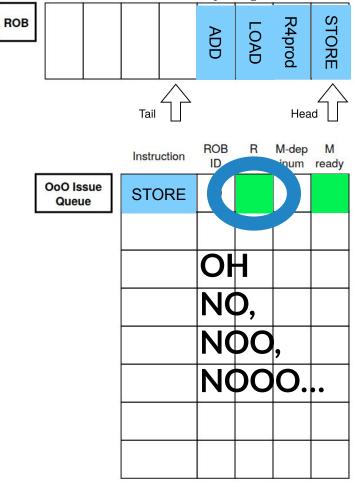


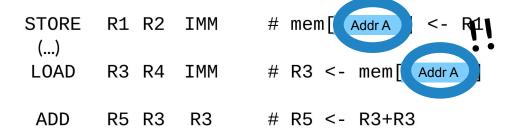


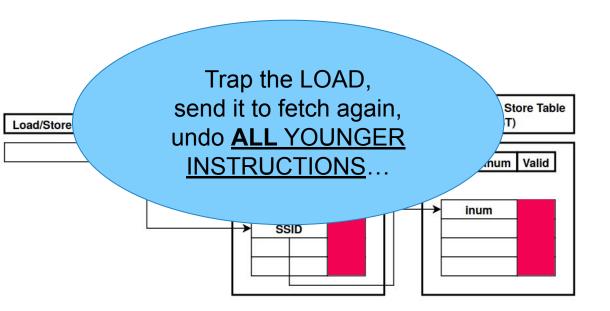


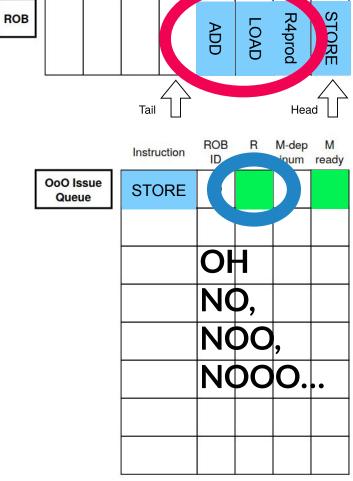


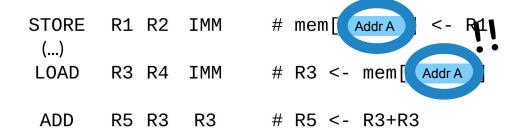




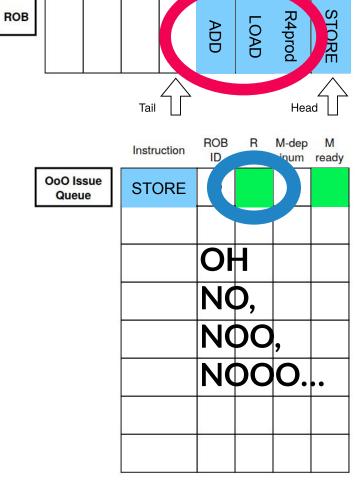


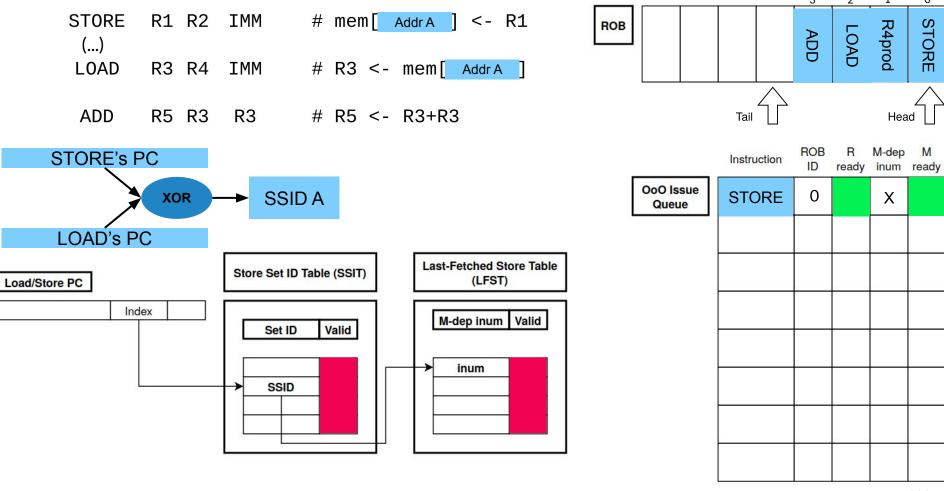


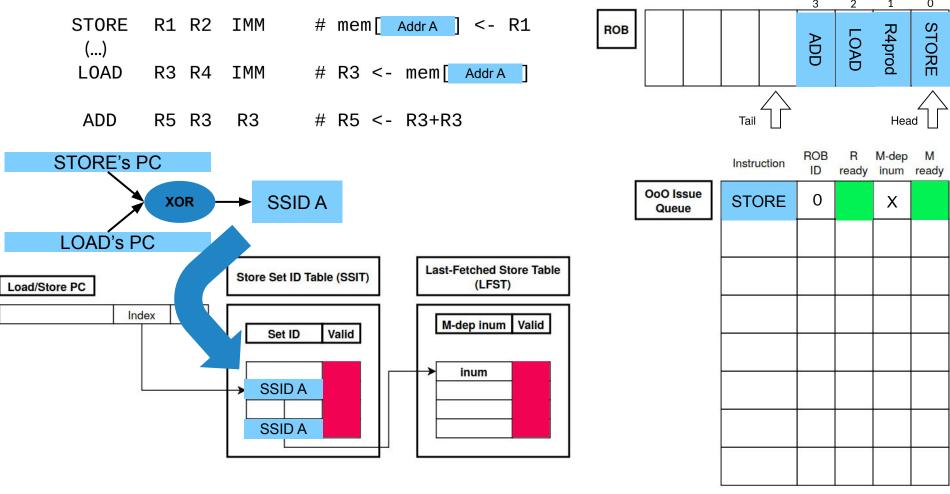


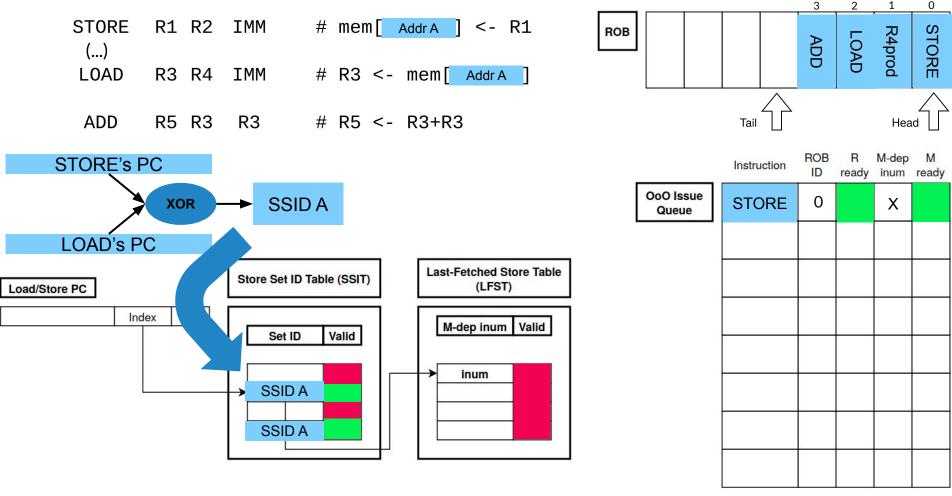


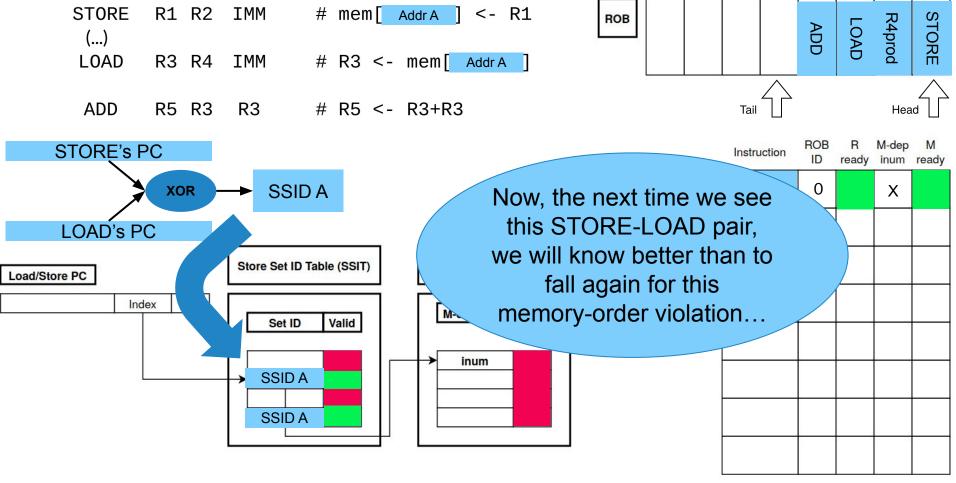


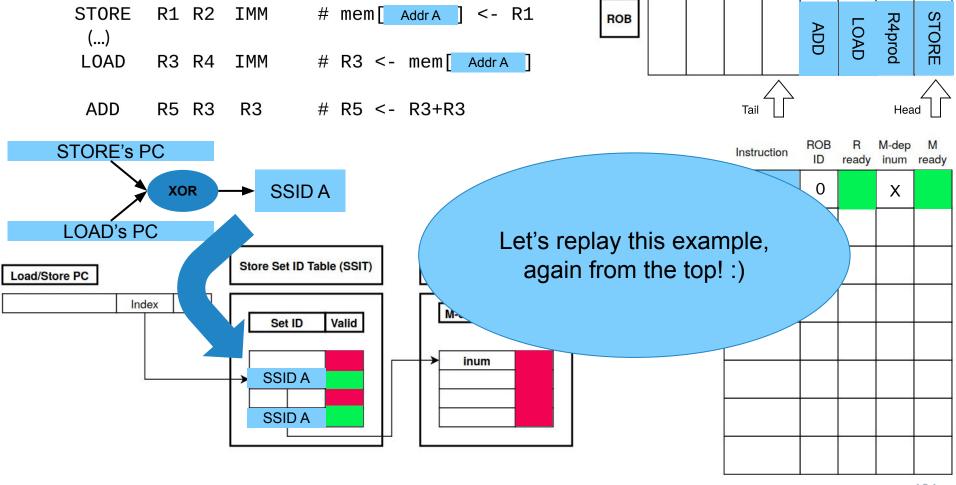


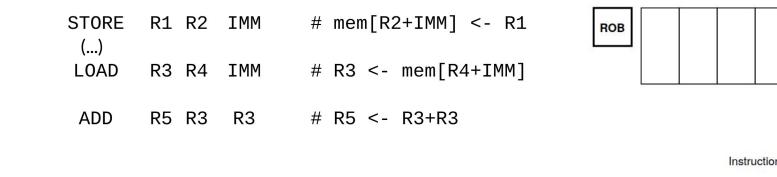


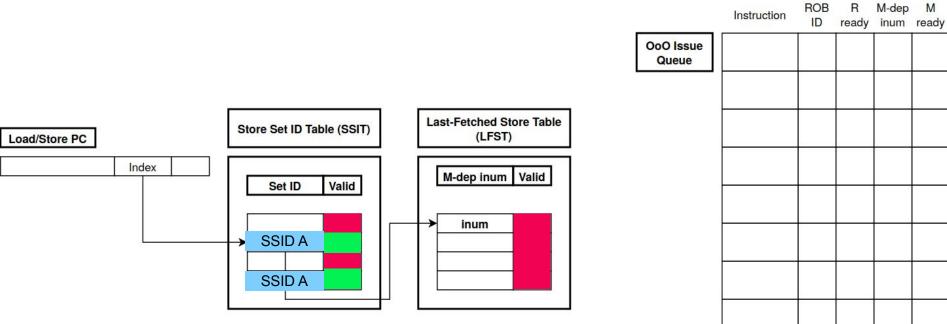




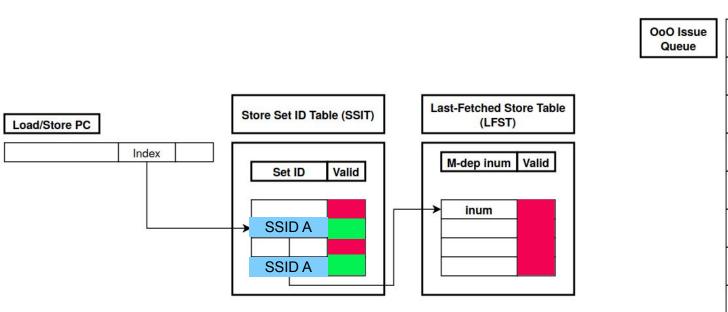


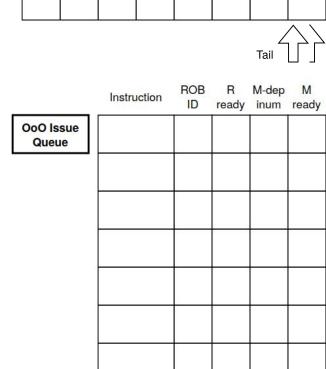




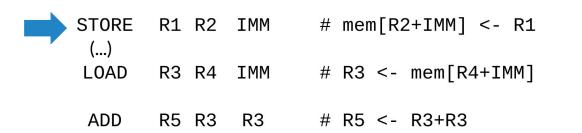


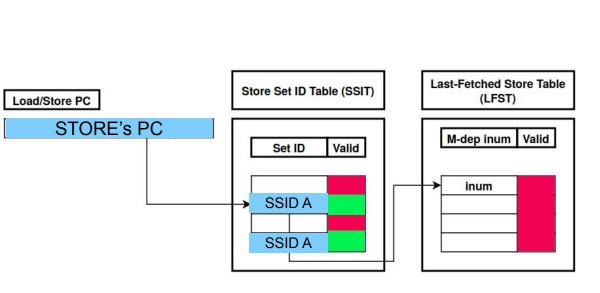


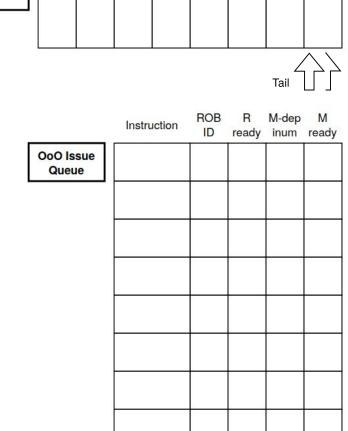




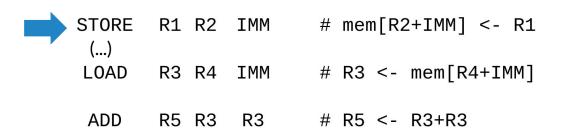
ROB

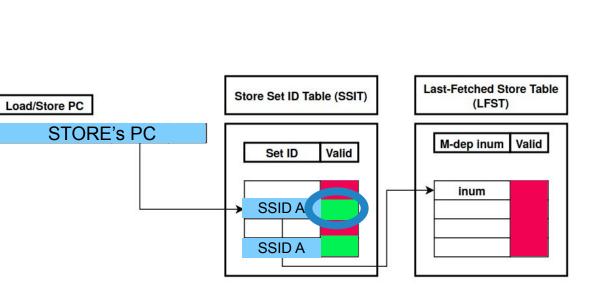


