

Ruby - Bug #16807

Ruby 2.7 segfault loading sources under GC.stress

04/22/2020 08:03 AM - qnighy (Masaki Hara)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:	ruby 2.7.1p83 (2020-03-31 revision a0c7c23c9c) [x86_64-darwin19]	Backport: 2.5: DONTNEED, 2.6: DONTNEED, 2.7: DONE
Description Originally seen in https://github.com/protocolbuffers/protobuf/pull/7386, but reproduces without C extension. Reproduction: place these four files from this gist: • tests/ ◦ gc_test.rb ◦ generated_code_pb.rb ◦ generated_code_proto2_pb.rb • lib/ ◦ google/ ▪ protobuf.rb Then I got the following: <pre>\$ ruby -Ilib tests/gc_test.rb /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb:72: [BUG] Segmentation fault at 0x00007fd23ba8e608 ruby 2.7.1p83 (2020-03-31 revision a0c7c23c9c) [x86_64-darwin19] -- Crash Report log information ----- See Crash Report log file under the one of following: * ~/Library/Logs/DiagnosticReports * /Library/Logs/DiagnosticReports for more details. Don't forget to include the above Crash Report log file in bug reports. -- Control frame information ----- c:0007 p:---- s:0052 e:000051 CFUNC :require c:0006 p:0111 s:0047 e:000046 METHOD /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb:72 c:0005 p:0005 s:0031 e:000030 TOP /Users/qnighy/workdir/ruby-parse-failure/tests/generated_code_pb.rb:4 [FINISH] c:0004 p:---- s:0028 e:000027 CFUNC :require c:0003 p:0111 s:0023 e:000022 METHOD /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb:72 c:0002 p:0064 s:0007 E:000d38 EVAL tests/gc_test.rb:8 [FINISH] c:0001 p:0000 s:0003 E:001d80 (none) [FINISH] -- Ruby level backtrace information ----- tests/gc_test.rb:8:in `<main>' /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb:72:in `require' /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb:72:in `require' /Users/qnighy/workdir/ruby-parse-failure/tests/generated_code_pb.rb:4:in `<top (required)>' /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb:72:in `require' /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb:72:in `require' -- Machine register context -----</pre>		

```
rax: 0x00000000c27c19ab rbx: 0x0000000000000000 rcx: 0x00007fcc27c818b0
rdx: 0x00000000c27c19ab rdi: 0x0000000000000000 rsi: 0x00007fcc2a015c10
rbp: 0x00007ffeed341d80 rsp: 0x00007ffeed341d40 r8: 0x0000000000000000
r9: 0x0000000000000028 r10: 0x00007fcc27c0b030 r11: 0xffffffffcd3acd8990
r12: 0x0000000000000000 r13: 0x0000000000000000 r14: 0x0000000000000000
r15: 0x0000000000000000 rip: 0x0000000102a3724e rfl: 0x0000000000010282
```

