Ruby master - Bug #4929

test/dl/test_func.rb was crashed on Mac

06/26/2011 03:09 PM - kosaki (Motohiro KOSAKI)

Status:	Closed		
Priority:	Normal		
Assignee:	tenderlovemaking (Aaron Patterson)		
Target version:	1.9.3		
ruby -v:	ruby 1.9.3dev (2011-06-20 trunk 32176) [x86_64-darwin10.7.4]	**Backport:**	

Description

% time make test-all TESTS="-v -q --gc-stress ../test/dl/test_func.rb"

./miniruby -I../lib -I. -I.ext/common ../tool/runruby.rb --extout=.ext -- "../test/runner.rb" --ruby="./miniruby -I../lib -I. -I.ext/common ../tool/runruby.rb --extout=.ext --" -v -q --gc-stress ../test/dl/test_func.rb
Run options: "--ruby=./miniruby -I../lib -I. -I.ext/common ../tool/runruby.rb --extout=.ext --" -v -q --gc-stress

Running tests:

DL::TestBase#test_empty = 0.02 s = .
DL::TestFunc#test_atof = 0.05 s = .
DL::TestFunc#test_empty = 0.01 s = .
DL::TestFunc#test_isdigit = 0.05 s = .
DL::TestFunc#test_name = 0.03 s = .
DL::TestFunc#test_qsort1 = /Users/kosaki/ruby/test/dl/test_func.rb:92: [BUG] Bus Error
ruby 1.9.3dev (2011-06-26 trunk 32230) [x86_64-darwin10.7.4]

-- Control frame information ---
c:0034 p:---- s:0138 b:0138 l:000137 d:000137 CFUNC :initialize
c:0033 p:---- s:0136 b:0136 l:000135 d:000135 CFUNC :new
c:0032 p:0018 s:0132 b:0132 l:001e30 d:000131 LAMBDA /Users/kosaki/ruby/test/dl/test_func.rb:92
c:0031 p:---- s:0128 b:0128 l:000127 d:000127 FINISH
c:0030 p:---- s:0126 b:0126 l:000125 d:000125 CFUNC :call
c:0029 p:0059 s:0119 b:0119 l:000118 d:000118 METHOD /Users/kosaki/ruby/build/.ext/common/dl/func.rb:55
c:0028 p:0161 s:0111 b:0111 l:001e30 d:001e30 METHOD /Users/kosaki/ruby/test/dl/test_func.rb:96
c:0027 p:0063 s:0105 b:0105 l:000440 d:000440 METHOD /Users/kosaki/ruby/lib/minitest/unit.rb:948
c:0026 p:---- s:0099 b:0099 l:000098 d:000098 FINISH
c:0025 p:---- s:0097 b:0097 l:000096 d:000096 CFUNC :call
c:0024 p:0065 s:0093 b:0093 l:000058 d:000092 LAMBDA /Users/kosaki/ruby/lib/test/unit.rb:198
c:0023 p:---- s:0089 b:0089 l:000088 d:000088 FINISH
c:0022 p:0025 s:0087 b:0087 l:000086 d:000086 METHOD /Users/kosaki/ruby/lib/test/unit/testcase.rb:17
c:0021 p:0090 s:0083 b:0083 l:000071 d:000082 BLOCK /Users/kosaki/ruby/lib/minitest/unit.rb:787
c:0020 p:---- s:0077 b:0077 l:000076 d:000076 FINISH
c:0019 p:---- s:0075 b:0075 l:000074 d:000074 CFUNC :map
c:0018 p:0124 s:0072 b:0072 l:000071 d:000071 METHOD /Users/kosaki/ruby/lib/minitest/unit.rb:780
c:0017 p:0020 s:0064 b:0063 l:000053 d:000062 BLOCK /Users/kosaki/ruby/lib/test/unit.rb:570
c:0016 p:---- s:0059 b:0059 l:000058 d:000058 FINISH
c:0015 p:---- s:0057 b:0057 l:000056 d:000056 CFUNC :each
c:0014 p:0053 s:0054 b:0054 l:000053 d:000053 METHOD /Users/kosaki/ruby/lib/test/unit.rb:568
c:0013 p:0189 s:0048 b:0048 l:000047 d:000047 METHOD /Users/kosaki/ruby/lib/minitest/unit.rb:746
c:0012 p:0013 s:0038 b:0038 l:000037 d:000037 METHOD /Users/kosaki/ruby/lib/minitest/unit.rb:909
c:0011 p:0012 s:0035 b:0035 l:000026 d:000034 BLOCK /Users/kosaki/ruby/lib/minitest/unit.rb:896
c:0010 p:---- s:0032 b:0032 l:000031 d:000031 FINISH
c:0009 p:---- s:0030 b:0030 l:000029 d:000029 CFUNC :each
c:0008 p:0068 s:0027 b:0027 l:000026 d:000026 METHOD /Users/kosaki/ruby/lib/minitest/unit.rb:895
c:0007 p:0029 s:0023 b:0023 l:000022 d:000022 METHOD /Users/kosaki/ruby/lib/minitest/unit.rb:884
c:0006 p:0022 s:0019 b:0019 l:000018 d:000018 METHOD /Users/kosaki/ruby/lib/test/unit.rb:21
c:0005 p:0016 s:0015 b:0015 l:000014 d:000014 METHOD /Users/kosaki/ruby/lib/test/unit.rb:635
c:0004 p:0019 s:0012 b:0012 l:000011 d:000011 METHOD /Users/kosaki/ruby/lib/test/unit.rb:639
c:0003 p:0146 s:0008 b:0007 l:0021d8 d:001dc0 EVAL ../test/runner.rb:13
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH

