CS 70 Spring 2017 — Discrete Mathematics and Probability Theory — Satish Rao — HW 1

1 Sundry

Before you start your homework, write down your team. Who else did you work with on this homework? List names and email addresses. (In case of homework party, you can also just describe the group.) How did you work on this homework? Working in groups of 3-5 will earn credit for your "Sundry" grade.

Please copy the following statement and sign next to it:

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up.

I certify that all solutions are entirely in my words and that I have not looked at another student's solutions. I have credited all external sources in this write up. (Signature here)

2 Short Answer: Logic

For each question, please answer in the correct format. When an expression is asked for, it may simply be a number, or an expression involving variables in the problem statement, you have to figure out which is appropriate.

1. Let the statement, $(\forall x \in R, \exists y \in R)\ G(x,y)$, be true for predicate $G(x,y)$ and R being the real numbers.

   Which of the following statements is certainly true, certainly false, or possibly true.

   (a) $G(3,4)$
   (b) $(\forall x \in R) G(x,3)$
   (c) $(\exists y) G(3,y)$
   (d) $(\forall y) \neg G(3,y)$
   (e) $(\exists x) G(x,4)$

2. True or False?
   $(\forall x)(\exists y)(P(x,y) \wedge \neg Q(x,y)) \equiv \neg(\exists x)(\forall y)(P(x,y) \implies Q(x,y))$

3. True or False?
   $(\exists x)((\forall y P(x,y)) \wedge (\forall z Q(x,z))) \equiv ((\exists x)(\forall y) P(x,y)) \wedge ((\exists x)(\forall z) Q(x,z))$

4. Give an expression using terms involving $\vee, \wedge$ and $\neg$ which is true if and only if exactly one of X, Y, and Z are true. (Just to remind you: $(X \wedge Y \wedge Z)$ means all three of X,Y,Z are true, $(X \vee Y \vee Z)$ means at least one of X,Y and Z is true.)

Solution:

1. Let the statement, $(\forall x \in R, \exists y \in R)\ G(x,y)$, be true for predicate $G(x,y)$ and R being the real numbers.

   Which of the following statements is certainly true, certainly false, or possibly true.

   (a) **Possibly true.**
   The statement only guarantees there exists some y such that $G(3,y)$ is true, not that $G(3,4)$ in particular is true, so this is possibly but not necessarily true.
   Choose $G(x,y)$ to be always true and statement is true.
   Choose $G(x,y)$ to be $x > y$ to be false.

   (b) **Possibly true.**
   In the same vein as the previous part, we are guaranteed the existence of *a* y for each x, not that $G(x,3)$ is necessarily true.
   Choose $G(x,y)$ to be always true and statement is true.
   Choose $G(x,y)$ to be $x > y$ to be false.

   (c) **True.**
   The original statement is that for every x, there is a y where $G(x,y)$ is true which implies that for $x = 3$, there is a y where $G(x,y)$ is true.

   (d) **False.**
   This is the negation of the statement above.

   (e) **Possibly true.**
   This is similar to part b. We don't have information about $G(x,3)$ specifically - only that there exists a y for x such that $G(x,y)$ is true.
   Choose $G(x,y)$ to be always true and statement is true.
   Choose $G(x,y)$ to be $y \neq 4$.

2. **True**.
   We use manipulations to show that these two are equivalent.
   $\forall x \exists y (P(x,y) \wedge \neg Q(x,y))$
   $\equiv (\forall x)(\exists y)\neg(\neg P(x,y) \vee Q(x,y))$
   $\equiv (\forall x)(\exists y)\neg(P(x,y) \implies Q(x,y))$
   $\equiv \neg(\exists x)(\forall y)(P(x,y) \implies Q(x,y))$

3. **False**.
The right hand sides states that there is some value of x that satisfies $P(x,y)$ for all y, and some (potentially different) value of x that satisfies $Q(y,z)$ for all y. However, the left hand side can only be implied from the right hand side if these two values of x are the same.

