Ruby 1.8 - Bug #2781

crash when gc_mark()ing already free'd locals of cloned scope

02/23/2010 08:48 AM - coderrr (coderrr .)

Status:	Open
Priority:	Normal
Assignee:	
Target version:	
ruby -v:	>= 1.8.7-p248

Description

=begin
This causes a segfault on >= 1.8.7-p248

```
def def_x(arg)
Object.send :define_method, :x do
def_x lambda{}
end
end

GC.stress = true  # unnecessary but makes it occur faster
def_x nil
n = 3 # minimum for crash, increase if needed
n.times { x 0 }
```

This bug was caused by the fix i suggested for #1322,
http://github.com/rubyspec/matzruby/commit/7c646cbba0815b3c9c7dc76f80fae58b30ec66b4.

The previous fix is flawed in that it added the SCOPE_MALLOC flag to the scope just so scope_dup() didn't process it. This had the side-effect that gc_mark_children() now processes the scope whereas it would not have before. A better fix is the following, which instead of adding the SCOPE_MALLOC flag, we add a check for the SCOPE_CLONE flag to scope_dup(). This fixes bug #1322 as well as the segfault: http://github.com/coderrr/matzruby/commit/249c7d9912b961a9350f300ed148857100a659f8

Please check the patch for other unforseen side effects. I didn't see any changes in rubyspec failures from p174 to a patched p248.
=end

History

#1 - 02/24/2010 05:01 AM - coderrr (coderrr .)

=begin
just realized the check for SCOPE_CLONE is also no longer needed before freeing locals:
http://github.com/coderrr/matzruby/commit/9c80aae67002e443314033b04ceb9c6e5b886c57
=end

#2 - 03/02/2010 06:11 PM - coderrr (coderrr .)

=begin
By the way, this causes the popular web framework sinatra to segfault due to
http://github.com/sinatra/sinatra/blob/master/lib/sinatra/base.rb#L687-702
=end

#3 - 08/31/2010 05:42 AM - tmm1 (Aman Gupta)

=begin
I can confirm that this is still an issue in 1.8.7-p302 (I had to increase n=3000 to reproduce on linux).

It is also causing segfaults when using Sinatra <= 0.9.5. The segfaults in Sinatra are fixed as of >= 0.9.6 with this patch:
http://github.com/sinatra/sinatra/commit/ae34a6fde5e15e9ba3ca40cf800d0366e44eec1f
=end