COMP 2711H Notes

by Frank

I. Proofs and Reasoning

- Boolean Algebra

Basic operations of boolean algebra:

Negation: $\neg p$

p	$\neg p$
0	1
1	0

Disjunction: $p \vee q$

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Conjunction: $p \wedge q$

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Implication: $p \to q$

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Exlusive or: $p \oplus q := (p \vee q) \wedge \neg(p \wedge q)$

A ***Tautology*** is a statement that is always true, denoted as T.
A ***Contradiction*** is a statement that is always false, denoted as F.

Equivalence: $(p \equiv q) = (p \Leftrightarrow q) := (p \to q) \wedge (q \to p)$ is a tautology.

Theorem:

Modus Ponens: $p \wedge (p \to q) \implies q$
Hypothetical Syllogism: $(p \to q) \wedge (q \to r) \implies p \to r$
Modus Tollens: $(p \to q) \wedge (\neg q) \implies \neg p$

Theorem:

1) $\neg(p \vee q) \iff \neg p \wedge \neg q$
2) $\neg(p \wedge q) \iff \neg p \vee \neg q$
3) $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$
4) $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$
5) $p \to q \iff \neg p \vee q$

s^d is the ***dual statement*** of s obtained by replacing $\wedge \leftrightarrow \vee$, $T \leftrightarrow F$ in s. We have $s \equiv s' \iff s^d \equiv s'^d$.

A ***proof*** for $\left(\bigwedge_{i=1}^{n} h_i\right) \to c$ is a sequence $p_0, p_1, \ldots, p_k = c$ such that $\forall i, p_i = h_j$ or $\bigwedge_{m=0}^{i-1} p_m \implies p_i$

$p(x)$ is a ***predicate*** if it becomes a proposition when x is replaced by a value in our universe.

Quantifier: ***Universal quantifier*** $\forall$ (for all) and ***Existential quantifier*** $\exists$ (there exists)

- Natural Number System

The set of natural numbers is constructed by ***Peano's Axioms***.

1) 0 is a natural number.
2) Every natural number n has a successor $s(n)$.
3) $\forall n, m \in \mathbf{N}$, if $s(n) = s(m)$, then $n = m$.
4) $\forall n \in \mathbf{N}, s(n) \neq 0$.
5) If K is a set such that $\begin{cases} 0 \in K \\ \forall n \in \mathbf{N}, n \in K \to s(n) \in K \end{cases}$, then $K \supseteq \mathbf{N}$.

Theorem: To prove $\forall n \in \mathbf{N}, p(n)$, it's sufficient to show $\begin{cases} p(0) \\ \forall n \in \mathbf{N}, p(n) \to p(n+1) \end{cases}$.

Definition of ***addition***:
1) $\forall n, n + 0 = n$
2) $\forall n, m,\ \ n + s(m) = s(n+m)$

Definition of ***multiplication***:
1) $\forall n, n \times 0 = 0$
2) $\forall n, m,\ \ n \times s(m) = n \times m + n$

Definition of $\leq$: $n \leq m \iff \exists x, n + x = m$

Mathematical Induction: $\begin{cases} K \subseteq \mathbf{N} \\ 0 \in K \\ \forall n \in \mathbf{N}, n \in K \to s(n) \in K \end{cases} \implies K = \mathbf{N}$

Well-ordering Principle: Every non-empty subset $A \subseteq \mathbf{N}$ has a smallest element.

Infinite Descent: There is no infinite sequence $a_1, a_2, \ldots \in \mathbf{N}$ such that $a_1 > a_2 > \cdots$.

Theorem: Mathematical Induction $\iff$ Well-ordering Principle $\iff$ Infinite Descent

Strong Induction: To prove $\forall n \in \mathbb{N}, p(n)$, it's sufficient to show $\begin{cases} p(0) \\ \forall n \in \mathbf{N}, \bigwedge_{i=0}^{n} p(i) \to p(n+1) \end{cases}$.

II. Enumerative Combinatorics

- Permutation and Combination

Permutation: $P_r^n = P(n,r) := \dfrac{n!}{(n-r)!}$.

Combination: $C_r^n = C(n,r) = \dbinom{n}{r} := \dfrac{n!}{r!(n-r)!}$.

