Ruby - Bug #948

dl: cannot pass double value correctly on all x86_64 systems

12/30/2008 01:27 AM - kubo (Takehiro Kubo)

Status:	Closed		
Priority:	Normal		
Assignee:	tenderlovemaking (Aaron Patterson)		
Target version:	1.9.2		
ruby -v:	ruby 1.9.2dev (2010-02-03 trunk 26544) [x86_64-darwin10.2.0]	**Backport:**	

Description

=begin
ext/dl/test/test_dl2.rb doesn't fail on x86_64 linux. But it is by chance.
It fails just by changing as follows.

--- ext/dl/test/test_dl2.rb (revision 21182)
+++ ext/dl/test/test_dl2.rb (working copy)
@@ -34,8 +34,8 @@

```
def test_sin()
  cfunc = CFunc.new(@libm['sin'], TYPE_DOUBLE, 'sin')
```

- x = cfunc.call([3.14/2].pack("d").unpack("l!*"))
- assert_equal(x, Math.sin(3.14/2))

- x = cfunc.call([1.57].pack("d").unpack("l!*"))

- assert_equal(x, Math.sin(1.57))

  cfunc = CFunc.new(@libm['sin'], TYPE_DOUBLE, 'sin')
  x = cfunc.call([-3.14/2].pack("d").unpack("l!*"))

dl passes function arguments as long types. But on x86_64 linux, the
first double value is passed by XMM0 register and the first long
value is by RDI. sin() expects that the argument is passed by XMM0.
But dl passes it by RDI.

The test had passed because calculating 3.14/2 set XMM0 register and the
value had not been changed until cfunc.call was called. sin() got the
argument by XMM0 which happened to be 3.14/2.

I have tested this on x86_64 linux. But I guess it will fail on all x86_64 systems.
See: http://en.wikipedia.org/wiki/X86_calling_conventions
"Microsoft x64 calling convention" and "AMD64 ABI convention"

I guess it is extremely hard to fix this.
=end

History

#1 - 12/30/2008 07:19 PM - yugui (Yuki Sonoda)

- Category set to ext

- Target version set to 1.9.1 Release Candidate

=begin

=end

#2 - 12/30/2008 09:05 PM - yugui (Yuki Sonoda)

- Target version changed from 1.9.1 Release Candidate to 1.9.1 RC2

=begin

=end

#3 - 01/16/2009 01:41 PM - yugui (Yuki Sonoda)

- Target version changed from 1.9.1 RC2 to 1.9.2

=begin

=end

#4 - 12/01/2009 07:13 PM - ujihisa (Tatsuhiro Ujihisa)

- Status changed from Open to Assigned

- Assignee set to tenderlovemaking (Aaron Patterson)

=begin

=end

#5 - 02/03/2010 10:41 AM - tenderlovemaking (Aaron Patterson)

- Status changed from Assigned to Closed

- ruby -v set to ruby 1.9.2dev (2010-02-03 trunk 26544) [x86_64-darwin10.2.0]

=begin
DL now uses libffi for function calling. Steer clear of using CFunc#call. Use Function#call instead, and you will use libffi which will deal with x86_64 systems.
=end