CS1231 - 1 - Logic

1 Proofs

- Direct
- Equivalence (contrapositive, $\neg p \Rightarrow \neg q, p \Rightarrow q$)
- Exhaustion (by cases)
- Construction
- Counter Example
- Contradiction
- Contrapositive
- Induction (Base case, induction hypothesis)
- Combinatorial

2 Propositional Logic

- Negation ($\neg$)
- Conjunction/And ($\wedge$)
- Disjunction/Or ($\vee$)
- Exclusive disjunction/XOR ($\bigoplus$)
- Conditional/If-Then/Implies ($\Rightarrow$)
  - $p \Rightarrow q$
    - p - premise
    - q - consequence
  - Converse (of $p \Rightarrow q$ is $q \Rightarrow p$)
  - Contrapositive (of $p \Rightarrow q$ is $\neg p \Rightarrow \neg q$)

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

- Bi-conditional ($\Leftrightarrow$)

p	q	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

- True ($\top$)
- False ($\bot$)

2.1 Precedence (High to low)

$\neg \quad \oplus \quad \vee \quad \wedge \quad \Rightarrow \quad \Leftrightarrow$

2.2 Demorgan's law (Negation of AND/OR)

$(p \vee q) \equiv \ p \wedge \ q, \qquad (p \wedge q) \equiv \ p \vee \ q$

p	q	$\neg p$	$\neg q$	$p \vee q$	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p \vee \neg q$
0	0	1	1	0	1	1	0	1	1
0	1	1	0	1	0	0	0	1	1
1	0	0	1	1	0	0	0	1	1
1	1	0	0	1	0	0	1	0	1

3 Predicate Logic

`odd(n)` $\Rightarrow$ n is odd

`odd('×'('+'(3, 2), 5))` $\Rightarrow$ $(3+2) \times 5$ is odd

3.1 Quantifiers

$\forall$	For all
$\exists$	There exists

$F[t/X] \Rightarrow$ is Formula, F, where we substitude X with t

4 Post Systems

- Alphabet/symbols $\rightarrow$ words
- Axioms: collection of words
- Inferance rules: $P_1, ..., P_n \vdash P_{n+1}$, where P_i are word patterns containing variables
- $A \vdash B$: A proves B

Example:

Given:

- Alphabet: A, B, C
- Axioms: A, BC
- Rules: $BX \vdash XX$, $A, XX \vdash XBA$

Prove CBA

- BC (Axiom)
- CC ($BX \vdash XX$)
- A, Axiom
- $A, CC \vdash CBA$
- CBA

Assume BB. Then prove BABA

- BB (Assumption)
  - A (Axiom)
  - $A, BB \vdash BBA(A, XX \vdash XBA)$
  - $BBA \vdash BABA(BX \vdash XX)$

Consider discharge rule $(XX \vdash XAXA) \vdash XA$

- ... continue from above ... $BB \vdash BABA$
- $(BB \vdash BABA) \vdash BA((XX \vdash XAXA) \vdash XA)$

5 Natural Deduction

- $A, B \vdash A \wedge B$ (Conjuction introducation)
- $(A \wedge B) \vdash A$, $(A \wedge B) \vdash B$ (Conjunction elimination)
- $A \vdash (A \vee B)$, $B \vdash (A \vee B)$ (Disjuction introduction)

- $(A \Rightarrow X, B \Rightarrow X, A \vee B) \vdash X$ (Disjunction elimination)
- $\neg\neg A = A$ (Double negation)
- $(A \Rightarrow (B \wedge \neg B)) \vdash \neg A$ (Negation introduction)
- $(A \vdash B) \vdash (A \Rightarrow B)$ (Implication introduction)

5.1 Others

$(A \wedge B) \vdash (B \wedge A)$**, Conjunction Commutativity**

1. $A \wedge B$ (Premise)
2. A $(A \wedge B \vdash A)$
3. B $(A \wedge B \vdash B)$
4. $B \vdash A$ $(B, A \vdash B \wedge A)$

$A \vdash \neg\neg A$**, Double negation introduction**

1. F_1, (premise)
2. Assume $\neg F_1$
   (a) $F_1 \wedge \neg F_1$, (conjuction introduction with 1 & 2)
3. $\neg F_1 \Rightarrow F_1 \wedge \neg F_1$, (implication introduction of 2 & 2.1)
4. $\neg\neg F_1$, (negation introduction with 3)

$F_1, \neg F_1 \vdash F_2$**, Negation elimination**

$F_1, F_1 \Rightarrow F_2 \vdash F_2$**, Implication Elimination/Modus Ponens**

1. F_1, (premise)
2. $F_1 \Rightarrow F_2$, (premise)
3. $F_1 \vee F_1$, (disjunction introduction with 1 & 1)
4. F_2 by disjunction elimination with 3, 2, 2

6 Propositional Calculus

- Interpretation (I) is mapping of propositions to truth values
  - **Logical Consequence** ($vDash$)

