COMP 3011
DESIGN AND ANALYSIS OF ALGORITHMS
FALL 2024

Math Foundations

LI Bo
Department of Computing
The Hong Kong Polytechnic University

MATH FOUNDATIONS

STATEMENTS AND THEIR USE

Statement: a mathematical expression which is either true or false

Examples: $2 \in \{x \in R | x \leq 5\}$ (true) or $3^2 + 5^2 = 82$ (false)

Note: The domain of the variables matters!

- $1.5 \in \{x \in R | x \leq 5\}$ (true)
- $1.5 \in \{x \in N | x \leq 5\}$ (false)

R: real numbers
Q: rational numbers
N: natural numbers

- ***Theorem:*** to state an important result.
- ***Lemma:*** for smaller results that are intermediate steps to show a theorem.
- ***Claim:*** for even smaller results that are intermediate steps to show a lemma.
- ***Conjecture:*** for statements that you believe are true, but you can't prove them.
- ***Fact/Observation:*** for mathematical facts that are general knowledge (Example: $2 > 1$).

FORMAL MATHEMATICAL PROOFS

A ***formal mathematical proof*** of a statement S consists of an ordered (maybe even numbered) sequence of statements.

$$A \text{ implies } B, B \text{ implies } C, \cdots, X \text{ implies the claim}$$

Each ***statement*** in a proof is

- an assumption or
- it follows from previous statements or from the assumptions in S by a rule of inference

Note:

- Expressions whose truth cannot be determined cannot occur in proofs.
- For each expression, all involved variables must be defined.

SIMPLE PROOF TECHNIQUES

Proof by ***Example***: give an example and show that it satisfies the statement.

- for proving existential statements ("There exists…") E.g. There exists a rational number being an integer
- for disproving universal statements ("For all…") E.g. All rational numbers are integers

Proof by ***Exhaustive Enumeration***: list all elements (satisfying the assumption) and show that they all satisfy the statement.

- for proving universal statements ("For all…") E.g. All integers are rational numbers
- for disproving existential statements ("There exists…") E.g. There exists a rational number being irrational

Proof by ***Contradiction***: assume the negation of the statement and derive a contradiction.

EXAMPLE: PROOF BY EXAMPLE

Prove statement: *there exists a prime number between 80 and 90*

Proof. $p = 83$.■

Incomplete Proof!

Proof.

- $p = 83$
- $83>80$ and $83<90$
- show that 83 is a prime number by exhaustive enumeration:

  $2, 3, 4, \cdots, \sqrt{83}$ does not divide 83. ■

PROOF BY EXAMPLE

Disprove statement: *for all prime number* $n > 1, 2^n - 1$ *is prime.*

Proof:

- $n = 11$.
- $n > 1$ and n is a prime number (2, 3 do not divide 11).
- $2^n - 1 = 2047 = 23 * 89$ is not a prime number.■

MATHEMATICAL INDUCTION

- Summation formulas like $\sum_{i=1}^{n} 2i + 1 = n$^2 for all integer $n \geq 1$.
- Inequalities like $2^n < n!$ for every integer $n \geq 4$.
- Divisibility results like $n^3 - n$ is divisible by 3 for every integer $n \geq 1$.

Variation

- Assume true for all $n_0 \leq n \leq k$.
- Prove for $P(k+1)$.

Statement: $P(n)$ for $n \geq n_0$.

- ***Base Case***: prove statement $P(1)$.
- ***Induction Step***: Assume the statement is true for some integer $k \geq n_0$, i.e., $P(k)$.

  (This is the ***Induction Hypothesis***.)

  Prove statement $P(k+1)$.
- ***Conclusion***: the statement $P(n)$ holds for all integer $n \geq n_0$.

PROVING AND USING STATEMENTS

- Existential Statements (∀)
- Universal Statements (∃)
- Disjunction Statements (∨)
- Conjunction Statements (∧)
- Implication Statements (“if… then…”)
- Equivalence Statements (“iff”)

EXISTENTIAL STATEMENTS

There exists x such that $A(x)$ (assumption), $P(x)$ (property).

Example: *there exists* x *s.t.* $x \geq 0$, *and* $x \geq 10$.

Proof:

- Give an example $\boldsymbol{x}$ satisfying the assumption $A(x)$.
- Show that $P(x)$ holds.

Example: pick $x = 11 \geq 0$, and $x \geq 10$.

UNIVERSAL STATEMENTS

For all x such that $A(x)$ (assumption), then $P(x)$ (property).

- In general, x can be a set of elements. E.g., $\forall\ a, b, c$ s.t. $A(a, b, c), P(a, b, c)$.
- ***Example***: for all sets A, B, C s.t. $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Proof:

- Let x be an arbitrarily chosen element satisfying the assumption $A(x)$.
- Show that $P(x)$ holds.

Example: let x be an arbitrary element in A

- $A \subseteq B$ implies for all $t \in A, t \in B$; thus $x \in B$
- $B \subseteq C$ implies for all $t \in B, t \in C$; thus $x \in C$
- Thus $A \subseteq C$.

For all $x \in A, x \in B$;

NEGATION, DISJUNCTION, CONJUNCTION

- The ***negation*** of

$$\text{for all } x \text{ s.t. } A(x), P(x)$$

  is

$$\text{for some } x \text{ s.t. } A(x), \neg P(x)$$

For all number x such that x is rational, x is an integer.

$\Big\downarrow$ ***negation***

For some number x such that x is rational, x is not an integer.

- ***Disjunction***: To prove P1 or P2 or . . . or Pn is true
  - show one of P1, P2, . . . , Pn is true
  - often done by case analysis

- ***Conjunction***: P1 and P2 and . . . and Pn is true
  - show all of P1, P2, . . . , Pn are true

IMPLICATION AND EQUIVALENCE STATEMENTS

If P, then Q

Proof:

- assume P is true and show Q, or
- assume $\neg$Q is true and show $\neg$P (proof by contradiction)

P if and only if Q ($P \leftrightarrow Q$)

Proof:

- show "if P then Q" and
- show "if Q then P"

EXAMPLE

Prove statement: for all sets A, B, $A \cup B = A$ if and only if $B \subseteq A$.

Proof.

- Proving if $A \cup B = A$, then $B \subseteq A$.
  - Pick any $x \in B$
  - Since $A \cup B = A$, $x \in A$, then $B \subseteq A$
- Proving if $B \subseteq A$, then $A \cup B = A$.
  - It is obvious $A \subseteq A \cup B$
  - To show $A \cup B \subseteq A$, pick any $x \in A \cup B$
  - We need to show $x \in A$

- $x \in A \cup B$
- If $x \in A$, we are done
- If $x \in B$, we know $B \subseteq A$ and thus $x \in A$

Thank you!