CS1231S

AY20/21 Sem 1

01. PROOFS

sets of numbers

$\mathbb{N}$: natural numbers ($\mathbb{Z}_{\geq 0}$)
$\mathbb{Z}$: integers
$\mathbb{Q}$: rational numbers
$\mathbb{R}$: real numbers
$\mathbb{C}$: complex numbers

basic properties of integers

closure (under addition and multiplication)
$$x + y \in \mathbb{Z} \wedge xy \in \mathbb{Z}$$
commutativity
$$a + b = b + a \wedge ab = ba$$
associativity
$$a + b + c = a + (b + c) = (a + b) + c$$
$$abc = a(bc) = (ab)c$$
distributivity
$$a(b + c) = ab + ac$$
trichotomy
$$(a < b) \vee (a > b) \vee (a = b)$$
transitive law
$$(a < b) \wedge (b < c) \implies (a < c)$$

definitions

even/odd
n is even $\leftrightarrow \exists k \in \mathbb{Z} \mid n = 2k$
n is odd $\leftrightarrow \exists k \in \mathbb{Z} \mid n = 2k + 1$
prime/composite
n is prime $\leftrightarrow n > 1$ and $\forall r, s \in \mathbb{Z}^+, n = rs \rightarrow (r = n) \vee (r = s)$
n is composite $\leftrightarrow n > 1$ and $\exists r, s \in \mathbb{Z}^+ s.t. n = rs$ and $1 < r < n$ and $1 < s < n$
divisibility (d divides n)
$n \mid d \leftrightarrow \exists k \in \mathbb{Z} \mid n = kd$
rationality
r is rational $\leftrightarrow \exists a, b \in \mathbb{Z} \mid r = \frac{a}{b}$ and $b \neq 0$
floor/ceiling
$\lfloor x \rfloor$: largest integer y such that $y \leq x$
$\lceil x \rceil$: smallest integer y such that $y \geq x$

rules of inference

generalisation	elimination
$p, \therefore p \vee q$	$p \vee q; \sim q, \therefore p$
specialisation	transitivity
$p \wedge q, \therefore p$	$p \rightarrow q; q \rightarrow r; \therefore p \rightarrow r$

04. METHODS OF PROOF

Proof by Exhaustion/Cases

1. list out possible cases
   1.1. Case 1: n is odd OR If $n = 9$, ...
   1.2. Case 2: n is even OR If $n = 16$, ...
2. therefore ...

Proof by Contradiction

1. Suppose that ...
   1.1. ⟨proof⟩
   1.2. ... but this contradicts ...
2. Therefore the assumption that ... is false. Hence ....

Proof by Contraposition

1. Contrapositive statement: $\sim q \rightarrow \sim p$
2. let $\sim q$
   2.1. ⟨proof⟩
   2.2. hence $\sim q$
3. $\therefore p \rightarrow q$

Proof by Induction

1. For each $n \in \mathbb{Z}_{\geq 1}$, let $P(n)$ be the proposition "..."
2. (base step) $P(1)$ is true because ⟨manual method⟩
3. (induction step)
   3.1. let $k \in \mathbb{Z}_{\geq 1}$ s.t. $P(k)$ is true
   3.2. Then ...
   3.3. proof that $P(k + 1)$ is true - e.g. $P(k + 1) = P(k) + term_{k+1}$
   3.4. So $P(k + 1)$ is true.
4. Hence $\forall n \in \mathbb{Z}_{\geq 1} P(n)$ is true by MI.

Proofs for Sets

Equality of Sets (A=B)

1. ($\Rightarrow$)
   1.1. Take any $z \in A$.
   1.2. ...
   1.3. $\therefore z \in B$.
2. ($\Leftarrow$)
   2.1. Take any $z \in B$.
   2.2. ...
   2.3. $\therefore z \in A$.