c:0001 p:0000 s:0002 b:0002 l:0021d8 d:0021d8 TOP

-- Ruby level backtrace information --
../test/runner.rb:13:in <main>'
/Users/kosaki/ruby/lib/test/unit.rb:639:inrun'
/Users/kosaki/ruby/lib/test/unit.rb:635:in run'
/Users/kosaki/ruby/lib/test/unit.rb:21:inrun'
/Users/kosaki/ruby/lib/minitest/unit.rb:884:in run'
/Users/kosaki/ruby/lib/minitest/unit.rb:895:in_run'
/Users/kosaki/ruby/lib/minitest/unit.rb:895:in each'
/Users/kosaki/ruby/lib/minitest/unit.rb:896:inblock in _run'
/Users/kosaki/ruby/lib/minitest/unit.rb:909:in run_tests'
/Users/kosaki/ruby/lib/minitest/unit.rb:746:in_run_anything'
/Users/kosaki/ruby/lib/test/unit.rb:568:in _run_suites'
/Users/kosaki/ruby/lib/test/unit.rb:568:ineach'
/Users/kosaki/ruby/lib/test/unit.rb:570:in block in _run_suites'
/Users/kosaki/ruby/lib/minitest/unit.rb:780:in_run_suite'
/Users/kosaki/ruby/lib/minitest/unit.rb:780:in map'
/Users/kosaki/ruby/lib/minitest/unit.rb:787:inblock in _run_suite'
/Users/kosaki/ruby/lib/test/unit/testcase.rb:17:in run'
/Users/kosaki/ruby/lib/test/unit.rb:198:inblock (2 levels) in non_options'
/Users/kosaki/ruby/lib/test/unit.rb:198:in call'
/Users/kosaki/ruby/lib/minitest/unit.rb:948:inrun'
/Users/kosaki/ruby/test/dl/test_func.rb:96:in test_qsort1'
/Users/kosaki/ruby/build/.ext/common/dl/func.rb:55:incall'
/Users/kosaki/ruby/build/.ext/common/dl/func.rb:55:in call'
/Users/kosaki/ruby/test/dl/test_func.rb:92:inblock in test_qsort1'
/Users/kosaki/ruby/test/dl/test_func.rb:92:in new'
/Users/kosaki/ruby/test/dl/test_func.rb:92:ininitialize'

-- C level backtrace information ---

See Crash Report log file under ~/Library/Logs/CrashReporter or
/Library/Logs/CrashReporter, for the more detail of.

-- Other runtime information ---

- Loaded script: ../test/runner.rb

- Loaded features:

  0 enumerator.so
  1 /Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/enc/encdb.bundle
  2 /Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/enc/trans/transdb.bundle
  3 /Users/kosaki/ruby/lib/rubygems/defaults.rb
  4 /Users/kosaki/ruby/lib/tsort.rb
  5 /Users/kosaki/ruby/lib/rubygems/deprecate.rb
  6 /Users/kosaki/ruby/lib/rubygems/dependency_list.rb
  7 /Users/kosaki/ruby/lib/rubygems/path_support.rb
  8 /Users/kosaki/ruby/build/rbconfig.rb
  9 /Users/kosaki/ruby/lib/rubygems/exceptions.rb
  10 /Users/kosaki/ruby/lib/rubygems/custom_require.rb
  11 /Users/kosaki/ruby/lib/rubygems/version.rb
  12 /Users/kosaki/ruby/lib/rubygems/requirement.rb
  13 /Users/kosaki/ruby/lib/rubygems/platform.rb
  14 /Users/kosaki/ruby/lib/rubygems/specification.rb
  15 /Users/kosaki/ruby/lib/rubygems.rb
  16 /Users/kosaki/ruby/lib/optparse.rb
  17 /Users/kosaki/ruby/lib/minitest/unit.rb
  18 /Users/kosaki/ruby/lib/prettyprint.rb
  19 /Users/kosaki/ruby/lib/pp.rb
  20 /Users/kosaki/ruby/lib/test/unit/assertions.rb
  21 /Users/kosaki/ruby/lib/test/unit/testcase.rb
  22 /Users/kosaki/ruby/lib/test/unit.rb
  23 /Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/dl.bundle
  24 /Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/fiddle.bundle
  25 /Users/kosaki/ruby/build/.ext/common/fiddle/function.rb

```
      26 /Users/kosaki/ruby/build/.ext/common/fiddle/closure.rb
      27 /Users/kosaki/ruby/build/.ext/common/fiddle.rb
      28 /Users/kosaki/ruby/build/.ext/common/dl.rb
      29 /Users/kosaki/ruby/lib/open3.rb
      30 /Users/kosaki/ruby/lib/timeout.rb
      31 /Users/kosaki/ruby/test/ruby/envutil.rb
      32 /Users/kosaki/ruby/test/dl/test_base.rb
      33 /Users/kosaki/ruby/lib/thread.rb
      34 /Users/kosaki/ruby/build/.ext/common/dl/callback.rb
      35 /Users/kosaki/ruby/build/.ext/common/dl/stack.rb
      36 /Users/kosaki/ruby/build/.ext/common/dl/value.rb
      37 /Users/kosaki/ruby/build/.ext/common/dl/func.rb
      38 /Users/kosaki/ruby/test/dl/test_func.rb


[NOTE]
You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html

Process:         ruby-trunk [16156]
Path:            /Users/kosaki/ruby/build/ruby-trunk
Identifier:      ruby-trunk
Version:         ??? (???)
Code Type:       X86-64 (Native)
Parent Process:  gnumake [16155]

Date/Time:       2011-06-26 15:04:04.571 +0900
OS Version:      Mac OS X 10.6.7 (10J4138)
Report Version:  6

Exception Type:  EXC_BAD_ACCESS (SIGABRT)
Exception Codes: KERN_PROTECTION_FAILURE at 0x00000001010cffb0
Crashed Thread:  0  Dispatch queue: com.apple.main-thread

Application Specific Information:
abort() called

Thread 0 Crashed:  Dispatch queue: com.apple.main-thread
0   libSystem.B.dylib               0x00007fff885225d6 __kill + 10
1   libSystem.B.dylib               0x00007fff885c2cde abort + 83
2   libruby.1.9.1.dylib             0x0000000010003e29d 0x100003000 + 242333
3   libruby.1.9.1.dylib             0x0000000100106b02 0x100003000 + 1063682
4   libSystem.B.dylib               0x00007fff8853466a _sigtramp + 26
5   ???                             0x00000001010cffb0 0 + 4312596400
6   libruby.1.9.1.dylib             0x0000000010017a5a3 check_funcall + 179 (vm_method.c:358)
7   libruby.1.9.1.dylib             0x0000000100093140 convert_type + 144 (object.c:2045)
8   libruby.1.9.1.dylib             0x0000000100097b91 rb_convert_to_integer + 241 (object.c:2166)
9   dl.bundle                       0x0000000010035b229 rb_dlptr_initialize + 105 (cptr.c:146)
10  libruby.1.9.1.dylib             0x0000000100179ac4 vm_call0 + 612 (vm_eval.c:79)
11  libruby.1.9.1.dylib             0x00000001001807fe rb_funcall2 + 366 (vm_eval.c:652)
12  libruby.1.9.1.dylib             0x00000001000955e3 rb_class_new_instance + 51 (object.c:1628)
13  libruby.1.9.1.dylib             0x00000001001839f3 vm_call_method + 931 (vm_insnhelper.c:404)
14  libruby.1.9.1.dylib             0x0000000100172f7e vm_exec_core + 20270 (insns.def:1012)
15  libruby.1.9.1.dylib             0x0000000100178313 vm_exec + 1459 (vm.c:1180)
16  libruby.1.9.1.dylib             0x0000000010017967d rb_vm_invoke_proc + 877 (vm.c:591)
17  libruby.1.9.1.dylib             0x0000000100179b47 vm_call0 + 743 (vm_insnhelper.c:428)
18  libruby.1.9.1.dylib             0x00000001001807fe rb_funcall2 + 366 (vm_eval.c:652)
19  fiddle.bundle                   0x0000000100364875 callback + 661 (closure.c:101)
20  libffi.dylib                    0x00007fff84f29b07 ffi_closure_unix64_inner + 540
21  libffi.dylib                    0x00007fff84f28fa6 ffi_closure_unix64 + 70
22  libSystem.B.dylib               0x00007fff885d08da _qsort + 439
23  libffi.dylib                    0x00007fff84f28e24 ffi_call_unix64 + 76
24  libffi.dylib                    0x00007fff84f298c7 ffi_call + 803
25  fiddle.bundle                   0x00000001003655a0 function_call + 672 (function.c:127)
26  libruby.1.9.1.dylib             0x00000001001839f3 vm_call_method + 931 (vm_insnhelper.c:404)
27  libruby.1.9.1.dylib             0x000000010017369e vm_exec_core + 22094 (insns.def:1048)
