A Case for Unlimited Watchpoints

Joseph L. Greathouse[†], Hongyi Xin*, Yixin Luo [†‡], Todd Austin[†]

[†]University of Michigan

*Carnegie Mellon University

[‡]Shanghai Jiao Tong University

UNIVERSITY OF MICHIGAN

ASPLOS, London, UK
March 5, 2012

Goal of This Work

MAKE

SOFTWARE

FAST

Goal of This Work

MAKE

dynamic

SOFTWARE

analysis

FAST

Goal of This Work

MAKE

dynamic

SOFTWARE

analysis

FASTer

Dynamic Software Analysis

Bounds Checking

Data Race Detection

Taint Analysis

Deterministic Execution

Transactional Memory

Speculative Parallelization

Dynamic Software Analysis

Bounds Checking

10-80x

Data Race Detection

2-300x

Taint Analysis

2-30x

Deterministic Execution

2-10x

Transactional Memory

2-50x

Speculative Parallelization

2-4x

Real Goal of This Work

Generic Hardware to Accelerate Many Dynamic Software Analyses

Real Goal of This Work

Generic Hardware to Accelerate Many Dynamic Software Analyses

WATCHPOINTS

Hardware-Assisted Watchpoints

- HW Interrupt when touching watched data

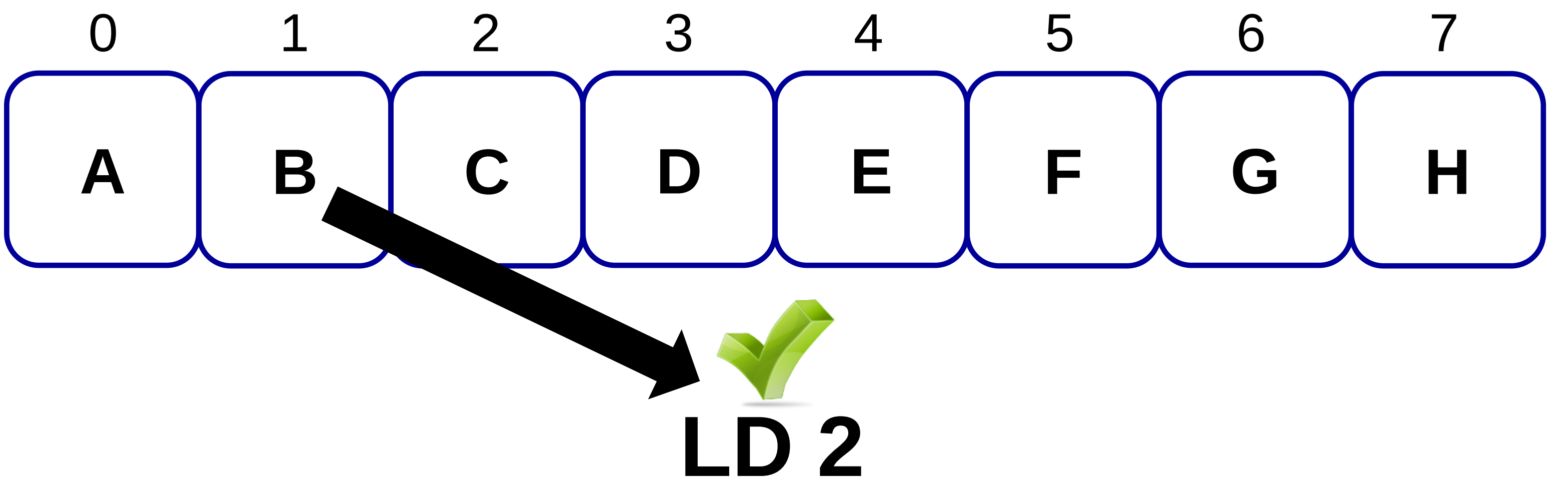
Hardware-Assisted Watchpoints

- HW Interrupt when touching watched data

0	1	2	3	4	5	6	7
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**

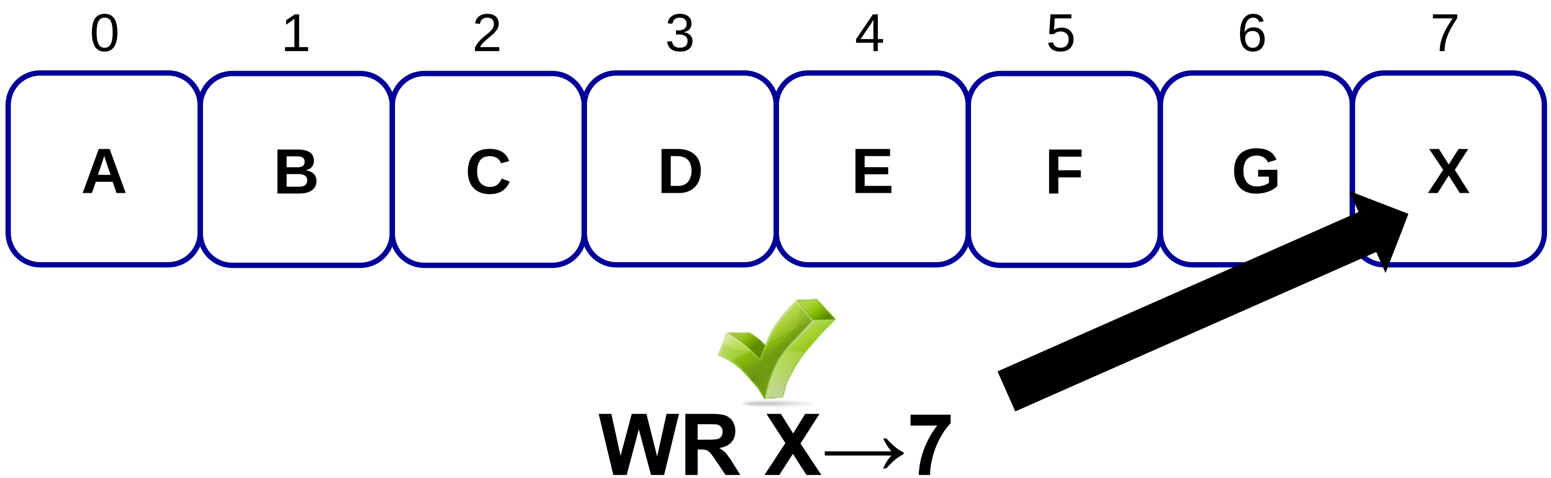
Hardware-Assisted Watchpoints

- HW Interrupt when touching watched data



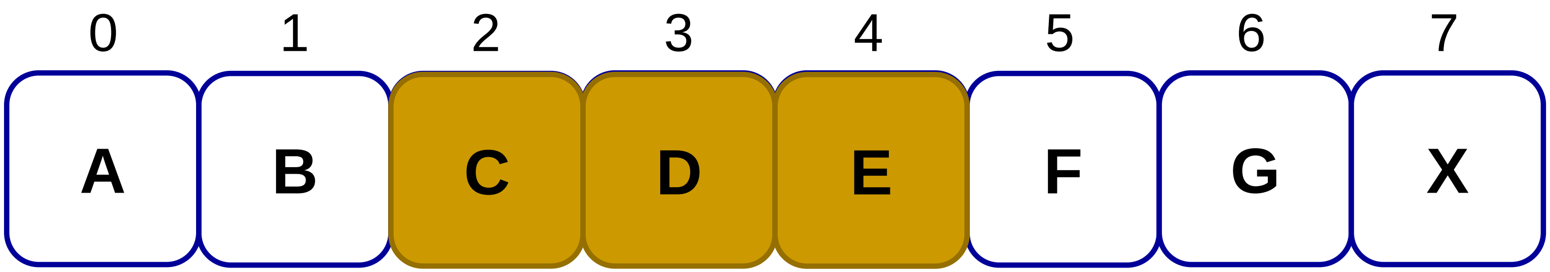
Hardware-Assisted Watchpoints

- HW Interrupt when touching watched data



Hardware-Assisted Watchpoints

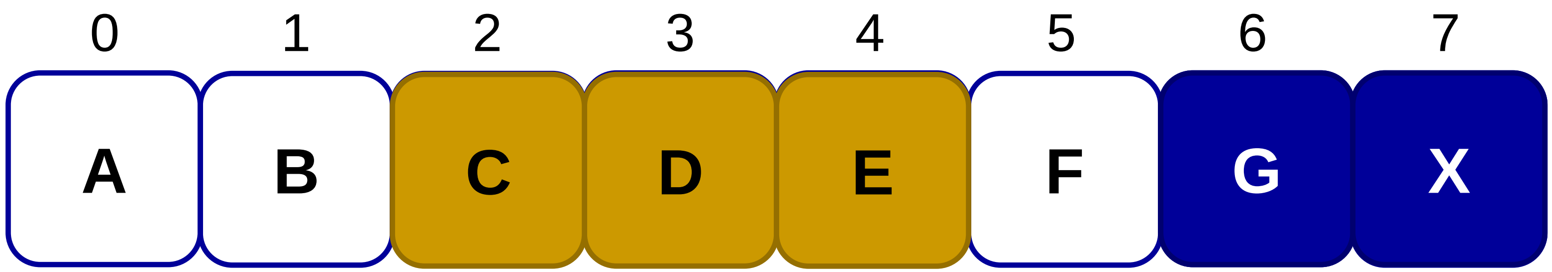
- HW Interrupt when touching watched data



R-Watch 2-4

Hardware-Assisted Watchpoints

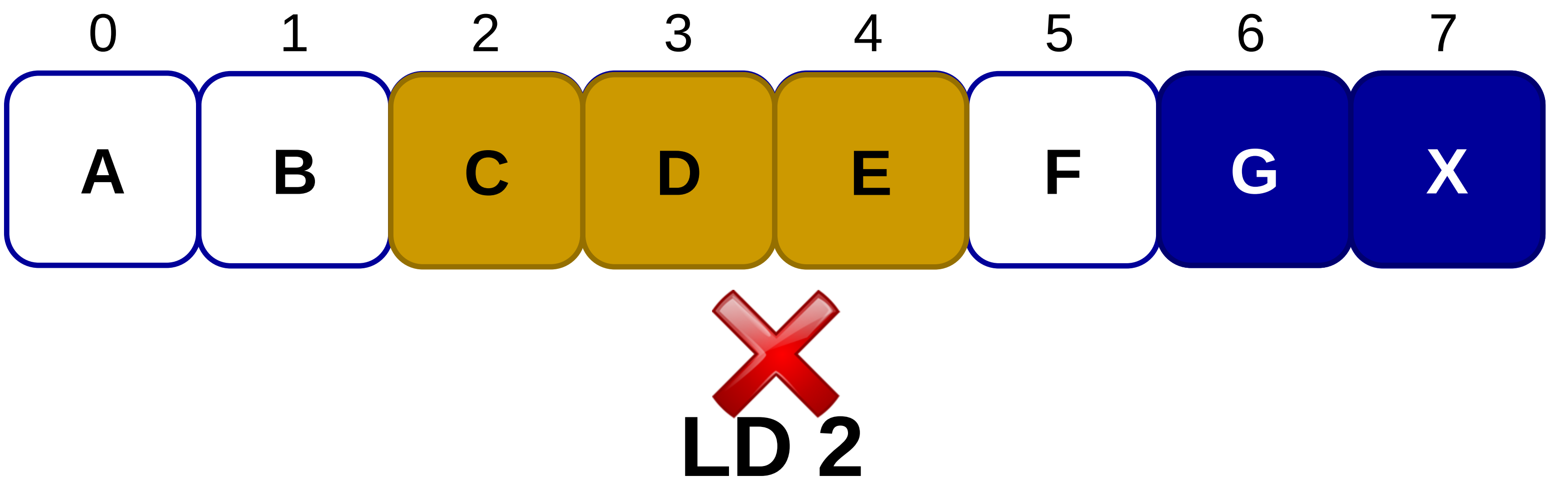
- HW Interrupt when touching watched data



