Lecture 13
Feb. 26th, 2015

PROMGRAM CORRECTNESS

b^n for $b>0, n\in\mathbb{N}$

$236^{123} = 236\cdots236 = (236^{61})(236^{61})\cdot 236 = (236^{61})^2\cdot 236 = ((236^{30})^2\cdot 236)^2\cdot 236 = (((236^{15})^2)^2\cdot 236)^2\cdot 236$

in python:

```
    # pre : n∈N, b∈R and b≠0 in case 0^0 bothers you.
    # post: return b^n.

    def pow( b,n):
        if n>= 1: ?
            p=pow(b, n//2)
            if n%2==1:
                return p * p * b
            else:
                return p* p
        else:
            return 1 (n=1) ?
```

For $n\in\mathbb{N}$, Let $Q(n)$ be: IF pre(n,b), THEN Post(n,b)

If $b\in\mathbb{R}$ and $b\neq 0$ then pow(b,n) returns b^n.

Base Case: $n=0$. suppose $b\in\mathbb{R}$, $b\neq 0$.

From code, pow(b,n) strings 1st branch, returns $1=b^0=b^n$

IS: let $n\in\mathbb{N}$, assume $n\geq 1$

(IH): Assume Q for all natural numbers less than n.

Suppose $b\in\mathbb{R}$, $b\neq 0$

From code and $n\geq 1$: calls pow$(b, \lfloor\frac{n}{2}\rfloor)$

Since $n>0$: $\frac{n}{2}<n$, so $\lfloor\frac{n}{2}\rfloor<n$

also $\lfloor\frac{n}{2}\rfloor\in\mathbb{Z}$ and $\frac{n}{2}\geq\frac{1}{2}\geq 0$

So $\lfloor\frac{n}{2}\rfloor\in\mathbb{N}$

So $Q(\lfloor\frac{n}{2}\rfloor)$ by IH $\wedge$ $(\in\mathbb{N}, b\in\mathbb{R}, b\neq 0)$

So PRE is true for pow$(b,\lfloor\frac{n}{2}\rfloor)$, so pow$(b,\lfloor\frac{n}{2}\rfloor)$ returns $b^{\lfloor\frac{n}{2}\rfloor}$ so $p=b^{\lfloor\frac{n}{2}\rfloor}$

If n is odd: 1st inner branch of First Branch

returns $p*p*b = b^{\lfloor\frac{n}{2}\rfloor}b^{\lfloor\frac{n}{2}\rfloor}b = b^{\frac{n-1}{2}}b^{\frac{n-1}{2}}b = b^{n-1}b = b^n$

If n is even: returns $p*p = b^{\lfloor\frac{n}{2}\rfloor}b^{\lfloor\frac{n}{2}\rfloor} = b^{\frac{n}{2}}b^{\frac{n}{2}} = b^n$

```
    def pow(b,n) :
        m=0
        r=1
        while m<n :
            r=r * b
            m=m+1
        return r
```

For $i\in\mathbb{N}$, let r_i, m_i be the values of r, m after i iteration.

$r_0=1$, $m_0=0$.

$r_{i+1}=r_i\cdot b$, $m_{i+1}=m_i+1$ for each $i\in\mathbb{N}$

So finally $m_i=i$, $r_i=b^i$

For $i \in \mathbb{N}$, let $I(i)$ be : if there are more than i iterations, then $m_i = i$, $r_i = b^i$.

recursive $\Rightarrow$ complete induction
loops $\Rightarrow$ simple induction

Proof by Simple Induction

$I(0)$: $m_0 = 0$, $r_0 = 1 = b^0$

IS: let $i \in \mathbb{N}$, assume $I(i)$

Assume more than $i+1$ iterations, so more than i iterations.

So by $I(i)$: $m_i = i$, $r_i = b^i$.

So $r_{i+1} = b \cdot r_i = b^i \cdot b = b^{i+1}$ and $m_{i+1} = m_i + 1 = i + 1$