```

```
28  libruby.1.9.1.dylib           0x0000000100178313 vm_exec + 1459 (vm.c:1180)
29  libruby.1.9.1.dylib           0x0000000100179d6a vm_call0 + 1290 (vm_eval.c:66)
30  libruby.1.9.1.dylib           0x00000001000486c9 rb_method_call + 361 (proc.c:1426)
31  libruby.1.9.1.dylib           0x00000001001839f3 vm_call_method + 931 (vm_insnhelper.c:404)
32  libruby.1.9.1.dylib           0x0000000100172f7e vm_exec_core + 20270 (insns.def:1012)
33  libruby.1.9.1.dylib           0x0000000100178313 vm_exec + 1459 (vm.c:1180)
34  libruby.1.9.1.dylib           0x000000010017967d rb_vm_invoke_proc + 877 (vm.c:591)
35  libruby.1.9.1.dylib           0x0000000100183dff vm_call_method + 1967 (vm_insnhelper.c:428)
36  libruby.1.9.1.dylib           0x000000010017369e vm_exec_core + 22094 (insns.def:1048)
37  libruby.1.9.1.dylib           0x0000000100178313 vm_exec + 1459 (vm.c:1180)
38  libruby.1.9.1.dylib           0x0000000100186630 rb_yield + 640 (vm.c:591)
39  libruby.1.9.1.dylib           0x00000001000121b1 rb_ary_collect + 113 (array.c:2220)
40  libruby.1.9.1.dylib           0x00000001001839f3 vm_call_method + 931 (vm_insnhelper.c:404)
41  libruby.1.9.1.dylib           0x0000000100172f7e vm_exec_core + 20270 (insns.def:1012)
42  libruby.1.9.1.dylib           0x0000000100178313 vm_exec + 1459 (vm.c:1180)
43  libruby.1.9.1.dylib           0x0000000100186630 rb_yield + 640 (vm.c:591)
44  libruby.1.9.1.dylib           0x00000001000094fe rb_ary_each + 78 (array.c:1477)
45  libruby.1.9.1.dylib           0x00000001001839f3 vm_call_method + 931 (vm_insnhelper.c:404)
46  libruby.1.9.1.dylib           0x0000000100172f7e vm_exec_core + 20270 (insns.def:1012)
47  libruby.1.9.1.dylib           0x0000000100178313 vm_exec + 1459 (vm.c:1180)
48  libruby.1.9.1.dylib           0x0000000100186630 rb_yield + 640 (vm.c:591)
49  libruby.1.9.1.dylib           0x00000001000094fe rb_ary_each + 78 (array.c:1477)
50  libruby.1.9.1.dylib           0x00000001001839f3 vm_call_method + 931 (vm_insnhelper.c:404)
51  libruby.1.9.1.dylib           0x0000000100172f7e vm_exec_core + 20270 (insns.def:1012)
52  libruby.1.9.1.dylib           0x0000000100178313 vm_exec + 1459 (vm.c:1180)
53  libruby.1.9.1.dylib           0x000000010017860b rb_iseq_eval_main + 507 (vm.c:1422)
54  libruby.1.9.1.dylib           0x00000001000430c2 ruby_exec_internal + 178 (eval.c:201)
55  libruby.1.9.1.dylib           0x0000000100045dec ruby_run_node + 60 (eval.c:248)
56  ruby-trunk                  0x0000000100000ecf main + 79 (main.c:40)
57  ruby-trunk                  0x0000000100000e74 start + 52

Thread 1:
0   libSystem.B.dylib             0x00007fff8850ef8a __semwait_signal + 10
1   libSystem.B.dylib             0x00007fff88512da1 _pthread_cond_wait + 1286
2   libruby.1.9.1.dylib           0x0000000100190256 thread_timer + 198 (thread_pthread.c:295)
3   libSystem.B.dylib             0x00007fff8850d4f6 _pthread_start + 331
4   libSystem.B.dylib             0x00007fff8850d3a9 thread_start + 13

Thread 0 crashed with X86 Thread State (64-bit):
rax: 0x0000000000000000  rbx: 0x000000000000005c  rcx: 0x00007fff5fbfbac8  rdx: 0x0000000000000000
rdi: 0x0000000000003f1c  rsi: 0x0000000000000006  rbp: 0x00007fff5fbfbae0  rsp: 0x00007fff5fbfbac8
r8: 0x00007fff70f2da40   r9: 0x0000000000000000  r10: 0x00007fff8851e616  r11: 0xffffff80002e4730
r12: 0x00007fff5fbfbaf0  r13: 0x00000001001a5a22  r14: 0x0000000010083d550  r15: 0x00007fff5fbfc208
rip: 0x00007fff885225d6  rfl: 0x0000000000000206  cr2: 0x00000001010cffb0

Binary Images:
0x100000000 -       0x100000fff +ruby-trunk ??? (???)  /Users/kosaki/ruby/build/ruby-trunk
0x100003000 -       0x100226ff7 +libruby.1.9.1.dylib 1.9.1 (compatibility 1.9.1)  /Users/kosaki/ruby/build/libruby.1.9.1.dylib
0x10034a000 -       0x10034bfff +encdb.bundle ??? (???)  /Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/enc/encdb.bundle
0x10034e000 -       0x10034ffff +transdb.bundle ??? (???)
/Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/enc/trans/transdb.bundle
0x100353000 -       0x10035dff7 +dl.bundle ??? (???)  /Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/dl.bundle
0x100363000 -       0x100365ff7 +fiddle.bundle ??? (???)  /Users/kosaki/ruby/build/.ext/x86_64-darwin10.7.4/fiddle.bundle
0x7fff5fc00000 -    0x7fff5fc3bdef  dyld 132.1 (???)  /usr/lib/dyld
0x7fff805a7000 -    0x7fff8065dfff  libobjc.A.dylib 227.0.0 (compatibility 1.0.0)  /usr/lib/libobjc.A.dylib
0x7fff84f28000 -    0x7fff84f29fff  libffi.dylib ??? (???)  /usr/lib/libffi.dylib
0x7fff862ec000 -    0x7fff862f0ff7  libmathCommon.A.dylib 315.0.0 (compatibility 1.0.0)  /usr/lib/system/libmathCommon.A.dylib
0x7fff86677000 -    0x7fff866f4fef  libstdc++.6.dylib 7.9.0 (compatibility 7.0.0)  /usr/lib/libstdc++.6.dylib
0x7fff884d3000 -    0x7fff88694fff  libSystem.B.dylib 125.2.10 (compatibility 1.0.0)  /usr/lib/libSystem.B.dylib
0x7fff88789000 -    0x7fff887d5fff  libauto.dylib ??? (???)  /usr/lib/libauto.dylib
0x7fffffe00000 -    0x7fffffe01fff  libSystem.B.dylib ??? (???)  /usr/lib/libSystem.B.dylib
```

