

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

$$n \text{ is even} \leftrightarrow \exists k \in \mathbb{Z} \mid n = 2k$$

$$n \text{ is odd} \leftrightarrow \exists k \in \mathbb{Z} \mid n = 2k + 1$$

prime/composite

$$n \text{ is prime} \leftrightarrow n > 1 \text{ and } \forall r, s \in \mathbb{Z}^+, n = rs \rightarrow (r = n) \vee (s = n)$$

$$n \text{ is composite} \leftrightarrow n > 1 \text{ and } \exists r, s \in \mathbb{Z}^+ s.t. n =$$

$$rs \text{ and } 1 < r < n \text{ and } 1 < s < n$$

divisibility (d divides n)

$$d \mid n \leftrightarrow \exists k \in \mathbb{Z} \mid n = kd$$

rationality

$$r \text{ is rational} \leftrightarrow \exists a, b \in \mathbb{Z} \mid r = \frac{a}{b} \text{ and } b \neq 0$$

floor/ceiling

$$\lfloor x \rfloor : \text{largest integer } y \text{ such that } y \leq x$$

$$\lceil x \rceil : \text{smallest integer } y \text{ such that } y \geq x$$

rules of inference

generalisation

$$p, \therefore p \vee q$$

specialisation

$$p \wedge q, \therefore p$$

elimination

$$p \vee q; \sim q, \therefore p$$

transitivity

$$p \rightarrow q; q \rightarrow r; \therefore p \rightarrow r$$

04. METHODS OF PROOF

Proof by Exhaustion/Cases

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

Proof by Contradiction

- Suppose that ...
 - <proof>
 - ...but this contradicts ...
- Therefore the assumption that ... is false.
Hence

Proof by Contraposition

- Contrapositive statement: $\sim q \rightarrow \sim p$
- let $\sim q$
 - <proof>
 - hence $\sim p$
- $\therefore p \rightarrow q$

Proof by Construction

- Let $x = 3, y = 4, z = 5$.
- Then $x, y, z \in \mathbb{Z}_{\geq 1}$ and $x^2 + y^2 = 3^2 + 4^2 = 9 + 16 = 25 = 5^2$.
- Thus $\exists x, y, z \in \mathbb{Z}_{\geq 1}$ such that $x^2 + y^2 = z^2$.

Proof by Induction

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

Proofs for Sets

Equality of Sets (A=B)

- (\Rightarrow)
 - Take any $z \in A$.
 - ...
 - $\therefore z \in B$.
- (\Leftarrow)
 - Take any $z \in B$.
 - ...
 - $\therefore z \in A$.

Element Method

- $A \cap (B \setminus C) = \{x : x \in A \wedge x \in (B \setminus C)\}$ (by def. of \cap)
- $= \{x : x \in A \wedge (x \in B \wedge x \notin C)\}$ (by def. of \setminus)
- ...
- $= (A \cap B) \setminus C$ (by def. of \setminus)

Other Proofs

iff ($A \leftrightarrow B$)

- (\Rightarrow) Suppose A .
 - ... <proof> ...
 - Hence $A \rightarrow B$
- (\Leftarrow) Suppose B .
 - ... <proof> ...
 - Hence $B \rightarrow A$

02. COMPOUND STATEMENTS

operations

- \sim : negation (not)
- \wedge : conjunction (and)
- \vee : disjunction (or) - coequal to \wedge
- \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

- vacuously true** : hypothesis is false
- implication law** : $p \rightarrow q \equiv \sim p \vee q$
- common if/then statements:
 - if p then q: $p \rightarrow q$
 - p if q: $q \rightarrow p$
 - p only if q: $p \rightarrow q$
 - p iff q: $p \leftrightarrow q$

- contrapositive** : $\sim q \rightarrow \sim p$
- inverse** : $\sim p \rightarrow \sim q$
- converse** : $q \rightarrow p$

converse \equiv inverse
statement \equiv contra-
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
- sylogism** : (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

$$p \rightarrow q$$

$$q$$

$$\therefore p$$

inverse error

$$p \rightarrow q$$

$$\sim p$$

$$\therefore \sim q$$

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 $\forall, \exists, \wedge, \vee$

