From Array Domains to Abstract Interpretation Under Store-Buffer-Based Memory Models

Thibault Suzanne, Antoine Miné

Static Analysis: 23rd International Symposium, SAS 2016
September, 2016, Edinburgh, UK

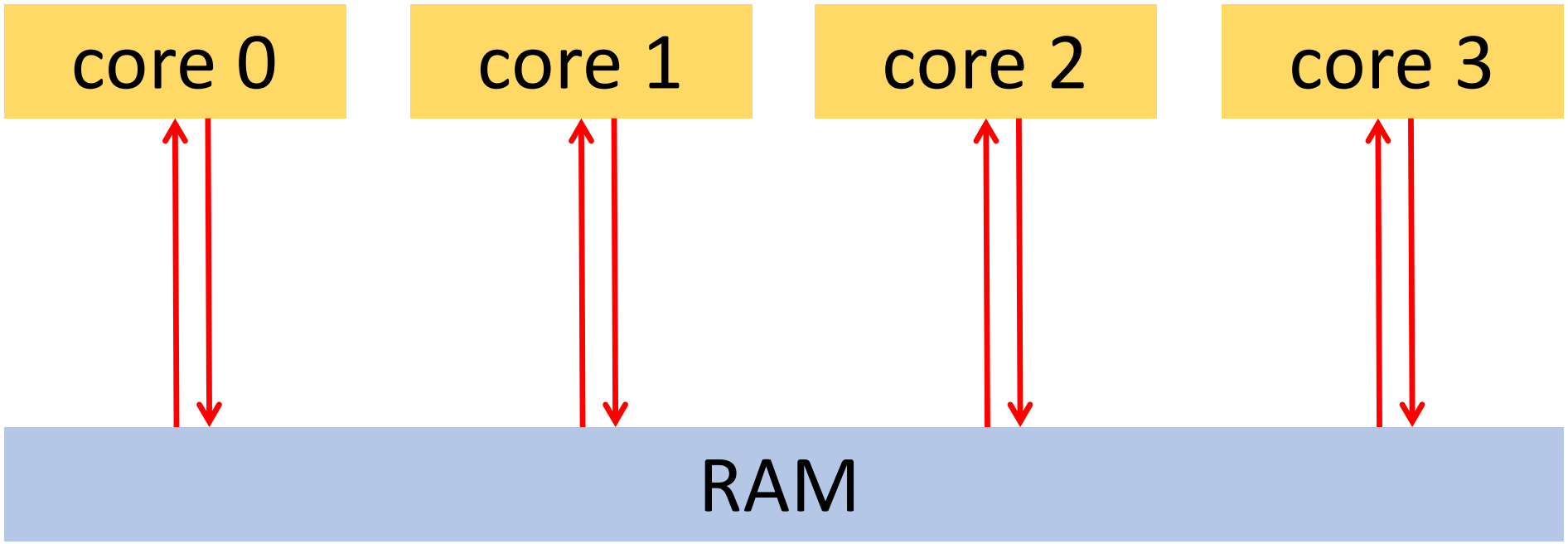
De quoi s’agit-il?

- New abstract interpretation of concurrent programs
- Setting: Weak memory consistency
- Model: store-buffer (FIFO) of infinite size

- including theoretical model, proof and working implementation (OCaml)