Related issues:

Related to Ruby master - Bug #4927: crash on test/coverage/test_coverage.rb	**Closed**	**06/26/2011**

Associated revisions

Revision 9f3914ab - 07/27/2011 05:15 PM - nobu (Nobuyoshi Nakada)

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32712 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32712 - 07/27/2011 05:15 PM - nobu (Nobuyoshi Nakada)

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.

Revision 32712 - 07/27/2011 05:15 PM - nobu (Nobuyoshi Nakada)

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.

Revision 32712 - 07/27/2011 05:15 PM - nobu (Nobuyoshi Nakada)

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.

Revision 32712 - 07/27/2011 05:15 PM - nobu (Nobuyoshi Nakada)

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.

Revision 32712 - 07/27/2011 05:15 PM - nobu (Nobuyoshi Nakada)

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.

Revision 32712 - 07/27/2011 05:15 PM - nobu (Nobuyoshi Nakada)

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.

Revision 60053a0a - 07/28/2011 02:47 PM - nagachika (Tomoyuki Chikanaga)

- ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of xmalloc() to allocate an array for arguments of callback procedure, to prevent arguments from being swept by GC. [ruby-core:38546] [Bug #4929]

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@32725 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 32725 - 07/28/2011 02:47 PM - nagachika (Tomoyuki Chikanaga)

- ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of xmalloc() to allocate an array for arguments of callback procedure, to prevent arguments from being swept by GC. [ruby-core:38546] [Bug #4929]

Revision 32725 - 07/28/2011 02:47 PM - nagachika (Tomoyuki Chikanaga)

- ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of xmalloc() to allocate an array for arguments of callback procedure, to prevent arguments from being swept by GC. [ruby-core:38546] [Bug #4929]

Revision 32725 - 07/28/2011 02:47 PM - nagachika (Tomoyuki Chikanaga)

- ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of xmalloc() to allocate an array for arguments of callback procedure, to prevent arguments from being swept by GC. [ruby-core:38546] [Bug #4929]

Revision 32725 - 07/28/2011 02:47 PM - nagachika (Tomoyuki Chikanaga)

- ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of xmalloc() to allocate an array for arguments of callback procedure, to prevent arguments from being swept by GC. [ruby-core:38546] [Bug #4929]

Revision 32725 - 07/28/2011 02:47 PM - nagachika (Tomoyuki Chikanaga)

- ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of xmalloc() to allocate an array for arguments of callback procedure, to prevent arguments from being swept by GC. [ruby-core:38546] [Bug #4929]

Revision 32725 - 07/28/2011 02:47 PM - nagachika (Tomoyuki Chikanaga)

- ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of xmalloc() to allocate an array for arguments of callback procedure, to prevent arguments from being swept by GC. [ruby-core:38546] [Bug #4929]