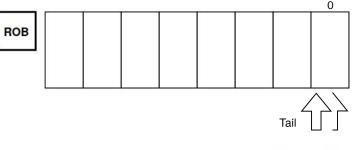


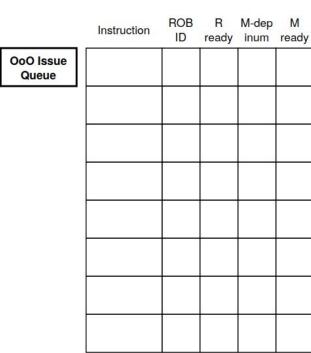


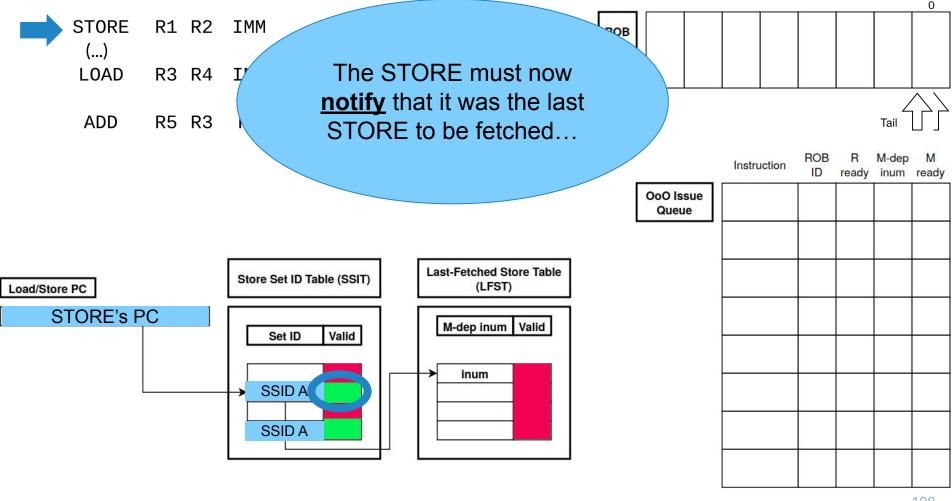
ROB

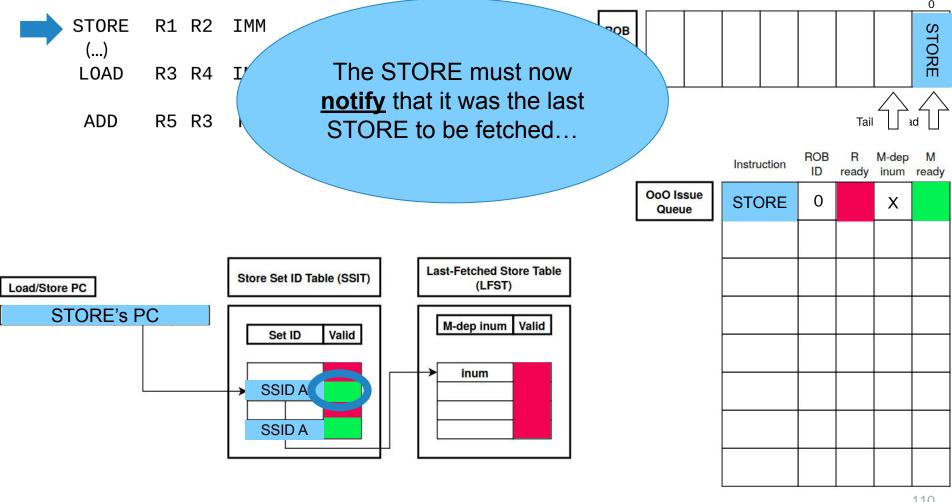


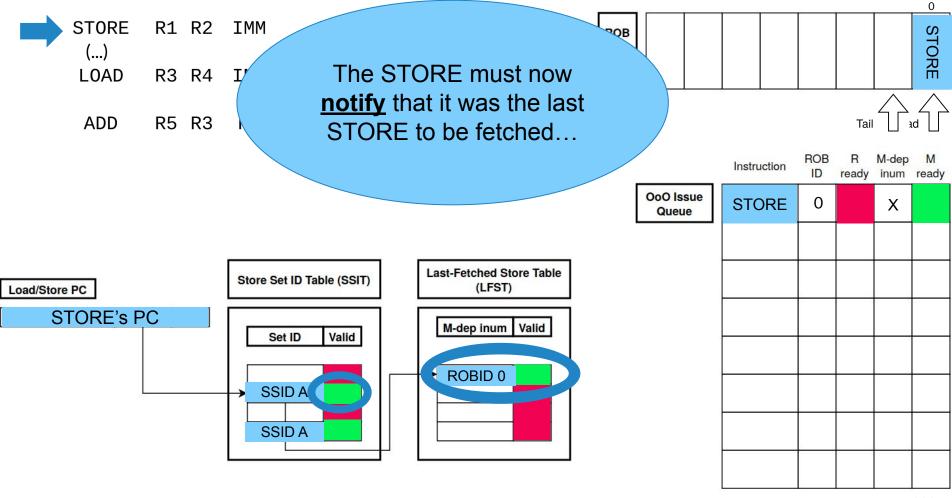


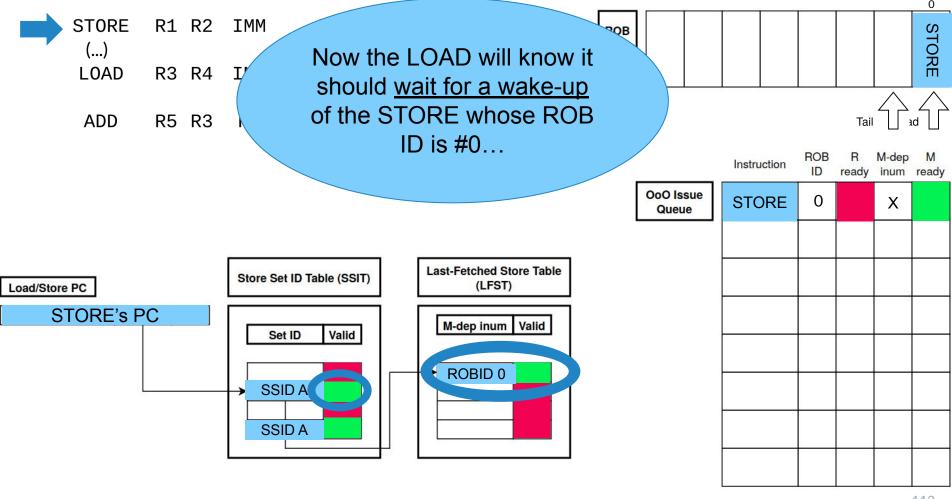


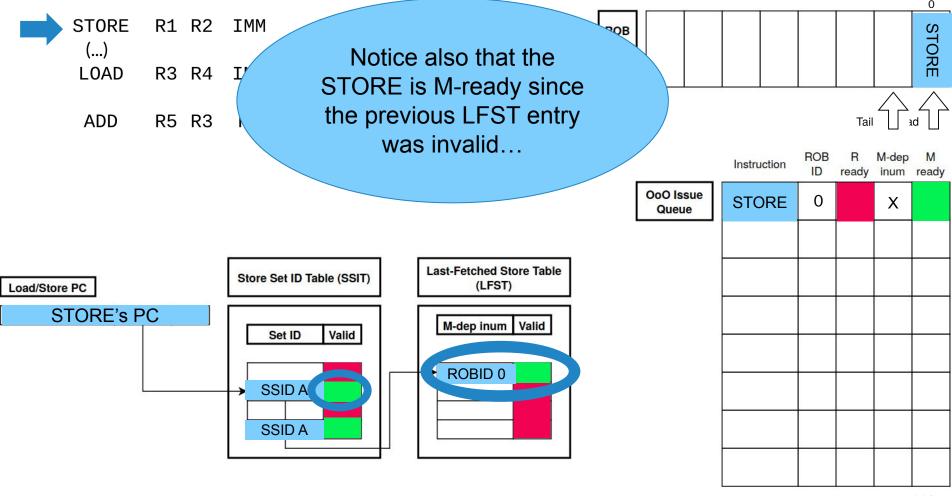


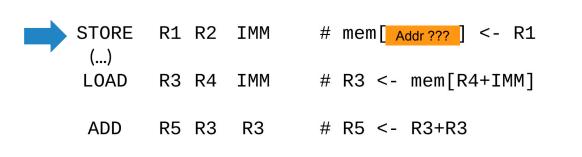


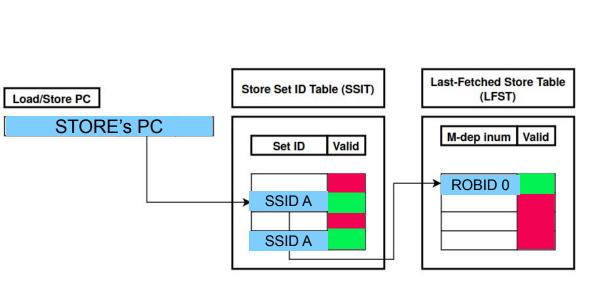


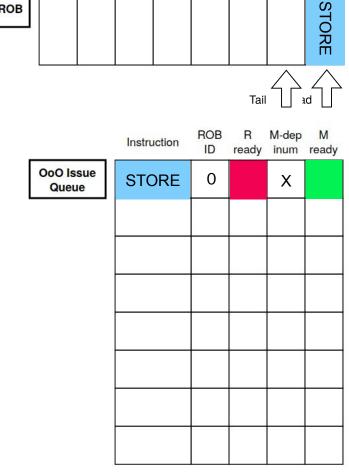




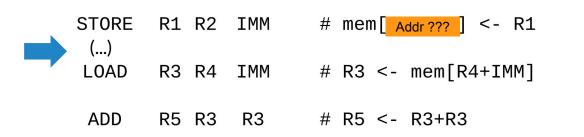




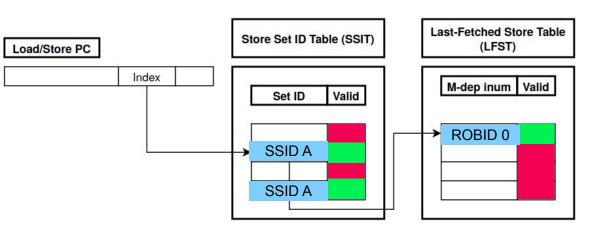


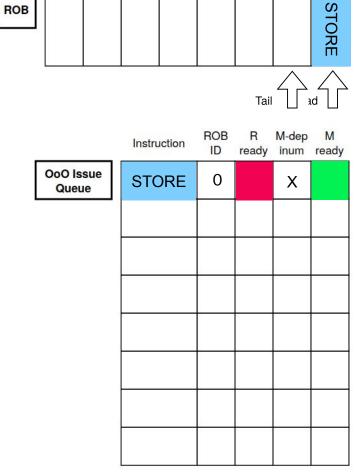


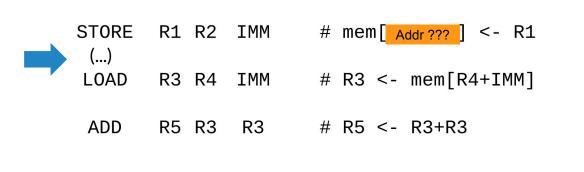
ROB



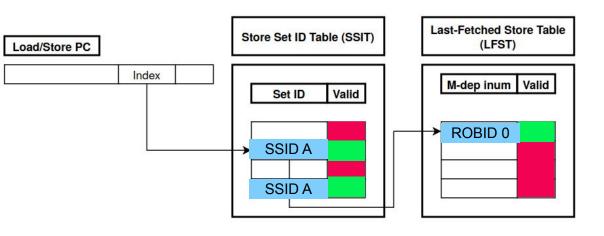
R4-producer instr.

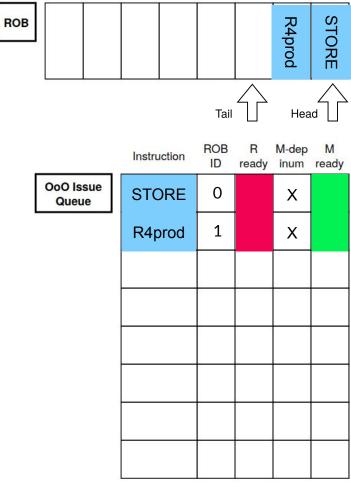


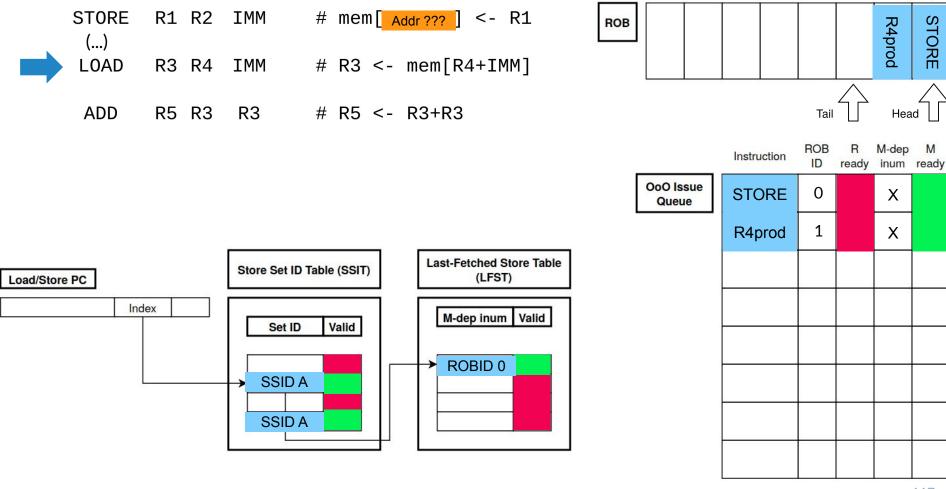


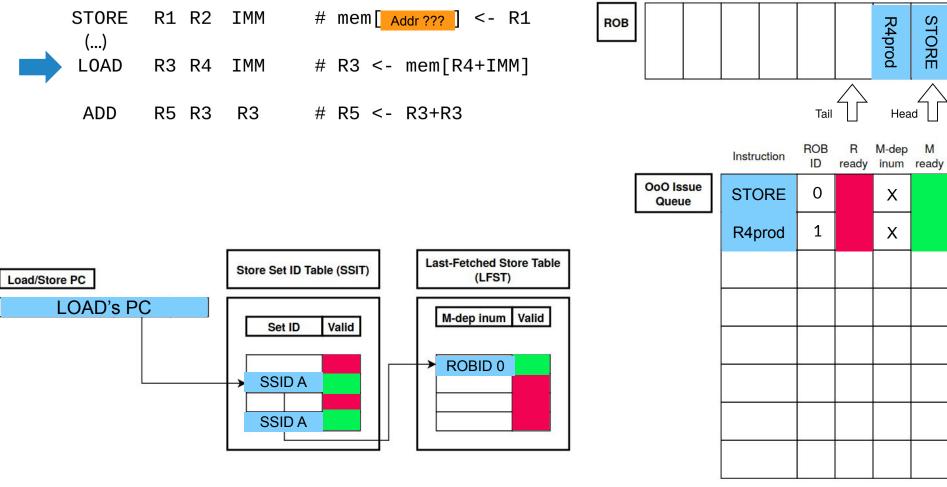


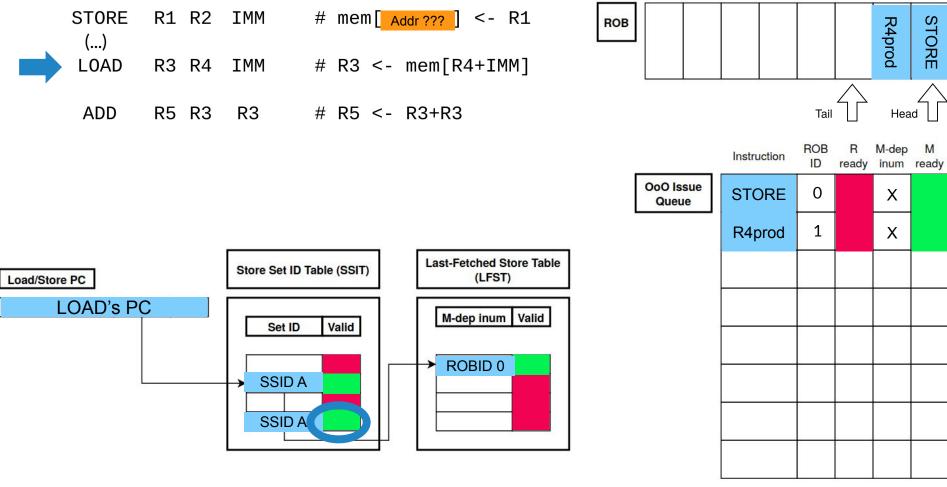
R4-producer instr.

