CS 70 Discrete Mathematics and Probability Theory
Spring 2015 Vazirani HW 2

Due Monday February 2 at noon

1. **Propositional logic**
   For each the following logical equivalence assertions, either prove it is true or give a counterexample showing it is false (i.e., some choices of P and Q such that one side of the equivalence is true and the other is false), together with a one to two sentence justification that it is indeed a counterexample.

   (a) $\forall x P(x) \equiv \neg\exists x \neg P(x)$
   (b) $\forall x \exists y P(x,y) \equiv \forall y \exists x P(x,y)$
   (c) $P \Rightarrow \neg Q \equiv \neg P \Rightarrow Q$
   (d) $(P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q) \equiv P \Leftrightarrow Q$

   Answer:

   (a) True. We use the fact that $\neg(\neg A) \equiv A$ for any proposition A. The full proof is:

   $$\forall x P(x) \equiv \neg(\neg(\forall x P(x))) \equiv \neg(\exists x \neg P(x)).$$

   (b) False. Take the universe of both x, y to be $\mathbb{N}$, and take $P(x,y)$ to be the statement "$x > y$". Then the left hand side $\forall x \exists y P(x,y)$ claims that for every $x \in \mathbb{N}$ we can find another natural number $y \in \mathbb{N}$ that is strictly less than x; this is false, since when $x = 0$ we cannot find such a y. The right hand side $\forall y \exists x P(x,y)$ claims that for all $y \in \mathbb{N}$ we can find $x \in \mathbb{N}$ that us strictly larger than y; this is true, e.g., we can take $x = y + 1$.

   (c) False. Take P and Q to be any true propositions (e.g., P is "$1+1=2$" and Q is "$1+2=3$"). Then $P \Rightarrow \neg Q$ is false while $\neg P \Rightarrow Q$ is true.

   (d) True. Recall that $P \Leftrightarrow Q$ is equivalent to $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$. Since $Q \Rightarrow P$ is equivalent to its contraposition $\neg P \Rightarrow \neg Q$, we conclude that $P \Leftrightarrow Q$ is also equivalent to $(P \Rightarrow Q) \wedge (\neg P \Rightarrow \neg Q)$.

   Note: You can use any counterexamples for (b) and (c).

2. **More quantifiers**
   Suppose we are trying to prove $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n. Instead, we succeeded in proving the following:

   $$\forall k \in \mathbb{N}, \text{ if } P(k) \text{ is true then } P(k+2) \text{ is true.}$$

   For each of the following assertions below, state whether: (A) it must always hold; or (N) it can never hold; or (C) it can hold but need not always. Give a very brief (one or two sentence) justification for your answers. The domain of all quantifiers is the natural numbers $\mathbb{N}$.

   (a) $\forall n\, P(n)$ is true

(b) If $P(0)$ is true then $\forall n\ P(n+2)$ is true

(c) If $P(0)$ is true then $\forall n\ P(2n)$ is true

(d) $\forall n\ P(n)$ is false

(e) If $P(0)$ and $P(1)$ are true then $\forall n\ P(n)$ is true

(f) $(\forall n \leq 10\ \ P(n)$ is true) and $(\forall n > 20\ P(n)$ is false)

(g) $[\forall n\ n \text{ prime} \Rightarrow P(n)] \Rightarrow [\forall n \geq 11\ P(n)]$

Answer: Consider the following propositions:

$Q(n)$ denotes the proposition "n is even"

$R(n)$ denotes the proposition "$n \geq 0$

Notice that both Q and R satisfy the weaker form of inductive step above, namely, if $Q(k)$ is true then $Q(k+2)$ is true. Similarly, if $R(k)$ is true then $R(k+2)$ is true. Note that $R(n)$ is true for all $n \in \mathbb{N}$, while $Q(n)$ is only true when n is even.

(a) **(C)**. Setting $P = Q$ makes the statement false, while setting $P = R$ makes the statement true.

(b) **(C)**. Use the same counterexamples from part (a). Note that knowing $P(0)$ is true only tells us $P(2n)$ is true for all $n \in \mathbb{N}$ (see part (c) below), but we cannot conclude anything about the odd terms $P(1), P(3), P(5), \ldots$.

