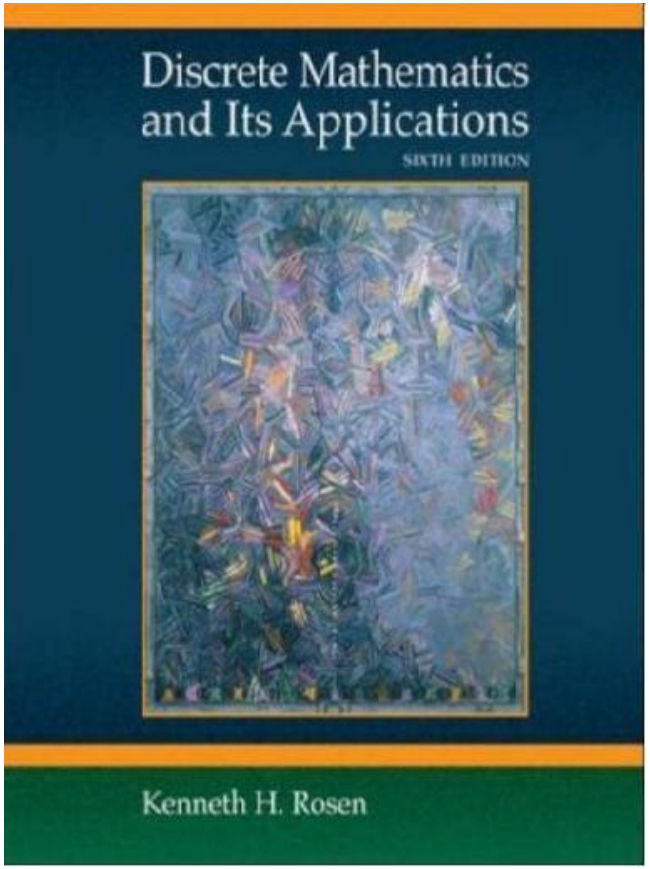
Jiangxi University of Science and Technology

Discrete Mathematics and Its Applications

Logic Module – Part II (proof methods)



Acknowledgement

- Most of these slides are adapted from ones created by Professor Bart Selman at Cornell University and Dr Johnnie Baker

Methods for Proving Theorems

Theorems, proofs, and Rules of Inference

When is a mathematical argument correct?
What techniques can we use to construct a mathematical argument?

Theorem – statement that can be shown to be true.

Axioms or postulates – statements which are given and assumed to be true.

Proof – sequence of statements, a valid argument, to show that a theorem is true.

Rules of Inference – rules used in a proof to draw conclusions from assertions known to be true.

Note:
Lemma is a "pre-theorem" or a result that needs to be proved to prove the theorem;
A **corollary** is a "post-theorem", a result which follows easily from the theorem that has been proved.
Conjecture is a statement believed to be true but for which there is not a proof yet. If the conjecture is proved true it becomes a thereom.
Fermat's theorem was a conjecture for a long time.

Valid Arguments (reminder)

- An argument is a sequence of propositions. The final proposition is called the conclusion of the argument while the other propositions are called the premises or hypotheses of the argument.
- An argument is valid whenever the truth of all its premises implies the truth of its conclusion.
- How to show that **q** logically follows from the hypotheses $(p_1 \wedge p_2 \wedge \ldots \wedge p_n)$?

Show that $(p_1 \wedge p_2 \wedge \ldots \wedge p_n) \rightarrow q$ is a tautology

One can use the rules of inference to show the validity of an argument.

Vacuous proof - if one of the premises is false then $(p1 \wedge p2 \wedge \ldots \wedge pn) \rightarrow q$ is vacuously True, since False implies anything.

Arguments involving universally quantified variables

- Note: Many theorems involve statements for universally quantified variables:

e.g., the following statements are equivalent:

- "If x>y, where x and y are positive real numbers, then $x^2 > y^2$ "

  "$\forall x \forall y$ (if $x > y > 0$ then $x^2 > y^2$) "

  Quite often, when it is clear from the context, theorems are proved without explicitly using the laws of universal instantiation and universal generalization.

