Comp0147: Discrete Math for Comp. Scientists

Foundations:	Core Concept:
- Sets theoric notation	- Linear Algebra
- Functions, Permutations	- Counting
- Euclid's algorithm	

Set Notations:

- $A = \{a, b, c\}$, $d \in A$: d is element that sits inside "bag" A (element: pointer)
- Empty set ϕ: bag with NO elements
- Set $A = B$
  - Need to prove:
    a) $A \subseteq B$: A subset of B
    b) $B \subseteq A$: B subset of A

Set Operations

- Union: $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$

- Intersection: $A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$

Cartesian product:

$$A \times B = \{(x, y) \mid (x \in A) \wedge (y \in B)\}$$

- Difference: $A \setminus B = \{x \mid (x \in A) \wedge (x \notin B)\}$

Symmetric difference:

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

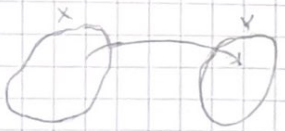
Complement of set A:

$$A^C = U \setminus A = \{x \mid (x \in U) \wedge (x \notin A)\}$$

For Laws check pC

Functions:

$f: X \to Y$



$\text{domain}(f) = \{x \mid f(x) \text{ is defined}\} = X$

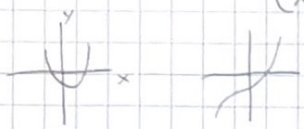
$\text{image}(f) = f(X)$

- Injection / Encodings:

  $f: X \to Y$ is an injection if for any x_1 and x_2 from X:

  $$(x_1 \neq x_2) \to (f(x_1) \neq f(x_2))$$

  (function with unique x and $f(x)$ values)



Not injection Injection

- Surjection (a.k.a. onto mapping)

  $f: X \to Y$ is a surjection if $f(X) = Y$ (range = given set)

  $$\forall y \in Y, \exists x \in X, f(x) = y$$

- Bijection / 1-1 correspondence

  $f: X \to Y$ is a bijection if f is injective and surjective.

  Inverse bijection $f^{-1}(y) = x$ exists if $f(x) = y$

- Sequential composition of functions

  let: $f: X \to Y$ and $g: Y \to Z$

  $h = f ; g \longrightarrow h(x) = g(f(x))$

  (1st apply f, then, apply g)

- Composition of injections

  let: $f: X \to Y$ and $g: Y \to Z$ (both injective)

  $h = f ; g$, $h: X \to Z$ (injection from $X \to Z$)

Composition of surjections

let: $f: X \to Y$ and $g: Y \to Z$ (both surjective)

$h: X \to Z$ (surjection $X \to Z$)

- Composition of bijection

  let: $f: X \to Y$ and $g: Y \to Z$ (both bijective)

  $h: X \to Z$ (bijection $X \to Z$, & exists inverse bijection $h^{-1}: Z \to X$)

Cardinality: Compare

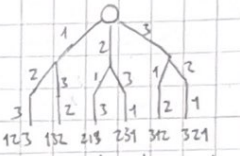
- $|X| \leq |Y|$ if there is an injection function $f: X \to Y$
- $|X| = |Y|$ if there exists a bijection / one-one correspondence h between X and Y. $h: X \leftrightarrow Y$
- Discrete Math: $|\mathbb{Q}| = |\mathbb{Z}| = |\mathbb{N}| = \aleph_0$ (countable), since continuum is not countable.

Finite Functions. Permutations S_n

given a bijection — permutation

$$\begin{matrix}1 & 2 & 3 & \dots & n\\ \downarrow & \downarrow & \downarrow & & \downarrow \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n)\end{matrix} \longrightarrow \begin{pmatrix}1 & 2 & 3 & \dots & n\\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n)\end{pmatrix} \longrightarrow$$

Counting Permutations



thus, $|S_n| = n!$

- Order of a permutation σ is smallest positive integer k, such that

$$\sigma^k = \mathcal{E}, \quad \mathcal{E}(x) = x$$

- Sign of permutation

$$syn(\sigma) \begin{cases} +1 & \text{if } \ell \text{ even} \\ -1 & \text{if } \ell \text{ odd} \end{cases}, \quad \ell = n^\circ \text{ of "disorders"}$$

Binary Relations:

- 2 variable relations

- Equivalence relations $E(x,y)$, Partitions,

  - "Reflexivity" $\forall x\, E(x,x)$ for any x, where $x == x$
  - "Symmetry" $\forall x,y\,(E(x,y) \rightarrow E(y,x))$
  - "Transitivity"

Ex.

$E_2(x,y)$ = "$x - y$ is even"

$[k]_2 = \{y \mid E_2(k,y)\}$ →

representative

$[0]_2$ = even = $\{0, 2, -2 \dots 2n, -2n\}$

$[1]_2$ = odd = $\{1, 3, -1 \dots 2n+1\}$

bit operations

$0 + 0 = 0$
$1 + 0 = 1$
$1 + 1 = 0$

- Equivalence: $x = y \pmod m$

$E_m(x,y)$ = "$(x-y)$ is divisible by m"

$G_m \{0, 1, 2, \dots, m-2, m-1\}$

$a \pmod m = [a]_m = \{y \mid (y-a)$ is divisible by $m\}$

- Congruence

if $a_1 = a_2 \pmod m$ & $b_1 = b_2 \pmod m$, then

$$\begin{cases} a_1 + b_1 = a_2 + b_2 \pmod m \\ a_1 \cdot b_1 = a_2 \cdot b_2 \pmod m \end{cases}, \text{ then} \rightarrow$$