Element Method

1. $A \wedge (B \cap C) = \{x : x \in A \wedge x \in (B \backslash C)\}$ (by def. of $\cap$)
2. $= \{x : x \in A \wedge (x \in B \wedge x \notin C)\}$ (by def. of $\backslash$)
3. ...
4. $= (A \cap B) \backslash C$ (by def. of $\backslash$)

Other Proofs

iff ($A \leftrightarrow B$)

1. ($\Rightarrow$) Suppose A.
   1.1. ... ⟨proof⟩ ...
   1.2. Hence $A \rightarrow B$
2. ($\Leftarrow$) Suppose B.
   2.1. ... ⟨proof⟩ ...
   2.2. Hence $B \rightarrow A$

02. COMPOUND STATEMENTS

operations

1 $\sim$: negation (not)
2 $\wedge$: conjunction (and)
2 $\vee$: disjunction (or) - coequal to $\wedge$
3 $\rightarrow$: if-then

logical equivalence

- identical truth values in truth table
- definitions
- to show non-equivalence:
  - truth table method (only needs 1 row)
  - counter-example method

conditional statements

$$hypothesis \rightarrow conclusion$$
$$antecedent \rightarrow consequent \tag{1}$$

- **vacuously true** : hypothesis is false
- **implication law** : $p \rightarrow q \equiv \sim p \vee q$

contrapositive : $\sim p \rightarrow \sim q$	converse $\equiv$ inverse
inverse : $\sim p \rightarrow \sim q$	statement $\equiv$ contra-
converse : $q \rightarrow p$	positive

- r is a **necessary** condition for s: $\sim r \rightarrow \sim s$ and $s \rightarrow r$
- r is a **sufficient** condition for s: $r \rightarrow s$
- **necessary** & **sufficient** : $\leftrightarrow$

valid arguments

- determining validity: construct truth table
  - valid $\leftrightarrow$ conclusion is true when premises are true
- **syllogism** : (argument form) 2 premises, 1 conclusion
- **modus ponens** : $p \rightarrow q; p; \therefore q$
- **modus tollens** : $p \rightarrow q; \sim q; \therefore \sim p$
- **sound argument** : is valid & all premises are true

fallacies

converse error	inverse error
$p \rightarrow q$	$p \rightarrow q$
q	$\sim p$
$\therefore p$	$\therefore \sim q$

03. QUANTIFIED STATEMENTS

- **truth set** of $P(x) = \{x \in D \mid P(x)\}$
- $P(x) \Rightarrow Q(x) : \forall x (P(x) \rightarrow Q(x))$
- $P(x) \Leftrightarrow Q(x) : \forall x (P(x) \leftrightarrow Q(x))$

relation between $\forall, \exists, \wedge, \vee$
- $\forall x \in D, Q(x) \equiv Q(x_1) \wedge Q(x_2) \wedge \cdots \wedge Q(x_n)$
- $\exists x \in D \mid Q(x) \equiv Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n)$

05. SETS

notation

- set roster notation [1]: $\{x_1, x_2, \ldots, x_n\}$
- set roster notation [2]: $\{x_1, x_2, x_3, \ldots\}$
- set-builder notation: $\{x \in \mathbb{U} : P(x)\}$

definitions

- **equal sets** : $A = B \leftrightarrow \forall x (x \in A \rightarrow x \in B)$
  - $A = B \leftrightarrow (A \subseteq B) \wedge (A \supseteq B)$
- **empty set**, $\emptyset$: $\emptyset \subseteq$ all sets
- **subset** : $A \subseteq B \leftrightarrow \forall x (x \in A \rightarrow x \in B)$
- **proper subset** : $A \subsetneq B \leftrightarrow (A \subseteq B) \wedge (A \neq B)$
- **power set** of A : $\mathcal{P}(A) = \{X \mid X \subseteq A\}$
  - $|\mathcal{P}(A)| = 2^{|A|}$, given that A is a finite set

- **cardinality** of a set, $\mid A \mid$: number of distinct elements
- **singleton** : sets of size 1
- **disjoint** : $A \cap B = \emptyset$

methods of proof for sets

- direct proof
- element method
- truth table

boolean operations

- **union:** $A \cup B = \{x : x \in A \vee x \in B\}$
- **intersection:** $A \cap B = \{x : x \in A \wedge x \in B\}$
- **complement** (of B in A): $A \backslash B = \{x : x \in A \wedge x \notin B\}$
- **complement** (of B): $\bar{B}$ or $B^c = U \backslash B$
  - set difference law: $A \backslash B = A \cap \bar{B}$

ordered pairs and cartesian products

- **ordered pair** : (x, y)
  - $(x, y) = (x', y') \leftrightarrow x = x'$ and $y = y'$
- **Cartesian product** :
  $A \times B = \{(x, y) : x \in A$ and $x \in B\}$
  - $|A \times B| = |A| \times |B|$
- **ordered tuples** : expression of the form $(x_1, x_2, \ldots, x_n)$