Methods of Proof

- Direct Proof
- Proof by Contraposition
- Proof by Contradiction
- Proof of Equivalences
- Proof by Cases
- Exhaustive Proof
- Existence Proofs
- Uniqueness Proofs
- Counterexamples

Direct Proof

- Proof of a statement $p \rightarrow q$

  Assume p

  From p derive q.

Example - direct proof

- Here's what you know:

  Premises:
  Mary is a Math major or a CS major.
  If Mary does not like discrete math, she is not a CS major.
  If Mary likes discrete math, she is smart.
  Mary is not a math major.

- Can you conclude Mary is smart?

Informally, what's the chain of reasoning?

Let
M - Mary is a Math major
C – Mary is a CS major
D – Mary likes discrete math
S – Mary is smart

$$((M \vee C) \wedge (\neg D \rightarrow \neg C) \wedge (D \rightarrow S) \wedge (\neg M)) \rightarrow S$$
?

Example - direct proof

- In general, to prove $p \rightarrow q$, assume p is true and show that q must also be true

$$((M \vee C) \wedge (\neg D \rightarrow \neg C) \wedge (D \rightarrow S) \wedge (\neg M)) \rightarrow S$$
?

- Since, p is a conjunction of all the premises, we instead make the equivalent assumption that all of the following premises are true
  - $M \vee C$
  - $\neg D \rightarrow \neg C$
  - $D \rightarrow S$
  - $\neg M$
- Then the truth of these premises are used to prove S is true

Example - direct proof

1. $M \vee C$	Given
2. $\neg D \rightarrow \neg C$	Given
3. $D \rightarrow S$	Given
4. $\neg M$	Given
5. C	Disjunctive Syllogism (1,4)
6. D	Modus Tollens (2,5)
7. S	Modus Ponens (3,6)

Mary is smart!

QED

QED or Q.E.D. --- quod erat demonstrandum

"which was to be demonstrated"or "I rest my case" ☺

Example 2: Direct Proof

Theorem:

If n is odd integer, then n^2 is odd.

$\forall n$ (n is odd) $\rightarrow$ (n^2 is odd)

Two definitions:

The integer is *even* if there exists an integer k such that n = 2k.

An is *odd* if there exists an integer k such that n = 2k+1.

Note: An integer is either even or odd, but not both.

This is an immediate consequence of the division algorithm: If a and b are positive integers, then there exist unique integers q and r with a = qb + r and $0 \leq r < b$

Other proofs can also be given, depending on what previous facts have already been established.

This fact is not needed in the first proof, is needed in a later proofs.

Example 2: Direct Proof

Theorem:

$\forall(n)\ P(n) \rightarrow Q(n)$,

where P(n) is "n is an odd integer" and Q(n) is "n^2 is odd."

We will show $P(n) \rightarrow Q(n)$

Example 2: Direct Proof

Theorem: If n is odd integer, then n^2 is odd.

Proof:

Let p denote "n is odd integer" and q denote "n^2 is odd"; we want to show that $p \rightarrow q$

Assume p, i.e., n is odd.

By definition $n = 2k + 1$, where k is some integer.

Therefore $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is by definition an odd number ($k' = (2k^2 + 2k)$). QED

Proof strategy hint:

Go back to definitions of concepts and start by trying a direct proof.

Proof by Contraposition

Proof of a statement $p \rightarrow q$ by contraposition

Recall the tautology of the equivalence of a implication and its contrapositive.

$$p \rightarrow q \equiv \neg q \rightarrow \neg p \text{ (the contrapositive)}$$

So, we can prove $p \rightarrow q$ by establishing the equivalent statement that

$$\neg q \rightarrow \neg p$$

So, we prove the implication $p \rightarrow q$ by first assuming $\neg q$, and showing that $\neg p$ follows

Example 1: Proof by Contraposition

- Example:

Prove that if a and b are integers, and $a + b \geq 15$, then $a \geq 8$ or $b \geq 8$.

$$(a + b \geq 15) \rightarrow (a \geq 8) \vee (b \geq 8)$$

(Assume $\neg q$)
(Show $\neg p$)

Suppose $(a < 8) \wedge (b < 8)$.
Then $(a \leq 7) \wedge (b \leq 7)$,
and $(a + b) \leq 14$,
and $(a + b) < 15$.