Theorem: $\displaystyle\sum_{i=0}^{n} \binom{n}{i} = 2^n$

Theorem: $\displaystyle\sum_{0 \leq j \leq i \leq n} \binom{n}{i}\binom{i}{j} = 3^n$

Theorem: $\displaystyle\sum_{0 \leq i_k \leq i_{k-1} \leq \cdots \leq i_1 \leq n} \binom{n}{i_1}\binom{i_1}{i_2}\cdots\binom{i_{k-1}}{i_k} = (k+1)^n$

Theorem: $\displaystyle\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^n\binom{n}{n} = \sum_{i=0}^{n} (-1)^i \binom{n}{i} = 0$

Theorem: $\displaystyle n\binom{n-1}{k} = \binom{n}{k+1}(k+1)$

Theorem: $\displaystyle\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$

Theorem: We have $\dfrac{(2n)!}{n!2^n}$ ways of pairings in set A with $2n$ elements:

Theorem: We have $d_n = (n-1)(d_{n-2} + d_{n-1})$ ways of derangement of n elements.

Theorem: Number of $\mathbf{Z}^+$ solutions for $x_1 + x_2 + \cdots + x_k = n$ is equal to $\binom{n-1}{k-1}$.

- Principle of Inclusion and Exclusion (PIE)

PIE for two sets: $|A \cup B| = |A| + |B| - |A \cap B|$

PIE for three sets: $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

PIE for k sets: Let $A_1, A_2, \ldots, A_k$ be finite sets. We have

$$\begin{aligned}\left|\bigcup_{i=1}^{k} A_i\right| = &\sum_{i_1} |A_{i_1}| \\ &- \sum_{i_1<i_2} |A_{i_1} \cap A_{i_2}| \\ &+ \sum_{i_1<i_2<i_3} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &\cdots \\ &+(-1)^{k+1} \sum_{i_1<i_2<\cdots<i_k} |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}|\end{aligned}$$

Generalized PIE: Denote $w(i_1, i_2, \ldots, i_t) := |A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_t}|$

$w(t) := \sum_{(i_1,\ldots i_t)} w(i_1, i_2, \ldots, i_t) = \sum_{\text{all possible}} |\text{intersection of } t \text{ sets}|$. We have $\left|\bigcup_{i=1}^{k} A_i\right| = \sum_{t=1}^{k} (-1)^{t+1} w(t)$

Theorem: $d_n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}$, where d_n is the number of ways of derangement of $\{1,2,\ldots,n\}$.

Proof: Denote $A_i :=$ the set of permutations such that $\pi(i) = i$.

We have $|A_i| = (n-1)!$, $|A_i \cap A_j| = (n-2)!$, ... , and $w(k) = \binom{n}{k}(n-k)!$

$$\begin{aligned}d_n &= |A_1^C \cap A_2^C \cap \cdots \cap A_n^C| \\ &= n! - |A_1 \cup A_2 \cup \cdots \cup A_n| \\ &= n! - w(1) + w(2) - \cdots + (-1)^n w(n) \\ &= n! + \sum_{i=1}^{n} (-1)^i \binom{n}{i} (n-i)! \\ &= n! + \sum_{i=1}^{n} (-1)^i \frac{n!}{i!} \\ &= n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}\end{aligned}$$

- Pigeonhole Principle

Let P and H be finite sets with $|P| > k|H|$. If $f : P \to H$, then $\exists h \in H, |f^{-1}(h)| \geq k+1$.

III. Graph Theory

- Graph Basics

A ***graph*** is an ordered pair $G = (V, E)$ consisting a set V for vertices and a set E for edges

u and v are ***neighbors/adjacent*** iff $\{u, v\} \in E$.

The ***degree*** of a vertex $d(v) := |\{\{u, v\} \in E \mid u \in V\}|$. We have $\sum_{v \in V} d(v) = 2|E|$.

> *Theorem*: If $\forall i \in V, d(i) \leq 2$ in $G = (V, E)$, then every CC of G is either a cycle or a path.
> *Theorem*: If $\forall i \in V, 2 \mid d(i)$, then $E = C_1 \sqcup C_2 \cdots \sqcup C_t$ where C_i's are cycles.
> *Theorem*: $d_1, \ldots, d_n$ is the degree sequence of a graph (not necessarily simple) iff $\sum d_i$ is even.