-- C level backtrace information -----

```
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_print_backtrace+0x19) [0x102be8a09]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_vm_bugreport+0xa8) [0x102be8ad8]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_bug_for_fatal_signal+0x1b5) [0x10296c485]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(sig_do_nothing+0x0) [0x102b11540]
/usr/lib/system/libsystem_platform.dylib(_sigtramp+0x1d) [0x7fff6a8435fd]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(mark_ast_value+0x6e) [0x102a3724e]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(iterate_buffer_elements+0x51) [0x102a37d81]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(iterate_node_values+0x38) [0x102a36fb8]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_ast_mark+0x81) [0x102a371d1]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(gc_mark_imemo+0x206) [0x1029a5ce6]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(gc_mark_children+0x123) [0x102997173]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(gc_mark_stacked_objects+0x79) [0x10299fe69]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(gc_mark_stacked_objects_all+0x1b) [0x1029a0a4b]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(gc_marks_rest+0x7f) [0x10299f74f]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(gc_marks+0x67) [0x1029a18e7]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(gc_start+0x364) [0x10299d944]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(garbage_collect+0x24) [0x1029947d4]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(garbage_collect_with_gvl+0x5f) [0x1029a63bf]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(objspace_malloc_gc_stress+0x8a) [0x1029a635a]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(objspace_xmalloc+0x2a) [0x102997d4a]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(ruby_xmalloc2_body+0x3c) [0x102997d0c]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(ruby_xmalloc2+0x1d) [0x10299c84d]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(str_new0+0x10b) [0x102b2ebfb]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_enc_str_new+0x50) [0x102b2eac0]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(parser_str_new+0x64) [0x102a8e814]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(parse_string+0x3a5) [0x102a89775]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(parser_yylex+0xb4) [0x102a84c64]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(yylex+0x34) [0x102a790e4]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(ruby_yyparse+0x583) [0x102a69eb3]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(yycompile0+0x15c) [0x102a8371c]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_suppress_tracing+0x14c) [0x102beb29c]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(yycompile+0xb2) [0x102a812d2]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_parser_compile_file_path+0x7e) [0x102a811ee]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(load_file_internal+0x777) [0x102b0a827]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_ensure+0x13c) [0x10297a54c]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(load_file+0x6c) [0x102b0813c]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_parser_load_file+0x83) [0x102b07dd3]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(load_iseq_eval+0x51) [0x1029ee9e1]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(require_internal+0x505) [0x1029eca35]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_require_string+0x27) [0x1029ebbb7]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_f_require+0x19) [0x1029ebb89]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(call_cfunc_1+0x30) [0x102bdd300]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_cfunc_with_frame+0x39b) [0x102bceb7b]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_cfunc+0x8c) [0x102bc5f9c]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_sendish+0xe8) [0x102bd4398]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_exec_core+0x3e0e) [0x102bab21e]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_vm_exec+0x192) [0x102bc0092]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_iseq_eval+0x30) [0x102bc1010]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(load_iseq_eval+0xd6) [0x1029eea66]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(require_internal+0x505) [0x1029eca35]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_require_string+0x27) [0x1029ebbb7]
```

```
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_f_require+0x19) [0x1029ebb89]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(call_cfunc_1+0x30) [0x102bdd300]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_cfunc_with_frame+0x39b) [0x102bceb7b]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_cfunc+0x8c) [0x102bc5f9c]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_method_each_type+0xd1) [0x102bc5601]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_method_each_type+0x365) [0x102bc5895]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_method+0x1a1) [0x102bc5331]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_call_general+0x2d) [0x102ba6b7d]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_sendish+0xe8) [0x102bd4398]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(vm_exec_core+0x3e0e) [0x102bab21e]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_vm_exec+0x192) [0x102bc0092]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_iseq_eval_main+0x30) [0x102bc1150]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(rb_ec_exec_node+0x12b) [0x102978c1b]
/Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib(ruby_run_node+0x73) [0x102978ab3]
/Users/qnighy/.rbenv/versions/2.7.1/bin/ruby(main+0x68) [0x1028b6f08]
```