   Choose $P(x,y)$ to be $xy = 0$.
   Choose $Q(x,z)$ to be $x+z > z$.
   The right hand formula is true; choose $x = 0$ for first term and $x = 1$ for second.
   The left hand side is false; no single choice of x can satisfy $P(x,y)$ for all y and $Q(x,z)$ for all z.

4. $(X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge Y \wedge \neg Z) \vee (\neg X \wedge \neg Y \wedge Z)$
This question is just testing whether you did the Karnaugh map problem which codes up each table entry with a single conjuction.

3 Equivalent or Not

Determine whether the following equivalences hold, and give brief justifications for your answers. Clearly state whether or not each pair is equivalent.

(a) $\forall x\, \exists y\, \big(P(x) \Rightarrow Q(x,y)\big) \;\equiv\; \forall x\, \big(P(x) \Rightarrow (\exists y\, Q(x,y))\big)$

(b) $\neg \exists x\, \forall y\, \big(P(x,y) \Rightarrow \neg Q(x,y)\big) \;\equiv\; \forall x\, \big((\exists y\, P(x,y)) \wedge (\exists y\, Q(x,y))\big)$

(c) $\forall x\, \big((\exists y\, Q(x,y)) \Rightarrow P(x)\big) \;\equiv\; \forall x\, \exists y\, \big(Q(x,y) \Rightarrow P(x)\big)$

Solution:

(a) The equivalence holds.
Justification: We can rewrite the claim as $\forall x\, \exists y\, \big(\neg P(x) \vee Q(x,y)\big) \;\equiv\; \forall x\, \big(\neg P(x) \vee (\exists y\, Q(x,y))\big)$. Clearly, the two sides are the same if $\neg P(x)$ is true. If $\neg P(x)$ is false, then the two sides are still the same, because $\forall x\, \exists y\, \big(\text{False} \vee Q(x,y)\big) \;\equiv\; \forall x\, \big(\text{False} \vee (\exists y\, Q(x,y))\big)$.

(b) The equivalence does not hold.
Justification: Using De Morgan's Law to distribute the negation on the left side yields $\forall x\, \exists y\, \big(P(x,y) \wedge Q(x,y)\big)$. But $\exists$ does not distribute over $\wedge$. There could exist different values of y such that $P(x,y)$ and $Q(x,y)$ for a given x, but not necessarily the same value.

(c) The equivalence does not hold.
Justification: We can rewrite the claim as $\forall x\, \big((\neg(\exists y\, Q(x,y))) \vee P(x)\big) \;\equiv\; \forall x\, \exists y\, \big(\neg Q(x,y) \vee P(x)\big)$ By De Morgan's Law, distributing the negation on the right side of the equivalence changes the $\exists y$ to $\forall y$, and the two sides are clearly not the same. Another approach to the problem is to consider by linguistic example. Let x and y span the universe of all people, and let $Q(x,y)$ mean "Person x is Person y's offspring", and let $P(x)$ mean "Person x likes tofu". The right side claims that, for all Persons x, there exists some Person y such that either Person

x is not Person y's offspring or that Person x likes tofu. The left side claims that, for all Persons x, if there exists a parent of Person x, then Person x likes tofu. Obviously, these are not the same.

4 Counterfeit Coins

(a) Suppose you have 9 gold coins that look identical, but you also know one (and only one) of them is counterfeit. The counterfeit coin weighs slightly less than the others. You also have access to a balance scale to compare the weight of two sets of coins — i.e., it can tell you whether one set of coins is heavier, lighter, or equal in weight to another (and no other information). However, your access to this scale is very limited.

Can you find the counterfeit coin using *just two weighings*? Prove your answer.

(b) Now consider a generalization of the same scenario described above. You now have 3^n coins, $n \geq 1$, only one of which is counterfeit. You wish to find the counterfeit coin with just n weighings. Can you do it? Prove your answer.

