CS 70	Discrete Mathematics and Probability Theory	
Fall 2016	Seshia and Walrand	HW 1

Due Friday September 2 at 10PM

1. (10 points)

   (a) For each question, circle whether the statement is true or false.

   T F $\forall x \in \mathbb{Z}, x+1 \in \mathbb{Z}$.

   Answer: True. The statement, when translated into English, reads "for all integers x, $x+1$ is an integer."

   T F $\forall x \in \mathbb{Z}$, if $\frac{x}{2} \in \mathbb{Z}$ then $\frac{x+1}{2} \in \mathbb{Z}$.

   Answer: False. The statement reads "for all integers x, if $\frac{x}{2}$ is an integer, then $\frac{x+1}{2}$ is an integer." To disprove this statement, we simply need to show a counterexample. For example if $x = 2$, then $\frac{x}{2} = 1$ is an integer, but $\frac{x+1}{2} = \frac{3}{2}$ is not an integer.

   T F $\forall x \in \mathbb{Z}$, if $\frac{x}{2} \notin \mathbb{Z}$ then $\frac{x+1}{2} \in \mathbb{Z}$.

   Answer: True. The statement reads "for all integers x, if $\frac{x}{2}$ is not an integer, then $\frac{x+1}{2}$ is an integer." If $\frac{x}{2}$ is not an integer, it means that x is not even. But every number is either even or odd, so x must be odd. Therefore $x+1$ is even, and so $x+1$ is divisible by 2. Hence $\frac{x+1}{2}$ is an integer.

   T F $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}\ s.t.\ xy = 1$.

   Answer: False. The statement reads "for all integers x, there exists an integer y such that $xy = 1$." To disprove this, we simply need to provide a counterexample x. If we take $x = 2$, then no matter what y is, xy is going to be an even number, so xy can never be 1 for any integer y.

   T F $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Q}\ s.t.\ xy = 1$.

   Answer: False. The statement reads "for all integers x, there exists a rational number y such that $xy = 1$." This statement is valid for almost all x's; but it has a single counterexample. If we take $x = 0$, then no matter what y is, $xy = 0$. So for that particular x, $\nexists y \in \mathbb{Q}\ s.t.\ xy = 1$.

   (b) Consider the expression $\sum_{i=0}^{n} f(i)$. Circle each of the following expressions that it is equal to. Justify your answers.

   - $f(0) \cdot f(1) \cdot f(2) \cdots f(n-1) \cdot f(n)$

     Answer: Not equal. This expression is the product of $f(0), f(1), \ldots, f(n)$, whereas we were looking for the sum. As a counter example take $n = 1$, and $f(0) = 0$ and $f(1) = 1$. Then $\sum_{i=0}^{n} f(i) = 1$, whereas $f(0) \cdot f(1) = 0$.

   - $\sum_{i=0}^{n-1} (f(i) + f(n))$

     Answer: Not equal. The term $f(n)$ gets repeated $n-1$ times (once for each value of i) in this expression whereas it should appear just once. As a counter example take $n = 2$, and f to be the constant function 1. Then $\sum_{i=0}^{n} f(i) = 3$. But $\sum_{i=0}^{n-1} (f(i) + f(n)) = \sum_{i=0}^{1} 2 = 4$.

- $\left(\sum_{i=0}^{n-1} f(i)\right) + f(n)$

  Answer: Equal. The sum of n terms is always the sum of the first $n-1$ terms added with the last term. This expression is just that.

- $f(0) + f(1) + \cdots + f(n)$

  Answer: Equal. This is the sum of the n terms expanded in an explicit way.

- $\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} f(i) + \sum_{j=\lfloor \frac{n}{2} \rfloor + 1}^{n} f(j)$

  Answer: Equal. For any integer $0 \leq c < n$, we can break the sum $\sum_{i=0}^{n} f(i)$ into two parts: the sum of the terms where $i \leq c$ and the sum of the terms where $i \geq c+1$. Thus $\sum_{i=0}^{n} f(i) = \sum_{i=0}^{c} f(i) + \sum_{j=c+1}^{n} f(j)$. The expression in this statement is the special case where $c = \lfloor \frac{n}{2} \rfloor$

2. (3 points) Suppose we have four cards on a table. Each card has a color on one side (red, blue, or green) and a shape on the other side (square, circle, or triangle).

   Consider the following theory: "If a card is red, then it has a square on the other side."

   Suppose the sides facing up are as follows: red, blue, square, triangle.

   Which cards do you need to flip to test the theory?

   Answer: (This is a version of the "Wason selection task" devised by Peter Wason in 1966.)

   Two cards: red and triangle.

   If a card is blue on one side, it violates the antecedent (premise) of the implication, so you don't need to flip it.

   If it has a square, then it doesn't matter, the theory says nothing about the other side.

