CS 70 Discrete Mathematics and Probability Theory
Fall 2019 Alistair Sinclair and Yun S. Song

HW 1

Note: *This homework consists of two parts. The first part (questions 1-5) will be graded and will determine your score for this homework. The second part (questions 6-8) will be graded if you submit them, but will not affect your homework score in any way. You are strongly advised to attempt all the questions in the first part. You should attempt the problems in the second part only if you are interested and have time to spare.*

Part 1: Required Problems

1 Propositional Practice

In parts (a)-(c), convert the English sentences into propositional logic. In parts (d)-(f), convert the propositions into English. In part (f), let $P(a)$ represent the proposition that a is prime.

(a) There is one and only one real solution to the equation $x^2 = 0$.

(b) Between any two distinct rational numbers, there is another rational number.

(c) If the square of an integer is greater than 4, that integer is greater than 2 or it is less than -2.

(d) $(\forall x \in \mathbb{R})\ (x \in \mathbb{C})$

(e) $(\forall x, y \in \mathbb{Z})(x^2 - y^2 \neq 10)$

(f) $(\forall x \in \mathbb{N})\ [\ (x > 1) \implies (\exists a, b \in \mathbb{N})\ ((a + b = 2x) \wedge P(a) \wedge P(b))\ ]$

Solution:

(a) Let $p(x) = x^2$. The sentence can be read: "There is a solution x to the equation $p(x) = 0$, and any other solution y is equal to x". Or,

$$(\exists x \in \mathbb{R})\,((p(x) = 0) \wedge ((\forall y \in \mathbb{R})(p(y) = 0) \implies (x = y)))\,.$$

(b) The sentence can be read "If x and y are distinct rational numbers, then there is a rational number z between x and y." Or,

$$(\forall x, y \in \mathbb{Q})((x \neq y) \implies ((\exists z \in \mathbb{Q})(x < z < y \vee y < z < x))).$$

Equivalently,

$$(\forall x, y \in \mathbb{Q})((x = y) \vee (\exists z \in \mathbb{Q})(x < z < y \vee y < z < x)).$$

Note that $x < z < y$ is mathematical shorthand for $(x < z) \land (z < y)$, so the above statement is equivalent to

$$(\forall x, y \in \mathbb{Q})(x = y) \lor ((\exists z \in \mathbb{Q})((x < z) \land (z < y)) \lor ((y < z) \land (z < x))).$$

(c) $(\forall x \in \mathbb{N})\ ((x^2 > 4) \implies ((x > 2) \lor (x < -2)))$

(d) All real numbers are complex numbers.

(e) There are no integer solutions to the equation $x^2 - y^2 = 10$.

(f) For any natural number greater than 1, there are some prime numbers a and b such that $2x = a + b$.

In other words: Any even integer larger than 2 can be written as the sum of two primes.

Aside: This statement is known as Goldbach's Conjecture, and it is a famous unsolved problem in number theory (`https://xkcd.com/1310/`).

2 Tautologies and Contradictions

Classify each statement as being one of the following, where P and Q are arbitrary propositions:

- True for all combinations of P and Q (Tautology)
- False for all combinations of P and Q (Contradiction)
- Neither

Justify your answers with a truth table.

(a) $P \implies (Q \land P) \lor (\neg Q \land P)$

(b) $(P \lor Q) \lor (P \lor \neg Q)$

(c) $P \land (P \implies \neg Q) \land (Q)$

(d) $(\neg P \implies Q) \implies (\neg Q \implies P)$

(e) $(\neg P \implies \neg Q) \land (P \implies \neg Q) \land (Q)$

(f) $(\neg(P \land Q)) \land (P \lor Q)$

Solution:

(a) **Tautology**

P	Q	$Q \land P$	$\neg Q \land P$	$P \implies (Q \land P) \lor (\neg Q \land P)$
T	T	T	F	T
T	F	F	T	T
F	T	F	F	T
F	F	F	F	T

(b) **Tautology**

P	Q	$P \vee Q$	$P \vee \neg Q$	$(P \vee Q) \vee (P \vee \neg Q)$
T	T	T	T	T
T	F	T	T	T
F	T	T	F	T
F	F	F	T	T