A sequence $d_1, \ldots, d_n$ is ***graphic*** if it's the degree sequence of a simple graph.

> *Theorem*: A sequence $d_1 \leq d_2 \leq \cdots \leq d_n$ is graphic iff
> $d_1, d_2, \ldots, d_{n-d_n-1}, d_{n-d_n} - 1, \ldots, d_{n-2} - 1, d_{n-1} - 1$ is graphic.

The ***adjacency matrix*** is an $n \times n$ matrix where $A_{ij} = \begin{cases} 1 & \{i, j\} \in E \\ 0 & \{i, j\} \notin E \end{cases}$

A ***walk*** is a sequence of vertices and edges.

A ***trail*** is a walk that does not have repeated edges.

A ***path*** is a walk that does not have repeated vertices.

> *Theorem*: Every (u, v)-walk contains a (u, v)-path.

A ***circuit*** is a walk that begins and ends at the same vertex.

A ***cycle*** is a walk that no vertices other than v_0 repeats, which only appears at the beginning and the end.

An ***Eulerian circuit*** is a closed walk that passes over every edge exactly once.

> *Theorem*: A connected graph G is Eulerian iff all degrees are even.

A ***Hamiltonian cycle*** is a cycle that visits all vertices exaclty once.

A ***connected component*** (CC) is a maximal connected subset of vertices.

> *Theorem*: A graph with n vertices and m edges has at least $n - m$ CC.
> *Theorem*: Every connected graph has $m \geq n - 1$.

The ***eccentricity*** $\mathrm{ecc}(u) := \max_{v \in V} d(u, v)$.

The ***distance*** $d(u, v)$ is the minimum number of edges in a (u, v)-path.

The ***center*** of a graph $G = (V, E)$: u is a center iff $\forall v \in V, \mathrm{ecc}(u) \leq \mathrm{ecc}(v)$.

> *Theorem*: If T is a tree with $|E_T| \geq 3$, then no leaf is a center.
> *Theorem*: A tree T either has one center c or two neighboring centers c_1, c_2.

The ***radius*** of a graph $G = (V, E)$: If u is a center, $\mathrm{rad}(G) := \mathrm{ecc}(u)$.

The ***diameter*** of a graph $G = (V, E)$: $\mathrm{diam}(G) := \max_{u, v \in V} d(u, v)$.

Theorem: In every graph G, $\text{rad}(G) \leq \text{diam}(G) \leq 2 \cdot \text{rad}(G)$.

- Tree

A ***tree*** is a connected graph with $n-1$ edges.

A ***rooted tree*** is just a tree $T = (V, E)$ in which $r \in V$ is chosen as root.

Theorem: Let $G = (V, E)$ and $|V| = n$, $|E| = m$, then the following 6 statements are equivalent.

1) G is a tree.
2) G is connected and $m = n - 1$.
3) G is connected and has no cycles.
4) G has no cycles and $m = n - 1$.
5) There is a unique path between every pair of vertices.
6) G is connected and all edges of G are cuts.

A ***leaf*** is a vertex of degree 1.

Theorem: Every tree with $|V| \geq 2$ has at least 2 leaves.

Theorem: We have $2^{\binom{n}{2}}$ ways to form a graph $G = (V, E)$ with $|V| = n$.

Theorem: We have n^{n-2} ways to form a tree $T = (V, E)$ with $|V| = n$.

Theorem: Adding an edge to a tree creates exactly one cycle.

- Bipartite Graph

A graph $G = (V, E)$ is ***bipartite*** iff $V = V_1 \sqcup V_2$ such that every edge has one endpoint in V_1 and the other in V_2.

Theorem: A graph G is bipartite iff it has no odd cycles.

Theorem: Any graph G has a subgraph H with $|E_H| \geq \dfrac{|E_G|}{2}$ such that H is bipartite.

- Directed Graph and DAG

$G = (V, E)$ is a ***directed graph*** where V is the set of vertices and every $e \in E$ is of the form (u, v)

Theorem: In a directed graph G, if the out-degree of every vertex is at least 1, then there is a cycle.
Theorem: In a directed graph G, if the in-degree of every vertex is at least 1, then there is a cycle.

Two vertices u and v are ***strongly connected*** iff there is a (u, v)-path and a (v, u)-path

A ***strongly connected component*** (SCC) is a maximal subset of vertices such that every two of them are strongly connected.

