

Ruby - Bug #1137

I can modify literals

02/11/2009 02:17 AM - mame (Yusuke Endoh)

Status:	Closed	
Priority:	Normal	
Assignee:		
Target version:		
ruby -v:		Backport:

Description

```
=begin
#####

ObjectSpace #####
#####

def foo
  "foobarbaz"
end

ObjectSpace.each_object(String) do |s|
  s.replace("evil") if /foobarbaz/ =~ s && !s.frozen?
end

p foo #=> "evil"

def bar
  ls -l
end

ObjectSpace.each_object(String) do |s|
  s.replace("echo rm -rf /") if /ls -l/ =~ s && !s.frozen?
end

p bar #=> "rm -rf /\n"

##### freeze #####IRC ##

  • freeze #####
  • freeze ## finalizer #####

#####
```

Index: compile.c

```
--- compile.c (revision 22217)
+++ compile.c (working copy)
@@ -2120,7 +2120,7 @@
int cnt = 1;

  debugp_param("nd_lit", lit);

  • ADD_INSN1(ret, nd_line(node), putobject, node->nd_lit);

  • ADD_INSN1(ret, nd_line(node), putobject, rb_obj_freeze(node->nd_lit));

  while (list) {
    COMPILE(ret, "each string", list->nd_head);
    @@ -2236,6 +2236,7 @@
    rb_ary_push(ary, node->nd_head->nd_lit);
    node = node->nd_next;
```

████████████████████

@@ -2708,7 +2709,7 @@

$$\left. \begin{array}{l} \\ \end{array} \right\} @@ -4353,7 +4354,7 @@$$

```
@@ -4367,7 +4368,7 @@
}
```

```

• ADD_INSN1(ret, nd_line(node), putobject, node->nd_lit);
• ADD_INSN1(ret, nd_line(node), putobject, rb_obj_freeze(node->nd_lit));
  ADD_CALL(ret, nd_line(node), ID2SYM(idBackquote), INT2FIX(1));

  if (popped) {

```

Related issues:		
Related to Ruby - Bug #2965: method `===` called on hidden T_STRING object (N...	Closed	03/15/2010

#1 - 02/11/2009 04:21 AM - ko1 (Koichi Sasada)

Yusuke ENDOH wrote::

```
##### Regexp ##### Immutable #####  
#####Regexp #####
```


- switch (BUILTIN_TYPE(v)) {

- ██████████
- ██████████
- ██████████

~~~~~

- ██████████
- }
- rb\_ary\_push(iseq->mark\_ary, v);
- }
- return COMPILE\_OK;

--  
// SASADA Koichi at atdot dot net

=end

#3 - 02/11/2009 04:12 PM - usa (Usaku NAKAMURA)

=begin  
~~~~~

In message "[[ruby-dev:37959](#)] [Bug:trunk] I can modify literals"
on Feb.11,2009 02:16:05, [mame@tsg.ne.jp](#) wrote:

~~~~~ freeze ~~~~~IRC ~

- freeze ~~~~~
- freeze ~~~ finalizer ~~~~~

~~~~~

~~~~~ frozen ~~~~~ finalizer  
~~~~~  
~~~~~ ObjectSpace ~~~~~ finalizer ~~~~~  
~~~~~  
~~~~~  
~~~~~  
~~~~~ (~~~~~  
~~~~~) ~~~~~

Index: gc.c

```
--- gc.c (revision 22185)
+++ gc.c (working copy)
@@ -2261,9 +2261,11 @@ static VALUE
undefine_final(VALUE os, VALUE obj)
{
  rb_objspace_t *objspace = &rb_objspace;

  • if (OBJ_FROZEN(obj)) rb_error_frozen("object");
    if (finalizer_table) {
      st_delete(finalizer_table, (st_data_t*)&obj, 0);
    }
  • FL_UNSET(obj, FL_FINALIZE);
    return obj;
  }

@@ -2283,6 +2285,7 @@ define_final(int argc, VALUE *argv, VALU
```

VALUE obj, block, table;

```
rb_scan_args(argc, argv, "11", &obj, &block);
```

- if (OBJ_FROZEN(obj)) rb_error_frozen("object");
if (argc == 1) {
block = rb_block_proc();
}

~~~~~

--

U.Nakamura [usa@garbagecollect.jp](mailto:usa@garbagecollect.jp)

=end

#### #4 - 02/11/2009 05:44 PM - matz (Yukihiro Matsumoto)

```
=begin  
~~~~~
```

In message "Re: [\[ruby-dev:37964\]](#) Re: [Bug:trunk] I can modify literals"  
on Wed, 11 Feb 2009 16:11:06 +0900, "U.Nakamura" [usa@garbagecollect.jp](mailto:usa@garbagecollect.jp) writes:

```
{~~~~~frozen~~~~~finalizer
~~~~~  
{~~~~~ObjectSpace~~~~~finalizer~~~~~  
~~~~~  
~~~~~  
~~~~~  
~~~~~(~~~~~  
{~~~~~
```