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

05. SETS

notation

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

definitions

- equal sets** : $A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$
 - $A = B \leftrightarrow (A \subseteq B) \wedge (A \supseteq B)$
- 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, $|A|$: 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): $A \setminus B = \{x : x \in A \wedge x \notin B\}$
- complement** (of B): \bar{B} or $B^c = \mathbb{U} \setminus B$
 - set difference law: $A \setminus B = A \cap \bar{B}$

ordered pairs and cartesian products

- ordered pair** : (x, y)
 - $(x, y) = (x', y') \leftrightarrow x = x' \text{ and } y = y'$
- Cartesian product** :
 $A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$
 - $|A \times B| = |A| \times |B|$
- ordered tuples** : expression of the form (x_1, x_2, \dots, 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 $f = \{f(x) : x \in A\}$
 $= \{y \in B \mid y = f(x) \text{ for some } x \in A\}$
- 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,
 $f(X) = \{y \in B : y = f(x) \text{ for some } x \in X\}$
 - if $Y \subseteq B$, **pre-image** of Y,
 $f^{-1}(Y) = \{x \in A : y = f(x) \text{ for some } y \in Y\}$

injection & surjection

- **surjective** (onto) : codomain = range
 - $\forall y \in B, \exists x \in A (y = f(x))$
 - surjective test: $\forall Y \subseteq B, Y \subseteq f(f^{-1}(Y))$
- **injective** : one-to-one
 - $\forall x, x' \in A (f(x) = f(x') \Rightarrow x = x')$
 - injective test: $\forall X \subseteq A, X \subseteq f^{-1}(f(X))$
- **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 $k = 1$
 - \dots
 - we deduce that $P(0), P(1), \dots$ 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, \dots, 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

08. NUMBER THEORY

divisibility

- $n \bmod d$ is always non-negative.
- transitivity of divisibility
If $a \mid b$ and $b \mid c$, then $a \mid c$.
- closure lemma (non-standard name)
Let $a, b, d, m, n \in \mathbb{Z}$. If $d \mid m$ and $d \mid n$, then $d \mid am + bn$.
- division theorem
 $\forall n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+, \exists !q, r \in \mathbb{Z}$ s.t.
 $n = dq + r$ and $0 \leq r < d$
 $q = n \operatorname{div} d = \lfloor n/d \rfloor$
 $r = n \operatorname{mod} d = n - dq$

base-b representation

- of positive integer n is $(a_\ell a_{\ell-1} \dots a_0)_b$
where $\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \dots, a_\ell \in \{0, 1, \dots, b - 1\}$
s.t. $n = a_\ell b^\ell + a_{\ell-1} b^{\ell-1} + \dots + a_0 b^0$ and $a_\ell \neq 0$

greatest common divisor

- $m \operatorname{mod} n$
- if $m \neq 0$ and $n \neq 0$, then gcd(m, n) exists and is positive.
- **Euclidean Algorithm** for finding gcd

- Bezout's Lemma:
For all $m, n \in \mathbb{Z}$ with $n \neq 0$, there exist $s, t \in \mathbb{Z}$ such that $\textcolor{teal}{gcd(m, n)} = ms + nt$.
- Euclid's Lemma:
Let $m, n \in \mathbb{Z}^+$. If p is prime and $p \mid mn$, then $p \mid m$ or $p \mid n$.

prime factorization

- **Fundamental Theorem of Arithmetic**: Every integer $n \geq 2$ has a unique prime factorization in which the prime factors are arranged in nondecreasing order.
 - aka Prime Factorisation Theorem

modular arithmetic

- Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$.
- congruence
 $a \equiv b \pmod n \Leftrightarrow a \operatorname{mod} n = b \operatorname{mod} n$
Then $\exists k \in \mathbb{Z} \mid a = nk + b$ and $n \mid (a - b)$
- reflexivity
 $a \equiv a \pmod n$
- symmetry
 $a \equiv b \pmod n \rightarrow b \equiv a \pmod n$
- transitivity
 $a \equiv b \pmod n \wedge b \equiv c \pmod n \rightarrow a \equiv c \pmod n$

additive inverse

- b is an *additive inverse* of $a \operatorname{mod} n \Leftrightarrow a + b \equiv 0 \pmod n$.
- b is an *additive inverse* of $a \operatorname{mod} n \Leftrightarrow b \equiv -a \pmod n$.

