Ruby master - Bug #8624

illegal hardware instruction in csv test

07/11/2013 11:51 PM - akr (Akira Tanaka)

Status:	Closed		
Priority:	Normal		
Assignee:			
Target version:			
ruby -v:	ruby 2.1.0dev (2013-07-11 trunk 41923) [x86_64-linux]	**Backport:**	1.9.3: UNKNOWN, 2.0.0: UNKNOWN

Description

□□□□□□ illegal hardware instruction □□□□□□□□□□□□□□

% ./ruby -v
ruby 2.1.0dev (2013-07-11 trunk 41923) [x86_64-linux]
% ./ruby ../../ruby/test/runner.rb ../../ruby/test/csv
Run options:

Running tests:

[36/302] TestCSV::Encodings#test_can_write_csv_in_any_encoding
zsh: illegal hardware instruction ./ruby ../../ruby/test/runner.rb ../../ruby/test/csv

□□□□□□ clang □□□

% clang -v
clang version 3.3 (tags/RELEASE_33/final)
Target: x86_64-unknown-linux-gnu
Thread model: posix

valgrind □□□□□□□□□□□□□□□□□□□□

==21333== Memcheck, a memory error detector
==21333== Copyright (C) 2002-2011, and GNU GPL'd, by Julian Seward et al.
==21333== Using Valgrind-3.7.0 and LibVEX; rerun with -h for copyright info
==21333== Command: ./ruby ../../ruby/test/runner.rb ../../ruby/test/csv
==21333== Parent PID: 16519
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==   at 0x9135EF3: utf16be_mbc_to_code (utf_16be.c:112)
==21333==   by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==   by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==   by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==   by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==   by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==   by 0x324FF0: str_encode (transcode.c:2873)
==21333==   by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==   by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==   by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==   by 0x37216C: vm_exec_core (insns.def:1017)
==21333==   by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==   at 0x3BDC27: rb_enc_ascget (encoding.c:958)
==21333==   by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==   by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==   by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==   by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==   by 0x324FF0: str_encode (transcode.c:2873)
==21333==   by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==   by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)

```
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==    by 0x389A4D: invoke_block_from_c (vm.c:646)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x2A9DC7: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==    by 0x389A4D: invoke_block_from_c (vm.c:646)
==21333==    by 0x38DF29: vm_yield (vm.c:677)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9B56BC3: utf16le_mbc_enc_len (utf_16le.c:64)
==21333==    by 0x3BDA52: rb_enc_precise_mbclen (encoding.c:935)
==21333==    by 0x3BDBD2: rb_enc_ascget (encoding.c:954)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9B56D53: utf16le_mbc_to_code (utf_16le.c:102)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9B56E14: utf16le_mbc_to_code (utf_16le.c:107)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9B56E37: utf16le_mbc_to_code (utf_16le.c:107)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
```

```
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9D58C4D: utf32be_mbc_to_code (utf_32be.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9D58C6A: utf32be_mbc_to_code (utf_32be.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9D58C8E: utf32be_mbc_to_code (utf_32be.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9D58CAB: utf32be_mbc_to_code (utf_32be.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9D58CCF: utf32be_mbc_to_code (utf_32be.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
```

```
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9F5AC2A: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9F5AC4E: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9F5AC6B: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9F5AC8F: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
```

```
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9F5ACAC: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== Conditional jump or move depends on uninitialised value(s)
==21333==    at 0x9F5ACCF: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
vex amd64->IR: unhandled instruction bytes: 0xF 0xB 0x48 0x8B 0x45 0xF8 0xF 0xB6
==21333== valgrind: Unrecognised instruction at address 0x9f5acb2.
