Ruby - Bug #19100

Ruby 3 PRNG values diverge from Ruby 2 for some initial values

11/02/2022 04:10 PM - mweitekamp (Monica Weitekamp)

Status:	Closed		
Priority:	Normal		
Assignee:	nobu (Nobuyoshi Nakada)		
Target version:			
ruby -v:	3.1.2	**Backport:**	2.7: UNKNOWN, 3.0: UNKNOWN, 3.1: UNKNOWN

Description

The outputs of the Mersenne Twister implementation diverged from their expected results in Ruby 2 for initial pseudo-random number generator seeds between 2^32 and 2^33-1, inclusive. I used ruby versions 2.7.4 vs. 3.0.3, 3.0.4, and 3.1.2 to compare.

```
ARBITRARY_RAND_MAX = 2**32

# The below three outputs should generate different outputs in ruby 2 and ruby 3
prng = Random.new(2**32)
puts prng.seed
puts prng.rand(ARBITRARY_RAND_MAX)

prng2 = Random.new(2**33-1)
puts prng2.seed
puts prng2.rand(ARBITRARY_RAND_MAX)

prng3 = Random.new((2**32 + 2**33-1) / 2)
puts prng3.seed
puts prng3.rand(ARBITRARY_RAND_MAX)

# These next two examples should generate the same outputs in ruby 2 and ruby 3
prng4 = Random.new(2**32 - 1)
puts prng4.seed
puts prng4.rand(ARBITRARY_RAND_MAX)

prng5 = Random.new(2**33)
puts prng5.seed
puts prng5.rand(ARBITRARY_RAND_MAX)
```

Associated revisions

Revision b7e8876704648cee6866591ac1aca7a54faff742 - 11/10/2022 03:06 AM - nobu (Nobuyoshi Nakada)

[Bug #19100] Add init_int32 function to rb_random_interface_t

Distinguish initialization by single word from initialization by
array.

Revision b7e8876704648cee6866591ac1aca7a54faff742 - 11/10/2022 03:06 AM - nobu (Nobuyoshi Nakada)

[Bug #19100] Add init_int32 function to rb_random_interface_t

Distinguish initialization by single word from initialization by
array.

Revision b7e88767 - 11/10/2022 03:06 AM - nobu (Nobuyoshi Nakada)

[Bug #19100] Add init_int32 function to rb_random_interface_t

Distinguish initialization by single word from initialization by
array.

Revision bab8051d2d20a13f4aa26330a25e72ccec980f7a - 11/10/2022 04:56 PM - nobu (Nobuyoshi Nakada)

[Bug #19100] [DOC] Add NEWS about PRNG update and incompatiblity

Revision bab8051d2d20a13f4aa26330a25e72ccec980f7a - 11/10/2022 04:56 PM - nobu (Nobuyoshi Nakada)

[Bug #19100] [DOC] Add NEWS about PRNG update and incompatiblity

Revision bab8051d - 11/10/2022 04:56 PM - nobu (Nobuyoshi Nakada)

[Bug #19100] [DOC] Add NEWS about PRNG update and incompatiblity

History

#1 - 11/07/2022 07:41 AM - shyouhei (Shyouhei Urabe)

- Status changed from Open to Assigned

- Assignee set to nobu (Nobuyoshi Nakada)

Can confirm, and my git bisect shows that this was introduced in af5e87ab218c5f4e34c6cdb54ae119a7f0f9033f. @nobu (Nobuyoshi Nakada) can you take a look?

#2 - 11/09/2022 10:48 AM - nobu (Nobuyoshi Nakada)

This is a mistake on the interface.
The cause is MT initialization by single word is not distinguished from initialization by array now.
In other words, leading-zero-guard is just stripped but ignored.

Another initializer function is needed to fix this issue, but just adding it will break the binary compatibility.

This patch adds versioning to rb_random_interface_t and function member for initialization by single word.

#3 - 11/10/2022 08:39 AM - nobu (Nobuyoshi Nakada)

- Status changed from Assigned to Closed

Applied in changeset git|b7e8876704648cee6866591ac1aca7a54faff742.

[Bug #19100] Add init_int32 function to rb_random_interface_t

Distinguish initialization by single word from initialization by
array.