Theorem: A loopless directed graph G has no cycle iff every vertex of G is its own SCC.

A ***directed acyclic graph*** (DAG) is a directed graph without any cycle.

Given a directed graph $G = (V, E)$, a ***topological order*** is a permutation π of vertices such that every edge $e \in E$ is of the form $(\pi(i), \pi(j))$ with $i \leq j$.

Theorem: Every DAG has a topological order.

Theorem: A loopless directed graph G is a DAG iff G has a topological ordering.

- Weighted Graph and Related Algorithms

A ***weighted graph*** $G = (V, E, w)$ consists of a graph $G' = (V, E)$ and $w : E \to \mathbf{R}$

Every connected graph $G = (V, E)$ has a subgraph $T = (V, E_T)$ such that T is a tree. Such tree T is called a ***spanning tree***.

Theorem: Given a connected weighted graph G, a subtree $T = (V, E_T)$ is an ***MST*** (***minimum spanning tree***) if it is a spanning tree with least total weight.

Algorithms for MST: ***Kruskal's Algorithm*** and ***Prim's Algorithm***

A ***shortest-path tree*** (SPT) rooted at a vertex $v \in V$ of a connected, undirected graph $G = (V, E)$ is a spanning tree $T = (V, E_T)$ such that the path distance from root v to any other vertex $u \in V$ is the shortest path distance from v to u in G.

Constuct an ***adjacency matrix*** A where $A_{ij} = \begin{cases} w(\{i, j\}) & \{i, j\} \in E \\ +\infty & \{i, j\} \notin E \end{cases}$, operating on the $(\min, +)$ semiring
Calculation rule: $(A^2)_{ij} = \min_k (A_{ik} + A_{kj})$

Theorem: $(A^t)_{ij} =$ length of the shortest walk with exactly t edge from i to j.

By adding loops to all vertices, i.e. changing the diagnal entries of A to 0, we can have $(\tilde{A}^t)_{ij} =$ length of the shortest walk with at most t edge from i to j.

Theorem: $d(u, v) = \left(\tilde{A}^{|V|-1}\right)_{uv}$

Algorithms for SPT: ***Dijkstra's Algorithm***

- Matching, Vertex/Edge Cover and Independent Set

$M \subseteq E$ is a ***matching*** if no two edges in M shares an endpoint.

M is a ***maximal matching*** if $\nexists M' \supsetneq M$.

M is a ***maximum matching*** if $\forall M', |M'| \leq |M|$.

Suppose M is a matching in G. An ***alternating*** (u, v)***-walk*** is a walk that alternates between M and $E \backslash M$.

An ***augmenting path*** is an alternating path that starts and ends in $E \backslash M$, and the end vertices are unmatched.

Theorem: A matching M is maximum iff it does not have an augmenting path.

Theorem: In an X, Y-bipartite graph, there is a matching M saturating X iff $\forall S \subseteq X, |N(S)| \geq |S|$.

A ***vertex cover*** (VC) is a set A of vertices such that every edge has at least one endpoint in A.

An ***edge cover*** (EC) is a subuset $L \subseteq E$ such that every vertex is incident to at least one edge in L.
A set $I \subseteq V$ is an ***independent set*** (IS) if $\forall e \in E, e \nsubseteq I$.

Theorem: max IS + min VC $= n$	for all graphs
Theorem: min VC $=$ max matching	for bipartite graphs
Theorem: min VC $\geq$ max matching	for all graphs

Theorem: max matching + min EC $= n$ for all graphs without isolated vertices
Theorem: max IS = min EC for bipartite graphs without isolated vertices

- Flow Network

For a ***flow network***, we have a directed graph $G = (V, E)$, a ***source*** $s \in V$, a ***sink*** $t \in V$ and a ***capacity*** function $V \times V \to \mathbf{N}$.

A ***flow*** is a function $f : V \times V \to \mathbf{R}$ satisfying

1) $\forall u, v \in V, f(u, v) \le c(u, v)$
2) $\forall u, v \in V, f(u, v) = -f(v, u)$
3) $\forall u \in V, \sum_v f(u, v) = 0$

$f(u, v)$ represents the flow from u to v.

