CS240: Homework 6

Sahit Mandala

November 2, 2015

Problem 1

Partial Correctness

Let a, b be valid inputs on the program. We will consider several exhausive cases to show that this program returns the correct output (i.e. a^b).

Case 1: $b = 1$

In this cases, we know that $a^b = a^1 = a$. Since the conditional at (1) is satisfied, we do return a as the solution, as expected.

Case 2: $b \neq 1$ and b is odd

Since $b \neq 1$, we skip the conditional at line (1) and execute (2) as part of the else statement. That is, we run $r = FastPower(a, \lfloor \frac{b}{2} \rfloor)$. In this case, since $b \in \mathbb{Z}^+$ and $b \neq 1$, we know that $2 \leq b$. Since b is odd, we can further infer that $b \neq 2$, so $3 \leq b$. Alse, we can choose some $k \in \mathbb{Z}$ s.t. $b = 2k + 1$. But $3 \leq b = 2k + 1$ so $2 \leq 2k$ and thus $1 \leq k$. That is, $k \in \mathbb{Z}^+ \subset \mathbb{Z}$. Notice that $\lfloor \frac{b}{2} \rfloor = \lfloor \frac{2k+1}{2} \rfloor = \lfloor k + \frac{1}{2} \rfloor = \lfloor k \rfloor = k$, noting that k is an integer while 1/2 is just a decimal. So $r = FastPower(a, \lfloor \frac{b}{2} \rfloor) = FastPower(a, k)$, and since $a \in \mathbb{Z}, a \neq 0$ (as given) and $k \in \mathbb{Z}^+$, we know that $FastPower(a, k) = a^k$. So $r = a^k$.

Now we consider line (3). Since we know b is odd, the conditional triggers, so we return $a * r * r$. Note that $a * r * r = a * a^k * a^k = a * a^{2k} = a^{2k+1} = a^b$, recalling that $2k + 1 = b$. Hence, in this case, we in fact return the correct solution, a^b.

Case 2: $b \neq 1$ and b is even

Since $b \neq 1$, we skip the conditional at line (1) and execute (2) as part of the else statement. That is, we run $r = FastPower(a, \lfloor \frac{b}{2} \rfloor)$. In this case, since $b \in \mathbb{Z}^+$ and $b \neq 1$, we know that $2 \leq b$. Since b is even, we can choose some $k \in \mathbb{Z}$ s.t. $b = 2k$. But $2 \leq b = 2k$, so $1 \leq k$. That is, $k \in \mathbb{Z}^+ \subset \mathbb{Z}$. Notice that $\lfloor \frac{b}{2} \rfloor = \lfloor \frac{2k}{2} \rfloor = \lfloor k \rfloor = k$, noting that k is an integer. So $r = FastPower(a, \lfloor \frac{b}{2} \rfloor) = FastPower(a, k)$, and since $a \in \mathbb{Z}, a \neq 0$ (as given) and $k \in \mathbb{Z}^+$, we know that $FastPower(a, k) = a^k$. So $r = a^k$.

Now we consider line (3) and (4). Since we know b is even, so the conditional at (3) fails so we execute the else statement at (4); so we return $r * r$. Note that $r * r = a^k * a^k = a^{2k} = a^b$, recalling that $2k = b$. Hence, in this case, we in fact return the correct solution, a^b.

Hence, we have exhaused all cases on b to show that when the program terminates, it returns the correct output on valid input.

Termination

Let some arbitrary $a \in \mathbb{Z}, a \neq 0$ be given. To prove termination, we shall use proof by induction on b to show $P(b) : FastPower(a, b)$ terminates.

First, consider the base case $b = 1$ (noting that $b \in \mathbb{Z}^+$). During the execution of the program, we first trigger the conditional on line (1) since $b = 1$ and thus return a, terminating the program. Hence, we have shown $P(1)$.

Next, assume the strong inductive hypothesis for some $k \in \mathbb{N}$ with $1 \leq k$. That is, $\forall x \in \mathbb{N}$ with $1 \leq x \leq k, P(x)$. Or equivalently, for $\forall x \in \mathbb{N}$ with $1 \leq x \leq k$, $FastPower(a, x)$ terminates.

