

CSCI 150 Discrete Mathematics
Homework 1
Due 09/11/09

Saad Mneimneh
Visiting Professor
Hunter College of CUNY

Problem 1: Surprising implication

The OR operator \vee has the following truth table:

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

Show that for every two propositions P and Q , regardless of their truth value, the following is true:

$$(P \Rightarrow Q) \vee (Q \Rightarrow P)$$

This means that either P implies Q or Q implies P , a rather surprising result because P and Q can be completely unrelated.

Show this in two ways:

(a) using a truth table

Solution:

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

(b) replacing implication by an equivalent expression, e.g. $(p \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$.

Solution: $P \Rightarrow Q$ is equivalent to $\neg P \vee Q$:

$$(P \Rightarrow Q) \Leftrightarrow (\neg P \vee Q)$$

Therefore, our expression becomes:

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

Since P and its negation ($\neg P$) are combined by \vee (or), the result must be true regardless of the truth of P (the same can be said about Q). In other words, either P or $\neg P$ is true.

Problem 2: Finally a proof

Consider Fermat's theorem:

$$\forall \text{ integers } n > 2, a > 0, b > 0, c > 0, \quad a^n + b^n \neq c^n$$

(a) Identify the different parts of this proposition:

- the quantifier, and what it means
- the variables, and the possible values they can take
- the predicate

Solution:

- The quantifier is \forall , and it means that the predicate must be true for every possible combination of the variables, for the entire proposition to be true.
- the variables are n , a , b , and c . They are all positive integers (greater than 0). But n must be greater than 2.
- the predicate is $a^n + b^n \neq c^n$.

(b) This proposition was stated by Fermat in 1637, and was proved by Andrew Wiles in 1995. A student in CSCI 150, who has just learned about the logic of implications, suggested the following proof:

$$\text{pigs can fly} \Rightarrow \text{Fermat's theorem}$$

The student argues that since $P \Rightarrow Q$ is true whenever P is false, that implication must be true and, therefore, is a proof of Fermat's theorem. What is wrong about the student's proof?

Solution: The proposition

$$\text{pigs can fly} \Rightarrow \text{Fermat's theorem}$$

is true because it is of the form $P \Rightarrow Q$ and $P = (\text{pigs can fly})$ is false. However, this does not tell us anything about the truth of Q , which is Fermat's theorem in this case. Looking back at the truth table for implication, we see that both $F \Rightarrow F$ and $F \Rightarrow T$ are true. So Q can be either false or true, which does not prove anything about Fermat's theorem, except that it can be either false or true.

Problem 3: Proof by exhaustion

The absolute value of a real number x is defined as:

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Prove by exhaustions that for any two real numbers a and b , we have:

$$|a + b| \leq |a| + |b|$$

Note that there are infinite cases to consider for a and b (which would make proof by exhaustion impossible), but it is enough to consider only four cases:

- $a \geq 0, b \geq 0$
- $a \geq 0, b < 0$
- $a < 0, b \geq 0$
- $a < 0, b < 0$

Prove that the statement is true for each of the four case. Make sure you understand why these four cases are axhaustive.

Solution:

case 1: $a \geq 0, b \geq 0$

In this case, $|a| = a$, $|b| = b$, and $|a + b| = a + b$; therefore, $|a + b| = |a| + |b|$.

case 2: $a \geq 0, b < 0$

In this case, $|a| = a$, $|b| = -b$, and $|a+b|$ could be either $a+b$ or $-(a+b) = -a-b$:

- $|a + b| = a + b < a - b = |a| + |b|$, ($b < 0$)
- $|a + b| = -(a + b) = -a - b \leq a - b = |a| + |b|$, ($a \geq 0$)

case 3: $a < 0, b \geq 0$

This case is symmetric to the second case (switch the roles of a and b)

case 4: $a < 0, b < 0$

In this case, $|a| = -a$, $|b| = -b$, and $|a+b| = -a-b$; therefore, $|a+b| = |a|+|b|$.

Problem 4: Proof by contradiction

Prove by contradiction that there is no rational solution for $x^3 + x + 1 = 0$. This means assume that a rational solution r exists and, therefore,

$$r^3 + r + 1 = 0$$

$$r = a/b$$

where a/b is in reduced form, and both a and b are integers ($b \neq 0$). Arrive at a contradiction (argue about a and b being odd or even the same way we did in class for proving that $\sqrt{2}$ is irrational).

Solution: Let $r = a/b$ (reduced) be a solution to the above equation, then

$$(a/b)^3 + a/b + 1 = 0$$

Multiplying by b^3 , we get:

$$a^3 + ab^2 + b^3 = 0$$

case 1: a even, b odd

a^3 is even, ab^2 is even, and b^3 is odd: the expression is odd, a contradiction because 0 is even.

case 2: a odd, b even

a^3 is odd, ab^2 is even, and b^3 is even: the expression is odd, a contradiction because 0 is even.

case 3: a odd, b odd

a^3 is odd, ab^2 is odd, and b^3 is odd: the expression is odd, a contradiction because 0 is even.

case 4: a even, b even

A contradiction, since a/b is reduced.

Problem 5: Prime generating polynomial

Consider the following proposition:

$$\forall x \in \mathbb{N}, x^2 + x + 41 \text{ is prime}$$

We argued in class that this proposition is false because the predicate

$$x^2 + x + 41 \text{ is prime}$$

is false for $x = 40$ (try it).

The polynomial $x^2 + x + 41$ is the best known polynomial for generating prime numbers because it gives distinct primes for the 40 consecutive non-negative integers 0 to 39. This polynomial was discovered by Euler in 1772. In general, a polynomial of $p(x)$ of degree d can be written as

$$p(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$

where $a_d \neq 0$. It is not hard to show that no polynomial of degree $d \geq 1$ generates only prime numbers. In this problem you are asked to prove this **by contradiction**. Use the following true propositions:

- any polynomial $p(x)$ of degree $d \geq 1$ can be written as $p(x) = xq(x) + c$ where $q(x)$ is a polynomial of degree $d - 1$.
- if $p(x)$ generates only primes, then c must be prime.

- if x is a multiple of c , then $p(x)$ is also a multiple of c , e.g. if $x = kc$, then $p(kc) = kc \cdot q(kc) + c = c[k \cdot q(kc) + 1]$.
- a multiple of c is prime only if it is equal to c .
- if $q(x)$ has degree $d - 1$, then there can be at most $d - 1$ values for x for which $q(x) = 0$.

Solution: Let $p(x)$ be a polynomial of degree $d \geq 1$ that generates only primes $\Rightarrow p(x)$ can be expressed as $xq(x) + c$ where $q(x)$ has degree $d - 1$ and c is prime \Rightarrow given a multiple of c , say kc , $p(kc) = kcq(kc) + c$ is a multiple of c that is prime for infinitely many values of $k \in \{0, 1, 2, 3, \dots\} \Rightarrow p(kc) = c$ for infinitely many values of $k \in \{0, 1, 2, 3, \dots\} \Rightarrow kcq(kc) = 0$ for infinitely many values of $k \in \{0, 1, 2, 3, \dots\} \Rightarrow q(kc) = 0$ for infinitely many values of $k \in \{0, 1, 2, 3, \dots\}$. The last statement is obviously false. Therefore, the first statement must be false, which proves what we want to prove.