NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Discrete Mathematics

MH1812

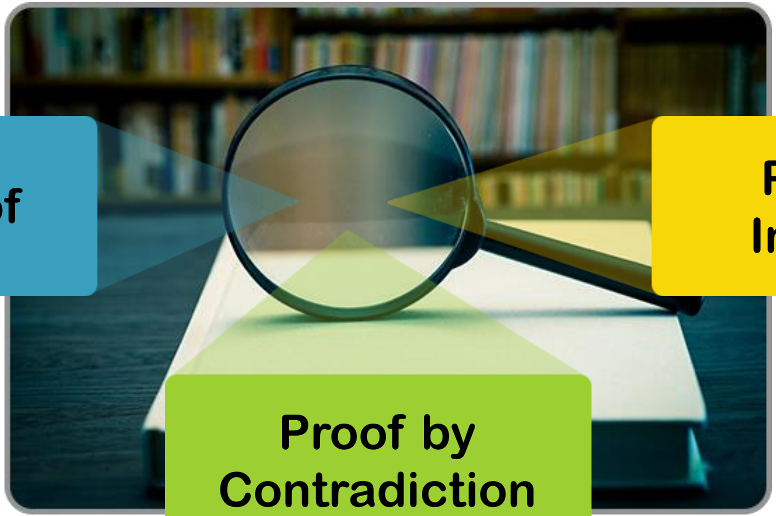
not in Midterm !

Topic 4 - Proof Techniques Summary

Types of Proof Techniques

A valid proof is a valid argument, i.e., the conclusion follows from the given assumptions.

Three Techniques



Direct Proof

Proof by Induction

Proof by Contradiction

Direct Proof: Example

$\mathbb{N} = \{1, 2, 3, \ldots\}$

Prove that $$\forall n \in N, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Define: $$S = \sum_{i=0}^{n} i = \underbrace{0+1+2+\ldots+n-1+n}_{n+1 \text{ Terms}}$$

Note: $$S = \sum_{i=0}^{n} i = n+n-1+\ldots+2+1+0$$

Sum up: $$2S = \overbrace{n+n+\ldots+n+n+n}^{n+1 \text{ Terms}}$$

$$2S = (n+1)\,n$$

Thus: $$S = \frac{n(n+1)}{2}$$

Proof by Induction: Mathematical Induction

Prove propositions of the form: $\forall n, P(n)$

$\forall n \in \mathbb{N}$

$\forall n \in \mathbb{R}$ ✗

The proof consists of two steps.

1 Basis Step

The proposition $P(1)$ is shown to be true.

2 Inductive Step

Assume $P(k)$ is true (when $n = k$), then prove $P(k + 1)$ is true (when $n = k + 1$).

When both steps are complete, we have proved that "$\forall n, P(n)$" is true.

$P(1)$ ↙ basis step

$\boxed{\forall k \in \mathbb{N},\ P(k) \to P(k+1)}$

↖ inductive step

$P(1) \to P(2)$

$\therefore P(2)$ (Modus ponens)

$P(2) \to P(3)$

$\therefore P(3)$ (Modus Ponens)

$\vdots$

Strong/Complete Induction

$$\boxed{\forall k \in \mathbb{N},\ P(1) \wedge P(2) \wedge \ldots \wedge P(k-1) \rightarrow P(k)}$$

Proof by Induction: Mathematical Induction (Example)

Prove that $\underbrace{\forall n \in N, \sum_{i=0}^{n} i = \frac{n(n+1)}{2}}_{P(n)}$

$\mathbb{N} = \{1, 2, \ldots\}$

Let $P(n)$ **denote:** $\left[\sum_{i=0}^{n} i = \frac{n(n+1)}{2}\right]$

LHS

RHS

Basis Step 1

$P(1)$ **is true.**

$0 + 1 = \frac{1(1+1)}{2}$

LHS

RHS

Proof by Induction: Mathematical Induction (Example)

(Inductive Step) Assume $P(k)$ **true,** $k > 0$**:**

$$\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$$

$\leftarrow P(k)$

Prove $P(k+1)$ **true:**

LHS of $P(k+1)$

$$\sum_{i=0}^{k+1} i = \sum_{i=0}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1)$$

RHS $P(k+1)$

$$= \frac{(k+1)(k+2)}{2} = \frac{(k+1)[(k+1)+1]}{2}$$

So, $P(n)$ **is true for** $n = k + 1$ **and thus true for all** n**:** $\forall n, P(n)$ **is true.**

Advice: write-out $P(k+1)$ $\boxed{\text{Practice!}}$

Proof by Contradiction/Contrapositive

Contradiction:

E.g., "$\sqrt{2}$ is irrational" = $P(2)$

suppose $\neg P(2)$ = "$\sqrt{2}$ is rational"

- We want to prove $\boxed{P(n)}$
- This is equivalent to proving that $\boxed{\neg P(n) \to F}$

Contrapositive:

E.g., "n^2 is even" $\to$ "n even"

$\equiv$ "n is odd" $\to$ "n^2 is odd"