multiplicative inverse

- b is a multiplicative inverse of $a \operatorname{mod} n \Leftrightarrow ab \equiv 1 \pmod n$.
- If b, b' are multiplicative inverses of a , then $b \equiv b' \pmod n$.
- exists $\Leftrightarrow \gcd(a, n) = 1$.
 - a, n are coprime
- to find multiplicative inverse: **Euclidean Algorithm**

LOGICAL EQUIVALENCES			SET IDENTITIES		
commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$	commutative laws	$A \cap B = B \cap A$	$A \cup B = B \cup A$
associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	associative laws	$(A \cap B) \cap C = A \cap (B \cap C)$	$(A \cup B) \cup C = A \cup (B \cup C)$
distributive laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	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	$p \wedge \text{true} \equiv p$	$p \vee \text{false} \equiv p$	identity laws	$A \cap U = A$	$A \cup \emptyset = A$
idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$	idempotent laws	$A \cap A = A$	$A \cup A = A$
universal bound laws	$p \vee \text{true} \equiv \text{true}$	$p \wedge \text{false} \equiv \text{false}$	universal bound laws	$A \cap \emptyset = \emptyset$	$A \cup U = U$
negation laws	$p \vee \sim p \equiv \text{true}$	$p \wedge \sim p \equiv \text{false}$	complement laws	$A \cap \overline{A} = \emptyset$	$A \cup \overline{A} = U$
double negation law	$\sim(\sim p) \equiv p$	—	double complement law	$\overline{(\overline{A})} = A$	—
absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$	absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
De Morgan's Laws	$\sim(p \vee q) \equiv \sim p \wedge \sim q$	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	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 : $(A \cap B) \cup (A \setminus B) = A$
- 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, \dots, A_n be pairwise disjoint finite sets. Then $|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|$
- 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 $g = g'$.
- E6.1.24 - $f \circ \text{id}_A = f$ and $\text{id}_A \circ f = f$
- T6.2.18 - bijective \Leftrightarrow has an inverse
- L7.3.19 - If $x \in \text{WFF}^+(\Sigma)$, then assigning false to all elements of Σ makes x evaluate to false.
- T7.3.20 - $\sim(\forall x \in \text{WFF}(\Sigma), \exists y \in \text{WFF}^+(\Sigma) \ y \equiv x) \equiv \exists x \in \text{WFF}(\Sigma) \ \forall y \in \text{WFF}^+(\Sigma) \ y \not\equiv x$ aka \sim (not) must be included in the definition of WFF.
- L8.1.5 - Let $d, n \in \mathbb{Z}$ with $d \neq 0$. Then $d \mid n \Leftrightarrow n/d \in \mathbb{Z}$
- L8.1.9 - Let $d, n \in \mathbb{Z}$. If $d \mid n$, then $-d \mid n$ and $d \mid -n$ and $-d \mid -n$
- L8.1.10 - Let $d, n \in \mathbb{Z}$. If $d \mid n$ and $d \neq 0$, then $|d| \leq |n|$
- L8.2.5 - **Prime Divisor Lemma** (non-standard name):
 - Let $n \in \mathbb{Z}_{\geq 2}$. Then n has a prime divisor.
- P8.2.6 - **sizes of prime divisors:**
 - Let n be a composite positive integer. Then n has a prime divisor $p \leq \sqrt{n}$.
- T8.2.8 - there are infinitely many prime numbers
- T8.3.13 - $\forall n \in \mathbb{Z}^+, \exists !\ell \in \mathbb{Z}_{\geq 0}$ and $a_0, a_1, \dots, a_\ell \in \{0, 1, \dots, b - 1\}$ such that \langle the definition of base- b representation \rangle holds.

- L8.4.11 - If $x, y, r \in \mathbb{Z}$ such that $x \bmod y = r$, then $\gcd(x, y) = \gcd(y, r)$.
- Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$ s.t. $a \equiv b \pmod n$ and $c \equiv d \pmod n$.
 - P8.6.6 - **addition:** Then $a + c \equiv b + d \pmod n$
 - P8.6.13 - **multiplication:** Then $ac \equiv bd \pmod n$

abbreviations

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