   The other two cases must be tested. If red, we need to check that the other side has a square. If triangle, we need to make sure that the other side is not red (contrapositive).

3. (8 points) Prove or Disprove.

   (a) $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$.

   Answer: True.

A	B	C	$A \vee (B \wedge C)$	$(A \vee B) \wedge (A \vee C)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

   (b) $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$.

Answer: True.

A	B	C	$A \wedge (B \vee C)$	$(A \wedge B) \vee (A \wedge C)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	F	F
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

(c) $A \implies (B \wedge C) \equiv (A \implies B) \wedge (A \implies C)$

Answer: True.

A	B	C	$A \implies (B \wedge C)$	$(A \implies B) \wedge (A \implies C)$
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	T	T

(d) $A \implies (B \vee C) \equiv (A \implies B) \vee (A \implies C)$

Answer: True.

A	B	C	$A \implies (B \vee C)$	$(A \implies B) \vee (A \implies C)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	F
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	T	T

4. (20 points) Propositional logic and Boolean circuits
The exclusive OR (written as XOR or $\oplus$) is just what it sounds like: $P \oplus Q$ is true when exactly one of P, Q is true.

(a) Show, using a truth table, that $P \oplus Q$ is equivalent to $(P \vee Q) \wedge \neg(P \wedge Q)$.

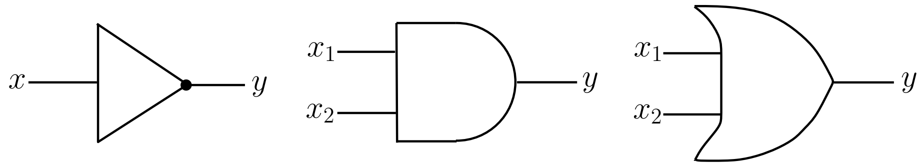
Answer: The truth tables can be found below.

P	Q	$P \vee Q$	$P \wedge Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge \neg(P \wedge Q)$
false	false	false	false	true	false
false	true	true	false	true	true
true	false	true	false	true	true
true	true	true	true	false	false

P	Q	$P \oplus Q$
false	false	false
false	true	true
true	false	true
true	true	false

The truth tables result in the same truth values. Therefore the two expressions are equivalent.

(b) Logic is key to many fundamental areas of computer science such as digital circuits. Below you can see the symbols for some of the common gates used in digital circuits. The wires all carry boolean values (true or false), and the ones coming in from the left are *input*s and the ones exiting from the right are *output*s.



These gates, from left to right, are NOT, AND, and OR. Below you can find their truth tables

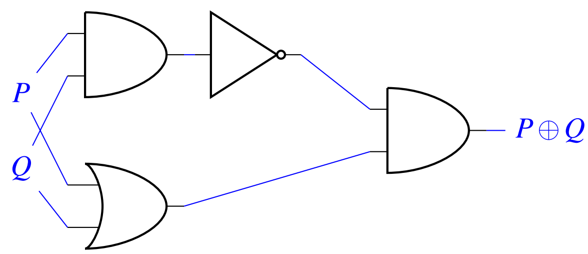
x	y
false	true
true	false

x_1	x_2	y
false	false	false
false	true	false
true	false	false
true	true	true

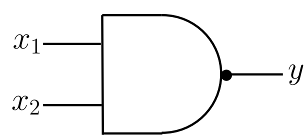
x_1	x_2	y
false	false	false
false	true	true
true	false	true
true	true	true

Using these logical gates, implement XOR. Assume that two input wires P and Q are given to you. Connect them using AND, OR, and NOT gates and produce an output wire whose value is always $P \oplus Q$. Draw the circuit you designed using the standard symbols for the gates.

Answer: We simply need to implement the expression from the previous part, which uses only $\neg, \vee, \wedge$ which correspond directly to NOT, OR, and AND gates. Below you can find the diagram corresponding to such implementation.



(c) (Optional) Another common gate used in hardware chips, is the NAND gate, which can be thought of as an AND whose output is inverted. Below you can find the symbol and the truth table for the NAND gate.



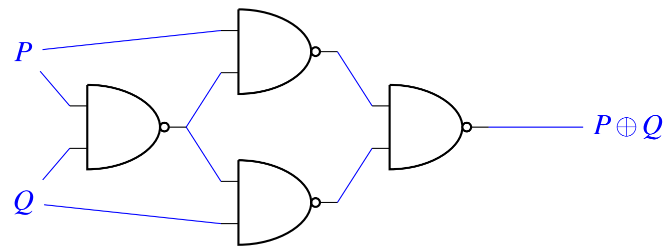
x_1	x_2	y
false	false	true
false	true	true
true	false	true
true	true	false

Implement XOR using the minimal number of NAND gates. You may only use NAND gates, and no other gate.

