OpenSMT 2 - Bug #3488

SIGSEGV in LRASolver

06/09/2016 09:48 - Antti Hyvärinen

Status:	Resolved	**Start date:**	06/09/2016
Priority:	Normal	**Due date:**	
Assignee:	Antti Hyvärinen	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

The following stack trace appears when running the example rec.c (attached)

Program received signal SIGSEGV, Segmentation fault.
0x00007ffff7a54750 in LAVar::U (this=0x0) at LAVar.h:284
284 assert(all_bounds[u_bound].delta);
(gdb) bt
#0 0x00007ffff7a54750 in LAVar::U (this=0x0) at LAVar.h:284
#1 0x00007ffff7a66411 in LAVar::isModelOutOfBounds (this=0x0) at LAVar.h:184
#2 0x00007ffff7a59947 in LRASolver::check (this=0x1af86d0, complete=false) at LRASolver.C:458
#3 0x00007ffff7a4a33a in TSolverHandler::check (this=0x1e07420, complete=false) at TSolverHandler.C:80
#4 0x00007ffff7a43652 in THandler::check (this=0x207d0f0, complete=false) at THandler.C:132
#5 0x00007ffff7abd382 in CoreSMTSolver::checkTheory (this=0x1aac0e0, complete=false) at Theory.C:91
#6 0x00007ffff7ab1138 in CoreSMTSolver::search (this=0x1aac0e0, nof_conflicts=100, nof_learnts=29) at CoreSMTSolver.C:1863
#7 0x00007ffff7ab325b in CoreSMTSolver::solve_ (this=0x1aac0e0, max_conflicts=0) at CoreSMTSolver.C:2424
#8 0x00007ffff7aa3717 in SimpSMTSolver::solve_ (this=0x1aac0e0, do_simp=false, turn_off_simp=true) at SimpSMTSolver.C:185
#9 0x00007ffff7b062d2 in SimpSMTSolver::solve (this=0x1aac0e0, assumps=..., do_simp=false, turn_off_simp=true) at ../../src/smtsolvers/SimpSMTSolver.h:263
#10 0x00007ffff7b03553 in Cnfizer::solve (this=0x170ccc8, en_frames=...) at Cnfizer.C:88
#11 0x00007ffff7ad1430 in MainSolver::solve (this=0x170cc90) at MainSolver.C:1090
#12 0x00007ffff7ad127e in MainSolver::check (this=0x170cc90) at MainSolver.C:1069
#13 0x0000000000589ccc in smtcheck_opensmt2t::solve (this=0xeab100) at solvers/smtcheck_opensmt2.cpp:845
#14 0x00000000004625f0 in prop_assertion_sumt::is_satisfiable (this=0x7fffffffc2f0, decider=...) at prop_assertion_sum.cpp:130
#15 0x0000000000462451 in prop_assertion_sumt::assertion_holds (this=0x7fffffffc2f0, assertion=..., ns=..., decider=..., interpolator=...) at prop_assertion_sum.cpp:51
#16 0x00000000004771b4 in summarizing_checkert::assertion_holds (this=0x7fffffffd700, assertion=..., store_summaries_with_assertion=false) at summarizing_checker.cpp:127
#17 0x0000000000455fbe in check_claims (ns=..., leaping_program=..., goto_functions=..., claim_map=..., claim_numbers=..., options=..., _message_handler=..., claim_nr=0) at check_claims.cpp:211
#18 0x000000000044fbff in funfrog_parseoptionst::check_function_summarization (this=0x7ffffffe2b0, ns=..., goto_functions=...) at parseoptions.cpp:562
#19 0x000000000044edeb in funfrog_parseoptionst::doit (this=0x7ffffffe2b0) at parseoptions.cpp:312
#20 0x00000000007c05dc in parseoptions_baset::main (this=0x7ffffffe2b0) at parseoptions.cpp:104
#21 0x00000000048079f in main (argc=2, argv=0x7ffffffea48) at main.cpp:36

History

#1 - 06/09/2016 09:50 - Antti Hyvärinen

When linking HiFrog dev branch to OpenSMT2 that is

#2 - 06/09/2016 23:22 - Karine Even Mendoza

The bug happens also when using the terminal of opensmt (in Z3 it returns SAT, is it the correct result?), with this error:
opensmt: Proof.C:280: void Proof::endChain(CRef): Assertion `clause_to_proof_der.find(res) == clause_to_proof_der.end( )' failed.
Aborted (core dumped)