QED

Proof strategy: Note that negation of conclusion is easier to start with here.

Example 2: Proof by Contraposition

Theorem:

For an integer n, if 3n + 2 is odd, then n is odd.

I.e. For n integer,

3n+2 is odd $\rightarrow$ n is odd

Again, negation of conclusion is easy to start with. Try direct proof. ☹

Proof by Contraposition:

Let p denote "3n + 2" is odd and q denote "n is odd"; we must show that p $\rightarrow$ q

The contraposition of our theorem is $\neg q \rightarrow \neg p$

n is even $\rightarrow$ 3n + 2 is even

Now we can use a direct proof

Assume $\neg q$, i.e, n is even therefore n = 2 k for some k

Therefore 3 n + 2 = 3 (2k) + 2 = 6 k + 2 = 2 (3k + 1) which is even.

QED

Proof by Contradiction

A – We want to prove p.

We show that:

$\neg p \rightarrow \mathbf{F}$ (i.e., a **False** statement , say $r \wedge \neg r$)

We conclude that $\neg p$ is false since (1) is **True** and therefore p is **True**.

B – We want to show $p \rightarrow q$

Assume the negation of the conclusion, i.e., $\neg q$

Show that $(p \wedge \neg q) \rightarrow \mathbf{F}$

Since $((p \wedge \neg q) \rightarrow \mathbf{F}) \Leftrightarrow (p \rightarrow q)$ (why?) we are done

$((p \wedge \neg q) \rightarrow \mathbf{F}) \Leftrightarrow \neg(p \wedge \neg q)$

$\Leftrightarrow p \rightarrow q$

Example 1: Proof by Contradiction

- Example:

Hmm. We will assume "not Hot" ≡ "Cold"

- Rainy days make gardens grow.
- Gardens don't grow if it is not hot.
- When it is cold outside, it rains.
- Prove that it's hot.

Let
R – Rainy day
G – Garden grows
H – It is hot

Given: $R \rightarrow G$
$\neg H \rightarrow \neg G$
$\neg H \rightarrow R$
Show: H

$$((R \rightarrow G) \wedge (\neg H \rightarrow \neg G) \wedge (\neg H \rightarrow R)) \rightarrow H$$
?

Example 1: Proof by Contradiction

Given: $R \rightarrow G$

$\neg H \rightarrow \neg G$

$\neg H \rightarrow R$

Show: H

1. $R \rightarrow G$	Given
2. $\neg H \rightarrow \neg G$	Given
3. $\neg H \rightarrow R$	Given
4. $\neg H$	assume negation of conclusion
5. R	MP (3,4)
6. G	MP (1,5)
7. $\neg G$	MP (2,4)
8. $G \wedge \neg G$	contradiction

$\therefore$ H

Aside: we assume it's either Hot or it is not Hot. Called the "*law of excluded middle*". In certain complex arguments, it's not so clearly valid. (hmm…) This led to

"constructive mathematics" and "intuitionistic mathematics".

Example2: Proof by Contradiction

Classic proof that $\sqrt{2}$ is irrational.

It's quite clever!!

Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = a/b$ for some integers a and b (relatively prime; no factor in common).

$\sqrt{2} = a/b$ implies

$2 = a^2/b^2$

$2b^2 = a^2$

Note: Here we again first go to the definition of concepts ("rational"). Makes sense! Definitions provide information about important concepts. In a sense, math is all about "What follows from the definitions and premises!

a^2 is even, and so a is even (a = 2k for some k)

$2b^2 = (2k)^2 = 4k^2$

$b^2 = 2k^2$

b^2 is even, and so b is even (b = 2k for some k)

But if a and b are both even, then they are not relatively prime!
Q.E.D.

Example2: Proof by Contradiction

- You're going to let me get away with that? ☺

Lemma: a^2 is even implies that a is even (i.e., $a = 2k$ for some k)??

Suppose to the contrary that a is not even.

Then $a = 2k + 1$ for some integer k

Then $a^2 = (2k + 1)(2k + 1) = 4k^2 + 4k + 1$

and a^2 is odd.

Then, as discussed earlier, a^2 is not even

contradiction

So, a really is even.

Corollary: An integer n is even if and only if n^2 is even

Why does the above statement follow immediately from previous work???