Define $|f| = \sum_v f(s, v) = \sum_v f(v, t)$

Algorithm for maximum flow: ***Ford-Fulkerson Algorithm***

Theorem: $f(A, B) = \sum_{a \in A} \sum_{b \in B} f(a, b)$
Theorem: $f(s, V) = |f| = \sum_{v \in V} f(s, v)$
Theorem: $f(A \sqcup B, C) = f(A, C) + f(B, C)$

A ***cut*** in G is a division $V = A \sqcup B$ such that $s \in A \wedge t \in B$

Denote $f(A, B) = |f|$ when $V = A \sqcup B$. We have $|f| = \sum_{u \in A} \sum_{v \in B} c(u, v)$.
Theorem: The maximum flow is equal to the minimum cut.

- Graph Coloring

Given a graph $G = (V, E)$, a ***proper coloring*** with k colors is a function $c : V \to \{1,2,\ldots,k\}$ such that for every $e \in E$, the two endpoints of e have different colors.

The ***chromatic number*** $\chi(G)$ is the least number of colors needed to properly color G.

$C \subseteq V$ is a ***clique*** if $\forall u, v \in C, \{u, v\} \in E$. Denote $w(G)$:= the size of a largest clique.

Denote $\alpha(G)$:= the size of a largest independent set. Suppose G has degree sequence $d_1 \ge d_2 \ge \cdots \ge d_n$.

Theorem: $\chi(G) \ge w(G)$, $\dfrac{n}{\alpha(G)} \le \chi(G) \le 1 + \max_i \left(\min\{d_i, i-1\}\right)$

Let G and H be graphs. The ***Cartesian product*** of G and H is $G \times H := (V_G \times V_H, E_{G \times H})$ where $E_{G\times H} := \left\{\left((u, v), (u, v')\right) : (v, v') \in H\right\} \cup \left\{\left((u, v), (u', v)\right) : (u, u') \in G\right\}$

Theorem: $\chi(G \times H) = \max\{\chi(G), \chi(H)\}$

IV. Number Theory

- The Set of Integer

Construction of $\mathbf{Z}$
1) $\mathbf{N} \subseteq \mathbf{Z}$
2) $n \in \mathbf{N} \backslash \{0\} \implies -n \in \mathbf{Z}$

An ***order*** on $\mathbf{Z}$ is a relation $\cdot < \cdot \subseteq \mathbf{Z} \times \mathbf{Z}$

For $a, b \in \mathbf{N}$, $a <_{\mathbf{Z}} b \iff a <_{\mathbf{N}} b$
For $a, b \in \mathbf{N} \backslash \{0\}$, $-a < 0 < b$, $-a < -b \iff b > a$

Definition of ***predecessor*** on $\mathbf{Z}$
1) $\forall a \in \mathbf{N} \backslash \{0\}, p(a) = p_{\mathbf{N}}(a)$
2) $p(0) = -1 = -s(0)$
3) $\forall a \in \mathbf{N} \backslash \{0\}, p(-a) = -s(a)$

Definition of ***addition*** on $\mathbf{Z}$
1) $\forall a \in \mathbf{Z}, a + 0 = a$
2) $\forall a \in \mathbf{Z}, \forall b \in \mathbf{N} \backslash \{0\}, a + b = s(a + p(b))$
3) $\forall a \in \mathbf{Z}, \forall b \in \mathbf{N} \backslash \{0\}, a + (-b) = p(a + s(-b))$

Definition of ***substraction*** on $\mathbf{Z}$
1) $a - 0 := 0$
2) $a - b := a + (-b)$
3) $a - (-b) := a + b$

Definition of ***multiplication*** on $\mathbf{Z}$
1) $\forall a \in \mathbf{Z}, a \cdot 0 = 0$
2) $\forall a \in \mathbf{Z}, \forall b \in \mathbf{N} \backslash \{0\}, a \cdot b = a \cdot p(b) + a$
3) $\forall a \in \mathbf{Z}, \forall b \in \mathbf{N} \backslash \{0\}, a \cdot (-b) = a \cdot s(-b) + (-a)$

- Divisibility

Theorem: $\forall a, b \in \mathbf{Z}, b > 0$, there exist unique $q, r \in \mathbf{Z}, 0 \leq r < b$ such that $a = q \cdot b + r$.

Divisibility: We say $b \mid a$ if $\exists q \in \mathbf{Z}, a = b \cdot q$.