The code that is sent to the solver is (if it helps):
(set-logic QF_LRA)
(declare-fun |funfrog::?callstart_symbol#4| () Bool)
(declare-fun |funfrog::?callend_symbol#4| () Bool)
(declare-fun |funfrog::?callstart_symbol#3| () Bool)
(declare-fun |funfrog::?callend_symbol#3| () Bool)
(declare-fun |goto_symex::guard#2| () Bool)
(declare-fun |c::f::a!0#3| () Real)
(declare-fun |c::f::a!0#1| () Real)

```
(declare-fun |c::f::$tmp::return_value_f$1!0#2| () Real)
(declare-fun |funfrog::c::f::?retval#2| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#1| () Real)
(declare-fun |c::f::a!0#5| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#3| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#4| () Real)
(declare-fun .oite0 () Real)
(declare-fun |funfrog::c::f::?retval#1| () Real)
(declare-fun |funfrog::?callstart_symbol#2| () Bool)
(declare-fun |funfrog::?callend_symbol#2| () Bool)
(declare-fun |funfrog::?error_symbol#1| () Bool)
(declare-fun |goto_symex::guard#1| () Bool)
(declare-fun |c::main::1::x!0#2| () Real)
(declare-fun |symex::nondet0| () Real)
(declare-fun |c::main::1::y!0#3| () Real)
(declare-fun |c::main::1::y!0#4| () Real)
(declare-fun .oite1 () Real)
(declare-fun |funfrog::?callstart_symbol#1| () Bool)
(declare-fun |funfrog::?callend_symbol#1| () Bool)
(declare-fun |funfrog::?callstart_symbol#5| () Bool)
(declare-fun |funfrog::?callend_symbol#5| () Bool)
(declare-fun |goto_symex::guard#3| () Bool)
(declare-fun |c::f::a!0#7| () Real)
(declare-fun |c::f::a!0#4| () Real)
(declare-fun |c::f::$tmp::return_value_f$1!0#6| () Real)
(declare-fun |funfrog::c::f::?retval#3| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#5| () Real)
(declare-fun |c::f::a!0#9| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#7| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#8| () Real)
(declare-fun .oite2 () Real)
(assert
(and
; XXX Partition: 0
(and (= |c::f::a!0#3| |c::f::a!0#1|) (= |goto_symex::guard#2| (not (<= 10 |c::f::a!0#3|))) (= |c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval#2|) (=
|c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval_tmp#1|) (= |c::f::a!0#3| |c::f::a!0#5|) (= |funfrog::c::f::?retval_tmp#3| (+ (- 10) |c::f::a!0#5|)) (=
|funfrog::c::f::?retval_tmp#4| .oite0) (= |funfrog::c::f::?retval_tmp#4| |funfrog::c::f::?retval#1|) (= (and |funfrog::?callstart_symbol#3|
|goto_symex::guard#2|) |funfrog::?callstart_symbol#4|) (or (not |funfrog::?callend_symbol#3|) (and |funfrog::?callstart_symbol#3| (or
|funfrog::?callend_symbol#4| (not |goto_symex::guard#2|)))))
; XXX Partition: 1
(and (= |c::main::1::x!0#2| |symex::nondet0|) (= |goto_symex::guard#1| (not (<= 0 (* |c::main::1::x!0#2| (- 1))))) (= |c::f::a!0#1| |c::main::1::x!0#2|) (=
|funfrog::c::f::?retval#1| |c::main::1::y!0#3|) (= |c::main::1::y!0#4| .oite1) (= (and |goto_symex::guard#1| (and |funfrog::?callstart_symbol#2| (and (not
(<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (* |c::main::1::x!0#2| (- 1))))))) |funfrog::?callstart_symbol#3|) (= (not (or (not (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))) (<= 0 |c::main::1::y!0#4|))) |funfrog::?error_symbol#1|) (or (not |funfrog::?callend_symbol#2|) (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))))