(c) **(A)**. Using our weaker inductive step, $P(0)$ is true implies $P(2)$ is also true, which in turn implies $P(4)$ is true, and so on. Formally, you can prove by induction that $P(2n)$ is true for all $n \in \mathbb{N}$.

(d) **(C)**. Setting $P = Q$ makes the statement false, while setting $P = \neg R$ makes the statement true.

(e) **(A)**. You can prove this using the usual mathematical induction with two base cases.

(f) **(N)**. If we know $P(0)$ and $P(1)$ are true, then $P(n)$ is true for all $n \in \mathbb{N}$ (from part (e)).

(g) **(A)**. The statement claims that if $P(n)$ is true for all prime numbers n, then $P(n)$ is true for all $n \geq 11$. Note that 2 and 3 are prime, and the same argument as in part (e) shows that if $P(2)$ and $P(3)$ are true, then $P(n)$ is true for all $n \geq 2$.

3. **Simple induction**

(a) Prove that $3 + 11 + 19 + \cdots + (8n-5) = 4n^2 - n$ for all integers $n \geq 1$.

(b) Prove that $1^3 + 2^3 + 3^3 + \cdots + n^3 = (1+2+3+\cdots+n)^2$ for all integers $n \geq 1$.

Hint: Part (b) involves a lot of algebra unless you do something clever. What is the right hand side?

Answer:

(a) We use induction on $n \geq 1$. The base case $n = 1$ is true because $3 = 4 \cdot 1^2 - 1$. Now assume the claim holds for some $n \geq 1$; we want to show that the claim also holds for $n+1$. We can write

$$\sum_{m=1}^{n+1} (8m-5) \ = \ \sum_{m=1}^{n} (8m-5) + (8(n+1)-5) \ = \ (4n^2 - n) + (8n+3) \ = \ 4(n+1)^2 - (n+1),$$

where in the calculation above we have used the inductive hypothesis to replace the first n terms in the summation with $4n^2 - n$. This completes the inductive step.

(b) Recall the formula $\sum_{m=1}^{n} m = \frac{1}{2}n(n+1)$ from Theorem 3.1 in Note 3. We use induction to prove that $\sum_{m=1}^{n} m^3 = \frac{1}{4}n^2(n+1)^2$. The base case $n = 1$ holds because $1 = \frac{1}{4} \cdot 1^2 \cdot 2^2$. Now assume the claim holds for some $n \geq 1$; we want to show that the claim also holds for $n+1$. We can write

$$\sum_{m=1}^{n+1} m^3 = \sum_{m=1}^{n} m^3 + (n+1)^3 = \frac{1}{4}n^2(n+1)^2 + (n+1)^3$$
$$= \frac{1}{4}(n+1)^2\left(n^2+4(n+1)\right) = \frac{1}{4}(n+1)^2(n+2)^2,$$

where in the calculation above we have used the inductive hypothesis to replace the first n terms in the summation with $\frac{1}{4}n^2(n+1)^2$. This completes the inductive step.

4. **Strong induction**
Let $x \in \mathbb{R}$ be such that $a_1 = x + \frac{1}{x} \in \mathbb{Q}$. Using strong induction, show that for each integer $n \geq 1$, $a_n = x^n + \frac{1}{x^n} \in \mathbb{Q}$.

Answer: We use strong induction on n. We check two base cases:

(a) $n = 1$: we have $a_1 = x + \frac{1}{x} \in \mathbb{Q}$ by assumption.

(b) $n = 2$: we can write

$$a_2 = x^2 + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 - 2 = a_1^2 - 2 \in \mathbb{Q}.$$

Now let $k \geq 2$ and suppose the claim holds for $1 \leq n \leq k$, i.e., assume that $a_1, a_2, \ldots, a_k \in \mathbb{Q}$. We want to show that $a_{k+1} \in \mathbb{Q}$. We can express a_{k+1} in terms of the previous values as follows:

$$a_{k+1} = x^{k+1} + \frac{1}{x^{k+1}} = \left(x^k + \frac{1}{x^k}\right)\left(x + \frac{1}{x}\right) - \left(x^{k-1} + \frac{1}{x^{k-1}}\right) = a_k \cdot a_1 - a_{k-1}.$$

The inductive hypothesis tells us that $a_1, a_{k-1}, a_k \in \mathbb{Q}$, so we conclude that $a_{k+1} \in \mathbb{Q}$ as well.

