CS 207 Discrete Mathematics – 2012-2013

Nutan Limaye

Indian Institute of Technology, Bombay
nutan@cse.iitb.ac.in

Mathematical Reasoning and Mathematical Objects

Lecture 1: What is a proof?

July 30, 2012

Credit Structure

Course credit structure

quizzes	20%
assignments	10%
mid-sem	30%
end-sem	40%

Office hours:	11:00am to 1:00pm (Wednesday)
TA meeting hours:	5:15pm to 6:15pm (Thursday) — ?

Course Outline

- Mathematical reasoning and mathematical objects
- Combinatorics
- Elements of graph theory
- Elements of abstract algebra

Course Outline

- Mathematical reasoning and mathematical objects
  - What is a proof? Types of proof methods
  - Induction
  - Sets, relations, functions, partial orders, graphs
- Combinatorics
- Elements of graph theory
- Elements of abstract algebra

Course Outline

- Mathematical reasoning and mathematical objects
  - What is a proof? Types of proof methods
  - Induction
  - Sets, relations, functions, partial orders, graphs

Text:	*Discrete Mathematics and its applictions, by Kenneth Rosen*
	Chapter 2 : $2.1, 2.2, 2.3$, Chapter 8 : $8.1, 8.5, 8.6$
Class notes:	will be uploaded on Moodle

- Combinatorics
- Elements of graph theory
- Elements of abstract algebra

What is a proposition?

A statement that is either true or false.

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
  $\forall$: for all,
  $\exists$: there exists,
  $\in, \notin$: contained in, and not contained in

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
  $\forall$: for all,
  $\exists$: there exists,
  $\in, \notin$: contained in, and not contained in
  $\mathbb{N}$: the set of natural numbers,
  $\mathbb{Z}$: the set of integers,
  $\mathbb{Q}$: the set of rationals,
  $\mathbb{Z}^+$: the set of positive integers,
  $\mathbb{R}$: the set of reals

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 - b^2 = c$;

What is a proposition?

A statement that is either true or false.

- $2 + 2 = 4$, every odd number is a prime, there are no even primes other than 2;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 + b^2 = c$;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{N} : a^2 - b^2 = c$;
- $\forall a, b \in \mathbb{N}, \exists c \in \mathbb{Z} : a^2 - b^2 = c$;

It is not always easy to tell whether a proposition is true or false.

Theorems and proofs

Theorem

If $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$

Theorems and proofs

Theorem

If $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$

(scratchpad)

Theorems and proofs

Theorem

If $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$

(scratchpad)

Proof.

As $-x^3 + 4x = x(4 - x^2)$, which is in fact $x(2-x)(2+x)$, the quantity is ~~positive~~ non-negative for $0 \leq x \leq 2$. Adding 1 to a non-negative quantity makes it positive. Therefore, the above theorem. $\square$

Theorems and Proofs

Given:	a number $n \in \mathbb{N}$
Check:	Is n prime?

Theorems and Proofs

Given: a number $n \in \mathbb{N}$
Check: Is n prime?

for $i = 2$ to $\sqrt{n}$ **do**
  if $i|n$ **then**
    output "no"
  end if
end for

Theorems and Proofs

Given: a number $n \in \mathbb{N}$
Check: Is n prime?

for $i = 2$ to $\sqrt{n}$ **do**
  if $i|n$ **then**
    output "no"
  end if
end for

Why is this algorithm correct?
Is there a number $n \in \mathbb{N}$ s.t
$\forall i : i \in \{2, 3, \ldots, \sqrt{n}\}\ i \nmid n$,
but $\exists j > \sqrt{n}$ s.t. $j|n$?

Is there a composite $n \in \mathbb{N}$ s.t. all its prime factors are greater than $\sqrt{n}$?

Theorems and Proofs

Is there a number $n \in \mathbb{N}$ s.t
$\forall i : i \in \{2, 3, \ldots, \sqrt{n}\}\ i \nmid n$,
but $\exists j > \sqrt{n}$ s.t. $j | n$?

Is there a composite $n \in \mathbb{N}$ s.t. all its prime factors are greater than $\sqrt{n}$?

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Proof.

As n is a composite, $\exists x, y \in \mathbb{N}, x, y < n : n = xy$. If $x > \sqrt{n}$ and $y > \sqrt{n}$ then $xy > n$. Therefore, one of x or y is less than or equal to $\sqrt{n}$. Say x is smaller than $\sqrt{n}$. It is either a composite or a prime. If it is a prime, then we are done. Else, it has prime factorization (axiom: unique factorization in $\mathbb{N}$) and again, we are done. □

Theorems and Proofs

Is there a number $n \in \mathbb{N}$ s.t
$\forall i : i \in \{2, 3, \ldots, \sqrt{n}\}\ i \nmid n$,
but $\exists j > \sqrt{n}$ s.t. $j | n$?