7 Boolean Algebra

- **Identity of** $\times$: $x \times 1 - x$
- **Identity of plus**: $x + 0 = x$
- **Complementation of** $\times$: $x \times \overline{x} = 0$
- **Complementation of** $+$: $x + \overline{x} = 1$
- **Associativity of** $\times$: $x \times (y \times z) = (x \times y) \times z$
- **Associativity of** $+$: $x + (y + z) = (x + y) + z$
- **Commutativity of** $\times$: $x \times y = y \times z$
- **Commutativity of** $+$: $x + y = y + z$
- **Distributivity of** $\times$ **over** $+$: $x \times (y + z) = (x \times y) + (x \times z)$
- **Distributivity of** $+$ **over** $\times$: $x + (y \times z) = (x + y) \times (x + z)$
- **Idempotence of** $\times$: $x \times x = x$
- **Idempotence of** $+$: $x + x = x$
- **Annihilator of** $\times$: $x \times 0 = 0$
- **Annihilator of** $+$: $x + 1 = 1$
- **Absorbsion of** $\times$: $x \times (x + y) = x$
- **Absorption of** $+$: $x + (x \times y) = x$
- **Double negation**: $\overline{\overline{x}} = x$
- **De Morgan's Law for** $\times$: $\overline{x \times y} = \overline{x} + \overline{y}$
- **De Morgan's Law for** $+$: $\overline{x + y} = \overline{x} \times \overline{y}$

CS1231 - Sets

1 Terminology

- $\in$: Membership
- $\subset$: Includes

2 Axiomatic Set Theory

2.1 Empty Set ($\varnothing$ or)

Set with no elements

$\underbrace{\exists X}_{\text{empty set}} \underbrace{(\forall Y (Y \notin X))}_{\text{no elements in set}}$

2.2 Empty set is a subset of all sets

$\underbrace{\forall X}_{\text{empty set}} \underbrace{\forall Z}_{\text{any set}} (\underbrace{\forall Y (Y \notin X)}_{\text{empty set}} \Rightarrow \underbrace{(X \subset Z)}_{\text{subset of any set}})$

2.3 Extensionality/Equality

Sets are equal iff the have the same elements

$\forall X \forall Y (\underbrace{(\forall Z (Z \in X \Leftrightarrow Z \in Y))}_{\text{same elements}} \Leftrightarrow X = Y)$

$\forall X \forall Y (\underbrace{(X \subset Y \wedge Y \subset X)}_{\text{subsets of each other}} \Leftrightarrow X = Y)$

2.4 Pairing

A set (Z) that contains sets X & Y exists

$\forall X \forall Y \exists Z \underbrace{\forall T ((T = X \vee T = Y)}_{\text{T is either in X or Y}} \Leftrightarrow T \in Z)$

2.5 Unordered Pair

Pair of 2 sets eg. $\{X, Y\}$ is the set that contains X & Y

2.6 Singleton

Set $\{X, X\} = \{X\}$ is called a singleton

2.7 Unions

If S is a set of sets, the T (the union) exists which contains all elements in a set in S

$\forall S \exists T \underbrace{\forall Y((Y \in T)}_{\text{all elems in union}} \Leftrightarrow \underbrace{\exists Z((Z \in S)}_{\text{one of the sets}} \wedge \underbrace{(Y \in Z)}_{\text{y is in one of the sets}}))$

2.8 Power Set ($\mathcal{P}(S)$)

All possible subsets of set

$\forall S \underbrace{\exists T}_{\text{a possible subset}} \underbrace{\forall X((X \in T)}_{\text{all elem of possible subset}} \underbrace{\Leftrightarrow (X \subset S)}_{\text{x an elem of the set}})$

Examples:

$\mathcal{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$

2.9 Regularity/Axiom of Foundation

Every non empty set has an element disjoint from the set. Also see math.stackexchange question

$\forall X(X \neq \varnothing \Rightarrow (\exists Y(Y \in X \wedge \forall Z(Z \in X \Rightarrow Z \notin Y))))$

Remember: everything is a set so ...

$0 = \varnothing$

$1 = \{0\}$

$2 = \{0, 1\}$

$3 = \{0, 1, 2\}$

$4 = \{0, 1, 2, 3\}$ ...

So 4 has 3 which is not in 2

2.9.1 No set is a member of itself

$\forall X(X \notin X)$

2.10 Infinity Set

$\exists X(\varnothing \in X \wedge (\forall Y(Y \in X \Rightarrow Y \cup Y \in X)))$

Example: $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, ...\}$

2.11 Separation

Given a set (X), selecting elements that satisfy a property (p) produces a set (Y)
$\forall X \exists Y \forall Z(Z \in Y \Leftrightarrow (Z \in X \wedge p(x)))$

3 Set Operations

3.1 Intersection $(\bigcap S)$

Let S be a set of sets. The intersection of sets in S is the set T that contains elements that belong to all the sets in S
$\forall S \exists T \forall Y((Y \in T) \Leftrightarrow \forall Z((Z \in S) \Rightarrow (Y \in Z)))$

- $A \cap \varnothing = \varnothing$
- $A \cap B = B \cap A$
- $A \cap (B \cap C) = (A \cap B) \cap C$
- $A \subset B \Leftrightarrow A \cap B = A$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