```
~~~~~...  
~~~~~
```

=end

#### #5 - 02/12/2009 10:36 AM - matz (Yukihiro Matsumoto)

```
=begin  
~~~~~
```

In message "Re: [\[ruby-dev:37959\]](#) [Bug:trunk] I can modify literals"  
on Wed, 11 Feb 2009 02:16:05 +0900, Yusuke ENDOH [mame@tsg.ne.jp](mailto:mame@tsg.ne.jp) writes:

```
{ObjectSpace ~~~~~
~~~~~
```

```
~~~~~ObjectSpace~~~~~  
~~~~~  
~~~~~
```

```
{~~~~~ freeze ~~~~~IRC ~
```

|

| - freeze ~~~~~

| - freeze ~~~~ finalizer ~~~~~

|

```
{~~~~~
```

```
~~~~~
```

- ObjectSpace~~~~~(~~~~~)
- ~~~~~(~~~~~)

```
~~~~~
```

....

```
~~~~~ObjectSpace~~~~~  
~~~~~  
~~~~~freeze~~~~~
```

```
~~~~~
```

=end

=begin  
~~~~~

At Thu, 12 Feb 2009 10:34:51 +0900,  
Yukihiro Matsumoto wrote in [\[ruby-dev:37969\]](#):

- ObjectSpace~~~~~(~~~~~)
- ~~~~~(~~~~)

~~~~~

....

~~~~~ObjectSpace~~~~~  
~~~~~  
~~~~~freeze~~~~~

freeze~~~~ObjectSpace~~~~~  
~~~~~String~~~~~  
rb\_str\_replace()~~~~intern.h~~~~~  
~~~~~

## Index: compile.c

--- compile.c (revision 22249)  
+++ compile.c (working copy)  
@@ -296,4 +296,5 @@ PRINTF\_ARGS(void ruby\_debug\_printf(const  
(name##body\_.last = &name##body\_.anchor, name = &name##body\_)

+#define hide\_obj(obj) (void)(RBASIC(obj)->klass = 0)

#include "optinsn.inc"  
@@ -2231,5 +2232,5 @@ compile\_array\_(rb\_iseq\_t \*iseq, LINK\_ANC  
if (opt\_p == Qtrue) {  
if (!popped) {

- [REDACTED]

- [REDACTED]  
node = node\_root;  
while (node) {

@@ -2710,4 +2711,5 @@ defined\_expr(rb\_iseq\_t \*iseq, LINK\_ANCHO  
if (needstr != Qfalse) {  
VALUE str = rb\_str\_new2(estr);

- [REDACTED]  
ADD\_INSN1(ret, nd\_line(node), putstring, str);  
iseq\_add\_mark\_object\_compile\_time(iseq, str);

@@ -4354,4 +4356,5 @@ iseq\_compile\_each(rb\_iseq\_t \*iseq, LINK\_  
debugp\_param("nd\_lit", node->nd\_lit);  
if (!popped) {

- [REDACTED]  
ADD\_INSN1(ret, nd\_line(node), putstring, node->nd\_lit);

}  
Index: string.c

=====

--- string.c (revision 22249)  
+++ string.c (working copy)  
@@ -816,6 +816,4 @@ rb\_obj\_as\_string(VALUE obj)  
}

-static VALUE rb\_str\_replace(VALUE, VALUE);

VALUE

```
rb_str_dup(VALUE str)
@@ -3723,5 +3721,5 @@ rb_str_gsub(int argc, VALUE *argv, VALUE
*/
```

**-static VALUE**

**+VALUE**

**rb\_str\_replace(VALUE str, VALUE str2)**

**{**

**Index: insns.def**

```
--- insns.def (revision 22249)
+++ insns.def (working copy)
@@ -374,5 +374,6 @@ putstring
(VALUE val)
{
```

- val = rb\_str\_new3(str);
- VALUE rb\_str\_replace(VALUE, VALUE);
- val = rb\_str\_replace(rb\_str\_new(0, 0), str);

```
@@ -461,5 +462,5 @@ duparray
(VALUE val)
{
```

- val = rb\_ary\_dup(ary);
- val = rb\_ary\_replace(rb\_ary\_new2(0), ary);

**Index: include/ruby/intern.h**

```
--- include/ruby/intern.h (revision 22249)
+++ include/ruby/intern.h (working copy)
@@ -618,4 +618,5 @@ VALUE rb_str_equal(VALUE str1, VALUE str
VALUE rb_str_drop_bytes(VALUE, long);
void rb_str_update(VALUE, long, long, VALUE);
+VALUE rb_str_replace(VALUE, VALUE);
VALUE rb_str_inspect(VALUE);
VALUE rb_str_dump(VALUE);
```

