Math 1

What is a Proof?

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

Propositions

- A proposition is a statement that is either true or false.
- For example, both of the following statements are propositions.
  - $2 + 3 = 5$ → true
  - $1 + 1 = 3$ → false

- How to check if a claimed proposition is true or false.

Propositions

- Claim: For every nonnegative integer n the value of $n^2 + n + 41$ is prime.
  - A prime number is a number that is divisible only by 1 and itself.
- Let's try some numerical representations: $\mathrm{P(n)} ::= n^2 + n + 41$
  - $P(0) = 41$ → prime
  - $P(1) = 43$ → prime
  - $P(2) = 47$ → prime
  - $P(3) = 53$ → prime, …, $p(39) = 1601$ → prime
  - $P(40) = 1681$ → NOT prime.
  - The claim fails.

Propositions

- The point is: you can't check a claim about an infinite set by checking a finite sample of its elements, no matter how large the sample.

- When we define propositions about all numbers or all items of some kind, we use this notation:

$$\forall n \in \mathbb{N}. p(n)\ is\ prime$$

  - $\mathbb{N}$ is the set of non-negative integers: 0, 1, 2, 3, …

Propositions

- Conjecture. [Euler] The equation $a^4 + b^4 + c^4 = d^4$ has no solutions when $\mathrm{a}, \mathrm{b}, \mathrm{c}, d$ are positive integers.
- The conjecture was proved false 218 years later when $a = 95800;\ b = 217519;\ c = 414560;\ d = 422481$

- In logical notation, Euler's Conjecture could be written:

$$\forall a \in \mathbb{Z}^+ \ \forall b \in \mathbb{Z}^+ \ \forall c \in \mathbb{Z}^+ \ \forall d \in \mathbb{Z}^+ \ . a^4 + b^4 + c^4 \neq d^4$$

Or

$$\forall a, b, c, d \in \mathbb{Z}^+ . \ a^4 + b^4 + c^4 \neq d^4$$

Propositions

- Proposition (Fermat's Last Theorem). There are no positive integers x, y and z such that

$$x^n + y^n = z^n$$

For some integer $n > 2$

  - After more than 300 years, this theorem was proved to hold for n up to 4,000,000

- Conjecture (Goldbach). Every even integer greater than 2 is the sum of two primes.
  - Goldbach's Conjecture dates to 1742. It is known to hold for all numbers up to 10^{18}, but to this day, no one knows whether it's true or false.

Propositions

- For a computer scientist, some of the most important things to prove are the correctness of programs and systems.
  - whether a program or system does what it's supposed to.

- Programs are buggy, and there's a growing community of researchers and practitioners trying to find ways to prove program correctness.

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

Predicates

- A predicate is a proposition whose truth depends on the value of one or more variables.
- For example, the predicate "n is a perfect square" can be written as

$$P(n) ::= "n\ is\ a\ perfect\ square"$$

- You cannot say that this predicate is true or false until you know the value of n.
  - If $n = 4$, then the predicate is true.
  - If $n = 5$, then the predicate is false.

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

The Axiomatic Method

- An **axiom** is a statement that is taken to be true, to serve as a premise or starting point for further reasoning and arguments.
  - Example: There is a straight-line segment between every pair of points.
- Starting from axioms, we establish proofs.
- A **proof** is a sequence of logical deductions from axioms and previously proved statements that concludes with the proposition in question.

The Axiomatic Method

- There are different terms refer to propositions that have been proved:
  - **Theorems** – important true propositions.
  - **Lemma** – a preliminary propositions useful for proving later propositions.
  - **Corollary** – a proposition that follows in just a few logical steps from a theorem.

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

Logical Deductions

- **Logical deductions**, or **inference rules**, are used to prove new propositions using previously proved ones.
- A fundamental inference rule is **modus ponens -** a proof of P together with a proof that P IMPLIES Q is a proof of Q.

$$\frac{P,\ P\ implies\ Q}{Q}$$

  - The statement above the line is called antecedents.
  - The statement below the line is called conclusion.
  - If the antecedents is proved, then the conclusion is proved.