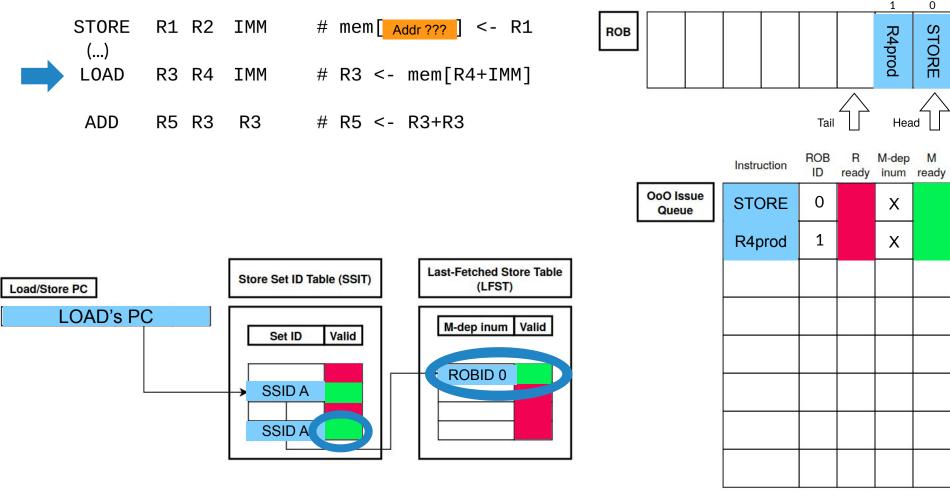


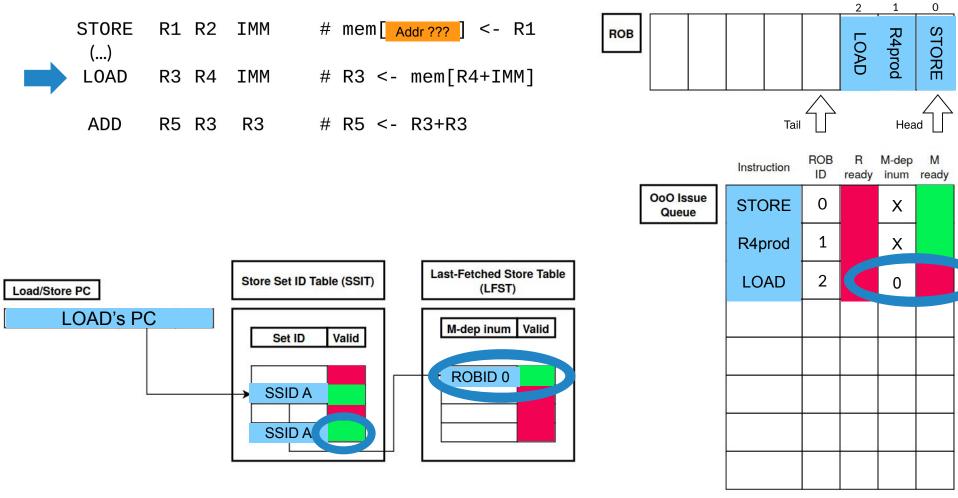


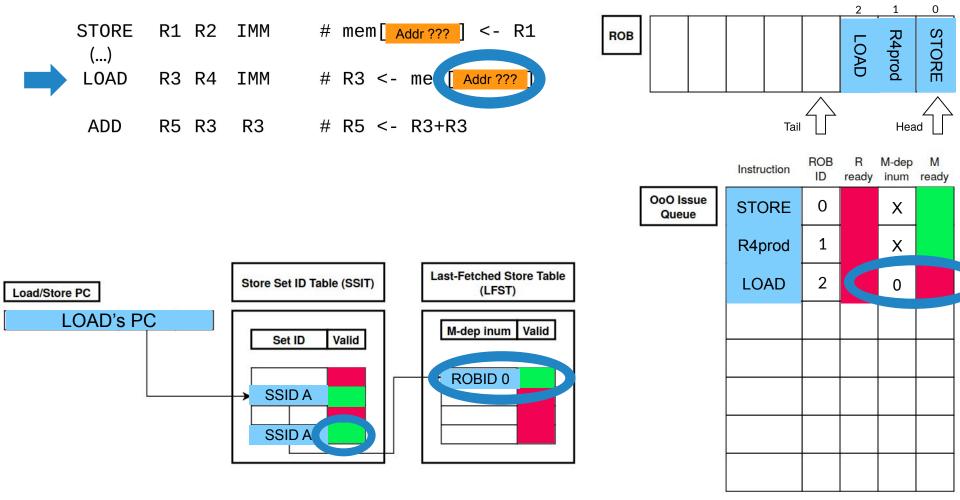


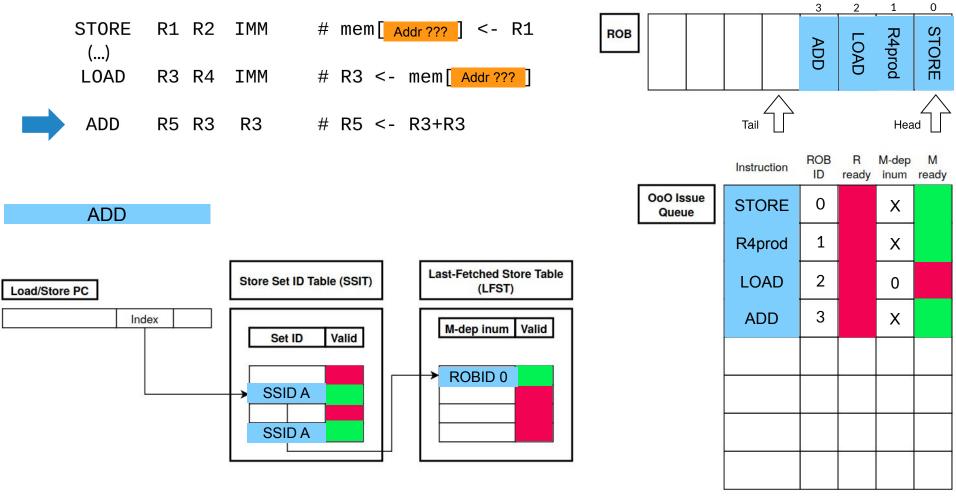


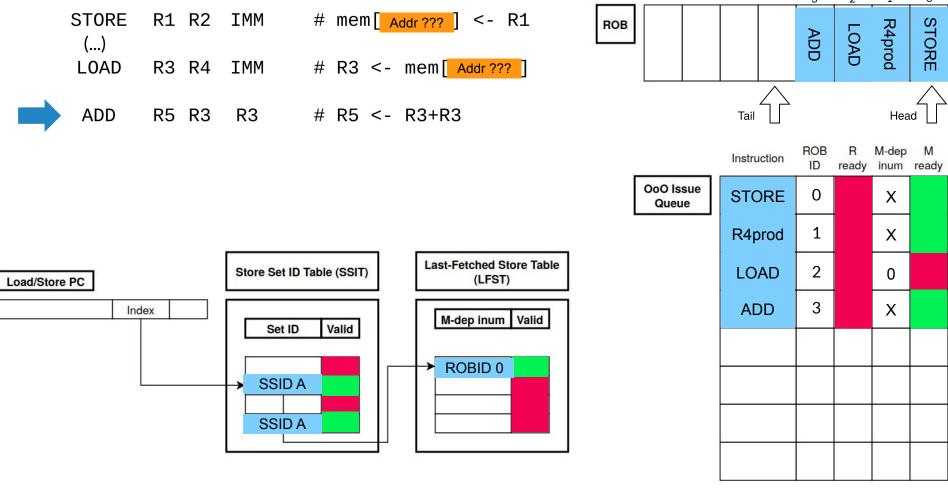


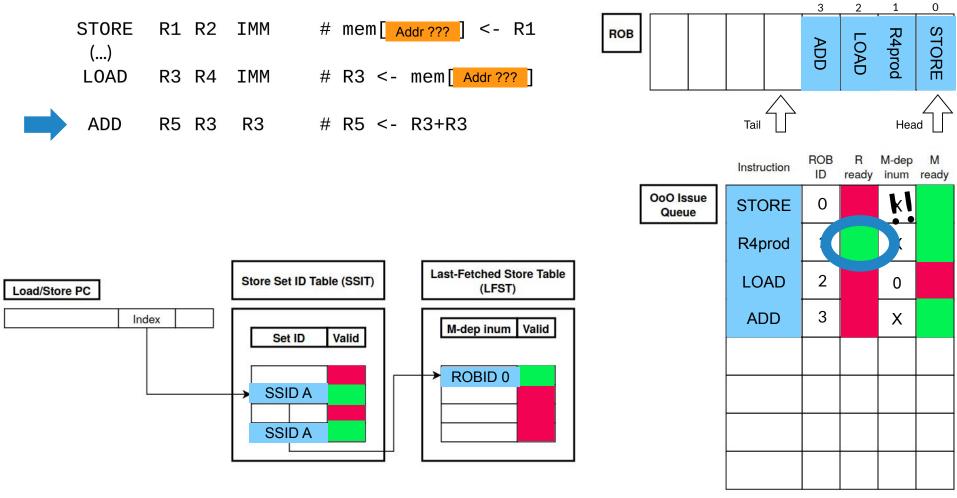


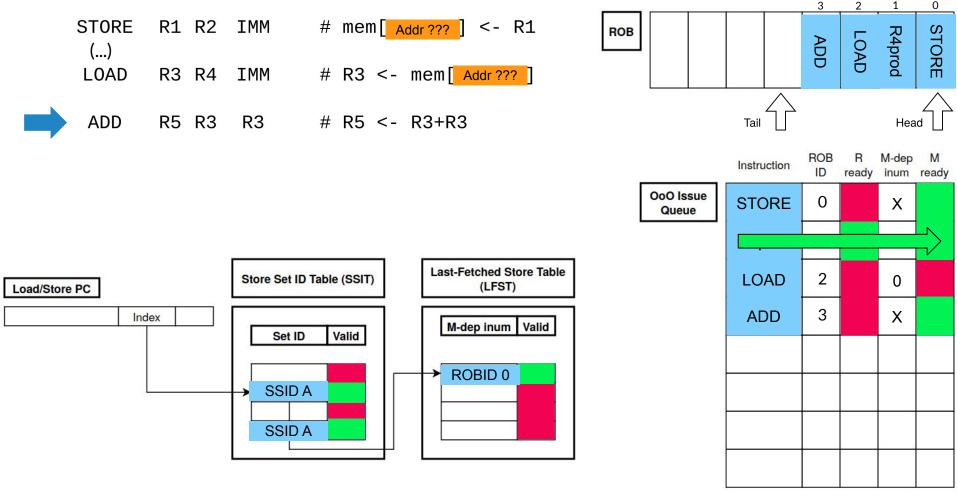


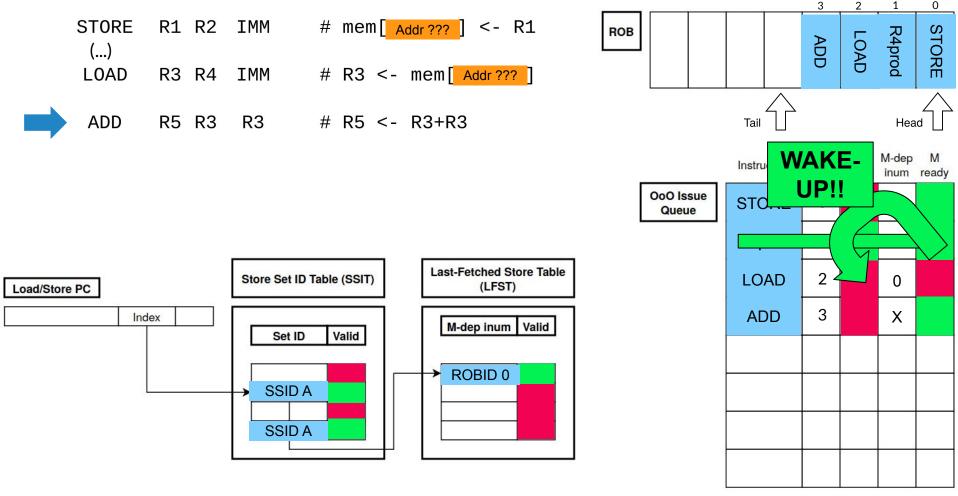


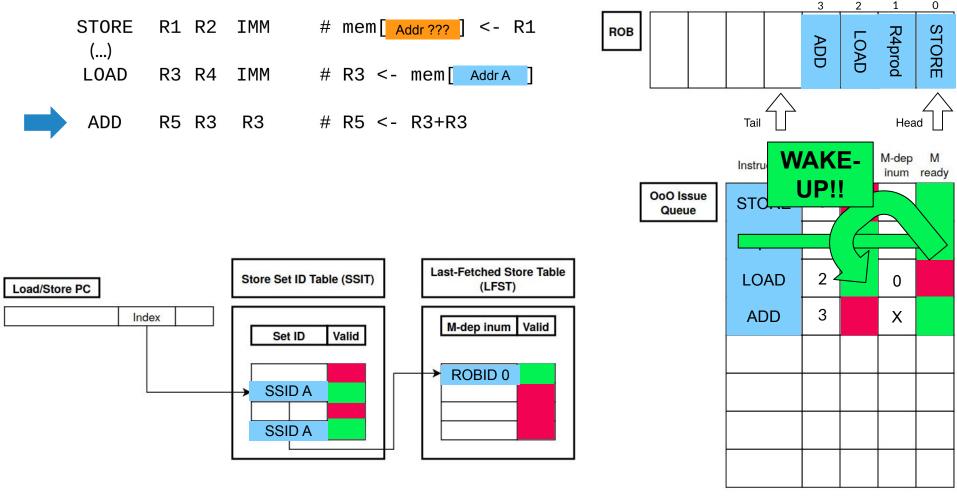


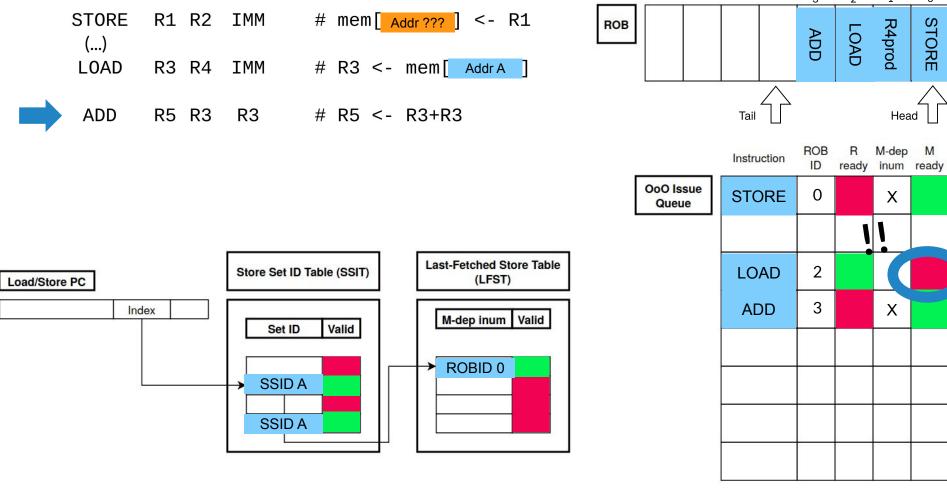


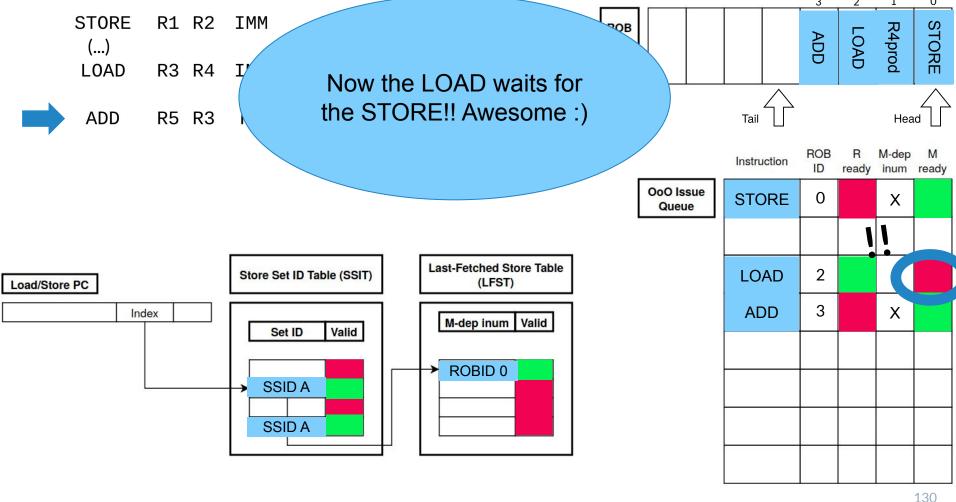


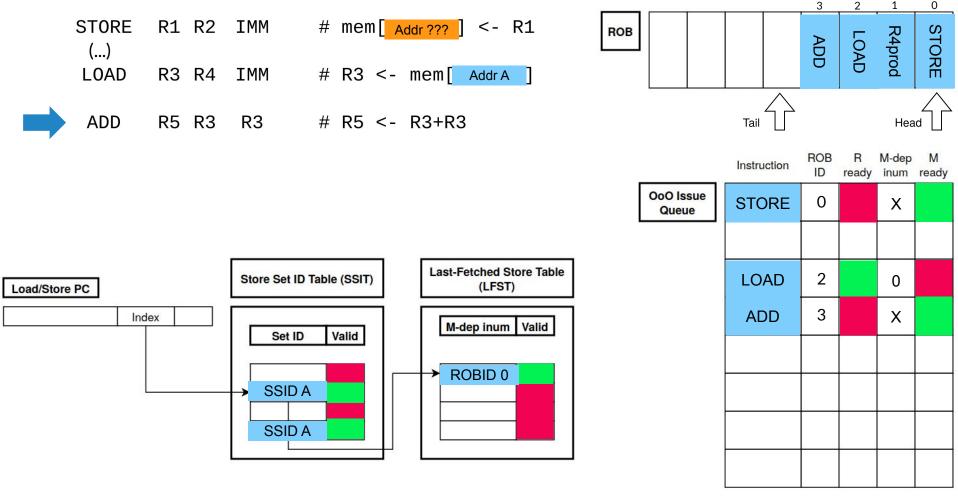


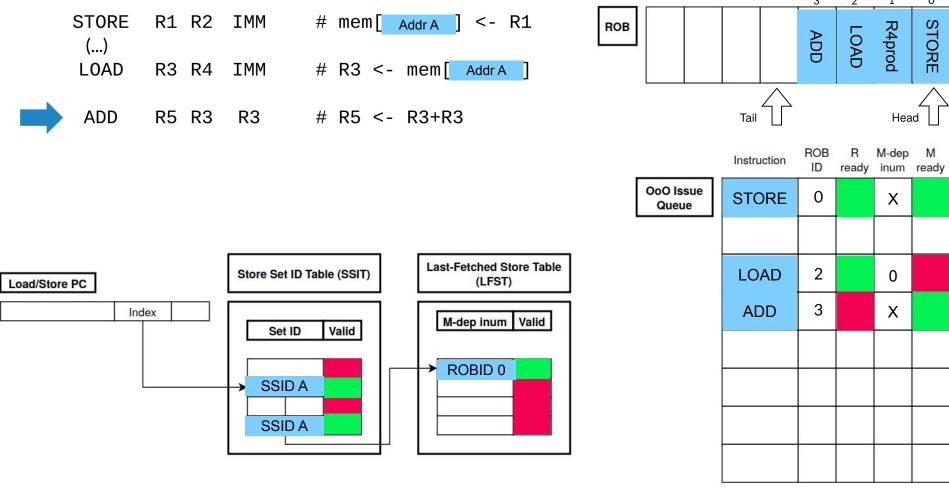


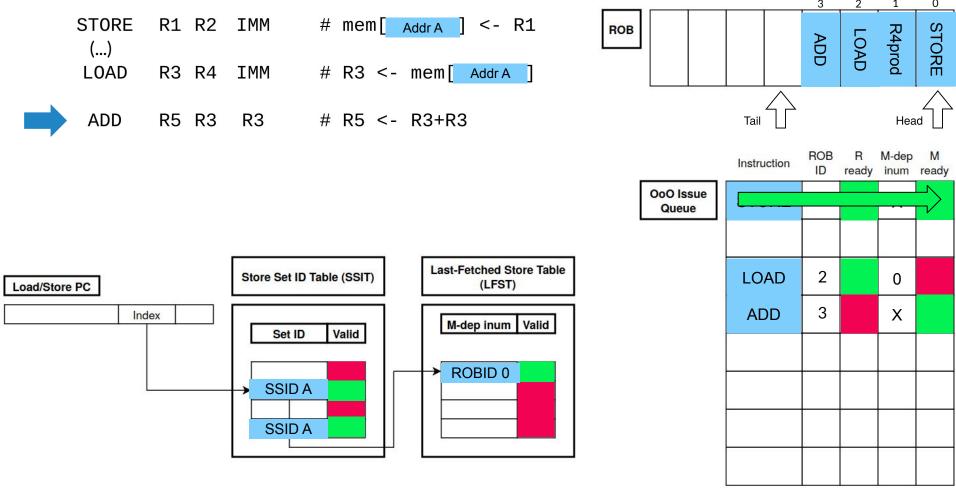


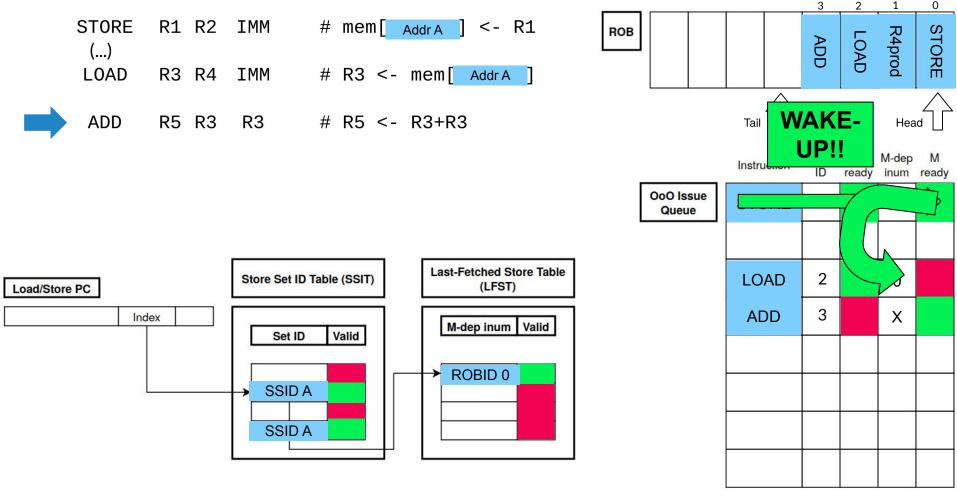


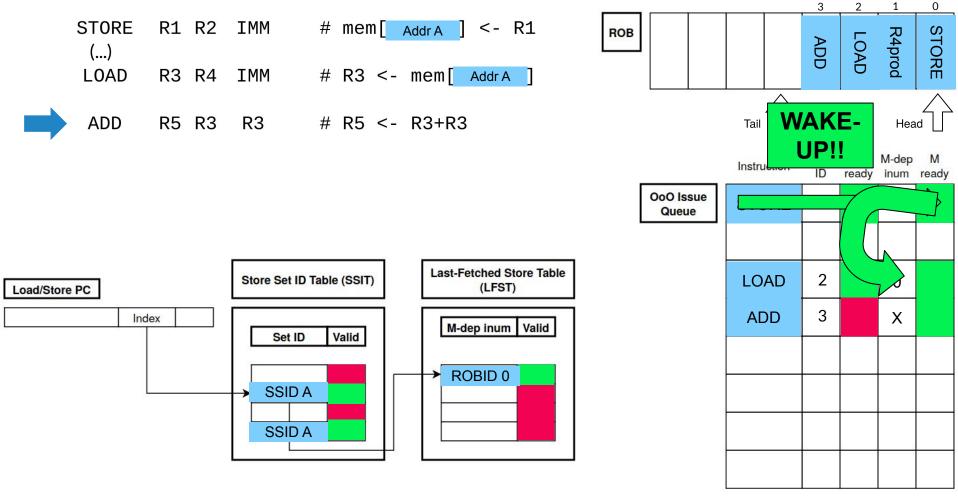


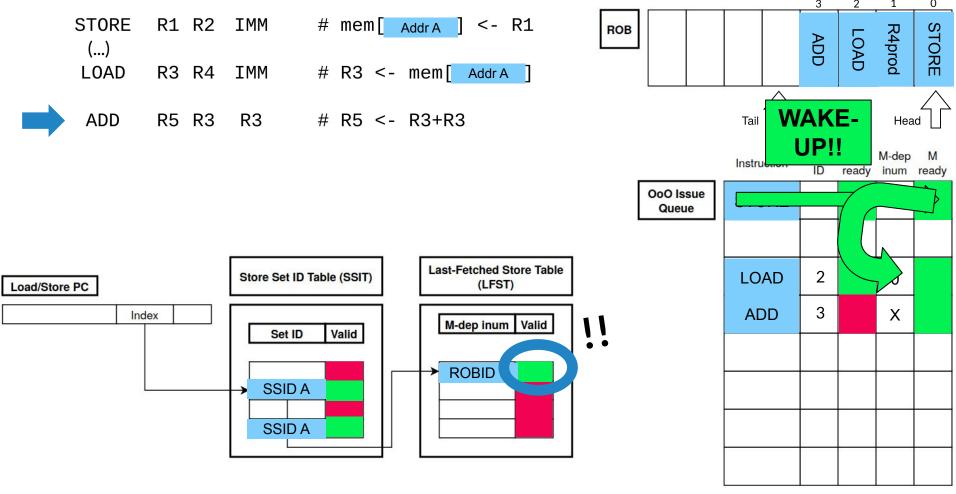


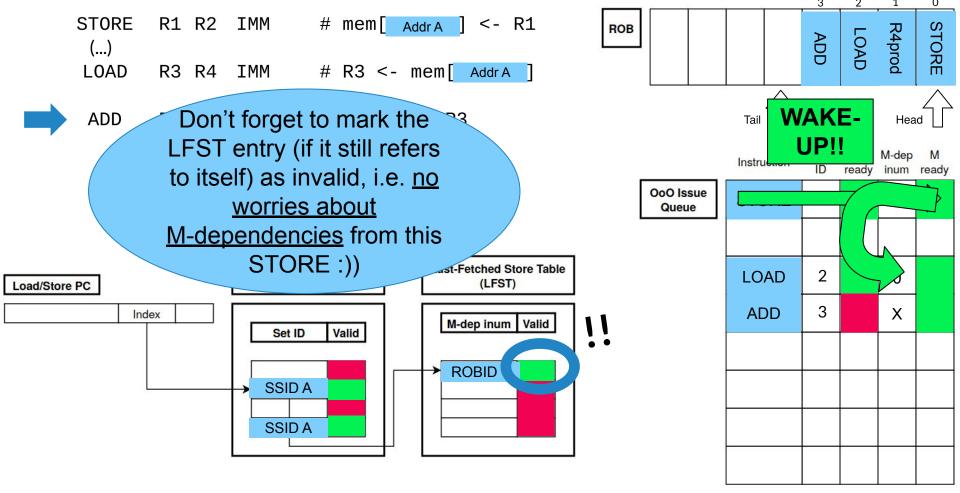


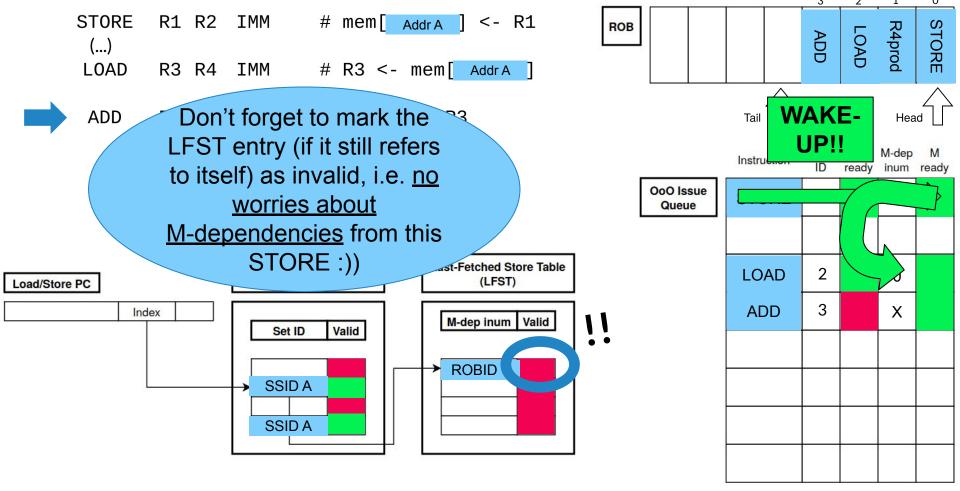


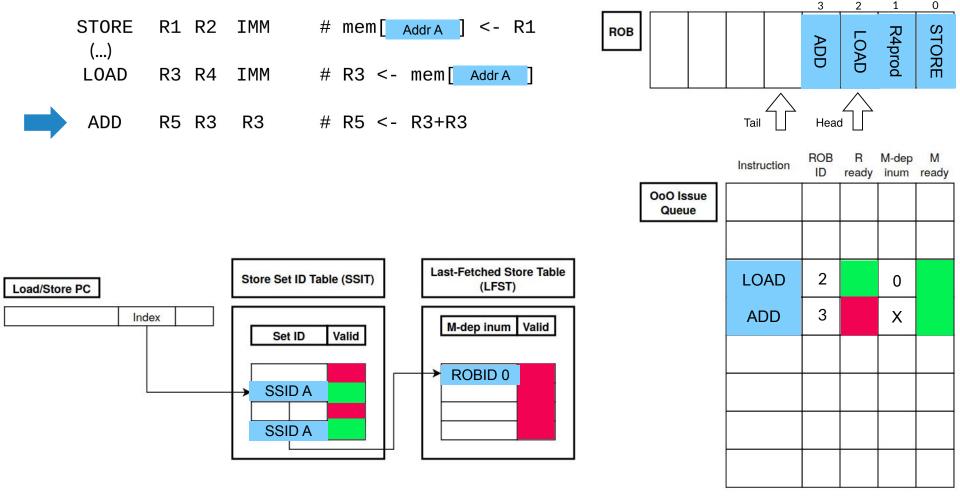


