DEPARTMENT OF
COMPUTER
SCIENCE

UNIVERSITY OF
OXFORD

Effective Verification of Low-Level Software with Nested Interrupts

Lihao Liang
University of Oxford

Joint work with Daniel Kroening (Oxford) and
Michael Tautschnig (Queen Mary, London)

FMCAD Student Forum, Portland 2013

Motivation

Motivation

- The interleaving semantics of interrupt-driven programs is subtle

Motivation

- The interleaving semantics of interrupt-driven programs is subtle
- Applying techniques/tools for concurrent software verification is bound to produce false positives

Contribution

- Develop a new symbolic encoding, based on partial orders, that models the semantics of programs with nested interrupts
- Implementation in CBMC
- Preliminary experimental results show that our technique effectively eliminates false positives

Preliminary Results

	LOC	#Int	Error(SC/Pty)	Time(SC/Pty)
qrcu_unsafe.c	112	2	Yes/No	**1.4s**/1.8s
read_write_lock_unsafe.c	34	4	Yes/No	0.2s/0.2s
fib_bench_longer_unsafe.c	33	2	Yes/No	2.5s/**0.3s**
queue_ok_safe.c	128	2	No/No	1m11s/**1m3s**
queue_unsafe.c	140	2	Yes/No	**1m35s**/1m40s
stack_safe.c	98	2	No/No	1m46s/**2.7s**
stack_unsafe.c	99	2	Yes/No	2.7s/**2.6s**
stateful01_unsafe.c	44	2	Yes/No	0.5s/0.5s

- Model interrupts as threads with priorities
- Eliminate counterexamples in a selected set of benchmarks from SV-COMP'13
- Runtime is comparable with CBMC SC (Sequential Consistency)