; XXX Partition: 2
(or |funfrog::?callstart_symbol#1| (not |funfrog::?callend_symbol#1|))
; XXX Partition: 3
(and |funfrog::?error_symbol#1| |funfrog::?callstart_symbol#1| (= |funfrog::?callend_symbol#1| |funfrog::?callstart_symbol#2|))
; XXX Partition: 4
(and (= |goto_symex::guard#2| (not (<= 10 |c::f::a!0#3|))) (= |c::f::a!0#7| |c::f::a!0#4|) (= |c::f::$tmp::return_value_f$1!0#6| |funfrog::c::f::?retval#3|) (=
|c::f::$tmp::return_value_f$1!0#6| |funfrog::c::f::?retval_tmp#5|) (= |c::f::a!0#7| |c::f::a!0#9|) (= |funfrog::c::f::?retval_tmp#7| (+ (- 10) |c::f::a!0#9|)) (=
|funfrog::c::f::?retval_tmp#8| .oite2) (= |funfrog::c::f::?retval#2| |funfrog::c::f::?retval_tmp#8|) (= (and |funfrog::?callstart_symbol#4|
|goto_symex::guard#3|) |funfrog::?callstart_symbol#5|) (or (not |funfrog::?callend_symbol#4|) (and |funfrog::?callstart_symbol#4| (or
|funfrog::?callend_symbol#5| (not |goto_symex::guard#3|)))))
; XXX Partition: 5
(and (= |c::f::a!0#3| |c::f::a!0#1|) (= |goto_symex::guard#2| (not (<= 10 |c::f::a!0#3|))) (= |c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval#2|) (=
|c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval_tmp#1|) (= |c::f::a!0#3| |c::f::a!0#5|) (= |funfrog::c::f::?retval_tmp#3| (+ (- 10) |c::f::a!0#5|)) (=
|funfrog::c::f::?retval_tmp#4| .oite0) (= |funfrog::c::f::?retval_tmp#4| |funfrog::c::f::?retval#1|) (= (and |funfrog::?callstart_symbol#3|
|goto_symex::guard#2|) |funfrog::?callstart_symbol#4|) (or (not |funfrog::?callend_symbol#3|) (and |funfrog::?callstart_symbol#3| (or
|funfrog::?callend_symbol#4| (not |goto_symex::guard#2|)))) (= |c::f::a!0#4| (+ 1 |c::f::a!0#3|)))
; XXX Partition: 6
(and (= |c::main::1::x!0#2| |symex::nondet0|) (= |goto_symex::guard#1| (not (<= 0 (* |c::main::1::x!0#2| (- 1))))) (= |c::f::a!0#1| |c::main::1::x!0#2|) (=
|funfrog::c::f::?retval#1| |c::main::1::y!0#3|) (= |c::main::1::y!0#4| .oite1) (= (and |goto_symex::guard#1| (and |funfrog::?callstart_symbol#2| (and (not
(<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (* |c::main::1::x!0#2| (- 1))))))) |funfrog::?callstart_symbol#3|) (= (not (or (not (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))) (<= 0 |c::main::1::y!0#4|))) |funfrog::?error_symbol#1|) (or (not |funfrog::?callend_symbol#2|) (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))))
; XXX Partition: 7
(or |funfrog::?callstart_symbol#1| (not |funfrog::?callend_symbol#1|))
; XXX Partition: 8
(and |funfrog::?error_symbol#1| |funfrog::?callstart_symbol#1| (= |funfrog::?callend_symbol#1| |funfrog::?callstart_symbol#2|))
```

```
; XXX oite symbol: .oite0
(and (or (not |goto_symex::guard#2|) (= |funfrog::c::f::?retval_tmp#1| .oite0)) (or |goto_symex::guard#2| (= |funfrog::c::f::?retval_tmp#3| .oite0)))
; XXX oite symbol: .oite1
(and (or |goto_symex::guard#1| (= 0 .oite1)) (or (not |goto_symex::guard#1|) (= |c::main::1::y!0#3| .oite1)))
; XXX oite symbol: .oite2
(and (or (not |goto_symex::guard#3|) (= |funfrog::c::f::?retval_tmp#5| .oite2)) (or |goto_symex::guard#3| (= |funfrog::c::f::?retval_tmp#7| .oite2)))
))
(check-sat)
```