Example 3: Proof by Contradiction

Theorem:
"There are infinitely many prime numbers"

(Euclid's proof, c 300 BC)
One of the most famous early proofs. An early intellectual "tour the force".

Proof by contradiction

Let P – "There are infinitely many primes"

Assume ¬P, i.e., "there is a finite number of primes" , call largest p_r.

Let's define R the product of all the primes, i.e, $R = p_1 \times p_2 \times \ldots \times p_r$.

Consider R + 1.

Now, R+1 is either prime or not:

(Clever "trick". The key to the proof.)

If it's prime, we have prime larger than p_r.

If it's not prime, let p* be a prime dividing (R+1). But p* cannot be any of p_1, p_2, … p_r (remainder 1 after division); so, p* not among initial list and thus p* is larger than p_r.

This contradicts our assumption that there is a finite set of primes, and therefore such an assumption has to be false which means that there are infinitely many primes.

Also, non-constructive.

See e.g. http://odin.mdacc.tmc.edu/~krc/numbers/infitude.html
http://primes.utm.edu/notes/proofs/infinite/euclids.html

Example 4: Proof by Contradiction

Theorem **"If 3n+2 is odd, then n is odd"**

Let p = "3n+2 is odd" and q = "n is odd"

1 – assume p and ¬q i.e., 3n+2 is odd and n is not odd

2 – because n is not odd, it is even

3 – if n is even, n = 2k for some k,

and therefore 3n+2 = 3 (2k) + 2 = 2 (3k + 1), which is even

4 – So, we have a contradiction, 3n+2 is odd and 3n+2 is even.

Therefore, we conclude p → q, i.e.,
"If 3n+2 is odd, then n is odd" Q.E.D.

Proof of Equivalences

To prove $p \leftrightarrow q$

show that $p \rightarrow q$

and $q \rightarrow p$.

The validity of this proof results from the fact that

$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$ is a tautology

Counterexamples

- Show that ∀(x) P(x) is false
- We need only to find a counterexample.

Counterexample

Show that the following statement is false:

“Every day of the week is a weekday”

Proof: ☺

Saturday and Sunday are weekend days.

Proof by Cases

To show $(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$

We use the tautology

$[(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q] \leftrightarrow [(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q)]$

A particular case of a proof by cases is an exhaustive proof in which all the cases are considered

Theorem:
"If n is an integer, then $n^2 \geq n$ "

Proof by cases

Case 1 n=0 $0^2 = 0$

Case 2 $n > 0$, i.e., $n \geq 1$.

We get $n^2 \geq n$ since we can multiply both sides of the inequality by n, which is positive.

Case 3 $n < 0$.

Then $n \times n > 0 \times n$ since n is negative and multiplying both sides of inequality by n changes the direction of the inequality). So, we have $n^2 > 0$ in this case.

In conclusion, $n^2 \geq n$ since this is true in all cases.

Existence Proofs

- Constructive existence proofs
  - **Example: "there is a positive integer that is the sum of cubes of positive integers in two different ways"**
  - **Proof: Show by brute force using a computer 1729 = 103 + 93 = 123 + 13**

- Non-constructive existence proofs
  - **Example: "∀n (integers), ∃p so that p is prime, and p > n."**
  - **Proof: Recall proof used to show there were infinitely many primes.**
  - **Very subtle – does not give an example of such a number, but shows one exists.**
  - **(Let P = product of all primes < n and consider P+1.)**

- **Uniqueness proofs** involve
- Existence proof
- Uniqueness proof

NON-CONSTRUCTIVE

Example 1 - Existence Proofs

- $\forall n$ (integers), $\exists p$ so that p is prime, and $p > n$.
- Proof: Let n be an arbitrary integer, and consider n! + 1. If (n! + 1) is prime, we are done since (n! + 1) > n. But what if (n! + 1) is composite?

If (n! + 1) is composite then it has a prime factorization, $p_1 p_2 \ldots p_n = (n! + 1)$

Consider the smallest p_i, and call it p. How small can it be?

So, p > n, and we are done.
BUT WE DON'T KNOW WHAT p IS!!!

Can it be 2?

Can it be 3?

Can it be 4?

Can it be n?

