CS 70 Discrete Mathematics and Probability Theory
Spring 2021

HW 1

1 Prove or Disprove

For each of the following, either prove the statement, or disprove by finding a counterexample.

(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 $\neg\big(a \leq 11 \vee b \leq 4\big)$). Since $a > 11$ and $b > 4$, $a + b > 15$ (note that $a + b > 15$ is equivalent to $\neg\big(a + b \leq 15\big)$). 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.

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

3 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. Note that if $m > 5$, then $m+2 > 3$ and $m-2 > 3$ so we can apply part (a) and 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.

4 Social Network

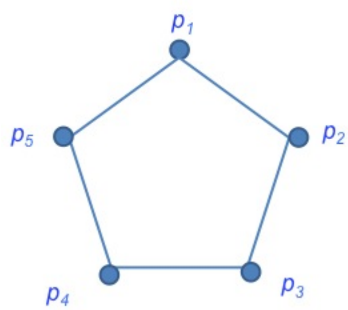
Consider the same setup as Q2 on the vitamin, where there are n people at a party, and every two people are either friends or strangers. Prove or provide a counterexample for the following statements.

(a) For all cases with $n = 5$ people, there exists a group of 3 people that are either all friends or all strangers.

(b) For all cases with $n = 6$ people, there exists a group of 3 people that are either all friends or all strangers.

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. We proceed with a proof by cases.

For any person p, we could divide the rest of people into 2 groups: the group of p's friends and the group of strangers. By pigeonhole principle, one of the groups must have at least 3 people.

Case 1a: p is friends with at least 3 people, and these friends are all strangers. Then p's friends form a group of at least 3 strangers.

Case 1b: p is friends with at least 3 people, and at least 2 of them are friends with each other. These two, along with p, form a group of 3 friends.

Case 2a: p is strangers with at least 3 people, and these strangers are all friends. Analogous to Case 1a, these strangers form a group of at least 3 friends.

Case 2b: p is strangers with at least 3 people, and at least 2 of them are not friends. Analogous to Case 1b, these 2 strangers form a group of at least strangers.

5 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.

6 Induction

Prove the following using induction:

(a) For all natural numbers $n > 2$, $2^n > 2n+1$.

(b) For all positive integers n, $1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

(c) For all positive natural numbers n, $\frac{5}{4} \cdot 8^n + 3^{3n-1}$ is divisible by 19.

Solution:

(a) The inequality is true for $n = 3$ because $8 > 7$. Let the inequality be true for $n = k$, such that $2^k > 2k+1$. Then,

$$2^{k+1} = 2 \cdot 2^k > 2 \cdot (2k+1) = 4k+2$$

We know $2k > 1$ because k is a positive integer. Thus:

$$4k+2 = 2k+2k+2 > 2k+1+2 = 2k+3 = 2(k+1)+1$$

We've shown that $2^{k+1} > 2(k+1)+1$, which completes the inductive step.

(b) We can verify that the statement is true for $n = 1$. Assume the statement holds for $n = k$, so that

$$\sum_{i=1}^{k} i^2 = \frac{k(k+1)(2k+1)}{6}.$$

Then we can write

$$\begin{aligned}
\sum_{i=1}^{k+1} i^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= (k+1)\left(\frac{k(2k+1)}{6} + (k+1)\right) \\
&= (k+1)\left(\frac{2k^2+k+6k+6}{6}\right) \\
&= (k+1)\left(\frac{2k^2+7k+6}{6}\right) \\
&= (k+1)\left(\frac{(2k+3)(k+2)}{6}\right) \\
&= \frac{(k+1)(2(k+1)+1)((k+1)+1)}{6},
\end{aligned}$$

as desired. Since we've shown that the statement holds for $n = k+1$, our proof is complete.

(c) For $n = 1$, the statement is "$10+9$ is divisible by 19", which is true. Assume that the statement holds for $n = k$, such that $\frac{5}{4} \cdot 8^k + 3^{3k-1}$ is divisible by 19. Then,

$$\begin{aligned}
\frac{5}{4} \cdot 8^{k+1} + 3^{3(k+1)-1} &= \frac{5}{4} \cdot 8 \cdot 8^k + 3^{3k+2} \\
&= 8 \cdot \frac{5}{4} \cdot 8^k + 3^3 \cdot 3^{3k-1} \\
&= 8 \cdot \frac{5}{4} \cdot 8^k + 8 \cdot 3^{3k-1} + 19 \cdot 3^{3k-1} \\
&= 8\left(\frac{5}{4} \cdot 8^k + 3^{3k-1}\right) + 19 \cdot 3^{3k-1}
\end{aligned}$$

The first term is divisible by the inductive hypothesis, and the second term is clearly divisible by 19. This completes our proof, as we've shown the statement holds for $k+1$.

7 Airport

Suppose that there are $2n+1$ airports where n is a positive integer. The distances between any two airports are all different. For each airport, exactly one airplane departs from it and is destined for the closest airport. Prove by induction that there is an airport which has no airplanes destined for it.

Solution:

For $n = 1$, let the 3 airports be A, B, C and let their distance be $|AB|, |AC|, |BC|$. Without loss of generality suppose B,C is the closest pair of airports (which is well defined since all distances are different). Then the airplanes departing from B and C are flying towards each other. Since the airplane from A must fly to somewhere else, no airplanes are destined for airport A.

Now suppose the statement is proven for $n = k$, i.e. when there are $2k+1$ airports. For $n = k+1$, i.e. when there are $2k+3$ airports, the airplanes departing from the closest two airports must be destined for each other's starting airports. Removing these two airports reduce the problem to $2k+1$ airports. From the inductive hypothesis, we know that among the $2k+1$ airports remaining, there is an airport with no incoming flights which we call airport Z. When we add back the two airports that we removed, the airplane flights may change; in particular, it is possible that an airplane will now choose to fly to one of these two airports (because the airports that were added may be closer than the airport to which the airplane was previously flying), but observe that none of the airplanes will is destined for the airport Z. Also, the two airports that were added back will have airplanes destined for each other, so they too will not be destined for airport Z. We conclude that the airport Z will continue to have no incoming flights when we add back the two airports, and so the statement holds for $n = k+1$. By induction, the claim holds for all $n \geq 3$.