-- Other runtime information -----

* Loaded script: tests/gc_test.rb

* Loaded features:

```
0 enumerator.so
1 thread.rb
2 rational.so
3 complex.so
4 ruby2_keywords.rb
5 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/encdb.bundle
6 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/trans/transdb.bundle
7 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/rbconfig.rb
8 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/compatibility.rb
9 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/defaults.rb
10 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/deprecate.rb
11 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/errors.rb
12 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/version.rb
13 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/requirement.rb
14 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/platform.rb
15 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/basic_specification.rb
16 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/stub_specification.rb
17 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/util.rb
18 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/text.rb
19 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/user_interaction.rb
20 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/specification_policy.rb
21 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/util/list.rb
22 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/specification.rb
23 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/exceptions.rb
24 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/bundler_version_finder.rb
25 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/dependency.rb
26 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_gem.rb
27 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor.bundle
28 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/monitor.rb
29 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_require.rb
30 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/core_ext/kernel_warn.rb
31 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems.rb
32 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/rubygems/path_support.rb
33 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/version.rb
34 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/core_ext/name_error.rb
35 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/levenshtein.rb
36 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/jaro_winkler.rb
37 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/spell_checker.rb
38 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/spell_checkers/name_error_checkers/class_name_checker.rb
39 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/spell_checkers/name_error_checkers/variable_name_checker.rb
```

```

 40 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/spell_checkers/name_error_ch
eckers.rb
 41 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/spell_checkers/method_name_c
hecker.rb
 42 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/spell_checkers/key_error_che
cker.rb
 43 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/spell_checkers/null_checker.
rb
 44 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/formatters/plain_formatter.r
b
 45 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean/tree_spell_checker.rb
 46 /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/did_you_mean.rb

* Process memory map:

1028b6000-1028b7000 r-x /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
1028b7000-1028b8000 r-- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
1028b8000-1028b9000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
1028b9000-1028ba000 r-- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
1028ba000-1028bc000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib
1028bc000-102c97000 r-x /Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib
102c97000-102c9c000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib
102c9c000-102c9e000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib
102c9e000-102cb4000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib
102cb4000-102e03000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib
102e03000-102e04000 r-- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e04000-102e05000 rw- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e05000-102e06000 r-- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e06000-102e07000 r-- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e07000-102e08000 rw- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e0a000-102e66000 r-x /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e66000-102e67000 r-- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e67000-102e68000 rw- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e68000-102e72000 r-- /usr/local/Cellar/gmp/6.2.0/lib/libgmp.10.dylib
102e72000-102e73000 --- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102e73000-102e79000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102e79000-102e7a000 --- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102e7a000-102e7b000 --- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102e7b000-102e81000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102e81000-102e82000 --- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102e82000-102ec2000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102ec2000-102edc000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102edc000-102fdc000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102fdc000-102fec000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
102fec000-10304c000 rw- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
10304c000-103050000 r-- /Users/qnighy/.rbenv/versions/2.7.1/bin/ruby
103050000-105050000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105050000-105064000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105064000-105070000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105070000-105071000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105071000-105112000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105112000-105113000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105113000-1051b4000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1051b4000-1051b5000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1051b5000-105256000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105256000-105257000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105257000-1052f8000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc

```

[illegible]

```

105d19000-105dba000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105dba000-105dbb000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105dbb000-105e5c000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105e5c000-105e5d000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105e5d000-105efe000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105efe000-105eff000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105eff000-105fa0000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105fa0000-105fa1000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
105fa1000-106042000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
106042000-106043000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
106043000-1060e4000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1060e4000-1060e5000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1060e5000-106186000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
106186000-106187000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
106187000-106228000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
106228000-106229000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
106229000-1062ca000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1062ca000-1062cb000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1062cb000-10636c000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
10636c000-10636d000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
10636d000-10640e000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
10640e000-10640f000 --- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
10640f000-1064b0000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1064b0000-1064b2000 r-x /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1064b2000-1064b3000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1064b3000-1064b4000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1064b4000-1064b5000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/enc
db.bundle
1064b5000-1064b7000 r-x /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/tra
ns/transdb.bundle
1064b7000-1064b8000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/tra
ns/transdb.bundle
1064b8000-1064b9000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/tra
ns/transdb.bundle
1064b9000-1064ba000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/enc/tra
ns/transdb.bundle
1064ba000-1064c9000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor
.bundle
1064c9000-1064e1000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor
.bundle
1064e1000-1064fe000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor

```

```

.bundle
1064fe000-106537000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor
.bundle
106537000-106539000 r-x /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor
.bundle
106539000-10653a000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor
.bundle
10653a000-10653b000 rw- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor
.bundle
10653b000-10653d000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/ruby/2.7.0/x86_64-darwin19/monitor
.bundle
10653d000-106a6e000 r-- /Users/qnighy/.rbenv/versions/2.7.1/lib/libruby.2.7.dylib
106a6e000-106a94000 r-- /usr/lib/system/libsystem_platform.dylib
1097ea000-10987c000 r-x /usr/lib/dyld
10987c000-109881000 r-- /usr/lib/dyld
109881000-109882000 rw- /usr/lib/dyld
109882000-1098b7000 rw- /usr/lib/dyld
1098b7000-1098ef000 r-- /usr/lib/dyld
70000d0bf000-70000d0c0000 --- /usr/lib/dyld
70000d0c0000-70000d142000 rw- /usr/lib/dyld
7fcc27c00000-7fcc27d00000 rw- /usr/lib/dyld
7fcc27d00000-7fcc27e00000 rw- /usr/lib/dyld
7fcc27e00000-7fcc27f00000 rw- /usr/lib/dyld
7fcc27f00000-7fcc28000000 rw- /usr/lib/dyld
7fcc28000000-7fcc28800000 rw- /usr/lib/dyld
7fcc28800000-7fcc28900000 rw- /usr/lib/dyld
7fcc28900000-7fcc28a00000 rw- /usr/lib/dyld
7fcc28a00000-7fcc28b00000 rw- /usr/lib/dyld
7fcc28b00000-7fcc28c00000 rw- /usr/lib/dyld
7fcc29000000-7fcc29800000 rw- /usr/lib/dyld
7fcc29800000-7fcc2a000000 rw- /usr/lib/dyld
7fcc2a000000-7fcc2a800000 rw- /usr/lib/dyld
7fcc2a800000-7fcc2b000000 rw- /usr/lib/dyld
7fcc2b000000-7fcc2b800000 rw- /usr/lib/dyld
7ffee934a000-7ffee9cb4a000 --- /usr/lib/dyld
7ffee9cb4a000-7ffeed34a000 rw- /usr/lib/dyld
7fff00000000-7fff80000000 r-- /usr/lib/dyld
7fff80000000-7fff85000000 r-- /usr/lib/dyld
7fff85000000-7fff85200000 rw- /usr/lib/dyld
7fff85200000-7fff87800000 r-- /usr/lib/dyld
7fff87800000-7fff87a00000 rw- /usr/lib/dyld
7fff87a00000-7fff88200000 r-- /usr/lib/dyld
7fff88200000-7fff88400000 rw- /usr/lib/dyld
7fff88400000-7fff88600000 rw- /usr/lib/dyld
7fff88600000-7fff88800000 r-- /usr/lib/dyld
7fff88800000-7fff88a00000 rw- /usr/lib/dyld
7fff88a00000-7fff89e00000 r-- /usr/lib/dyld
7fff89e00000-7fff8a000000 rw- /usr/lib/dyld
7fff8a000000-7fff8d600000 r-- /usr/lib/dyld
7fff8d600000-7fff8d800000 rw- /usr/lib/dyld
7fff8d800000-7fff8da00000 rw- /usr/lib/dyld
7fff8da00000-7fff90a00000 r-- /usr/lib/dyld
7fff90a00000-7fff90c00000 rw- /usr/lib/dyld
7fff90c00000-7fff90e00000 rw- /usr/lib/dyld
7fff90e00000-7fff91000000 rw- /usr/lib/dyld
7fff91000000-7fff91200000 rw- /usr/lib/dyld
7fff91200000-7fff91600000 r-- /usr/lib/dyld
7fff91600000-7fff91800000 rw- /usr/lib/dyld
7fff91800000-7fffc0000000 r-- /usr/lib/dyld
7fffc0000000-7fffffe00000 r-- /usr/lib/dyld
7fffffe00000-7fffffe01000 r-- /usr/lib/dyld
7fffffe62000-7fffffe63000 r-x /usr/lib/dyld
[IMPORTANT]
Don't forget to include the Crash Report log file under
DiagnosticReports directory in bug reports.

zsh: abort      ruby -Ilib tests/gc_test.rb

```

This is seen in Linux too in the aforementioned pull request, but I couldn't reproduce it in my local Linux machine.

Also reproduced with miniruby from the latest master (8474e6a).

Associated revisions

Revision b35bfa6abb7760e4323a4341dff840f59ddcfde1 - 10/01/2020 12:02 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0,e8edc34f0abe176b24975a1fed1f2c3782f0a252: [Backport #16807]

Use a linked list to eliminate imemo tmp bufs for managing local tables

This patch changes local table memory to be managed by a linked list rather than via the garbage collector. It reduces allocations from the GC and also fixes a use-after-free bug in the concurrent-with-sweep compactor I'm working on.

Remove unused struct member

I accidentally added this in 35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0, and it's making the size of RVALUE be too big. I'm sorry! orz

Revision b35bfa6abb7760e4323a4341dff840f59ddcfde1 - 10/01/2020 12:02 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0,e8edc34f0abe176b24975a1fed1f2c3782f0a252: [Backport #16807]

Use a linked list to eliminate imemo tmp bufs for managing local tables

This patch changes local table memory to be managed by a linked list rather than via the garbage collector. It reduces allocations from the GC and also fixes a use-after-free bug in the concurrent-with-sweep compactor I'm working on.