Theorem: $\forall a, b, c, d \in \mathbf{Z}$, we have the following properties
1) $a \mid 0, \ 1 \mid a, \ a \mid a$
2) $a \mid 1 \iff a \in \{1, -1\}$
3) $a \mid b \wedge c \mid d \implies ac \mid bd$
4) $a \mid b \wedge b \mid c \implies a \mid c$
5) $a \mid b \wedge b \mid a \iff a = \pm b$
6) $a \mid b \wedge a \mid c \iff a \mid (bx + cy), \forall x, y \in \mathbf{Z}$

Greatest common divisor (gcd): Let $a, b \in \mathbf{Z}$ and not both are 0. We say $d \in \mathbf{Z}$ is the gcd(a, b) iff
1) $d \mid a \wedge d \mid b$
2) $\forall d', d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$

Least common multiple (lcm): Let $a, b \in \mathbf{Z}$ and not both are 0. We say $m \in \mathbf{Z}$ is the lcm(a, b) iff
1) $a \mid m \wedge b \mid m$
2) $\forall m', a \mid m' \wedge b \mid m' \Rightarrow m \mid m'$

Theorem: $\forall a, b \in \mathbf{Z}$ that not both are 0, $\exists x, y \in \mathbf{Z}$ such that $\gcd(a, b) = ax + by$. Or equivalently, $\{ax + by \mid x, y \in \mathbf{Z}\} = \{q \cdot \gcd(a, b) \mid q \in \mathbf{Z}\}$

Theorem: $a \perp b \iff \gcd(a, b) = 1 \iff \exists x, y \in \mathbf{Z}, ax + by = 1$

Theorem: $\begin{cases} a \mid c \\ b \mid c \\ a \perp b \end{cases} \implies a \cdot b \mid c$

Theorem: $\begin{cases} a \mid b \cdot c \\ a \perp b \end{cases} \implies a \mid c$

Algorithm for gcd: ***Euclidean algorithm***

$\gcd(a, b)$:

if $b \mid a$: return b.

write $a = q \cdot b + r$.

return $\gcd(b, r)$.

Theorem: If $a = q \cdot b + r, 0 \leq r < b$, then $\gcd(a, b) = \gcd(b, r)$.

Theorem: $p \in \mathbf{Z}$ is prime iff its only divisors are $-1, 1, p, -p$.

Theorem: $p \in \mathbf{P}, p \mid ab \implies p \mid a \vee p \mid b$

Fundamental Theorem of Arithmetic: $\forall n > 1$, we can write $n = p_1 p_2 \cdots p_k$ where every p_i is a prime, and $p_1 \leq p_2 \leq \cdots \leq p_k$. This is called the ***prime factoriazation*** of n and it's unique.

Theorem: $\begin{cases} a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k} \\ b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \cdots \cdot p_k^{\beta_k} \end{cases} \implies \begin{cases} \gcd(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\min\{\alpha_2, \beta_2\}} \cdot \cdots \cdot p_k^{\min\{\alpha_k, \beta_k\}} \\ \operatorname{lcm}(a, b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdot p_2^{\max\{\alpha_2, \beta_2\}} \cdot \cdots \cdot p_k^{\max\{\alpha_k, \beta_k\}} \end{cases}$

Theorem: $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$

- Congrucence

Congrucence: We say $a \equiv b \pmod{n} \iff n \mid a - b$

Theorem: $\forall a, b, c, d, n \in \mathbf{Z}, n > 1$, we have the following properties (mod n)

1) $a \equiv a$
2) $a \equiv b \implies b \equiv a$
3) $a \equiv b, b \equiv c \implies a \equiv c$
4) $a \equiv b, c \equiv d \implies a + b \equiv c + d$
5) $a \equiv b, c \equiv d \implies ab \equiv cd$
6) $a \equiv b \implies a + c \equiv b + c$
7) $a \equiv b \implies ac \equiv bc$
8) $a \equiv b \implies a^k \equiv b^k$

$a^{-1} \in \mathbf{Z}$ is the ***modular multiplicative inverse*** of a mod n such that $a^{-1}a \equiv_n 1$.

Theorem: $a^{-1} \bmod n$ exists $\iff \gcd(a, n) = 1$

Theorem: If $p(x)$ be a polynomial with integer coefficients, then we have $a \equiv b \iff p(a) \equiv p(b)$.