Revision 34c7aaa1 - 07/28/2011 03:00 PM - nagachika (Tomoyuki Chikanaga)

merge revision 32725:

```
    * ext/fiddle/closure.c (callback): use rb_ary_tmp_new() instead of
      xmalloc() to allocate an array for arguments of callback procedure,
      to prevent arguments from being swept by GC. [ruby-core:38546]
      [Bug #4929]
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@32726 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 35c54610 - 02/14/2012 08:09 PM - naruse (Yui NARUSE)

merge revision(s) 32712,32718,32719: [Backport #6014]

```
    * ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark):
      workaround to mark wrapped object.  this is not a true fix,
      because [Bug #4929] is caused by the interface design of DL.

    * ext/dl/cptr.c (rb_dlptr_s_to_ptr): fix wrapping condition.

    * ext/dl/cptr.c (rb_dlptr_s_to_ptr): fix wrapping condition.

    * ext/dl/cptr.c (rb_dlptr_s_to_ptr): use rb_check_funcall.
```

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/branches/ruby_1_9_3@34604 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 06/26/2011 03:10 PM - kosaki (Motohiro KOSAKI)

This issue is only happend w/ --gc-stress.

i.e. seems similar with Bug#4927.

#2 - 07/08/2011 09:55 PM - kosaki (Motohiro KOSAKI)

- Status changed from Assigned to Closed

Hm,

Today's trunk don't reproduce this issue. I'll close this ticket.
Thanks guys!

#3 - 07/27/2011 12:22 PM - nagachika (Tomoyuki Chikanaga)

- Status changed from Closed to Open

Hi,

I've found that a similar problem remains at trunk(r32672) yet.
In my environment (Ubuntu 10.04.03), make test-all TESTS="-vq dl/test_func.rb -n test_qsort1.rb" cause SEGV.
It seems that CPtr.new in callback procedure cause SIGSEGV.
I'll re-open this ticket.

$ cat bug4929.rb
require "dl/func"

include DL

GC.stress = true
libc = dlopen("/lib/libc.so.6")
cb = Function.new(CFunc.new(0, TYPE_INT, 'qsort'),

```
[TYPE_VOIDP, TYPE_VOIDP]){|x,y|
CPtr.new(x)[0] <=> CPtr.new(y)[0]
}
qsort = Function.new(CFunc.new(libc['qsort'], TYPE_VOID, 'qsort'),
[TYPE_VOIDP, TYPE_INT, TYPE_INT, TYPE_VOIDP])
buff = "9341"
qsort.call(buff, buff.size, 1, cb)

$ ./ruby-trunk bug4929.rb
bug4929.rb:9: [BUG] Segmentation fault
ruby 1.9.4dev (2011-07-26 trunk 32672) [i686-linux]

-- Control frame information -----------------------------------------------
c:0008 p:---- s:0035 b:0035 l:000034 d:000034 CFUNC  :[]
c:0007 p:0022 s:0031 b:0031 l:001924 d:000030 LAMBDA bug4929.rb:9
c:0006 p:---- s:0027 b:0027 l:000026 d:000026 FINISH
c:0005 p:---- s:0025 b:0025 l:000024 d:000024 CFUNC  :call
c:0004 p:0059 s:0018 b:0018 l:000017 d:000017 METHOD /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl/func.rb:55
c:0003 p:0227 s:0010 b:0010 l:001924 d:001b2c EVAL   bug4929.rb:14
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:001924 d:001924 TOP

-- Ruby level backtrace information ----------------------------------------
bug4929.rb:14:in <main>'
/home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl/func.rb:55:incall'
/home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl/func.rb:55:in call'
bug4929.rb:9:inblock in '
bug4929.rb:9:in `[]'

