COL100: Introduction to Computer Science

4.1: More examples of correctness analysis

Principle(s) of mathematical induction

Version 1: base case $P(0)$, induction step $P(n) \Rightarrow P(n+1)$ for all $n \geq 0$

Version 2: base case $P(k)$, induction step $P(n) \Rightarrow P(n+1)$ for all $n \geq k$

Version 3: base case $P(0)$, induction step $P(0),\ldots, P(n) \Rightarrow P(n+1)$ for all $n \geq 0$

All these versions are *equivalent*! From any version you can prove the other two

Correctness of *rem*

$$rem(n, d) = \begin{cases} n & \text{if } n < d, \\ rem(n - d, d) & \text{otherwise} \end{cases}$$

Prove that $rem(n, d)$ computes n mod d, the remainder when n is divided by d.
i.e. if $r = rem(n, d)$, then $0 \leq r < d$, and $n = qd + r$ for some $q \in \mathbb{N}$.

We will use induction…

- On which variable?
- Using which version of induction?

We will use induction (version 3) on n.

Base case: $n = 0$. Then $r = 0$, so $0 \leq r < d$ and $n = 0d + r$.

Induction hypothesis: For all $m < n$, if $r = rem(m, d)$ then $0 \leq r < d$ and $m = qd + r$ for some $q \in \mathbb{N}$.

Induction step:

If $n < d$, then $r = rem(n, d) = n$, so $0 \leq r < d$ and $n = 0d + r$.

If $n \geq d$, then $r = rem(n, d) = rem(n - d, d)$.
By I.H., we have $0 \leq r < d$ and $n - d = qd + r$ for some $q \in \mathbb{N}$.
So $n = (q + 1)d + r$.

Euclidean algorithm for GCD

Described by Euclid around 300 BC.

Naïve version:

$$gcd(a, b) = \begin{cases} a & \text{if } a = b, \\ gcd(a - b, b) & \text{if } a > b, \\ gcd(a, b - a) & \text{if } a < b. \end{cases}$$

$gcd(49, 21)$
$= gcd(28, 21)$
$= gcd(7, 21)$
$= gcd(7, 14)$
$= gcd(7, 7)$
$= 7$

Prove that this computes the GCD of any two natural numbers $a, b \geq 1$.

Proof by induction on… what?

Lemma: If $a > b$, then GCD(a, b) = GCD($a - b$, b).

Proof: Let g = GCD(a, b).

Then g is a divisor of both a and b, so it is also a divisor of $a - b$.

Suppose d is another divisor of $a - b$ and b. Then d is also a divisor of a.
So d is a divisor of both a and b. But g is the greatest such divisor, so $g \geq d$.

$$gcd(a, b) = \begin{cases} a & \text{if } a = b, \\ gcd(a - b, b) & \text{if } a > b, \\ gcd(a, b - a) & \text{if } a < b. \end{cases}$$

We will prove the following proposition for all $n \geq 1$:

$$gcd(a, b) = \mathrm{GCD}(a, b) \text{ if } \max(a, b) = n.$$

Base case: $n = 1$. Then $a = b = 1$, so $gcd(a, b) = 1 = \mathrm{GCD}(a, b)$.

Induction hypothesis: $gcd(a, b) = \mathrm{GCD}(a, b)$ if $\max(a, b) < n$.

Induction step: To prove that $gcd(a, b) = \mathrm{GCD}(a, b)$ if $\max(a, b) = n$.

$$gcd(a, b) = \begin{cases} a & \text{if } a = b, \\ gcd(a - b, b) & \text{if } a > b, \\ gcd(a, b - a) & \text{if } a < b. \end{cases}$$

Induction hypothesis: $gcd(a, b) = \mathrm{GCD}(a, b)$ if $\max(a, b) < n$.

Induction step: To prove that $gcd(a, b) = \mathrm{GCD}(a, b)$ if $\max(a, b) = n$.

W.l.o.g., suppose $a = \max(a, b) = n$. Then $b \leq a$.

If $b = a$ then $gcd(a, b) = a = \mathrm{GCD}(a, b)$.

If $b < a$ then $gcd(a, b) = gcd(a - b, b) = \mathrm{GCD}(a - b, b)$ by I.H. since $a - b, b < n$.

We already know $\mathrm{GCD}(a - b, b) = \mathrm{GCD}(a, b)$ whenever $a > b$, so we are done.

Euclidean algorithm for GCD

Practical version (replacing repeated subtraction by modulo):

$$gcd(a, b) = \begin{cases} a & \text{if } b = 0, \\ gcd(b, a \bmod b) & \text{otherwise.} \end{cases}$$

$gcd(49, 21)$
$= gcd(21, 7)$
$= gcd(7, 0)$
$= 7$

Now we must allow *a*, *b* ≥ 0. (Why?)

This version is actually easier to prove correctness, simply by induction on *b*.

Afterwards

- Prove correctness of the second version of *gcd*.