Answer: We can implement each of the AND, OR, and NOT gates using NAND gates. But that does not necessarily use the minimum number of NAND gates. One can simply try to construct the truth tables for expressions built from just the NAND gate. Below you can find some of them.

P	Q	NAND(P,Q)	NAND(P,P)	NAND(Q,Q)	NAND$(P,\text{NAND}(P,Q))$
false	false	true	true	true	true
false	true	true	true	false	true
true	false	true	false	true	false
true	true	false	false	false	true

We can continue to write down the expressions that use at most two NANDs. Then we can see which ones combine to give us $P \oplus Q$. If we write down the expression NAND$(Q,\text{NAND}(P,Q))$ and take its NAND with NAND$(P,\text{NAND}(P,Q))$ we will get $P \oplus Q$. Note that this can be actually implemented with 4 NANDs because these two expressions share the NAND(P,Q) part. A little bit of search shows that using 3 NANDs we cannot implement the truth table for $P \oplus Q$. The diagram below depicts the answer with 4 NANDs.



5. (9 points)

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

(a) (3 points) $\forall x\, \exists y\, \big(P(x) \Rightarrow Q(x,y)\big) \;\equiv\; \forall x\, \big(P(x) \Rightarrow (\exists y\, Q(x,y))\big)$

Answer: 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) (3 points) $\neg \exists x\, \forall y\, \big(P(x,y) \Rightarrow \neg Q(x,y)\big) \;\equiv\; \forall x\, \big((\exists y\, P(x,y)) \wedge (\exists y\, Q(x,y))\big)$

Answer: 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) (3 points) $\forall x\, \exists y\, \big(Q(x,y) \Rightarrow P(x)\big) \;\equiv\; \forall x\, \big((\exists y\, Q(x,y)) \Rightarrow P(x)\big)$

Answer: 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.

6. (20 points) Counterfeit Coins

(a) (8 points) 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.

Answer: 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) (12 points) 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.

Answer: 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.

7. (15 points) 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 $n \in \mathbb{N}$, $(2n+1 \text{ is a multiple of } 3) \implies (n^2+1 \text{ is a multiple of } 3)$.

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.

Answer:

(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 $\neg P(n) \implies \neg Q(n)$ (bonus points will be given for pointing this out).

(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 $x-1 \leq y-1$.

8. (15 points) Prove or disprove each of the following statements. For each proof, state which of the proof types (as discussed in Note 2) you used.

(a) (3 points) For all natural numbers n, if n is odd then n^2+3n is even.

Answer: True.

Proof: We will use a direct proof. Assume n is odd. By the definition of odd numbers, $n = 2k+1$ for some natural number k. Substituting into the expression n^2+3n, we get $(2k+1)^2 + 3 \times (2k+1)$. Simplifying the expression yields $4k^2+10k+4$. This can be rewritten as $2 \times (2k^2+5k+2)$. Since $2k^2+5k+2$ is a natural number, by the definition of even numbers, n^2+3n is even. ■

(b) (3 points) For all real numbers a, b, if $a+b \geq 20$ then $a \geq 17$ or $b \geq 3$.

Answer: True.

Proof: We will use a proof by contraposition. Suppose that $a < 17$ and $b < 3$ (note that this is equivalent to $\neg(a \geq 17 \vee b \geq 3)$). Since $a < 17$ and $b < 3$, $a+b < 20$ (note that $a+b < 20$ is equivalent to $\neg(a+b \geq 20)$). Thus, if $a+b \geq 20$, then $a \geq 17$ or $b \geq 3$ (or both, as "or" is not "exclusive or" in this case). By contraposition, for all real numbers a, b, if $a + b \geq 20$ then $a \geq 17$ or $b \geq 3$. ■

(c) (3 points) For all real numbers r, if r is irrational then $r+1$ is irrational.

Answer: True.
Proof: We will use a proof by contraposition. Assume that $r+1$ is rational. Since $r+1$ is rational, it can be written in the form a/b where a and b are integers. Then r can be written as $(a-b)/b$. By the definition of rational numbers, r is a rational number, since both $a-b$ and b are integers. By contraposition, if r is irrational, then $r+1$ is irrational. ■

(d) (3 points) For all natural numbers n, $10n^3 > n!$.

Answer: False.
Proof: We will use proof by counterexample. Let $n = 10$. $10 \times 10^3 = 10,000$. $(10!) = 3,628,800$. Since $10n^3 < n!$, the claim is false. ■

(e) (3 points) For all natural numbers a where a^5 is odd, then a is odd.

Answer: True.
Proof: This will be proof by contrapositive. The contrapositive is "If a is even, then a^5 is even." Let a be even. By the definition of even, $a = 2k$. Then $a^5 = (2k)^5 = 2(16k^5)$, which implies a^5 even. By contraposition, for all natural numbers a where a^5 is odd, then a is odd. ■