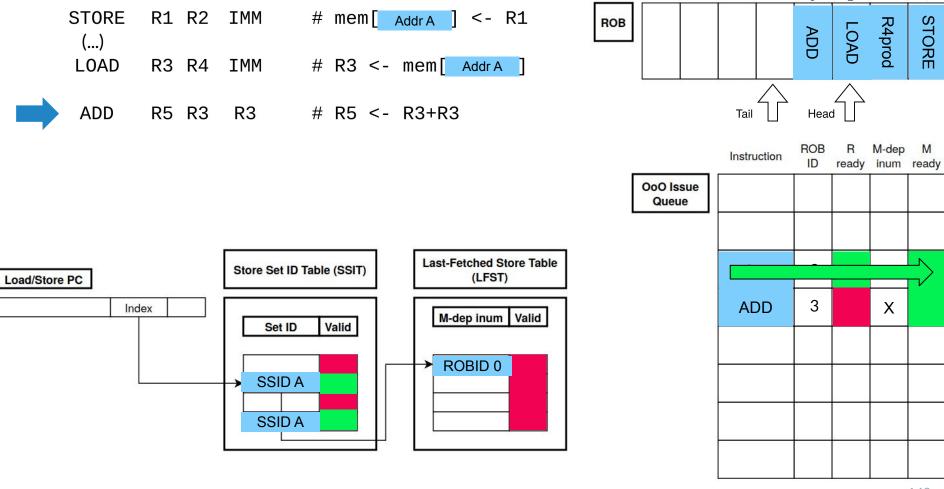


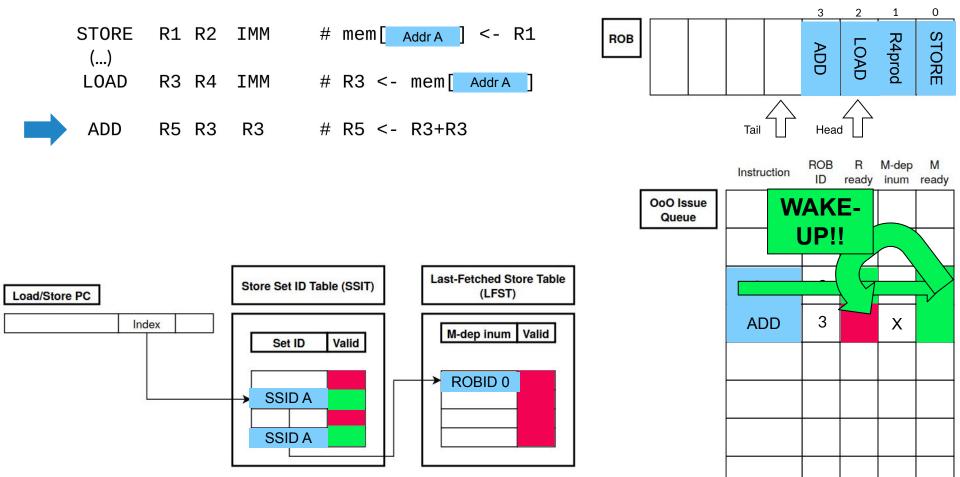


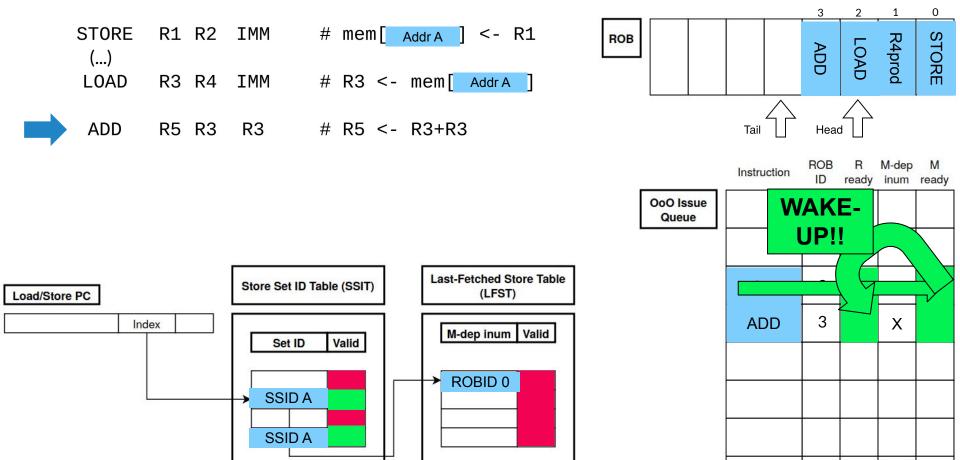


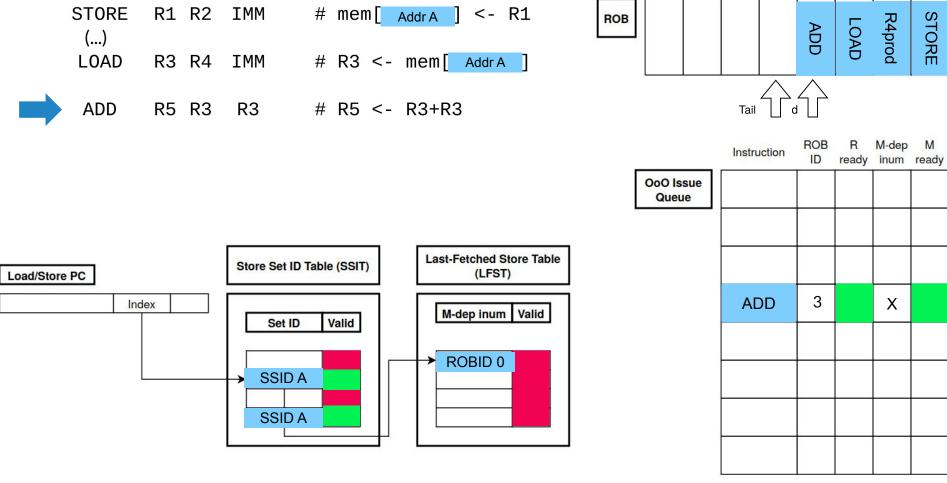


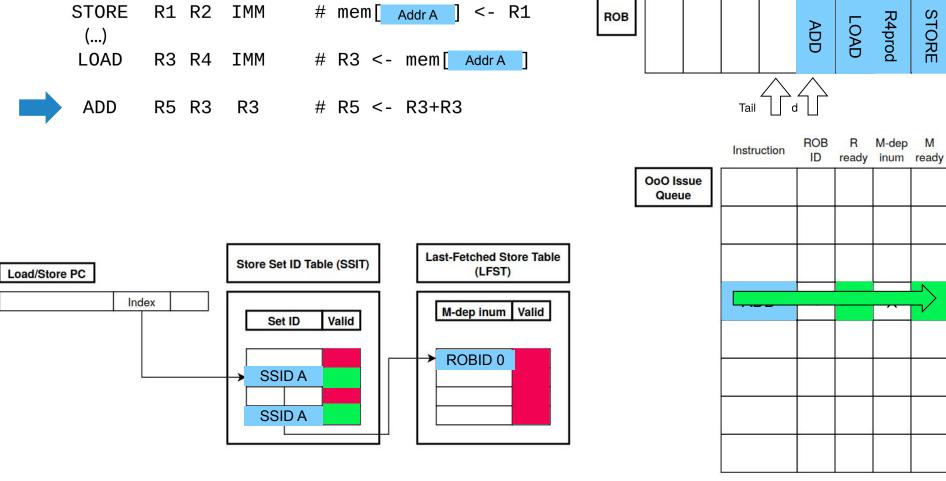


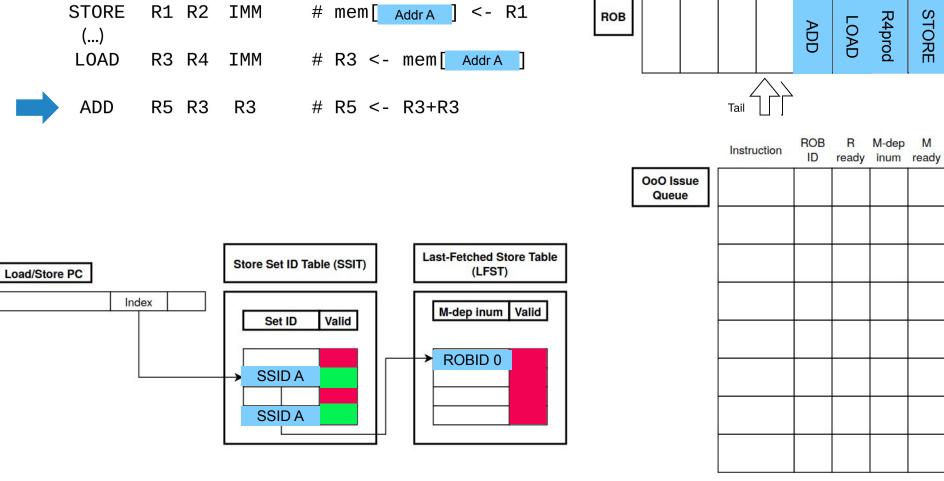


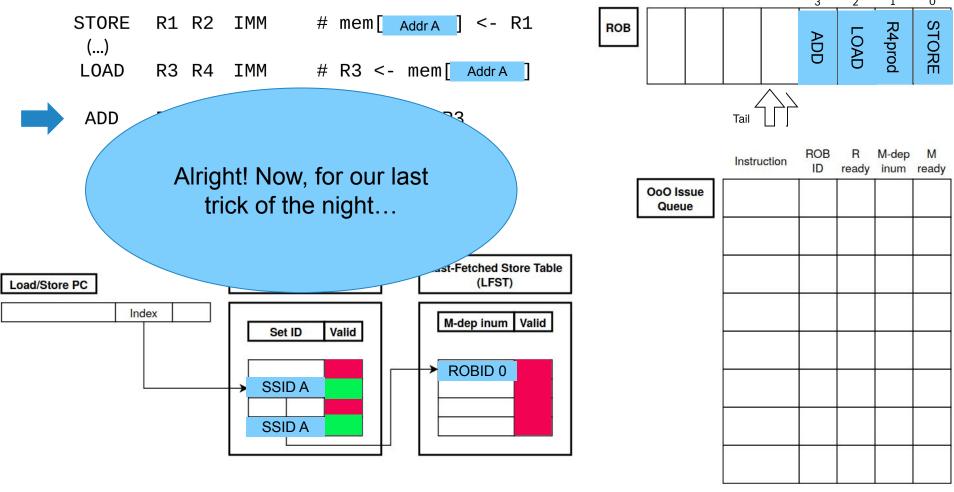


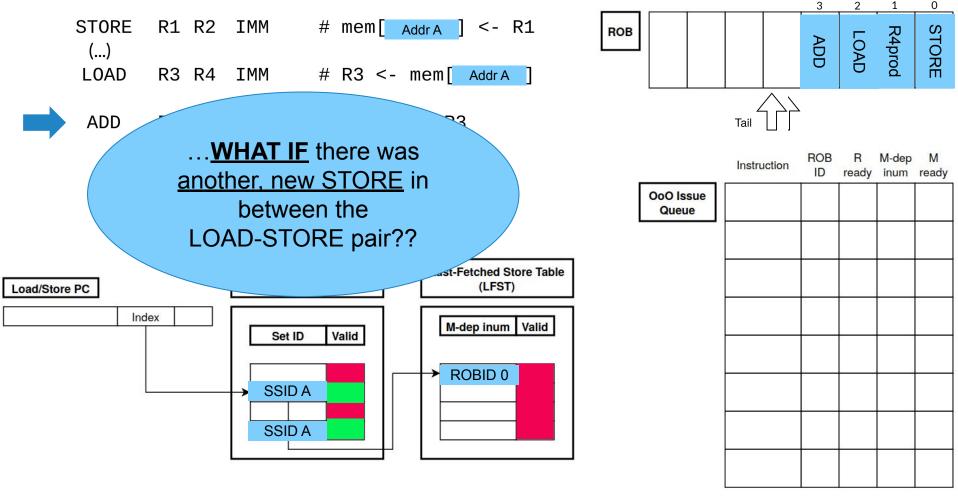


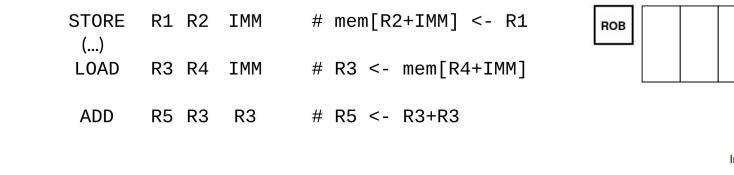


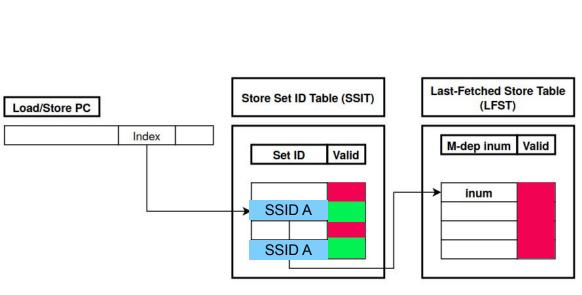


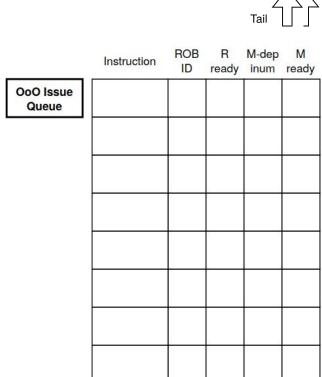


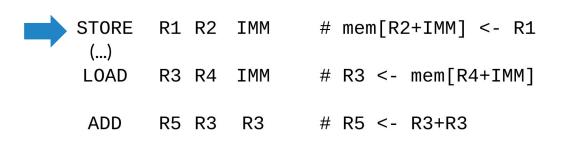


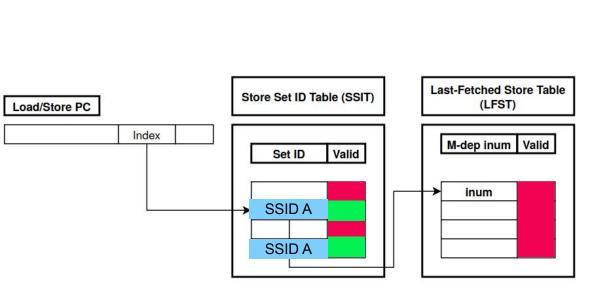


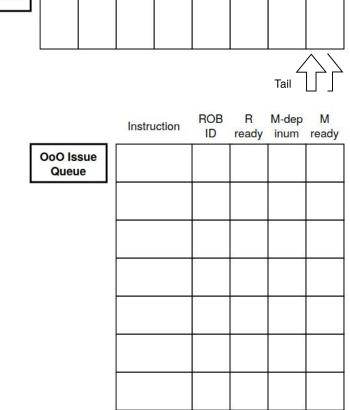


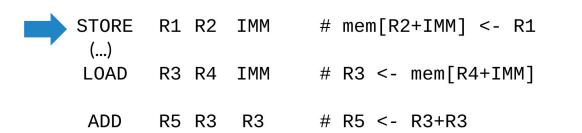


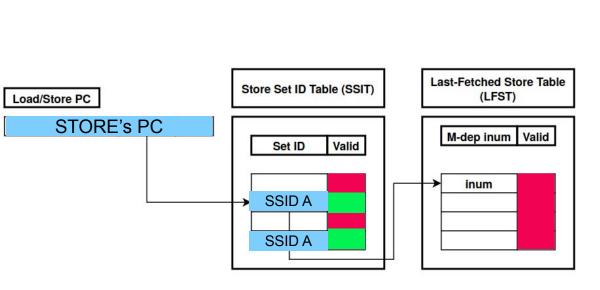


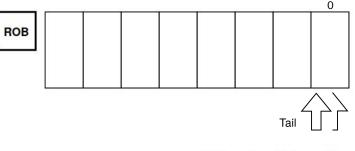


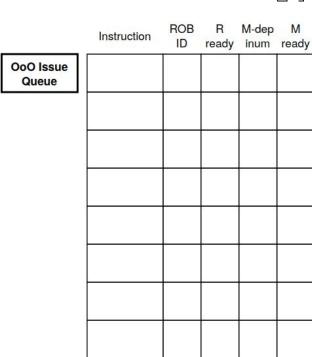


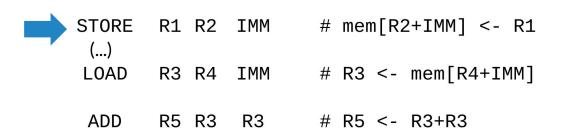


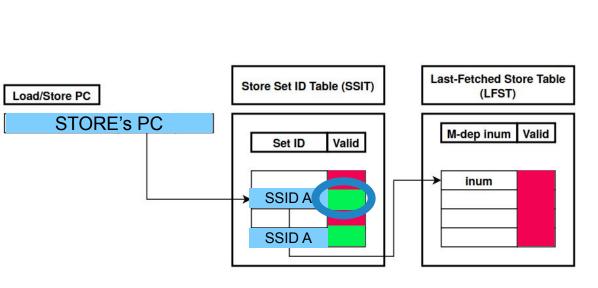


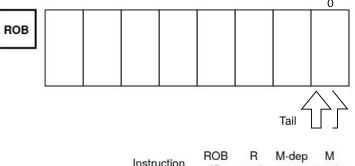


