Final Review

- Representation of integers in base $b$
- Logic
- Proof systems:
  - Direct Proof
  - Proof by contradiction
  - Contrapositive
- Sets Theory
- Functions
- Induction

NO CALCULATOR, NO CHEAT SHEET
Anything that you can assume in the proofs will be clearly given.
Final Review

- Representation of integers in base $b$
- Logic
- Proof systems:
  - Direct Proof
  - Proof by contradiction
  - Contrapositive
- Sets Theory
- Functions
- Induction

NO CALCULATOR, NO CHEAT SHEET

Anything that you can assume in the proofs will be clearly given.
Propositional Logic

- Every statement is either TRUE or FALSE
- There are logical connectives $\lor$, $\land$, $\neg$, $\Rightarrow$ and $\Leftrightarrow$.
- Two logical statements can be equivalent if the two statements answer exactly in the same way on every input.
- To check whether two logical statements are equivalent one can do one of the following:
  - Checking the Truth Table of each statement
  - Reducing one to the other using reductions
Propositional Logic

- Check the correctness of a statement: whether a sentence/paragraph/proposition is logically correct.
Propositional Logic

- Check the correctness of a statement: whether a sentence/paragraph/proposition is logically correct.
- Make deductions
Propositional Logic

- Check the correctness of a statement: whether a sentence/paragraph/proposition is logically correct.

- Make deductions

- Check if two propositions are equivalent.
Equivalence of statements/propositions

If the truth tables of two statement/propositions are identical then the two statement/propositions are equivalent.

One can also use various rules for propositional logic.
Rules of Propositional Logic

1. Commutative law:
   
   \((p \lor q) = (q \lor p)\) and \((p \land q) = (q \land p)\)

2. Associative law:
   
   \((p \lor (q \lor r)) = ((p \lor q) \lor r)\) and
   
   \((p \land (q \land r)) = ((p \land q) \land r)\)

3. Distributive law:
   
   \((p \lor (q \land r)) = (p \lor q) \land (p \lor r)\) and
   
   \((p \land (q \lor r)) = (p \land q) \lor (p \land r)\)

4. De Morgan’s Law:
   
   \(\neg(p \lor q) = (\neg p \land \neg q)\) and \(\neg(p \land q) = (\neg p \lor \neg q)\)
Sets

For example:
- Set of names of all students

Size of a set is the number of elements in the set. Size of set $A$ is denoted by $|A|$. 
Sets

For example:
- Set of names of all students
- Set of letters in the english alphabet
Sets

For example:
- Set of names of all students
- Set of letters in the english alphabet
- Set of digits. \( \{0, 1, \ldots, 9\} \) or \( \{0, 1\} \)

Size of a set is the number of elements in the set. Size of set \( A \) is denoted by \( |A| \).
Operations on Sets

- **Union**, $\cup$
  $A \cup B$ is the set of all elements that are in $A$ OR $B$.

- **Intersection**, $\cap$
  $A \cap B$ is the set of all elements that are in $A$ AND $B$.

- **Complement**, $A^c$ or $\bar{A}$
  $A^c$ is the set of elements NOT in $A$.

- **Cartesian Product**.
  For example: $A^3 = A \times A \times A$. 
Rules of Set Theory

Let $p$, $q$ and $r$ be sets.

1. Commutative law:
   
   \[(p \cup q) = (q \cup p) \quad \text{and} \quad (p \cap q) = (q \cap p)\]

2. Associative law:
   
   \[(p \cup (q \cup r)) = ((p \cup q) \cup r) \quad \text{and} \quad (p \cap (q \cap r)) = ((p \cap q) \cap r)\]

3. Distributive law:
   
   \[(p \cup (q \cap r)) = (p \cup q) \cap (p \cup r) \quad \text{and} \quad (p \cap (q \cup r)) = (p \cap q) \cup (p \cap r)\]

4. De Morgan’s Law:
   
   \[(p \cup q)^c = (p^c \cap q^c) \quad \text{and} \quad (p \cap q)^c = (p^c \cup q^c)\]
Set Theory and Propositional Logic is two mathematical language which follow very similar rules.
There are two important symbols: ∀ and ∃.

Some statements can be defined using a variable.

For example: $P_x = "4x^2 + 3$ is divisible by 5”

We can have statements like: $\forall x \in \mathbb{Z}, 4x^2 + 3$ is divisible by 5.

