

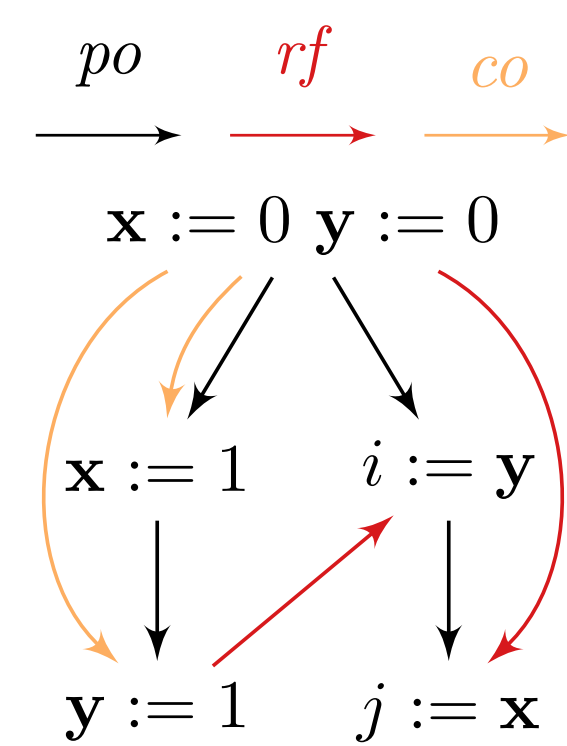
## EXAMPLE

**x** := 0, **y** := 0

**x** := 1 | *i* := **y**  
**y** := 1 | *j* := **x**

$\neg(i = 1 \wedge j = 0)$

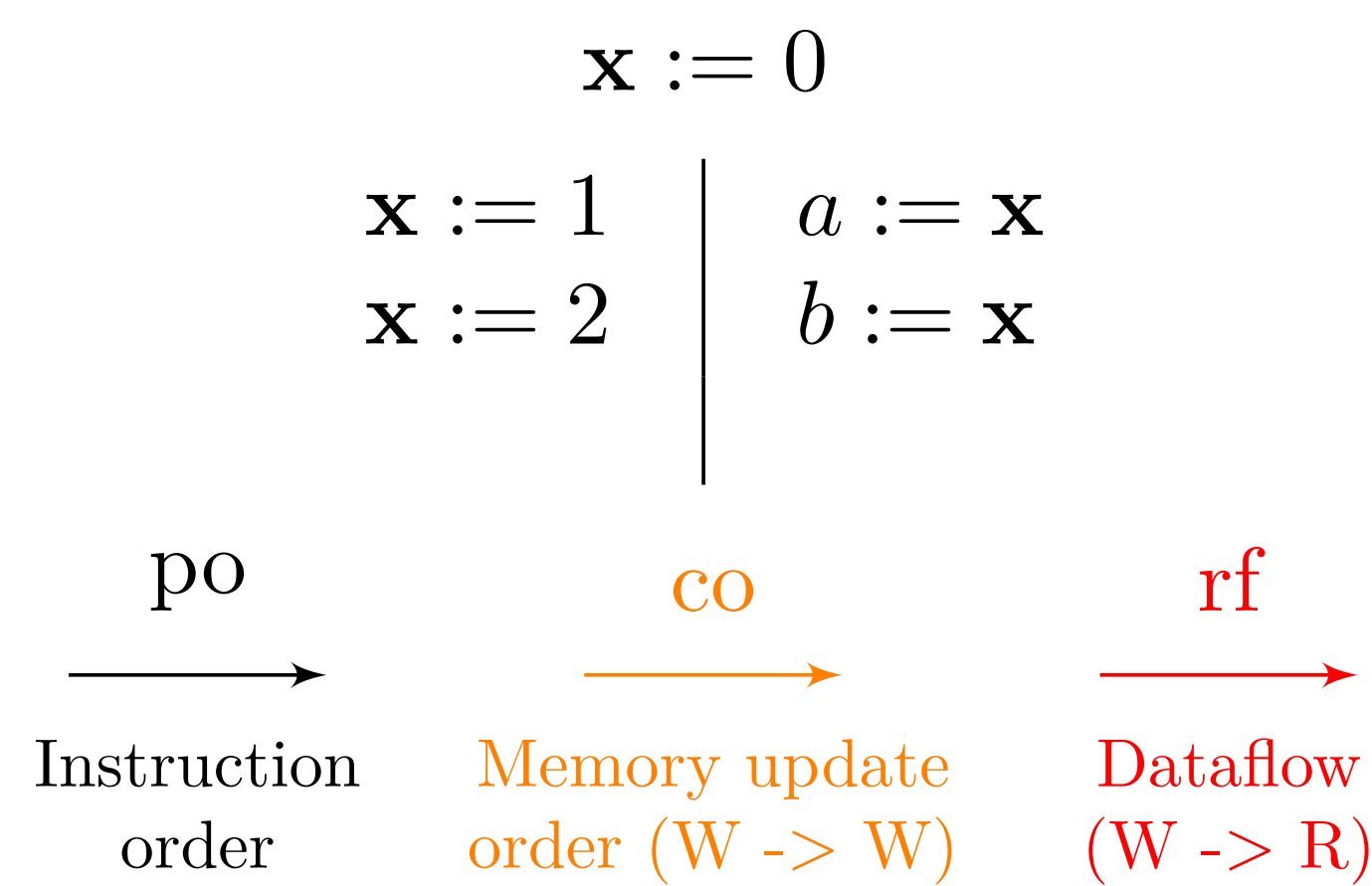
Program with property



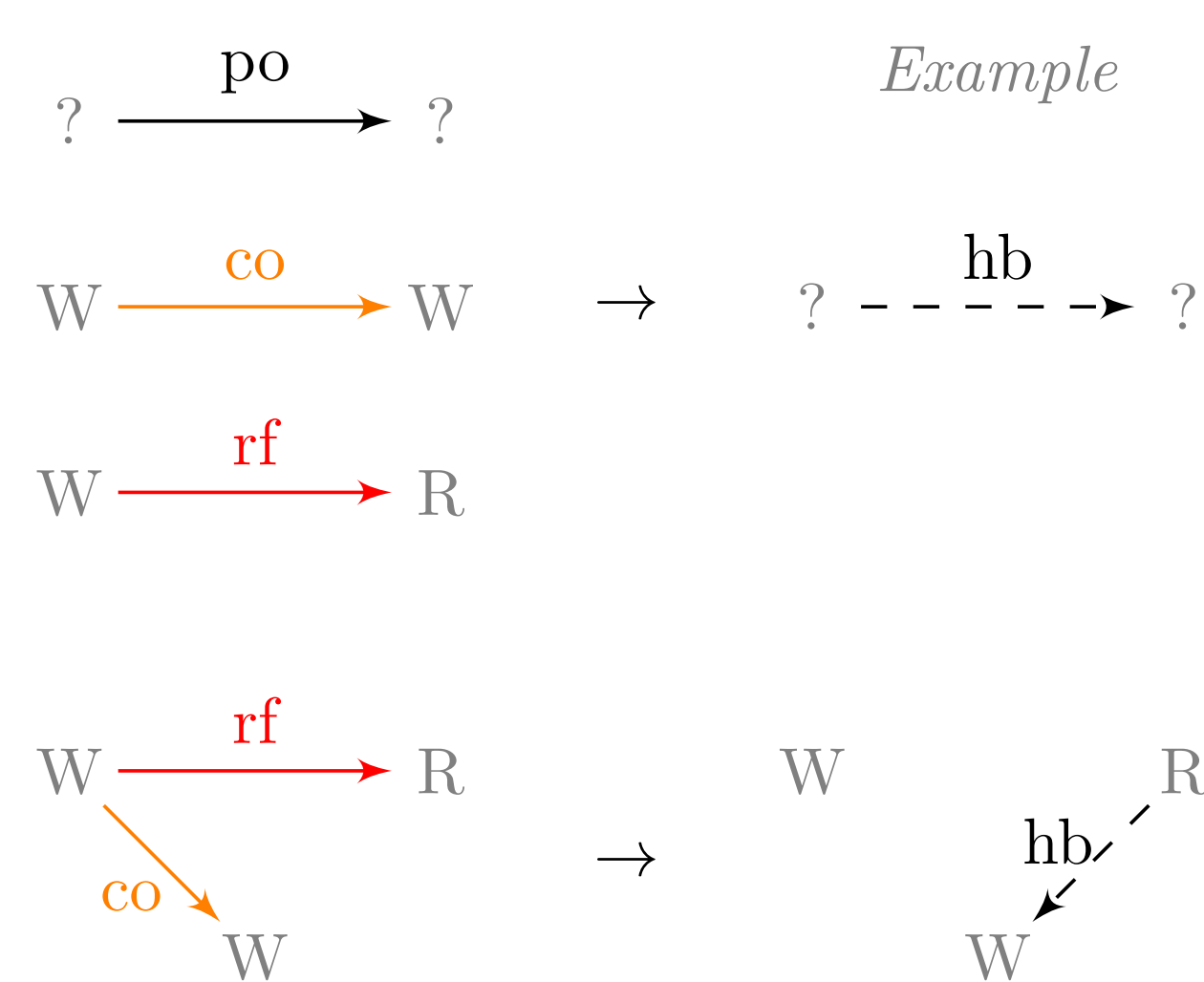
CEx. candidate

**Bold** variables are global, *italicized* variables are local.  
The program is safe under SC and TSO but not PSO.

## MEMORY MODELS OVERVIEW



$\forall r^x \exists w^x : w^x \xrightarrow{rf} r^x$   
 $\forall w_1^x, w_2^x : w_1^x \xrightarrow{co} w_2^x \vee w_2^x \xrightarrow{co} w_1^x$   
...



