Lecture 17

Context Bounding Checkers II

Zvonimir Rakamarić
University of Utah

Announcements

- Posted homework assignment 5
  - Our last homework assignment
  - Read and review two research papers
  - Due on Apr 6
  - We will discuss these papers in class on Apr 6
- Projects
  - Project updates on Tuesday, Apr 4 in my office
  - Work hard – less than 4 weeks left
- Posted research papers related to today's lecture
- Boot SMACK-v1.7.2 profile in aptlab

Last Time

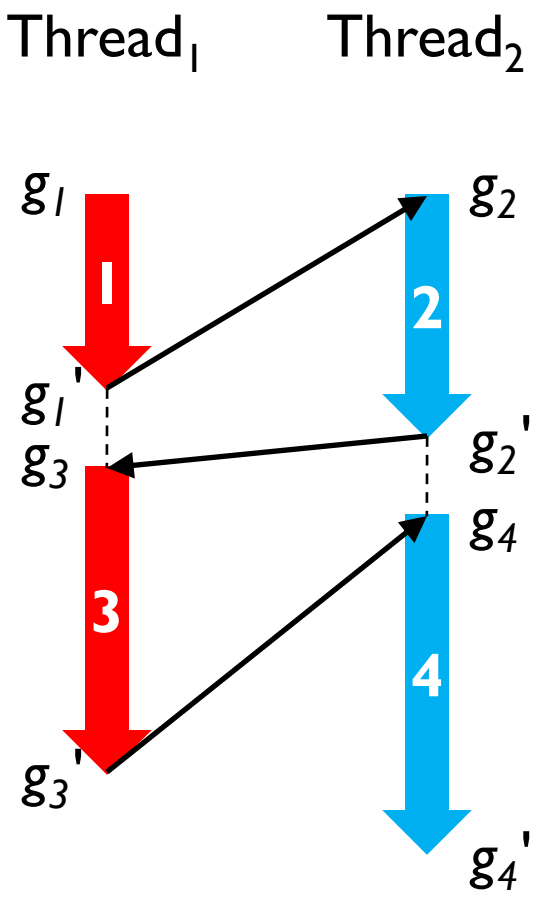
- Context-bounding and its benefits
- CHESS tool for dynamic preemption-bounding

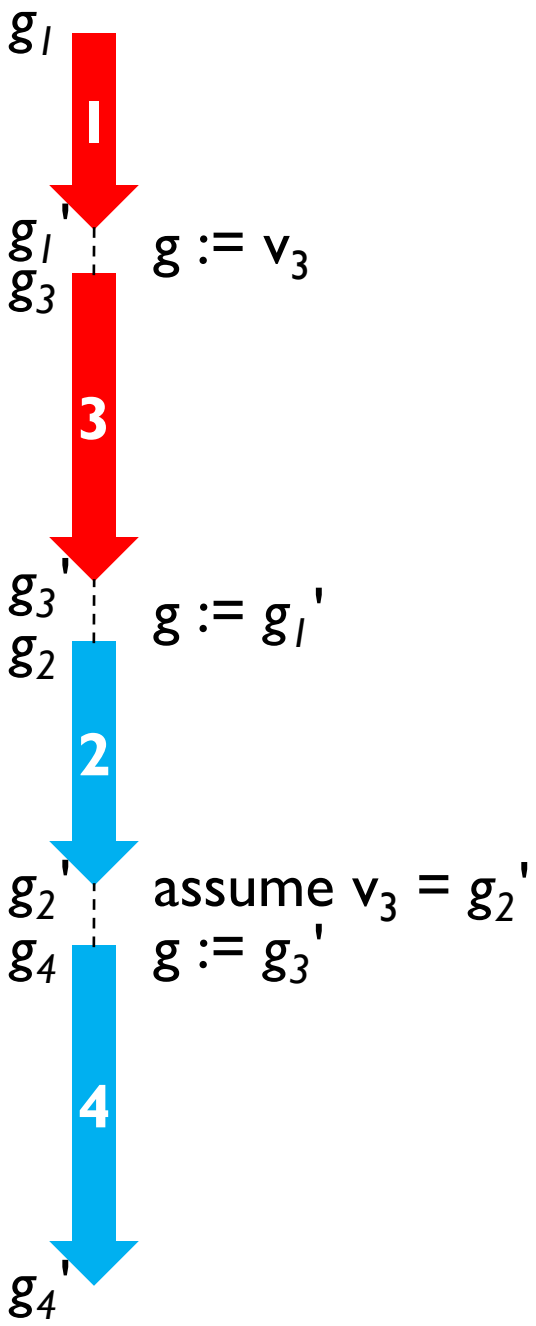
Concurrent Using Sequential

- Transform context bounded analysis of concurrent programs into analysis of sequential programs
- KISS [Qadeer, Wu, PLDI ‘04]
  - Only up to 2 context switches
- [Lal, Reps, CAV ‘08], [La Torre, Madhusudan, Parlato, CAV ‘09]
  - More general transformations, N context switches
  - Applied only on small, manually constructed Boolean programs