Consider $FastPower(a, k+1)$. We know that $1 \leq k$, so $2 \leq k + 1 \neq 1$; hence, we skip the statement at line (1). Now consider 2 cases:

Case 1: $k + 1$ is odd

Since $k + 1$ is odd, we can further infer that $k + 1 \neq 2$, so $3 \leq k + 1$. Also, we can choose some $m \in \mathbb{Z}$ s.t. $k + 1 = 2m + 1$. But $3 \leq k + 1 = 2m + 1$ so $2 \leq k = 2m$. This implies that $1 \leq m$ and $m \leq k$. Notice that $\lfloor \frac{k+1}{2} \rfloor = \lfloor \frac{2m+1}{2} \rfloor = \lfloor m + \frac{1}{2} \rfloor = \lfloor m \rfloor = m$, noting that m is an integer while 1/2 is just a decimal. So $FastPower(a, \lfloor \frac{k+1}{2} \rfloor) = FastPower(a, m)$, and since $1 \leq m \leq k$, we know that $FastPower(a, m)$ terminates by the inductive hypothesis. Hence, line (2) of the program terminates.

Now we consider line (3). Since we know $k + 1$ is odd, the conditional triggers at (3) triggers and we return a value, causing the program to terminate.

Case 2: $k + 1$ is even

Since $k+1$ is even, $2 \leq k+1$. Also, we can choose some $m \in \mathbb{Z}$ s.t. $k+1 = 2m$. But $2 \leq k+1 = 2m$ so $2 \leq k+1 = 2m$. This implies that $1 \leq m$. Also note that because $k-m = m-1$ and $1 \leq m \to 0 \leq m-1$ from above, we see that $m \leq k$. Notice that $\lfloor \frac{k+1}{2} \rfloor = \lfloor \frac{2m}{2} \rfloor = \lfloor m \rfloor = m$, noting that m is an integer. So $FastPower(a, \lfloor \frac{k+1}{2} \rfloor) = FastPower(a, m)$, and since $1 \leq m \leq k$, we know that $FastPower(a, m)$ terminates by the inductive hypothesis. Hence, line (2) of the program terminates.

Now we consider line (3) and (4). Since we know $k + 1$ is even, the conditional at (3) fails but triggers (4). Here, we return a value, causing the program to terminate.

We have exhausted all cases on $k + 1$ to show that the program $FastPower(a, k + 1)$ does terminate. Hence, by strong induction, we have shown $FastPower(a, b)$ terminates for all $b \in \mathbb{N}$ with $b \geq 1$ (or equivalently, $b \in \mathbb{Z}^+$). And since a was arbitrarily given as a valid input earlier, we see that $FastPower(a, b)$ terminates on all valid input

Problem 2

Part a

First, we write out the first few terms in the sequence, index starting at 0.

$A_0 = 2, A_1 = 1, A_2 = A_1 + 2A_0 = 5, A_3 = A_2 + 2A_1 = 7, A_4 = A_3 + 2A_2 = 17, A_5 = A_4 + 2A_3 = 31, A_6 = 65$

0	1	2	3	4	5	6
2	1	5	7	17	31	65

Part b

Looking at the values, we can see that after the first 2 values, the sequence values are close to 2^n, give or take 1. With this intuition, I propose the following solution F:

$F[n] = 2^n + (-1)^n$

Part c

Consider the predicate $P(n) : (F[n] = A_n)$. We would like to show $\forall n \in \mathbb{N}, P(n)$, so we will use srtong induction on n.

Base case $P(0)$: We are given that $A_0 = 2$ and $F[0] = 2^0 + (-1)^0 = 1 + 1 = 2$, so clearly, $A_0 = F[0]$. Thus, we have shown $P(0)$.

Strong inductive hypothesis: Next, let some $k \in \mathbb{N}$ be given and suppose that $\forall i \leq k, P(k)$ is true.

We want to show $P(k+1)$ is true. As a trivial case, suppose that $k+1 = 1$. Then $F[k+1] = F[1] = 2^1 + (-1)^1 = 2 - 1 = 1$ and we know $A_1 = 1$, so clearly $P(k+1) \equiv P(1)$ is true.

Now consider the case that $k+1 \neq 1$. Since $k \in \mathbb{N}$, it follows that $k \geq 0$ so $k+1 \geq 1$; since $k+1 \neq 1$, $k+1 > 1$. This means that we can utilize the relation $A_{k+1} = A_k + 2A_{k-1}$. By the strong induction hypothesis, we already have $P(k), P(k-1)$, noting that $k-1 \geq 0$ in this case, so $F[k] = 2^k + (-1)^k = A_k, F[k-1] = 2^{k-1} + (-1)^{k-1} = A_{k-1}$. Substitution reveals that: $A_{k+1} = (2^k + (-1)^k) + 2(2^{k-1} + (-1)^{k-1}) = (2^k + (-1)^k) + (2^k + 2(-1)^{k-1}) = (2^k + 2^k) + (-1)^k + 2(-1)^{k-1}$
$= (2^k + 2^k) + (-1)(-1)^{k-1} + 2(-1)^{k-1} = (2^{k+1}) + (-1)^{k-1} = (2^{k+1}) + (-1)(-1)(-1)^{k-1}$
$= (2^{k+1}) + (-1)^2(-1)^{k-1} = (2^{k+1}) + (-1)^{k+1}$

Hence, we have shown that $A_{k+1} = (2^{k+1}) + (-1)^{k+1} = F[k+1]$

Problem 3

Part a

For 0, we are already at the final step, the 0th, so no steps can be taken. Hence, there are 1 ways to take steps to get to the 0th step.