Solution:

(a) Yes. We provide a constructive proof.

Divide this set of coins into 3 subsets of 3 each. Select two of these subsets to weigh on the balance scale. If one subset is lighter than the other, that must be the one with the counterfeit coin. If both are equal weight, the third subset must contain the counterfeit coin.

Now from this subset of 3 coins, select two coins, put one each on either side of the balance scale. If one side is lighter, that's the counterfeit coin. If both equal, the third coin is counterfeit.

(b) Proof by induction.

Base case. Select two coins, put one each on either side of the balance scale. If one side is lighter, that's the counterfeit coin. If both equal, the third coin is counterfeit.

Induction step. Assume for 3^n coins, the counterfeit coin can be detected in n weighings. Now consider 3^{n+1} coins. Divide this set of coins into 3 subsets of 3^n each. Select two of these subsets to weigh on the balance scale. If one subset is lighter than the other, that must be the one with the counterfeit coin. If both are equal weight, the third subset must contain the counterfeit coin.

From the induction hypothesis, you can now detect the counterfeit coin from the identified subset in n weighings. Thus we have $n+1$ weighings overall.

5 Proof Checker

In this question, you will play "CS70 Grader": you are tasked with checking someone else's attempt at a proof. For each of the "proofs" below, say whether you think it is correct or incorrect. If you think the proof is incorrect, explain clearly and concisely where the logical error in the proof lies. (If you think the proof is correct, you do not need to give any explanation.) Simply saying that the claim (or the inductive hypothesis) is false is not a valid explanation.

(a) **Claim**: for all $n \in \mathbb{N}$, $(2n+1$ is a multiple of $3) \implies (n^2+1$ is a multiple of $3)$.

Proof: proof by contraposition. Assume $2n+1$ is not a multiple of 3.

- If $n = 3k+1$ for $k \in \mathbb{N}$, then $n^2+1 = 9k^2+6k+2$ is not a multiple of 3.
- If $n = 3k+2$ for $k \in \mathbb{N}$, then $n^2+1 = 9k^2+12k+5$ is not a multiple of 3.
- If $n = 3k+3$ for $k \in \mathbb{N}$, then $n^2+1 = 9k^2+18k+10$ is not a multiple of 3.

In all cases, we have concluded n^2+1 is not a multiple of 3, so we have proved the claim.

(b) **Claim**: for all $n \in \mathbb{N}$, $n < 2^n$.

Proof: the proof will be by induction on n.

- Base case: suppose that $n = 0$. $2^0 = 1$ which is greater than 0, so the statement is true for $n = 0$.
- Inductive hypothesis: assume $n < 2^n$.
- Inductive step: we need to show that $n+1 < 2^{n+1}$. By the inductive hypothesis, we know that $n < 2^n$. Plugging in $n+1$ in place of n, we get $n+1 < 2^{n+1}$, which is what we needed to show. This completes the inductive step.

(c) **Claim**: for all $x, y, n \in \mathbb{N}$, if $\max(x,y) = n$, then $x \leq y$.

Proof: the proof will be by induction on n.

- Base case: suppose that $n = 0$. If $\max(x,y) = 0$ and $x, y \in \mathbb{N}$, then $x = 0$ and $y = 0$, hence $x \leq y$.
- Inductive hypothesis: assume that, whenever we have $\max(x,y) = k$, then $x \leq y$ must follow.
- Inductive step: we must prove that if $\max(x,y) = k+1$, then $x \leq y$. Suppose x, y are such that $\max(x,y) = k+1$. Then, it follows that $\max(x-1, y-1) = k$, so by the inductive hypothesis, $x-1 \leq y-1$. In this case, we have $x \leq y$, completing the induction step.