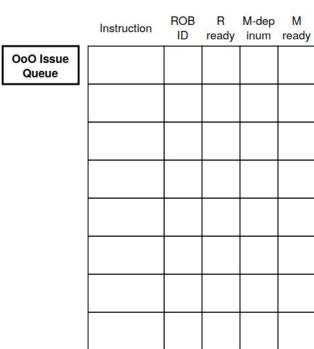


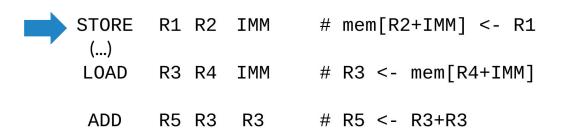


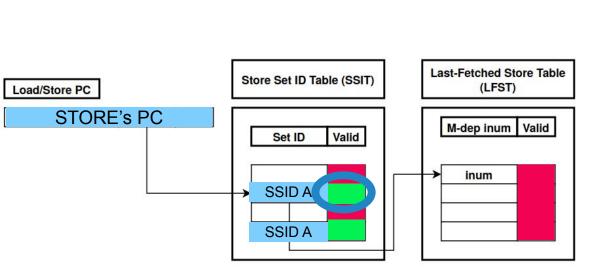


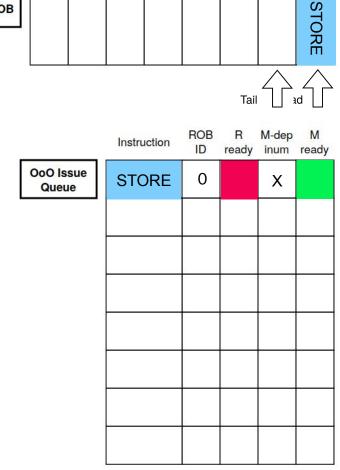


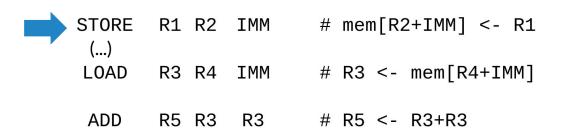


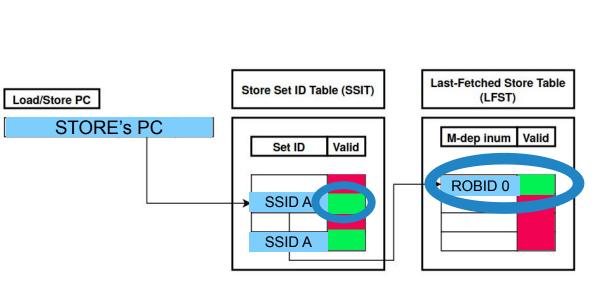


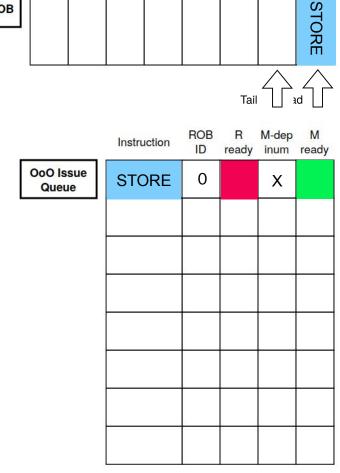


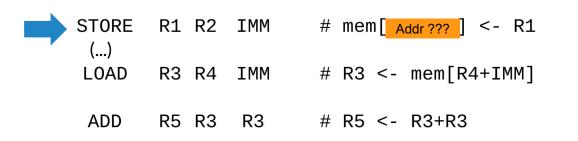


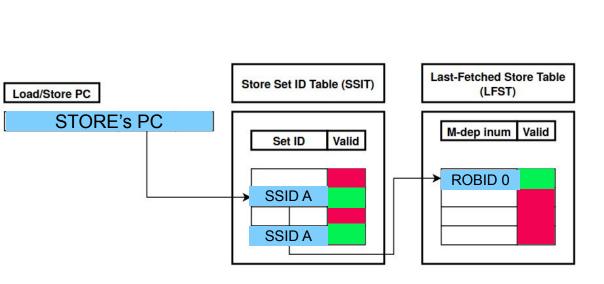


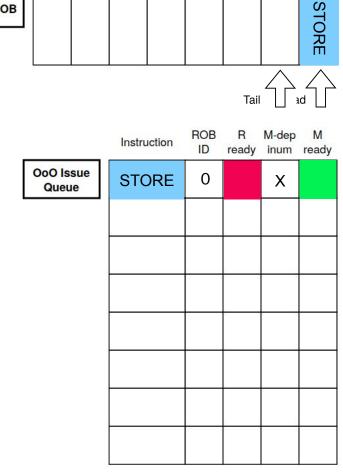


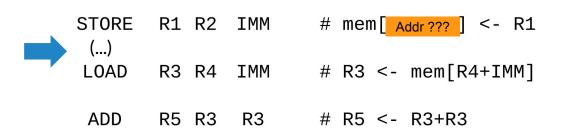


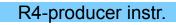


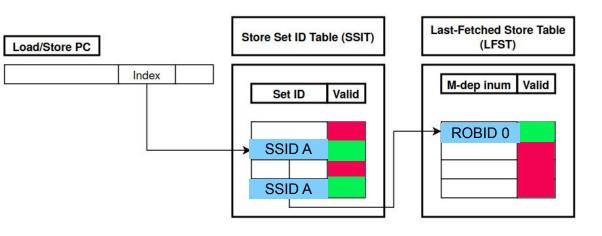


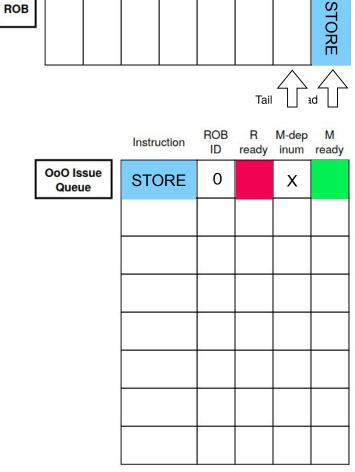


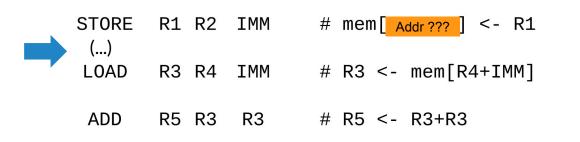




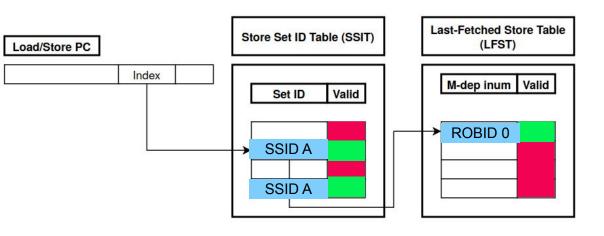


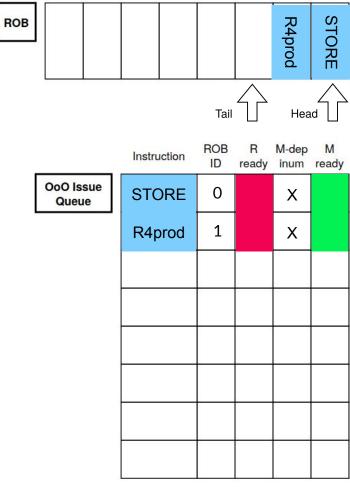


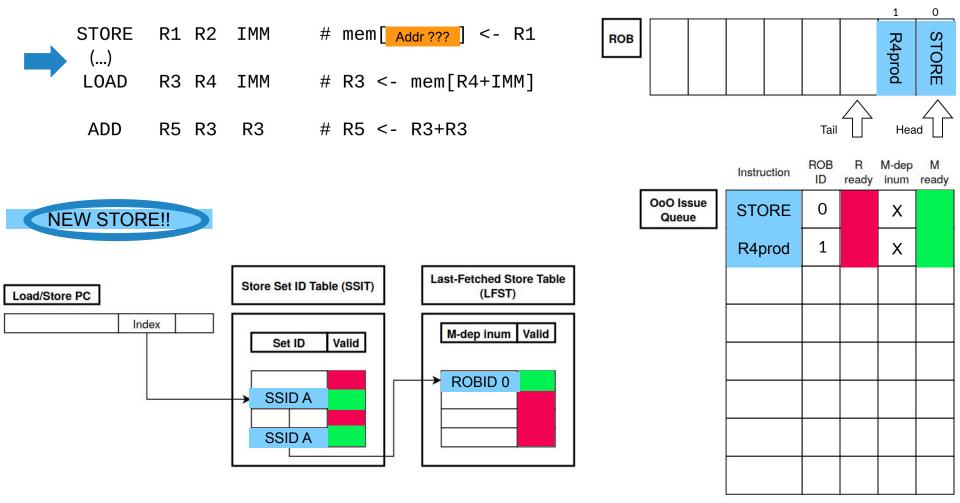


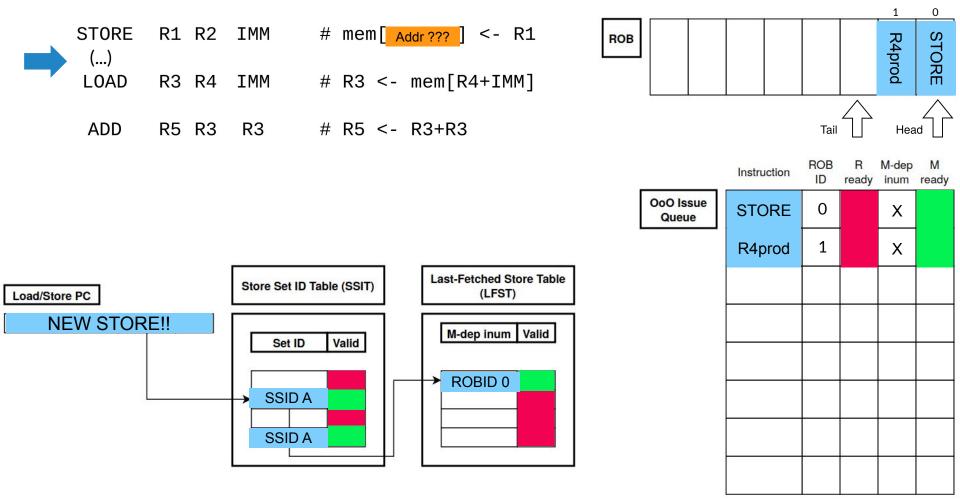


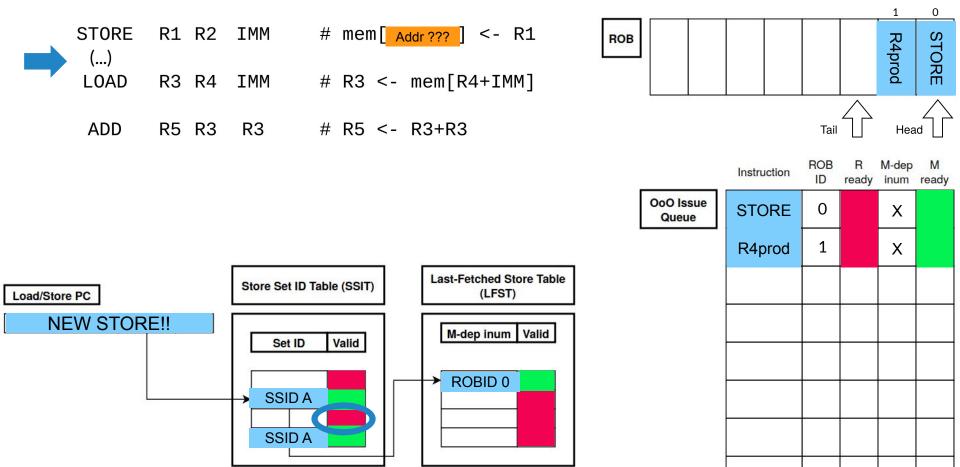
R4-producer instr.