==21333==    at 0x9F5ACB2: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==    by 0x389A4D: invoke_block_from_c (vm.c:646)
==21333==    by 0x38DF29: vm_yield (vm.c:677)
==21333==    by 0x37FCA2: rb_yield_0 (vm_eval.c:937)
==21333==    by 0x37FC64: rb_yield (vm_eval.c:947)
==21333==    by 0x3E6C7D: rb_ary_collect (array.c:2553)
==21333==    by 0x3907F2: call_cfunc_0 (vm_insnhelper.c:1354)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x371FFA: vm_exec_core (insns.def:1002)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==    by 0x38EF2B: vm_call0_body (vm_eval.c:170)
==21333==    by 0x37E5C2: vm_call0 (vm_eval.c:49)
==21333==    by 0x38E29D: rb_call0 (vm_eval.c:324)
==21333==    by 0x37F597: rb_call (vm_eval.c:585)
==21333==    by 0x37C600: rb_funcallv (vm_eval.c:807)
==21333==    by 0x131296: rb_obj_call_init (eval.c:1286)
==21333==    by 0x1B666F: rb_class_new_instance (object.c:1817)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==    by 0x389A4D: invoke_block_from_c (vm.c:646)
==21333==    by 0x38DF29: vm_yield (vm.c:677)
==21333==    by 0x37FCA2: rb_yield_0 (vm_eval.c:937)
```

```
==21333==    by 0x37FC64: rb_yield (vm_eval.c:947)
==21333==    by 0x3CE12A: rb_ary_each (array.c:1700)
==21333==    by 0x3907F2: call_cfunc_0 (vm_insnhelper.c:1354)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x371FFA: vm_exec_core (insns.def:1002)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==    by 0x389A4D: invoke_block_from_c (vm.c:646)
==21333==    by 0x38DF29: vm_yield (vm.c:677)
==21333==    by 0x37FCA2: rb_yield_0 (vm_eval.c:937)
==21333==    by 0x37FC64: rb_yield (vm_eval.c:947)
==21333==    by 0x3E6C7D: rb_ary_collect (array.c:2553)
==21333==    by 0x3907F2: call_cfunc_0 (vm_insnhelper.c:1354)
==21333== Your program just tried to execute an instruction that Valgrind
==21333== did not recognise.  There are two possible reasons for this.
==21333== 1. Your program has a bug and erroneously jumped to a non-code
==21333==    location.  If you are running Memcheck and you just saw a
==21333==    warning about a bad jump, it's probably your program's fault.
==21333== 2. The instruction is legitimate but Valgrind doesn't handle it,
==21333==    i.e. it's Valgrind's fault.  If you think this is the case or
==21333==    you are not sure, please let us know and we'll try to fix it.
==21333== Either way, Valgrind will now raise a SIGILL signal which will
==21333== probably kill your program.
==21333==
==21333== Process terminating with default action of signal 4 (SIGILL)
==21333==  Illegal opcode at address 0x9F5ACB2
==21333==    at 0x9F5ACB2: utf32le_mbc_to_code (utf_32le.c:62)
==21333==    by 0x3BDC1C: rb_enc_ascget (encoding.c:957)
==21333==    by 0x2A9DC1: str_fill_term (string.c:1508)
==21333==    by 0x2AA226: rb_str_fill_terminator (string.c:1549)
==21333==    by 0x32A661: str_encode_associate (transcode.c:2763)
==21333==    by 0x3234CA: encoded_dup (transcode.c:2898)
==21333==    by 0x324FF0: str_encode (transcode.c:2873)
==21333==    by 0x3907C9: call_cfunc_m1 (vm_insnhelper.c:1348)
==21333==    by 0x3965D3: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==21333==    by 0x394DD4: vm_call_cfunc (vm_insnhelper.c:1582)
==21333==    by 0x37216C: vm_exec_core (insns.def:1017)
==21333==    by 0x383A6F: vm_exec (vm.c:1198)
==21333==
==21333== HEAP SUMMARY:
==21333==     in use at exit: 13,054,473 bytes in 64,423 blocks
==21333==   total heap usage: 332,942 allocs, 268,519 frees, 132,063,934 bytes allocated
==21333==
==21333== LEAK SUMMARY:
==21333==    definitely lost: 264 bytes in 1 blocks
==21333==    indirectly lost: 1,057 bytes in 32 blocks
==21333==      possibly lost: 272 bytes in 1 blocks
==21333==    still reachable: 13,052,880 bytes in 64,389 blocks
==21333==         suppressed: 0 bytes in 0 blocks
==21333== Rerun with --leak-check=full to see details of leaked memory
==21333==
==21333== For counts of detected and suppressed errors, rerun with: -v
==21333== Use --track-origins=yes to see where uninitialised values come from
==21333== ERROR SUMMARY: 5292 errors from 18 contexts (suppressed: 4 from 4)
```

□□□□□□gcc □□□□□□□□□□□□□□□□

gcc □□□valgrind □□□□□□□□□□□□□□□□□□□

```
dew(23:18:29)% valgrind ./ruby test/runner.rb test/csv
==16910== Memcheck, a memory error detector
==16910== Copyright (C) 2002-2010, and GNU GPL'd, by Julian Seward et al.
==16910== Using Valgrind-3.6.0.SVN-Debian and LibVEX; rerun with -h for copyright info
==16910== Command: ./ruby test/runner.rb test/csv
==16910==
Run options:
```

Running tests:

[33/302] TestCSV::Encodings#test_auto_line_ending_detection==16910== Conditional jump or move depends on uninitialised value(s)
==16910== at 0x2887E7: rb_enc_ascget (encoding.c:958)
==16910== by 0x1FC905: str_fill_term (string.c:1508)
==16910== by 0x1FCBD5: rb_str_fill_terminator (string.c:1549)
==16910== by 0x22979B: str_encode_associate (transcode.c:2763)
==16910== by 0x229ADA: encoded_dup (transcode.c:2898)
==16910== by 0x2299C5: str_encode (transcode.c:2873)
==16910== by 0x258616: call_cfunc_m1 (vm_insnhelper.c:1348)
==16910== by 0x259206: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==16910== by 0x259340: vm_call_cfunc (vm_insnhelper.c:1582)
==16910== by 0x25DFE8: vm_exec_core (insns.def:1017)
==16910== by 0x26D3E0: vm_exec (vm.c:1198)
==16910== by 0x26BE91: invoke_block_from_c (vm.c:646)
==16910==
==16910== Conditional jump or move depends on uninitialised value(s)
==16910== at 0x1FC908: str_fill_term (string.c:1508)
==16910== by 0x1FCBD5: rb_str_fill_terminator (string.c:1549)
==16910== by 0x22979B: str_encode_associate (transcode.c:2763)
==16910== by 0x229ADA: encoded_dup (transcode.c:2898)
==16910== by 0x2299C5: str_encode (transcode.c:2873)
==16910== by 0x258616: call_cfunc_m1 (vm_insnhelper.c:1348)
==16910== by 0x259206: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==16910== by 0x259340: vm_call_cfunc (vm_insnhelper.c:1582)
==16910== by 0x25DFE8: vm_exec_core (insns.def:1017)
==16910== by 0x26D3E0: vm_exec (vm.c:1198)
==16910== by 0x26BE91: invoke_block_from_c (vm.c:646)
==16910== by 0x26BFD6: vm_yield (vm.c:677)
==16910==
[36/302] TestCSV::Encodings#test_can_write_csv_in_any_encoding==16910== Conditional jump or move depends on uninitialised value(s)
==16910== at 0x9164A58: utf16le_mbc_enc_len (utf_16le.c:64)
==16910== by 0x2886E9: rb_enc_precise_mbclen (encoding.c:935)
==16910== by 0x2887B3: rb_enc_ascget (encoding.c:954)
==16910== by 0x1FC905: str_fill_term (string.c:1508)
==16910== by 0x1FCBD5: rb_str_fill_terminator (string.c:1549)
==16910== by 0x22979B: str_encode_associate (transcode.c:2763)
==16910== by 0x229ADA: encoded_dup (transcode.c:2898)
==16910== by 0x2299C5: str_encode (transcode.c:2873)
==16910== by 0x258616: call_cfunc_m1 (vm_insnhelper.c:1348)
==16910== by 0x259206: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==16910== by 0x259340: vm_call_cfunc (vm_insnhelper.c:1582)
==16910== by 0x25DFE8: vm_exec_core (insns.def:1017)
==16910==
==16910== Conditional jump or move depends on uninitialised value(s)
==16910== at 0x9164B27: utf16le_mbc_to_code (utf_16le.c:102)
==16910== by 0x2887DF: rb_enc_ascget (encoding.c:957)
==16910== by 0x1FC905: str_fill_term (string.c:1508)
==16910== by 0x1FCBD5: rb_str_fill_terminator (string.c:1549)
==16910== by 0x22979B: str_encode_associate (transcode.c:2763)
==16910== by 0x229ADA: encoded_dup (transcode.c:2898)
==16910== by 0x2299C5: str_encode (transcode.c:2873)
==16910== by 0x258616: call_cfunc_m1 (vm_insnhelper.c:1348)
==16910== by 0x259206: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==16910== by 0x259340: vm_call_cfunc (vm_insnhelper.c:1582)
==16910== by 0x25DFE8: vm_exec_core (insns.def:1017)
==16910== by 0x26D3E0: vm_exec (vm.c:1198)
==16910==
[54/302] TestCSV::Encodings::DifferentOFS#test_can_write_csv_in_any_encoding==16910== Conditional jump or move depends on uninitialised value(s)
==16910== at 0x9164A6F: utf16le_mbc_enc_len (utf_16le.c:67)
==16910== by 0x2886E9: rb_enc_precise_mbclen (encoding.c:935)
==16910== by 0x2887B3: rb_enc_ascget (encoding.c:954)
==16910== by 0x1FC905: str_fill_term (string.c:1508)

```
==16910==    by 0x1FCBD5: rb_str_fill_terminator (string.c:1549)
==16910==    by 0x22979B: str_encode_associate (transcode.c:2763)
==16910==    by 0x229ADA: encoded_dup (transcode.c:2898)
==16910==    by 0x2299C5: str_encode (transcode.c:2873)
==16910==    by 0x258616: call_cfunc_m1 (vm_insnhelper.c:1348)
==16910==    by 0x259206: vm_call_cfunc_with_frame (vm_insnhelper.c:1492)
==16910==    by 0x259340: vm_call_cfunc (vm_insnhelper.c:1582)
==16910==    by 0x25DFE8: vm_exec_core (insns.def:1017)
==16910==
[150/302] TestCSV::Interface#test_enumerators_are_supported==16910== Warning: client switching stacks?  SP change:
0x7feffbfd8 --> 0x40b5fe8
==16910==          to suppress, use: --max-stackframe=34275090416 or greater
==16910== Warning: client switching stacks?  SP change: 0x40b3f88 --> 0x7feffbfe0
==16910==          to suppress, use: --max-stackframe=34275098712 or greater
[171/302] TestCSV::Interface::DifferentOFS#test_enumerators_are_supported==16910== Warning: client switching stacks?  SP
change: 0x7feffbea8 --> 0x4135fe8
==16910==          to suppress, use: --max-stackframe=34274565824 or greater
==16910==          further instances of this message will not be shown.
Finished tests in 55.632943s, 5.4284 tests/s, 141.5348 assertions/s.

302 tests, 7874 assertions, 0 failures, 0 errors, 0 skips

ruby -v: ruby 2.1.0dev (2013-07-11 trunk 41923) [x86_64-linux]
==16910==
==16910== HEAP SUMMARY:
==16910==     in use at exit: 5,802,437 bytes in 49,345 blocks
==16910==   total heap usage: 846,278 allocs, 796,933 frees, 401,745,300 bytes allocated
==16910==
==16910== LEAK SUMMARY:
==16910==    definitely lost: 1,444,516 bytes in 9,335 blocks
==16910==    indirectly lost: 2,525,593 bytes in 26,492 blocks
==16910==      possibly lost: 0 bytes in 0 blocks
==16910==    still reachable: 1,832,328 bytes in 13,518 blocks
==16910==         suppressed: 0 bytes in 0 blocks
==16910== Rerun with --leak-check=full to see details of leaked memory
==16910==
==16910== For counts of detected and suppressed errors, rerun with: -v
==16910== Use --track-origins=yes to see where uninitialised values come from
==16910== ERROR SUMMARY: 4703 errors from 5 contexts (suppressed: 4 from 4)
```