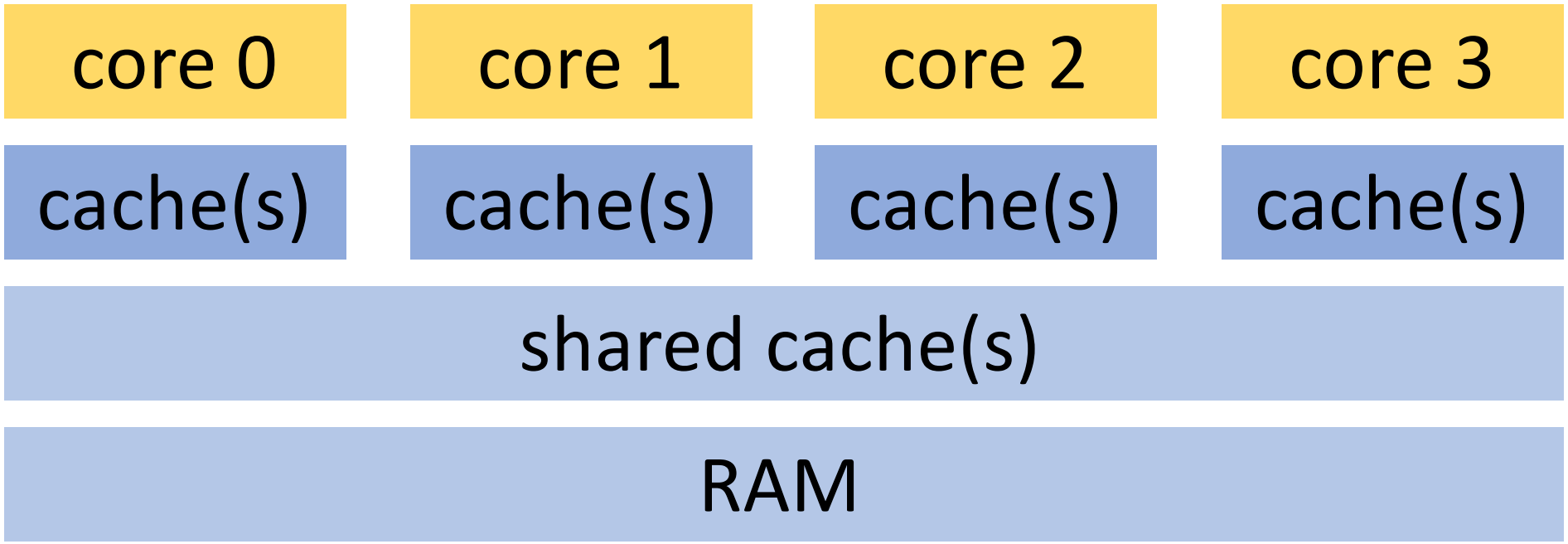
Memory models in Hardware and Languages

- **Strong consistency**



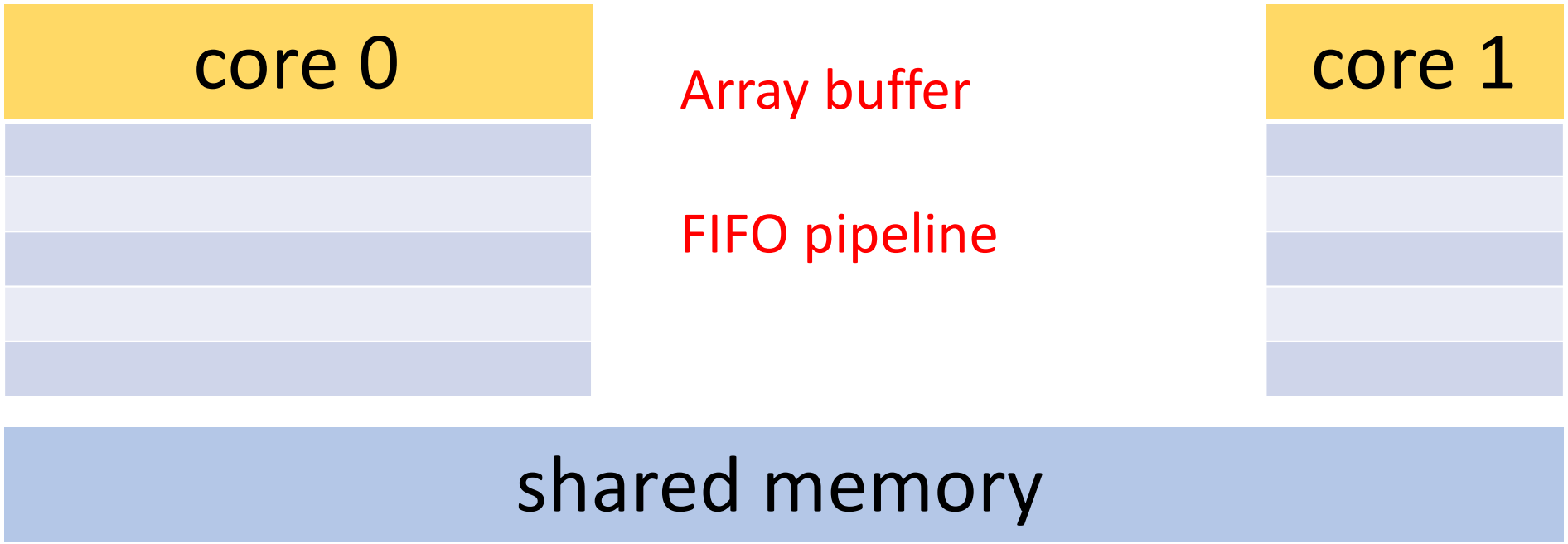
Memory models in Hardware and Languages

- **Weak consistency**



Memory models in Hardware and Languages

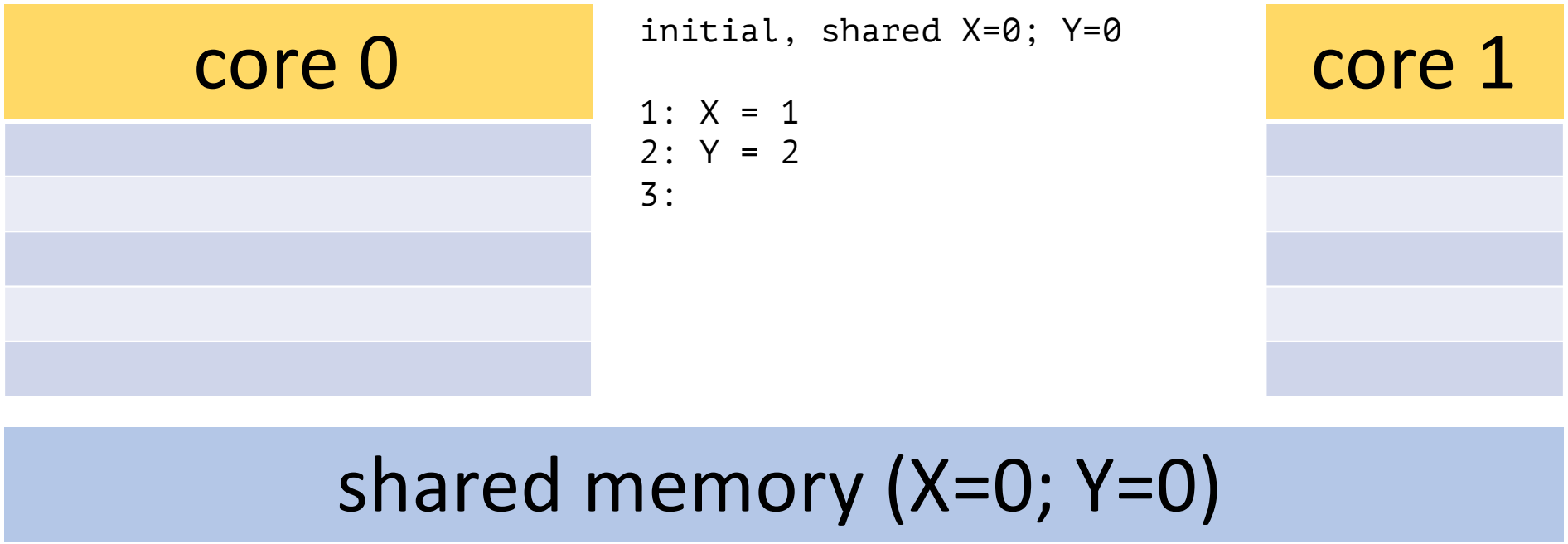
- Weak consistency. **TSO: total store ordering (x86)**



Memory models in Hardware and Languages

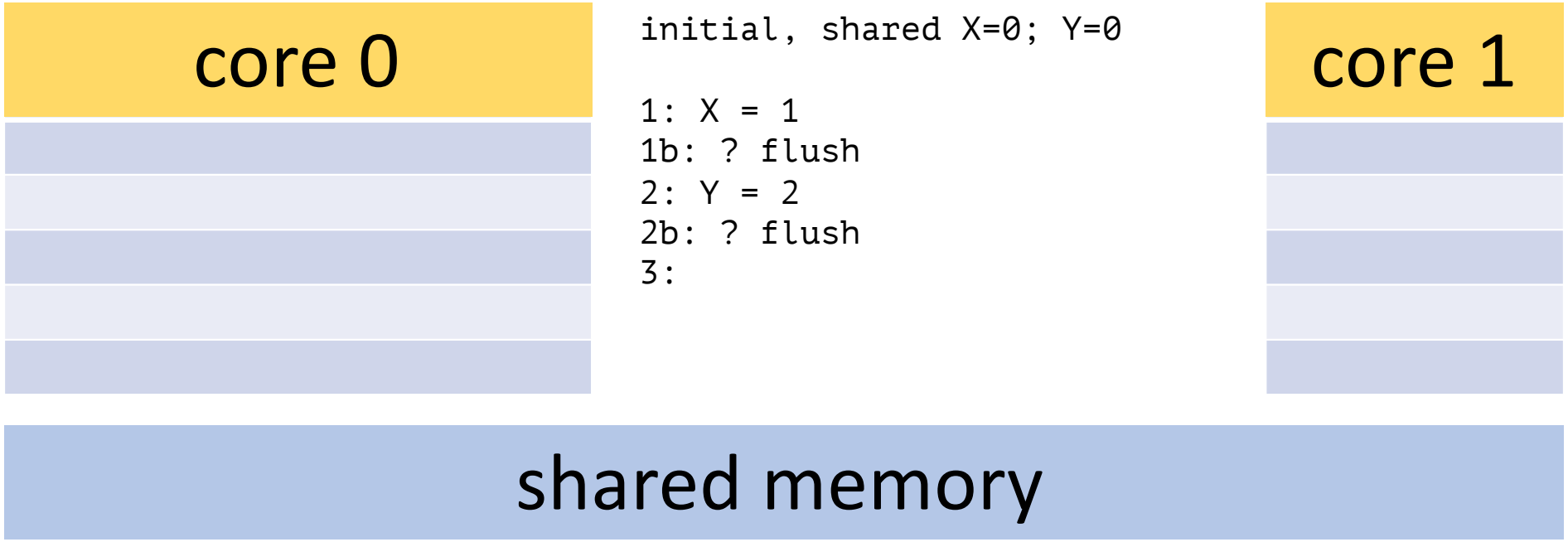
- Weak consistency. **TSO: total store ordering (x86)**

What can it see?



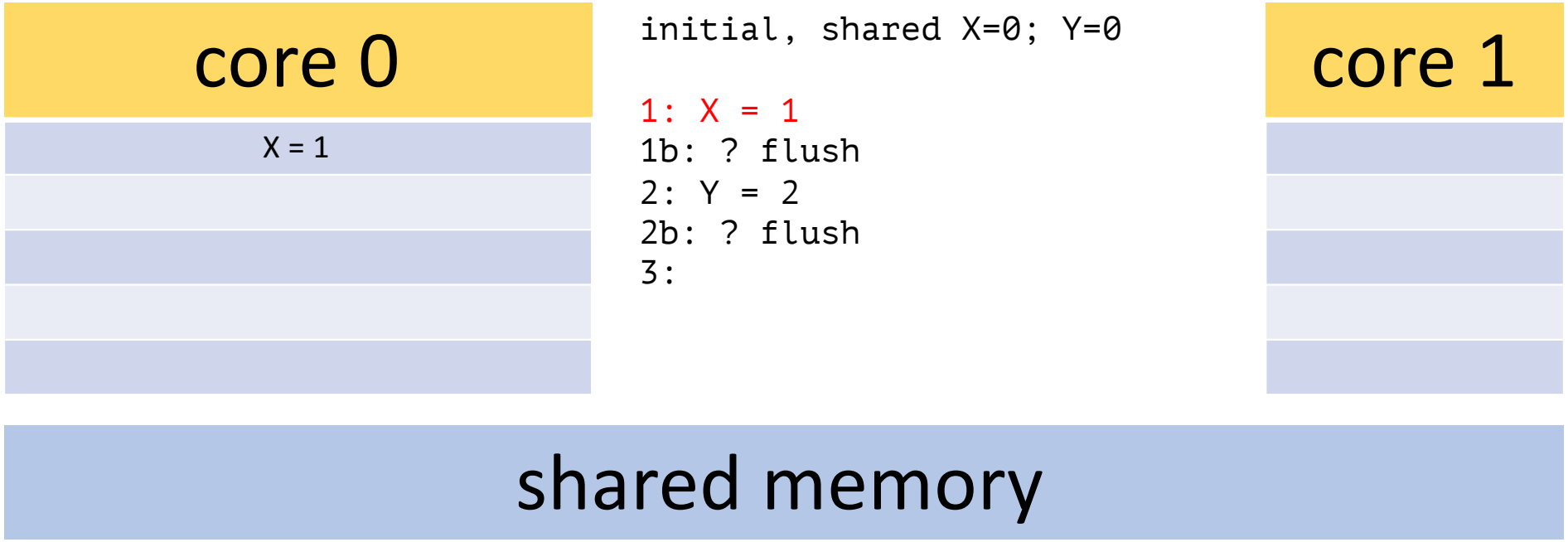
Memory models in Hardware and Languages

- Weak consistency. **TSO: total store ordering (x86)**



Memory models in Hardware and Languages

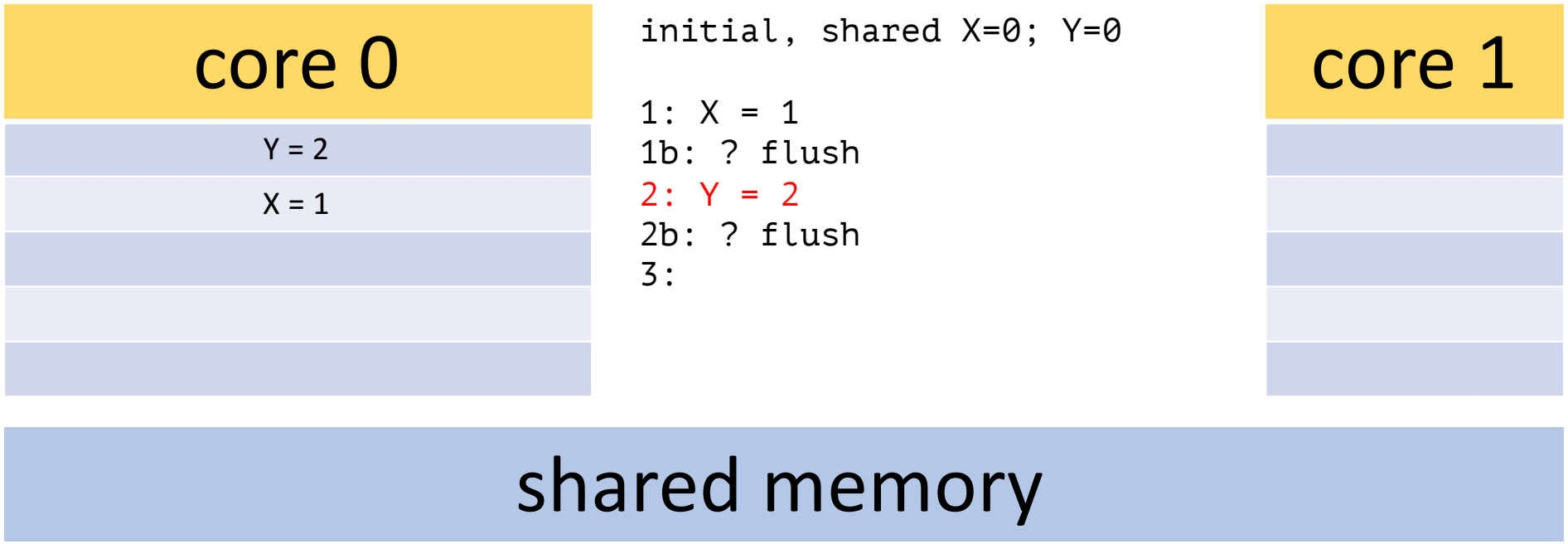
- Weak consistency. **TSO: total store ordering (x86)**