W-Watch 6-7

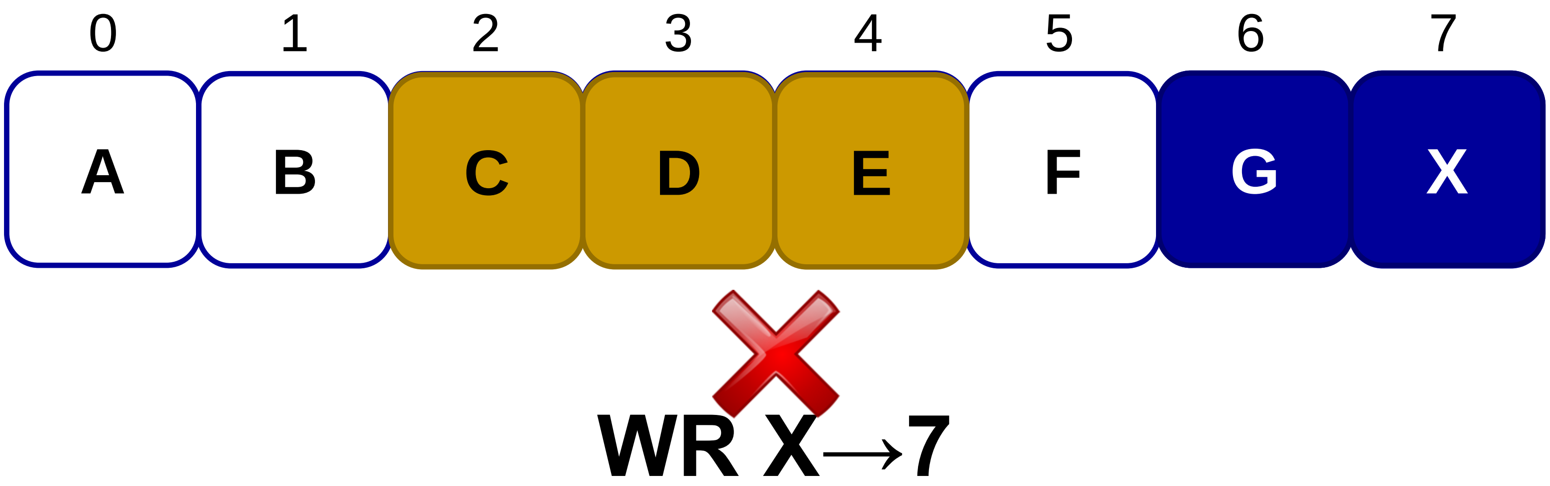
Hardware-Assisted Watchpoints

- HW Interrupt when touching watched data



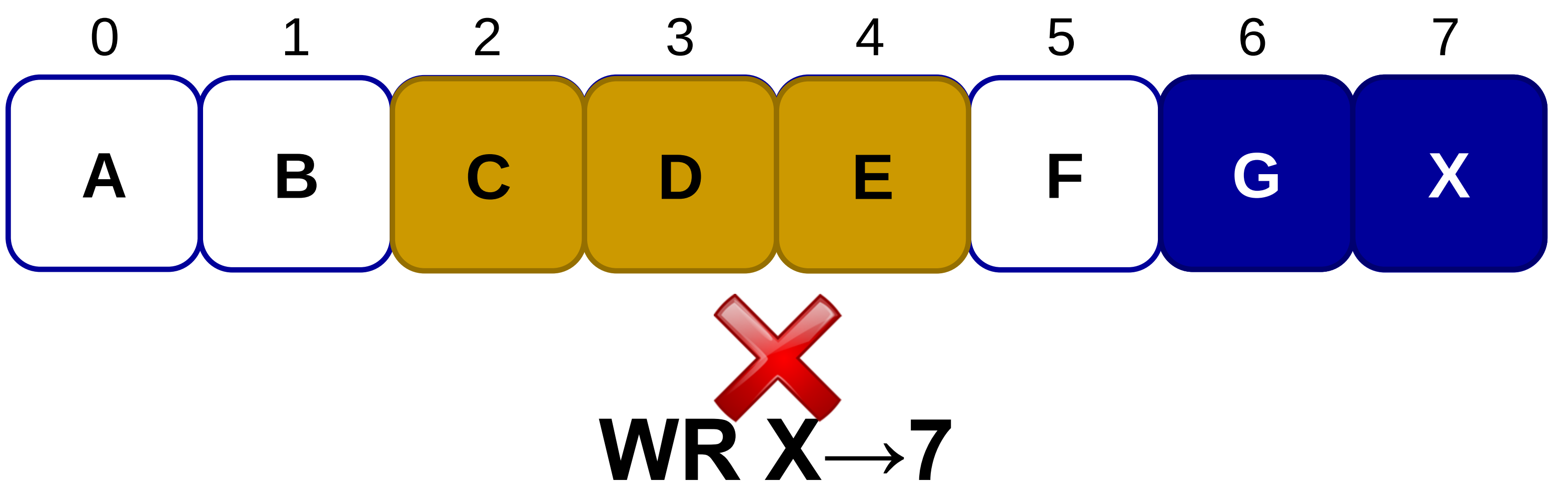
Hardware-Assisted Watchpoints

- HW Interrupt when touching watched data



Hardware-Assisted Watchpoints

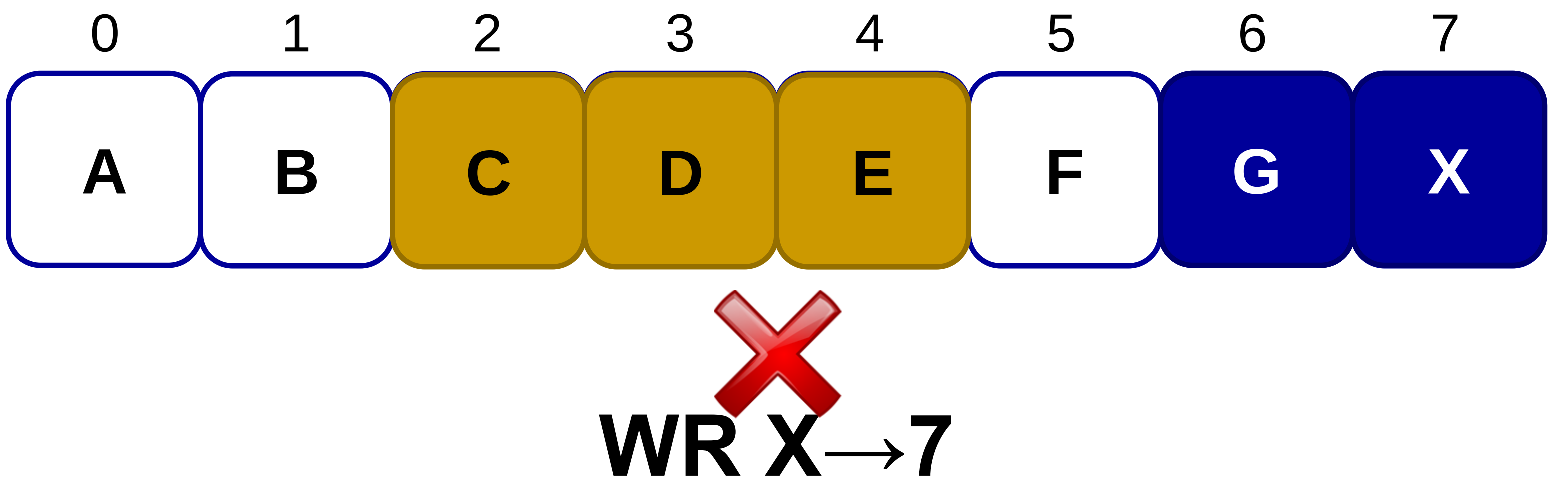
- HW Interrupt when touching watched data



- SW knows it's touching important data

Hardware-Assisted Watchpoints

- HW Interrupt when touching watched data



- SW knows it's touching important data
  - AT NO OVERHEAD

Dynamic Software Analysis

Bounds Checking

Data Race Detection

Taint Analysis

Deterministic Execution

Transactional Memory

Speculative Parallelization

Dynamic Software Analysis

Bounds Checking

Data Race Detection

Taint Analysis

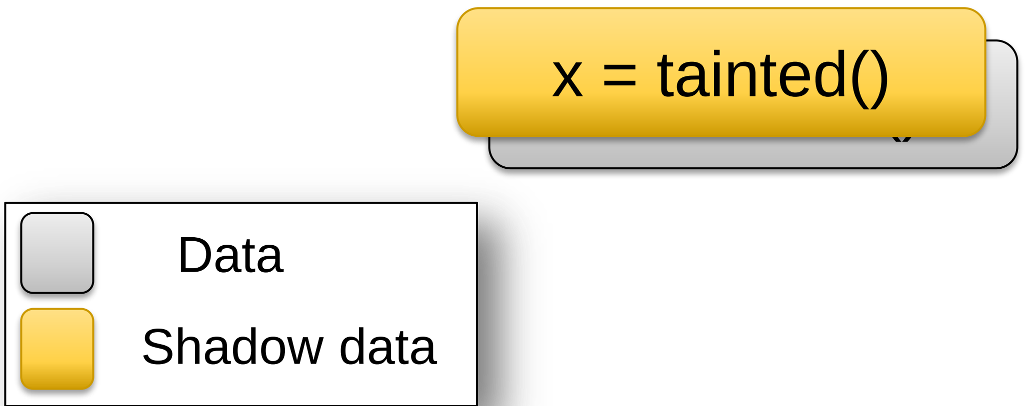
Deterministic Execution

Transactional Memory

Speculative Parallelization

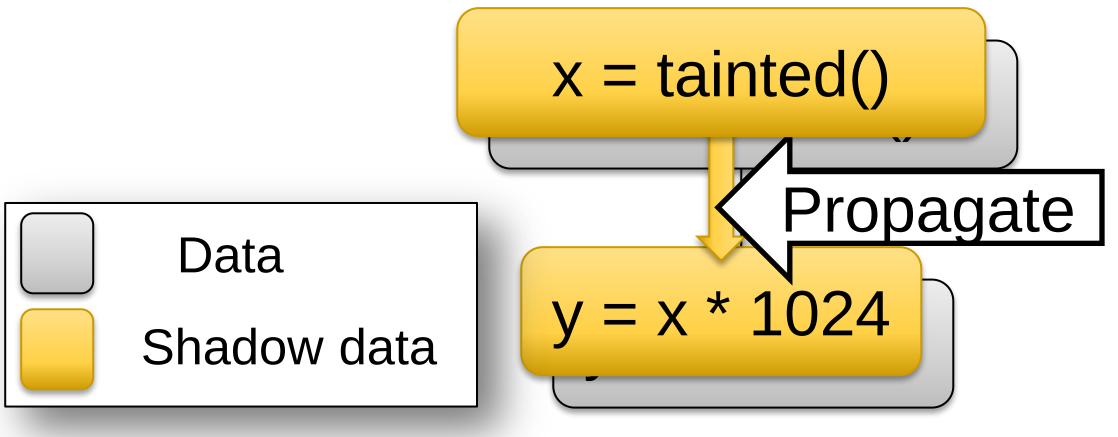
Watchpoint-Based Taint Analysis

- Taint analysis works on shadow values



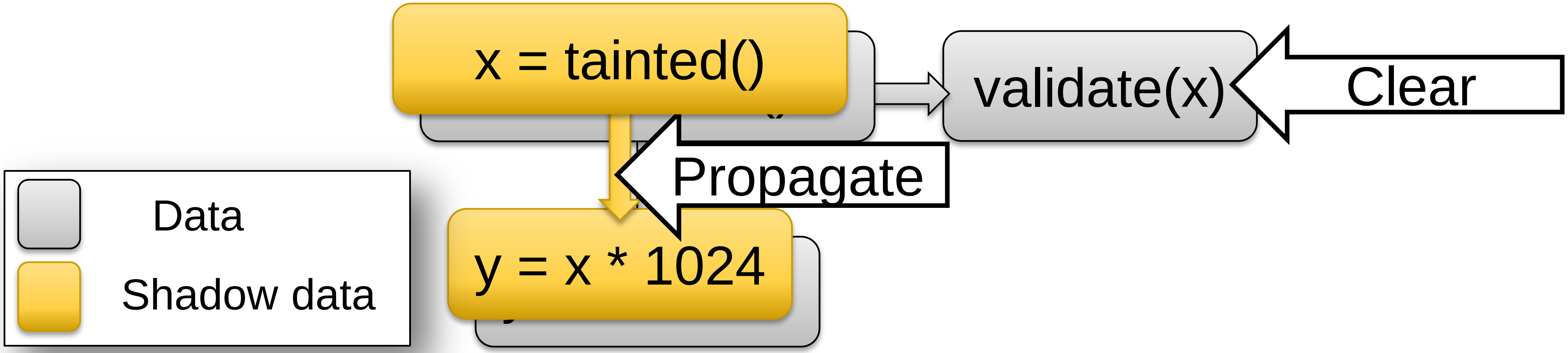
Watchpoint-Based Taint Analysis

- Taint analysis works on shadow values



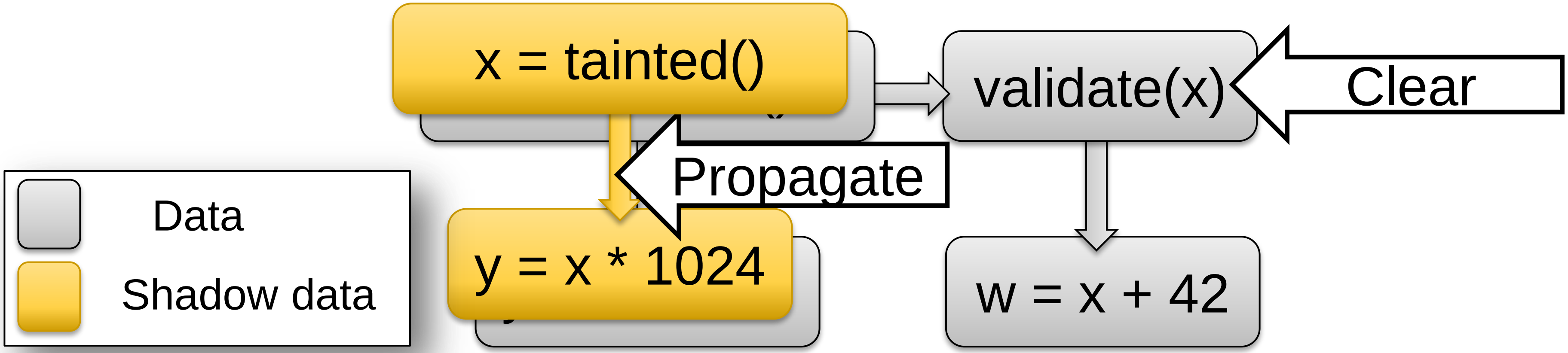
Watchpoint-Based Taint Analysis

- Taint analysis works on shadow values



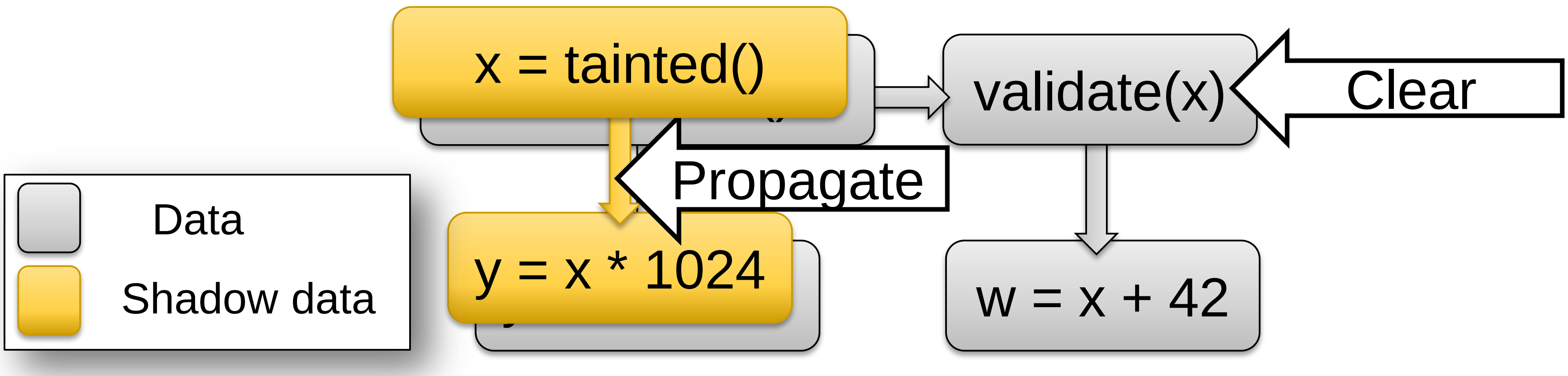
Watchpoint-Based Taint Analysis

- Taint analysis works on shadow values



Watchpoint-Based Taint Analysis

- Taint analysis works on shadow values



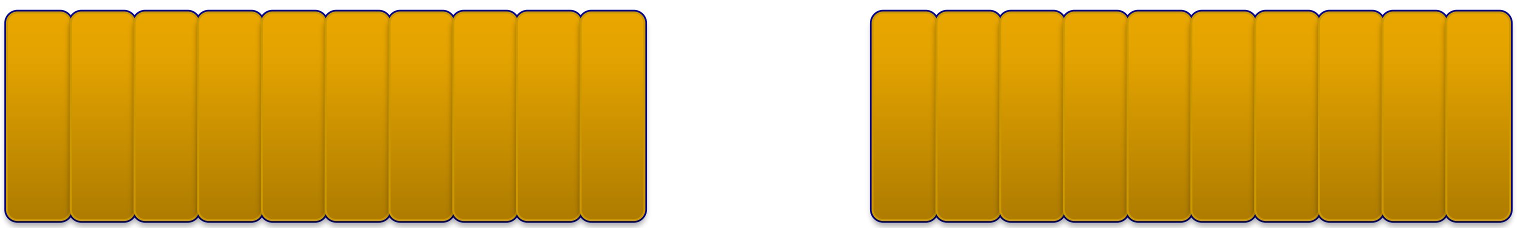
- Set R/W watchpoints on tainted values
- No tainted data? → **Run at full speed**

Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!

