Backport191 - Backport #1891

(:A .. :z).to_a results symbol table overflow

08/05/2009 10:12 PM - phasis68 (Heesob Park)

Status:	Assigned	
Priority:	Normal	
Assignee:	yugui (Yuki Sonoda)	

Description

=begin
I noticed that the range of symbol is dangerous.

Consider this:
$ irb
irb(main):001:0> ("A".."z").to_a
=> ["A", "B", "C", "D", "E", "F", "G", "H", "I", "J", "K", "L", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "V", "W", "X", "Y", "Z", "[", "\", "]", "^", "_", "", "a", "b", "c", "d", "e", "f", "g", "h", "i", "j", "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", "y", "z"]
irb(main):002:0> (:A..:z).to_a
RuntimeError: symbol table overflow (symbol DODUJ)
from (irb):2:insucc'
from (irb):2:in each'
from (irb):2:into_a'
from (irb):2
from /usr/local/bin/irb:12:in `'
irb(main):003:0> (:Za..:A).to_a
(irb):3: [BUG] Segmentation fault
ruby 1.9.1p243 (2009-07-16 revision 24175) [i686-linux]

-- control frame ----------
c:0024 p:---- s:0084 b:0084 l:000083 d:000083 CFUNC :<=>
c:0023 p:0010 s:0082 b:0082 l:00256c d:00167c EVAL (irb):3
c:0022 p:---- s:0080 b:0080 l:000079 d:000079 FINISH
c:0021 p:---- s:0078 b:0078 l:000077 d:000077 CFUNC :eval
c:0020 p:0027 s:0071 b:0071 l:000070 d:000070 METHOD /usr/local/lib/ruby/1.9.1/irb/workspace.rb:80
c:0019 p:0031 s:0064 b:0063 l:000062 d:000062 METHOD /usr/local/lib/ruby/1.9.1/irb/context.rb:218
c:0018 p:0030 s:0058 b:0058 l:000f94 d:000057 BLOCK /usr/local/lib/ruby/1.9.1/irb.rb:149
c:0017 p:0037 s:0050 b:0050 l:000049 d:000049 METHOD /usr/local/lib/ruby/1.9.1/irb.rb:263
c:0016 p:0011 s:0045 b:0045 l:000f94 d:000044 BLOCK /usr/local/lib/ruby/1.9.1/irb.rb:146
c:0015 p:0132 s:0041 b:0041 l:000024 d:000040 BLOCK /usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:244
c:0014 p:---- s:0038 b:0038 l:000037 d:000037 FINISH
c:0013 p:---- s:0036 b:0036 l:000035 d:000035 CFUNC :loop
c:0012 p:0009 s:0033 b:0033 l:000024 d:000032 BLOCK /usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:230
c:0011 p:---- s:0031 b:0031 l:000030 d:000030 FINISH
c:0010 p:---- s:0029 b:0029 l:000028 d:000028 CFUNC :catch
c:0009 p:0023 s:0025 b:0025 l:000024 d:000024 METHOD /usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:229
c:0008 p:0042 s:0022 b:0022 l:000f94 d:000f94 METHOD /usr/local/lib/ruby/1.9.1/irb.rb:145
c:0007 p:0011 s:0019 b:0019 l:001c64 d:000018 BLOCK /usr/local/lib/ruby/1.9.1/irb.rb:69
c:0006 p:---- s:0017 b:0017 l:000016 d:000016 FINISH
c:0005 p:---- s:0015 b:0015 l:000014 d:000014 CFUNC :catch
c:0004 p:0172 s:0011 b:0011 l:001c64 d:001c64 METHOD /usr/local/lib/ruby/1.9.1/irb.rb:68
c:0003 p:0039 s:0006 b:0006 l:001d4c d:000f84 EVAL /usr/local/bin/irb:12
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:001d4c d:001d4c TOP

-- Ruby level backtrace information----------
(irb):3:in <=>'
(irb):3:inirb_binding'
/usr/local/lib/ruby/1.9.1/irb/workspace.rb:80:in eval'
/usr/local/lib/ruby/1.9.1/irb/workspace.rb:80:inevaluate'
/usr/local/lib/ruby/1.9.1/irb/context.rb:218:in evaluate'
/usr/local/lib/ruby/1.9.1/irb.rb:149:inblock (2 levels) in eval_input'
/usr/local/lib/ruby/1.9.1/irb.rb:263:in signal_status'
/usr/local/lib/ruby/1.9.1/irb.rb:146:inblock in eval_input'

/usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:244:in block (2 levels) in each_top_level_statement'
/usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:230:inloop'
/usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:230:in block in each_top_level_statement'
/usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:229:incatch'
/usr/local/lib/ruby/1.9.1/irb/ruby-lex.rb:229:in each_top_level_statement'
/usr/local/lib/ruby/1.9.1/irb.rb:145:ineval_input'
/usr/local/lib/ruby/1.9.1/irb.rb:69:in block in start'
/usr/local/lib/ruby/1.9.1/irb.rb:68:incatch'
/usr/local/lib/ruby/1.9.1/irb.rb:68:in start'
/usr/local/bin/irb:12:in'

-- C level backtrace information ---
0x811c168 irb(rb_vm_bugreport+0x48) [0x811c168]
0x8148368 irb [0x8148368]
0x81483eb irb(rb_bug+0x2b) [0x81483eb]
0x80cf686 irb [0x80cf686]
0x265440 [0x265440]
0x80db277 irb [0x80db277]
0x8117e1a irb [0x8117e1a]
0x81183bd irb(rb_funcall+0x15d) [0x81183bd]
0x80a627b irb [0x80a627b]
0x805a1e2 irb(rb_rescue2+0x142) [0x805a1e2]
0x805a287 irb(rb_rescue+0x37) [0x805a287]
0x80a6fd9 irb [0x80a6fd9]
0x80a7169 irb(rb_range_new+0x29) [0x80a7169]
0x81111d1 irb [0x81111d1]
0x8115f85 irb [0x8115f85]
0x811721a irb [0x811721a]
0x8117921 irb [0x8117921]
0x8117c8f irb(rb_f_eval+0xcf) [0x8117c8f]
0x810d346 irb [0x810d346]
0x810e927 irb [0x810e927]
0x810f794 irb [0x810f794]
0x8111d84 irb [0x8111d84]
0x8115f85 irb [0x8115f85]
0x81164a6 irb [0x81164a6]
0x8116bd8 irb [0x8116bd8]
0x805a1e2 irb(rb_rescue2+0x142) [0x805a1e2]
0x810e4eb irb [0x810e4eb]
0x810e927 irb [0x810e927]
0x810f794 irb [0x810f794]
0x8111d84 irb [0x8111d84]
0x8115f85 irb [0x8115f85]
0x81164a6 irb [0x81164a6]
0x8116abe irb [0x8116abe]
0x810d346 irb [0x810d346]
0x810e927 irb [0x810e927]
0x810f794 irb [0x810f794]
0x8111d84 irb [0x8111d84]
0x8115f85 irb [0x8115f85]
0x81164a6 irb [0x81164a6]
0x8116abe irb [0x8116abe]
0x810d346 irb [0x810d346]
0x810e927 irb [0x810e927]
0x810f794 irb [0x810f794]
0x8111d84 irb [0x8111d84]
0x8115f85 irb [0x8115f85]
0x81160c5 irb(rb_iseq_eval_main+0x95) [0x81160c5]
0x805a92f irb(ruby_exec_node+0x9f) [0x805a92f]
0x805b982 irb(ruby_run_node+0x42) [0x805b982]
0x80594f0 irb(main+0x60) [0x80594f0]
0xb49dec /lib/libc.so.6(__libc_start_main+0xdc) [0xb49dec]
0x80593d1 irb [0x80593d1]

[NOTE]
You may encounter a bug of Ruby interpreter. Bug reports are welcome.
For details: http://www.ruby-lang.org/bugreport.html

=end

History

#1 - 08/06/2009 01:51 PM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Assigned

- Assignee set to matz (Yukihiro Matsumoto)

=begin

=end

#2 - 08/18/2009 02:07 AM - matz (Yukihiro Matsumoto)

- Status changed from Assigned to Closed

- % Done changed from 0 to 100

=begin
Applied in changeset r24573.
=end

#3 - 03/15/2010 03:14 PM - phasis68 (Heesob Park)

=begin
This bug still exists on ruby 1.9.1p376.

I think r24573 should be backported.

=end

#4 - 03/15/2010 03:18 PM - shyouhei (Shyouhei Urabe)

- Status changed from Closed to Assigned

- Assignee changed from matz (Yukihiro Matsumoto) to yugui (Yuki Sonoda)

=begin

=end

#5 - 03/15/2010 04:03 PM - nobu (Nobuyoshi Nakada)

- Category set to core

=begin

=end