Memory models in Hardware and Languages

- Weak consistency. **TSO: total store ordering (x86)**

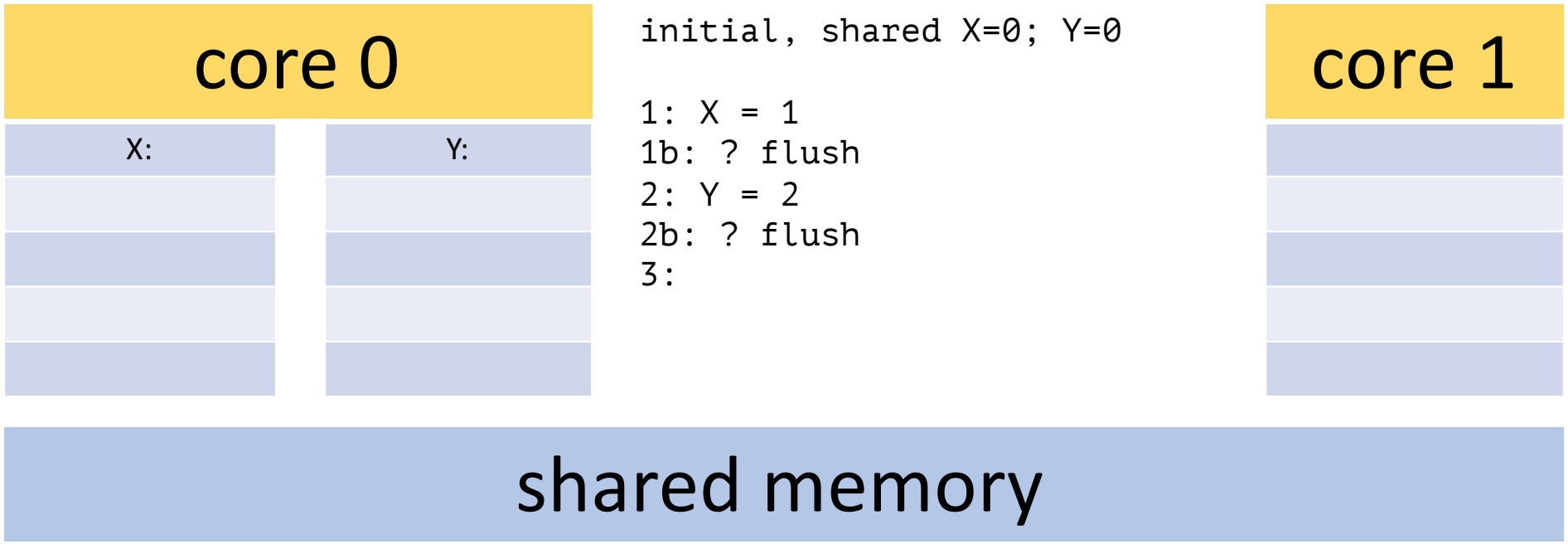
What can it see?



Memory models in Hardware and Languages

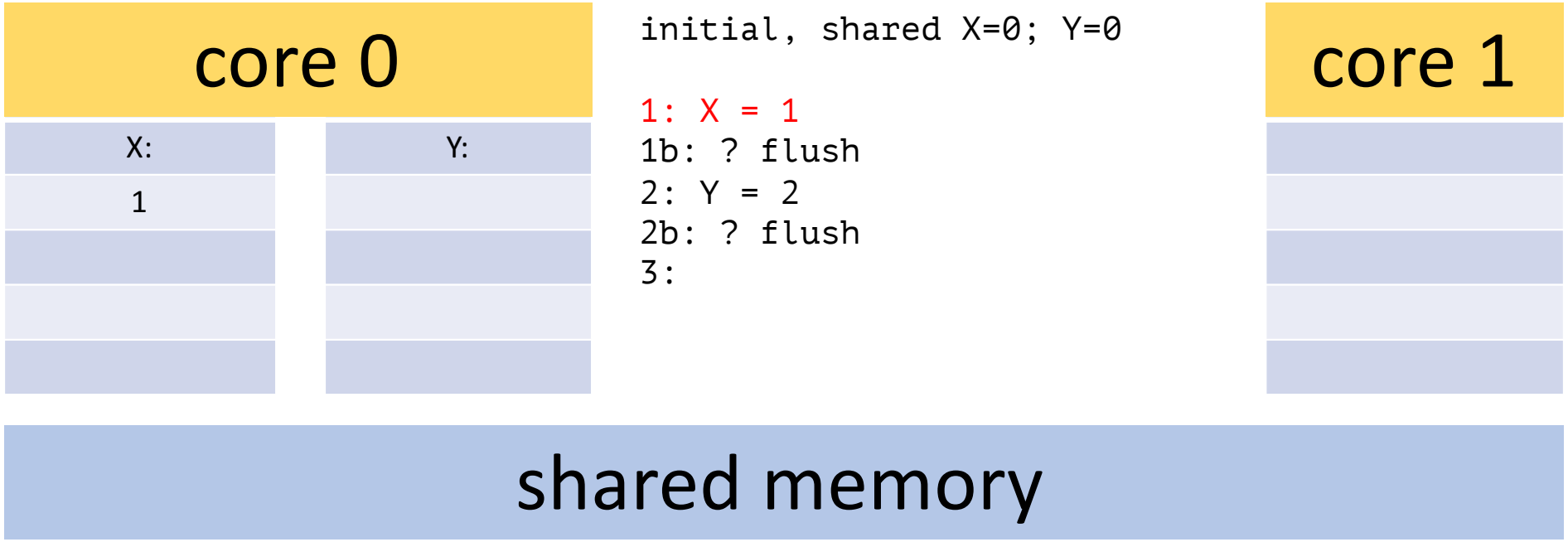
- Weak consistency. **PSO: partial store ordering (ARM)**

What can it see?



Memory models in Hardware and Languages

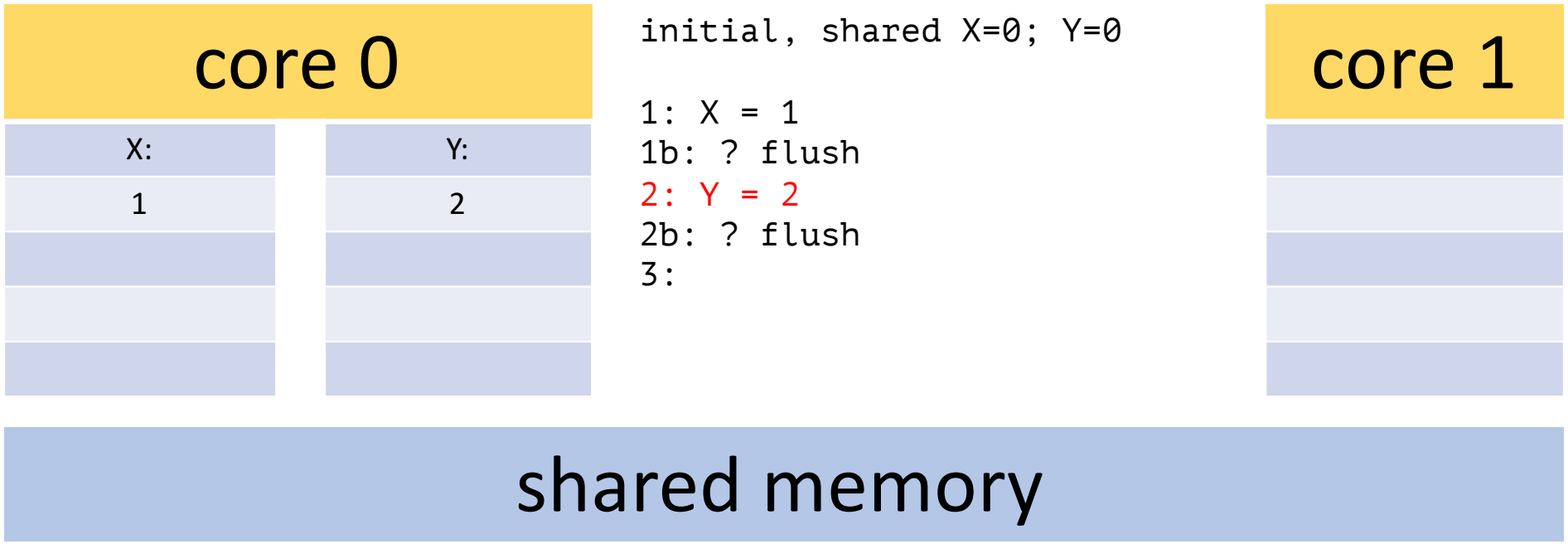
- Weak consistency. **PSO: partial store ordering (ARM)**