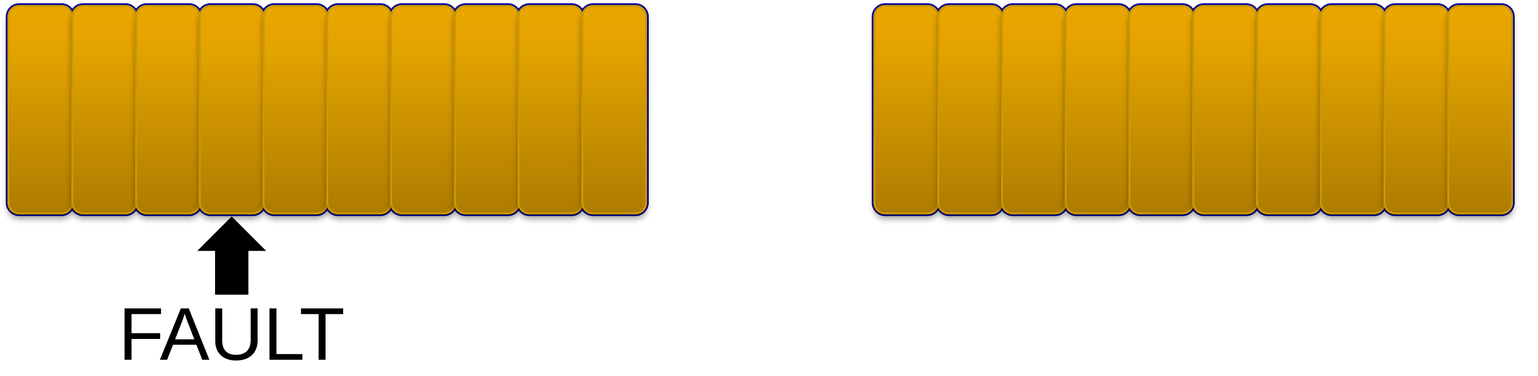
Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!



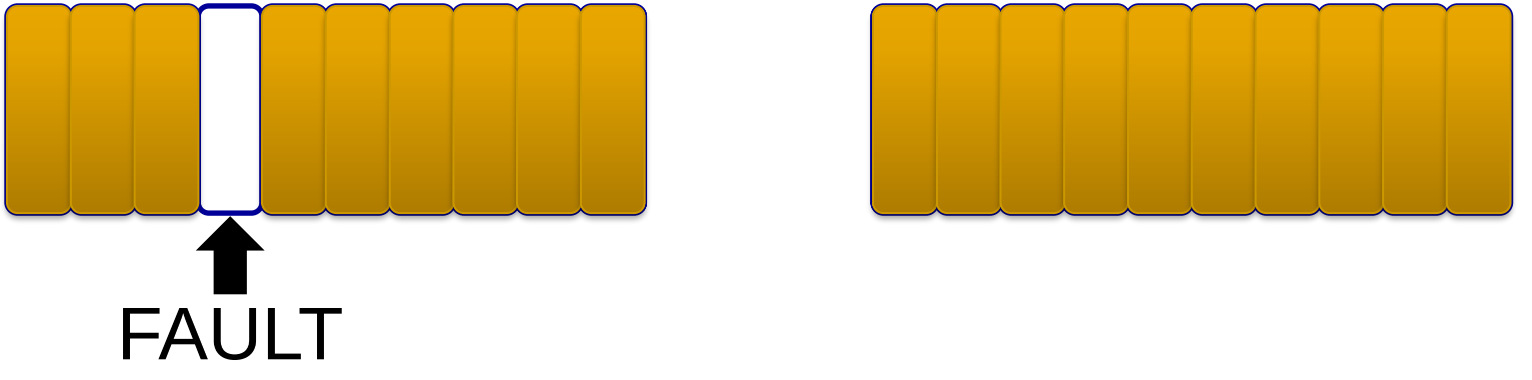
Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!



Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!

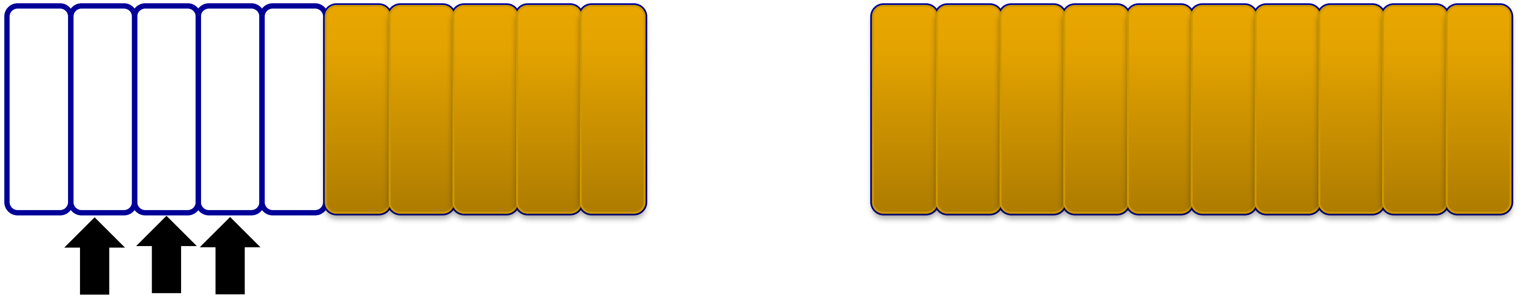


Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!

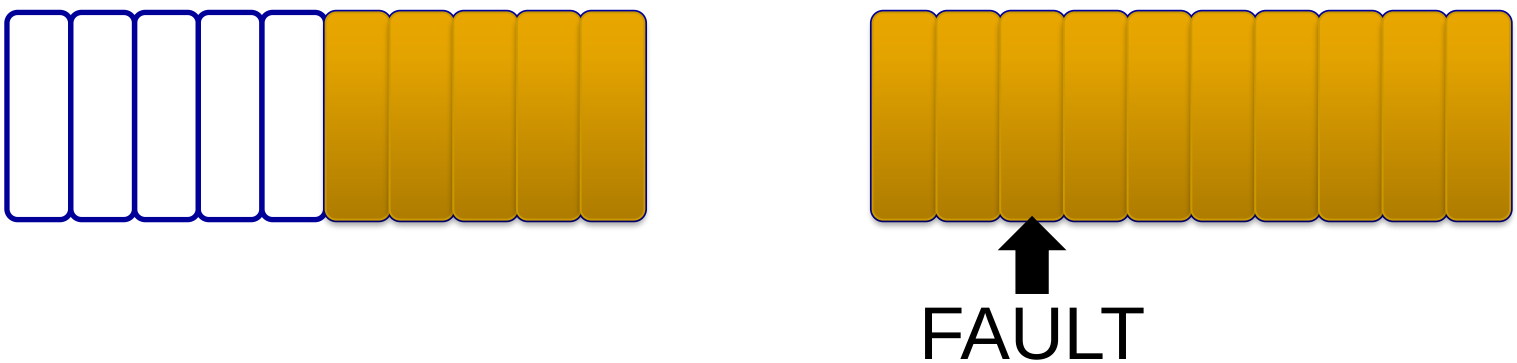
Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!



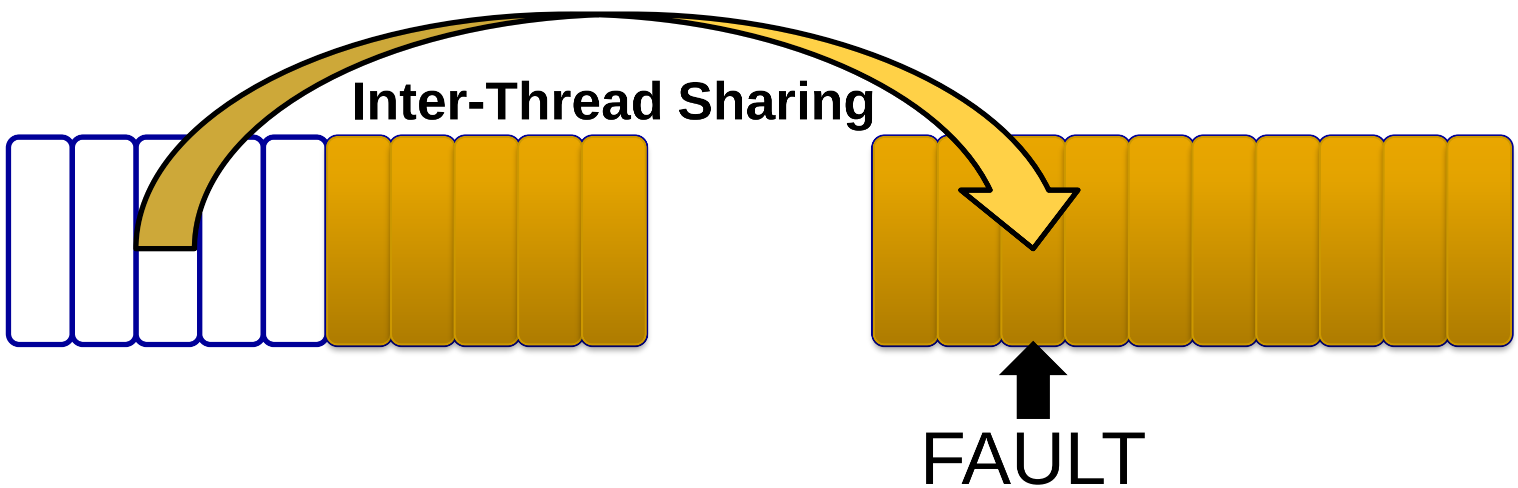
Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!



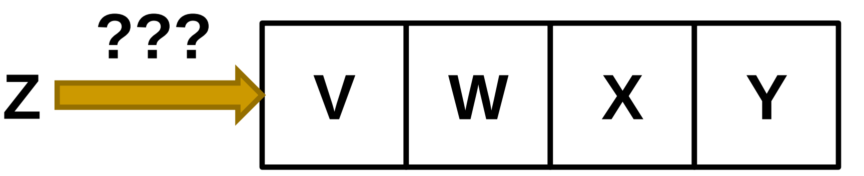
Watchpoint-Based Data Race Detection

- Find inter-thread data sharing, check locks
  - No sharing, no possible data race
  - Turn off detector until HW finds sharing!