Theorem: The equation $ax \equiv_n b$ is solvable $\iff d \mid b$, where $d = \gcd(a, n)$.

Theorem: The number of solution $0 \le x < n-1$ is $\begin{cases} 0 & d \nmid b \\ d & d \mid b \end{cases}$.

Chinese Remainder Theorem: Let $n_1, n_2, \ldots n_k \in \mathbf{Z}^+$ such that $\forall i \ne j, n_i \perp n_j$. The system of linear congrucences $\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$ has a unique solution mod $n_1 n_2 \cdots n_k$.

Proof: Denote $N := n_1 n_2 \cdots n_k$ and $N_i := \dfrac{N}{n_i}$, $n_i \perp N_i \implies \exists N_i^{-1} (\text{mod } n_i)$

$$\implies N_i^{-1} N_i \equiv \begin{cases} 1 \pmod{n_i} \\ 0 \pmod{n_j} \end{cases} \implies x = \left[\sum_{i=1}^{k} N_i^{-1} N_i a_i \right]_N \equiv a_i \pmod{n_i}$$

Fermat's Little Therorem: $\forall p \in \mathbf{P}, p \perp a \implies a^{p-1} \equiv_p 1$.

Proof: Since $\{1,2,\ldots,p-1\} = \left\{ [a]_p, [2a]_p, \ldots, [(p-1)a]_p \right\}$, we have $1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv a \cdot 2a \cdot \cdots \cdot (p-1)a = a^{p-1} \cdot 1 \cdot 2 \cdot \cdots \cdot (p-1) \pmod{p}$, hence $a^{p-1} \equiv_p 1$.

Theorem: If $b \equiv c \pmod{p-1}$, then $a^b \equiv a^c \pmod{p}$

Denote $S(n) := \{x \in \mathbf{Z} : 1 \le a \le n, a \perp n\}$

Euler's totient function $\varphi(n) := |S(n)| = \left| \{x \in \mathbf{Z} : 1 \le a \le n, a \perp n\} \right|$

Theorem: If $n \perp m$ then $\varphi(nm) = \varphi(n) \cdot \varphi(m)$

Proof: $f : \begin{array}{l} S(nm) \to S(n) \times S(m) \\ [x]_{nm} \mapsto \left([x]_n, [x]_m\right) \end{array}$ is bijective using CRT. Hence $|S(nm)| = |S(n) \times S(m)|$.

Theorem: Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, then $\varphi(n) = n \left(1 - \dfrac{1}{p_1}\right)\left(1 - \dfrac{1}{p_2}\right) \cdots \left(1 - \dfrac{1}{p_k}\right)$.

Euler's Theorem: $a \perp n \implies a^{\varphi(n)} \equiv_n 1$.

Proof: Since $\left\{x_1, x_2, \ldots, x_{\varphi(n)}\right\} = \left\{a x_1, a x_2, \ldots, a x_{\varphi(n)}\right\}$, by multiplying together we get $a^{\varphi(n)} \equiv_n 1$.

Wilson's Theorem: $\forall p \in \mathbf{P}, (p-1)! \equiv_p -1$.

- Cryptography

Symmetric Encryption: Alice and Bob are communicating via a channel, and someone can intercept between them.

We need an ***encryption function*** $\mathrm{Enc}_k : \Sigma^n \to \Sigma^n$ and a ***decryption function*** $\mathrm{Dec}_k : \Sigma^n \to \Sigma^n$ satisfying $\forall k \, \forall m, \mathrm{Dec}_k\left(\mathrm{Enc}_k(m)\right) = m$.

The ***Diffie-Hellman-Merkle Key Exchange*** consists of the following steps:

1) Alice chooses a huge prime number p and a primitive root g, and anounces them. g is a primitive root iff $\{g^0, g^1, \ldots, g^{p-2}\} = \{1,2,\ldots, p-1\}$.
2) Alice chooses a secret random number a. Bob chooses a secret random number b.
3) Alice sends $[g^a]_p$. Bob sends $[g^b]_p$.
4) Alice computes $\left[(g^b)^a\right]_p$. Bob computes $\left[(g^a)^b\right]_p$.
5) $[g^{ab}]_p$ is the key for Alice and Bob.

