

Homework 9

Debugging

Due: Wednesday, November 15th, 11:59PM (Hard Deadline)

Submission Instructions

Submit this assignment on [Gradescope](#). You may find the free online tool [PDFescape](#) helpful to edit and fill out this PDF. You may also print, handwrite, and scan this assignment.

There may multiple answers for each question. If you are unsure, state your assumptions and your reasoning for why you think your answer makes sense.

1 Gitting started

Please clone the following repository:

```
> git clone https://github.com/c4cs/debugging-basics.git
```

This repository contains 4 branches: `master`, `gdb-debug-1`, `gdb-debug-2`, and `valgrind-debug`. Each part of this homework will take place on a different branch.

2 Finding primes

The repository you have cloned is an attempt at a program to find prime numbers. It will search from 3 up to a maximum number input by the user.

The program intends to follow the structure:

- o prompt user for upper bound
- o for N=3..upper bound:
 - check if N is prime
 - * if no prime n between 1..sqrt(N) divides N, then prime
 - save whether N is prime for future loops to use
 - if N is prime, print N

2.1 Debugging with gdb

You may find it helpful to consult the [gdb lecture notes](#) or this [quick command reference](#).

First, make sure you are on the `gdb-debug-1` branch:

```
> git branch
  master
* gdb-debug-1
```

Next, build and run the supplied program:

```
> make
> ./prime
Find all prime numbers between 3 and ?
10
Segmentation fault (core dumped)
> gdb -q ./prime
Reading symbols from ./prime...done.
(gdb) run
Starting program: /media/sf_prime/prime
Find all prime numbers between 3 and ?
10

Program received signal SIGSEGV, Segmentation fault.
0x000000000040068f in check_prime (k=3) at check.c:15
15     if (is_prime[j] == 1)
```

Explain in what case(s) executing this line of code could cause a segmentation fault?

What gdb commands could you run next to prove your hypothesis right or wrong?

Now checkout gdb-debug-2:

```
> git checkout gdb-debug-2
> make
> ./prime
Find all prime numbers between 3 and ?
10
3 is a prime
5 is a prime
7 is a prime
9 is a prime
```

Copy your debugging session and add notes explaining your thought process as you track down why this program thinks 9 is a prime.

Hint: It looks like things go well up until 9. A good place to start then may be to break in and observe how the code determines whether 9 is a prime number.

This homework is based off of a simplified and updated version of this gdb tutorial: <http://heather.cs.ucdavis.edu/~matloff/UnixAndC/CLanguage/Debug.html> If you would like some more practice, or simply a slightly different explanation of the material, this may be a good source.

3 Valgrind

Valgrind is a different kind of debugging tool. It is essentially a type of virtual machine (like a simpler VirtualBox). Valgrind actually recompiles every assembly instruction to allow it to intercept and monitor all of the hardware calls made by the child process. While this is very powerful and gives valgrind a lot of insight, it is also very slow, which can be problematic for debugging large pieces of software.

Valgrind also can be challenging when libraries (such as the STL, or Boost) do funny things with memory that result in a large number of false warnings. We will look at valgrind in more depth during the second week on debugging tools. For today, let's just explore the basic functionality and check out the kind of things that valgrind can catch that gdb can't.

First, we'll need to install valgrind

```
> sudo apt-get install valgrind
```

Now, checkout the valgrind branch

```
> git checkout valgrind-debug
```

Notice (perhaps `gitk --all`) that the valgrind branch builds on the master branch, with all the compiler warnings turned on. It has also cherry-picked the fix "Stop searching for primes once \sqrt{k} is reached", that is the same commit object that managed to end up on two different histories. This is one example of how git can be both very powerful, and very confusing.

Finally, this branch adds a commit that consolidates they two source code files into one and gets rid of all of the global variables in the process. Unfortunately, this refactoring may also have inroduced a bug.

We run valgrind very similarly to gdb:

```
> make
> valgrind ./prime
==11959== Memcheck, a memory error detector
==11959== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==11959== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==11959== Command: ./prime
==11959==
Find all prime numbers between 3 and ?
10
3 is a prime
==11959== Conditional jump or move depends on uninitialised value(s)
==11959==    at 0x400683: check_prime (prime.c:32)
==11959==    by 0x400739: main (prime.c:52)
==11959==
5 is a prime
7 is a prime
==11959==
==11959== HEAP SUMMARY:
==11959==    in use at exit: 0 bytes in 0 blocks
==11959== total heap usage: 0 allocs, 0 frees, 0 bytes allocated
==11959==
==11959== All heap blocks were freed -- no leaks are possible
==11959==
==11959== For counts of detected and suppressed errors, rerun with: -v
==11959== Use --track-origins=yes to see where uninitialised values come from
==11959== ERROR SUMMARY: 3 errors from 1 contexts (suppressed: 0 from 0)
```

(The numbers in the left column are the process ID. They will be different for every person)

Notice that “3 is a prime” printed before this warning. Why was this warning not emitted when running `check_prime(3, ...)`?

These tools really get powerful when you combine them. We can run valgrind in a way that lets gdb connect to it, and allows us to debug/inspect whenever valgrind detects a problem:

```
> valgrind --vgdb=yes --vgdb-error=0 ./prime
```

In another terminal, follow the directions that valgrind prints to connect gdb. In this case, valgrind has already ‘run’ the program for you and inserted a breakpoint at the very beginning of the program, we just need to ‘continue’ it. The program will run until valgrind encounters an issue, at which point valgrind will automatically break for you.

```
(gdb) continue
```

```
valgrind terminal:
```

```
==23589== Conditional jump or move depends on uninitialised value(s)
==23589==    at 0x400623: check_prime (prime.c:32)
==23589==    by 0x4006C4: main (prime.c:52)
==23589==
==23589== (action on error) vgdb me ... # this is where valgrind waits for gdb
```

```
gdb terminal:
```

```
Program received signal SIGTRAP, Trace/breakpoint trap.
0x000000000400623 in check_prime (k=5, is_prime=0xffefff910) at prime.c:32
32      if (is_prime[j] == 1) # this is the problematic line of code
```

What is the value of `j` at this point?

What is the value of `is_prime[j]` at the point?

Use git to look at the most recent commit. What line of code was deleted that should not have been?