-- C level backtrace information -------------------------------------------
./ruby-trunk() [0x816850d] ../ruby/vm_dump.c:796
./ruby-trunk() [0x81ad6a9] ../ruby/error.c:265
./ruby-trunk(rb_bug+0x33) [0x81ad763] ../ruby/error.c:284
./ruby-trunk() [0x80f73e0] ../ruby/signal.c:610
[0x5c1410]
./ruby-trunk() [0x8153795] ../ruby/vm_insnhelper.c:317
./ruby-trunk() [0x815ae5a] ../ruby/vm_insnhelper.c:404
./ruby-trunk() [0x8160b2e] ../ruby/insns.def:1979
./ruby-trunk() [0x8165538] ../ruby/vm.c:1180
./ruby-trunk() [0x8158536] ../ruby/vm.c:637
./ruby-trunk() [0x81585de] ../ruby/vm_insnhelper.c:429
./ruby-trunk() [0x815884b] ../ruby/vm_eval.c:104
/home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/fiddle.so(callback+0x1ea) [0x5ea85a] ../../../ruby/ext/fiddle/closure.c:101
/usr/lib/libffi.so.5(+0x4316) [0xa09316]
/usr/lib/libffi.so.5(+0x46fa) [0xa096fa]
/lib/libc.so.6(+0x2e390) [0x336390] msort.c:142
/lib/libc.so.6(+0x2e25d) [0x33625d] msort.c:53
/lib/libc.so.6(qsort_r+0x239) [0x3367f9] msort.c:294
/lib/libc.so.6(qsort+0x2e) [0x3368fe] msort.c:304
/usr/lib/libffi.so.5(ffi_call_SYSV+0x17) [0xa0963f]
/usr/lib/libffi.so.5(ffi_call+0x6f) [0xa0946f]
/home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/fiddle.so(+0x1c35) [0x5e9c35] ../../../ruby/ext/fiddle/function.c:125
./ruby-trunk() [0x8153795] ../ruby/vm_insnhelper.c:317
./ruby-trunk() [0x815ae5a] ../ruby/vm_insnhelper.c:404
./ruby-trunk() [0x8162bc2] ../ruby/insns.def:1048
./ruby-trunk() [0x8165538] ../ruby/vm.c:1180
./ruby-trunk(rb_iseq_eval_main+0x1ce) [0x816591e] ../ruby/vm.c:1421
./ruby-trunk() [0x805c012] ../ruby/eval.c:204
./ruby-trunk(ruby_run_node+0x32) [0x805deb2] ../ruby/eval.c:251
./ruby-trunk() [0x805b20a] ../ruby/main.c:38
/lib/tls/i686/cmov/libc.so.6(__libc_start_main+0xe6) [0x158bd6] libc-start.c:232
./ruby-trunk() [0x805b111]

-- Other runtime information -----------------------------------------------
```

- Loaded script: bug4929.rb

- Loaded features:

  ```
  0 enumerator.so
  1 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/encdb.so
  2 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/trans/transdb.so
  3 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/rubygems/defaults.rb
  4 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/rbconfig.rb
  5 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/rubygems/deprecate.rb
  ```

6 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/rubygems/exceptions.rb
7 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/rubygems/custom_require.rb
8 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/rubygems.rb
9 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/dl.so
10 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/fiddle.so
11 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/fiddle/function.rb
12 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/fiddle/closure.rb
13 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/fiddle.rb
14 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl.rb
15 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/thread.rb
16 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl/callback.rb
17 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl/stack.rb
18 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl/value.rb
19 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/dl/func.rb

- Process memory map:

00110000-00119000 r-xp 00000000 08:01 1900550 /lib/tls/i686/cmov/libcrypt-2.11.1.so
00119000-0011a000 r--p 00008000 08:01 1900550 /lib/tls/i686/cmov/libcrypt-2.11.1.so
0011a000-0011b000 rw-p 00009000 08:01 1900550 /lib/tls/i686/cmov/libcrypt-2.11.1.so
0011b000-00142000 rw-p 00000000 00:00 0
00142000-00295000 r-xp 00000000 08:01 1900548 /lib/tls/i686/cmov/libc-2.11.1.so
00295000-00296000 ---p 00153000 08:01 1900548 /lib/tls/i686/cmov/libc-2.11.1.so
00296000-00298000 r--p 00153000 08:01 1900548 /lib/tls/i686/cmov/libc-2.11.1.so
00298000-00299000 rw-p 00155000 08:01 1900548 /lib/tls/i686/cmov/libc-2.11.1.so
00299000-0029c000 rw-p 00000000 00:00 0
00304000-00306000 r-xp 00000000 08:01 715438 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/encdb.so
00306000-00307000 r--p 00001000 08:01 715438 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/encdb.so
00307000-00308000 rw-p 00002000 08:01 715438 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/encdb.so
00308000-0044a000 r-xp 00000000 08:01 1884264 /lib/libc-2.11.1.so
0044a000-0044b000 ---p 00142000 08:01 1884264 /lib/libc-2.11.1.so
0044b000-0044d000 r--p 00142000 08:01 1884264 /lib/libc-2.11.1.so
0044d000-0044e000 rw-p 00144000 08:01 1884264 /lib/libc-2.11.1.so
0044e000-00451000 rw-p 00000000 00:00 0
0046f000-00471000 r-xp 00000000 08:01 762073 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/trans/transdb.so
00471000-00472000 r--p 00001000 08:01 762073 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/trans/transdb.so
00472000-00473000 rw-p 00002000 08:01 762073 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/enc/trans/transdb.so
005c1000-005c2000 r-xp 00000000 00:00 0 [vdso]
005e8000-005eb000 r-xp 00000000 08:01 715461 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/fiddle.so
005eb000-005ec000 r--p 00002000 08:01 715461 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/fiddle.so
005ec000-005ed000 rw-p 00003000 08:01 715461 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/fiddle.so
00697000-006b4000 r-xp 00000000 08:01 1884621 /lib/libgcc_s.so.1
006b4000-006b5000 r--p 0001c000 08:01 1884621 /lib/libgcc_s.so.1
006b5000-006b6000 rw-p 0001d000 08:01 1884621 /lib/libgcc_s.so.1
0082c000-00850000 r-xp 00000000 08:01 1900552 /lib/tls/i686/cmov/libm-2.11.1.so
00850000-00851000 r--p 00023000 08:01 1900552 /lib/tls/i686/cmov/libm-2.11.1.so
00851000-00852000 rw-p 00024000 08:01 1900552 /lib/tls/i686/cmov/libm-2.11.1.so
00908000-0090a000 r-xp 00000000 08:01 1900551 /lib/tls/i686/cmov/libdl-2.11.1.so
0090a000-0090b000 r--p 00001000 08:01 1900551 /lib/tls/i686/cmov/libdl-2.11.1.so
0090b000-0090c000 rw-p 00002000 08:01 1900551 /lib/tls/i686/cmov/libdl-2.11.1.so
009e7000-009ee000 r-xp 00000000 08:01 1900564 /lib/tls/i686/cmov/librt-2.11.1.so
009ee000-009ef000 r--p 00006000 08:01 1900564 /lib/tls/i686/cmov/librt-2.11.1.so
009ef000-009f0000 rw-p 00007000 08:01 1900564 /lib/tls/i686/cmov/librt-2.11.1.so
00a05000-00a0a000 r-xp 00000000 08:01 2154925 /usr/lib/libffi.so.5.0.10
00a0a000-00a0b000 ---p 00005000 08:01 2154925 /usr/lib/libffi.so.5.0.10
00a0b000-00a0c000 r--p 00005000 08:01 2154925 /usr/lib/libffi.so.5.0.10
00a0c000-00a0d000 rw-p 00006000 08:01 2154925 /usr/lib/libffi.so.5.0.10
00bea000-00bff000 r-xp 00000000 08:01 1900562 /lib/tls/i686/cmov/libpthread-2.11.1.so
00bff000-00c00000 r--p 00014000 08:01 1900562 /lib/tls/i686/cmov/libpthread-2.11.1.so
00c00000-00c01000 rw-p 00015000 08:01 1900562 /lib/tls/i686/cmov/libpthread-2.11.1.so
00c01000-00c03000 rw-p 00000000 00:00 0
00e42000-00e52000 r-xp 00000000 08:01 715466 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/dl.so
00e52000-00e53000 r--p 0000f000 08:01 715466 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/dl.so
00e53000-00e54000 rw-p 00010000 08:01 715466 /home/chikanaga/opt/ruby-trunk/lib/ruby/1.9.1/i686-linux/dl.so
00f0e000-00f29000 r-xp 00000000 08:01 1884259 /lib/ld-2.11.1.so
00f29000-00f2a000 r--p 0001a000 08:01 1884259 /lib/ld-2.11.1.so
00f2a000-00f2b000 rw-p 0001b000 08:01 1884259 /lib/ld-2.11.1.so
08048000-08229000 r-xp 00000000 08:01 937708 /home/chikanaga/opt/ruby-trunk/src/build/ruby-trunk
08229000-0822a000 r--p 001e0000 08:01 937708 /home/chikanaga/opt/ruby-trunk/src/build/ruby-trunk
0822a000-0822b000 rw-p 001e1000 08:01 937708 /home/chikanaga/opt/ruby-trunk/src/build/ruby-trunk
0822b000-0823b000 rw-p 00000000 00:00 0
09968000-09b9d000 rw-p 00000000 00:00 0 [heap]
b77be000-b783f000 rw-p 00000000 00:00 0
b783f000-b78c0000 r--p 00000000 08:01 2203743 /usr/lib/locale/ja_JP.utf8/LC_CTYPE

b78c0000-b78c3000 rw-p 00000000 00:00 0
b78c8000-b78c9000 rw-p 00000000 00:00 0
b78c9000-b78ca000 r-xp 00000000 00:00 0
b78ca000-b78cb000 rw-p 00000000 00:00 0
b78cb000-b78cc000 ---p 00000000 00:00 0
b78cc000-b78cf000 rw-p 00000000 00:00 0
b78cf000-b78d6000 r--s 00000000 08:01 2173072 /usr/lib/gconv/gconv-modules.cache
b78d6000-b78d8000 rw-p 00000000 00:00 0
bf90a000-bf91f000 rw-p 00000000 00:00 0 [stack]

[NOTE]
You may have encountered a bug in the Ruby interpreter or extension libraries.
Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html

#4 - 07/28/2011 02:15 AM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r32712.
Motohiro, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

- ext/dl/cfunc.c (dlcfunc_mark), ext/dl/cptr.c (dlptr_mark): workaround to mark wrapped object. this is not a true fix, because [Bug #4929] is caused by the interface design of DL.