3.2 Disjoint

2 sets are disjoint iff $S \cap T = \varnothing$

3.2.1 Mutally Disjoint

Let S be a set of sets. All sets $T \in S$ are disjoint if every 2 different sets are disjoint. "Theres no intersection between sets"
$\forall X \in S \forall Y \in S(X \neq Y \Rightarrow X \cap Y = \varnothing)$

3.2.2 Partition

Let S be a set, V be a set of non-empty subsets in S. Then V is a partition of S iff

- Sets V are mutually disjoint
- Union of sets in V equals S

3.3 Difference

3.3.1 Non Symmetric (\)

$A \backslash B$

"In A, not in B"

Complement

$\overline{T}^S$ is the complement of T in S $(S \backslash T)$

$\forall X (X \in A \backslash B \Leftrightarrow (X \in A \wedge X \notin B))$

3.3.2 Symetric Difference ($-$)

"Elements that belong in one of the sets but not both"

$\forall X (X \in (A - B) \Leftrightarrow (X \in A) \oplus X \in T)$

- $\oplus$: XOR

Relations

1 Basics

1.1 Ordered Pair

$A \times B = < a, b > |a \in A \wedge b \in B$

$< x, y >$

1.2 Cartesian Product ($A \times B$)

$\forall X \forall Y (< X, Y > \in (A \times B) \Leftrightarrow (X \in A) \wedge (Y \in B))$

1.2.1 Generalized

Let V be set of sets, generalized cartesian product is:

$\prod\limits_{S \in V} S = S_1 \times S_2 ... \times S_n = < s_1, s_2, ..., s_n >$

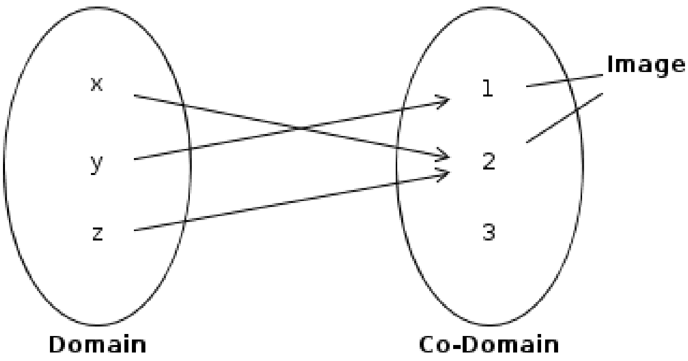
1.3 Tuples

$< X_1, X_2, ..., X_n >$

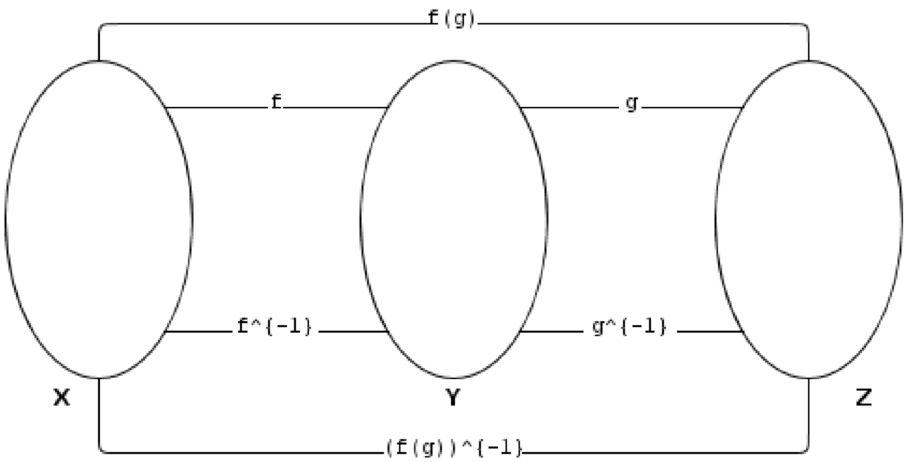
2 Relations

A binary relation from A to B noted $\mathcal{R}$ is a subset of $A \times B$

- $a\mathcal{R}b \quad \Rightarrow \quad < a, b > \in \mathcal{R}$
- **Domain ("the X")**: $\mathcal{D}om(\mathcal{R}) = \{s \in S | \exists t \in T(s\mathcal{R}t)\}$
- **Image ("the actual Y")**: $\mathcal{I}m(\mathcal{R}) = \{t \in T | \exists s \in S(s\mathcal{R}t)\}$
- **Co-domain/Range ("all possible Y")**: $co\mathcal{D}om(\mathcal{R}) = T$



- **Inverse/Converse**: $\forall s \in S \forall t \in T(s\mathcal{R}^{-1}t \Leftrightarrow t\mathcal{R}s)$
- **Composition**: $(g \circ f) = f(g(x))$
  - **Associative**: $h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f$
  - $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$



3 Properties

3.1 Reflexive

All elements have a self loop. $\forall x \in A(x \, \mathcal{R} \, x)$

3.2 Symmetric

Every relation is bi-directional. $\forall x, y \in A(x \, \mathcal{R} \, y \Rightarrow y \, \mathcal{R} \, x)$