06. FUNCTIONS

definitions

- **function/map** from A to B : assignment of each element of A to exactly one element of B.
  - $f : A \rightarrow B$: "f is a function from A to B"
  - $f : x \rightarrow y$: "f maps x to y"
  - **domain** of f = A
  - **codomain** of f = B
  - **range/image** of f = $\{f(x) : x \in A\}$
    $= \{y \in B \mid y = f(x)$ for some $x \in A\}$
- **identity function** on A, $\text{id}_A : A \rightarrow A$
  - $\text{id}_A : x \rightarrow x$
  - range = domain = codomain = A
- **well-defined function** : every element in the domain is assigned to exactly one element in the codomain

equality of functions

- same codomain and domain
- for all $x \in$ codomain, same output

function composition

- $(g \circ f)(x) = g(f(x))$
- for $(g \circ f)$ to be well defined, codomain of f must be equal to the domain of g
- $\times$ commutative
- $\checkmark$ associative

image & pre-image

for $f : A \rightarrow B$
- if $X \subseteq A$, **image** of X,
  $f(X) = \{y \in B : y = f(x)$ for some $x \in X\}$
- if $Y \subseteq B$, **pre-image** of X,
  $f^{-1}(Y) = \{x \in A : y = f(x)$ for some $y \in Y\}$

injection & surjection

- **surjective** : codomain = range
  - $\forall y \in B, \exists x \in A \ (y = f(x))$
- **injective** : one-to-one
  - $\forall x, x' \in A(f(x) = f(x') \Rightarrow x = x')$
- **bijective** : both surjective & injective
  - has an inverse

inverse

- $\forall x \in A, \forall y \in B(f(x) = y \Leftrightarrow g(y) = x)$

07. INDUCTION

mathematical induction

to prove that $\forall n \in \mathbb{Z}_{\geq m}(P(n))$ is true,
- base step: show that $P(m)$ is true
- induction step: show that $\forall k \in \mathbb{Z}_{\geq m}(P(k) \Rightarrow P(k+1))$ is true.
  - induction hypothesis: assumption that $P(k)$ is true

strong MI

to prove that $\forall n \in \mathbb{Z}_{\geq 0}(P(n))$ is true,
- base step: show that $P(0), P(1)$ are true
- induction step: show that
  $\forall k \in \mathbb{Z}_{\geq 0}(P(0) \cdots \wedge P(k+1) \Rightarrow P(k+2))$ is true.
justification:
- $P(0) \wedge P(1)$ by base case
- $P(0) \wedge P(1) \rightarrow P(2)$ by induction with $k = 0$
- $P(0) \wedge P(1) \wedge P(2) \rightarrow P(3)$ by induction with $k = 1$
- $\cdots$
- we deduce that $P(0), P(1), \ldots$ are all true by a series of **modus ponens**

well-ordering principle

- every nonempty subset of $\mathbb{Z}_{\geq 0}$ has a smallest element.
- application: recursion has a base case

RECURSION

a sequence is **recursively defined** if the definition of a_n involves $a_0, a_1, \ldots, a_{n-1}$ for all but finitely many $n \in \mathbb{Z}_{\geq 0}$.

recursive definitions

e.g. recursive definition for $\mathbb{Z}$
1. (**base clause**) $0 \in \mathbb{Z}_{\geq 0}$
2. (**recursion clause**) If $x \in \mathbb{Z}_{\geq 0}$, then $x + 1 \in \mathbb{Z}_{\geq 0}$
3. (**minimality clause**) Membership for $\mathbb{Z}_{\geq 0}$ can be demonstrated by (finitely many) successive applications of the clauses above

recursion vs induction

- **recursion** - to define the set
- **induction** - to show things about the set

well-formed formulas (WFF)

in propositional logic

define the set of WFF(Σ) as follows
1. (base clause) every element ρ of Σ is in WFF(Σ)
2. (recursion clause) if x, y are in WFF(Σ), then $\sim x$ and $(x \wedge y)$ and $(x \vee y)$ are in WFF(Σ)
3. (minimality clause) Membership for WFF(Σ) can be demonstrated by (finitely many) successive applications of the clauses above