- We want to prove $\boxed{P(n) \to Q(n)}$
- This is equivalent to proving that $\boxed{\neg Q(n) \to \neg P(n)}$

Compute 15^{2018} modulo 7 (10 points).

$$ab \pmod{n} \equiv \underline{(a \bmod n)}\underline{(b \bmod n)}$$

$$15^{2018} \equiv \underbrace{15 \cdot 15 \cdot 15 \cdot \cdots \cdot 15}_{2018} \equiv \underbrace{1 \cdot 1 \cdot \cdots \cdot 1}_{2018}$$

$$\equiv \underline{\underline{1}} \pmod{7}$$

$$15 \equiv 1 \pmod{7}$$

$$16^{2018} \pmod 7 \qquad 2 \pmod 7 ?$$

$$16^{2018} = \underbrace{16 \cdot 16 \cdot \ldots \cdot 16}_{2018} \equiv \underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{2018} \pmod 7$$

$$\equiv \underbrace{(2 \cdot 2 \cdot 2)}_{\underset{1}{\parallel}} \cdot \underbrace{(2 \cdot 2 \cdot 2)} \cdot \ldots \cdot 2 \pmod 7$$

Note $2^3 \equiv 1 \pmod 7$

$$2018 \pmod 3 \equiv 2016 + 2$$

$$\equiv 2 \pmod 3$$

$$\equiv (2^3)^k \cdot 2^2 \pmod 7$$

$$\equiv 1 \cdot 2^2$$

16^{2018}

$$\equiv 4 \pmod 7$$

$$\equiv 11$$

$$\equiv 18$$

$$\vdots$$

Consider the set S of multiples of 4 that is $S = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$. Is the set S closed under multiplication? Justify your answer(10 points).

$\forall\, a, b \in S, \quad a \cdot b \in S?$ Yes

Justification

Take $a, b \in S$ $\qquad A, B \in \mathbb{Z}$

$\Rightarrow \quad a = 4A$

$\qquad b = 4B$

Then $\quad a \cdot b = 4A \cdot 4B = 4(\underbrace{4A \cdot B}_{\in \mathbb{Z}})$

$\therefore\ a \cdot b \in S$

looks more complicated

1. Prove or disprove the following statement (20 points):

$$\underbrace{(p \to (q \to r))}_{LHS} \equiv ((p \wedge q) \to r).$$

$p = T$

$q = F$

$r = T$

$LHS = p \to (q \to r) \equiv \neg p \vee (q \to r)$ conversion thm

$\equiv \neg p \vee (\neg q \vee r)$ ''

$\equiv (\neg p \vee \neg q) \vee r$ associativity

$\equiv \neg (p \wedge q) \vee r$ De Morgan

$\equiv (p \wedge q) \to r$ conversion

1. Prove or disprove the following statement (20 points):

$$(p \to (q \to r)) \equiv ((p \wedge q) \to r).$$

p	q	r	$q \to r$	$p \to (q \to r)$	$p \wedge q$	$p \wedge q \to r$
T	T	T	T	T	T	T
T	T	F	F	F	T	F
T	F	T	T	T	F	T
T	F	F	T	T	F	T
F	T	T	T	T	F	T
F	T	F	F	T	F	T
F	F	T	T	T	F	T
F	F	F	T	T	F	T

Decide whether the following argument is valid (20 points):

$$\left.\begin{array}{l} p \\ p \to q \end{array}\right\} \therefore q$$

$$\left.\begin{array}{l} q \\ \neg q \vee r \end{array}\right\} \therefore r$$

$$\begin{array}{l} p \\ p \to q \\ \neg q \vee r \\ \therefore r \end{array}$$

1. p
2. $p \to q$
3. $\neg q \vee r \equiv q \to r$ (conversion)
4. $\therefore q$ (modus ponens on 1 & 2)

$\therefore r$ (modus ponens on 3 & 4)

Decide whether the following argument is valid (20 points):

$$\begin{array}{l} p \\ p \to q \\ \neg q \vee r \\ \therefore r \end{array}$$

Premises

p	q	r	$p \to q$	$\neg q$	$\neg q \vee r$
T	T	T	T	F	T
T	T	F	T	F	F
T	F	T	F		
T	F	F	F		

critical row

conclusion (r) is true

$\forall$ critical rows

$\therefore$ argument is valid.

Given sets $A = \{3, 4\}$, $B = \{2, 3, 5\}$, and $P(x, y)$ denotes "$x^2 - y^2 \geq 5$", determine the truth value of the following statement and justify your answer :

1. $\forall x \in A, \exists y \in B, P(x, y)$ (15 points). T

For $x = 3$ take $y = 2$ then $P(x,y) = T$

For $x = 4$ take $y = 2$ then $P(x,y) = T$

2. $\exists x \in A, \forall y \in B, P(x, y)$ (15 points). F

Try $x = 3$, for $y = 5$ have $P(x,y) = F$ ✗

Try $x = 4$, for $y = 5$ have $P(x,y) = F$ ✗