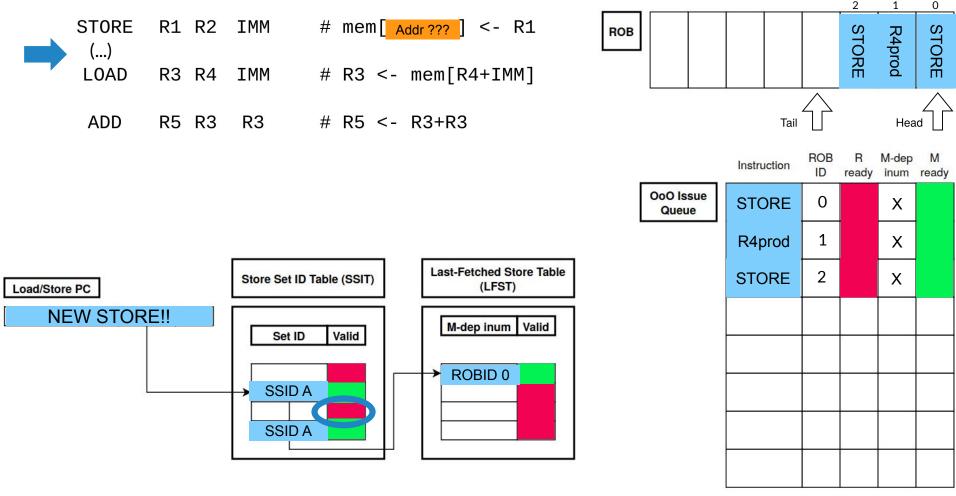


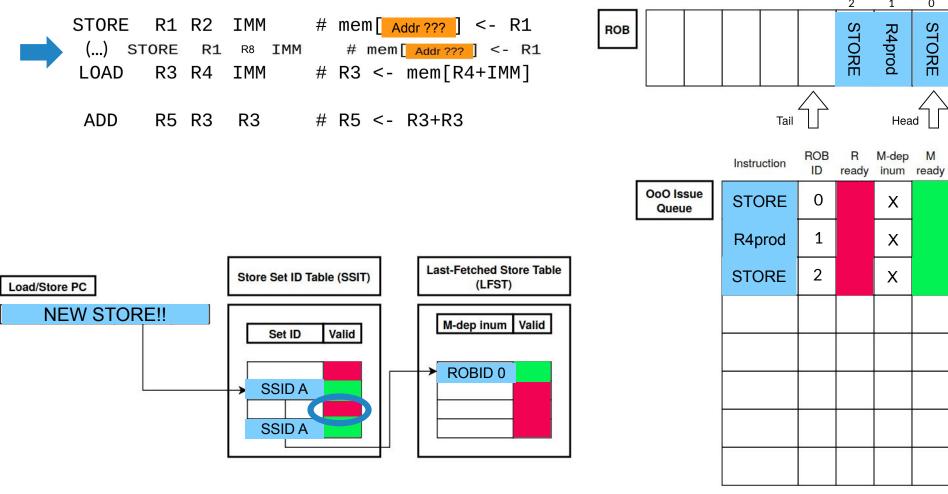


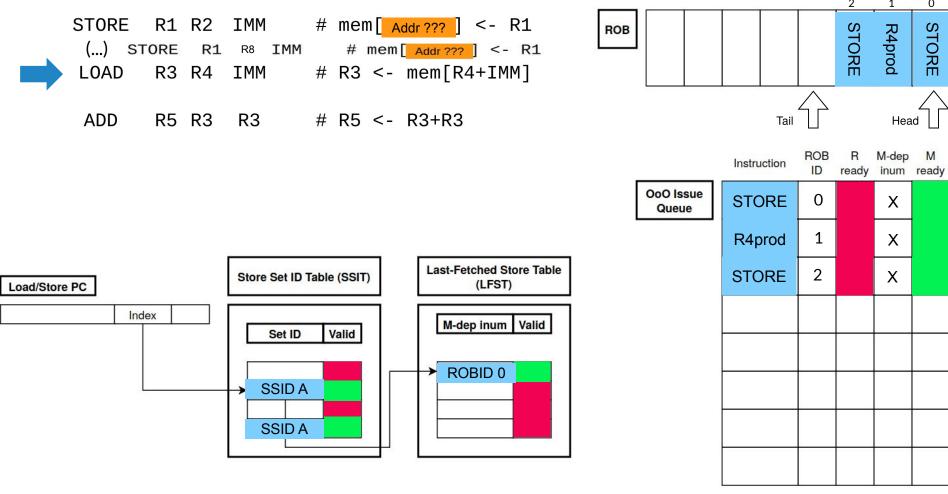


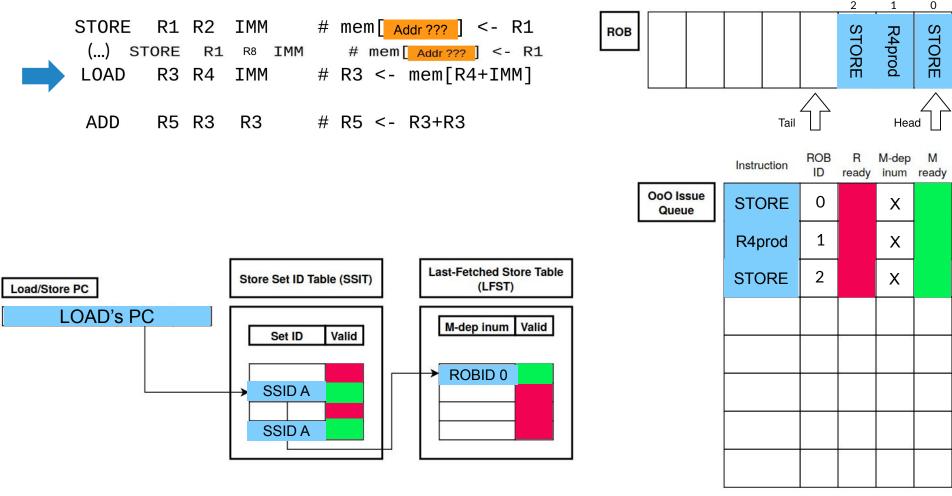


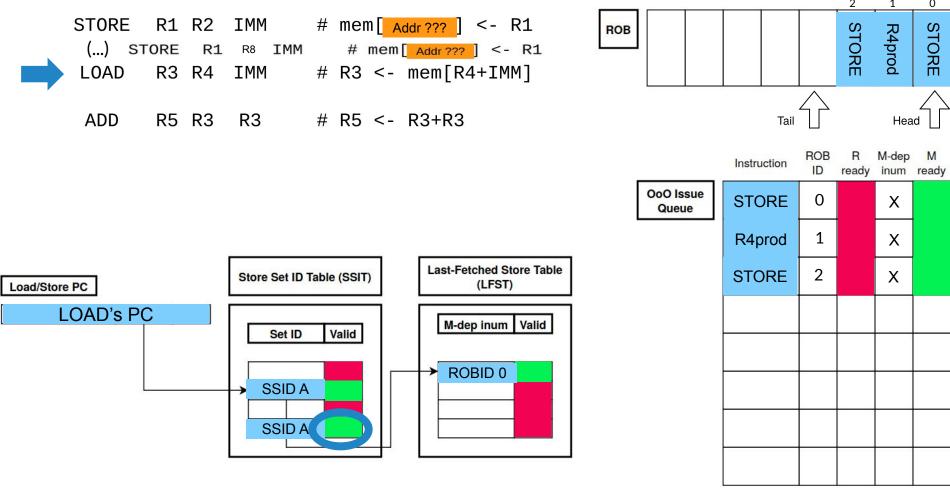


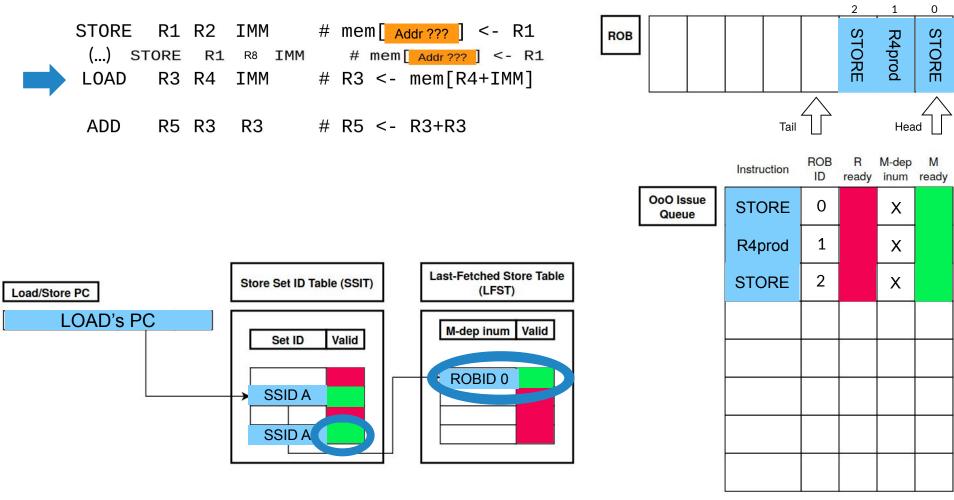


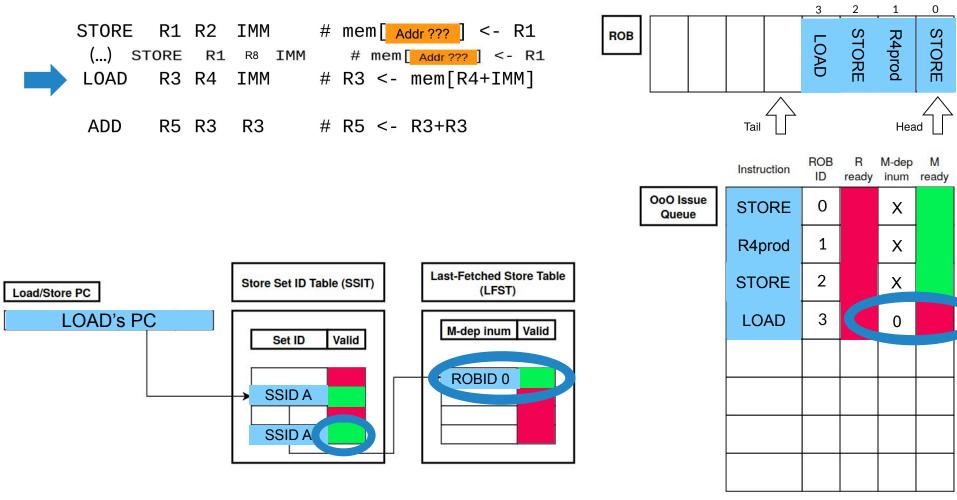


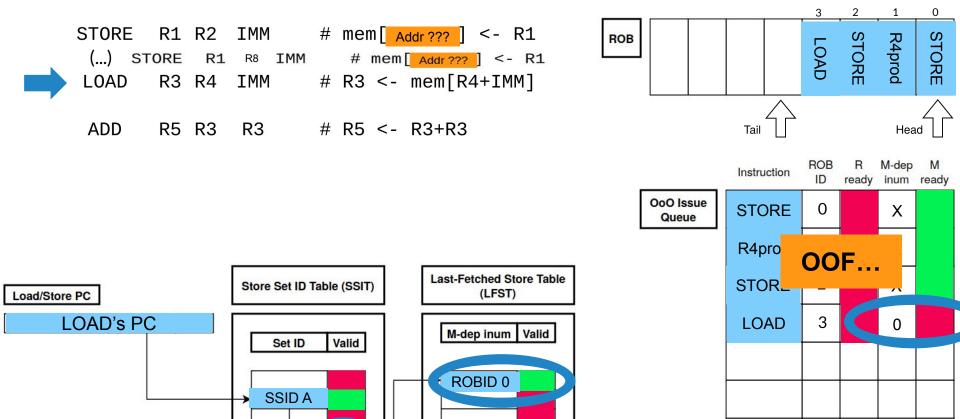




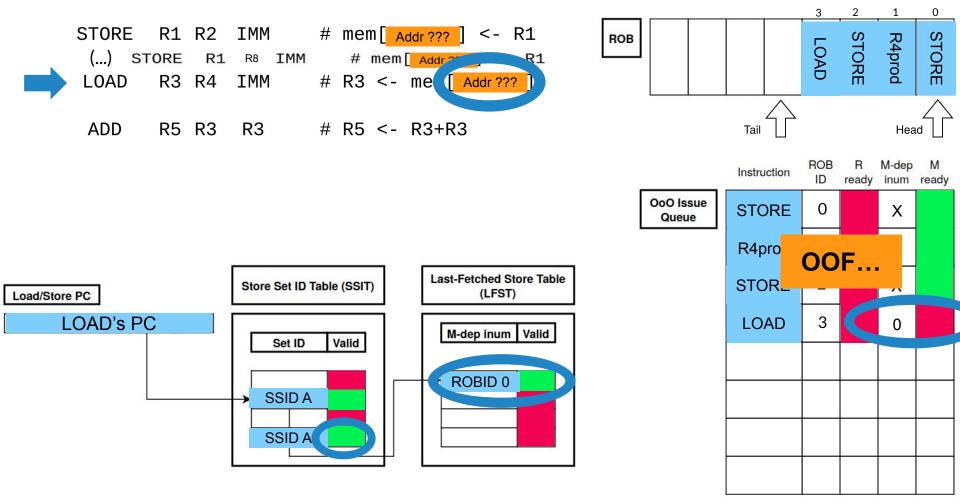


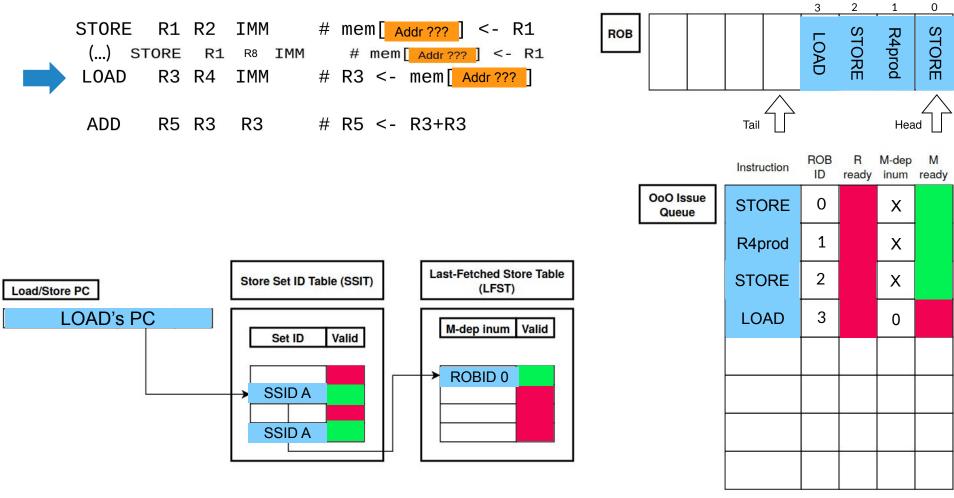


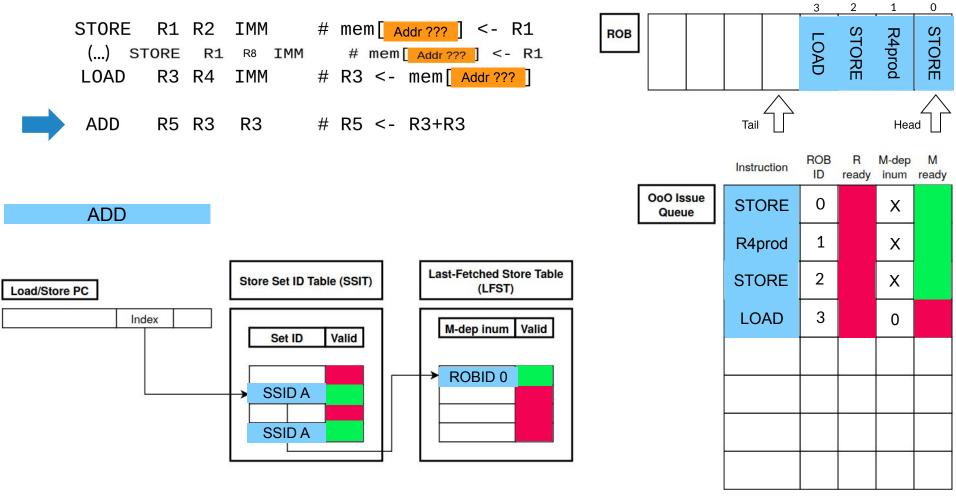


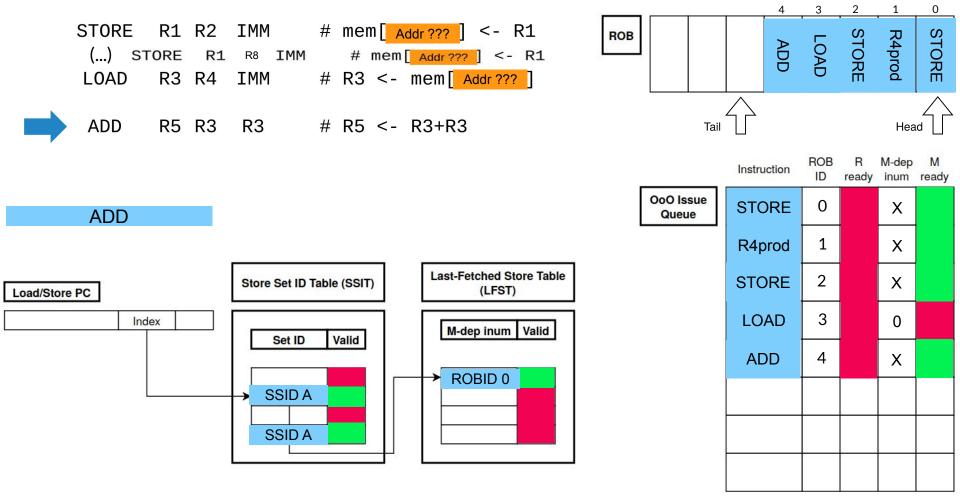


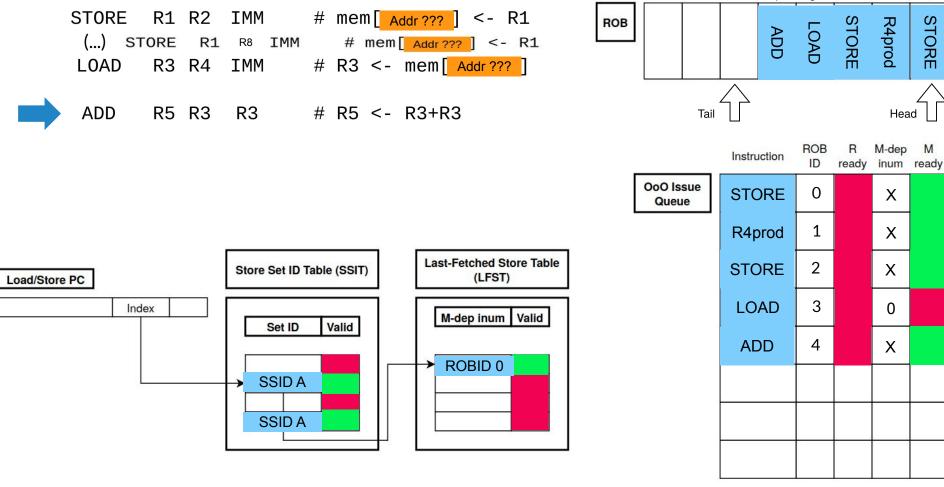
SSID A

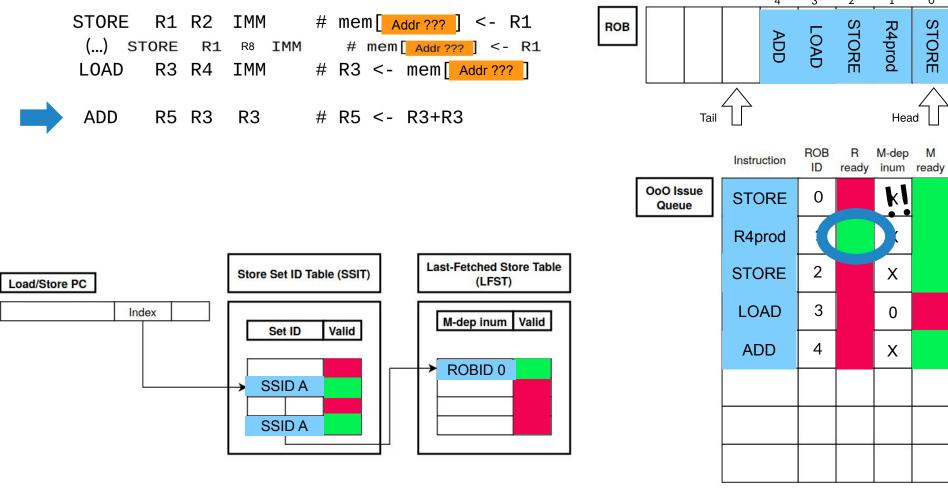


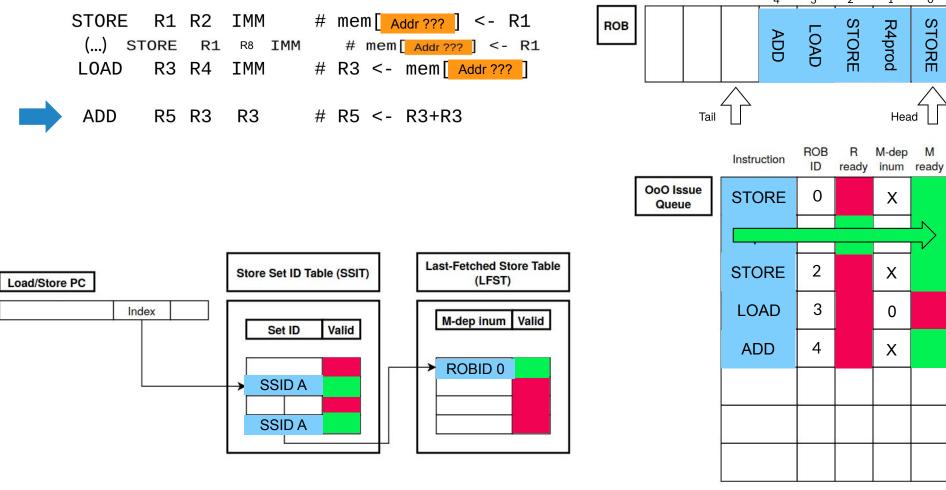


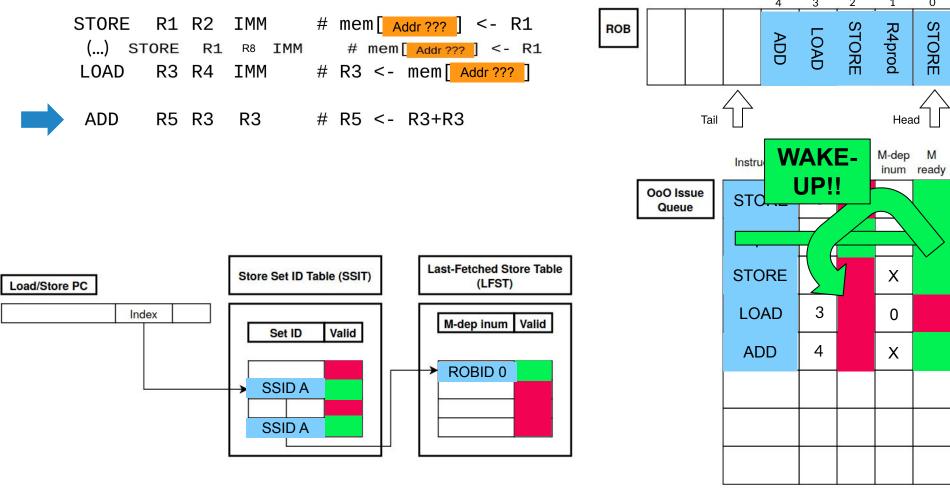


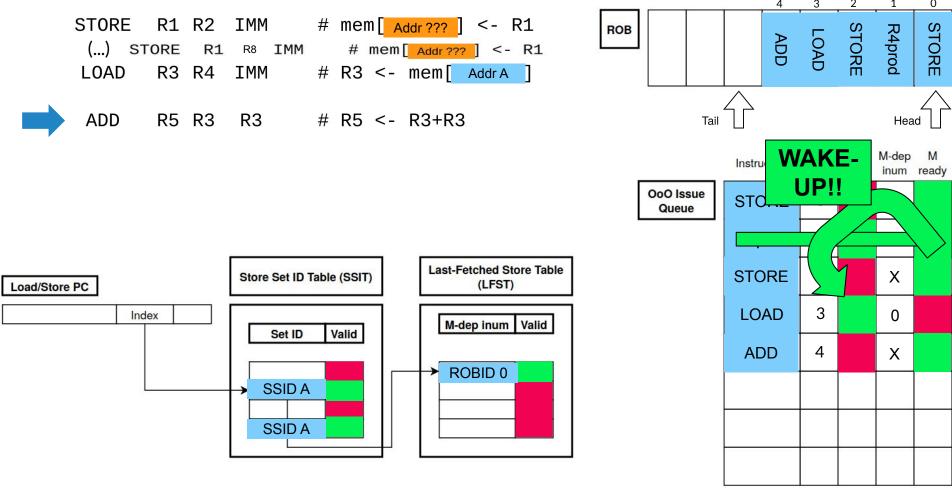


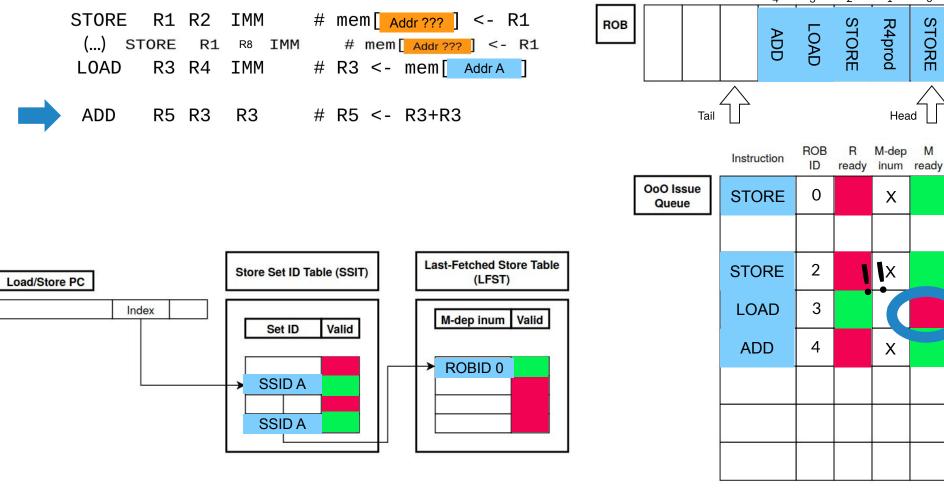


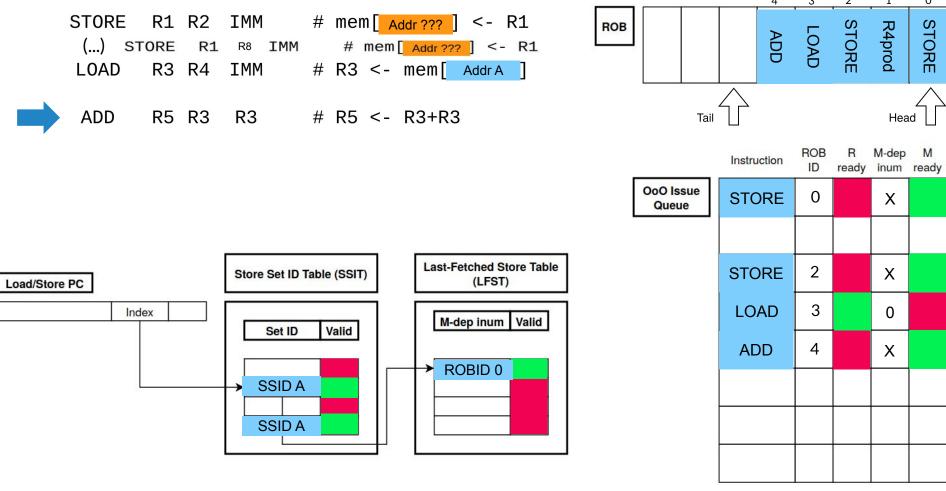


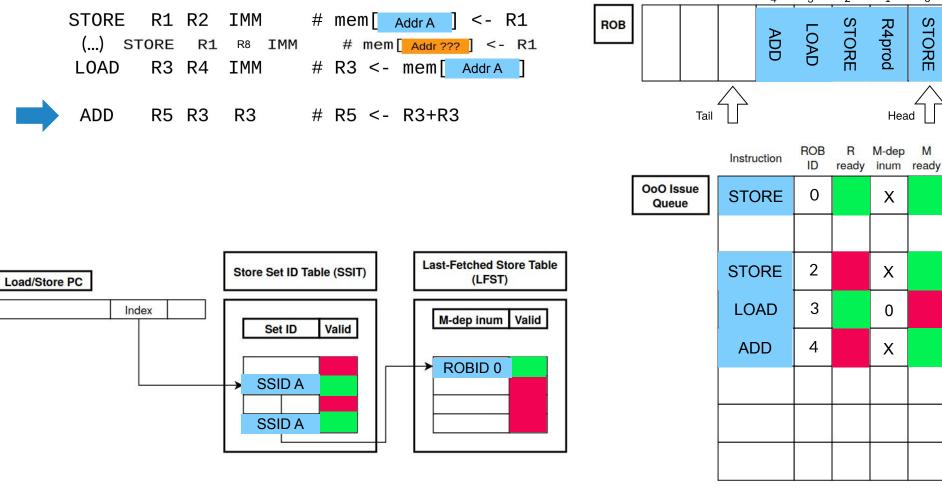


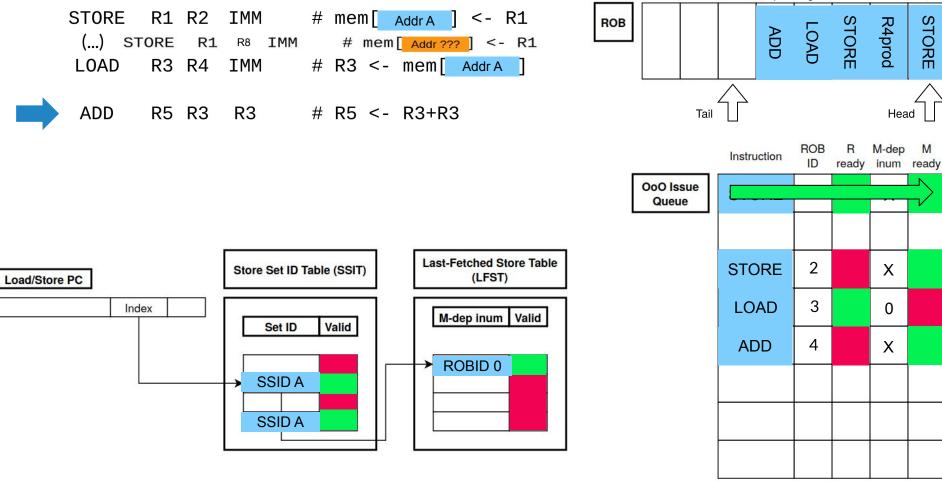


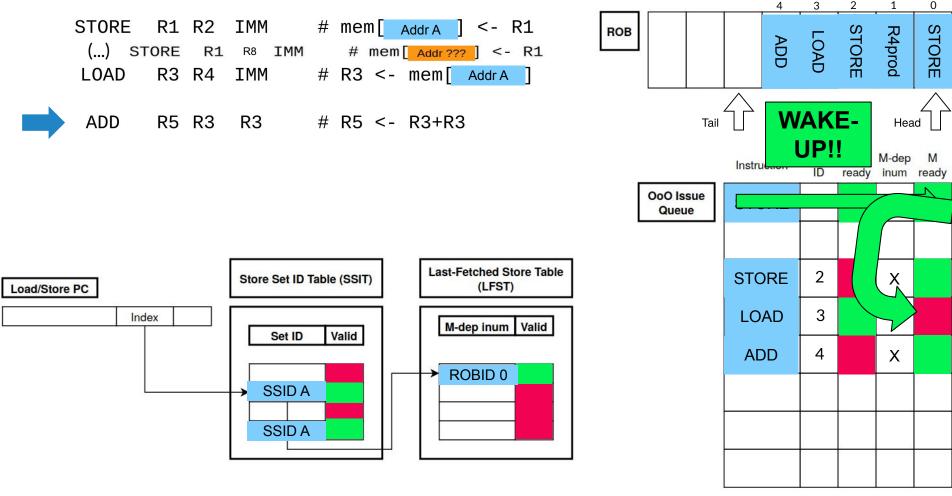


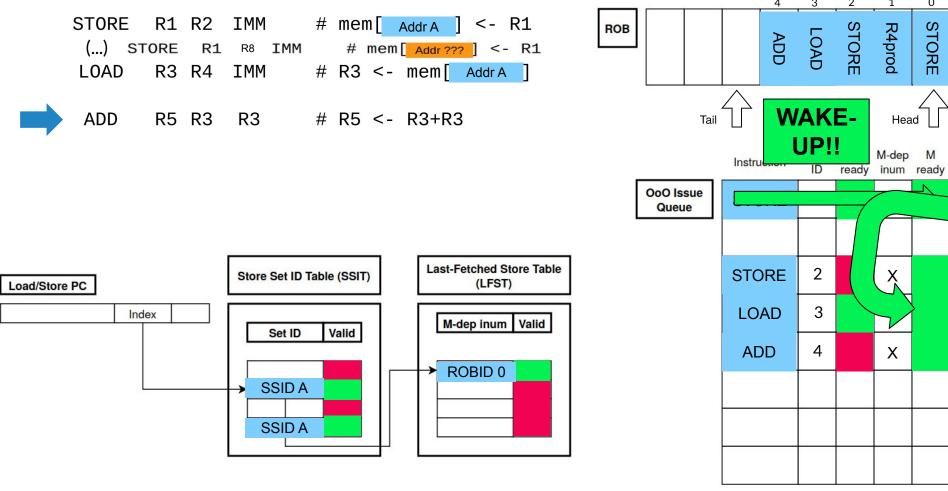


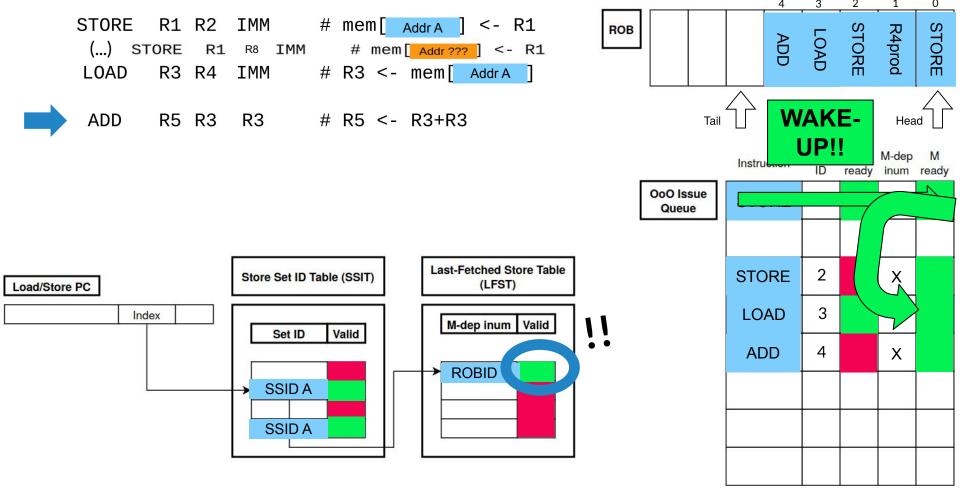


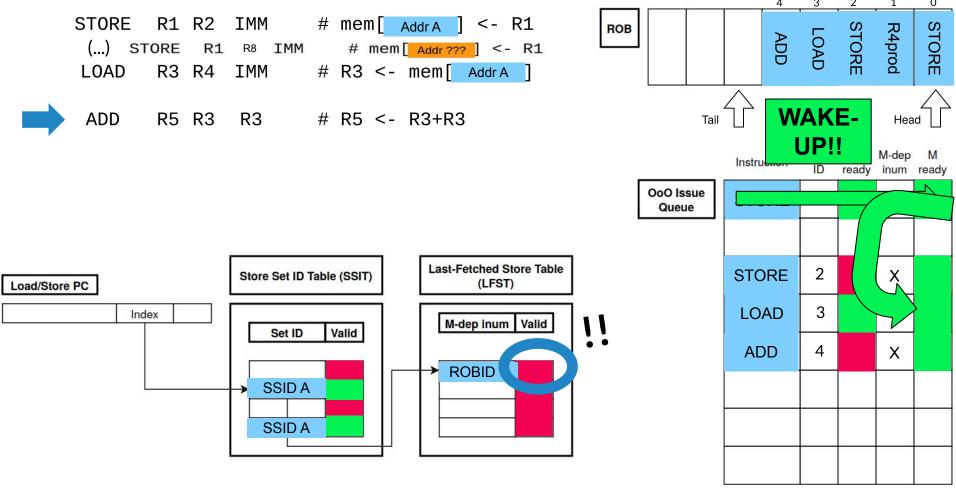


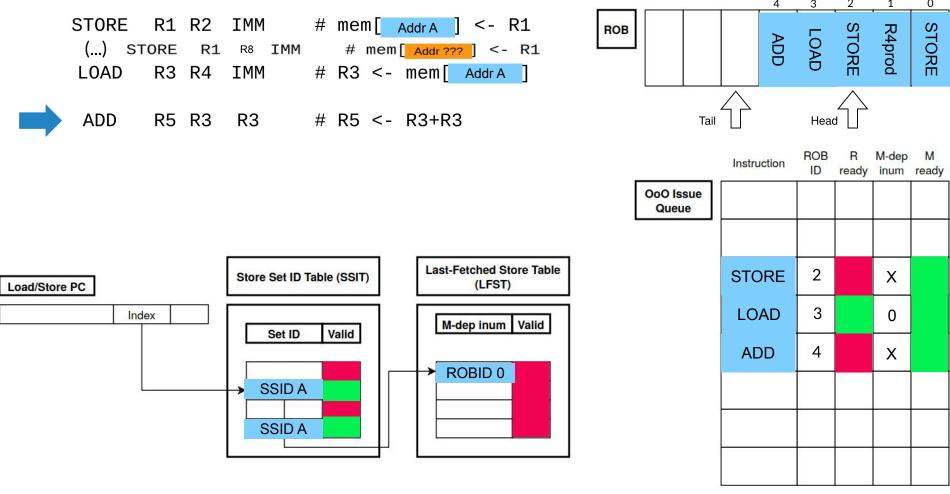


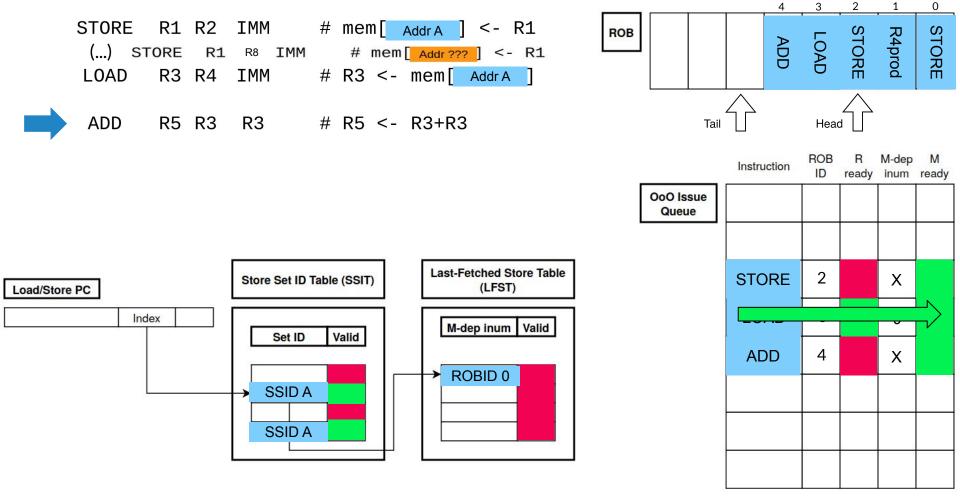


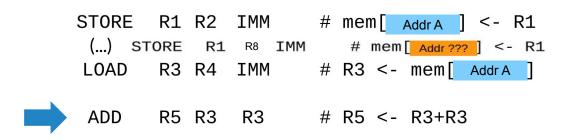


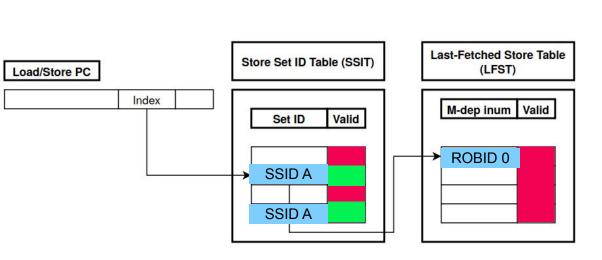


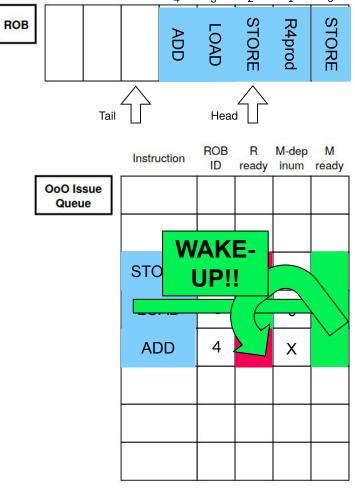


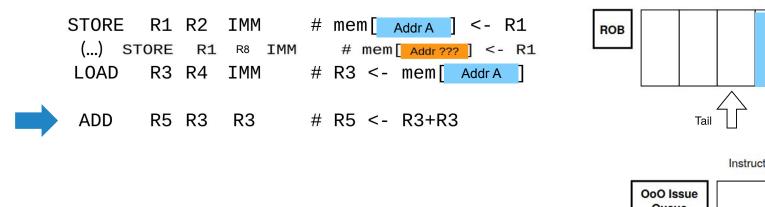


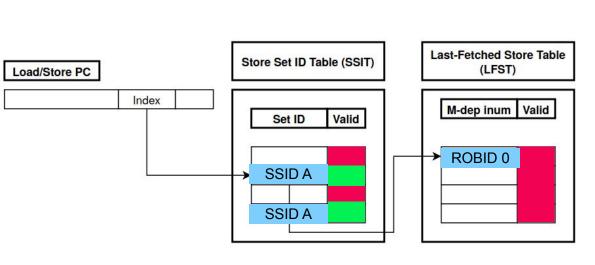


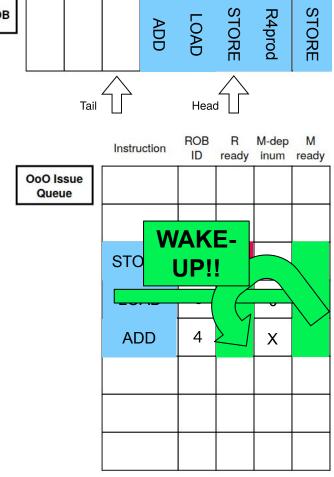


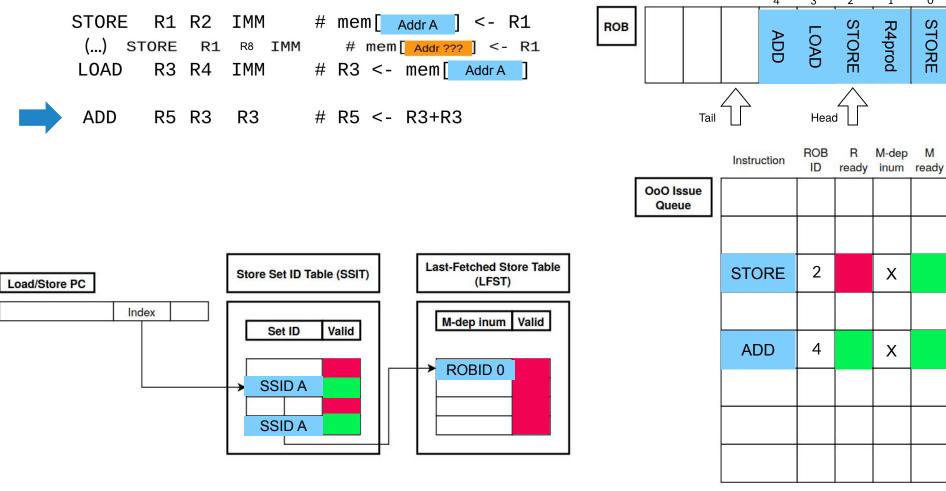


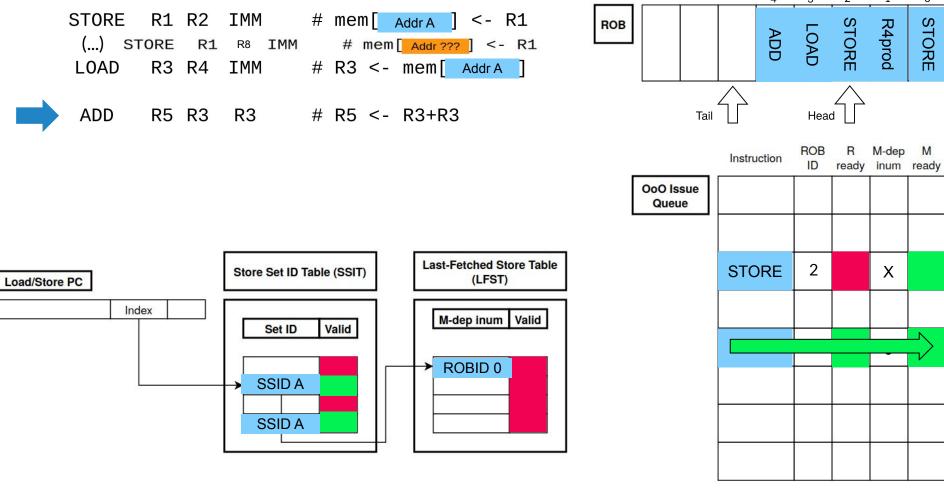