Is there a composite $n \in \mathbb{N}$ s.t. all its prime factors are greater than $\sqrt{n}$?

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Proof.

As n is a composite, $\exists x, y \in \mathbb{N}, x, y < n : n = xy$. If $x > \sqrt{n}$ and $y > \sqrt{n}$ then $xy > n$. Therefore, one of x or y is less than or equal to $\sqrt{n}$. Say x is smaller than $\sqrt{n}$. It is either a composite or a prime. If it is a prime, then we are done. Else, it has prime factorization (axiom: unique factorization in $\mathbb{N}$) and again, we are done. $\square$

Axioms

Euclid in 300BC invented the method of axioms-and-proofs.

Using only a handful of axioms called Zermelo-Fraenkel and Choice (ZFC) and a few rules of deductions the entire mathematics can be deduced!

Proving theorems starting from ZFC alone is tedious. 20,000+ lines proof for $2 + 2 = 4$

We will assume a whole lot of axioms to prove theorems: all familiar facts from high school math.

Class problems

- (CW1.1) Prove that for any $n \in \mathbb{N}$, $n(n^2 - 1)(n + 2)$ is divisible by 4. (what about divisible by 8?)
- (CW1.2) Prove that for any $n \in \mathbb{N}$, $2^n < (n + 2)!$

Bogus proofs

Theorem (Bogus)

$1/8 > 1/4$

Proof.

$$3 > 2$$
$$3\log_{10}(1/2) > 2\log_{10}(1/2)$$
$$\log_{10}(1/2)^3 > \log_{10}(1/2)^2$$
$$(1/2)^3 > (1/2)^2$$

□

Another bogus proof

Theorem

For all non-negative numbers a, b $\frac{a+b}{2} \geq \sqrt{ab}$

Proof.

$$\begin{aligned} \frac{a+b}{2} &\geq^? \sqrt{ab} \\ a+b &\geq^? 2\sqrt{ab} \\ a^2+2ab+b^2 &\geq^? 4ab \\ a^2-2ab+b^2 &\geq^? 0 \\ (a-b)^2 &\geq 0 \end{aligned}$$

□

Proof Methods

Proof by contrapositive

Theorem

If r is irrational then $\sqrt{r}$ is also irrational.

Proof by contrapositive

Theorem

If r is irrational then $\sqrt{r}$ is also irrational.

Definition (Contrapozitive)

The contrapositive of "if P then Q" is "if $\neg Q$ then $\neg P$"

Proof by contrapositive

Theorem

If r is irrational then $\sqrt{r}$ is also irrational.
If $\sqrt{r}$ is rational then r is rational.

Proof.

Suppose $\sqrt{r}$ is rational. Then $\sqrt{r} = p/q$ for $p, q \in \mathbb{Z}$. Therefore, $r = p^2/q^2$. $\square$

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even.

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. (CW2.1) If p^2 is even, then p is even.

Proof by contradiction

Theorem

$\sqrt{2}$ is irrational.

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even.
If p^2 is even, then p is even. (why?)
Suppose not, i..e p^2 is even but p is not. Then $p = 2k + 1$ for some integer k. $p^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. As $4(k^2 + k)$ is even, $4k^2 + 4k + 1$ is odd, which is a contradiction.

Proof by contradiction

Theorem

$\sqrt{2}$ is irrational.

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. If p^2 is even, then p is even.

Proof by contradiction

Theorem

$\sqrt{2}$ *is irrational.*

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. If p^2 is even, then p is even. Therefore, $p = 2k$ for some $k \in \mathbb{Z} \Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2k^2 \Rightarrow q^2$ is even. Therefore, q is even. That is, p, q have a common factor. This leads to a contradiction. $\square$

Proof by contradiction

Theorem

$\sqrt{2}$ is irrational.

Proof.

Suppose not. Then there exists $p, q \in \mathbb{Z}$ such that $\sqrt{2} = p/q$, where p, q do not have any common divisors. Therefore, $2q^2 = p^2$, i.e. p^2 is even. If p^2 is even, then p is even. Therefore, $p = 2k$ for some $k \in \mathbb{Z} \Rightarrow 2q^2 = 4k^2 \Rightarrow q^2 = 2k^2 \Rightarrow q^2$ is even. Therefore, q is even. That is, p, q have a common factor. This leads to a contradiction. $\square$

(CW2.2) Prove that there are infinitely many primes.

Well-ordering principle and Induction

Axiom (WOP)

Every nonempty set of non-negative integers has a smallest element.