Note: We need to check two base cases because the inductive step for a_{k+1} uses the inductive hypothesis for a_k and a_{k-1}. Alternatively, we can also start by defining $a_0 = x^0 + \frac{1}{x^0} = 2 \in \mathbb{Q}$ and only check one base case $n = 1$, because then the recurrence $a_{k+1} = a_k \cdot a_1 - a_{k-1}$ already holds for $k = 1$. In either case, you should point out that you need two base cases; otherwise take 2 points off.

5. **Strengthening the induction hypothesis**
Let $a_0 = 1$ and $a_n = 2a_{n-1} + 7$. Prove that there is a constant $C > 0$, which does not depend on n, such that $a_n \leq C \cdot 2^n$ for all $n \in \mathbb{N}$.

Hint: Strengthen the induction hypothesis into $a_n \leq C \cdot 2^n - D$ for some constant D. What value of D should you choose to make the proof easiest?

Answer: We use induction to prove a stronger statement that $a_n \leq 8 \cdot 2^n - 7$ for all $n \in \mathbb{N}$. The base case $n = 0$ is true because $a_0 = 1 = 8 \cdot 2^0 - 7$. Suppose the claim holds for some $n \in \mathbb{N}$; we want to show the claim also holds for $n+1$. Using the recursion, we can write

$$a_{n+1} = 2a_n + 7 \leq 2\left(8 \cdot 2^n - 7\right) + 7 = 8 \cdot 2^{n+1} - 7,$$

where we have applied the inductive hypothesis to obtain the inequality above. This completes the induction step.

Note: You can use any value of $C \geq 8$, but note that $C = 8$ is the smallest choice that makes the inequality true for all $n \in \mathbb{N}$. You can also use any value for D, as long as your proof is correct.

6. **Proofs to grade**
Assign a grade of A (correct) or F (failure) to the following proof. If you give an F, explain exactly what is wrong with the structure or the reasoning in the *proof* (rather than just saying that the claim is false). You should justify all your answers.

   (a) **Claim:** For every $n \in \mathbb{N}$, $n^2 + n$ is odd.

   Proof: We use mathematical induction.

   Base Case: The natural number 1 is odd.

   Inductive Step: Suppose $k \in \mathbb{N}$ and $k^2 + k$ is odd. Then,

$$(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = (k^2 + k) + (2k + 2)$$

   is the sum of an odd and an even integer. Therefore, $(k+1)^2 + (k+1)$ is odd. By the Principle of Mathematical Induction, the property that $n^2 + n$ is odd is true for all natural numbers n. ♠

   (b) **Claim:** $(\forall n \in \mathbb{N})(7^n = 1)$.

   Proof: We use strong induction.

   Base Case: Certainly $7^0 = 1$. Inductive step: Now suppose that $7^j = 1$ for all $0 \leq j \leq k$.

   We need to show that $7^j = 1$ for all $j, 0 \leq j \leq k+1$. To do this, we need only to prove that $7^{k+1} = 1$. But,

$$7^{k+1} = \frac{(7^k \cdot 7^k)}{7^{k-1}} = \frac{(1 \cdot 1)}{1} = 1$$

   Hence, by the Principle of Strong Induction, $7^m = 1$ for all $m \in \mathbb{N}$. ♡

Answer:

   (a) **(F)**. The base case is wrong. When $n = 0$ we have $n^2 + n = 0^2 + 0 = 0$, not 1 as stated. Even if we use the base case $n = 1$, we will have $n^2 + n = 1^2 + 1 = 2$, which is even, not odd.

   (b) **(F)**. The recurrence in the proof above expresses 7^{k+1} in terms of 7^k and 7^{k-1}. However, when $k = 0$, this involves the term $7^{0-1} = 7^{-1}$, which is not covered by our base case $n = 0$. In other words, the recurrence in the proof above only works for $k \geq 1$, so if we want to use the argument above, we also need another base case $n = 1$.

