

Ruby - Bug #3236

ISeq.load [BUG] iseq_set_sequence: ic_index overflow

05/03/2010 12:09 AM - nagachika (Tomoyuki Chikanaga)

Status:	Closed	
Priority:	Normal	
Assignee:	ko1 (Koichi Sasada)	
Target version:		
ruby -v:	ruby 1.9.2dev (2010-05-02 trunk 27590) [x86_64-darwin10.3.0]	Backport:

Description

```
=begin
RubyGems: iseq load
$ cat iseq_load.rb
require "iseq"

iseq = ISeq.compile("@a[0]")
puts iseq.disasm
ISeq.load(iseq.to_a)

$ ruby-trunk -v iseq_load.rb
ruby 1.9.2dev (2010-05-02 trunk 27590) [x86_64-darwin10.3.0]
== disasm: <RubyVM::InstructionSequence:@>=====
0000 trace      1          ( 1)
0002 getinstancevariable :@a, ic:0
0005 putobject    0
0007 opt_aref     ic:2
0009 leave
iseq_load.rb:5: [BUG] iseq_set_sequence: ic_index overflow: index: 2, size: 0
ruby 1.9.2dev (2010-05-02 trunk 27590) [x86_64-darwin10.3.0]

-- control frame -----
c:0004 p:---- s:0011 b:0011 l:000010 d:000010 CFUNC :load
c:0003 p:0075 s:0007 b:0007 l:0014a8 d:000bc0 EVAL iseq_load.rb:5
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:0014a8 d:0014a8 TOP

-- Ruby level backtrace information -----
iseq_load.rb:5:in <main>' iseq_load.rb:5:in load'

-- C level backtrace information -----
0 ruby-trunk 0x0000000100177acb rb_vm_bugreport + 120
1 ruby-trunk 0x0000000100034f90 report_bug + 313
2 ruby-trunk 0x00000001000350b5 rb_bug + 241
3 ruby-trunk 0x000000010014a328 iseq_set_sequence + 2456
4 ruby-trunk 0x0000000100148f1c iseq_setup + 118
5 ruby-trunk 0x00000001001590e5 iseq_build_body + 2250
6 ruby-trunk 0x000000010015989f rb_iseq_build_from_ary + 1789
7 ruby-trunk 0x000000010015bbe3 iseq_load + 1788
8 ruby-trunk 0x000000010015bcb2 rb_iseq_load + 47
9 iseq.bundle 0x0000000100540eb5 iseq_s_load + 53
10 ruby-trunk 0x000000010016b040 call_cfunc + 282
11 ruby-trunk 0x000000010016aea7 vm_call_cfunc + 284
12 ruby-trunk 0x000000010016a07c vm_call_method + 373
13 ruby-trunk 0x0000000100164cae vm_exec_core + 11207
14 ruby-trunk 0x00000001001745e9 vm_exec + 147
15 ruby-trunk 0x0000000100174fca rb_iseq_eval_main + 45
16 ruby-trunk 0x0000000100039cd9 ruby_exec_internal + 193
17 ruby-trunk 0x0000000100039dfd ruby_exec_node + 30
```

```
18 ruby-trunk          0x0000000100039dd0 ruby_run_node + 56
19 ruby-trunk          0x0000000100000dcb main + 79
20 ruby-trunk          0x0000000100000d74 start + 52
21 ???                 0x0000000000000003 0x0 + 3
```

[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>

```
##### iseq #####(ic_size)#####make check
#####($prefix/lib/ruby/1.9.1/**/*.rb)##### ISeq.load #####
##### ic_index ic_size #####
```

Index: compile.c

--- compile.c (revision 27590)

+++ compile.c (working copy)

@@ -1434,7 +1434,7 @@

```
{
int ic_index = FIX2INT(operands[j]);
IC ic = &iseq->ic_entries[ic_index];
```

- [REDACTED]
- [REDACTED]

```
rb_bug("iseq_set_sequence: ic_index overflow: index: %d, size: %d",
      ic_index, iseq->ic_size);
}
```

@@ -5269,6 +5269,8 @@

break;

case TS_IC:

argv[j] = op;

- [REDACTED]
- [REDACTED]

```
break;
case TS_ID:
argv[j] = rb_convert_type(op, T_SYMBOL,
```

=end

Associated revisions

Revision 576252ae9d2b5e9601897eeca3aa2f25353068fc - 05/04/2010 02:10 PM - wanabe (_ wanabe)

- compile.c (iseq_build_body): update iseq->ic_size.
a patch from Tomoyuki Chikanaga. see #3236.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@27616 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 576252ae9d2b5e9601897eeca3aa2f25353068fc - 05/04/2010 02:10 PM - wanabe (_ wanabe)

- compile.c (iseq_build_body): update iseq->ic_size.
a patch from Tomoyuki Chikanaga. see #3236.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@27616 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 576252ae - 05/04/2010 02:10 PM - wanabe (_ wanabe)

- compile.c (iseq_build_body): update iseq->ic_size.

a patch from Tomoyuki Chikanaga. see #3236.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@27616 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 0356eef426342a3305924b6438bd29914d9cc57e - 05/05/2010 01:33 PM - wanabe (_ wanabe)

- compile.c (iseq_set_sequence): fix check range of ic_index.
a patch from Tomoyuki Chikanaga. #3236

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@27632 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

History

#1 - 05/04/2010 11:04 PM - wanabe (_ wanabe)

```
=begin
ic_index []
ic_size []
iseq_load []
=end
```

#2 - 05/05/2010 09:11 PM - wanabe (_ wanabe)

```
=begin
[]

[] ic_index []
[] r27616 []
[]
=end
```

#3 - 05/05/2010 10:12 PM - mame (Yusuke Endoh)

```
=begin
[]

InstructionSequence#load [] iseq gem [] third
party ([]) [] gem [] redmine [] Bug
[]
[]
[]
```

verifier

```
hunk []
rb_bug [] ic_entries []
[]
```

```
--
Yusuke Endoh mame@tsg.ne.jp
=end
```

#4 - 05/05/2010 10:37 PM - wanabe (_ wanabe)

- Status changed from Open to Closed
- % Done changed from 0 to 100

```
=begin
This issue was solved with changeset r27632.
Tomoyuki, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

=end
```

#5 - 05/06/2010 07:42 AM - nagachika (Tomoyuki Chikanaga)

```
=begin
[]

[]
=end
```