#3 - 09/09/2016 09:56 - Karine Even Mendoza

Hi Antti,

There are two claims checked in rec.c, the second one is the one causing the problem and I think it is the same code as before.
I think it is the last input before mainSolver->check(), and here inside somewhere it will get the seg fault, right?

Just in case it is not the same code, here it is:

```
(set-logic QF_LRA)
(declare-fun |funfrog::?callstart_symbol#4| () Bool)
(declare-fun |funfrog::?callend_symbol#4| () Bool)
(declare-fun |funfrog::?callstart_symbol#3| () Bool)
(declare-fun |funfrog::?callend_symbol#3| () Bool)
(declare-fun |goto_symex::guard#2| () Bool)
(declare-fun |c::f::a!0#3| () Real)
(declare-fun |c::f::a!0#1| () Real)
(declare-fun |c::f::$tmp::return_value_f$1!0#2| () Real)
(declare-fun |funfrog::c::f::?retval#2| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#1| () Real)
(declare-fun |c::f::a!0#5| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#3| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#4| () Real)
(declare-fun .oite0 () Real)
(declare-fun |funfrog::c::f::?retval#1| () Real)
(declare-fun |funfrog::?callstart_symbol#2| () Bool)
(declare-fun |funfrog::?callend_symbol#2| () Bool)
(declare-fun |funfrog::?error_symbol#1| () Bool)
(declare-fun |goto_symex::guard#1| () Bool)
(declare-fun |c::main::1::x!0#2| () Real)
(declare-fun |symex::nondet0| () Real)
(declare-fun |c::main::1::y!0#3| () Real)
(declare-fun |c::main::1::y!0#4| () Real)
(declare-fun .oite1 () Real)
(declare-fun |funfrog::?callstart_symbol#1| () Bool)
(declare-fun |funfrog::?callend_symbol#1| () Bool)
(declare-fun |funfrog::?callstart_symbol#5| () Bool)
(declare-fun |funfrog::?callend_symbol#5| () Bool)
(declare-fun |goto_symex::guard#3| () Bool)
(declare-fun |c::f::a!0#7| () Real)
(declare-fun |c::f::a!0#4| () Real)
(declare-fun |c::f::$tmp::return_value_f$1!0#6| () Real)
(declare-fun |funfrog::c::f::?retval#3| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#5| () Real)
(declare-fun |c::f::a!0#9| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#7| () Real)
(declare-fun |funfrog::c::f::?retval_tmp#8| () Real)
(declare-fun .oite2 () Real)
(assert
(and
; XXX Partition: 0
(and (= |c::f::a!0#3| |c::f::a!0#1|) (= |goto_symex::guard#2| (not (<= 10 |c::f::a!0#3|))) (= |c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval#2|) (=
|c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval_tmp#1|) (= |c::f::a!0#3| |c::f::a!0#5|) (= |funfrog::c::f::?retval_tmp#3| (+ (- 10) |c::f::a!0#5|)) (=
|funfrog::c::f::?retval_tmp#4| .oite0) (= |funfrog::c::f::?retval_tmp#4| |funfrog::c::f::?retval#1|) (= (and |funfrog::?callstart_symbol#3|
|goto_symex::guard#2|) |funfrog::?callstart_symbol#4|) (or (not |funfrog::?callend_symbol#3|) (and |funfrog::?callstart_symbol#3| (or
|funfrog::?callend_symbol#4| (not |goto_symex::guard#2|)))))
; XXX Partition: 1
(and (= |c::main::1::x!0#2| |symex::nondet0|) (= |goto_symex::guard#1| (not (<= 0 (* |c::main::1::x!0#2| (- 1))))) (= |c::f::a!0#1| |c::main::1::x!0#2|) (=
|funfrog::c::f::?retval#1| |c::main::1::y!0#3|) (= |c::main::1::y!0#4| .oite1) (= (and |goto_symex::guard#1| (and |funfrog::?callstart_symbol#2| (and (not
(<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (* |c::main::1::x!0#2| (- 1))))))) |funfrog::?callstart_symbol#3|) (= (not (or (not (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))) (<= 0 |c::main::1::y!0#4|))) |funfrog::?error_symbol#1|) (or (not |funfrog::?callend_symbol#2|) (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))))