7. **Recursion and induction**
Below is a recursive algorithm for computing the result raising a number to a non-negative integer power $n \in \mathbb{N}$. Use induction to prove that this algorithm is correct, i.e., it returns x^n.

   function POWER(x, n)
      if $n = 0$ **then**
         return 1
      if n is even **then**
         return POWER$(x, \frac{n}{2})^2$
      else

return $x \times$ POWER$(x, n-1)$

Answer: We want to prove that for all $x \in \mathbb{R}$ and $n \in \mathbb{N}$, the algorithm POWER(x,n) returns x^n. Let $x \in \mathbb{R}$ be arbitrary. We prove the claim using strong induction on n. The base case $n = 0$ is true because POWER$(x,0)$ returns $1 = x^0$ (in this problem we take 0^0 to be 1, so the base case still holds even for $x = 0$). Now let $k \in \mathbb{N}$ and suppose the claim holds for $0 \le n \le k$; we want to show that POWER$(x, k+1) = x^{k+1}$. We consider two cases:

(a) If k is odd, then $k+1$ is even, so by the specification of the algorithm,

$$\text{POWER}(x, k+1) \;=\; \text{POWER}(x, \frac{k+1}{2})^2 \;=\; \left(x^{(k+1)/2}\right)^2 \;=\; x^{k+1},$$

where we have used the inductive hypothesis POWER$(x, \frac{k+1}{2}) = x^{(k+1)/2}$.

(b) If k is even, then $k+1$ is odd, so by the specification of the algorithm,

$$\text{POWER}(x, k+1) \;=\; x \times \text{POWER}(x,k) \;=\; x \times x^k \;=\; x^{k+1},$$

where we have used the inductive hypothesis POWER$(x,k) = x^k$.

This completes the inductive step.

8. **Tower of Brahma**
This puzzle was invented by the French mathematician, Edouard Lucas, in 1883. Accompanying the puzzle is a story:

In the great temple at Benares beneath the dome which marks the center of the world, rests a brass plate in which are fixed three diamond needles, each a cubit high and as thick as the body of a bee. On one of these needles, at creation, God placed sixty-four disks of pure gold, the largest disk resting on the brass plate and the others getting smaller and smaller up to the top one. This is the Tower of Brahma. Day and Night unceasingly, the priests transfer the disks from one diamond needle to another according to the fixed and immutable laws of Brahma, which require that the priest on duty must not move more than one disk at a time and that he must place this disk on a needle so that there is no smaller disk below it. When all the sixty-four disks shall have been thus transferred from the needle on which at the creation God placed them to one of the other needles, tower, temple and priests alike will crumble into dust, and with a thunderclap the world will vanish.

The priests are duty bound to minimize the number of moves to transfer the tower. Fill in the details of the recursive algorithm that the priests use to move the disks. What is the exact number of moves required to carry out this task as a function of n, the number of disks on the original needle? Prove by induction that your bound is correct. Assuming that the priests can move a disk each second, roughly how many years does the prophecy predict before the destruction of the World? For comparison, the age of the Earth is estimated to be 4.6 billion years.

Answer: We design an algorithm TOWER(n,a,b) which moves a tower of the n *smallest* disks from needle a to needle b. Here a and b are two of the three needles (let's call the other needle c). The algorithm TOWER(n,a,b) assumes that needle a has $\ge n$ disks ordered from smallest to largest, while the disks on needles b and c are all larger than the n disks that we want to move. Of course, since TOWER(n,a,b) only wants to move the n smallest disks, any other disks on the needles do not interfere with the moves involving these n disks.

Here is the definition of $\text{TOWER}(n,a,b)$. The first recursive call $\text{TOWER}(n-1,a,c)$ moves the smallest $n-1$ disks from a to c, while the second recursive call $\text{TOWER}(n-1,c,b)$ moves the $n-1$ disks from c to b.

function $\text{TOWER}(n,a,b)$
  if $n=1$ **then**
    move disk from a to b
  else
    $\text{TOWER}(n-1,a,c)$
    move the n-th disk from a to b
    $\text{TOWER}(n-1,c,b)$

We now show that this algorithm makes 2^n-1 moves to transfer the tower, and moreover, any algorithm that successfully transfers the tower must make at least 2^n-1 moves.