Find *co* and *rf* for a given *po* such that *hb* is acyclic.

## TOOLS FOR WEAK MEMORY

### Exhaustive Enumeration

Generate execution candidates, and check their consistency

**Herd7** [2]

(memory model simulator)  
Litmus tests CAT  
memory model

### Stateless Model Checking

Generate increasingly larger, always consistent executions (traces)

**GenMC** [5], **Nidhugg** [1],

...  
(Subset of) C11  
Custom library

### Bounded Model Checking

Encode constraints of the memory model in the SMT query

**Dartagnan** [4]

(SV-COMP flavored) C  
Subset of CAT

## VIOLATION WITNESS EXAMPLE

Thread 0	waypoint type	value	line	column
	assume	$\backslash at(\mathbf{x}, 0) = 0$	0	<i>middle</i>
	assume	$\backslash at(\mathbf{y}, 0) = 0$	0	<i>end</i>
	thread_start	1, 2	1	0
Thread 1				
	assume	$\backslash at(\mathbf{x}, 1) = 1$	1	<i>end</i>
	assume	$\backslash at(\mathbf{y}, 1) = 1$	2	<i>end</i>
Thread 2				
	assume	$i = \backslash at(\mathbf{x}, 1)$	1	<i>end</i>
	assume	$j = \backslash at(\mathbf{y}, 1)$	2	<i>end</i>
	target	-	2	<i>end</i>

A violation witness, encoding a violation under PSO

## CORRECTNESS WITNESS EXAMPLE

invariant type	value	line	column
location	$\backslash at(\mathbf{x}, 0) = 0$	0	<i>middle</i>
location	$\backslash at(\mathbf{y}, 0) = 0$	0	<i>end</i>
location	$\backslash at(\mathbf{x}, 1) = 1$	1 ( <i>left</i> )	<i>end</i>
location	$\backslash at(\mathbf{y}, 1) = 1$	2 ( <i>left</i> )	<i>end</i>
location	$\exists a : a \in \{0, 1\}$ $i = \backslash at(\mathbf{x}, a)$	1 ( <i>right</i> )	<i>end</i>
location	$\exists a, b : a, b \in \{0, 1\}$ $j = \backslash at(\mathbf{y}, a)$ $i = \backslash at(\mathbf{x}, b)$ $b = 1 \implies a = 1$	2 ( <i>right</i> )	<i>end</i>
location	$\neg(i = 1 \wedge j = 0)$	2 ( <i>right</i> )	<i>end</i>

A correctness witness, encoding a proof over SC

## MAPPING VERDICTS TO WITNESSES

$\backslash at(\mathbf{e}, \mathbf{id})$ : Built-in ACSL construct (*abused a bit*)

- referring to the value of the expression **e** in the state at label **id** [3]
- Our *state labels* are integers, and denote ordering of memory events.
- Correctness: *state labels* are **symbolic** integers, and denote ordering of memory events.

## FUTURE PLANS

- Implement witness serialization (THETA, CPACHECKER)
- Implement violation witness checking (THETA)
- Implement correctness witness checking (THETA)



## REFERENCES

- [1] Agarwal, P., Chatterjee, K., Pathak, S., Pavlogiannis, A., Toman, V.: Stateless Model Checking Under a Reads-Value-From Equivalence. In: Silva, A., Leino, K.R.M. (eds.) Computer Aided Verification. pp. 341–366. Springer International Publishing, Cham (2021)
- [2] Alglave, J., Maranget, L., Tautschnig, M.: Herding Cats: Modelling, Simulation, Testing, and Data Mining for Weak Memory. ACM Trans. Program. Lang. Syst. **36**(2) (jul 2014). <https://doi.org/10.1145/2627752>
- [3] Baudin, P., Cuoq, P., Filliatre, J.C., Marché, C., Monate, B., Moy, Y., Prevosto, V.: ACSL: ANSI/ISO C Specification Language v1.20. Tech. rep., Frama-C (2024)
- [4] Gavrilenco, N., Ponce-de León, H., Furbach, F., Heljanko, K., Meyer, R.: BMC for Weak Memory Models: Relation Analysis for Compact SMT Encodings. In: Dillig, I., Tasiran, S. (eds.) Computer Aided Verification. pp. 355–365. Springer International Publishing, Cham (2019)
- [5] Kokologiannakis, M., Vafeiadis, V.: GenMC: A Model Checker for Weak Memory Models. In: Computer Aided Verification: 33rd International Conference, CAV 2021, Virtual Event, July 2023, 2021, Proceedings, Part I. p. 427440. Springer-Verlag, Berlin, Heidelberg (2021). [https://doi.org/10.1007/978-3-030-81685-8\\_20](https://doi.org/10.1007/978-3-030-81685-8_20)

## REPORT