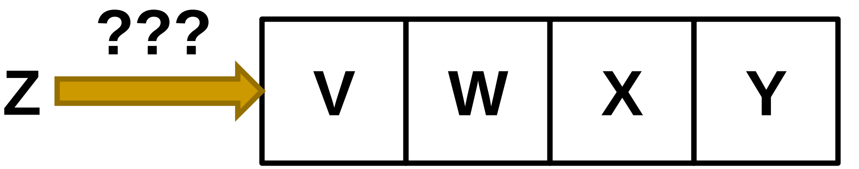
Needed Watchpoint Capabilities

- Large Number

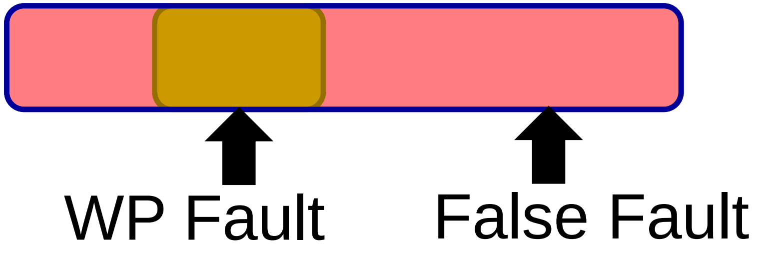


Needed Watchpoint Capabilities

- Large Number

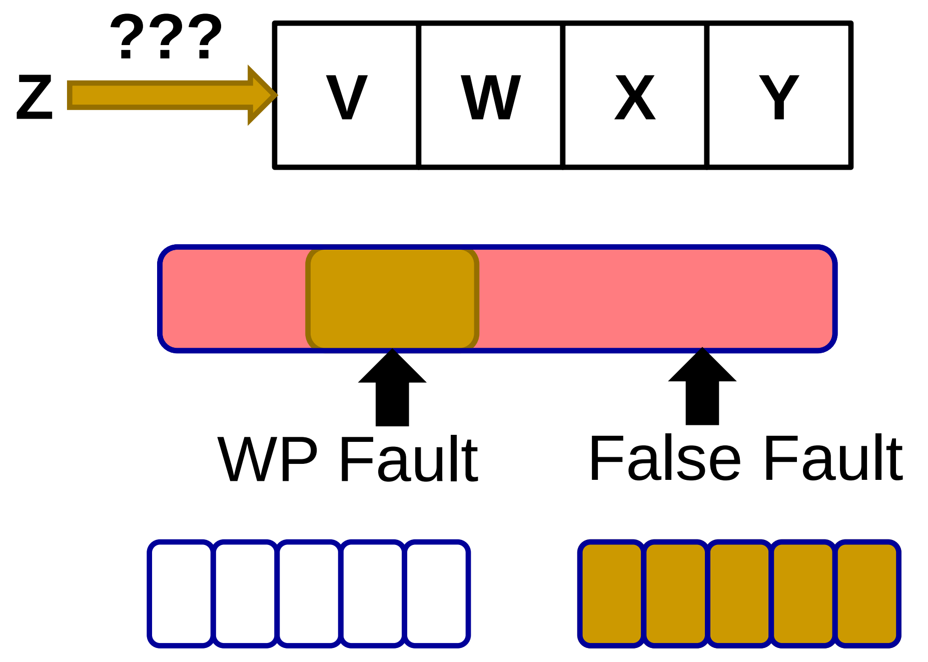


- Fine-grained



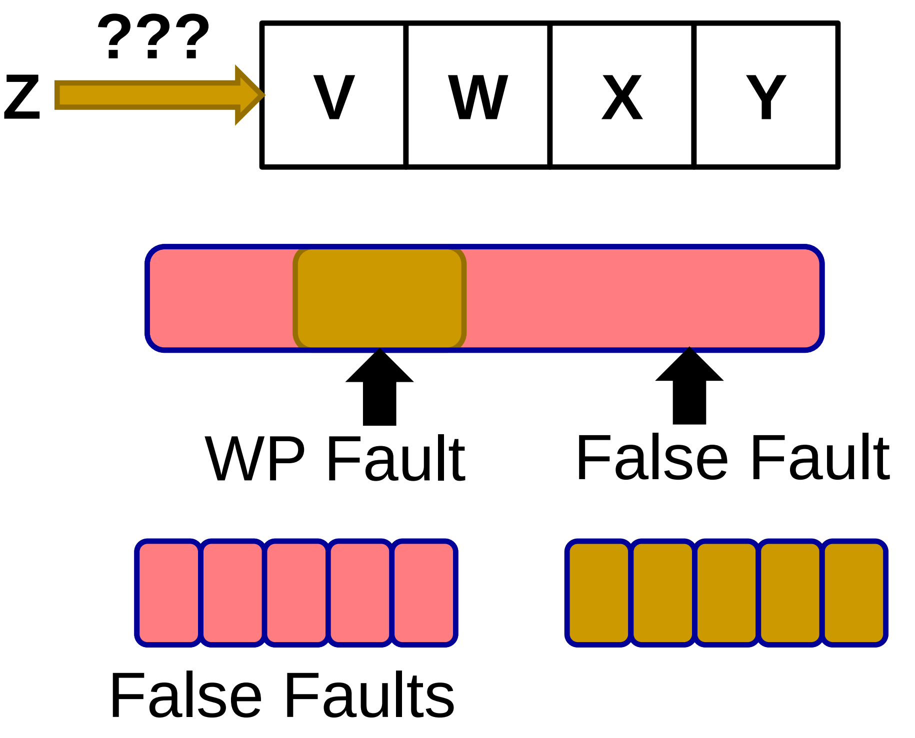
Needed Watchpoint Capabilities

- Large Number
- Fine-grained
- Per Thread



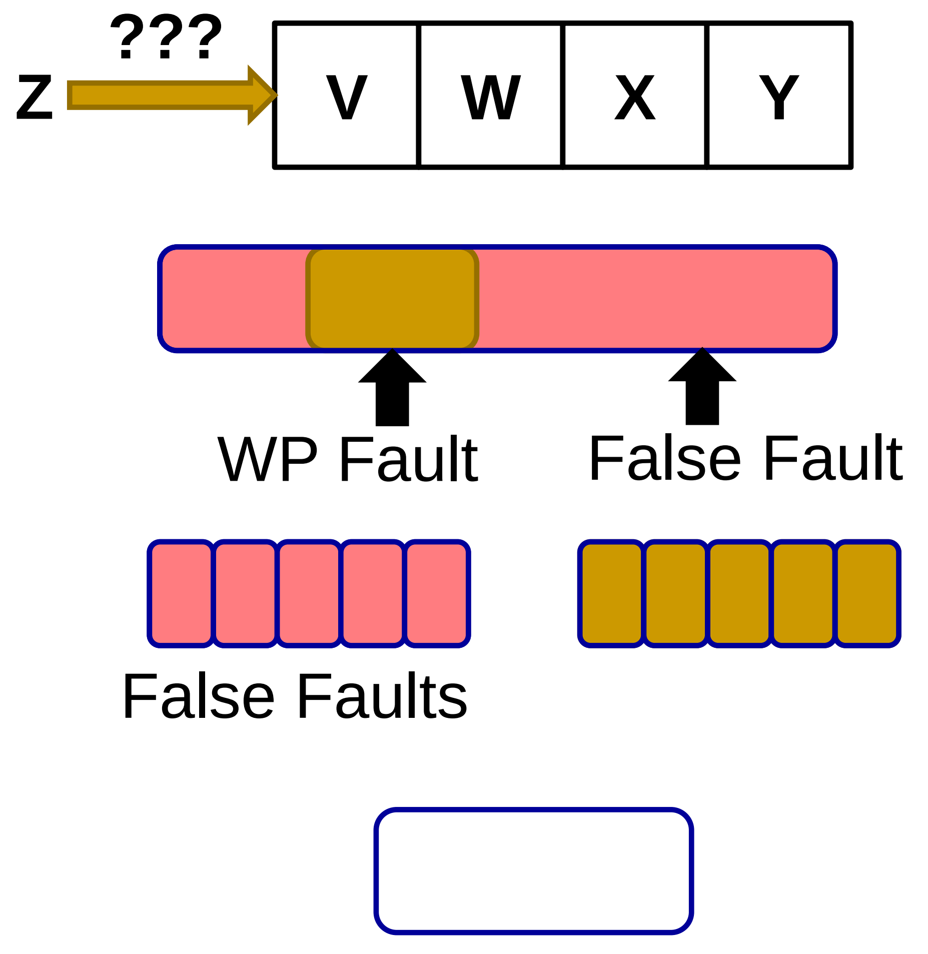
Needed Watchpoint Capabilities

- Large Number
- Fine-grained
- Per Thread



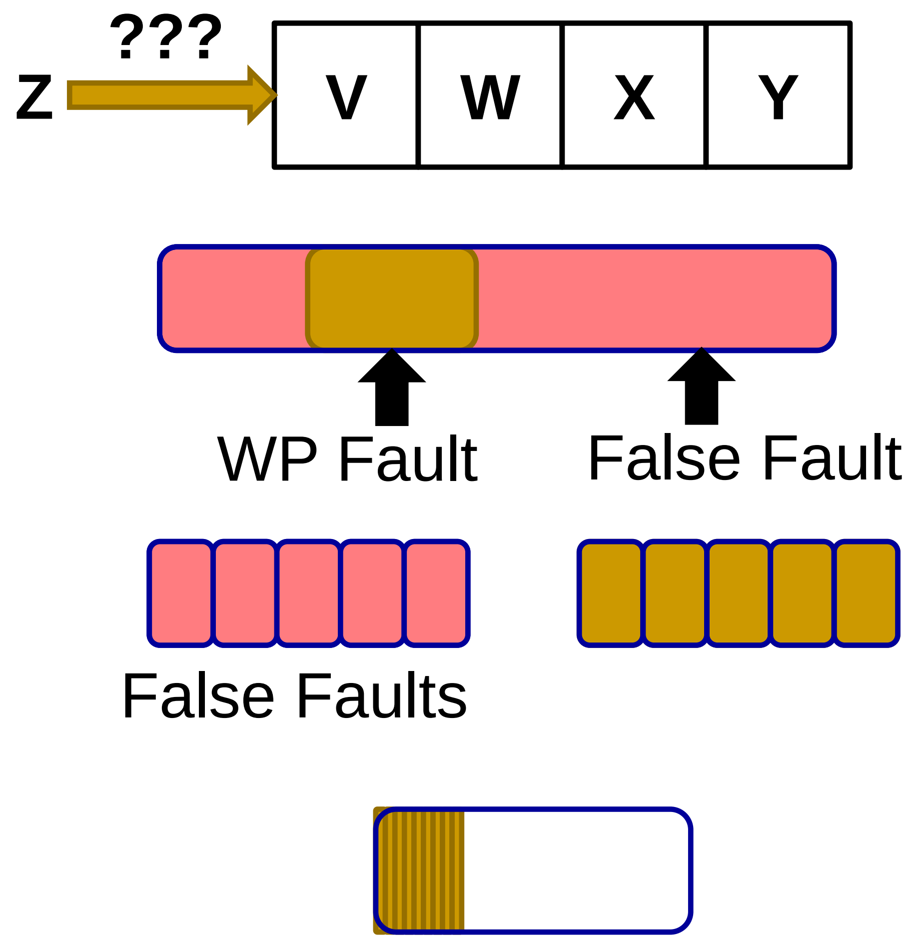
Needed Watchpoint Capabilities

- Large Number
- Fine-grained
- Per Thread
- Ranges



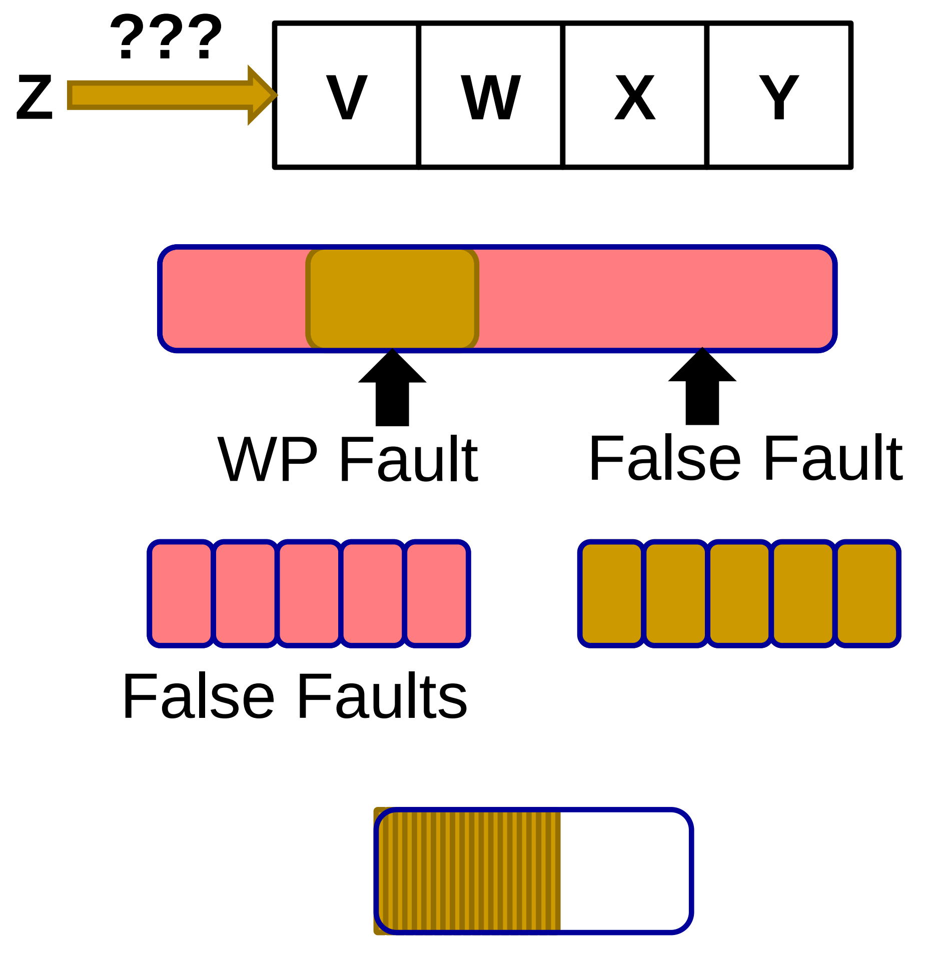
Needed Watchpoint Capabilities

- Large Number
- Fine-grained
- Per Thread
- Ranges



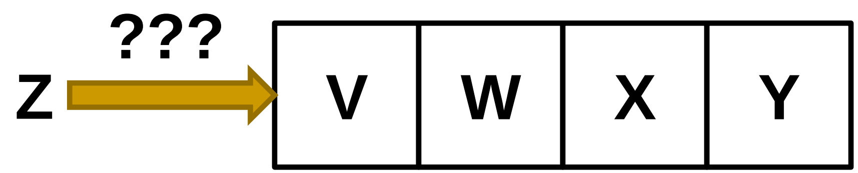
Needed Watchpoint Capabilities

- Large Number
- Fine-grained
- Per Thread
- Ranges

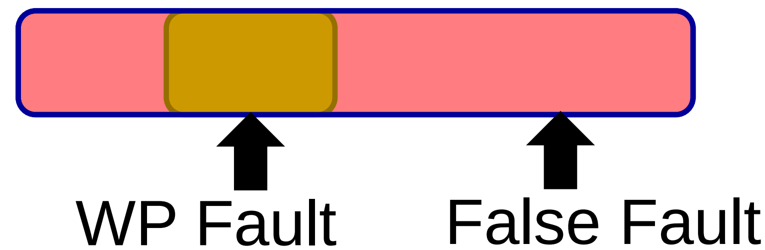


Needed Watchpoint Capabilities

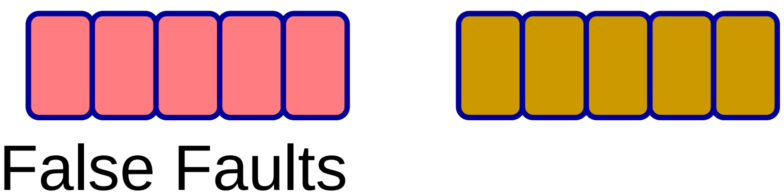
- Large Number



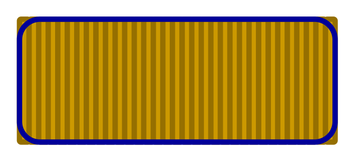
- Fine-grained



- Per Thread

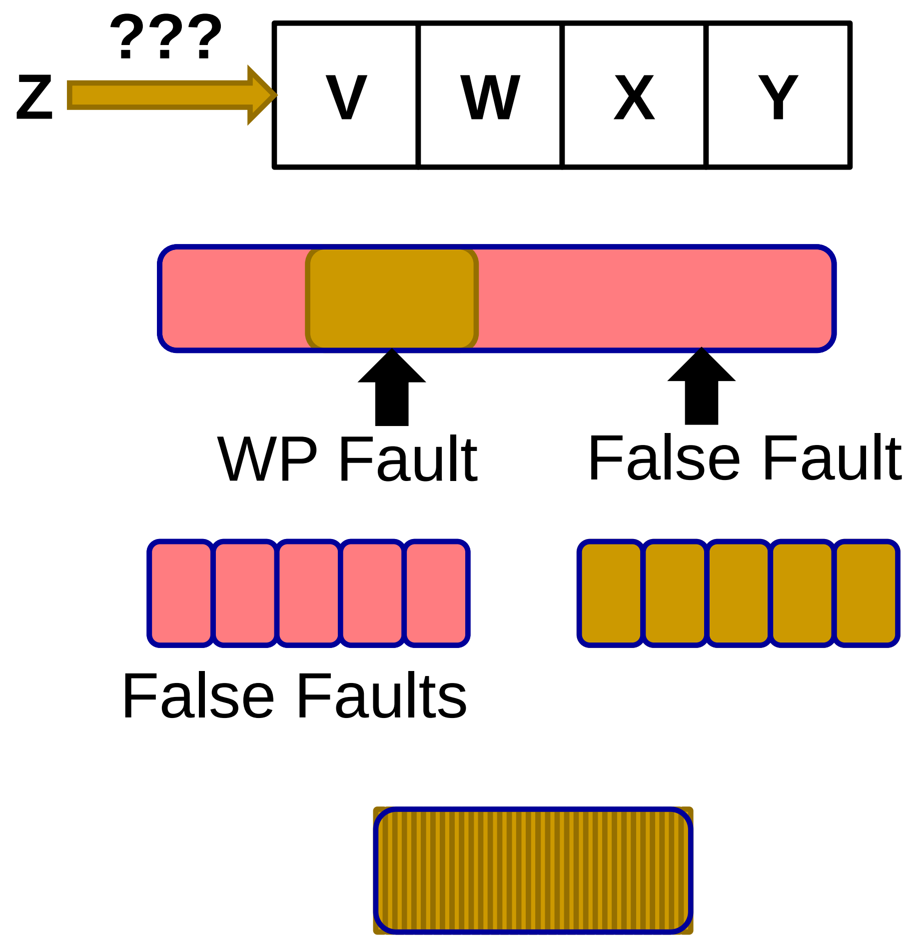


- Ranges



Needed Watchpoint Capabilities

- Large Number
- Fine-grained
- Per Thread
- Ranges
- Others in Paper



Existing Watchpoint Solutions

- Watchpoint Registers
  – Limited number (4-16), small reach (4-8 bytes)