3.3 Transitive

If theres a relation from X to Y and Y to Z, then theres also a relation from X to Z (Triangle). $\forall x, y, z \in A((x \, \mathcal{R} \, y \wedge y \, \mathcal{R} \, z) \Rightarrow x \, \mathcal{R} \, z)$

4 Equivalence Relation

iff relation is reflexive, symetric, transitive

4.1 Equivalance Class

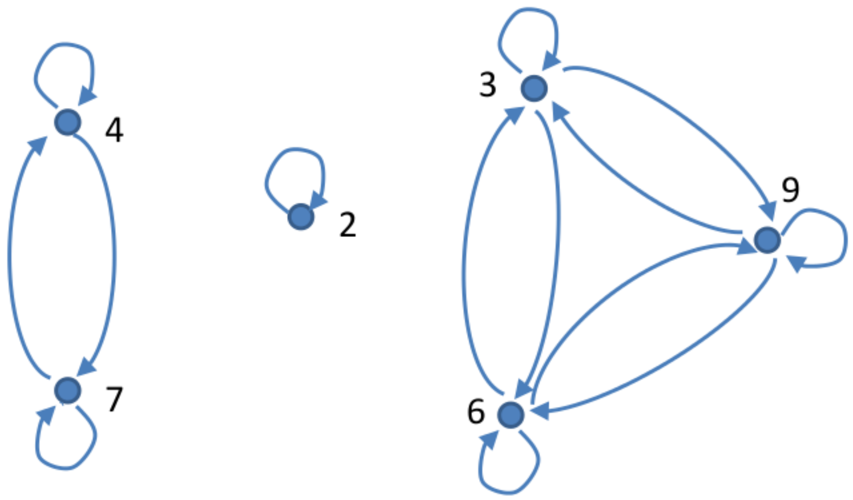
Sets resulting from equivalence relation

$E_x^{\mathcal{R}} = \{y \in A | x\mathcal{R}y\}$

4.2 Set of Equivalance Classes

$A/\mathcal{R} = \{s \in \mathcal{P}(A) | \exists x \in A(s = E_x^{\mathcal{R}})\}$

Example:



$$
\begin{aligned}
A/\mathcal{R} &= \{E_2^{\mathcal{R}}, E_3^{\mathcal{R}}, E_4^{\mathcal{R}}\} && (1)\\
&= \{\{2\}, \{3,6,9\}, \{4,7\}\} && (2)
\end{aligned}
$$

5 Congruence modulo n

$\forall x, y \in \mathbb{Z}(x\mathcal{R}y \Leftrightarrow n\backslash(x-y))$

Where $n\backslash m$ means n divides m. Or $\exists k \in \mathbb{Z}, m = kn$

Proof

1. Reflexive: $\forall x \in \mathbb{Z}, n\backslash(x-x)$
2. Symmetric: $\forall x, y \in \mathbb{Z}$ if $n\backslash(x-y)$ then $n\backslash(y-x)$
3. Transitive:

(a) Given any $x, y, z \in \mathbb{Z}$ if $n \backslash (x-y)$ and $n \backslash (y-z)$, then $\exists k_1, k_2 \in \mathbb{Z}$ such that $x - y = k_1 n$ and $y - z = k_2 n$

(b) Thus $(x-y)+(y-z) = k_1 n + k_2 n$ which simplifies to $x - z = (k_1 + k_2)n$. This means $n \backslash (x-z)$

4. Hence, this is an equivalence relation

5.1 Partition induced by equivalence relation

Let $\mathcal{R}$ be equivalence relation, then $A \backslash \mathcal{R}$ is a partition of A

<u>Proof</u>:

1. 2 related elements are in same equivalence class
   (a) Assuming that $a \in E_b$ leads to $E_a \subset E_b$ and $E_b = E_a$, thus equals
   (b) Let $a, b \in A$, suppose $a \in E_b$
   (c) $b\mathcal{R}a$ by dfn equivalence class
   (d) Let c be any element in E_a
   (e) $a\mathcal{R}c$
   (f) $b\mathcal{R}c$ by transitivity from (c). Thus $c \in E_b$. Then $E_a \subset E_b$
   (g) Let d be any element in E_b
   (h) $b\mathcal{R}d$
   (i) $d\mathcal{R}b$ by symmetry
   (j) $d\mathcal{R}a$ by (c) and symmetry
   (k) $d \in E_a$. Thus $E_b \subset E_a$
   (l) $E_a \subset E_b \wedge E_b \subset E_a$ thus $E_a = E_b$
2. 2 equivalence class are disjoint, or are equal
   (a) Since statement is in form $p \Rightarrow (q \vee r)$, we can proof $(p \wedge \neg q) \Rightarrow r$
   (b) $E_a \cap E_b \neq \varnothing$ (Premise)
   (c) $\exists x (x \in E_a \cap E_b)$
   (d) $\exists x (x \in E_a \wedge x \in E_b)$
   (e) $a\mathcal{R}x \wedge b\mathcal{R}x$
   (f) $x\mathcal{R}b$
   (g) $a\mathcal{R}b$
   (h) $E_a = E_b$
3. Union of all equivalence classes is A