; XXX Partition: 2
(or |funfrog::?callstart_symbol#1| (not |funfrog::?callend_symbol#1|))
; XXX Partition: 3
```

```
(and |funfrog::?error_symbol#1| |funfrog::?callstart_symbol#1| (= |funfrog::?callend_symbol#1| |funfrog::?callstart_symbol#2|))
; XXX Partition: 4
(and (= |goto_symex::guard#2| (not (<= 10 |c::f::a!0#3|))) (= |c::f::a!0#7| |c::f::a!0#4|) (= |c::f::$tmp::return_value_f$1!0#6| |funfrog::c::f::?retval#3|) (=
|c::f::$tmp::return_value_f$1!0#6| |funfrog::c::f::?retval_tmp#5|) (= |c::f::a!0#7| |c::f::a!0#9|) (= |funfrog::c::f::?retval_tmp#7| (+ (- 10) |c::f::a!0#9|)) (=
|funfrog::c::f::?retval_tmp#8| .oite2) (= |funfrog::c::f::?retval#2| |funfrog::c::f::?retval_tmp#8|) (= (and |funfrog::?callstart_symbol#4|
|goto_symex::guard#3|) |funfrog::?callstart_symbol#5|) (or (not |funfrog::?callend_symbol#4|) (and |funfrog::?callstart_symbol#4| (or
|funfrog::?callend_symbol#5| (not |goto_symex::guard#3|)))))
; XXX Partition: 5
(and (= |c::f::a!0#3| |c::f::a!0#1|) (= |goto_symex::guard#2| (not (<= 10 |c::f::a!0#3|))) (= |c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval#2|) (=
|c::f::$tmp::return_value_f$1!0#2| |funfrog::c::f::?retval_tmp#1|) (= |c::f::a!0#3| |c::f::a!0#5|) (= |funfrog::c::f::?retval_tmp#3| (+ (- 10) |c::f::a!0#5|)) (=
|funfrog::c::f::?retval_tmp#4| .oite0) (= |funfrog::c::f::?retval_tmp#4| |funfrog::c::f::?retval#1|) (= (and |funfrog::?callstart_symbol#3|
|goto_symex::guard#2|) |funfrog::?callstart_symbol#4|) (or (not |funfrog::?callend_symbol#3|) (and |funfrog::?callstart_symbol#3| (or
|funfrog::?callend_symbol#4| (not |goto_symex::guard#2|)))) (= |c::f::a!0#4| (+ 1 |c::f::a!0#3|)))
; XXX Partition: 6
(and (= |c::main::1::x!0#2| |symex::nondet0|) (= |goto_symex::guard#1| (not (<= 0 (* |c::main::1::x!0#2| (- 1))))) (= |c::f::a!0#1| |c::main::1::x!0#2|) (=
|funfrog::c::f::?retval#1| |c::main::1::y!0#3|) (= |c::main::1::y!0#4| .oite1) (= (and |goto_symex::guard#1| (and |funfrog::?callstart_symbol#2| (and (not
(<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (* |c::main::1::x!0#2| (- 1)))))))) |funfrog::?callstart_symbol#3|) (= (not (or (not (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))) (<= 0 |c::main::1::y!0#4|))) |funfrog::?error_symbol#1|) (or (not |funfrog::?callend_symbol#2|) (and (or
|funfrog::?callend_symbol#3| (not |goto_symex::guard#1|)) (and |funfrog::?callstart_symbol#2| (and (not (<= 100 |c::main::1::x!0#2|)) (not (<= (- 8) (*
|c::main::1::x!0#2| (- 1)))))))))
; XXX Partition: 7
(or |funfrog::?callstart_symbol#1| (not |funfrog::?callend_symbol#1|))
; XXX Partition: 8
(and |funfrog::?error_symbol#1| |funfrog::?callstart_symbol#1| (= |funfrog::?callend_symbol#1| |funfrog::?callstart_symbol#2|))
; XXX oite symbol: .oite0
(and (or (not |goto_symex::guard#2|) (= |funfrog::c::f::?retval_tmp#1| .oite0)) (or |goto_symex::guard#2| (= |funfrog::c::f::?retval_tmp#3| .oite0)))
; XXX oite symbol: .oite1
(and (or |goto_symex::guard#1| (= 0 .oite1)) (or (not |goto_symex::guard#1|) (= |c::main::1::y!0#3| .oite1)))
; XXX oite symbol: .oite2
(and (or (not |goto_symex::guard#3|) (= |funfrog::c::f::?retval_tmp#5| .oite2)) (or |goto_symex::guard#3| (= |funfrog::c::f::?retval_tmp#7| .oite2)))
))
(check-sat)
```

#4 - 12/09/2016 13:50 - Antti Hyvärinen

- Status changed from New to Resolved

- % Done changed from 0 to 100

This seems to be fixed now in master, all examples are running as expected.

Files

rec.c	219 Bytes	06/09/2016	Antti Hyvärinen