Logical Deductions

- Example of modus ponens:

If today is Tuesday, then Ali will go to work.

Today is Tuesday. Therefore, Ali will go to work.

Logical Deductions

- Other inference rules:

$$\frac{(P\ implies\ Q), (Q\ implies\ R)}{P\ implies\ R}$$

$$\frac{NOT(P)\ implies\ NOT(Q)}{Q\ implies\ P}$$

The following is wrong

$$\frac{NOT(P)\ implies\ NOT(Q)}{P\ implies\ Q}$$

- You can interpret it as: the non-occurrence of P implies the non-occurrence of Q. In turn, if Q occurs, then P must have occurred.

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

Proving an Implication

- Propositions of the form “If P, then Q” are called implications.
  - Often rephrased as “P IMPLIES Q.”
- Examples:
  - Quadratic formula: if $ax^2 + bx + c = 0$ and $a \neq 0$, then $x = \frac{\left(-b \pm \sqrt{b^2 - 4ac}\right)}{2a}$
- Two ways to prove implications:
  - Direct proof.
  - Proof the contrapositive.

Proving an Implication

- Direct proof - to prove that P implies Q:
  - Assume that P is true.
  - Show that Q logically follows.

- **Example**: if $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$
- **Solution**:
  - Let's factor $-x^3 + 4x$ to $x(2 - x)(2 + x)$.
  - So, for $0 \leq x \leq 2$, all the terms of $x(2 - x)(2 + x)$ are non-negative.
  - Then, by adding 1, we get $x(2 - x)(2 + x) + 1 > 0$

Proving an Implication

- Prove the contrapositive: An implication ("$P\ IMPLIES\ Q$") is logically equivalent to its contrapositive $NOT(Q)\ IMPLIES\ NOT(P)$
  - Sometimes it is easier than direct proofs.
- Example: if r is irrational, then $\sqrt{r}$ is irrational.
  - A number is rational when it equals a quotient of integers —that is, if it equals $\frac{m}{n}$ for some integers m and n.
  - So, we must show that r is not a ratio of integers, then $\sqrt{r}$ is not a ratio of integers

Proving an Implication

- **Solution:**
  - Assume that $\sqrt{r}$ is rational
  - Then r is rational.
  - $\therefore \sqrt{r} = \frac{m}{n}$
  - Square both sides → $r = \frac{m^2}{n^2}$
  - $\because m^2$ and n^2 are integers, then r is rational.

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

Proving an “If and Only If”

- If and only if statement is a biconditional statement, means that either the two sides of the statements are true, or both are false.
  - Abbreviated as iff
- Example: I wear a hat iff it is sunny.
- To prove iff statements:
  - Prove each statement implies the other.
    - The statement “P iff Q” = ”P implies Q” and “Q implies P”
  - Construct a chain of iff statements
    - Prove P is equivalent to a second statement, which is equivalent to the third statement, an so forth until you reach Q.

Proving an “If and Only If”

- **Example:** The standard deviation of a sequence of values $x_1, x_2, \ldots, x_n$ is defined to be:

$$\sqrt{\frac{(x_1 - \mu)^2 + (x_2 - \mu)^2 + \cdots + (x_n - \mu)^2}{n}}$$

Where μ is the mean

The standard deviation of a sequence of values $x_1, x_2, \ldots, x_n$ is zero iff all the values are equal to the mean.

Proving an "If and Only If"

- **Solution**:
  - construct a chain of iff implications, assuming that the standard deviation is 0

$$\sqrt{\frac{(x_1-\mu)^2+(x_2-\mu)^2+\cdots+(x_n-\mu)^2}{n}}=0$$

  - ∵ 0 is the only number whose square root is 0, then

$$(x_1-\mu)^2+(x_2-\mu)^2+\cdots+(x_n-\mu)^2=\ 0$$

  - ∵ Squares of real numbers are always nonnegative, so every term on the left-hand side of equation is nonnegative.
  - ∴ $(x-\mu)^2=0$
  - ∴ $x=\mu$
  - ∴ every value x is equal to the mean