(a) Proof $A = \bigcup_{S \in A \backslash \mathcal{R}} S$

i. Suppose x is any element of A

ii. $x \mathcal{R} x$

iii. $x \in E_x$

iv. $E_x \in A \backslash \mathcal{R}$

v. $x \in \bigcup_{S \in A \backslash \mathcal{R}} S$

vi. So $A \subset \bigcup_{S \in A \backslash \mathcal{R}} S$

vii. Suppose x is any element in $\bigcup_{S \in A \backslash \mathcal{R}} S$

viii. $\exists S \in A \backslash \mathcal{R}(x \in S)$ (x must belong in some S)

ix. $\exists y \in A(S \in E_y)$ (S is an equivalence class of some y

x. $E_y \subset A$

xi. $x \in E_y \Rightarrow x \in A$

xii. Thus $\bigcup_{S \in A \backslash \mathcal{R}} S \subset A$

xiii. Hence equals

(b) Proof distinct equiv. class mutually disjoint

i. Suppose E_u amd E_v are 2 distinct equivalence class

ii. $\exists u, v \in A(u \in E_u \wedge v \in E_v)$

iii. Hence either $E_u \cap E_v = \varnothing$ or $E_u = E_v$

iv. Since $E_v \neq E_u$, we conclude $E_u \cap E_v = \varnothing$

5.2 (prop 5.4.2)

If $\mathcal{R}$ is an eqivalence relation on set A and a, b are 2 elements in A. If $a \mathcal{R} b$ then $E_a = E_b$

5.3 (prop 5.4.3)

If $\mathcal{R}$ is an equivalence relation on set A, and a, b are elements in A, then either $E_a \cap E_b = \varnothing$ or $E_a = E_b$

5.4 (prop 5.4.4)

Given partition of a set, there exists an equivalence relation whose equivalence classes make up the partition.

5.5 (dfn 5.5.1) Transitive closure

Transitive closure, denoted $\mathcal{R}^*$, is a relation that is:

- Transitive
- $\mathcal{R} \subset \mathcal{R}^*$
- If S is any other transitive relation such that $\mathcal{R} \subset S$, then $\mathcal{R}^* \subset S$

6 Partial & Total Orders

6.1 Anti-symmetric (dfn 5.6.1)

$$\forall x, y \in A\ (\underbrace{(x\mathcal{R}y \wedge y\mathcal{R}x)}_{\text{bi-directional arrow}} \Rightarrow \underbrace{x = y}_{\text{self-loop}})$$

6.2 Partial Order (dfn 5.6.2)

Partial order if its <u>reflexive, anti-symmetric and transitive</u>

6.3 Hasse Diagram

1. Draw directed graph with <u>arrows pointing upwards</u>
2. Eliminate all self loops
3. Eliminate all arrows implied by transitivity
4. Remove directions of arrows

6.4 Comparable

Let $\preceq$ be a partial order. a, b are comparable if either $a \preceq b$ or $b \preceq a$.

6.5 Total Order

If all elements are comparable

$$\forall x, y \in A\ (x \preceq y \vee y \preceq x)$$

6.6 Maximal

No (comparable) larger element

$$\forall y \in A\ (x \preceq y \Rightarrow x = y)$$

6.7 Maximum

Denoted $\top$. Only one

$$\forall x \in A \ (x \preceq \top)$$

6.8 Minimal

$$\forall y \in A \ (y \leq x \Rightarrow x = y)$$

6.9 Minimum

$$\forall x \in A \ (\bot \preceq x)$$

6.10 Well Ordered (dfn 5.6.9)

Well ordered if every non-empty subset contains a minimum element

$$\forall S \in \mathcal{P}(A) \ (S \neq \varnothing \Rightarrow (\exists x \in S \ \forall y \in S \ (x \preceq y)))$$

Functions

1 Function (dfn 6.1.1)

All elements of Domain can only have 1 outgoing arrow

$$\forall x \in S\ \exists y \in T\ (x\ f\ y \land (\forall z \in T\ (x\ f\ z \Rightarrow y = z)))$$

OR

$$\forall x \in S\ \exists! y \in T (x\ f\ y)$$

2 Injective

All elements in CoDomain have at most 1 incoming arrow

$$\forall y \in T\ \forall x_1, x_2 \in S\ ((f(x_1) = y) \land (f(x_2) = y)) \Rightarrow x_1 = x_2$$

3 Surjective

All elements in CoDomain have at least 1 incoming arrow

$$\forall y \in T\ \exists x \in S\ (f(x) = y)$$

4 Bijective

Injective & Surjective. All elements in Domain have exactly 1 image, same vice versa

- (prop 6.1.12) If f is bijective, f^{-1} is bijective

5 Composition

$$(g \circ f)(x) \Leftrightarrow g(f(x))$$

Number Theory (& Systems)

1 Number Theory

1.1 Natural Numbers ($\mathbb{N}$)

Smallest set such that

1. $\exists 0 (0 \in \mathbb{N})$
2. There exists a successor function s on $\mathbb{N}$. $s(n)$ (denoted n') is the successor of n. (Successor is $n+1$)
3. $\forall n \in \mathbb{N}(n' \neq 0)$
4. $\forall n, m \in \mathbb{N}(n' = m' \Rightarrow n = m)$
5. $\forall K \subset \mathbb{N} \forall n \in \mathbb{N}((0 \in K \wedge (n \in K \Rightarrow n' \in K)) \Rightarrow K = \mathbb{N})$