(c) **Contradiction**

P	Q	$P \implies \neg Q$	$P \wedge (P \implies Q) \wedge (Q)$
T	T	F	F
T	F	T	F
F	T	T	F
F	F	T	F

(d) **Tautology**

P	Q	$\neg P \implies Q$	$\neg Q \implies P$	$(\neg P \implies Q) \implies (\neg Q \implies P)$
T	T	T	T	T
T	F	T	T	T
F	T	T	T	T
F	F	F	F	T

(e) **Contradiction**

P	Q	$P \implies \neg Q$	$\neg P \implies \neg Q$	$(P \implies \neg Q) \wedge (\neg P \implies \neg Q) \wedge (Q)$
T	T	F	T	F
T	F	T	T	F
F	T	T	F	F
F	F	T	T	F

(f) **Neither**

P	Q	$P \vee Q$	$\neg(P \wedge Q)$	$(P \vee Q) \wedge (\neg(P \wedge Q))$
T	T	T	F	F
T	F	T	T	T
F	T	T	T	T
F	F	F	T	F

3 Implication

Which of the following assertions are true no matter what proposition Q represents? For any false assertion, state a counterexample (i.e. come up with a statement $Q(x,y)$ that would make the implication false). For any true assertion, give a brief explanation for why it is true.

(a) $\exists x \exists y Q(x,y) \implies \exists y \exists x Q(x,y)$.

(b) $\forall x \exists y Q(x,y) \implies \exists y \forall x Q(x,y)$.

(c) $\exists x \forall y Q(x,y) \implies \forall y \exists x Q(x,y)$.

(d) $\exists x \exists y Q(x,y) \implies \forall y \exists x Q(x,y)$.

Solution:

(a) True. There exists can be switched if they are adjacent; $\exists x, \exists y$ and $\exists y, \exists x$ means there exists x and y in our universe.

(b) False. Let $Q(x,y)$ be $x < y$, and the universe for x and y be the integers. Or let $Q(x,y)$ be $x = y$ and the universe be any set with at least two elements. In both cases, the antecedent is true and the consequence is false, thus the entire implication statement is false.

(c) True. The first statement says that there is an x, say x' where for every y, $Q(x,y)$ is true. Thus, one can choose $x = x'$ for the second statement and that statement will be true again for every y. Note: 4c and 4d are not logically equivalent. In fact, the converse of 4d is 4c, which we saw is false.

(d) False. Suppose Q is the statement "y is 5, and x is any integer". The antecedent is true when $y = 5$, but for $y \neq 5$, there is no x that will make it true.

4 Prove or Disprove

(a) $(\forall n \in \mathbb{N})$ if n is odd then $n^2 + 4n$ is odd.

(b) $(\forall a, b \in \mathbb{R})$ if $a + b \leq 15$ then $a \leq 11$ or $b \leq 4$.

(c) $(\forall r \in \mathbb{R})$ if r^2 is irrational, then r is irrational.

(d) $(\forall n \in \mathbb{Z}^+)$ $5n^3 > n!$. (Note: $\mathbb{Z}^+$ is the set of positive integers)

Solution:

(a) **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 $n^2 + 4n$, we get $(2k+1)^2 + 4 \times (2k+1)$. Simplifying the expression yields $4k^2 + 12k + 5$. This can be rewritten as $2 \times (2k^2 + 6k + 2) + 1$. Since $2k^2 + 6k + 2$ is a natural number, by the definition of odd numbers, $n^2 + 4n$ is odd.
Alternatively, we could also factor the expression to get $n(n+4)$. Since n is odd, $n+4$ is also odd. The product of 2 odd numbers is also an odd number. Hence $n^2 + 4n$ is odd.

(b) **Answer**: True.
Proof: We will use a proof by contraposition. Suppose that $a > 11$ and $b > 4$ (note that this is equivalent to $\neg(a \leq 11 \vee b \leq 4)$). Since $a > 11$ and $b > 4$, $a + b > 15$ (note that $a + b > 15$ is equivalent to $\neg(a + b \leq 15)$). Thus, if $a + b \leq 15$, then $a \leq 11$ or $b \leq 4$.