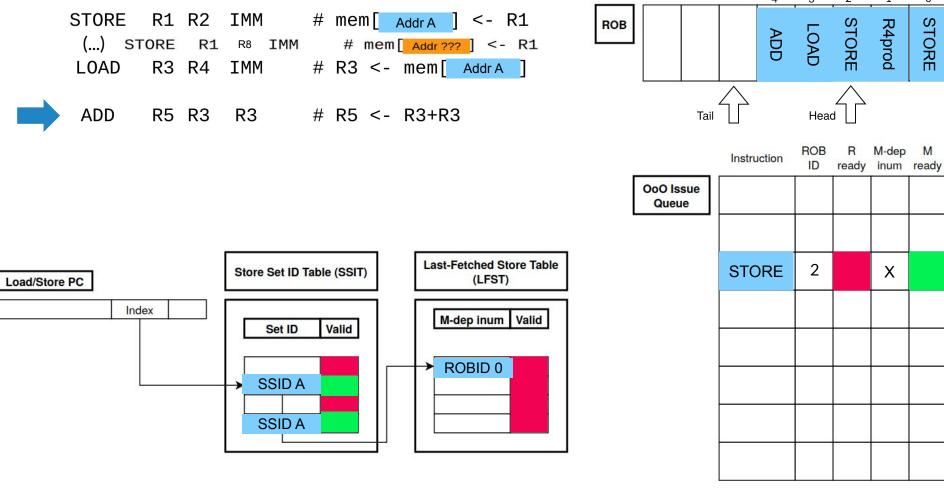


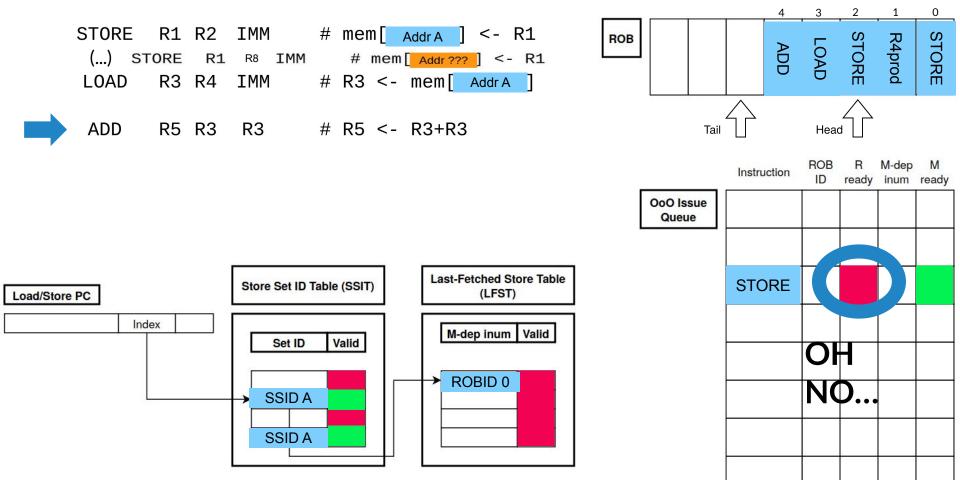


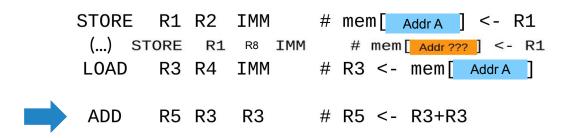


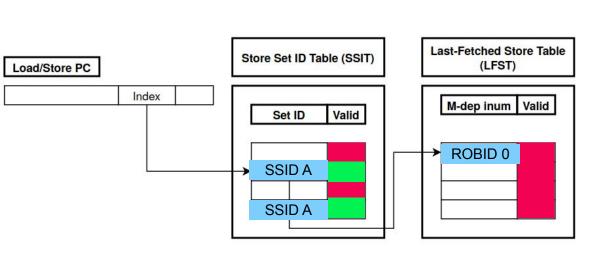


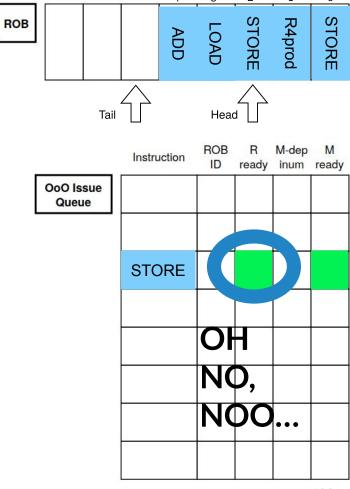


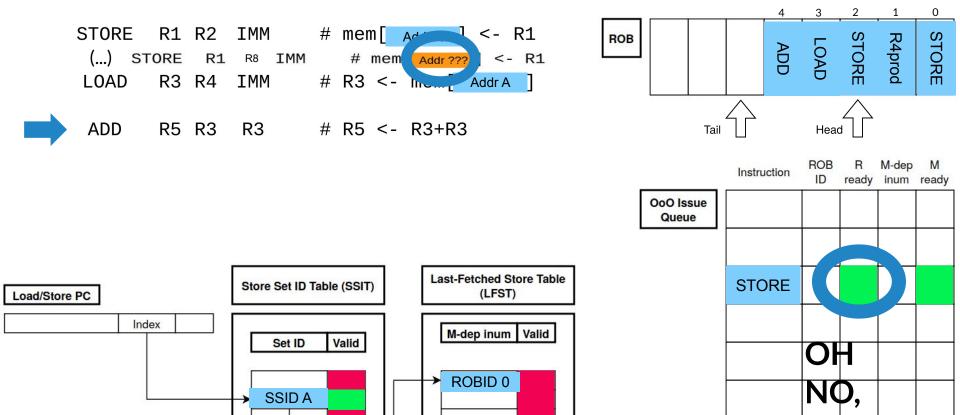




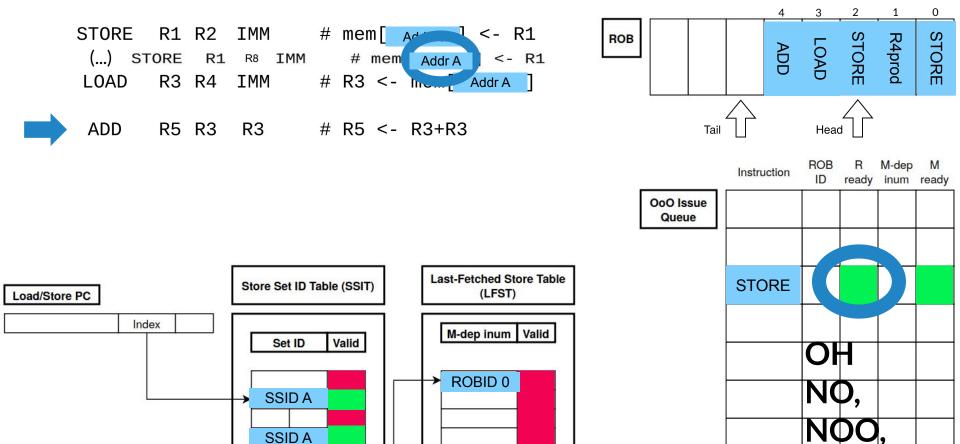








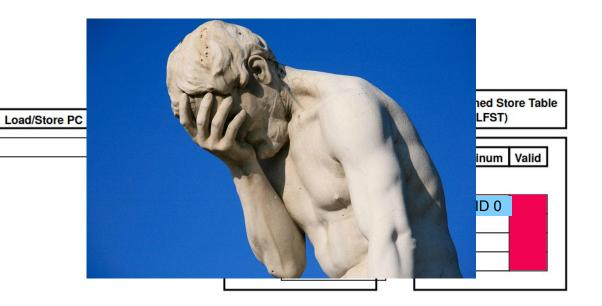
SSID A

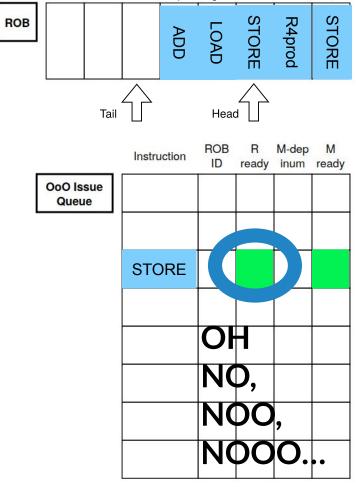


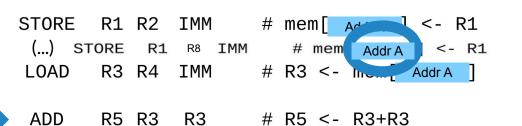




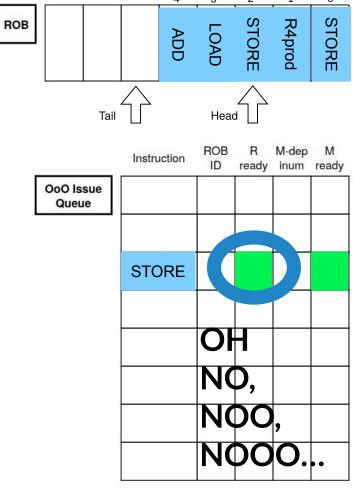
ADD R5 R3 R3 # R5 <- R3+R3

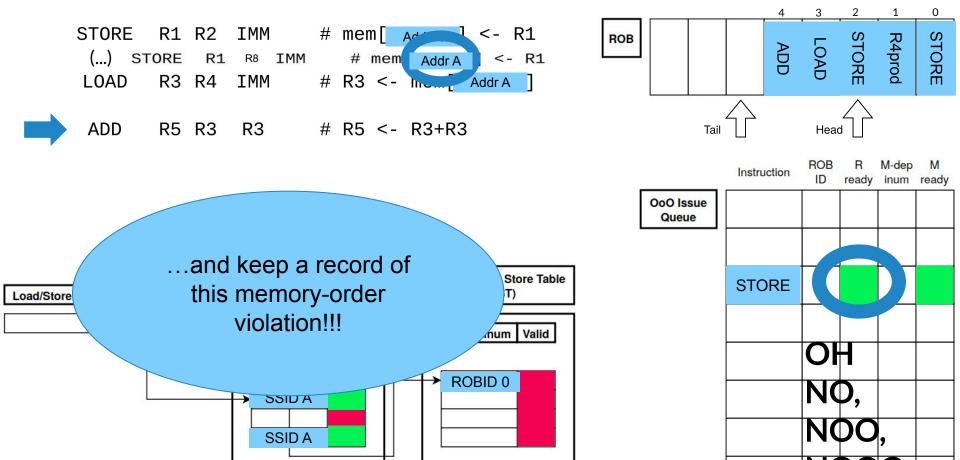


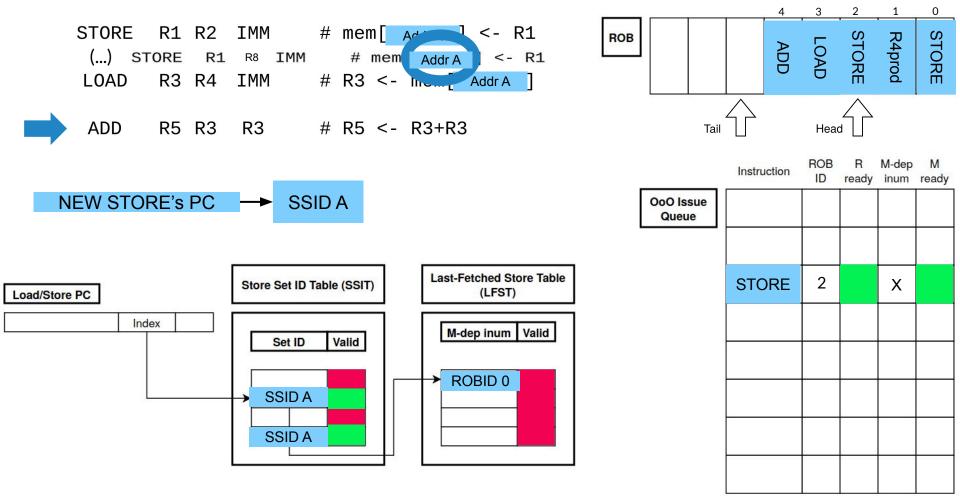


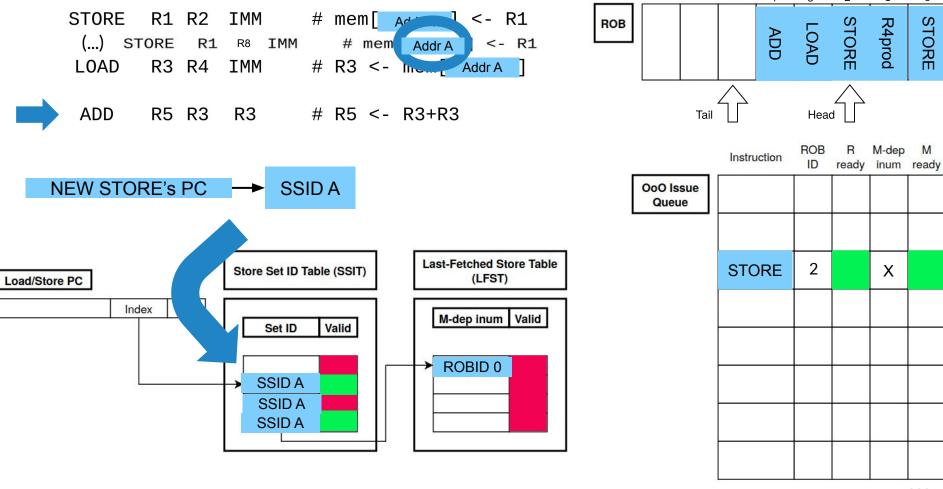


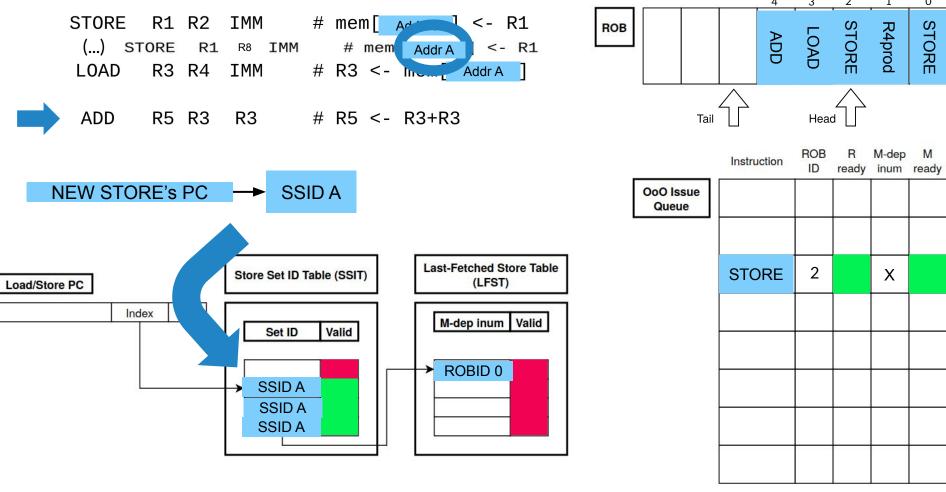


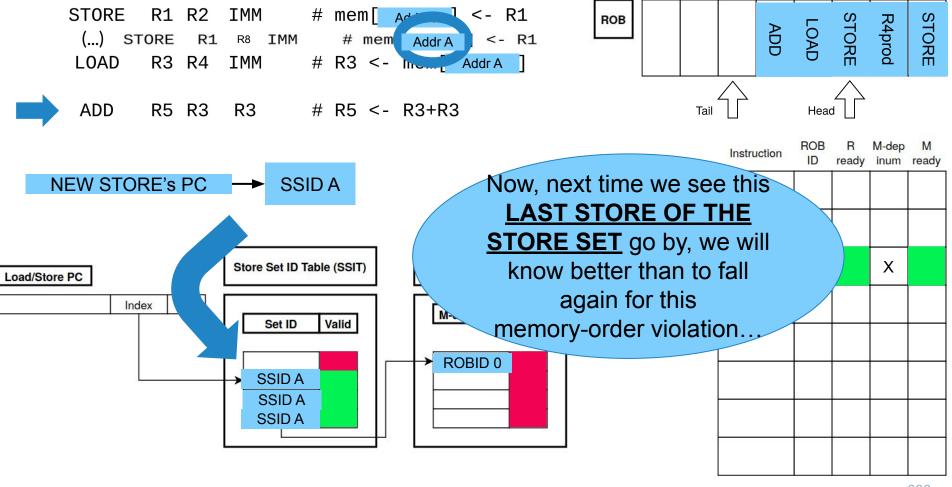


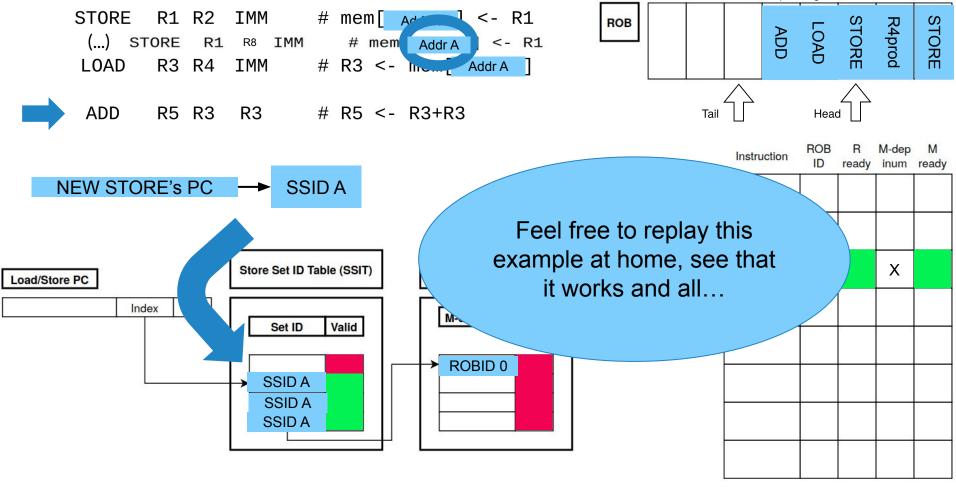










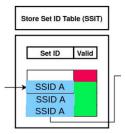


Assignment Rules



- 1. If neither the LOAD nor the STORE been assigned a store set, a SSID is generated and assigned to both instructions
- 2. If only the LOAD has been assigned a store set, the STORE is assigned to the LOAD's store set
- 3. If only the STORE has been assigned a store set, the LOAD is assigned to the STORE store set
- 4. If both the LOAD and the STORE have already been assigned to store sets, one of the two store sets is declared the "winner" and the other inherits the winner SSID.

Clear conditions



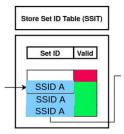


A SSIT entry is validated and an SSID is assigned to the corresponding entry when a LOAD or a STORE is involved in a memory-order violation. However, these entries in the SSIT remain valid for the rest of the program.