Solution:

(a) The proof is incorrect. You want to prove an implication of the form $P(n) \implies Q(n)$ for every n, where $P(n)$ is "$2n+1$ is a multiple of 3" and $Q(n)$ is "n^2+1 is a multiple of 3". The contrapositive is $\neg Q(n) \implies \neg P(n)$. Your proof begins with $\neg P(n)$ and concludes with

$\neg Q(n)$, so you have shown $\neg P(n) \implies \neg Q(n)$, which is the converse, not contrapositive. Besides, $n = 0$ is not covered in the proof. Note: when $n = 3k+1$, $2n+1 = 6k+3$ is a multiple of 3, so the case is redundant to prove $\neg P(n) \implies \neg Q(n)$.

(b) Using induction requires showing that, given a true proposition $P(n)$, it follows that $P(n+1)$. This proof simply changes n to $n+1$, which is not valid justification for induction. The inductive hypothesis must assume that the theorem is true for some value of n, not for every value of n. One way to make this proof valid would be to show that, given $n < 2^n$ for some $n \geq 0$, multiplying the right side by 2 will increase it by at least one. Then, it follows that $n+1 < 2^{n+1}$, which completes justification for induction.

(c) The problem lies in the application of the inductive hypothesis. More specifically, the incorrect step is: "Then it follows that $\max(x-1, y-1) = k-1$, so by the inductive hypothesis, $x-1 \leq y-1$." The problem is that $x-1$ or $y-1$ might be negative (this happens when $x = 0$ or $y = 0$). Then the inductive hypothesis no longer applies, since $x-1$ and $y-1$ are not both natural numbers, so we cannot conclude that $x-1 \leq y-1$.

6 Preserving Set Operations

Prove that inverse images preserve set operations but images typically do not:

1. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.
2. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.
3. $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.
4. $f(A \cup B) = f(A) \cup f(B)$.
5. $f(A \cap B) \subseteq f(A) \cap f(B)$, and give an example where equality does not hold.
6. $f(A \setminus B) \supseteq f(A) \setminus f(B)$, and give an example where equality does not hold.

Solution:

In order to prove equality $A = B$, we need to prove that A is a subset of B, $A \subset B$ and that B is a subset of A, $B \subset A$. To prove that LHS is a subset of RHS we need to prove that if an element is a member of LHS then it is also an element of the RHS.

1. Suppose x is such that $f(x) \in A \cup B$. Then either $f(x) \in A$, in which case $x \in f^{-1}(A)$, or $f(x) \in B$, in which case $x \in f^{-1}(B)$, so in either case we have $x \in f^{-1}(A) \cup f^{-1}(B)$. This proves that $f^{-1}(A \cup B) \subseteq f^{-1}(A) \cup f^{-1}(B)$.

   Now, suppose that $x \in f^{-1}(A) \cup f^{-1}(B)$. Suppose, without loss of generality, that $x \in f^{-1}(A)$. Then $f(x) \in A$, so $f(x) \in A \cup B$, so $x \in f^{-1}(A \cup B)$. The argument for $x \in f^{-1}(B)$ is the same. Hence, $f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B)$.

2. Suppose x is such that $f(x) \in A \cap B$. Then $f(x)$ lies in both A and B, so x lies in both $f^{-1}(A)$ and $f^{-1}(B)$, so $x \in f^{-1}(A) \cap f^{-1}(B)$. So $f^{-1}(A \cap B) \subseteq f^{-1}(A) \cap f^{-1}(B)$.

   Now, suppose that $x \in f^{-1}(A) \cap f^{-1}(B)$. Then, x is in both $f^{-1}(A)$ and $f^{-1}(B)$, so $f(x) \in A$ and $f(x) \in B$, so $f(x) \in A \cap B$, so $x \in f^{-1}(A \cap B)$. So $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$.

3. Suppose x is such that $f(x) \in A \setminus B$. Then, $f(x) \in A$ and $f(x) \notin B$, which means that $x \in f^{-1}(A)$ and $x \notin f^{-1}(B)$, which means that $x \in f^{-1}(A) \setminus f^{-1}(B)$. So $f^{-1}(A \setminus B) \subseteq f^{-1}(A) \setminus f^{-1}(B)$.

