Ruby trunk - Bug #2030

Math.gamma(x) seg faults for integer x larger than 2<<63-1

09/02/2009 12:52 PM - hasari (Hiro Asari)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 1.9.2dev (2009-09-02 trunk 24735) [i386-darwin10.0.0]	**Backport:**	

Description

=begin
$ ruby19 -e 'puts Math.gamma(2<<63-1); puts Math.gamma(2<<63)'
Infinity
-e:1: [BUG] Segmentation fault
ruby 1.9.2dev (2009-09-02 trunk 24735) [i386-darwin10.0.0]

-- control frame ----------
c:0004 p:---- s:0011 b:0011 l:000010 d:000010 CFUNC :gamma
c:0003 p:0052 s:0007 b:0006 l:001488 d:000b18 EVAL   -e:1
c:0002 p:---- s:0004 b:0004 l:000003 d:000003 FINISH
c:0001 p:0000 s:0002 b:0002 l:001488 d:001488 TOP

-- Ruby level backtrace information--
-e:1:in <main>'
-e:1:ingamma'

-- C level backtrace information ---

[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

Abort trap

Incidentally, the URL at the end of this output should be updated. (Is that a separate ticket?)
=end

History

#1 - 09/02/2009 02:13 PM - nobu (Nobuyoshi Nakada)

=begin
Hi,

At Wed, 2 Sep 2009 12:52:23 +0900,
Hiro Asari wrote in [ruby-core:25257]:

> $ ruby19 -e 'puts Math.gamma(2<<63-1); puts Math.gamma(2<<63)'
> Infinity
> -e:1: [BUG] Segmentation fault
> ruby 1.9.2dev (2009-09-02 trunk 24735) [i386-darwin10.0.0]

I couldn't reproduce it on i386-darwin9.8.0. Maybe, due to the
differences of gcc or system library versions?

> Incidentally, the URL at the end of this output should be updated. (Is that a separate ticket?)

Yes, please.

--

Nobu Nakada

=end

#2 - 09/02/2009 02:27 PM - nobu (Nobuyoshi Nakada)

=begin
Hi,

At Wed, 2 Sep 2009 12:52:23 +0900,
Hiro Asari wrote in [ruby-core:25257]:

> Incidentally, the URL at the end of this output should be updated. (Is that a separate ticket?)

Now I've created a new ticket,
http://redmine.ruby-lang.org/issues/show/2031

--
Nobu Nakada

=end

#3 - 09/02/2009 02:28 PM - hasari (Hiro Asari)

=begin
That could very well be dependent. I used GCC came with Snow Leopard.

Indeed, I still have 1.9.1 that I built with 10.5.7, and it appears to be OK.

$ ~/.multiruby/install/1.9.1-p243/bin/ruby -v -e 'puts Math.gamma(2<<256)'
ruby 1.9.1p243 (2009-07-16 revision 24175) [i386-darwin9.7.0]
Infinity

If this is a compiler option-dependent issue, then I don't think it's worth it pursue it any further.

I apologize for the noise.
=end

#4 - 09/02/2009 02:29 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Feedback

=begin

=end

#5 - 09/02/2009 02:40 PM - nobu (Nobuyoshi Nakada)

=begin
Hi,

At Wed, 2 Sep 2009 14:30:25 +0900,
Hiro Asari wrote in [ruby-core:25261]:

> That could very well be dependent. I used GCC came with Snow Leopard.
>
> Indeed, I still have 1.9.1 that I built with 10.5.7, and it appears to be OK.
>
> $ ~/.multiruby/install/1.9.1-p243/bin/ruby -v -e 'puts Math.gamma(2<<256)'
> ruby 1.9.1p243 (2009-07-16 revision 24175) [i386-darwin9.7.0]
> Infinity
>
> If this is a compiler option-dependent issue, then I don't think it's worth it pursue it any further.

Does this patch fix it?

And, could you show the result of:
make math.S && sed -n '/math_gamma:/,/^[^.]/p' math.S

Index: math.c
===
--- math.c (revision 24737)
+++ math.c (working copy)

@@ -669,5 +669,5 @@ math_gamma(VALUE obj, VALUE x)
if (fracpart == 0.0 &&
0 < intpart &&

- (size_t)intpart <= sizeof(fact_table)/sizeof(*fact_table)) {
- intpart <= (double)sizeof(fact_table)/sizeof(*fact_table)) { return DBL2NUM(fact_table[(int)intpart - 1]); }

--
Nobu Nakada

=end

#6 - 09/02/2009 02:45 PM - hasari (Hiro Asari)

=begin
Yes, the patch appears to work.