Memory models in Hardware and Languages

- Weak consistency. **PSO: partial store ordering (ARM)**

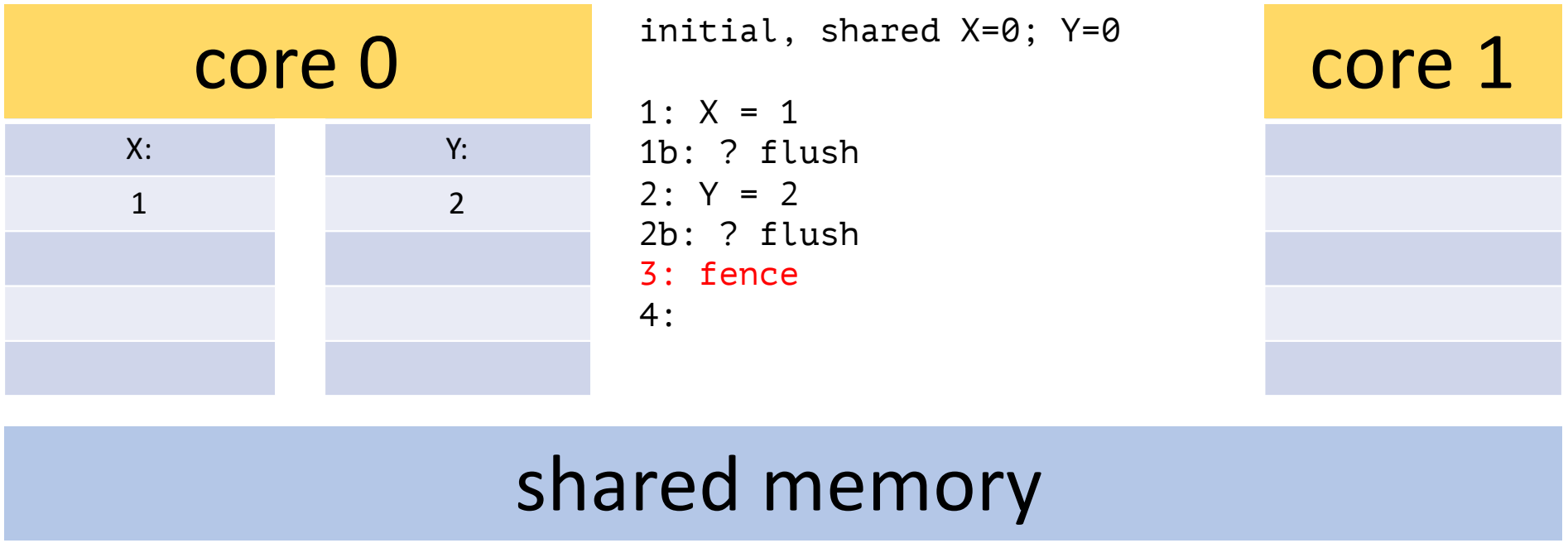
What can it see?



Memory models in Hardware and Languages

- Weak consistency. **PSO: partial store ordering (ARM)**

What can it see?

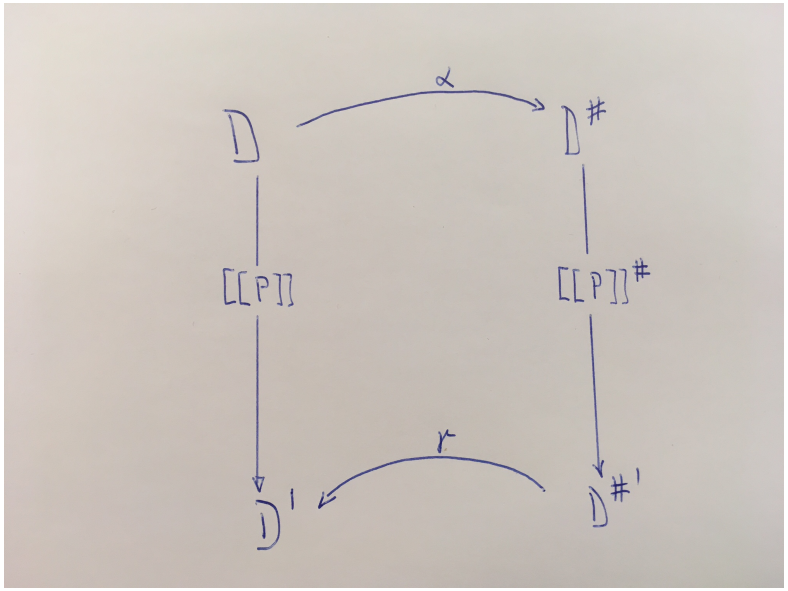


Verification: Model checkers

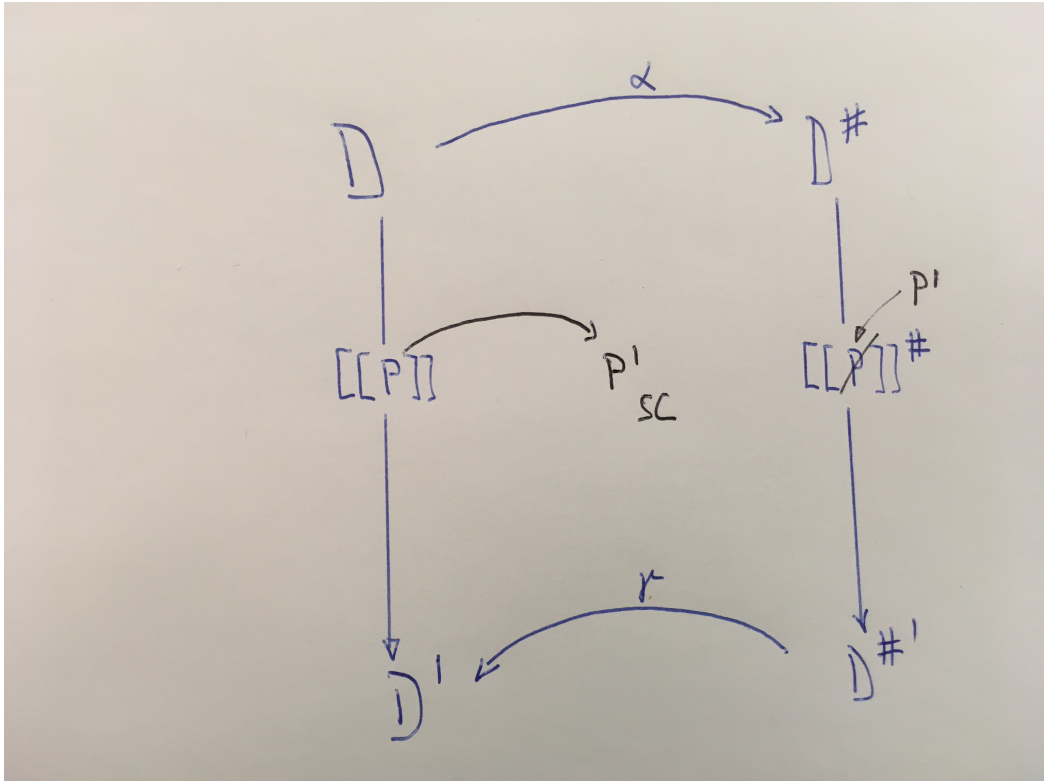
- Promela / spin
- Scyther: crypto protocols

- Limitation: only finite state space
- State space explosion

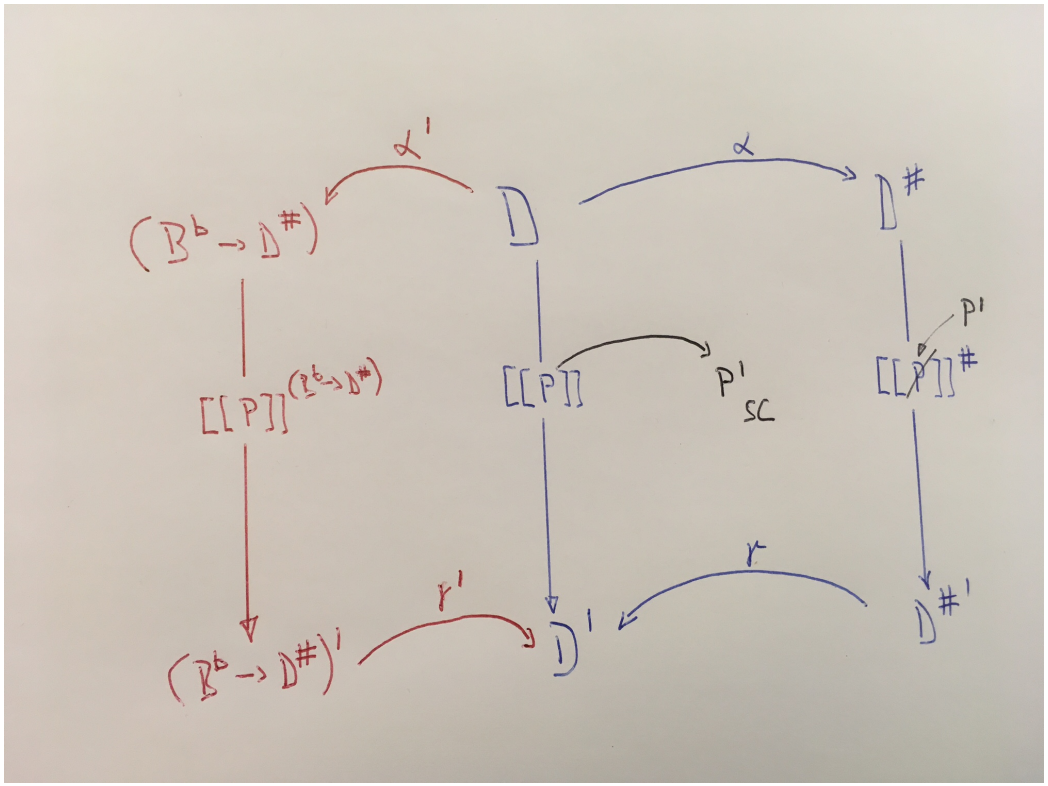
Verification: Abstract interpretation. SC



Verification: Abstract interpretation. Dan et al.