Example 2: Existence proof

Thm. There exists irrational numbers x and y such that x^y is rational.

Proof.
$\sqrt{2}$ is irrational (see earlier proof).

"Start with something you know about rational / irrational numbers."

Consider: $z = \sqrt{2}^{\sqrt{2}}$

Non-constructive!

We have two possible cases:
z is rational. Then, we're done (take $x = \sqrt{2}$ and $y = \sqrt{2}$).
z is irrational. Now, let x = z and $y = \sqrt{2}$. And consider:

$x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2}\,\sqrt{2})} = \sqrt{2}^2 = 2$, which is rational. So, we're done.

Since, either 1) or 2) must be true, it follows that there does exist irrational x and y such that x^y is rational. Q.E.D.

So… what is it: is $\sqrt{2}^{\sqrt{2}}$ rational or not?? guess?

It's irrational but requires very different proof…

Poisonous

Example 3: Non-constructive proof

•From game theory.

•Consider the game "Chomp".

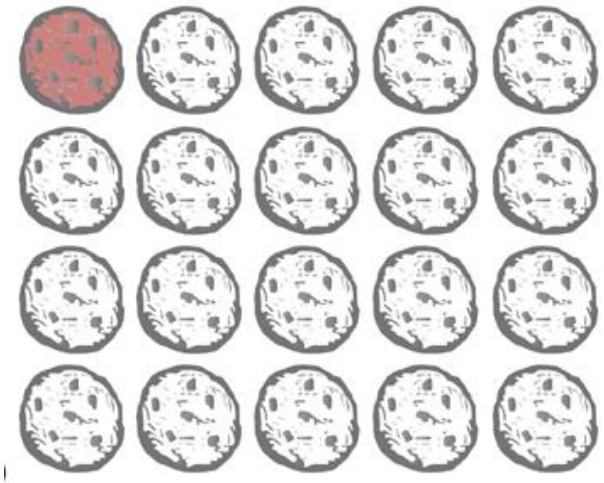
•Two players. Players take turn eating

•at least one of the remaining cookies.

•At each turn, the player also eats all cookies to the left and below the cookie he or she selects.

•The player who is "forced" to eat the poisened cookie loses. ☹

•Is there a winning strategy for either player?



m x n cookies

Winning strategy for a player:
"A way of making moves" that is guaranteed to lead to a win, no matter what the opponent does. (How big to write down?)

•Claim: First player has a winning strategy!

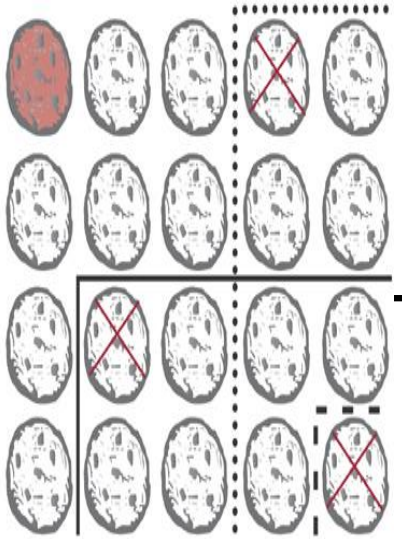
•Proof. (non-constructive)

•First, note that the game cannot end in a "draw".

•After at most m x n moves, someone has eaten the last cookie. ☹

•Consider the following strategy for the first player:

•--- Start by eating the cookie in the bottom right corner.



Three possible moves

--- Now, two possibilities:

1) This is part of a winning strategy for 1st player (and thus player has winning strategy). OR
2) 2nd player can now make a move that is part of the winning strategy for the 2nd player.

But, if 2) is the case, then 1st player can follow a winning strategy by on the first move making the move of the second player and following his or her winning strategy! So, again, 1st player has winning strategy. Q.E.D.

This is called a "strategy stealing" argument. Think through carefully to convince yourself!
(**Actual** strategy not known for general boards!)

Corner is "null move"

Is first choice of the bottom right cookie essential? If so, why?

Fallacies

- Fallacies are incorrect inferences. Some common fallacies:

1. The Fallacy of Affirming the Consequent
2. The Fallacy of Denying the Antecedent
3. Begging the question or circular reasoning

The Fallacy of Affirming the Consequent

If the butler did it he has blood on his hands.
The butler had blood on his hands.
Therefore, the butler did it.