1.1.1 Less than equals ($\leq$)

$$\forall n, m \in \mathbb{N}_c(n \leq m \Leftrightarrow n \subset m)$$

($\mathbb{N}_c, \leq$) is a partial order

1. We prove $(\mathbb{N}_c, \leq)$ is a pre-order
   (a) $(\mathbb{N}_c, \leq)$ is reflexive by reflecivity of $\subset$
   (b) $(\mathbb{N}_c, \leq)$ is transitive by transitivity of $\subset$
   (c) Therefore a pre-order
2. $(\mathbb{N}_c, \leq)$ is anti-symmetric by anti-symmetry of $\subset$
3. Therefore a partial order

Ordering Lemma

$$n \leq m \vee m \leq n$$

($\mathbb{N}_c, \leq$) is a total order

1. We know $(\mathbb{N}_c, \leq)$ is a partial order
2. We know any 2 distinct elements in $\mathbb{N}_c$ are comparable by ordering lemma
3. Therefore total order

$(\mathbb{N}_c, \leq)$ is a well ordered

1. Sketch: prove every subset of $\mathbb{N}_c$ has a smallest element

1.1.2 Addition

- $\forall n \in \mathbb{N}(n + 0 = n)$
- $\forall n, m \in \mathbb{N}(n + m' = (n + m)')$

1.1.3 Multiplication

- $\forall n \in \mathbb{N}(n \times 0 = 0)$
- $\forall n, m \in \mathbb{N}(n \times m' = (n \times m) + n)$

1.2 Natural Numbers

Let $\approx$ be a relation on $\mathbb{N} \times \mathbb{N}$ such that

$$\forall n_1, n_2, m_1, m_2(< n_1, n_2 > \approx < m_1, m_2 > \Leftrightarrow n_2 + m_1 = m_2 + n_1)$$

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/ \approx$$

n if $< 0, n >$. $-n$ if $< n, 0 >$

1.2.1 Addition

$$< a_1, a_2 > + < b_1, b_2 > = < a_1 + b_1, a_2 + b_2 >$$

1.2.2 Subtraction

$$< a_1, a_2 > - < b_1, b_2 > = < a_1 + b_2, a_2 + b_1 >$$

1.2.3 Multiplication

$$< a_1, a_2 > \times < b_1, b_2 > = < (a_1 \times b_2) + (a_2 \times b_1), (a_1 \times b_1) + (a_2 \times b_2) >$$

1.3 Rational Numbers

$$\forall n_1, m_1 \in \mathbb{Z} \forall n_2, m_2 \in (\mathbb{Z} \backslash \{0\})$$

$$(< n_1, n_2 > \approx < m_1, m_2 > \Leftrightarrow n_2 \times m_1 = m_2 \times n_1)$$

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \backslash 0)) / \approx$$

1.3.1 Multiplication

$$a \times b = < a_1 \times b_1, a_2 \times b_2 > = \frac{a_1 \times b_1}{a_2 \times b_2}$$

1.3.2 Addition

$$a + b = < (a_1 \times b_2) + (b_1 \times b_2), a_2 \times b_2 >$$

1.3.3 Subtraction

$$a - b = < (a_1 \times b_2) - (b_2 \times a_2), a_2 \times b_2 >$$

2 Divisibility

m divides n, denoted $\boxed{\underbrace{m}_{\text{divisor}} \mid n}$

$\exists q \in \mathbb{N}(n = m \times q)$

2.1 Proposition 8.2.2

$$m \mid n \Rightarrow m \leq n$$

2.2 Proposition 8.2.3 - Remainder less than divisor

$$n \in \mathbb{N}\ m \in \mathbb{N}^+\ ((n = q \times m + r) \wedge (r < m))$$

2.3 Division Algorithm (Proposition 8.2.4)

$$n \in \mathbb{N}\ m \in \mathbb{N}^+\ \exists! q,\ r \in \mathbb{N}\ (n = q \times m + r \wedge r < m)$$

- n : dividend
- m : divisor
- r : remainder OR modulo m of n
- q : quotient

3 Co-prime

n and m are **relatively prime/co-prime**, denoted $\boxed{n \perp m}$ iff

$$\forall c \in \mathbb{N}^+ \; (((c|n) \land (c|m)) \Rightarrow c = 1)$$

4 Prime numbers

$$p > 1 \land (\forall n \in \mathbb{N}^+ \; (n \mid p \Rightarrow (n = p \lor n = 1)))$$

4.1 Composite (not prime)

$$\neg\text{prime}(n) \land n \neq 1$$

4.1.1 A composite number can be expressed as a multiple of 2 $\mathbb{N}^+$ (Proposition 8.2.9)

$$\exists n, m \in \mathbb{N}^+ \; ((1 < n < q) \land (1 < m < q) \land q = n \times m)$$