Existing Watchpoint Solutions

- Watchpoint Registers
  - Limited number (4-16), small reach (4-8 bytes)

- Virtual Memory
  - Coarse-grained, per-process, *only* aligned ranges

Existing Watchpoint Solutions

- Watchpoint Registers
  - Limited number (4-16), small reach (4-8 bytes)
- Virtual Memory
  - Coarse-grained, per-process, *only* aligned ranges
- ECC Mangling
  - Per physical address, all cores, no ranges

Meeting These Requirements

- Unlimited Number of Watchpoints
  - Store in memory, <u>cache</u> on chip
- Fine-Grained
  - Watch full virtual addresses
- Per-Thread
  - Watchpoints cached per core/thread
  - TID Registers
- Ranges
  - **Range Cache**

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0xffff_ffff	Not Watched	1
			0
			0

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0xffff_ffff	Not Watched	1
			0
			0

Set Addresses
0x5 – 0x2000
R-Watched

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0x4	Not Watched	1
0x5	0x2000	R Watched	1
0x2001	0xffff_ffff	Not Watched	1

Set Addresses
0x5 – 0x2000
R-Watched

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0x4	Not Watched	1
0x5	0x2000	R Watched	1
0x2001	0xffff_ffff	Not Watched	1

Load Address
0x400

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0x4	Not Watched	1
0x5	0x2000	R Watched	1
0x2001	0xffff_ffff	Not Watched	1

≤ 0x400?

≥ 0x400?

Load Address
0x400

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0x4	Not Watched	1
0x5	0x2000	R Watched	1
0x2001	0xffff_ffff	Not Watched	1

≤ 0x400?

≥ 0x400?

Load Address
0x400

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0x4	Not Watched	1
0x5	0x2000	R Watched	1
0x2001	0xffff_ffff	Not Watched	1

≤ 0x400?

≥ 0x400?

Load Address
0x400

Range Cache

Start Address	End Address	Watchpoint?	Valid
0x0	0x4	Not Watched	1
0x5	0x2000	R Watched	1
0x2001	0xffff_ffff	Not Watched	1

≤ 0x400?

≥ 0x400?

WP Interrupt

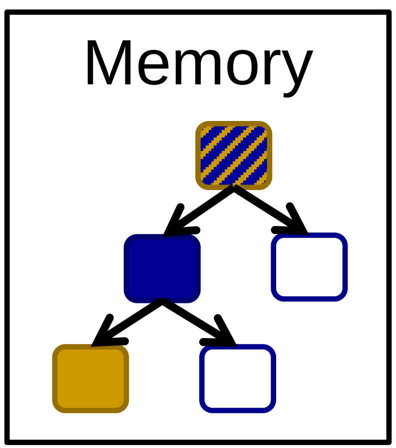
Load Address 0x400

Watchpoint System Design I

- Store Ranges in Main Memory

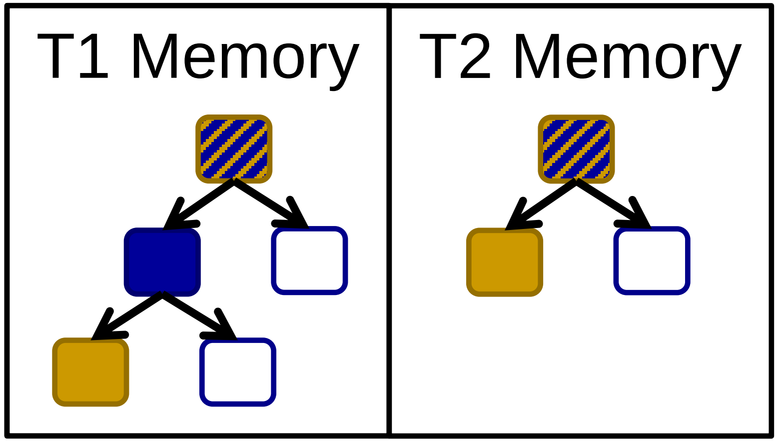
Watchpoint System Design I

- Store Ranges in Main Memory



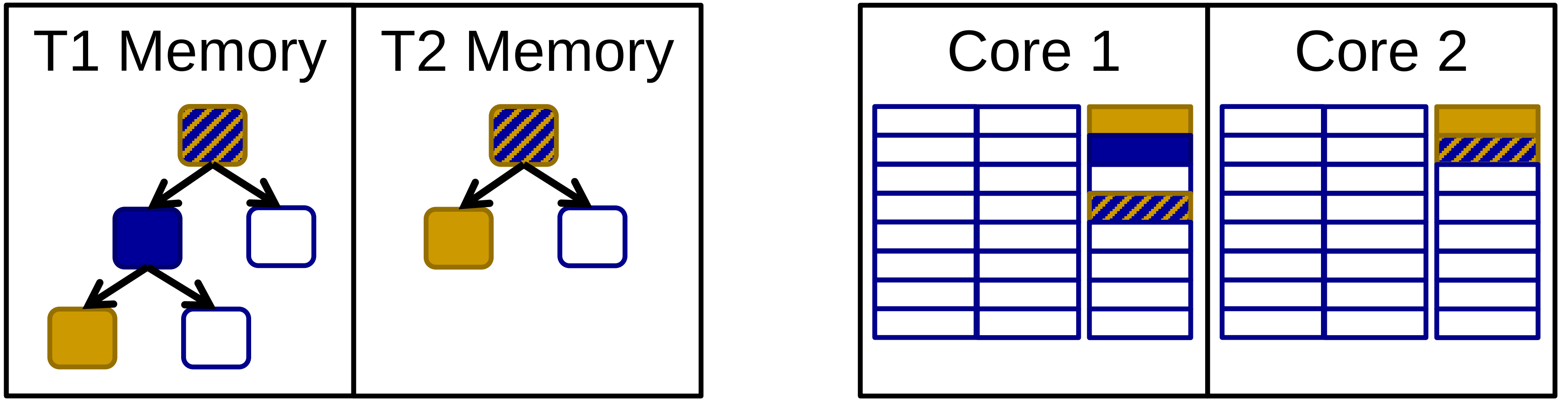
Watchpoint System Design I

- Store Ranges in Main Memory
- Per-Thread Ranges, Per-Core Range Cache



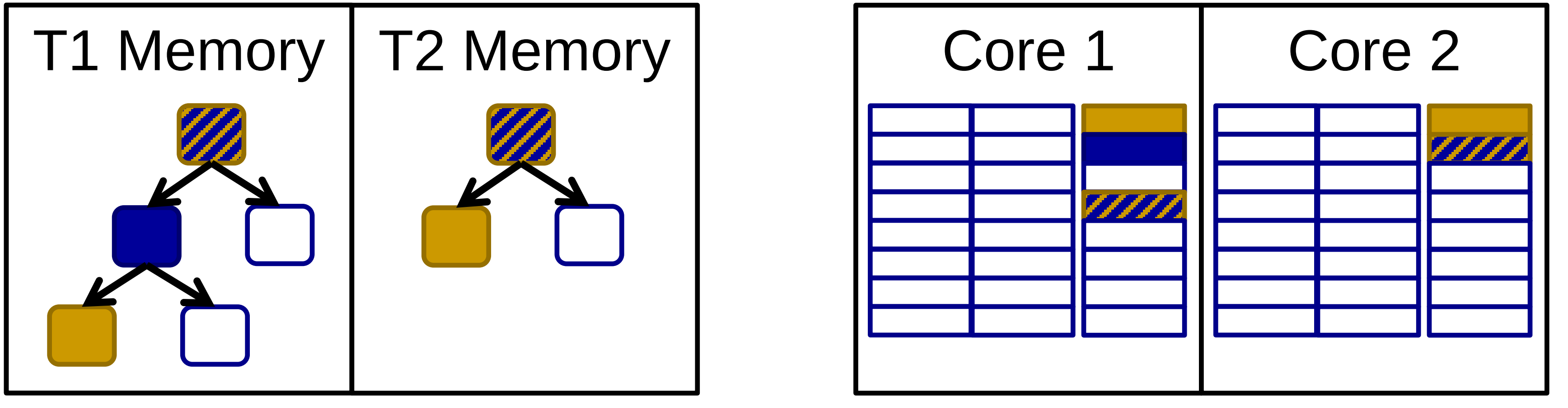
Watchpoint System Design I

- Store Ranges in Main Memory
- Per-Thread Ranges, Per-Core Range Cache



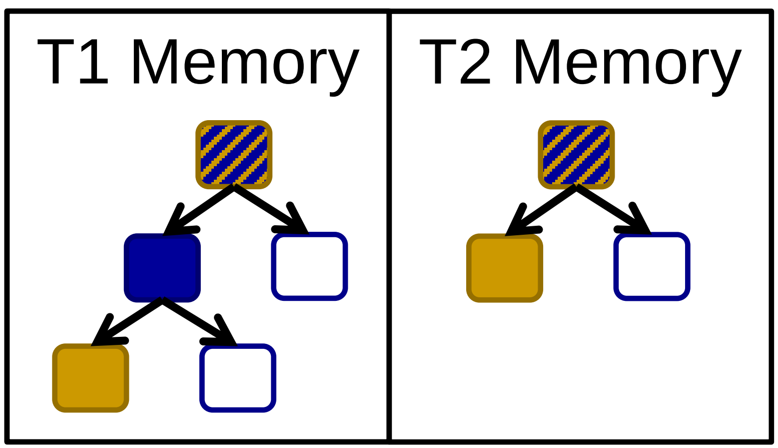
Watchpoint System Design I

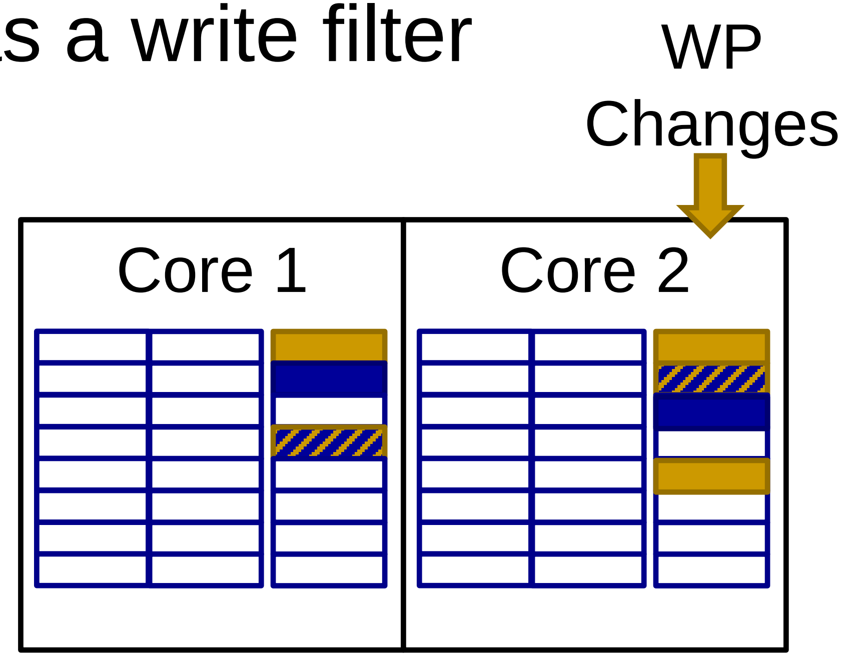
- Store Ranges in Main Memory
- Per-Thread Ranges, Per-Core Range Cache
- Software Handler on RC miss or overflow



Watchpoint System Design I

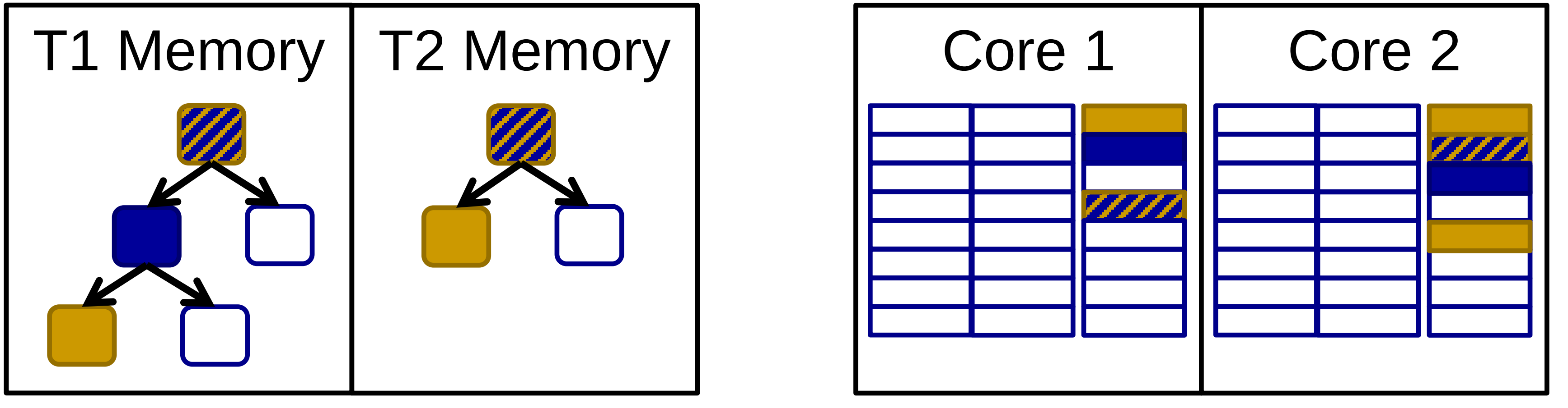
- Store Ranges in Main Memory
- Per-Thread Ranges, Per-Core Range Cache
- Software Handler on RC miss or overflow
- Write-back RC works as a write filter





