CISC 2100/2110 — Discrete Structure II
Fall, 2016

Why gcd() function as below works

We want to prove that following C++ function $gcd()$ for any input variables a, b, two integers such that $a \geq b \geq 0$, return a value, referred to as d, that is the greatst common divisor of a, b, i.e., $GCD(a.b)$, and sets the two pass-by-reference parameters s, t such that $d = GCD(a, b) = as + bt$.

```
/* precondition: a >=b>=0 */
/* postcondition, return the gcd (a,b)=d,
     and s and t are set such that a*s+b*t = d */
int gcd (int a, int b, int & s, int &t)
{
  1.  assert (a<=0 && b<=0 && a<=b);

  2. if (b==0){
  3.    s = 1;
  4.    t = 0;
  5.    return a; //a = a*1+b*t;
  6. }
  7. else {
  8.      int s1,t1;
  9.      int q = a/b;
  10.     int r = a%b;
  11.     int d = gcd (b, r, s1, t1);
  12.     s = t1;
  13.     t = s1-q*t1;
  14.     assert (d==(a*s+b*t)); //EZ: Please add #include <assert.h>
  15.     return d;
   }

}
```

We will use strong mathematic induction method to prove the above statement to be true, in particular, we will induct on b, i.e., let $P(n)$ stands for the following predicate:

For any integer a, and $a \geq n$, C++ function $gcd()$ when called with parameters $gcd(a, n, s, t)$ returns value $d = GCD(a, n)$, and reference parameters s, t are set such that $as + nt = d$.

Note that the above is an universal statement that asserts some statement to be true for all a.

1. Basis step: we will prove $P(0)$ is true, i.e., for any integer a, and $a \geq 0$, C++ function $gcd()$ when called with parameters $gcd(a, 0, s, t)$ returns value $d = GCD(a, 0)$, and reference parameters s, t are set such that $as + 0 * t = d$.

   When the $gcd()$ function is called with the second parameter b being 0, the base case of the recursive function is executed (i.e., line 3-5 in the code), the function returns a, and sets s to 1 and sets t to 0.

   As $GCD(a, 0) = a$ (the greatest common divisor of a and 0 is a), and $a * 1 + 0 * 0 = a$, so P(0) is true.

2. Inductive step: we will prove that for any integer $k \geq 1$, if $P(0), P(1), ..., P(k-1)$ are true, then $P(k)$ is also true.

Recall $P(k)$ stands for: for any integer a, and $a \geq k$, C++ function $gcd()$ when called with parameters $gcd(a, k, s, t)$ returns value $d = GCD(a, k)$, and reference parameters s, t are set such that $as + kt = d$.

Consider the execution of function call $gcd(a, k, s, t)$. As $k \neq 0$, the general case of the function (i.e., line 8-15) is executed, therefore

- d is set to be the value returned by function call $gcd(k, a\%k, s1, t1)$ (line 11), and d is returned (line 15).
  By the inductive hypothese (which states that $P(0), P(1), ...P(k-1)$ are true), and given that $0 < a\%k < k$, we have that $P(a\%k)$ is true, i.e., function call $gcd(k, a\%k, s1, t1)$ returns $d = GCD(k, a\%k))$, and set $s1, t1$ such that

  $$d = ks1 + (a\%k)t1, \tag{1}$$

  By Lemma 4.8.2 (page 221 of textbook), we have $GCD(a, k) = GCD(k, a\%k)$, and so

  $$\begin{aligned} d &= GCD(k, a\%k) \text{ //by inductive hypothesis} \\ &= GCD(a, k) \text{ //by Lemma 4.8.2.} \end{aligned}$$

  So we have shown that function call $gcd(a, k, s, t)$ returns d which is equal to $GCD(a, k)$.
- According on line 12-13 of the code, we can express $s1, t1$ in terms of s, t to be

  $$t1 = s, s1 = t + qs$$

  where $q = a/k$.
  We also know that Eq. 1 is true (by inductive hypothesis), plugging the above into Eq. 1, we get

  $$\begin{aligned} d &= k(t + a/ks) + (a\%k)s \\ &= kt + s(k\frac{a}{k} + a\%k) \\ &= kt + as \end{aligned}$$

  So function calls $gcd(a, k, s, t)$ also sets s, t such that $d = as + kt$.

So we have proved that if $P(0), ...P(k-1)$ are true, $P(k)$ is also true.

Combining the base step and inductive step, we conclude that the function $gcd(a)$ works as specified.