5 GCD (Proposition 8.2.10)

There exists a unique number $c \in \mathbb{N}^+$ such that

$$\underbrace{(c \mid n) \land (c \mid m)}_{\text{common divisor}} \land \underbrace{(\forall q \in \mathbb{N}^+(((q|n) \land (q|m)) \Rightarrow q \leq c))}_{\text{largest unique}}$$

5.1 GCD of co-prime numbers is 1 (Proposition 8.2.12)

$$n \perp m \Leftrightarrow gcd(n, m) = 1$$

5.2 Bezout Identity (Proposition 8.2.13)

$$n, m \in \mathbb{N}^+ \qquad \exists a, b \in \mathbb{Z} \; (n \times a + m \times b = gcd(m, n))$$

5.3 Euclid's Lemma (Prop. 8.2.15)

$$n, m, p \in \mathbb{N}^+ \qquad (\text{prime}(p) \land (p \mid n \times m)) \Rightarrow (p|n \lor p|m)$$

6 Factorization

Factorization of n is a collection of possible duplicate prime numbers, p_i, such that

$$n = \Pi_{i \in I} p_i$$

7 Fundamental Theorem of Arithmetic

Every $\mathbb{N}^+$ has a unique factorization

7.1 Common divisor divides the GCD (Prop. 8.3.4)

$$\forall q \in \mathbb{N}^+ \ (((q|n) \wedge (q|m)) \Rightarrow q|gcd(m,n))$$

7.2 LCM

7.2.1 (Prop. 8.3.5)

$$n, m \in \mathbb{N}^+ \qquad (n|c) \wedge (m|c) \wedge (\forall q \in \mathbb{N}^+ \ (((n|q) \wedge (m|q)) \Rightarrow c \leq q))$$

7.2.2 (Prop. 8.3.6)

$$(n|lcm(n,m)) \wedge (m|lcm(n,m)) \wedge (\forall q \in \mathbb{N}^+ \ ((n|q) \wedge (m|q) \Rightarrow lcm(n,m) \leq q))$$

7.2.3 LCD (Prop. 8.3.7)

$$\forall q \in \mathbb{N}^+ \ ((n|q) \wedge (m|q)) \Rightarrow lcd(n,m)|q$$

8 Modular Arithmetic

n is congruent to (m modulo c), denoted $n \equiv m \pmod{c}$ iff

$$(m < n \wedge c|n-m) \vee (n < m \wedge c|m-n) \vee (n = m)$$

8.1 (Prop. 8.4.2)

$$n \equiv m \pmod{c} \Leftrightarrow (n \bmod c = m \bmod c)$$

8.2 Congruence relation

$$< n, m > \in \equiv_{\text{mod } c} \text{ iff } n \equiv_{\text{mod } c} m$$

8.3 (Prop. 8.4.5)

$$(n + m) \text{ mod } c = (n \text{ mod } c + m \text{ mod } c) \text{ mod } c$$

8.4 (Prop. 8.4.6)

$$(n \times m) \text{ mod } c = (n \text{ mod } c \times m \text{ mod } c) \text{ mod } c$$

8.5 (Prop. 8.4.7)

$$(n_1 \equiv m_1 (\text{mod } c) \wedge n_2 \equiv m_2 (\text{mod } c)) \Rightarrow (n_1 + n_2 \equiv (m_1 + m_2)(\text{mod } c))$$

8.6 (Prop. 8.4.8)

$$(n_1 \equiv m_1 (\text{mod } c) \wedge n_2 \equiv m_2 (\text{mod } c)) \Rightarrow (n_1 \times n_2 \equiv (m_1 \times m_2)(\text{mod } c))$$

8.7 Fermat's Little Theorem

$$\text{prime}(p) \Rightarrow a^p \equiv a (\text{mod } p)$$

8.7.1 (Prop 8.4.10)

$$(\text{prime}(p) \wedge a \perp p) \Rightarrow a^{p-1} \equiv 1 (\text{mod } p)$$

CS1231 - Cardinality

1 Cardinality

- Count of elements in set
- **Bijection $\Rightarrow$ Same cardinality**
  1. (Injective) $f(m) = f(n) \Rightarrow m = n$
  2. (Surjective) $\forall y \in Y$, show that $\exists x \in X$ such that $f(x) = y$

1.1 Cardinality Relation

Is equivalence relation

- Reflexive: $|A| = |A|$
- Symmetric: $|A| = |B| \Rightarrow |B| = |A|$
- Transitive: $(|A| = |B| \wedge |B| = |C|) \Rightarrow |A| = |C|$

2 Countably infinite

- Set is countably infinite if $|S| = \mathcal{N}_0 = |Z^+|$
- If a set can be **listed**, its countably infinite (prop. 9.3.4)
- If A and B is countably infinite, then so is $A \times B$ (since they can be listed)
- (Generalized) The cartesian product of many countably infinite sets is also countably infinite (prop. 9.3.6)
- Union of countably many countable sets is countable (prop. 9.3.7)
- Subset of a countable set is countable
- Superset of an uncountable set is uncountable