Watchpoint System Design I

- Store Ranges in Main Memory
- Per-Thread Ranges, Per-Core Range Cache
- Software Handler on RC miss or overflow
- Write-back RC works as a write filter
- Precise, user-level watchpoint faults



Experimental Evaluation Setup

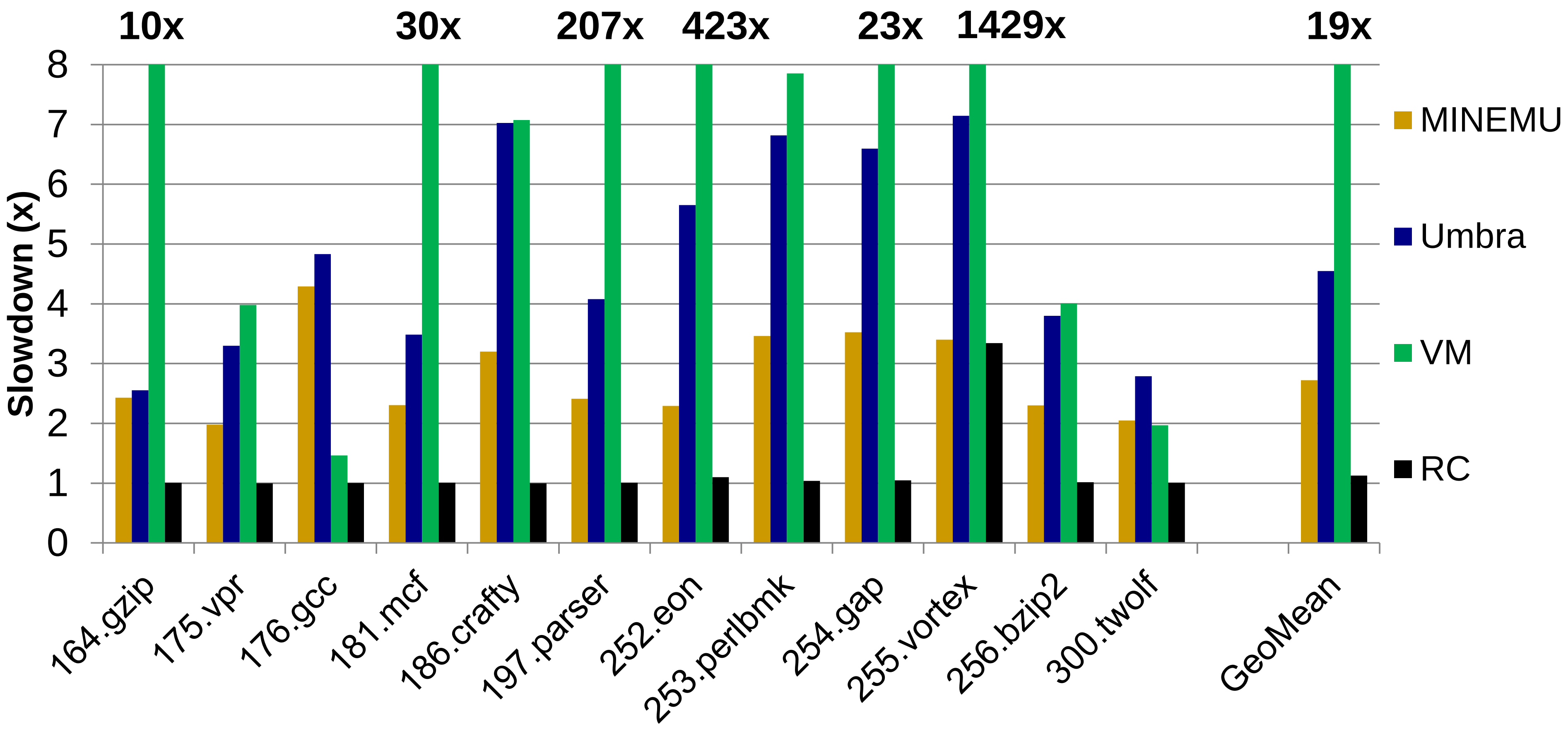
- Pin-based Simulation
  - Every memory access through HW simulator
  - Count pipeline-exposed events
  - Record all other events
- Trace-based timing simulator

- Taint analysis on SPEC INT2000
- Race Detection on Phoenix and PARSEC

- <u>Comparing only shadow value checks</u>

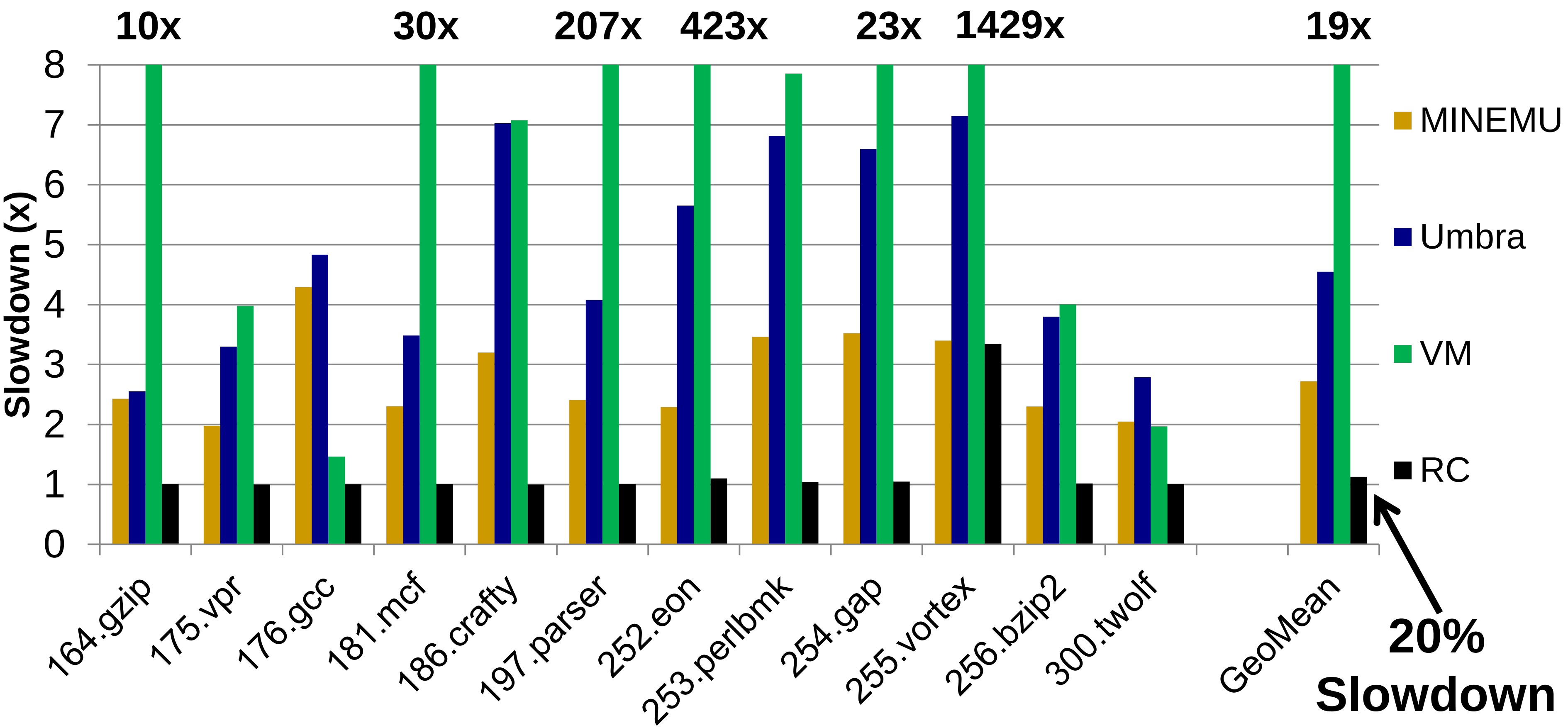
Watchpoint-Based Taint Analysis

- 128 entry Range Cache



Watchpoint-Based Taint Analysis

- 128 entry Range Cache



The Need for Many Small Ranges

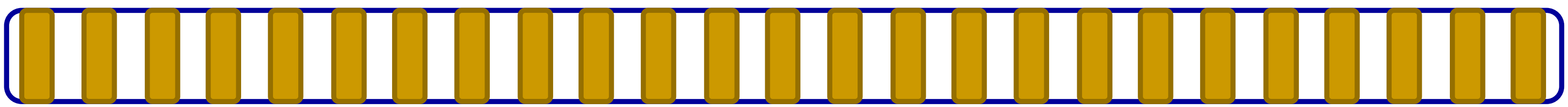
- Some watchpoints better suited for ranges

  - 32b Addresses: 2 ranges x 64b each = **16B**

The Need for Many Small Ranges

- Some watchpoints better suited for ranges

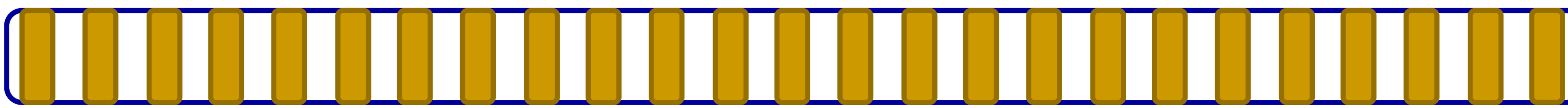
  - 32b Addresses: 2 ranges x 64b each = **16B**
- Some need large # of small watchpoints



The Need for Many Small Ranges

- Some watchpoints better suited for ranges

  - 32b Addresses: 2 ranges x 64b each = **16B**
- Some need large # of small watchpoints

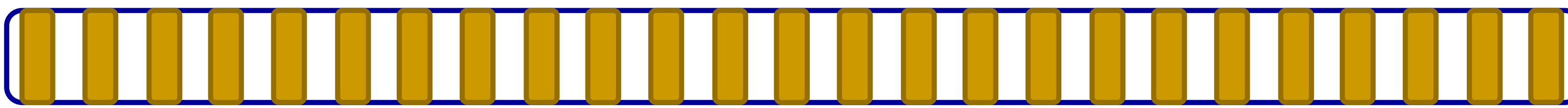


  - 51 ranges x 64b each = **408B**
  - Better stored as bitmap? 51 bits!

The Need for Many Small Ranges

- Some watchpoints better suited for ranges

  - 32b Addresses: 2 ranges x 64b each = **16B**
- Some need large # of small watchpoints

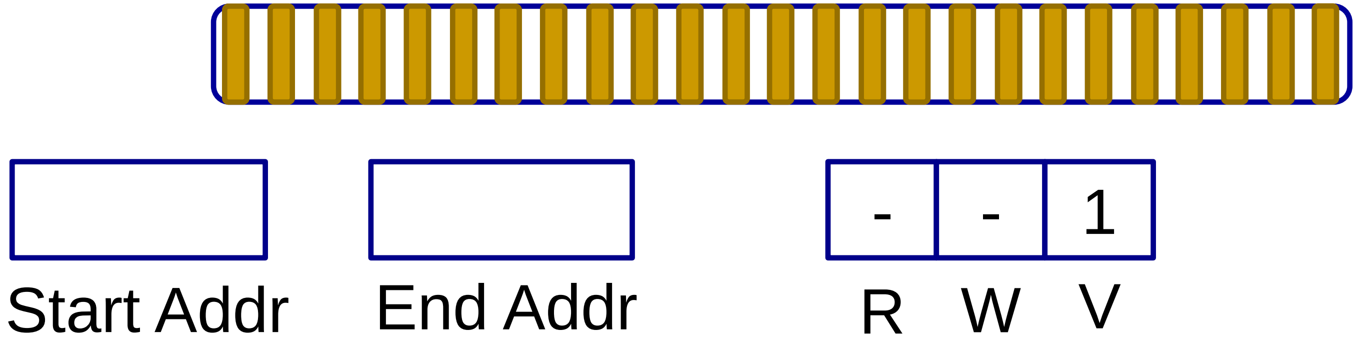


  - 51 ranges x 64b each = **408B**
  - Better stored as bitmap? 51 bits!

- Taint analysis has good ranges
- Byte-accurate race detection does not..

