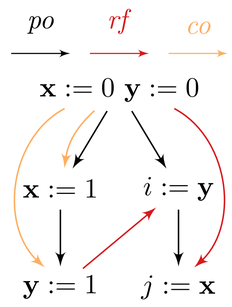
Software Verification Witnesses for Weak Memory

Levente Bajczi
https://leventebajczi.com

EXAMPLE

$$\mathbf{x} := 0, \mathbf{y} := 0$$
$$\begin{array}{l|l} \mathbf{x} := 1 & i := \mathbf{y} \\ \mathbf{y} := 1 & j := \mathbf{x} \end{array}$$
$$\neg(i = 1 \wedge j = 0)$$

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

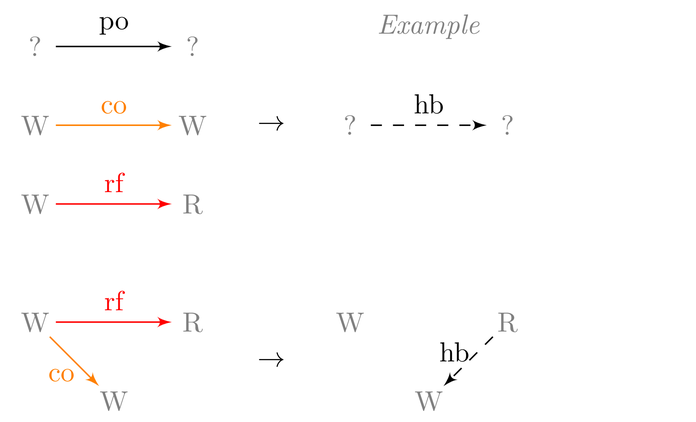
$$\mathbf{x} := 0$$
$$\begin{array}{l|l} \mathbf{x} := 1 & a := \mathbf{x} \\ \mathbf{x} := 2 & b := \mathbf{x} \end{array}$$

po — Instruction order

co — Memory update order (W -> W)

rf — Dataflow (W -> R)

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



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	*middle*
	assume	$\backslash at(\mathbf{y}, 0) = 0$	0	*end*
	thread_start	1, 2	1	0
Thread 1				
	assume	$\backslash at(\mathbf{x}, 1) = 1$	1	*end*
	assume	$\backslash at(\mathbf{y}, 1) = 1$	2	*end*
Thread 2				
	assume	$i = \backslash at(\mathbf{x}, 1)$	1	*end*
	assume	$j = \backslash at(\mathbf{y}, 1)$	2	*end*
	target	-	2	*end*

A violation witness, encoding a violation under PSO

Correctness Witness Example

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

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] Gavrilenko, 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

Report

This research was partially funded by the ÚNKP-24-3 New National Excellence Program of the Ministry of Innovation and Technology, from the National Research, Development and Innovation Fund of Hungary (grant no. ÚNKP-24-3-BME-213).
The Doctoral Excellence Fellowship Programme (DCEP) is funded by the National Research Development and Innovation Fund of the Ministry of Culture and Innovation and the Budapest University of Technology and Economics, under a grant agreement with the National Research, Development and Innovation Office.