Or $\exists x \in \mathbb{Z}, 4x^2 + 3$ is divisible by 5.
Rules of negation

\[ \neg (\forall x, \ P_x) = (\exists x, \ \neg P_x). \]
\[ \neg (\exists x, \ P_x) = (\forall x, \ \neg P_x). \]
Proof Techniques

To prove statement $B$ from $A$:
Proof Techniques

To prove statement $B$ from $A$:

- **Direct Proof:**
  
  $A \implies B$

- **Proof by contradiction:**
  
  $(\neg B \land A)$ gives a contradiction

- **Proof by Contrapositive:** $A \implies B$ is same as proving $\neg B \implies \neg A$.

- **Induction**
Proofs done in class

- Square of an odd integer is of form \( 4k + 1 \).
Proofs done in class

- Square of an odd integer is of form $4k + 1$.
- Primes, greater than 3, is of form $6k + 1$ or $6k + 5$. 
Proofs done in class

- Square of an odd integer is of form $4k + 1$.
- Primes, greater than 3, is of form $6k + 1$ or $6k + 5$.
- A prime $p$ is either 2 or 3 or $p^2$ is of form $6k + 1$. 

$\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{2} + \sqrt{3}$ are not rational.

$\forall n \geq 1 + 2 + \cdots + n = \frac{n(n + 1)}{2}$

Prove that for all $n \geq 5$, $n^2 \geq 4n + 5$

If $a_n = a_{n-1} + 2$ and $a_1 = 2$ prove that $a_n = 2^n$

If $a_n = a_{n-1} + a_{n-2}$ and $a_1 = a_2 = 1$ then $a_n = 1$
Proofs done in class

- Square of an odd integer is of form $4k + 1$.
- Primes, greater than 3, is of form $6k + 1$ or $6k + 5$.
- A prime $p$ is either 2 or 3 or $p^2$ is of form $6k + 1$.
- $\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{2} + \sqrt{3}$ are not rational.
Proofs done in class

- Square of an odd integer is of form $4k + 1$.
- Primes, greater than 3, is of form $6k + 1$ or $6k + 5$.
- A prime $p$ is either 2 or 3 or $p^2$ is of form $6k + 1$.
- $\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{2} + \sqrt{3}$ are not rational.
- $\forall n \ 1 + 2 + \cdots + n = n(n + 1)/2$
Proofs done in class

- Square of an odd integer is of form $4k + 1$.
- Primes, greater than 3, is of form $6k + 1$ or $6k + 5$.
- A prime $p$ is either 2 or 3 or $p^2$ is of form $6k + 1$.
- $\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{2} + \sqrt{3}$ are not rational.
- $\forall n \ 1 + 2 + \cdots + n = n(n + 1)/2$
- Prove that for all $n \geq 5$, $n^2 \geq 4n + 5$
Proofs done in class

- Square of an odd integer is of form $4k + 1$.
- Primes, greater than 3, is of form $6k + 1$ or $6k + 5$.
- A prime $p$ is either 2 or 3 or $p^2$ is of form $6k + 1$.
- $\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{2} + \sqrt{3}$ are not rational.
- $\forall n \ 1 + 2 + \cdots + n = n(n + 1)/2$
- Prove that for all $n \geq 5$, $n^2 \geq 4n + 5$
- If $a_n = a_{n-1} + 2$ and $a_1 = 2$ prove that $a_n = 2n$
Proofs done in class

- Square of an odd integer is of form $4k + 1$.
- Primes, greater than 3, is of form $6k + 1$ or $6k + 5$.
- A prime $p$ is either 2 or 3 or $p^2$ is of form $6k + 1$.
- $\sqrt{2}$ and $\sqrt{3}$ and $\sqrt{2} + \sqrt{3}$ are not rational.
- $\forall n \ 1 + 2 + \cdots + n = n(n + 1)/2$
- Prove that for all $n \geq 5$, $n^2 \geq 4n + 5$
- If $a_n = a_{n-1} + 2$ and $a_1 = 2$ prove that $a_n = 2n$
- If $a_n = a_{n-1} + a_{n-2}$ and $a_1 = a_2 = 1$ then

$$a_n = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right)$$
If we have to prove “∀n ≥ r P(n) is True.”

Let us induct on n.

- Base Case: Prove that the P(r) is true.
- Induction Hypothesis: Let for some k ≥ r P(k) is true.
- Inductive Step: We want to show, assuming IH, P(k + 1) is true.

By induction we have proved that ∀n ≥ r P(n) is true.
If we have to prove \( \forall n \geq r \ P(n) \) is True.

Let us induct on \( n \).

- **Base Case:** Prove that the \( P(r) \) and \( P(r + 1) \) is true.
- **Induction Hypothesis:** Let for some \( k \geq r \ P(k) \) and \( P(k + 1) \) is true.
- **Inductive Step:** We want to show, assuming IH, \( P(k + 2) \) is true.

By induction we have proved that \( \forall n \geq r \ P(n) \) is true.