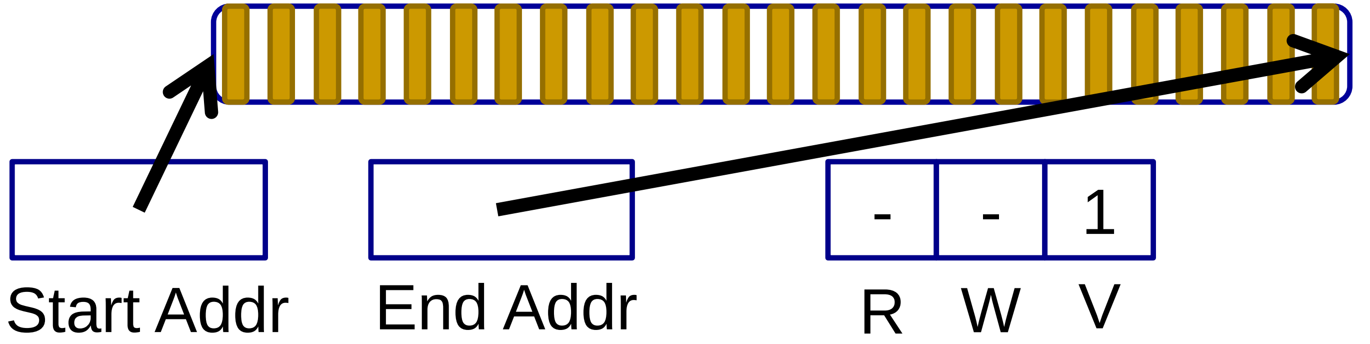
Watchpoint System Design II

- Make some RC entries point to bitmaps



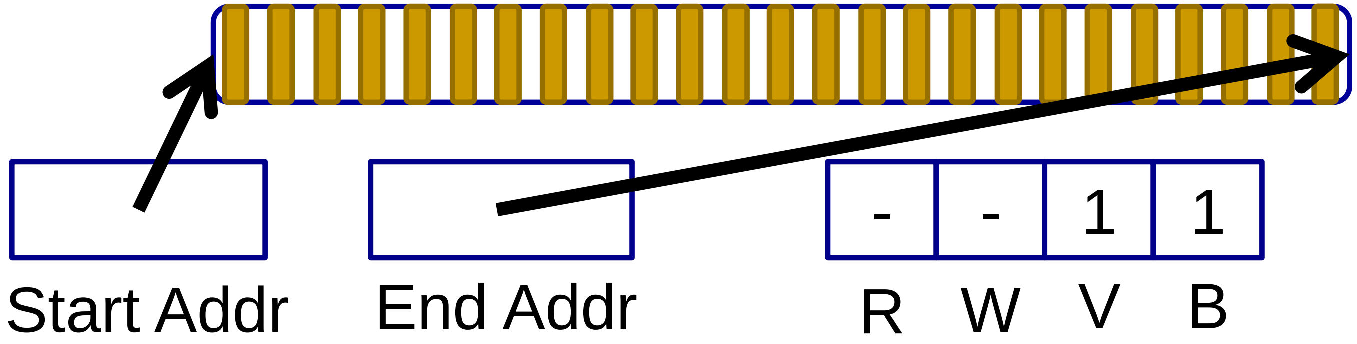
Watchpoint System Design II

- Make some RC entries point to bitmaps



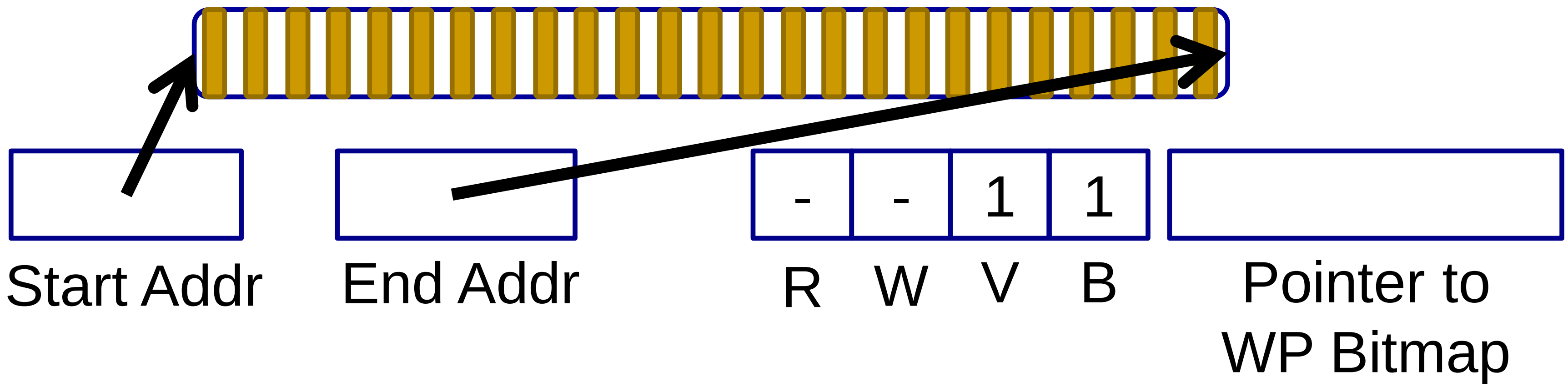
Watchpoint System Design II

- Make some RC entries point to bitmaps



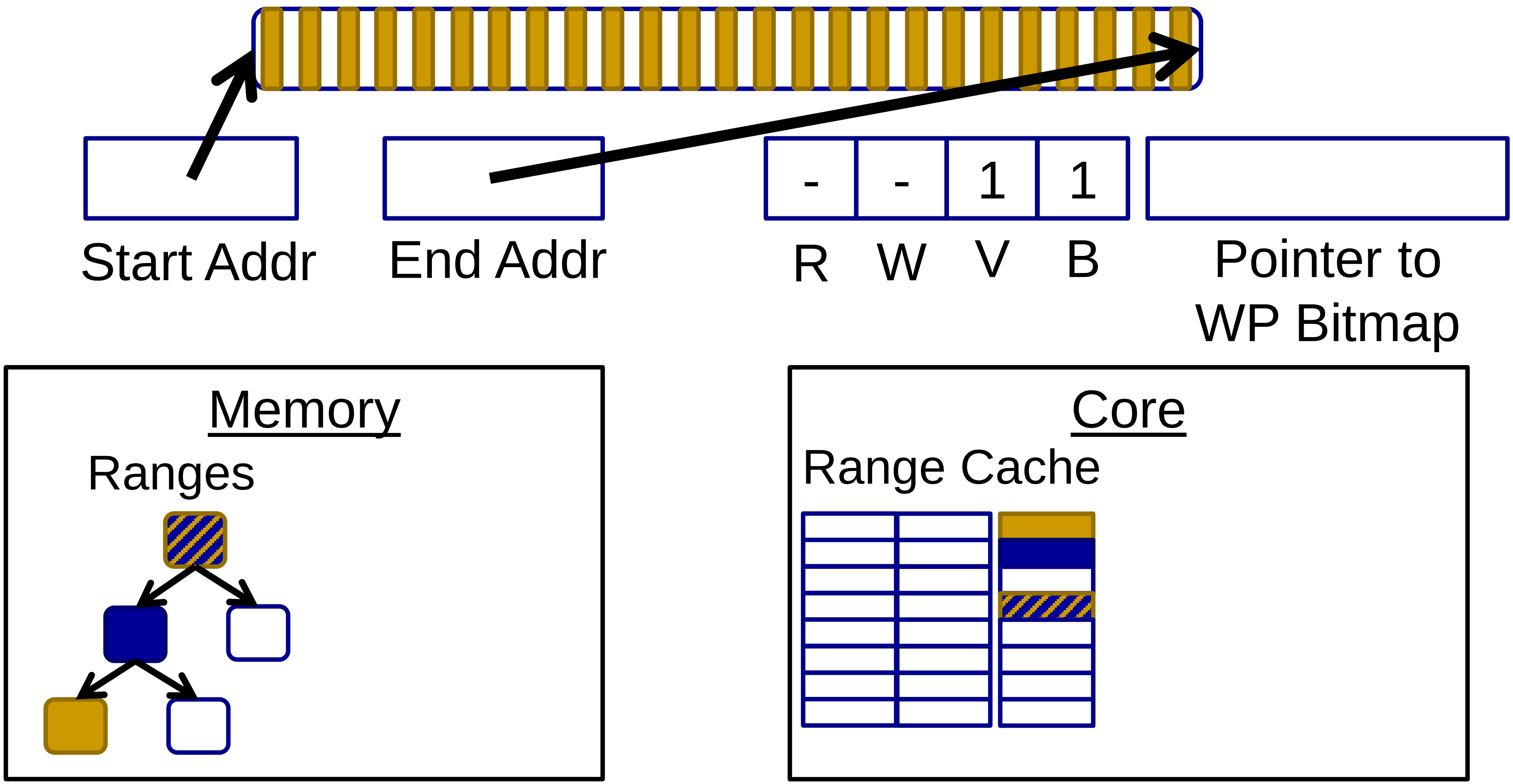
Watchpoint System Design II

- Make some RC entries point to bitmaps



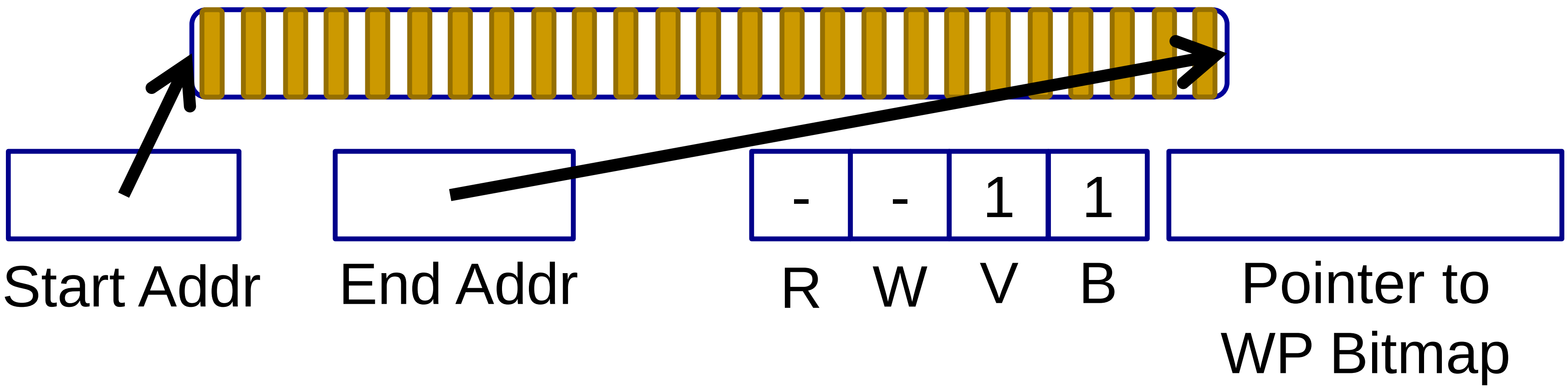
Watchpoint System Design II

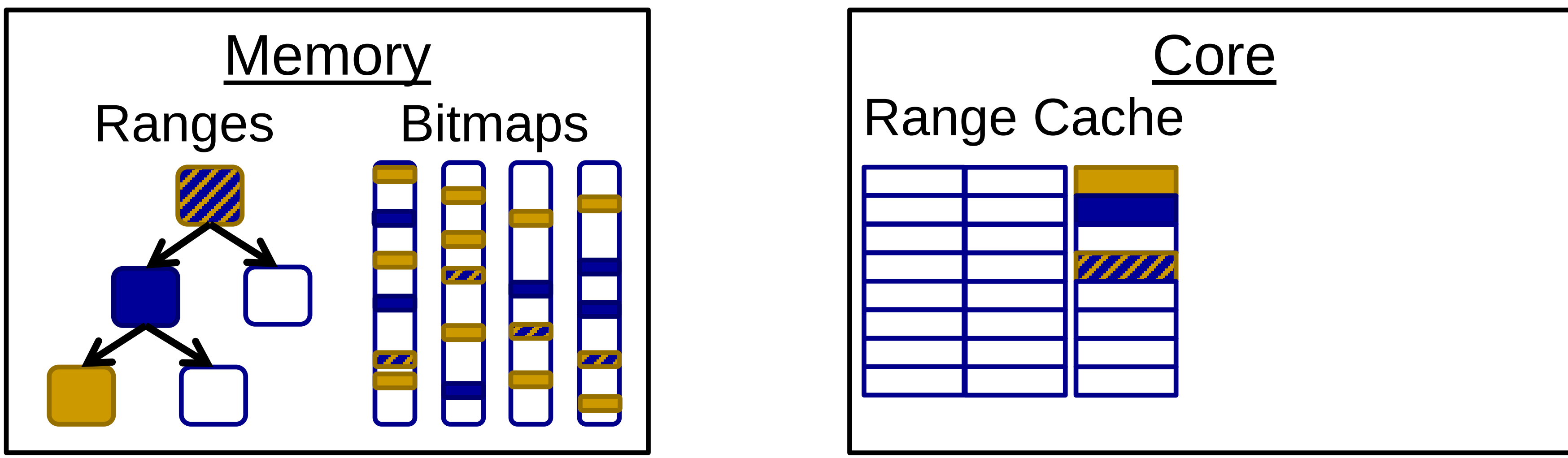
- Make some RC entries point to bitmaps



Watchpoint System Design II

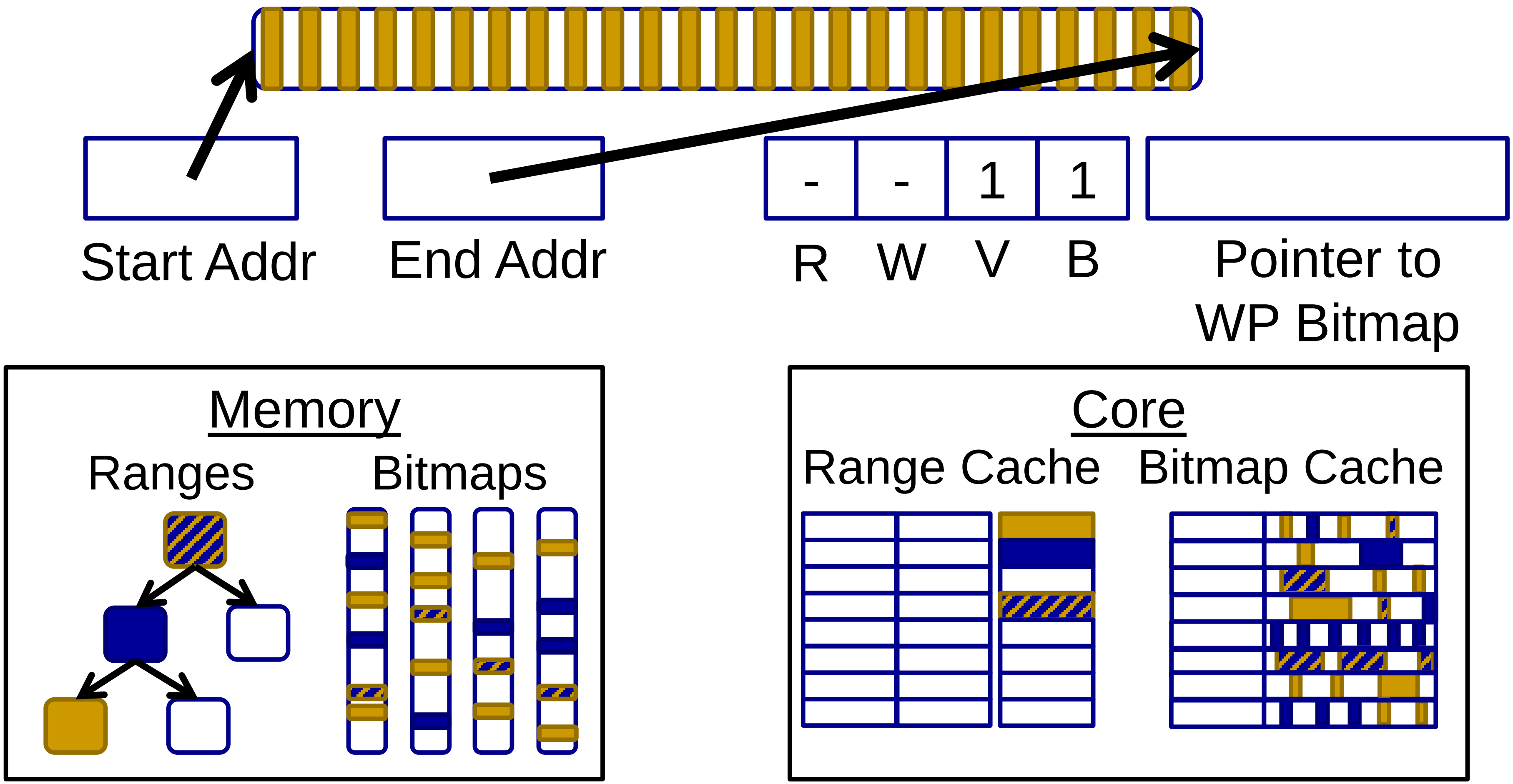
- Make some RC entries point to bitmaps





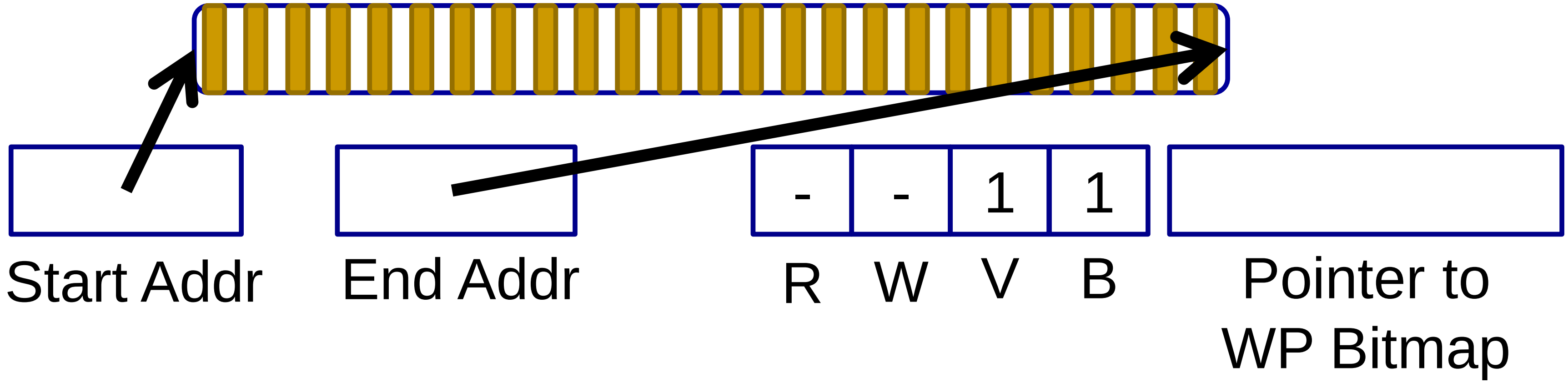
Watchpoint System Design II

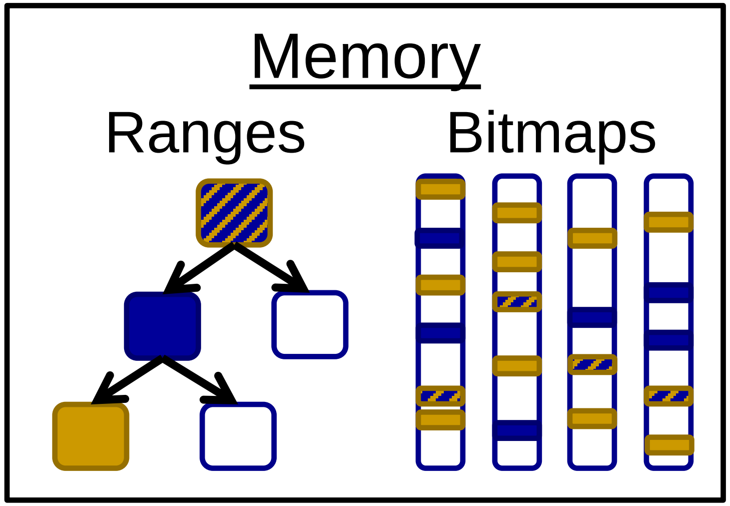
- Make some RC entries point to bitmaps

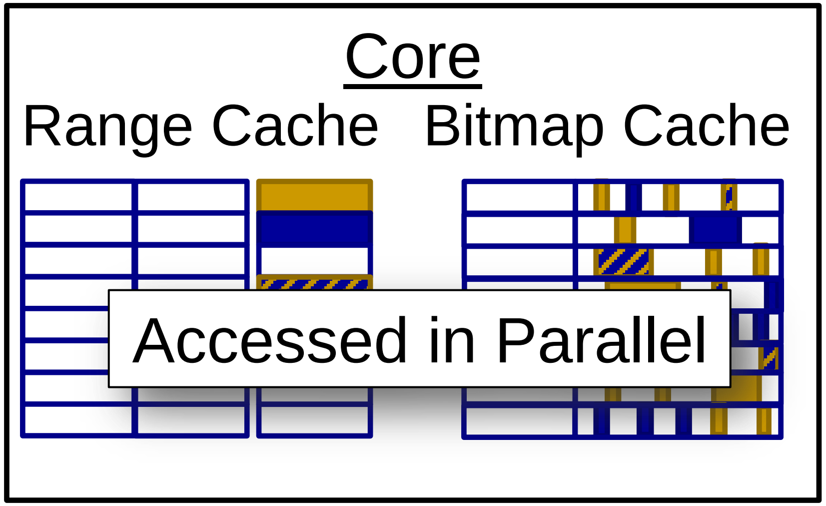


Watchpoint System Design II