Simple Translation Example

- Translation of one concurrent trace
- Two threads: $Thread_1$, $Thread_2$
- One shared variable: g
- 3 context switches, 4 execution segments (or contexts)
- Main idea [Lal, Reps, CAV ’08]
  - Avoid storing local state
  - Introduce unconstrained symbolic “prophecy” values instead of still unavailable “future” values
  - Constrain them when “future” values become available


Thread1
Thread2
g1
g2
1
2
g1'
g3
g2'
g4
3
4
g3'
g4'


g1
1
g1'
g := v3
g3
3
g3'
g := g1'
g2
2
g2'
assume v3 = g2'
g4
g := g3'
4
g4'

Lal-Reps Translation

- N contexts per thread, shared variable g

$T_1 \,||\, T_2$

assert *F*

INIT;

L_1: INIT_K; T_1^s;

L_2: INIT_K; T_2^s;

L_3: END;

assert *F*

k := 1;

int $g_1, g_2, \ldots g_N, v_2, \ldots v_N$;
int k;
assume ($g_2 = v_2$ && $g_3 = v_3$ ... $g_N = v_N$);

st ⇒
ContextSwitch();
if (k == 1) st[g_1/g];
else if (k == 2) st[g_2/g];
…

assume ($g_1 = v_2$ && $g_2 = v_3$ …);

ContextSwitch()
ensures old(k) <= k && k <= N;

Sequentialization Example in Boogie

- Follow Lal-Reps translation and replace TODOs with code segments that are missing

Field Abstraction Example

- Fields = {`f`, `g`}
- Tracked fields = {`f`}

- Before

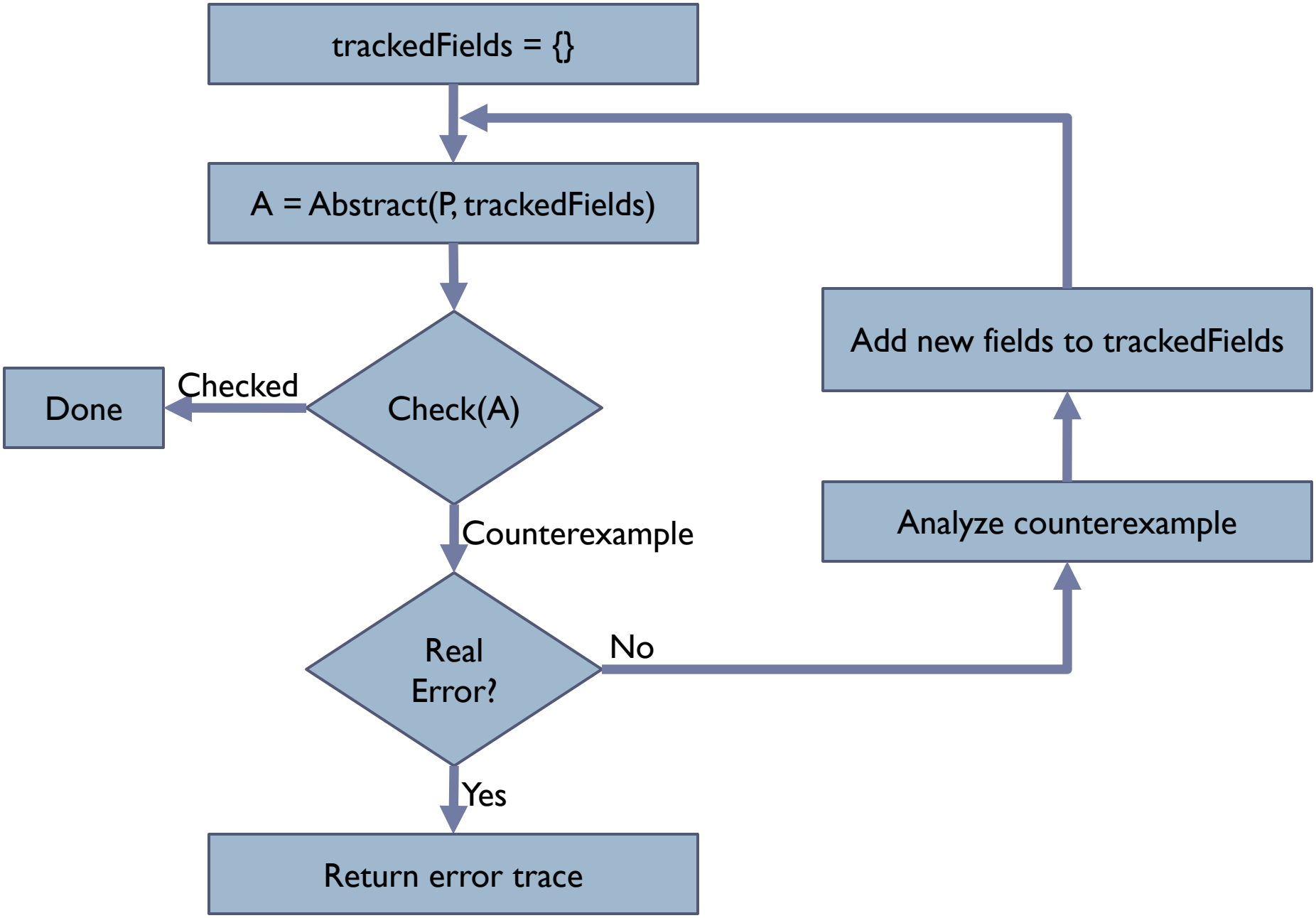
```
tmp = x->f;
tmp = x->g;
y->g = tmp;
```