(c) **Answer**: True.

Proof: We will use a proof by contraposition. Assume that r is rational. Since r is rational, it can be written in the form $\frac{a}{b}$ where a and b are integers with $b \neq 0$. Then r^2 can be written as $\frac{a^2}{b^2}$. By the definition of rational numbers, r^2 is a rational number, since both a^2 and b^2 are integers, with $b \neq 0$. By contraposition, if r^2 is irrational, then r is irrational.

(d) **Answer**: False.

Proof: We will use proof by counterexample. Let $n = 7$. $5 \times 7^3 = 1715$. $7! = 5040$. Since $5n^3 < n!$, the claim is false.

5 Twin Primes

(a) Let $p > 3$ be a prime. Prove that p is of the form $3k+1$ or $3k-1$ for some integer k.

(b) *Twin primes* are pairs of prime numbers p and q that have a difference of 2. Use part (a) to prove that 5 is the only prime number that takes part in two different twin prime pairs.

Solution:

(a) First we note that any integer can be written in one of the forms $3k$, $3k+1$, or $3k+2$. (Note that $3k+2$ is equal to $3(k+1)-1$. Since k is arbitary, we can treat these as equivalent forms).

We can now prove the contrapositive: that any integer $m > 3$ of the form $3k$ must be composite. Any such integer is divisible by 3, so this is true right away. Thus our original claim is true as well.

(b) We can check all the primes up to 5 to see that of these, only 5 takes part in two twin prime pairs (3,5 and 5,7). What about primes > 5?

For any prime $m > 5$, we can check if $m+2$ and $m-2$ are both prime. We can do a proof by cases based on the two forms from part (a).

Case 1: m is of the form $3k+1$. Then $m+2 = 3k+3$, which is divisible by 3. So $m+2$ is not prime.

Case 2: m is of the form $3k-1$. Then $m-2 = 3k-3$, which is divisible by 3. So $m-2$ is not prime.

So in either case, at least one of $m+2$ and $m-2$ is not prime.

Note: *This concludes the first part of the homework. The problems below are optional, will not affect your score, and should be attempted only if you have time to spare.*

Part 2: Optional Problems

6 Social Network

Suppose that $p_1, p_2, \dots, p_n$ denote n people where every two people are either friends or strangers. Let Friends(x,y) be the predicate "x and y are friends". Prove or provide a counterexample for the following statements.

(a) For all cases with $n = 5$ people, there exists a group of 3 people that are either all friends or all strangers. In mathematical notation we write this as:

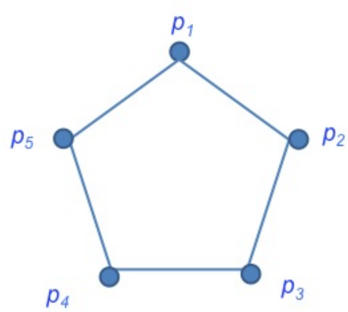
$$\exists(i,j,k) \in \{1,2,\dots,5\}^3 \text{ such that } i<j<k \text{ and } (\text{Friends}(p_i,p_j) \wedge \text{Friends}(p_j,p_k) \wedge \text{Friends}(p_i,p_k)) \vee (\neg\text{Friends}(p_i,p_j) \wedge \neg\text{Friends}(p_j,p_k) \wedge \neg\text{Friends}(p_i,p_k)).$$

(b) For all cases with $n = 6$ people, there exists a group of 3 people that are either all friends or all strangers. In mathematical notation we write this as:

$$\exists(i,j,k) \in \{1,2,\dots,6\}^3 \text{ such that } i<j<k \text{ and } (\text{Friends}(p_i,p_j) \wedge \text{Friends}(p_j,p_k) \wedge \text{Friends}(p_i,p_k)) \vee (\neg\text{Friends}(p_i,p_j) \wedge \neg\text{Friends}(p_j,p_k) \wedge \neg\text{Friends}(p_i,p_k)).$$

Solution:

(a) The statement is false. A counterexample is shown below where people are connected if they are friends and unconnected if they are strangers. In this example, at most 2 are friends or strangers.



(b) The statement is true.