Verification: Abstract interpretation. This study



Comparison

		buffer size	
		n	∞
state size	m	Model Checker	-----
	∞	Dan et al.	This study

PSO model: concrete domain $\mathscr{D}$

$\mathbb{N}^{>0}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$VarMem \triangleq \{x^{mem} \mid x \in Var\} \tag{1}$$

$$Mem \triangleq VarMem \to \mathbb{V} \qquad Reg \triangleq VarReg \to \mathbb{V} \tag{2}$$

$$\forall x \in Var, T \in Thread, N \in \mathbb{N},\ VarBuf(x,T,N) \triangleq \left\{x_i^T \mid 1 \le i \le N\right\} \tag{3}$$

$$Buf(x,T,N) \triangleq VarBuf(x,T,N) \to \mathbb{V} \tag{4}$$

$$BufSizes \triangleq (Var \times Thread) \to \mathbb{N} \tag{5}$$

$$\mathscr{S} \triangleq \bigcup_{N \in BufSizes} \left(Mem \times Reg \times \prod_{\substack{x \in Var \\ T \in Thread}} Buf(x,T,N(x,T)) \right) \tag{6}$$

$$\mathscr{D} \triangleq \mathcal{P}(\mathscr{S}) \tag{7}$$

Fig. 3. A concrete domain for PSO programs

PSO model: concrete domain $\mathscr{D}$

$\mathbb{N}^{>0}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$VarMem \triangleq \{x^{mem} \mid x \in Var\} \quad (1)$$

$$Mem \triangleq VarMem \to \mathbb{V} \qquad Reg \triangleq VarReg \to \mathbb{V} \quad (2)$$

$$\forall x \in Var, T \in Thread, N \in \mathbb{N}, VarBuf(x,T,N) \triangleq \left\{x_i^T \mid 1 \le i \le N\right\} \quad (3)$$

$$Buf(x,T,N) \triangleq VarBuf(x,T,N) \to \mathbb{V} \quad (4)$$

$$BufSizes \triangleq (Var \times Thread) \to \mathbb{N} \quad (5)$$

$$\mathscr{S} \triangleq \bigcup_{N \in BufSizes} \left(Mem \times Reg \times \prod_{\substack{x \in Var \\ T \in Thread}} Buf(x,T,N(x,T)) \right) \quad (6)$$

$$\mathscr{D} \triangleq \mathcal{P}(\mathscr{S}) \quad (7)$$

Fig. 3. A concrete domain for PSO programs

PSO model: concrete domain $\mathscr{D}$

$\mathbb{N}^{>0}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$VarMem \triangleq \{x^{mem} \mid x \in Var\} \quad (1)$$

$$Mem \triangleq VarMem \to \mathbb{V} \qquad Reg \triangleq VarReg \to \mathbb{V} \quad (2)$$

$$\forall x \in Var, T \in Thread, N \in \mathbb{N},\ VarBuf(x,T,N) \triangleq \left\{x_i^T \mid 1 \le i \le N\right\} \quad (3)$$

$$Buf(x,T,N) \triangleq VarBuf(x,T,N) \to \mathbb{V} \quad (4)$$

$$BufSizes \triangleq (Var \times Thread) \to \mathbb{N} \quad (5)$$

$$\mathscr{S} \triangleq \bigcup_{N \in BufSizes} \left(Mem \times Reg \times \prod_{\substack{x \in Var \\ T \in Thread}} Buf(x,T,N(x,T)) \right) \quad (6)$$

$$\mathscr{D} \triangleq \mathcal{P}(\mathscr{S}) \quad (7)$$

Fig. 3. A concrete domain for PSO programs

PSO model: concrete domain $\mathscr{D}$

$\mathbb{N}^{>0}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$VarMem \triangleq \{x^{mem} \mid x \in Var\} \tag{1}$$

$$Mem \triangleq VarMem \to \mathbb{V} \qquad Reg \triangleq VarReg \to \mathbb{V} \tag{2}$$

$$\forall x \in Var, T \in Thread, N \in \mathbb{N},\ VarBuf(x,T,N) \triangleq \left\{x_i^T \mid 1 \le i \le N\right\} \tag{3}$$

$$Buf(x,T,N) \triangleq VarBuf(x,T,N) \to \mathbb{V} \tag{4}$$

$$BufSizes \triangleq (Var \times Thread) \to \mathbb{N} \tag{5}$$

$$\mathscr{S} \triangleq \bigcup_{N \in BufSizes} \left(Mem \times Reg \times \prod_{\substack{x \in Var \\ T \in Thread}} Buf(x,T,N(x,T)) \right) \tag{6}$$

$$\mathscr{D} \triangleq \mathcal{P}(\mathscr{S}) \tag{7}$$

Fig. 3. A concrete domain for PSO programs

PSO model: concrete semantics $[\![.]\!]_T : \mathscr{D} \to \mathscr{D}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$\forall T \in \mathit{Thread}, [\![.]\!]_T : \mathscr{D} \to \mathscr{D} \tag{8}$$

$$[\![x := e]\!]_T\{S\} \triangleq [\![x_1^T := e]\!] \circ [\![x_2^T := x_1^T]\!] \circ \ldots \\ \ldots \circ [\![x^T_{N_S(x,T)+1} := x^T_{N_S(x,T)}]\!] \circ [\![add\ x^T_{N_S(x,T)+1}]\!]\{S\} \tag{9}$$

$$[\![r := x]\!]_T\{S\} \triangleq \begin{cases} [\![r := x^{mem}]\!]S & \text{if } N_S(x,T) = 0 \\ [\![r := x_1^T]\!]S & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{10}$$

$$[\![\texttt{mfence}]\!]_T\{S\} \triangleq \begin{cases} S & \text{if } \forall x \in \mathit{Var}, N_S(x,T) = 0 \\ \emptyset & \text{otherwise} \end{cases} \tag{11}$$

$$[\![\texttt{flush}\ x]\!]_T\{S\} \triangleq \begin{cases} \emptyset & \text{if } N_S(x,T) = 0 \\ [\![drop\ x^T_{N_S(x,T)}]\!] \circ [\![x^{mem} := x^T_{N_S(x,T)}]\!]\{S\} & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{12}$$

$$\forall X \in \mathscr{D}, [\![ins]\!]_T X \triangleq \bigcup_{S \in X} [\![ins]\!]_T\{S\} \tag{13}$$

Fig. 4. Concrete semantics in PSO

PSO model: concrete semantics $[\![.]\!]_T : \mathscr{D} \to \mathscr{D}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$\forall T \in \mathit{Thread}, [\![.]\!]_T : \mathscr{D} \to \mathscr{D} \tag{8}$$

$$[\![x := e]\!]_T\{S\} \triangleq [\![x_1^T := e]\!] \circ [\![x_2^T := x_1^T]\!] \circ \ldots \tag{9}$$
$$\ldots \circ [\![x^T_{N_S(x,T)+1} := x^T_{N_S(x,T)}]\!] \circ [\![add\ x^T_{N_S(x,T)+1}]\!]\{S\}$$

$$[\![r := x]\!]_T\{S\} \triangleq \begin{cases} [\![r := x^{mem}]\!]S & \text{if } N_S(x,T) = 0 \\ [\![r := x_1^T]\!]S & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{10}$$

$$[\![\texttt{mfence}]\!]_T\{S\} \triangleq \begin{cases} S & \text{if } \forall x \in \mathit{Var}, N_S(x,T) = 0 \\ \emptyset & \text{otherwise} \end{cases} \tag{11}$$

$$[\![\texttt{flush}\ x]\!]_T\{S\} \triangleq \begin{cases} \emptyset & \text{if } N_S(x,T) = 0 \\ [\![drop\ x^T_{N_S(x,T)}]\!] \circ [\![x^{mem} := x^T_{N_S(x,T)}]\!]\{S\} & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{12}$$

$$\forall X \in \mathscr{D}, [\![ins]\!]_T X \triangleq \bigcup_{S \in X} [\![ins]\!]_T\{S\} \tag{13}$$

Fig. 4. Concrete semantics in PSO

PSO model: concrete semantics $[\![.]\!]_T : \mathscr{D} \to \mathscr{D}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2=e	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1	x_3^2	z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$\forall T \in \mathit{Thread}, [\![.]\!]_T : \mathscr{D} \to \mathscr{D} \tag{8}$$

$$[\![x := e]\!]_T\{S\} \triangleq [\![x_1^T := e]\!] \circ [\![x_2^T := x_1^T]\!] \circ \ldots \tag{9}$$
$$\ldots \circ [\![x^T_{N_S(x,T)+1} := x^T_{N_S(x,T)}]\!] \circ [\![add\ x^T_{N_S(x,T)+1}]\!]\{S\}$$

$$[\![r := x]\!]_T\{S\} \triangleq \begin{cases} [\![r := x^{mem}]\!]S & \text{if } N_S(x,T) = 0 \\ [\![r := x_1^T]\!]S & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{10}$$

$$[\![\texttt{mfence}]\!]_T\{S\} \triangleq \begin{cases} S & \text{if } \forall x \in \mathit{Var}, N_S(x,T) = 0 \\ \emptyset & \text{otherwise} \end{cases} \tag{11}$$

$$[\![\texttt{flush}\ x]\!]_T\{S\} \triangleq \begin{cases} \emptyset & \text{if } N_S(x,T) = 0 \\ [\![drop\ x^T_{N_S(x,T)}]\!] \circ [\![x^{mem} := x^T_{N_S(x,T)}]\!]\{S\} & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{12}$$

$$\forall X \in \mathscr{D}, [\![ins]\!]_T X \triangleq \bigcup_{S \in X} [\![ins]\!]_T\{S\} \tag{13}$$

Fig. 4. Concrete semantics in PSO

PSO model: concrete semantics $[\![.]\!]_T : \mathscr{D} \to \mathscr{D}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1	x_3^2	z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$\forall T \in \mathit{Thread}, [\![.]\!]_T : \mathscr{D} \to \mathscr{D} \tag{8}$$

$$[\![x := e]\!]_T\{S\} \triangleq [\![x_1^T := e]\!] \circ [\![x_2^T := x_1^T]\!] \circ \ldots \tag{9}$$
$$\ldots \circ [\![x^T_{N_S(x,T)+1} := x^T_{N_S(x,T)}]\!] \circ [\![\mathit{add}\ x^T_{N_S(x,T)+1}]\!]\{S\}$$

$$[\![r := x]\!]_T\{S\} \triangleq \begin{cases} [\![r := x^{mem}]\!]S & \text{if } N_S(x,T) = 0 \\ [\![r := x_1^T]\!]S & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{10}$$

$$[\![\texttt{mfence}]\!]_T\{S\} \triangleq \begin{cases} S & \text{if } \forall x \in \mathit{Var}, N_S(x,T) = 0 \\ \emptyset & \text{otherwise} \end{cases} \tag{11}$$

$$[\![\texttt{flush}\ x]\!]_T\{S\} \triangleq \begin{cases} \emptyset & \text{if } N_S(x,T) = 0 \\ [\![\mathit{drop}\ x^T_{N_S(x,T)}]\!] \circ [\![x^{mem} := x^T_{N_S(x,T)}]\!]\{S\} & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{12}$$

$$\forall X \in \mathscr{D}, [\![ins]\!]_T X \triangleq \bigcup_{S \in X} [\![ins]\!]_T\{S\} \tag{13}$$