Well-ordering principle and Induction

Axiom (WOP)

Every nonempty set of non-negative integers has a smallest element.

Axiom (Induction)

Let $P(n)$ be a property of non-negative integers. If

1. *$P(0)$ is true (Base case)*
2. *for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$ (Induction step)*

then $P(n)$ is true for for all $n \in \mathbb{N}$.

Well-ordering principle and Induction

Axiom (WOP)

Every nonempty set of non-negative integers has a smallest element.

Axiom (Induction)

Let $P(n)$ be a property of non-negative integers. If

1. *$P(0)$ is true (Base case)*
2. *for all $n \geq 0$, $P(n) \Rightarrow P(n+1)$ (Induction step)*

then $P(n)$ is true for for all $n \in \mathbb{N}$.

Axiom (Strong Induction)

Let $P(n)$ be a property of non-negative integers. If

1. *$P(0)$ is true (Base case)*
2. *$[\forall k \in \{0, 1, \ldots, n\} : P(k)] \Rightarrow P(n+1)$ (Induction step)*

then $P(n)$ is true for for all $n \in \mathbb{N}$.

WOP $\Rightarrow$ Induction

Theorem

Well-ordering principle implies Induction

Proof.

Let $P(0)$ be true and for each $n \geq 0$, let $P(n) \Rightarrow P(n+1)$.
Let us assume for the sake of contradiction that $P(n)$ is not true for all positive integers.
Let $C = \{i \mid P(i) \text{ is false}\}$. As C is non-empty and non-negative integers C has a smallest element (due to WOP), say i_0.
Now, $i_0 \neq 0$. Also $P(i_0 - 1)$ is true, as $i_0 - 1$ is not in C. But $P(i_0 - 1) \Rightarrow P(i_0)$, which is a contradiction. $\square$

WOP $\Rightarrow$ Induction

Theorem

Well-ordering principle implies Induction

Proof.

Let $P(0)$ be true and for each $n \geq 0$, let $P(n) \Rightarrow P(n+1)$.
Let us assume for the sake of contradiction that $P(n)$ is not true for all positive integers.
Let $C = \{i \mid P(i) \text{ is false}\}$. As C is non-empty and non-negative integers C has a smallest element (due to WOP), say i_0.
Now, $i_0 \neq 0$. Also $P(i_0 - 1)$ is true, as $i_0 - 1$ is not in C. But $P(i_0 - 1) \Rightarrow P(i_0)$, which is a contradiction. $\square$

Theorem

WOP $\Leftrightarrow$ Induction $\Leftrightarrow$ Strong Induction [HW]

Using Induction to prove theorems

Theorem

$2^n \leq (n+1)!$

Proof.

Base case ($n = 0$): $2^0 = 1 = 1!$

Using Induction to prove theorems

Theorem

$2^n \leq (n+1)!$

Proof.

Base case ($n = 0$): $2^0 = 1 = 1!$
Induction hypothesis: $2^n \leq (n+1)!$.

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &\leq 2 \cdot (n+1)! \text{ (by indiction hypothesis)} \\ &\leq (n+2) \cdot (n+1)! \\ &\leq (n+2)! \end{aligned}$$

□

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
(Such an s exists due to WOP.)

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.
And, now we can repeat the argument with respect to A.
Therefore, if (A, B, C) is a solution then so is (α, β, γ).

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$:
$4a^3 + 2b^3 = c^3$

Proof.

Suppose (for the sake of contradiction) this has a solution over $\mathbb{N}$.
Let (A, B, C) be the solution with the smallest value of b in S.
Observe that C^3 is even. Therefore, C is even. Say $C = 2\gamma$.
Therefore, $4A^3 + 2B^3 = 8\gamma^3$, i.e. $2A^3 + B^3 = 4\gamma^3$.
Now, B^3 is even and so is B. Say $B = 2\beta$. $\therefore 2A^3 + 8\beta^3 = 4\gamma^3$.
And, now we can repeat the argument with respect to A.
Therefore, if (A, B, C) is a solution then so is (α, β, γ).
But $\beta < B$, which is a contradiction.

Using Well-ordering principle to prove theorems

Here is a slightly non-trivial example:

Theorem

The following equation does not have any solutions over $\mathbb{N}$ *:*
$4a^3 + 2b^3 = c^3$

It is not always as easy to prove such theorems.

Conjecture (Euler, 1769)

There are no positive integer solutions over $\mathbb{Z}$ *to the equation:*

$$a^4 + b^4 + c^4 = d^4$$

Integer values for a, b, c, d that do satisfy this equation were first discovered in 1986.
It took more two hundred years to prove it.