Remove unused struct member

I accidentally added this in 35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0, and it's making the size of RVALUE be too big. I'm sorry! orz

Revision b35bfa6a - 10/01/2020 12:02 PM - nagachika (Tomoyuki Chikanaga)

merge revision(s) 35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0,e8edc34f0abe176b24975a1fed1f2c3782f0a252: [Backport #16807]

Use a linked list to eliminate imemo tmp bufs for managing local tables

This patch changes local table memory to be managed by a linked list rather than via the garbage collector. It reduces allocations from the GC and also fixes a use-after-free bug in the concurrent-with-sweep compactor I'm working on.

Remove unused struct member

I accidentally added this in 35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0, and it's making the size of RVALUE be too big. I'm sorry! orz

History

#1 - 04/22/2020 09:49 AM - nobu (Nobuyoshi Nakada)

ID list in NODE_SCOPE seems corrupted.
Maybe a GC compaction related issue?

#2 - 10/01/2020 11:39 AM - mame (Yusuke Endoh)

This issue still reproduces on ruby_2_7 branch, and does not on master.

I investigated the issue. local_tbl() allocates imemo_tmpbuf for a local variable table and returns a pointer to the buffer. And then, node_newnode_with_locals() creates a AST node with the pointer. However, if GC may occur on the allocation of the new NODE, the table is freed, so the NODE contains a dangling pointer, which cause a very rare segfault issue.

I created a patch to fix the issue. But it does not apply to master because the relevant functions have been drastically refactored at 35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0, which also (maybe unknowingly) fixes the issue. So, we may backport the commit to ruby_2_7.

```
diff --git a/parse.y b/parse.y
```



```

index dc9c37555d..7734beecdf 100644
--- a/parse.y
+++ b/parse.y
@@ -518,7 +518,7 @@ static NODE *symbol_append(struct parser_params *p, NODE *symbols, NODE *symbol)
    static NODE *match_op(struct parser_params*, NODE*, NODE*, const YYLTYPE*, const YYLTYPE*);
-static ID *local_tbl(struct parser_params*);
+static VALUE local_tbl(struct parser_params*);
    static VALUE reg_compile(struct parser_params*, VALUE, int);
    static void reg_fragment_setenc(struct parser_params*, VALUE, int);
@@ -11819,7 +11819,7 @@ local_pop(struct parser_params *p)
    }
#ifdef RIPPER
-static ID*
+static VALUE
    local_tbl(struct parser_params *p)
    {
        int cnt_args = vtable_size(p->lvtbl->args);
@@ -11849,17 +11849,18 @@ local_tbl(struct parser_params *p)
        buf[cnt + 1] = (ID)tbl;
        RB_OBJ_WRITTEN(p->ast, Qnil, tbl);
-        return buf;
+        return tbl;
    }
    static NODE*
    node_newnode_with_locals(struct parser_params *p, enum node_type type, VALUE a1, VALUE a2, const rb_code_loca
tion_t *loc)
    {
-        ID *a0;
        NODE *n;
-        a0 = local_tbl(p);
+        VALUE tbl = local_tbl(p);
+        ID *a0 = tbl ? RB_IMEMO_TMPBUF_PTR(tbl) : 0;
        n = NEW_NODE(type, a0, a1, a2, loc);
+        RB_GC_GUARD(tbl);
        return n;
    }

```

#3 - 10/01/2020 11:42 AM - nagachika (Tomoyuki Chikanaga)

- Status changed from Open to Closed

- Backport changed from 2.5: UNKNOWN, 2.6: UNKNOWN, 2.7: UNKNOWN to 2.5: DONTNEED, 2.6: DONTNEED, 2.7: REQUIRED

Thank you for your report.

It seems that the git:35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0 fixed this issue.
I will backport it to ruby_2_7 branch.

#4 - 10/01/2020 12:02 PM - nagachika (Tomoyuki Chikanaga)

- Backport changed from 2.5: DONTNEED, 2.6: DONTNEED, 2.7: REQUIRED to 2.5: DONTNEED, 2.6: DONTNEED, 2.7: DONE

ruby_2_7 b35bfa6abb7760e4323a4341dff840f59ddcfde1 merged revision(s)
35ba2783fe6b3316a6bbc6f00bf975ad7185d6e0,e8edc34f0abe176b24975a1fed1f2c3782f0a252.