Fig. 4. Concrete semantics in PSO

PSO model: concrete semantics $[\![.]\!]_T : \mathscr{D} \to \mathscr{D}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1	x_3^2	z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$\forall T \in \mathit{Thread}, [\![.]\!]_T : \mathscr{D} \to \mathscr{D} \tag{8}$$

$$[\![x := e]\!]_T\{S\} \triangleq [\![x_1^T := e]\!] \circ [\![x_2^T := x_1^T]\!] \circ \ldots \tag{9}$$
$$\ldots \circ [\![x^T_{N_S(x,T)+1} := x^T_{N_S(x,T)}]\!] \circ [\![\mathit{add}\ x^T_{N_S(x,T)+1}]\!]\{S\}$$

$$[\![r := x]\!]_T\{S\} \triangleq \begin{cases} [\![r := x^{mem}]\!]S & \text{if } N_S(x,T) = 0 \\ [\![r := x_1^T]\!]S & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{10}$$

$$[\![\texttt{mfence}]\!]_T\{S\} \triangleq \begin{cases} S & \text{if } \forall x \in \mathit{Var}, N_S(x,T) = 0 \\ \emptyset & \text{otherwise} \end{cases} \tag{11}$$

$$[\![\texttt{flush}\ x]\!]_T\{S\} \triangleq \begin{cases} \emptyset & \text{if } N_S(x,T) = 0 \\ [\![\mathit{drop}\ x^T_{N_S(x,T)}]\!] \circ [\![x^{mem} := x^T_{N_S(x,T)}]\!]\{S\} & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{12}$$

$$\forall X \in \mathscr{D}, [\![ins]\!]_T X \triangleq \bigcup_{S \in X} [\![ins]\!]_T\{S\} \tag{13}$$

Fig. 4. Concrete semantics in PSO

PSO model: concrete semantics $[\![.]\!]_T : \mathscr{D} \to \mathscr{D}$

thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1	x_2^2	z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$\forall T \in \mathit{Thread}, [\![.]\!]_T : \mathscr{D} \to \mathscr{D} \tag{8}$$

$$[\![x := e]\!]_T\{S\} \triangleq [\![x_1^T := e]\!] \circ [\![x_2^T := x_1^T]\!] \circ \ldots \\ \ldots \circ [\![x^T_{N_S(x,T)+1} := x^T_{N_S(x,T)}]\!] \circ [\![add\ x^T_{N_S(x,T)+1}]\!]\{S\} \tag{9}$$

$$[\![r := x]\!]_T\{S\} \triangleq \begin{cases} [\![r := x^{mem}]\!]S & \text{if } N_S(x,T) = 0 \\ [\![r := x_1^T]\!]S & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{10}$$

$$[\![\texttt{mfence}]\!]_T\{S\} \triangleq \begin{cases} S & \text{if } \forall x \in \mathit{Var}, N_S(x,T) = 0 \\ \emptyset & \text{otherwise} \end{cases} \tag{11}$$

$$[\![\texttt{flush}\ x]\!]_T\{S\} \triangleq \begin{cases} \emptyset & \text{if } N_S(x,T) = 0 \\ [\![drop\ x^T_{N_S(x,T)}]\!] \circ [\![x^{mem} := x^T_{N_S(x,T)}]\!]\{S\} & \text{if } N_S(x,T) \geq 1 \end{cases} \tag{12}$$

$$\forall X \in \mathscr{D}, [\![ins]\!]_T X \triangleq \bigcup_{S \in X} [\![ins]\!]_T\{S\} \tag{13}$$

Fig. 4. Concrete semantics in PSO

Abstraction: handling ∞

- Key insight: summarize and partition.

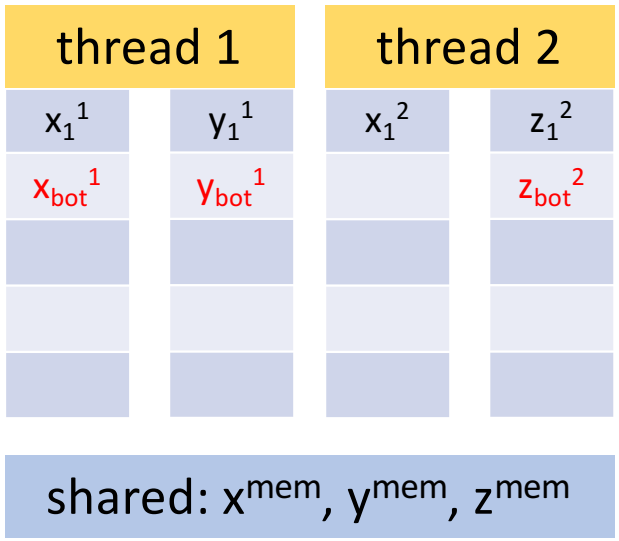
thread 1		thread 2	
x_1^1	y_1^1	x_1^2	z_1^2
x_2^1	y_2^1		z_2^2
x_3^1	y_3^1		z_3^2
x_4^1			
x_5^1			

shared: x^{mem}, y^{mem}, z^{mem}

$$\alpha_{sum} : \mathscr{D} \rightarrow \mathscr{D}^{\natural}$$

Abstraction: handling ∞

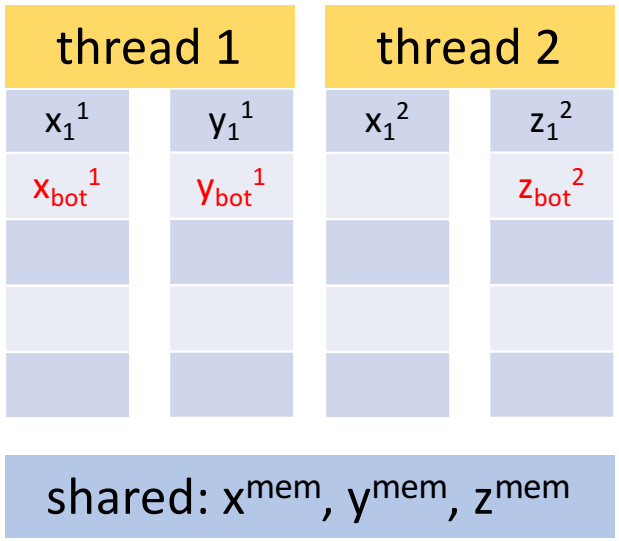
- Key insight: summarize and partition.



$$\alpha_{sum} : \mathscr{D} \rightarrow \mathscr{D}^\natural$$

Abstraction: handling ∞

- Key insight: summarize and partition.



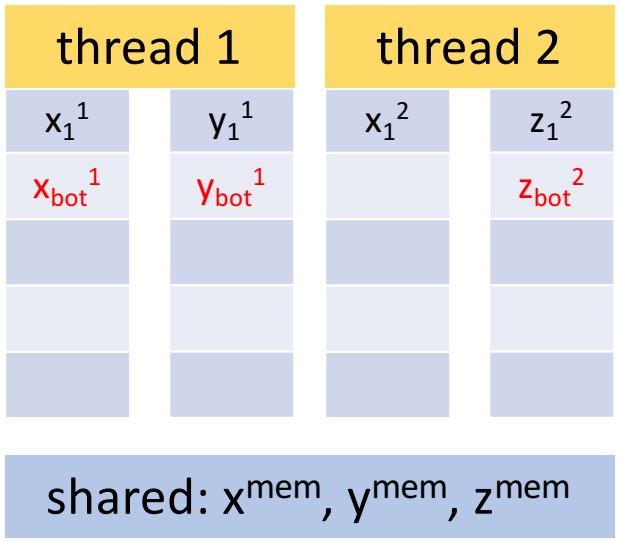
$$\alpha_{sum} : \mathscr{D} \rightarrow \mathscr{D}^{\natural}$$

∞ solved

cost: loosing precision

$$\gamma_{sum} : \mathscr{D}^{\natural} \rightarrow \mathscr{D}$$

Abstraction: partial buffer state information



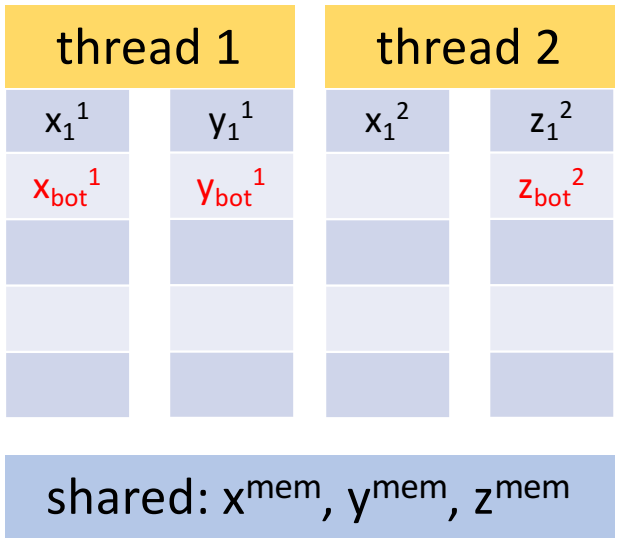
$$\mathscr{B}^\flat \triangleq Var \times Thread \to \{0; 1; 1+\} \tag{14}$$

$$\delta : \mathscr{S} \to \mathscr{B}^\flat \tag{15}$$

$$\delta(S) \triangleq \lambda(x, T).\begin{cases} 0 & \text{if } N_S(x,T) = 0 \\ 1 & \text{if } N_S(x,T) = 1 \\ 1+ & \text{if } N_S(x,T) > 1 \end{cases} \tag{16}$$