```
--
--- Bug
--- Bug

```

=end

**#7 - 02/12/2009 04:55 PM - matz (Yukihiro Matsumoto)**

```
=begin

```

In message "Re: [\[ruby-dev:37971\]](#) Re: [Bug:trunk] I can modify literals"  
on Thu, 12 Feb 2009 11:35:16 +0900, Nobuyoshi Nakada [nobu@ruby-lang.org](mailto:nobu@ruby-lang.org) writes:

```
|freeze ObjectSpace
|String
|rb_str_replace()intern.h
|
```

```
freeze

```

=end

**#8 - 02/12/2009 07:47 PM - nobu (Nobuyoshi Nakada)**

- Status changed from Open to Closed

- % Done changed from 0 to 100

```
=begin
Applied in changeset r22255.
=end
```

#9 - 02/13/2009 05:05 AM - ko1 (Koichi Sasada)

```
=begin

```

Yukihiro Matsumoto wrote::

```
|freeze ObjectSpace
|String
|rb_str_replace()intern.h
|

freeze
freeze
```

```
freeze

```

```
--
// SASADA Koichi at atdot dot net
```

```
=end
```

#10 - 02/13/2009 06:18 AM - ko1 (Koichi Sasada)

```
=begin

```

```
rb_replace API
rb_from()

```

## Index: array.c

```
--- array.c (22272)
+++ array.c (22272)
@@ -1468,6 +1468,12 @@ rb_ary_dup(VALUE ary)
return dup;
}

+VALUE
+rb_ary_new_from(VALUE ary)
+{
+
+ • return rb_ary_new4(RARRAY_LEN(ary), RARRAY_PTR(ary));
+}

extern VALUE rb_output_fs;
```

## static VALUE

## Index: insns.def

```
--- insns.def (22272)
+++ insns.def (22272)
@@ -373,7 +373,7 @@ putstring
()
(VALUE val)
{
+
+ • val = rb_str_replace(rb_str_new(0, 0), str);
+
+ • val = rb_str_new_from(str);
+}


```

```
/**
@@ -460,7 +460,7 @@ duparray
()
(VALUE val)
{

 • val = rb_ary_replace(rb_ary_new2(0), ary);

 • val = rb_ary_new_from(ary);
}
```

```
/**
```

## Index: vm\_core.h

```
--- vm_core.h (000000 22272)
+++ vm_core.h (000000)
@@ -598,6 +598,9 @@ NOINLINE(void rb_gc_save_machine_context

#define sysstack_error GET_VM()->special_exceptions[ruby_error_sysstack]

+VALUE rb_str_new_from(VALUE str);
+VALUE rb_ary_new_from(VALUE ary);
+
/* for thread */
```

## #if RUBY\_VM\_THREAD\_MODEL == 2

## Index: iseq.c

```
--- iseq.c (000000 22272)
+++ iseq.c (000000)
@@ -704,7 +704,7 @@ insn_operand_intern(rb_iseq_t *iseq,
if (hidden_obj_p(op)) {
switch (BUILTIN_TYPE(op)) {
case T_STRING:

 • [REDACTED]

 • [REDACTED]
break;
case T_ARRAY:
op = rb_ary_replace(rb_ary_new2(0), op);
```

## Index: string.c

```
--- string.c (000000 22272)
+++ string.c (000000)
@@ -829,6 +829,11 @@ rb_str_dup(VALUE str)
return str_duplicate(rb_obj_class(str), str);
}

+VALUE
+rb_str_new_from(VALUE str)
+{

 • return rb_str_replace(str_alloc(rb_cString), str);
+}

/*

 • call-seq:

--
// SASADA Koichi at atdot dot net

=end

#11 - 02/13/2009 06:38 AM - ko1 (Koichi Sasada)

=begin
```

SASADA Koichi wrote::

Yukihiro Matsumoto wrote::

```
|freeze[]ObjectSpace[]String[]
|rb_str_replace()intern.h[]
|freeze[]

[]freeze[]
```

```
[] freeze []
[]
```

```
[] freeze []
[]
[] freeze []
```

```
--
// SASADA Koichi at atdot dot net

=end
```

#12 - 02/13/2009 08:05 AM - matz (Yukihiro Matsumoto)

```
=begin
[] []
```

In message "Re: [\[ruby-dev:37985\]](#) Re: [Bug:trunk] I can modify literals" on Fri, 13 Feb 2009 06:36:47 +0900, SASADA Koichi [ko1@atdot.net](mailto:ko1@atdot.net) writes:

```
|> [] freeze []
|> []
|
|[] freeze []
|[]
|[] freeze []

[]
[]freeze[]
[]
[]
```

```
=end
```