DESCRIPTION an...@gmail.com created issue #1

The `Test.java` in the enclosed archive crashed ART with the following log:

```
03-30 14:10:22.998  6199  6199 F libc    : Fatal signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x412cffbe0 in tid 6199 (main), pid 6199 (main)
03-30 14:10:23.372  6213  6213 F DEBUG   : *** *** *** *** *** *** *** *** *** *** *** *** *** *** *** ***
03-30 14:10:23.372  6213  6213 F DEBUG   : Build fingerprint: 'google/sdk_gphone64_x86_64/emu64xa:Tiramisu/TPP2.220218.008/8250781:userdebug/dev-keys'
03-30 14:10:23.372  6213  6213 F DEBUG   : Revision: '0'
03-30 14:10:23.372  6213  6213 F DEBUG   : ABI: 'x86_64'
03-30 14:10:23.372  6213  6213 F DEBUG   : Timestamp: 2022-03-30 14:10:23.044674221+0200
03-30 14:10:23.372  6213  6213 F DEBUG   : Process uptime: 6s
03-30 14:10:23.372  6213  6213 F DEBUG   : Cmdline: dalvikvm -cp /data/local/tmp/test.jar Test
03-30 14:10:23.372  6213  6213 F DEBUG   : pid: 6199, tid: 6199, name: main  >>> dalvikvm <<<
03-30 14:10:23.372  6213  6213 F DEBUG   : uid: 2000
03-30 14:10:23.372  6213  6213 F DEBUG   : signal 11 (SIGSEGV), code 1 (SEGV_MAPERR), fault addr 0x0000000412cffbe0
03-30 14:10:23.372  6213  6213 F DEBUG   :     rax 0000000012cffbd8  rbx 0000000012cffb78  rcx 00007b146b077010  rdx 00007ffca88b8d68
03-30 14:10:23.372  6213  6213 F DEBUG   :     r8  00007b1274c4a200  r9  0000000012cffc18  r10 00000000fffff800  r11 00007b150b304d58
03-30 14:10:23.372  6213  6213 F DEBUG   :     r12 0000000012d9d0c0  r13 0000000012e40348  r14 00000000ffffffff  r15 0000000000000000
03-30 14:10:23.373  6213  6213 F DEBUG   :     rdi 000000007031ce08  rsi 000000000000000c
03-30 14:10:23.373  6213  6213 F DEBUG   :     rbp 0000000012d9ca70  rsp 00007ffca88b8d60  rip 000000004337e309
03-30 14:10:23.373  6213  6213 F DEBUG   : backtrace:
03-30 14:10:23.373  6213  6213 F DEBUG   :       #00 pc 0000000002005309  /memfd:jit-cache (deleted) (Test.lMeth+1273)
03-30 14:10:23.373  6213  6213 F DEBUG   :       #01 pc 0000000000368c59  /apex/com.android.art/lib64/libart.so (nterp_helper+2153) (BuildId: f9c22944c82b378
03-30 14:10:23.373  6213  6213 F DEBUG   :       #02 pc 00000000000023e2  [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.v
03-30 14:10:23.373  6213  6213 F DEBUG   :       #03 pc 0000000002001ba9  /memfd:jit-cache (deleted) (Test.mainTest+329)
03-30 14:10:23.373  6213  6213 F DEBUG   :       #04 pc 00000000003692ed  /apex/com.android.art/lib64/libart.so (nterp_helper+3837) (BuildId: f9c22944c82b378
03-30 14:10:23.373  6213  6213 F DEBUG   :       #05 pc 0000000000001e1c  [anon:dalvik-classes.dex extracted in memory from /data/local/tmp/test.jar] (Test.m
03-30 14:10:23.373  6213  6213 F DEBUG   :       #06 pc 0000000000372016  /apex/com.android.art/lib64/libart.so (art_quick_invoke_static_stub+806) (BuildId:
03-30 14:10:23.373  6213  6213 F DEBUG   :       #07 pc 00000000003f1a49  /apex/com.android.art/lib64/libart.so (art::ArtMethod::Invoke(art::Thread*, unsigne
03-30 14:10:23.374  6213  6213 F DEBUG   :       #08 pc 00000000007e4fc1  /apex/com.android.art/lib64/libart.so (art::JValue art::InvokeWithVarArgs<art::ArtM
03-30 14:10:23.374  6213  6213 F DEBUG   :       #09 pc 0000000000644a74  /apex/com.android.art/lib64/libart.so (art::JNI<false>::CallStaticVoidMethodV(_JNIE
03-30 14:10:23.374  6213  6213 F DEBUG   :       #10 pc 0000000000002a84  /apex/com.android.art/bin/dalvikvm64 (_JNIEnv::CallStaticVoidMethod(_jclass*, _jmet
03-30 14:10:23.374  6213  6213 F DEBUG   :       #11 pc 000000000000271c  /apex/com.android.art/bin/dalvikvm64 (art::dalvikvm(int, char**)+2060) (BuildId: c4
03-30 14:10:23.374  6213  6213 F DEBUG   :       #12 pc 0000000000001ef5  /apex/com.android.art/bin/dalvikvm64 (main+5) (BuildId: c4b9abdc3d0244c2262af6c81d3
03-30 14:10:23.374  6213  6213 F DEBUG   :       #13 pc 00000000000505f9  /apex/com.android.runtime/lib64/bionic/libc.so (__libc_init+89) (BuildId: 4a49f5f71
```

