Ruby 1.8 - Bug #5641

String sharing with dup

11/16/2011 08:47 PM - Eregon (Benoit Daloze)

Status:	Open
Priority:	Normal
Assignee:	
Target version:	
ruby -v:	ruby 1.8.7 (2011-06-30 patchlevel 352) [i686-darwin10.8.0]

Description

Hello,

I am not sure this is not intended, but the string sharing behavior is not working at least in this case on my machine:

```
str = "a" * 1024 * 1024
a = 1000.times.map { str.dup }
p :done
sleep # check your memory, oops ruby took a GB!
```

It only happens on 1.8 (neither 1.9, nor jruby/rbx).
I poked around a bit in the code with gdb and noticed a few things:

#dup is calling #initialize_copy, which is defined by rb_str_replace for strings.

In rb_str_replace(str, str2):
str2 is is a pointer to the original string, str is the string being created as a copy of str2.
It goes to line 2333 (the pointer copy) and that seems right.
However, at line 2335, the call str_make_independent(str) will actually memcpy() the whole C string under and thus str->ptr will be different than str->ptr2, and the underlying bytes be copied.