- Abstraction…

```
tmp = x->f;
tmp = x->get();
y->g = tmp;
```

Field Abstraction CEGAR

- How to discover tracked fields automatically?
- Algorithm based on CounterExample Guided Abstraction Refinement (CEGAR) framework


trackedFields = {}
A = Abstract(P, trackedFields)
Check(A)
Checked
Done
Counterexample
Real Error?
No
Yes
Return error trace
Analyze counterexample
Add new fields to trackedFields

Experimental Results

- Initial prototype implementation: STORM
  - Currently implemented in Corral
- Windows Device Drivers
- Harness
  - Creates driver request that gets processed concurrently by multiple routines
    - Dispatch | Cancellation
    - Dispatch | Cancellation | Completion
    - Dispatch | Cancellation | Completion | DPC
- Checked property
  - Driver request cannot be used after it has been completed (i.e. use after free)

Varying Number of Contexts N

- Manually provided tracked fields

Driver	kLOC	#T	Routine	1	2	3	4	5
usbsamp Bug found!	4	3	read	17.9	37.7	65.8	66.8	85.2
			write	17.8	48.8	52.3	74.3	109.7
			ioctl	4.4	5.0	5.1	5.3	5.4
usbsamp_fix	4	3	read	16.9	28.2	38.6	46.7	47.5
			write	18.1	32.2	46.9	52.5	63.6
			ioctl	4.8	4.7	5.1	5.1	5.2
mqueue	14	4	read	62.1	161.5	236.2	173.0	212.4
			write	48.6	113.4	171.2	177.4	192.3
			ioctl	120.6	198.6	204.7	176.1	199.9
daytona	22	2	ioctl	3.4	3.8	4.2	4.5	5.6
serial	32	3	read	36.5	95.4	103.4	240.5	281.4
			write	37.3	164.3	100.8	233.0	649.8

Field Abstraction CEGAR

- N=2

Driver	Routine	#Fields Total	#TFieds Manual	#TFields CEGAR	#CEGAR Iterations	Time (s)
daytona	ioctl	53	3	3	3	244.3
mqueue	read	72	7	9	9	3446.3
	write			8	8	3010.0
	ioctl			9	9	3635.6
usbsamp_fix	read	113	1	3	3	4382.4
	write			4	4	2079.2
	ioctl			0	0	21.7
serial	read	214	5	5	5	3013.7
	write			4	3	1729.4

Bug Found (usbsamp)

- Sample driver in WinDDK
  - Example of how to write device drivers
    - Copy-pasted by driver vendors
  - Checked using existing tools
- Bug confirmed and fixed
- Requires 3 context switches
  - SLAM (SDV) – checks sequential code
  - KISS – only up to 2 context switches

→ Bug could not be found by other tools

Bug Found

$Thread_1$ Dispatch Routine	$Thread_2$ Cancellation Routine

ReadRoutine(req) {
  ...
  WdfRequestMarkCancelable(
  req, CancelRoutine);
  ...
  WdfRequestComplete(req);
  ...
}
	CancelRoutine(req) {
	  assume (CancelRoutineSet
	  && !reqCompleted);
	  ...
	  GetRequestContext(req);
	  ...
	}