   Now, suppose that $x \in f^{-1}(A) \setminus f^{-1}(B)$. Then, $x \in f^{-1}(A)$ and $x \notin f^{-1}(B)$, so $f(x) \in A$ and $f(x) \notin B$, so $f(x) \in A \setminus B$, so $x \in f^{-1}(A \setminus B)$. So $f^{-1}(A) \setminus f^{-1}(B) \subseteq f^{-1}(A \setminus B)$.

4. Suppose that $x \in A \cup B$. Then either $x \in A$, in which case $f(x) \in f(A)$, or $x \in B$, in which case $f(x) \in f(B)$. In either case, $f(x) \in f(A) \cup f(B)$, so $f(A \cup B) \subseteq f(A) \cup f(B)$.

   Now, suppose that $y \in f(A) \cup f(B)$. Then either $y \in f(A)$ or $y \in f(B)$. In the first case, there is an element $x \in A$ with $f(x) = y$; in the second case, there is an element $x \in B$ with $f(x) = y$. In either case, there is an element $x \in A \cup B$ with $f(x) = y$, which means that $y \in f(A \cup B)$. So $f(A) \cup f(B) \subseteq f(A \cup B)$.

5. Suppose $x \in A \cap B$. Then, x lies in both A and B, so $f(x)$ lies in both $f(A)$ and $f(B)$, so $f(x) \in f(A) \cap f(B)$. Hence, $f(A \cap B) \subseteq f(A) \cap f(B)$.

   Consider when there are elements $a \in A$ and $b \in B$ with $f(a) = f(b)$, but A and B are disjoint. Here, $f(a) = f(b) \in f(A) \cap f(B)$, but $f(A \cap B)$ is empty (since $A \cap B$ is empty).

6. Suppose $y \in f(A) \setminus f(B)$. Since y is not in $f(B)$, there are no elements in B which map to y. Let x be any element of A that maps to y; by the previous sentence, x cannot lie in B. Hence, $x \in A \setminus B$, so $y \in f(A \setminus B)$. Hence, $f(A) \setminus f(B) \subseteq f(A \setminus B)$.

   Consider when $B = \{0\}$ and $A = \{0, 1\}$, with $f(0) = f(1) = 0$. One has $A \setminus B = \{1\}$, so $f(A \setminus B) = \{0\}$. However, $f(A) = f(B) = \{0\}$, so $f(A) \setminus f(B) = \varnothing$.

7 Grid Induction

A bug is walking on an infinite 2D grid. He starts at some location $(i, j) \in \mathbb{N}^2$ in the first quadrant, and is constrained to stay in the first quadrant (say, by walls along the x and y axes). Every second he does one of the following (if possible):

(i) Jump one inch down, to $(i, j-1)$.

(ii) Jump one inch left, to $(i-1, j)$.

For example, if he is at $(5, 0)$, his only option is to jump left to $(4, 0)$.

Prove that no matter how he jumps, he will always reach $(0, 0)$ in finite time.

Solution:

First, consider proving the statement for all starting locations $(x,0)$, by simple induction. Then prove $(0,1)$ directly (only one possible move). Then consider $(1,1)$: Depending on the move, this reduces to either $(0,1)$ or $(1,0)$. Use this idea to prove by strong induction for all starting locations $(x,1)$. Consider doing the same thing for all $(x,2)$, then generalize by induction for (x,y).

Finally, introduce and motivate the potential method as another way of solving the problem: turn the grid 45-degrees counter clockwise, so the bug always moves down. Its "potential energy" $\Phi = x+y$ decreases by exactly one every turn.