- Make some RC entries point to bitmaps

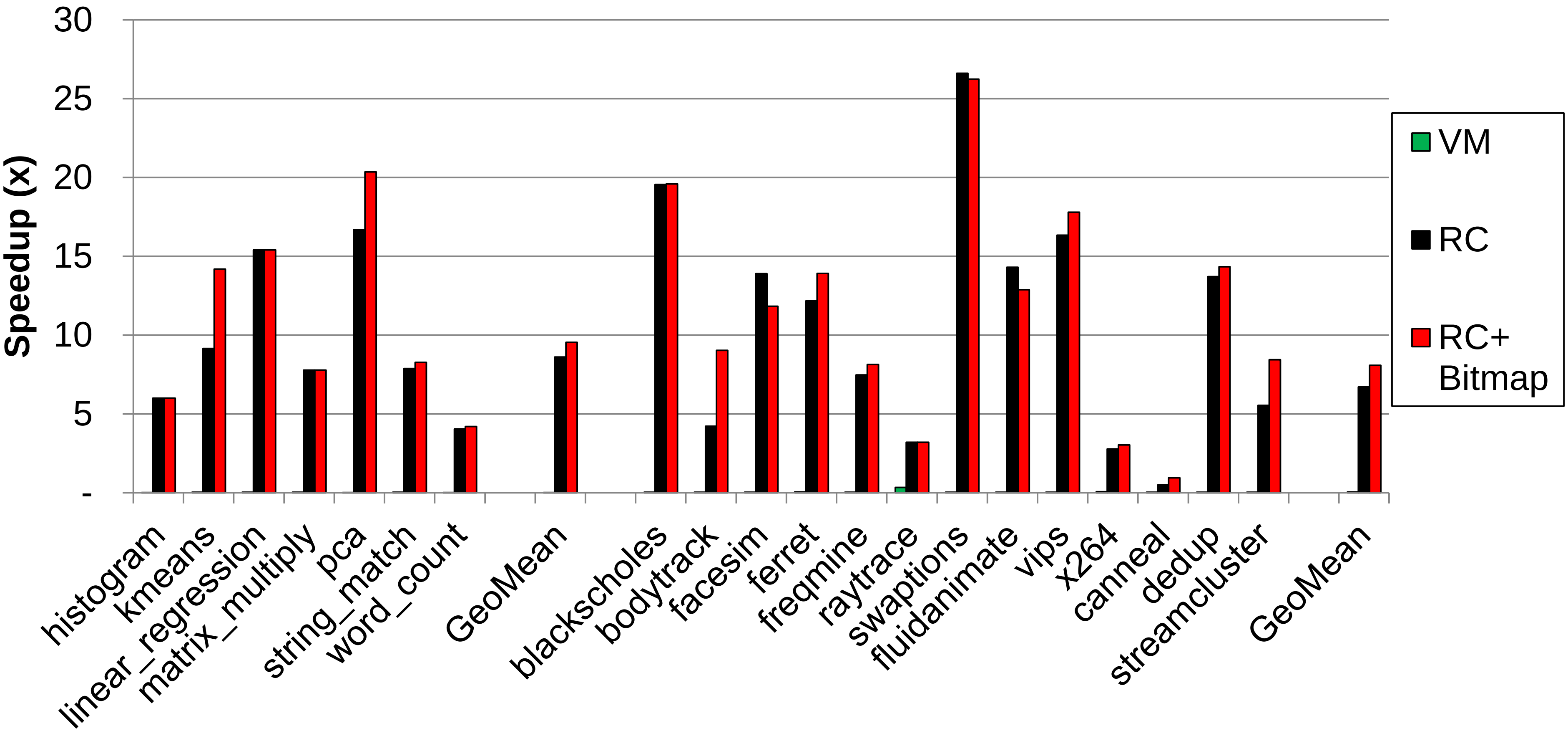






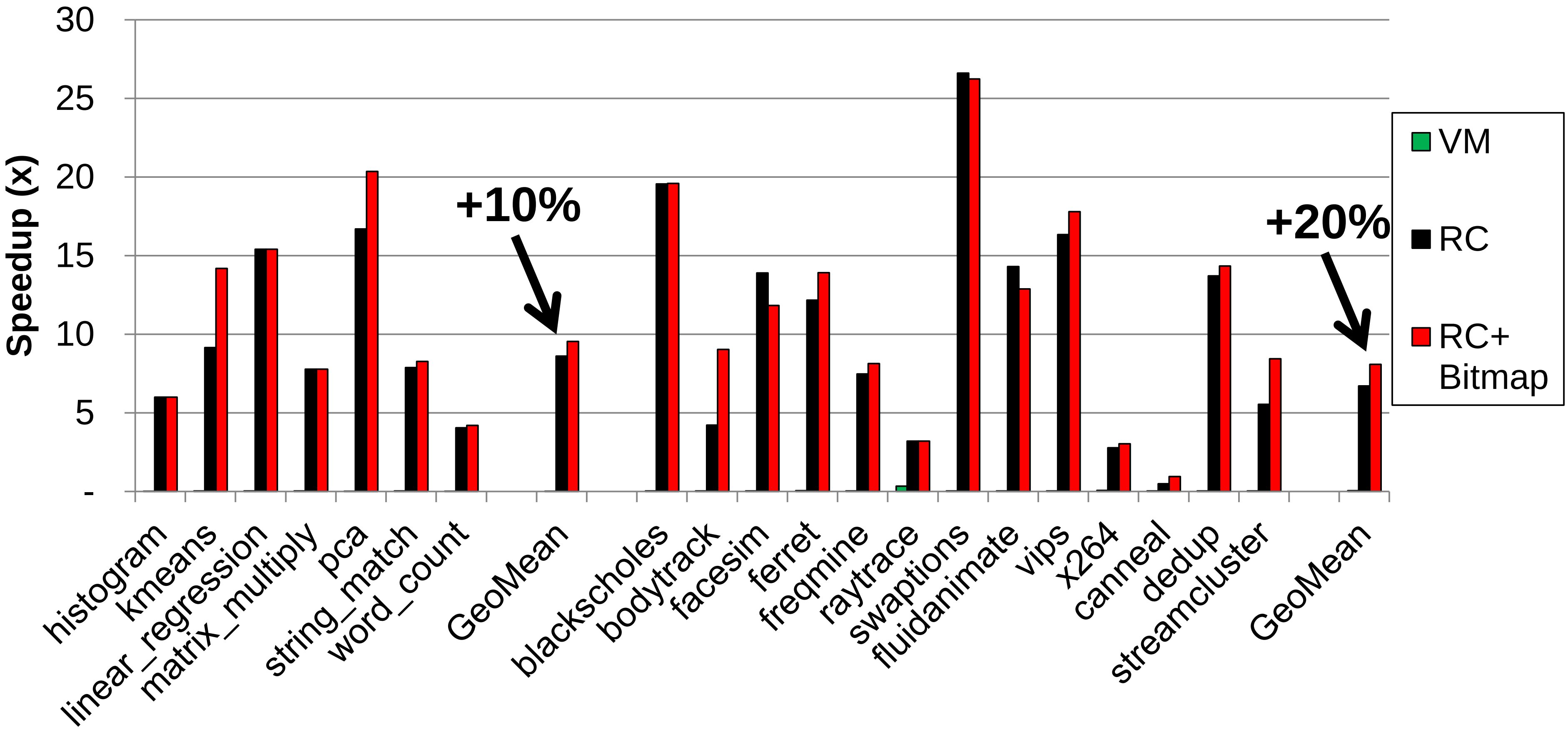
Watchpoint-Based Data Race Detection

- RC now 64 entries, added 2KB bitmap cache



Watchpoint-Based Data Race Detection

- RC now 64 entries, added 2KB bitmap cache



Conclusions & Future Directions

- **Watchpoints** a useful generic mechanism
- Numerous SW systems can utilize a well-designed WP system
- In the future:
  - Clear microarchitectural analysis
  - **More** software systems, different algorithms

Thank You

BACKUP SLIDES

Existing Watchpoint Solutions

- Watchpoint Registers
  - \+ Fine-grained, *can* be per-thread
  - – Limited number (4-16), small reach (4-8 bytes)
- Virtual Memory
  - \+ Virtually unlimited number
  - – Coarse-grained, per-process, *only* aligned ranges
- ECC Mangling
  - \+ Unlimited, finer-grained
  - – Per physical address, no ranges

Width Test