surfboard:ruby[svn:24735]$ make math.S && sed -n '/math_gamma:/,/^[^.]/p' math.S
gcc -O3 -g -Wall -Wno-unused-parameter -Wno-parentheses -Wno-missing-field-initializers -Wshorten-64-to-32 -Wpointer-arith -Wwrite-strings -pipe
-I. -I.ext/include/i386-darwin10.0.0 -I./include -I. -DRUBY_EXPORT -D_XOPEN_SOURCE -D_DARWIN_C_SOURCE -o math.S -S math.c
math_gamma:
LFB63:
.loc 1 639 0
LVL167:
pushq %rbp
LCFI62:
movq %rsp, %rbp
LCFI63:
subq $32, %rsp
LCFI64:
LBB271:
LBB273:
.loc 2 1203 0
testb $3, %sil
je L346
LBE273:
.loc 2 1204 0
testb $1, %sil
je L377
L348:
LBE271:
.loc 1 669 0
movq %rsi, %rdi
LVL168:
call __rb_to_float
LVL169:
movq %rax, %rsi
LVL170:
L355:
.loc 1 670 0
movsd 16(%rsi), %xmm0
movsd %xmm0, -32(%rbp)
LVL171:
.loc 1 671 0
leaq -8(%rbp), %rdi
LVL172:
call _modf
LVL173:
.loc 1 672 0
xorpd %xmm1, %xmm1
ucomisd %xmm1, %xmm0
jne L356
jp L356
movsd -8(%rbp), %xmm0
LVL174:
ucomisd %xmm1, %xmm0
jbe L356
ucomisd LC34(%rip), %xmm0
jbe L378
L356:
.loc 1 677 0
call _error
movl $0, (%rax)
.loc 1 678 0
movsd -32(%rbp), %xmm0

```
call	__tgamma
movsd	%xmm0, -24(%rbp)
LVL175:
movsd	-32(%rbp), %xmm0
ucomisd %xmm0, %xmm0
jne L371
jp L371
movsd	-24(%rbp), %xmm0
ucomisd %xmm0, %xmm0
jne L374
jp L374
L371:
LBB275:
.loc 1 29 0
call	__error
LBB276:
movl	(%rax), %edi
testl	%edi, %edi
jne L368
LBE276:
LBE275:
.loc 1 680 0
movsd	-24(%rbp), %xmm0
call	__rb_float_new
.loc 1 681 0
leave
ret
LVL176:
L346:
LBB280:
LBB272:
.loc 2 1209 0
testq	$-5, %rsi
jne L352
.loc 2 1210 0
cmpq	$4, %rsi
je L348
.loc 2 1211 0
testq	%rsi, %rsi
je L348
L352:
LBE272:
LBE280:
.loc 1 669 0
movl	(%rsi), %eax
andl	$31, %eax
cmpl	$4, %eax
jne L348
jmp L355
L377:
LBB281:
LBB274:
.loc 2 1205 0
cmpq	$2, %rsi
je L348
.loc 2 1206 0
cmpb	$14, %sil
je L348
.loc 2 1207 0
cmpq	$6, %rsi
jne L352
jmp L348
LVL177:
L378:
LBE274:
LBE281:
.loc 1 672 0
jp L356
.loc 1 675 0
cvttsd2si	%xmm0, %eax
cltq
leaq	-8+_fact_table.7022(%rip), %rdx
movsd	(%rdx,%rax,8), %xmm0
call	__rb_float_new
.loc 1 681 0
```

leave
ret
LVL178:
L368:
LBB282:
LBB277:
.loc 1 30 0
leaq	LC29(%rip), %rdi
call	_rb_sys_fail
L374:
LBE277:
.loc 1 29 0
call	__error
LBB278:
movl	(%rax), %r8d
testl	%r8d, %r8d
jne L368
LBE278:
.loc 1 35 0
call	__error
LBB279:
movl	$33, (%rax)
jmp L374
LBE279:
LBE282:
LFE63:
.align 4,0x90
_math_sqrt:

=end

#7 - 09/02/2009 03:39 PM - nobu (Nobuyoshi Nakada)

=begin
Hi,

At Wed, 2 Sep 2009 14:45:56 +0900,
Hiro Asari wrote in [ruby-core:25263]:

> Yes, the patch appers to work.
>
> surfboard:ruby[svn:24735]$ make math.S && sed -n '/math_gamma:/,/LF[E]/p' math.S
> gcc -O3 -g -Wall -Wno-unused-parameter -Wno-parentheses -Wno-missing-field-initializers -Wshorten-64-to-32 -Wpointer-arith -Wwrite-strings
> -pipe -I. -I.ext/include/i386-darwin10.0.0 -I./include -I. -DRUBY_EXPORT -D_XOPEN_SOURCE -D_DARWIN_C_SOURCE   -o math.S -S
> math.c
> _math_gamma:
> LFB63:
> .loc 1 639 0
> LVL167:
> pushq	%rbp

It's x86_64, not i386. OK, I could reproduce it with x86_64 on
darwin 9.8.0.

Wrong platform name is another issue.

--
Nobu Nakada

=end

#8 - 09/02/2009 04:57 PM - nobu (Nobuyoshi Nakada)

- Status changed from Feedback to Closed

- % Done changed from 0 to 100

=begin
Applied in changeset r24738.
=end