Here is an example proof:

We can strengthen the Induction Hypothesis to show that the number of steps required from (i,j) is exactly $i+j$ for all naturals $i,j \in \mathbb{N}$. The base case is obvious. For the induction step, the bug either moves to $(i,j-1)$ or $(i-1,j)$ in one step, and by the induction hypothesis a further $i+j-1$ steps are required, for total of $i+j$.

Next: What if the bug could jump left either 1 or 2 inches?

8 A Tricky Game

(a) CS 70 course staff invite you to play a game: Suppose there are n^2 coins in a $n \times n$ grid ($n > 0$), each with their heads side up. In each move, you can pick one of the n rows or columns and flip over all of the coins in that row or column. However, you are not allowed to re-arrange them in any other way. You have an unlimited number of moves. If you happen to reach a configuration where there is exactly one coin with its tails side up, you will win the game. Are you able to win this game? Find all values of n for which you can win the game, and prove your statement. In other words, for each value of n that you listed, prove that you can win the game; then, prove that it is impossible to win the game for all other values of n.

(b) (Optional) Now, suppose we change the rules: If the number of "tails" is between 1 and $n-1$, you win. Are you able to win this game? Does that apply to all n? Prove your answer.

Solution:

(a) When $n=1$, the answer is trivial. Let's then analyze the base case when $n=2$. We will prove the following lemma.

Lemma: The 2×2 puzzle is unwinnable.

Proof: Let P be the property that the number of coins in a configuration with heads side up on the 2×2 grid is even. Note that P is true initially, and moreover it is not disturbed by flipping of any row or column. Hence is a P is an invariant of the configuration. By induction on the number of moves, P holds after any number of moves, and so we can only reach configurations where P is true.

(In other words, we let $Q(k)$ denote the proposition that P holds after any sequence of k moves. The base case $Q(0)$ holds trivially. Also, $Q(k) \implies Q(k+1)$ holds for all $k \geq 0$, since every sequence of $k+1$ moves can be decomposed into a sequence of k moves followed by one more move, and if P holds before this last move, it holds after the last move, too, since P is not disturbed by flipping of any single row or column. Therefore by induction $Q(k)$ holds for all $k \geq 0$.)

But now the configuration with exactly one coins tails side up is incompatible with P and consequently is unreachable by any finite set of moves. Therefore the 2×2 puzzle is unwinnable.

Now, we will use the lemma to prove the following theorem.

Theorem: The $n \times n$ puzzle is winnable if and only if $n = 1$.

Proof: We show that the puzzle is unwinnable when $n \geq 3$. Suppose not, i.e., there is some winning sequence of moves that leaves just a single coin with "tails" side up at some location L. Consider any 2×2 sub-grid containing location L. Then we have found a sequence of moves which takes this 2×2 sub-grid from the initial all-heads position to a position containing 3 heads and 1 tail. But this is impossible, by the previous result. Hence our assumption that there exists a winning sequence of moves must have been impossible, which proves the theorem.

(b) Similarly, when $n = 1$, the answer is trivial. We will prove the following theorem:

Theorem: The game remains unwinnable for all $n \geq 2$.

Proof: Consider any pair of rows of coins. Let P be the property that the two rows are identically configured, and Q be the property that these two rows are exact inverses of each other (i.e., each head in the first row corresponds to a tail in the second row, and vice versa). Then (for every pair of rows) $P \vee Q$ is an invariant of the game, since it holds initially and is not disturbed by any move.

Now there are only two cases: either there is some winning sequence of moves, or there is not. In the former case, in the winning final configuration some rows must have t tails, for some $1 \leq t \leq n-1$. This implies that every other row has either t or $n-t$ tails in it (according to whether it is P or Q that is true for this pair of rows), and since $t \geq 1$ and $n-t \geq 1$, this means that every row must have at least one coin with "tails" side up, for a total of at least n tails in the winning configuration. This is an absurdity. But this means the first case is impossible, hence the second case must always hold, and there can be no winning the puzzle when $n \geq 2$.