Associated revisions

Revision 8b8cce32 - 07/12/2013 07:28 AM - nobu (Nobuyoshi Nakada)

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

git-svn-id: svn+ssh://ci.ruby-lang.org/ruby/trunk@41930 b2dd03c8-39d4-4d8f-98ff-823fe69b080e

Revision 41930 - 07/12/2013 07:28 AM - nobu (Nobuyoshi Nakada)

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

Revision 41930 - 07/12/2013 07:28 AM - nobu (Nobuyoshi Nakada)

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

Revision 41930 - 07/12/2013 07:28 AM - nobu (Nobuyoshi Nakada)

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

Revision 41930 - 07/12/2013 07:28 AM - nobu (Nobuyoshi Nakada)

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

Revision 41930 - 07/12/2013 07:28 AM - nobu (Nobuyoshi Nakada)

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

Revision 41930 - 07/12/2013 07:28 AM - nobu (Nobuyoshi Nakada)

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

History

#1 - 07/12/2013 04:28 PM - nobu (Nobuyoshi Nakada)

- Status changed from Open to Closed

- % Done changed from 0 to 100

This issue was solved with changeset r41930.
Akira, thank you for reporting this issue.
Your contribution to Ruby is greatly appreciated.
May Ruby be with you.

---

encoding.c: refill terminator at associating encoding

- encoding.c (rb_enc_associate_index): refill the terminator if it becomes longer than before. [ruby-dev:47500] [Bug #8624]
- string.c (str_null_char, str_fill_term): get rid of out of bound access.
- string.c (rb_str_fill_terminator): add a parameter for the length of new terminator.

#2 - 07/12/2013 04:34 PM - nobu (Nobuyoshi Nakada)

□□□x86_64-linux□□□□□illegal hardware instruction□□□□□□
valgrind□□□□□□□□x86_64-darwn□□valgrind□□□□□□□□□□
illegal hardware instruction□□□□□□□□□□

□□□□□□valgrind□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□reopen□□□□□□□

#3 - 07/12/2013 06:53 PM - akr (Akira Tanaka)

2013/7/12 nobu (Nobuyoshi Nakada) nobu@ruby-lang.org:

> □□□x86_64-linux□□□□□illegal hardware instruction□□□□□□
> valgrind□□□□□□□□x86_64-darwn□□valgrind□□□□□□□□□□
> illegal hardware instruction□□□□□□□□□□
>
> □□□□□□valgrind□□□□□□□□□□□□□□□□□□□□□□□□□□□□
> □□reopen□□□□□□□

r41931 □□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□
--
[□□ □][□□□ □□□][Tanaka Akira]