Fig. 5. A partial information on states buffers to partition them

Abstraction: partial buffer state information



$$\gamma_2 : (\mathscr{B}^\flat \to \mathscr{D}^\sharp) \to (\mathscr{B}^\flat \to \mathscr{D}) \tag{22}$$

$$\gamma_2(X^\sharp) \triangleq \lambda b^\flat . \gamma_{sum}(X^\sharp(b^\flat)) \tag{23}$$

$$\gamma : (\mathscr{B}^\flat \to \mathscr{D}^\sharp) \to \mathscr{D} \tag{24}$$

$$\gamma \triangleq \gamma_1 \circ \gamma_2 = \lambda X^\sharp . \left\{ S \in \mathscr{S} \mid S \in \gamma_{sum}(X^\sharp(\delta(S))) \right\} \tag{25}$$

Fig. 8. Summarising the buffers to regain a bounded representation

2 steps:

1) summarize
2) resolve partition

Abstract transformers

$$\forall T \in \mathit{Thread}, \{\!|.|\!\} : (\mathscr{B}^\flat \times \mathscr{D}^\natural) \to \mathcal{P}(\mathscr{B}^\flat \times \mathscr{D}^\natural) \tag{26}$$

$$\{\!|r := x|\!\}^\sharp_T(b^\flat, X^\natural) = \begin{cases} \left\{b^\flat, [\![r := x^{mem}]\!]X^\natural\right\} & \text{if } b^\flat(x^T) = 0 \\ \left\{b^\flat, [\![r := x_1^T]\!]X^\natural\right\} & \text{otherwise} \end{cases} \tag{27}$$

$$\{\!|x := e|\!\}^\sharp_T(b^\flat, X^\natural) = \begin{cases} \left\{b^\flat[x^T := 1], [\![x_1^T := e]\!] \circ [\![\mathit{add}\ x_1^T]\!]X^\natural\right\} & \text{if } b^\flat(x^T) = 0 \\ \left\{b^\flat[x^T := 1+], \right. & \\ \left. [\![x_1^T := e]\!] \circ [\![x_{bot}^T := x_1^T]\!] \circ [\![\mathit{add}\ x_{bot}^T]\!]X^\natural\right\} & \text{if } b^\flat(x^T) = 1 \\ \left\{b^\flat, [\![x_1^T := e]\!] \circ [\![\mathit{fold}\ x_{bot}^T, x_2^{temp}]\!]\right. & \\ \left. \quad \circ [\![x_2^{temp} := x_1^T]\!] \circ [\![\mathit{add}\ x_2^{temp}]\!]X^\natural\right\} & \text{if } b^\flat(x^T) = 1+ \end{cases} \tag{28}$$

$$\{\!|\texttt{mfence}|\!\}^\sharp_T(b^\flat, X^\natural) = \begin{cases} \left\{b^\flat, X^\natural\right\} & \text{if } \forall x \in \mathit{Var}, b^\flat(x_T) = 0 \\ \emptyset & \text{otherwise} \end{cases} \tag{29}$$

$$\{\!|\text{flush } x|\!\}^\sharp_T(b^\flat, X^\natural) = \begin{cases} \emptyset & \text{if } b^\flat(x^T) = 0 \\ \left\{b^\flat[x^T := 0], [\![\mathit{drop}\ x_1^T]\!] \circ [\![x^{mem} := x_1^T]\!]X^\natural\right\} & \text{if } b^\flat(x^T) = 1 \\ \left\{\begin{array}{r} b^\flat, [\![\mathit{drop}\ x^{temp}]\!] \circ [\![x^{mem} := x^{temp}]\!] \\ \circ [\![\mathit{expand}\ x_{bot}^T, x^{temp}]\!]X^\natural; \\ b^\flat[x^T := 1], [\![\mathit{drop}\ x_{bot}^T]\!] \circ [\![x^{mem} := x_{bot}^T]\!]X^\natural \end{array}\right\} & \text{if } b^\flat(x^T) = 1+ \end{cases} \tag{30}$$

$$\forall T \in \mathit{Thread}, [\![.]\!]^\sharp_T : (\mathscr{B}^\flat \to \mathscr{D}^\natural) \to (\mathscr{B}^\flat \to \mathscr{D}^\natural) \tag{31}$$

$$[\![ins]\!]^\sharp_T X^\sharp = \lambda b^\flat. \bigcup_{\substack{\exists b_1^\flat \in \mathscr{B}^\flat, \\ (b^\flat, X^\natural) \in \{\!|ins|\!\}^\sharp_T(b_1^\flat, X^\sharp(b_1^\flat))}}^\natural X^\natural \tag{32}$$

Fig. 9. Abstract semantics with summarisation

Abstract transformers on partitions {.}

$$\forall T \in \mathit{Thread}, \{\!|.|\!\} : (\mathscr{B}^\flat \times \mathscr{D}^\natural) \to \mathcal{P}(\mathscr{B}^\flat \times \mathscr{D}^\natural)$$

$$\{\!|r := x|\!\}^\sharp_T(b^\flat, X^\natural) = \begin{cases} \{b^\flat, [\![r := x^{mem}]\!] X^\natural\} & \text{if } b^\flat(x^T) = 0 \\ \{b^\flat, [\![r := x_1^T]\!] X^\natural\} & \text{otherwise} \end{cases} \tag{27}$$

Abstract transformers on partitions {.}

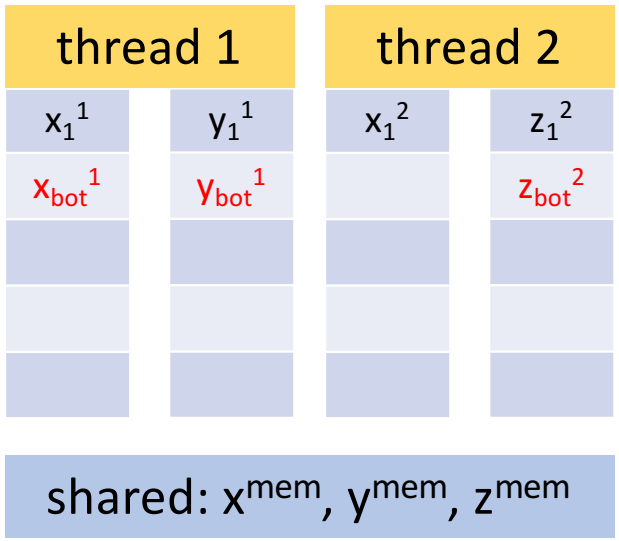
$$\{\!|x := e|\!\}^{\sharp}_{T}(b^{\flat}, X^{\natural}) = \begin{cases} \left\{ b^{\flat}[x^T := 1], [\![x_1^T := e]\!] \circ [\![add\ x_1^T]\!] X^{\natural} \right\} & \text{if } b^{\flat}(x^T) = 0 \\ \left\{ b^{\flat}[x^T := 1+], \right. \\ \left. [\![x_1^T := e]\!] \circ [\![x_{bot}^T := x_1^T]\!] \circ [\![add\ x_{bot}^T]\!] X^{\natural} \right\} & \text{if } b^{\flat}(x^T) = 1 \\ \left\{ b^{\flat}, [\![x_1^T := e]\!] \circ [\![fold\ x_{bot}^T, x_2^{temp}]\!] \right. \\ \quad \left. \circ [\![x_2^{temp} := x_1^T]\!] \circ [\![add\ x_2^{temp}]\!] X^{\natural} \right\} & \text{if } b^{\flat}(x^T) = 1+ \end{cases} \tag{28}$$

Abstract transformers [[.]] using the {.}

$$\forall T \in Thread, [\![.]\!]^\sharp_T : (\mathscr{B}^\flat \to \mathscr{D}^\natural) \to (\mathscr{B}^\flat \to \mathscr{D}^\natural)$$

$$[\![ins]\!]^\sharp_T X^\sharp = \lambda b^\flat. \bigcup_{\substack{\exists b_1^\flat \in \mathscr{B}^\flat, \\ (b^\flat, X^\natural) \in \{\!|ins|\!\}^\sharp_T (b_1^\flat, X^\sharp(b_1^\flat))}}^{\natural} X^\natural$$

Abstraction: partial buffer state information



$$\gamma_2 : (\mathscr{B}^\flat \to \mathscr{D}^\sharp) \to (\mathscr{B}^\flat \to \mathscr{D}) \tag{22}$$

$$\gamma_2(X^\sharp) \triangleq \lambda b^\flat . \gamma_{sum}(X^\sharp(b^\flat)) \tag{23}$$

$$\gamma : (\mathscr{B}^\flat \to \mathscr{D}^\sharp) \to \mathscr{D} \tag{24}$$

$$\gamma \triangleq \gamma_1 \circ \gamma_2 = \lambda X^\sharp . \left\{ S \in \mathscr{S} \mid S \in \gamma_{sum}(X^\sharp(\delta(S))) \right\} \tag{25}$$

Fig. 8. Summarising the buffers to regain a bounded representation

2 steps:

1) summarize
2) resolve partition

My own code example

```
// condition to test @ label
{@ (0:end, 1:end) 0:ry0 <= 0:rx0 && 1:ry1 <= 1:rx1 }

// precondition
x0 = 0, y0 = 0, x1 = 0, y1 = 0, rx0 = 0, ry0 = 0, rx1 = 0, ry1 = 0

### thread T0 ###

x0 := 1
y0 := 1
x0 := 2
ry0 := y1
rx0 := x1
label1 end
```