LOGICAL EQUIVALENCES

commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
distributive laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
identity laws	$p \wedge true \equiv p$	$p \vee false \equiv p$
idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
universal bound laws	$p \vee true \equiv true$	$p \wedge false \equiv false$
negation laws	$p \vee \sim p \equiv true$	$p \wedge \sim p \equiv false$
double negation law	$\sim(\sim p) \equiv p$	—
absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
De Morgan's Laws	$\sim(p \vee q) \equiv \sim p \wedge \sim q$	$\sim(p \wedge q) \equiv \sim p \vee \sim q$

SET IDENTITIES

commutative laws	$A \cap B = B \cap A$	$A \cup B = B \cup A$
associative laws	$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$
distributive laws	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
identity laws	$A \cap U = A$	$A \cup \emptyset = A$
idempotent laws	$A \cap A = A$	$A \cup A = A$
universal bound laws	$A \cap \emptyset = \emptyset$	$A \cup U = U$
complement laws	$A \cap \overline{A} = \emptyset$	$A \cup \overline{A} = U$
double **complement** law	$\overline{(\overline{A})} = A$	—
absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
De Morgan's Laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$

....

proven:

- L1E1 - the product of 2 consecutive odd numbers is always odd.
- L1E5 - the difference between 2 consecutive squares is always odd
- L4E4 - the sum of any 2 even integers is even
- L4T4.6.1 - there is no greatest integer
- L4T4.3.1 - for all positive integers a and b, if $a|b$, then $a \leq b$.
- L1P4.6.4 - for all integers n, if n^2 is even then n is even
- L4T4.2.1 - all integers are rational numbers
- L4T4.2.2 - the sum of any 2 rational numbers is rational
- L1E7 - there exist irrational numbers p and q such that p^q is rational
- L4T4.7.1 - $\sqrt{2}$ is irrational.
- L4T4.3.2 - the only divisors of 1 are 1 and -1.
- L4T4.3.3 - **transitivity of divisibility**
    - if $a|b$ and $b|c$, then $a|c$.
- L3T3.2.1 - **negation of a universal statement**:
    - $\sim(\forall x \in D, P(x)) \equiv \exists x \in D \mid \sim P(x)$
- L3T3.2.2 - **negation of an existential statement**:
    - $\sim(\exists x \in D \mid P(x)) \equiv \forall x \in D, \sim P(x)$
- L5T5.1.14 - there exists a unique set with no element. It is denoted by $\emptyset$.
- L5E5.3.7 - for all A, B: $(A \cap B) \cup (A \backslash B) = A$
- L5T5.3.11(1) - let A, B be disjoint finite sets. Then $|A \cup B| = |A| + |B|$
- L5T5.3.11(2) - let $A_1, A_2, \ldots, A_n$ be pairwise disjoint finite sets. Then $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$
- L5T5.3.12 - **Inclusion-Exclusion Principle**:
    - for all finite sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$
- L6T6.1.26 - **associativity of function composition**:
    - $f \circ (g \circ h) = (f \circ g) \circ h$
- L6P2.6.16 - **uniqueness of inverses**:
    - If g, g' are inverses of $f : A \rightarrow B$, then $g = g'$.
- L6E6.1.24 - $f \circ \text{id}_A = f$ and $\text{id}_A \circ f = f$
- L6T6.2.18 - bijective $\Leftrightarrow$ has an inverse
- L7L7.3.19 - If $x \in \text{WFF}^+(\Sigma)$, then assigning false to all elements of Σ makes x evaluate to false.
- L7T7.3.20 - $\sim(\forall x \in \text{WFF}(\Sigma), \exists y \in \text{WFF}^+(\Sigma) \; y \equiv x) \equiv \exists x \in \text{WFF}(\Sigma) \; \forall y \in \text{WFF}^+(\Sigma) \; y \not\equiv x$ aka $\sim$ (not) must be included in the definition of WFF.

abbreviations

- L - lecture
- L - lemma
- E - example
- P - proposition
- T - theorem