$+ \pmod 3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times \pmod 3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$$\begin{cases} 2 + 1 = 3 \pmod 3 = 0 \pmod 3 \\ 2 \cdot 2 = 4 \pmod 3 = 1 \pmod 3 \end{cases}$$

Purpose: Introduce Groups "+", "×"

$(\mathbb{Z}, +)$ "additive" group - properties

a) closure $\forall x, y \mid (x \in \mathbb{Z}) \wedge (y \in \mathbb{Z}) \rightarrow (x + y \in \mathbb{Z})$ Operations in a set, stay, in that set

b) associativity $\forall x, y, z \in \mathbb{Z} \mid (x+y)+z = x+(y+z)$

c) neutral There is an integer $0 \mid \forall x \in \mathbb{Z} \mid x + 0 = 0 + x = x$

d) invertibility $\forall x, y \in \mathbb{Z} \mid y = -x \rightarrow x + y = y + x = 0$

e) commutativity $\forall x, y \in \mathbb{Z} \mid x + y = y + x$

Theorem: Any operation has an existing and unique solution

$a + z = b$ has unique solution $z = b - a = (-a) + b$

proof:

a) "Existence": $a + \underbrace{((-a) + b)}_{z} = a - a + b = b$

b) "Uniqueness": given z_1 and z_2 from $\mathbb{Z}$,

assume: $a + z_1 = b$ & $a + z_2 = b$ $\Big\} z_1 = z_2 = b$

$-a$ $-a$

$(\mathbb{R}^+, \times)$ "multiplicative" group

a) closure $\forall x, y \in \mathbb{R}^+ \rightarrow x \cdot y \in \mathbb{R}^+$

b) associativity $\forall x, y, z \in \mathbb{R}^+ \mid (x \cdot y) \cdot z = x \cdot (y \cdot z)$

c) neutral There is a neutral 1, such that $\forall x \in \mathbb{R}^+ \mid x \cdot 1 = 1 \cdot x = x$

d) invertibility $\forall x, y \in \mathbb{R}^+ \mid y = x^{-1} \rightarrow x \cdot y = y \cdot x = 1$

e) commutativity $\forall x, y \in \mathbb{R}^+ \mid x \cdot y = y \cdot x$

Theorem:

$\forall a, b \in \mathbb{R}^+ \mid a \cdot z = b$ has unique solution $z = a^{-1} \cdot b$

proof:

a) Existence

b) Uniqueness there is a problem $\rightarrow$ many combination can lead to same result,

Permutations

$\varepsilon = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$ $\sigma_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ $\sigma_2 = \sigma_1^2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$ $\text{syn} = -1$ (odd)

$\sigma_2 = \begin{matrix}1&2&3\\\downarrow&\downarrow&\downarrow\\2&3&1\\\downarrow&\downarrow&\downarrow\\3&1&2\end{matrix}$ $\sigma_2\sigma = \begin{matrix}1&2&3\\\downarrow&\downarrow&\downarrow\\3&1&2\\\downarrow&\downarrow&\downarrow\\1&2&3\end{matrix}$ $\Rightarrow$

multiplication table

$\circ$	ε	σ_1	σ_2
ε	ε	σ_1	σ_2
σ_1	σ_1	σ_2	ε
σ_2	σ_2	ε	σ_1

"multiplicative" group of integers modulo m, $G_m^\times$

$G_m^\times = \{a \mid (1 \le a \le m) \wedge (gdc(a,m) = 1)\}$ forms w.r.t. multiplication modulo m

$\varphi(m) = |G_m^\times|$ — Euler totient function

a) Closure: $\forall a,b \mid gcd(a,m) \wedge gdc(b,m) = 1 \rightarrow gcd(a\cdot b, m) = 1$

b) associativity is there

c) neutral $gcd(1,m) = 1$

d) invertibility $\forall a \in G_m^\times$, there is a $y \in G_m^\times$ such that $a \cdot y = 1 \pmod m$, $y = a^{-1}$

subgroups

Let G be a group & $H \subseteq G$ iff

i) Closure $\forall x,y \mid x \in H \wedge y \in H \rightarrow x \cdot y \in H$

ii) Neutral $\varepsilon \in H$

iii) Invertibility $\forall x \in H \; (x^{-1} \in H)$

Cyclic subgroups — group that can be generated by a single element

let $H = \{a^k \mid k \in \mathbb{Z}\}$ H is a subgroup, because a can generate the entire group

ex. $\{\ldots, a^{-2}, a^{-1}, \varepsilon, a^1, a^2, \ldots\}$, $\varepsilon = a^0$

Lagrange Theorem

Let $G = \{g_1, g_2, g_3, \ldots, g_n\}$ of order n

and $H \subseteq G = \{h_1, h_2, \ldots, h_k\}$ of order k

$\Big\}$ $\frac{n}{k} = \ell$ (disjoint subsets) of same size

$\Downarrow$

$k\ell = n$

example: $x \cdot y \pmod{10}$ group

$G = \{1, 3, 7, 9\}$

$H = \{1, 9\}$

$\Downarrow$

$*\pmod{10}$	1	9
$1 * H$	1	9
$3 * H$	3	7
$7 * H$	7	3
$9 * H$	9	1

$\Rightarrow \ell = 2 \times k = 4 = n$

$\{1,9\}$ $\{3,7\}$