Claim: The number of single disk moves made by the algorithm $\text{TOWER}(n,a,b)$ is 2^n-1.

Proof of claim: By (simple) induction on n.

Base case: When there is $n=1$ disk, the algorithm clearly only makes only one move.

Induction hypothesis: Assume $\text{TOWER}(k,a,b)$ takes 2^k-1 moves.

Induction step: $\text{TOWER}(k+1,a,b)$ involves two recursive calls $\text{TOWER}(k,a,c)$ and $\text{TOWER}(k,c,b)$, plus the move of a single disk. By the induction hypothesis, each of the two recursive invocations takes 2^k-1 moves, for a grand total of $2(2^k-1)+1=2^{k+1}-1$. □

We now show that any algorithm must make at least 2^n-1 moves. Let $M(n)$ be the smallest number of moves that suffices to move a tower of n disks. Before the lowest disk is moved, the tower consisting of the top $n-1$ disks must be moved. Then the bottom disk must be moved. Finally the tower consisting of the top $n-1$ disks must be moved back on top of the repositioned bottom disk. The first task requires at least $M(n-1)$ steps. The second takes 1 step. And the last task requires at least $M(n-1)$ steps.

So we get the inequality that $M(n) \geq 2M(n-1)+1$, with $M(1)=1$. We can now conclude (e.g., by induction on n) that $M(n) \geq 2^n-1$. The proof is identical to the one above, with the equal sign $=$ replaced by the inequality $\geq$.

Claim: Any algorithm must make at least 2^n-1 moves to transfer a tower of n disks.

Proof of claim: By (simple) induction on n.

Base case: When there is $n=1$ disk, any algorithm needs at least $1=2^1-1$ move.

Induction hypothesis: Assume transferring a tower of k disks takes at least 2^k-1 moves.

Induction step: For a $k+1$ tower, before the lowest disk is moved, the tower consisting of the top k disks must be moved. Then the bottom disk must be moved. Finally the tower consisting of the top k disks must be moved back on top of the repositioned bottom disk. By the induction hypothesis, the first task requires at least 2^k-1 steps. The second takes 1 step. And again by the induction hypothesis, the last task requires at least 2^k-1 steps, giving a total of at least $(2^k-1)+1+(2^k-1)=2^{k+1}-1$. □

Finally, let us substitute the value $n=64$ from the original problem. In this case the number of steps needed is

$$f(64) \;=\; 2^{64}-1 \;>10^{19}.$$

There are $365 \times 24 \times 3600 = 31536000 < 10^8$ seconds in a year, so assuming each step takes 1 second, the computation above shows that moving a tower of 64 disks require more than $10^{19}/10^8 = 10^{11}$ (100 billion) years, much longer than the age of the earth.

9. **(Extra Credit)**

Prove that $\sqrt{2\sqrt{3\sqrt{4\cdots\sqrt{n}}}} < 3$.

(*Hint:* what can you say about the quantity $\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}}$?).

Answer: We will prove the following more general statement: for all $n \geq 1$ and all $1 \leq k \leq n$,

$$b_{n,k} < k+1,$$

where $b_{n,k} = \sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}}$. The original problem is the special case $k = 2$.

Let $n \geq 1$ be arbitrary. Treating n as fixed, we prove the claim above by *backward* induction on k:

(a) *Base case* $k = n$: the inequality that we want to show is $b_{n,n} = \sqrt{n} < n+1$, which is true for all $n \geq 1$.

(b) *Inductive hypothesis*: assume the claim holds for some $2 \leq k \leq n$, i.e., $b_{n,k} < k+1$.

(c) *(Backward) inductive step*: we want to show that the claim holds for $k-1$. Note that we can write

$$b_{n,k-1} = \sqrt{(k-1)\sqrt{k\sqrt{(k+1)\cdots\sqrt{n}}}} = \sqrt{(k-1)\cdot b_{n,k}}$$

Then using the inductive hypothesis,

$$b_{n,k-1} \; < \; \sqrt{(k-1)\cdot(k+1)} \; = \; \sqrt{k^2-1} \; < \; k \; = \; (k-1)+1.$$

This completes the backward inductive step.

We conclude that the claim holds for all $1 \leq k \leq n$.