Result

```
Running test ps_simple
Domain oct, 0 steps before widening
Property 1 could not be verified (wrong, or domain too imprecise).
Time 4.677846
```

```
Running test ps_simple
Domain polka, 0 steps before widening
Property 1 could not be verified (wrong, or domain too imprecise).
Time 0.892813
```

PSO

My own code example with fences

```
// condition to test @ label
{@ (0:end, 1:end) 0:ry0 <= 0:rx0 && 1:ry1 <= 1:rx1 }

// precondition
x0 = 0, y0 = 0, x1 = 0, y1 = 0, rx0 = 0, ry0 = 0, rx1 = 0, ry1 = 0

### thread T0 ###

x0 := 1
mfence
y0 := 1
mfence
x0 := 2
mfence
ry0 := y1
rx0 := x1
label end
```

Result with fences

```
Running test ps_fences
Domain oct, 0 steps before widening
Property 1 verified.
Time 0.203982
```

```
Running test ps_fences
Domain polka, 0 steps before widening
Property 1 verified.
Time 0.050472
```

Code example from paper

```
/* Property to check: At labels (bp0; bp1), tail < h1 */
                        int head;

     /* ENQUEUE */          |    /* DEQUEUE */
     int h1;                |    int tail, h2;
                            |
     while true {           |    tail = head;
         h1 = head;         |    while true {
         bp0:               |        h2 = head;
         h1 = h1 + 1;       |        while (tail >= h2) {
         head = h1;         |            h2 = head;
     }                      |        }
                            |        bp1:
                            |        tail = tail + 1;
                            |    }
```

```
Running test queue
Domain oct, 1 steps before widening
Property 1 verified.
Time 0.089992
```

Benchmark

Algorithm	Domain	Fences	Time	Mem	Domain	Fences	Time	Mem
Abp	Oct	-	-	-	Bdd+Oct	0	0.3	32
	Poly	-	-	-	Bdd+Poly	0	0.3	32
	AGT	0	6	167				
Bakery	Oct	-	-	-	Bdd+Oct	-	-	-
	Poly	-	-	-	Bdd+Poly	-	-	-
	AGT	4	3429	10951				
Concloop	Oct	2	0.19	38	Bdd+Oct	2	0.29	34
	Poly	2	0.24	37	Bdd+Poly	2	0.29	34
	AGT	2	6	504				
Dekker	Oct	4	23	52	Bdd+Oct	4	62	42
	Poly	4	22	50	Bdd+Poly	4	66	43
	AGT	4	121	1580				
Kessel	Oct	-	-	-	Bdd+Oct	4	4	33
	Poly	-	-	-	Bdd+Poly	4	4	34
	AGT	4	6	198				
Loop2 TLM	Oct	-	-	-	Bdd+Oct	**0**	4.3	34
	Poly	-	-	-	Bdd+Poly	**0**	4.2	34
	AGT	2	36	1650				
Peterson	Oct	4	1.53	39	Bdd+Oct	4	2.77	32
	Poly	4	1.53	39	Bdd+Poly	4	2.94	33
	AGT	4	20	901				
Queue	Oct	**0**	0.15	36.9	Bdd+Oct	**0**	0.70	34.3
	Poly	1	0.2	34.7	Bdd+Poly	**0**	0.31	33.3
	AGT	1	1	108				

Fig. 12. Experimental results. Times in sec, Mem in MB.

Benchmark

Algorithm	Domain	Fences	Time	Mem	Domain	Fences	Time	Mem
Abp	Oct	-	-	-	Bdd+Oct	0	0.3	32
	Poly	-	-	-	Bdd+Poly	0	0.3	32
	AGT	0	6	167				
Bakery	Oct	-	-	-	Bdd+Oct	-	-	-
	Poly	-	-	-	Bdd+Poly	-	-	-
	AGT	4	3429	10951				
Concloop	Oct	2	0.19	38	Bdd+Oct	2	0.29	34
	Poly	2	0.24	37	Bdd+Poly	2	0.29	34
	AGT	2	6	504				
Dekker	Oct	4	23	52	Bdd+Oct	4	62	42
	Poly	4	22	50	Bdd+Poly	4	66	43
	AGT	4	121	1580				
Kessel	Oct	-	-	-	Bdd+Oct	4	4	33
	Poly	-	-	-	Bdd+Poly	4	4	34
	AGT	4	6	198				
Loop2 TLM	Oct	-	-	-	Bdd+Oct	**0**	4.3	34
	Poly	-	-	-	Bdd+Poly	**0**	4.2	34
	AGT	2	36	1650				
Peterson	Oct	4	1.53	39	Bdd+Oct	4	2.77	32
	Poly	4	1.53	39	Bdd+Poly	4	2.94	33
	AGT	4	20	901				
Queue	Oct	**0**	0.15	36.9	Bdd+Oct	**0**	0.70	34.3
	Poly	1	0.2	34.7	Bdd+Poly	**0**	0.31	33.3
	AGT	1	1	108				

Fig. 12. Experimental results. Times in sec, Mem in MB.

Benchmark

Algorithm	Domain	Fences	Time	Mem	Domain	Fences	Time	Mem
Abp	Oct	-	-	-	Bdd+Oct	0	0.3	32
	Poly	-	-	-	Bdd+Poly	0	0.3	32
	AGT	0	6	167				
Bakery	Oct	-	-	-	Bdd+Oct	-	-	-
	Poly	-	-	-	Bdd+Poly	-	-	-
	AGT	4	3429	10951				
Concloop	Oct	2	0.19	38	Bdd+Oct	2	0.29	34
	Poly	2	0.24	37	Bdd+Poly	2	0.29	34
	AGT	2	6	504				
Dekker	Oct	4	23	52	Bdd+Oct	4	62	42
	Poly	4	22	50	Bdd+Poly	4	66	43
	AGT	4	121	1580				
Kessel	Oct	-	-	-	Bdd+Oct	4	4	33
	Poly	-	-	-	Bdd+Poly	4	4	34
	AGT	4	6	198				
Loop2 TLM	Oct	-	-	-	Bdd+Oct	**0**	4.3	34
	Poly	-	-	-	Bdd+Poly	**0**	4.2	34
	AGT	2	36	1650				
Peterson	Oct	4	1.53	39	Bdd+Oct	4	2.77	32
	Poly	4	1.53	39	Bdd+Poly	4	2.94	33
	AGT	4	20	901				
Queue	Oct	**0**	0.15	36.9	Bdd+Oct	**0**	0.70	34.3
	Poly	1	0.2	34.7	Bdd+Poly	**0**	0.31	33.3
	AGT	1	1	108				

Fig. 12. Experimental results. Times in sec, Mem in MB.

Benchmark

Algorithm	Domain	Fences	Time	Mem	Domain	Fences	Time	Mem
Abp	Oct	-	-	-	Bdd+Oct	0	0.3	32
	Poly	-	-	-	Bdd+Poly	0	0.3	32
	AGT	0	6	167				
Bakery	Oct	-	-	-	Bdd+Oct	-	-	-
	Poly	-	-	-	Bdd+Poly	-	-	-
	AGT	4	3429	10951				
Concloop	Oct	2	0.19	38	Bdd+Oct	2	0.29	34
	Poly	2	0.24	37	Bdd+Poly	2	0.29	34
	AGT	2	6	504				
Dekker	Oct	4	23	52	Bdd+Oct	4	62	42
	Poly	4	22	50	Bdd+Poly	4	66	43
	AGT	4	121	1580				
Kessel	Oct	-	-	-	Bdd+Oct	4	4	33
	Poly	-	-	-	Bdd+Poly	4	4	34
	AGT	4	6	198				
Loop2 TLM	Oct	-	-	-	Bdd+Oct	**0**	4.3	34
	Poly	-	-	-	Bdd+Poly	**0**	4.2	34
	AGT	2	36	1650				
Peterson	Oct	4	1.53	39	Bdd+Oct	4	2.77	32
	Poly	4	1.53	39	Bdd+Poly	4	2.94	33
	AGT	4	20	901				
Queue	Oct	**0**	0.15	36.9	Bdd+Oct	**0**	0.70	34.3
	Poly	1	0.2	34.7	Bdd+Poly	**0**	0.31	33.3
	AGT	1	1	108				

Fig. 12. Experimental results. Times in sec, Mem in MB.

Benchmark

Algorithm	Domain	Fences	Time	Mem	Domain	Fences	Time	Mem
Abp	Oct	-	-	-	Bdd+Oct	0	0.3	32
	Poly	-	-	-	Bdd+Poly	0	0.3	32
	AGT	0	6	167				
Bakery	Oct	-	-	-	Bdd+Oct	-	-	-
	Poly	-	-	-	Bdd+Poly	-	-	-
	AGT	4	3429	10951				
Concloop	Oct	2	0.19	38	Bdd+Oct	2	0.29	34
	Poly	2	0.24	37	Bdd+Poly	2	0.29	34
	AGT	2	6	504				
Dekker	Oct	4	23	52	Bdd+Oct	4	62	42
	Poly	4	22	50	Bdd+Poly	4	66	43
	AGT	4	121	1580				
Kessel	Oct	-	-	-	Bdd+Oct	4	4	33
	Poly	-	-	-	Bdd+Poly	4	4	34
	AGT	4	6	198				
Loop2 TLM	Oct	-	-	-	Bdd+Oct	**0**	4.3	34
	Poly	-	-	-	Bdd+Poly	**0**	4.2	34
	AGT	2	36	1650				
Peterson	Oct	4	1.53	39	Bdd+Oct	4	2.77	32
	Poly	4	1.53	39	Bdd+Poly	4	2.94	33
	AGT	4	20	901				
Queue	Oct	**0**	0.15	36.9	Bdd+Oct	**0**	0.70	34.3
	Poly	1	0.2	34.7	Bdd+Poly	**0**	0.31	33.3
	AGT	1	1	108				

Fig. 12. Experimental results. Times in sec, Mem in MB.

Discussion

- Good things
- Limitations
- Suggested improvements

Acknowledgment

- Thibault Suzanne for the VM with the working analyzer
- Andrei Dan for interesting discussion