15-122: Principles of Imperative Computation

Recitation 12a — Josh Zimmerman

modpow_one

Let's consider the function `modpow_one(a, b, c)` which computes (a^b) % c. This function has many practical applications, including being a key part of the RSA cryptography algorithm.

```
1  int modpow_one(int a, int b, int c)
2  //@requires a >= 0 && b >= 0 && c > 0;
3  //@requires c - 1 <= int_max()/max(a, c - 1);
4  //@ensures 0 <= \result && \result < c;
5  {
6     int res = 1 % c;
7     while (b > 0)
8     //@loop_invariant 0 <= res && res < c;
9     {
10       res *= a;
11       res = res % c;
12       b--;
13    }
14    return res;
15 }
```

Prove that this function satisfies its postcondition.

modpow_two

Now we'll look at a different implementation, `modpow_two`.

```
1  int modpow_two(int a, int b, int c)
2  //@requires a >= 0 && b >= 0 && c > 0;
3  //@requires (c - 1) <= int_max()/max(a, c - 1);
4  //@ensures \result == modpow_one(a, b, c);
5  {
6     int res = 1 % c;
7     int pow = 0;
8     while (pow < b)
9
10    ____________________________________________
11
12    ____________________________________________
13    {
14       if (0 < pow && pow <= b/2) {
15          res *= res;
16          res = res % c;
17          pow *= 2;
18       }
19       else {
20          res *= a;
21          res = res % c;
22          pow++;
23       }
24    }
25    return res;
26 }
```

Is this function asymptotically faster than, slower than, or the same speed as `modpow_one`? Explain.

Write loop invariants for `modpow_two`.

Now, prove that if the preconditions to `modpow_two` are satisfied, it satisfies its postcondition.

If it helps, you can assume that $0^0 = 0$, even though it's actually indeterminate. You can also assume that `modpow_one` obeys the properties that
`(modpow_one(a, b, c) * a) % c == modpow_one(a, b + 1, c)` and
`(modpow_one(a, b, c) * modpow_one(a, b, c)) % c == modpow_one(a, 2*b, c)`

Questions?

If you have any more questions and we're not out of time, ask them now. There will also be a review session on Sunday at 5pm in Rashid Auditorium (GHC 4401) if you have more questions or you want a review of some specific topic.

Exam details

The midterm is on Tuesday, during the normal lecture time (9:00-10:20). Make sure to bring a photo ID with you to the exam. Follow the list below to determine where to go on the morning of the exam.
– Recitations A-E: GHC (Gates-Hillman Center) 4401 (Rashid), the usual lecture room
– Recitation F (All of it), G (Last name A-Q): NSH (Newell-Simon Hall) 3305
– Recitation G (Last name R-Z), H (All of it): NSH (Newell-Simon Hall) 1507