For 1 step, the person can only take a single step to reach that 1st step, and then he/she is done. Hence, there is only 1 way to that 1st step.

For 2 step, the person can only take a single 2-step to reach that 2nd step, and then he/she is done. The person can also take 2 1-steps to reach the top. There are all possible ways to the top, so there are only 2 ways to the top in this case.

For 3 step, the person can either: take 3 1-steps, take 1 1-step and then 1 2-step, or take 1 2-step and then 1 1-step. Here, there are a total of 3 ways to get to the 3rd step:

To summarize:

#Steps	0	1	2	3
Moves	0	1	2	3

Part b

Suppose that the person has n steps in front of them. If $n = 0$, there is 1 way to get to that step. If there is $n = 1$ steps in front of them, there is only 1 way to the 1st step. For $n \geq 1$, the person can either take a 1-step or 2-step. If they take a 1-step, there are n-1 steps to go. If they take a 2-step, they have n-2 steps to go. The number of ways to the top step n can be marginalized on these 2 decisions potential: # for steps n = # of ways to 1-step * # of ways to get n-1 steps + # of ways to 2-step * number of ways for n-2 steps. In recurrence form, noting the cases $n = 1, n = 2$:

$A_n = A_{n-1} + A_{n-2}$,$A_0 = 1$,$A_1 = 1$

Part c

In our case, we see that $c_1 = c_2 = 1$, so the quadratic equation becomes $r^2 - r - 1$. The roots of the equation, by the quadratic formula, are:

$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = \frac{1 \pm \sqrt{1 - 4(-1)}}{2} = \frac{1 \pm \sqrt{5}}{2}$

So we have roots $r_1 = \frac{1+\sqrt{5}}{2}, r_2 = \frac{1-\sqrt{5}}{2}$.

So the closed form of this reccurence relation is:
$A_n = \alpha(\frac{1+\sqrt{5}}{2})^n + \beta(\frac{1-\sqrt{5}}{2})^n$.
Solving for α, β, we shall utilize $A_1 = 1, A_2 = 2$:
$A_0 = \alpha(\frac{1+\sqrt{5}}{2})^0 + \beta(\frac{1-\sqrt{5}}{2})^0 = 1 \rightarrow \alpha + \beta = 1$
$A_1 = \alpha(\frac{1+\sqrt{5}}{2})^2 + \beta(\frac{1-\sqrt{5}}{2})^1 = 1 \rightarrow \alpha(1+\sqrt{5})^1 + \beta(1-\sqrt{5})^1 = 2$
$\alpha(1+\sqrt{5})^1 + \beta(1-\sqrt{5})^1 - \alpha + \beta = \alpha\sqrt{5} - \beta\sqrt{5} = 2 - 1 = 1 \rightarrow \alpha - \beta = \frac{1}{\sqrt{5}}$
$\frac{\alpha+\beta+\alpha-\beta}{2} = \alpha = (1 + \frac{1}{\sqrt{5}})/2, \beta = 1 - \alpha = 1 - (1 + \frac{1}{\sqrt{5}})/2 = (1 - \frac{1}{\sqrt{5}})/2$
$A_n = (1 + \frac{1}{\sqrt{5}})/2(\frac{1+\sqrt{5}}{2})^n + (1 - \frac{1}{\sqrt{5}})/2(\frac{1-\sqrt{5}}{2})^n = (\frac{1+\sqrt{5}}{2\sqrt{5}})(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2\sqrt{5}})(\frac{1-\sqrt{5}}{2})^n$
$= (\frac{1}{\sqrt{5}})(\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1}{\sqrt{5}})(\frac{1-\sqrt{5}}{2})^{n+1} = (\frac{1}{\sqrt{5}})(\frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}})$
Hence, we have found a closed form for the sequence:
$A_n = (\frac{1}{\sqrt{5}})(\frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}})$

Part d

Using our formula at 8,
$A_8 = (\frac{1}{\sqrt{5}})(\frac{(1+\sqrt{5})^{8+1} - (1-\sqrt{5})^{8+1}}{2^{8+1}}) = (\frac{1}{\sqrt{5}})(\frac{(1+\sqrt{5})^9 - (1-\sqrt{5})^9}{2^9}) = (0.4472)(\frac{(38918.73) - (-6.7356)}{512}) = 33.998 \approx$ 34.
Hence, there are 34 ways of traversing 8 steps.