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

Proof by Contradiction

- Proof by contradiction: assume the proposition is false and show that this leads to a contradiction.
  - Called indirect proof.
- Example: prove by contradiction $\sqrt{2}$ is irrational number

Proof by Contradiction

1. Let $p =$ "$\sqrt{2}\ is\ irrational$". To prove by contradiction, we suppose $\neg p$ is true.
2. $\neg p$ means that $\sqrt{2}$ is rational
3. $\because \sqrt{2}$ is rational
4. $\therefore \sqrt{2} = \frac{a}{b}$, which is the same as $2 = a^2/b^2$
5. $\therefore a^2 = 2b^2$, this means that a^2 is even number because it has the form a $= 2k$
6. $\therefore (2k)^2 = 2b^2 \rightarrow 4k^2 = 2b^2 \rightarrow 2k^2 = b^2$
7. $\because b^2 = 2k^2$, then b is even.
8. $\because b$ and a are both even numbers
9. $\therefore a$ and b have a common factor of 2
10. $\therefore$ if we have $\frac{a}{2} \div \frac{b}{2} = \frac{c}{d}$, where c and d have no common factors
11. $\therefore \sqrt{2} = \frac{c}{d}$, which is false. (suppose $c = 1$ and $d = 2$)

Content
Propositions
Predicates
The Axiomatic Method
Logical Deductions
Proving an Implication
Proving an If and only If
Proof by Contradiction
Exercises

Proof by Contradiction

Problem 1.2.
What's going on here?!

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \left(\sqrt{-1}\right)^2 = -1.$$

(a) Precisely identify and explain the mistake(s) in this *bogus* proof.

(b) Prove (correctly) that if $1 = -1$, then $2 = 1$.

(c) Every *positive* real number r has two square roots, one positive and the other negative. The standard convention is that the expression $\sqrt{r}$ refers to the *positive* square root of r. Assuming familiar properties of multiplication of real numbers, prove that for positive real numbers r and s,

$$\sqrt{rs} = \sqrt{r}\sqrt{s}. \tag{1.7}$$

Proof by Contradiction

a) The issue is with $\sqrt{(-1)(-1)} = \sqrt{-1}\,\sqrt{-1}$,

We know that $\sqrt{ab} = \sqrt{a}\,\sqrt{b}$ is a valid property FOR POSITIVE REAL NUMBERS.

But, in this case we are bogusly moving from the space of positive real numbers to the space of imaginary numbers.

b) Assume 1 = -1

- Divide by 2, $\frac{1}{2} = -\frac{1}{2}$
- Add $3/2$, $\frac{1}{2} + \frac{3}{2} = -\frac{1}{2} + \frac{3}{2} \rightarrow \frac{4}{2} = \frac{2}{2} = 2 = 1$

Proof by Contradiction

c) Start with $rs = rs$

- $(\sqrt{rs})^2 = (\sqrt{r}\,)^2(\sqrt{s}\,)^2$
- $= (\sqrt{r}\,\sqrt{r})\,(\sqrt{s}\,\sqrt{s})$
- $= \sqrt{r}\,(\sqrt{r}\sqrt{s}\,)\sqrt{s}$
- $= (\sqrt{r}\,\sqrt{s}\,)(\sqrt{r}\sqrt{s})$
- $= (\sqrt{r}\,\sqrt{s}\,)^2$
- $\sqrt{rs} = (\sqrt{r}\,\sqrt{s}\,)$

Proof by Contradiction

Problem 1.13.
Prove that if $a \cdot b = n$, then either a or b must be $\leq \sqrt{n}$, where a, b, and n are nonnegative real numbers. *Hint:* by contradiction, Section 1.8.

Proof by Contradiction

- Assume that both $a > \sqrt{n}$ and b $> \sqrt{n}$ and $a \cdot b = n$ (as stated in the question)
- Then, a $\cdot\, b > \sqrt{n}\sqrt{n}$
- But $\sqrt{n}\sqrt{n} = n$
- Thus, we conclude that $a \cdot b > n$, which is a contradiction.
- Hence, the claim is true.