Environment to reproduce the problem

Android Build: Tiramisu; TPP2.220218.008

```
$ adb shell getprop ro.system.build.id
TPP2.220218.008
```

Android Build Tools: bulid-tools;33.0.0-rc2

```
$ ./build-tools/33.0.0-rc2/d8 --version
D8 3.3.11-dev (build 5d015d7a69cc8b662b4f28a71ff2a4dfd5adc1bb from go/r8bot (luci-r8-custom-ci-xenial-13-fsvv))
```

HotSpot and OpenJDK: java-11-openjdk-amd64

```
$ java -version
openjdk version "11.0.14" 2022-01-18
OpenJDK Runtime Environment (build 11.0.14+9-Ubuntu-0ubuntu2.20.04)
OpenJDK 64-Bit Server VM (build 11.0.14+9-Ubuntu-0ubuntu2.20.04, mixed mode, sharing)
$ javac -version
javac 11.0.14
```

Please also check the following link for the bugreport (of `adb bugreport`): https://drive.google.com/file/d/1XX5-SOLxH0oK9qN2UC1jd_pCNlFpCp6a/view?usp=sharing

We have already shared the above bugreport with android-bugreport@google.com.

Steps to reproduce the problem (including sample code if appropriate)

> Note, `Test.class` and `test.jar` are precompiled using `javac` and `d8` as aforementioned

Push `test.jar` to the emulator

```
$ adb push test.jar /data/local/tmp/
```

Run in dalvikvm

```
$ adb shell dalvikvm -cp /data/local/tmp/test.jar Test
```

Check the return code

```
$ echo $?
139
```

What happened

ART crashed with return code 139

What you think the correct behavior should be

ART does not crash

deleted
0 B

✓ Links (2)

Links (2)

"Please also check the following link for the bugreport (of adb bugreport): https://drive.google.com/file/d/1XX5-SOLxH0oK9qN2UC1jd_pCNlFpCp6a/view?usp=sharing"
" https://android-review.googlesource.com/2041623 Fix last value generation in loop optimization."

COMMENTS

ad...@google.com <ad...@google.com>

Assigned to ad...@google.com.

ad...@google.com <ad...@google.com> #2

We have passed this to the development team and will update this issue with more information as it becomes available.

vm...@google.com <vm...@google.com> #3

Marked as fixed, reassigned to vm...@google.com.

The underlying issue was fixed by
https://android-review.googlesource.com/2041623 Fix last value generation in loop optimization.
The fix shall be available in Android 13 Beta 2 (to be released).