Proof: For any person p_i, we could divide the rest of people into 2 groups: the group of p_i's friends and the group of strangers. One of the groups must have at least 3 people.

Case (1): At least 3 people are p_i's friends.

Let $\{j,k,l\} \subset \{1,2,\dots,6\} \setminus \{i\}$ and $j<k<l$ (distinct) such that

$$(\text{Friends}(p_j,p_i) \wedge \text{Friends}(p_k,p_i) \wedge \text{Friends}(p_l,p_i)).$$

If p_j, p_k, and p_l are all strangers, the statement is true. If not, $\exists\{m,n\} \subset \{i,j,k\}$ where $m < n$ (distinct) such that Friends(p_m, p_n). Then p_m, p_n, and p_i are all friends.

Case (2): At least 3 people are strangers to p_i.

Let $\{j,k,l\} \subset \{1,2,\ldots,6\} \setminus \{i\}$ and $j < k < l$ (distinct) such that

$$(\neg \text{Friends}(p_j, p_i) \wedge \neg \text{Friends}(p_k, p_i) \wedge \neg \text{Friends}(p_l, p_i)).$$

If p_j, p_k, and p_l are all friends, the statement is true. If not, $\exists\{m,n\} \subset \{i,j,k\}$ where $m < n$ (distinct) such that $\neg$Friends(p_m, p_n). Then p_m, p_n, and p_i are all strangers.

7 Preserving Set Operations

For a function f, define the image of a set X to be the set $f(X) = \{y \mid y = f(x) \text{ for some } x \in X\}$. Define the inverse image or preimage of a set Y to be the set $f^{-1}(Y) = \{x \mid f(x) \in Y\}$. Prove the following statements, in which A and B are sets. By doing so, you will show that inverse images preserve set operations, but images typically do not.

Hint: For sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. To prove that $X \subseteq Y$, it is sufficient to show that $(\forall x)\ ((x \in X) \implies (x \in Y))$.

(a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(b) $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$.

(c) $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

(d) $f(A \cup B) = f(A) \cup f(B)$.

(e) $f(A \cap B) \subseteq f(A) \cap f(B)$, and give an example where equality does not hold.

(f) $f(A \setminus B) \supseteq f(A) \setminus f(B)$, 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, $A \subseteq B$ and that B is a subset of A, $B \subseteq A$. 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.

(a) 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, $f^{-1}(A) \cup f^{-1}(B) \subseteq f^{-1}(A \cup B)$.

(b) 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 $f^{-1}(A) \cap f^{-1}(B) \subseteq f^{-1}(A \cap B)$.

(c) 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 $f^{-1}(A) \setminus f^{-1}(B) \subseteq f^{-1}(A \setminus B)$.

(d) 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 $f(A) \cup f(B) \subseteq f(A \cup B)$.

(e) 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).

(f) 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 $f(A) \setminus f(B) = \varnothing$.

8 A Weighty Proof

You have 10 bags, each containing 100 coins. Nine of the 10 bags contain genuine gold coins, whereas one bag contains fake coins that are visually indistinguishable from the real gold coins. You don't know which bag has the fake coins, but you do know that real gold coins weigh 10g each while fake ones weigh 10.001g each. You can open the bags, look inside them, take out a few coins, mix them up, etc. You have a weighing machine that you can use *exactly once* – on which you can place a bunch of coins, press a button, and obtain a printed slip showing the weight of the coins placed, down to the milligram.

Prove that this setup is sufficient to determine which bag has the fake coins.

Solution: We can prove that this setup is sufficient by providing an algorithm that finds the fake coins.

Take 1 coin from the first bag, 2 coins from the second bag, and so on up to 10 coins from the tenth bag. Weigh these 55 coins using the given weighing scale. If the first bag had the fake coins, the weighing scale would read 550g + 1mg. If the second bag had the fake coins, the scale would read 550g + 2mg, and so on.

In general, suppose the k^{th} bag has the fake coins. Then the weighing scale would read $w = 550$g + $k$mg. Thus, no matter what value k takes, $w - 550 = k$.

Thus, based on the reading w (in grams) from the weighing scale, you can exactly pinpoint that bag $(w - 550)$ had the fake coins.