This argument has the form

$$\frac{\begin{array}{l} P \rightarrow Q \\ Q \end{array}}{\therefore\ P}$$

or $((P \rightarrow Q) \wedge Q) \rightarrow P$ which is not a tautology and therefore not a valid rule of inference

The Fallacy of Denying the Antecedent

- *If the butler is nervous, he did it.*
- *The butler is really mellow.*
- *Therefore, the butler didn't do it.*

This argument has the form

$$P \rightarrow Q$$
$$\neg P$$
$$\therefore \neg Q$$

or $((P \rightarrow Q) \wedge \neg P) \rightarrow \neg Q$ which is not a tautology and therefore not a valid rule of inference

Begging the question or circular reasoning

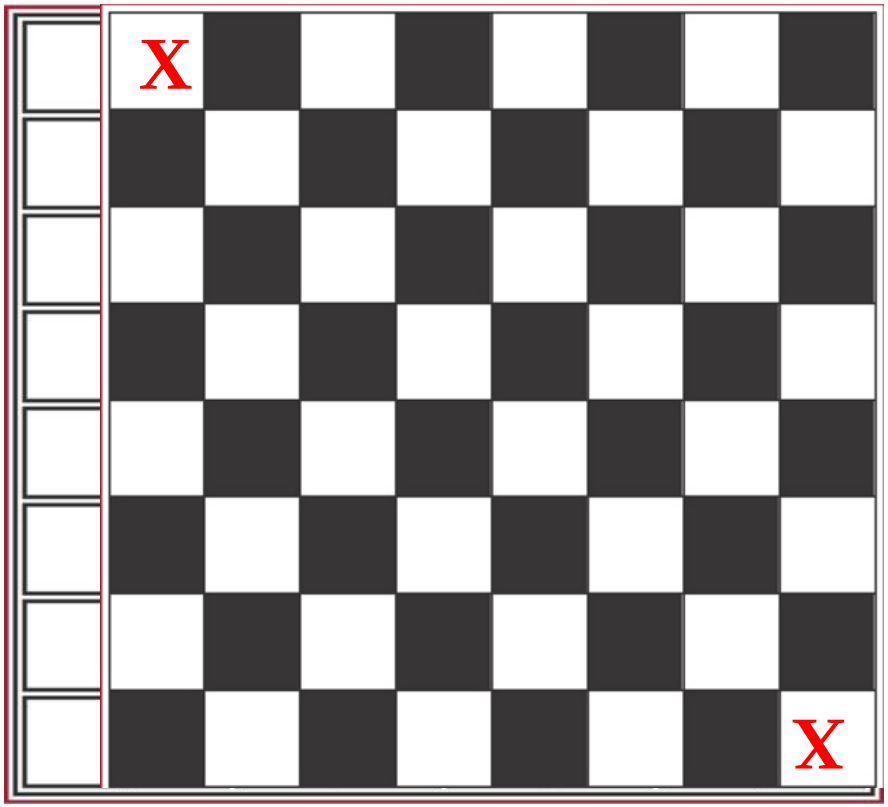
This occurs when we use the truth of the statement being proved (or something equivalent) in the proof itself.

Example:
Conjecture: *if n^2 is even then n is even.*
Proof: If n^2 is even then $n^2 = 2k$ for some k. Let $n = 2m$ for some m. Hence, x must be even.

Note that the statement $n = 2m$ is introduced without any argument showing it.

Notoriously hard problem
automated theorem prover
--- requires "true cleverness"

Final example Tiling



Standard checkerboard. 8x8 = 64 squares

A domino

62 squares: 32 black
30 white
31 doms.: 31 black
31 white squares!

Can you use 32 dominos to cover the board? Easily! (many ways!)

What about the mutilated checkerboard? Hmm… **No! Why?** Use counting?

What is the proof based upon?
Proof uses clever coloring and counting argument.
Note: also valid for board and dominos without b&w pattern!
(use proof by contradiction)

Additional Proof Methods Covered in CS23022

- Induction Proofs
- Combinatorial proofs
- But first we have to cover some basic notions on sets, functions, and counting.