2.1 $\mathbb{Q}$ is countable

1. $\mathbb{Q}^+$, $\frac{a}{b}$, can be expressed as $< a, b >$. Where $a, b \in \mathbb{Z}^+$ and $a \perp b$ (unique representation of $\mathbb{Q}^+$)

2. $\mathbb{Q}^+ \subset \mathbb{Z}^+ \times \mathbb{Z}^+$
3. Therefore, $\mathbb{Q}^+$ is countable (subset of a countable set)
4. $\mathbb{Q}^-$, similar to $\mathbb{Q}^+$, can be expressed as $< -m, n >$
5. Theres a bijection $f(< -m, n >) =< m, n >$ thus $\mathbb{Q}^-$ is countable (same cardinality if theres a bijection)
6. $< 0, 1 >$ is countable (1 element)
7. $\mathbb{Q}^+ \cup \mathbb{Q}^- \cup < 0, 1 >$ is countable (union of countable sets is countable)

2.2 $\mathbb{R}$ is uncountable

Cantor's argument

2.3 Injection but no surjection $\rightarrow$ larger cardinality

If theres an injection $f : A \rightarrow B$ but no surjection, then $|A| < |B|$

2.4 Cardinality of power set larger than set

$$|A| < |\mathcal{P}(A)|$$

2.5 (Theroem 9.4.6)

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{Z}^+)|$$

Combinatorics

1 An Overview

- Sum/Product rule
- Permutations & Combinations
- Pigeonhole principle
- Inclusion/exclusion principle
- Recurrence relations
- Generating functions (power series)

2 Product rule (dependence on other tasks)

When operation can be broken down into 2 or more tasks. Number of ways to perform a task depend on how previous tasks are performed. Number of was to perform each task constant regardless of actions taken in prior tasks

Example

How to label seats with a letter and a positive integer not exceeding 100.

ways $= 26 \times 100 = 2600$

3 Sum rule (independent of other tasks)

When operation cannot be broken down into 2 or more tasks that cannot be down at the same time

Example

How to choose 1 orange and 1 apple from a basket of 10 oranges and 20 apples.

ways $= 10 + 20$

4 Difference rule

$$(\text{finiteSet}(A) \wedge (B \subset A)) \Rightarrow (|A - B| = |A| - |B|)$$

Example

How many passwords are there if: passwords are 6 to 8 alpha-numeric characters. Where passwords must contain ≥ 1 digit

Let P be total number of passwords. P_6, P_7, P_8 be passwords with 6, 7 or 8 alphanumeric characters long.

$P_i = \text{alphanumeric} - \text{all letters}$

$P_6 = 36^6 - 26^6$

$P_7 = 36^7 - 26^7$

$P_8 = 36^8 - 26^8$

$P = P_6 + P_7 + P_8$

5 Inclusion-Exclusion principle

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C|$$

6 Permutations

Ordered arrangement of objects.

Example

Permutations of "abc" $= 3 \times 2 \times 1 = 3!$

6.1 r-Permutations

$$P(n, r) = \frac{n!}{(n-r)!}$$

Example

How many permutations of "abcde" to create a string of length 3 $= 5!/2!$

6.2 r-Permutation with repetetion

$$n^r$$

How many possible stings of length 3 can I build with "abced" $= 5^3$

7 Combinations

Unordered selection of elements

7.1 r-Combinations

$$C(n,r) = \left(\begin{array}{c} a \\ b \end{array} \right) = \frac{n!}{r!(n-r)!}$$

$$C(n,r) = C(n,n-r)$$

7.2 r-Combination with repetition

$$C(n+r-1,r) = C(n+r-1,n-1)$$

8 Pigeonhole Principle

If $k+1$ or more objects are placed into k boxes, at least 1 box contains 2 or more objects

9 Inclusion-Exclusion Principle

$$|A_1 \cup A_2 \cup ... \cup A_n| = \sum_{1 \leq i \leq n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + ... + (-1)^{n+1} |A_1 \cap A_2 \cap ... \cap A_n|$$

OR

$$N(P_1' P_2' ...) = N - \sum_{i=1}^{n} N(P_i)$$

Graph Theory

Complete Graph - $|E(G)| = C(n, 2)$

Handshake Theorem - Sum of degree of all vertices is even $\sum d(G) = 2|E(G)|$

In an **undirected graph**, number of vertices with odd degree is even

Trail is **walk** with **distinct edges**

Path is **trail** with **distinct vertices**

Connected if theres a walk between every pair of distinct vertices

Theres a path between every pair of distinct vertices of a connected undirected graph

Euler trail is a trail (every edge exactly once) transversing **every edge of G**

Closed walk starts and ends at same vertex

Tour is a **closed walk** that transverse every edge of G at least once

Euler tour is a **tour** transversing **every edge exactly once**

Euler tour if **no vertices of odd degree**

Euler trail but not Euler tour if it has **exactly 2 vertices of odd degree**

Euler $\rightarrow$ Edges, Hamilton $\rightarrow$ Vertices

Hamilton path is a path containing **every vertex of G**

Cycle is a closed trail whose **origin/internal vertex are distinct**. (no duplicated internal vertex)

Hamilton cycle is a **cycle containing every vertex of G**