Unrelated LOADs or STOREs can share a SSIT entry after time, causing undesired dependences, a method of invalidating those entries is needed, authors propose two:

> ...

Clear conditions





Unrelated LOADs or STOREs can share a SSIT entry after time, causing undesired dependences, a method of invalidating those entries is needed, authors propose two:

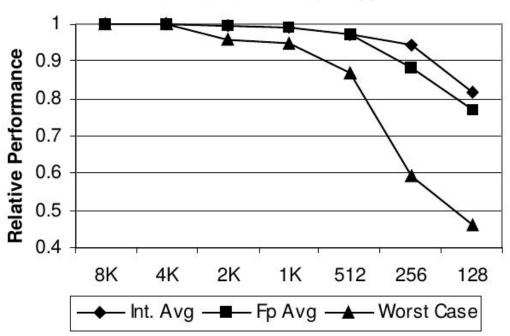
- Clear SSIT after an arbitrary amount of cycles, i.e. every million
- 2-bit counter per entry in a two-state branch-prediction fashion, where the MSB indicates if the entry is valid.

Every time a LOAD-STORE dependence is enforced, it is checked if it generates a false dependency, then, the counter of the STORE is updated

Table sizes



Figure 6.4: Peformance Sensitivity to Number of Entries in SSIT



Thoughts about the paper



- The store set invalidation mechanisms seems on the simpler side, counters could interfere in some patterns.
- They mention the benefit of requiring executing STOREs in store sets in order eliminates write-after-write hazard detection mechanisms, but what happens two STOREs to the same address do not have a LOAD causing a memory-order violation??
- In the example of two STOREs followed by a LOAD to the same address, if this piece of code is inside of a loop, what limits the first STORE in a second iteration to be issued before the LOAD of the first iteration (RAW memory hazard)?

Eskerrik asko!