Public Key Crypto (***Asymmetric Encryption***): I want everyone can encrypt, but only one person can decrypt.

Alice wants to send a message to Bob.

The ***El-Gamal Encryption*** consists of the following steps:

1) Bob chooses a huge prime p, a primitive root g and a secret value b, and publishes $e = (p, g, [g^b]_p)$.
2) Alice wants to send $m < p$ to Bob. She first chooses a secret value a and sends $\mathrm{Enc}_e(m) = ([g^a]_p, [m + g^{ab}]_p)$.
3) Bob computes $m = \left[m + g^{ab} - (g^a)^b\right]_p$ to get m.

The ***RSA Algorithm*** consists of the following steps:

1) Pick 2 huge primes p, q.
2) $n = p \cdot q$.
3) Pick a secret value d and let $e = d^{-1} \pmod{\mathrm{lcm}(p-1, q-1)}$.
4) Announce n, e.
5) Alice sends $\mathrm{Enc}_e(m) := [m^e]_n$ to Bob.
6) Bob computes $m = \mathrm{Dec}_d(\overline{m}) := [\overline{m}^d]_n$ to get m.

By Euler's theorem, we can check that $\forall m, \mathrm{Dec}_d\left(\mathrm{Enc}_d(m)\right) = [m^{ed}]_n = m$.

Digital Signature: I want only one person can encrypt, but everyone can decrypt.

We need a ***sign function*** $\mathrm{sign}_d : \Sigma^* \to \Sigma^*$ and a ***verify function*** $\mathrm{verify}_e : \Sigma^* \times \Sigma^* \to \{0,1\}$.

We need to ensure that only Alice can sign, but given the message and the signature, everyone can verify.

RSA signatures use RSA algorithm to both sign, encrypt, verify and decrypt, which consists of the following steps:

$$\begin{cases} \mathrm{sign}_d(m) := [m^d]_n \\ \mathrm{verify}_e(m, s) := \begin{cases} 1 & [s^e]_n = m \\ 0 & [s^e]_n \neq m \end{cases} \end{cases}$$

To send a message m from Alice to Bob, Alice should:

1) Compute $s = \mathrm{sign}_{d_{A,s}}(m)$.
2) $m' = (m \text{ concatenate } s)$.
3) $\overline{m} = \mathrm{Enc}_{e_{B,m}}(m')$.
4) Send $\overline{m}$ to Bob.

When Bob receives $\overline{m}$, Bob should:

1) $m' = \mathrm{Dec}_{d_{B,m}}(\overline{m})$
2) $m' = (m \text{ concatenate } s)$, so Bob get (m, s)

3) $\text{verify}_{e_{A,s}}(m, s)$

V. Set Theory

- ZFC Axiom System

Naive comprehension: $S = \{x : \varphi(x)\}$

Naive comprehension results in ***Russell's paradox***: $A := \{x : x \notin x\} \implies \begin{cases} A \in A \implies A \notin A \\ A \notin A \implies A \in A \end{cases}$.

Therefore we introduce ***Zermelo-Fraenkel set theory***.

In our language L, we support formulas:

1) Variables (e.g. $x, y, z, \ldots$) over sets
2) $\in, =$
3) Logical and boolean operators $\wedge, \vee, \neg, \forall, \exists$
4) Parentheses

Axioms (including Axiom of Choice)

1) (***Extensionality***) Two sets are equal iff they have the same elements.
$\forall x \forall y \; x = y \iff (\forall z \; z \in x \iff z \in y)$

2) (***Empty set***) There is a set with no elements.
$\exists x \forall y \; y \notin x$

Theorem: There is a unique set with no elements. We denote it as $\varnothing$.

3) (***Unordered pair***) If x and y are sets, there is a set $\{x, y\}$ whose elements are exactly x, y.
$\forall x \forall y \exists z (x \in z \wedge y \in z \wedge \forall w \; w \in z \implies (w = x \vee w = y))$

Ordered pair: $(x, y) := \big\{\{x\}, \{x, y\}\big\}$

Theorem: $(x, y) = (a, b) \iff x = a \wedge y = b$

4) (***Union***) If x is a set, there is a set consisting of all the elements of all the elements of x.
$\forall x \exists y \forall z (z \in y \iff \exists w (w \in x \wedge z \in w))$
We denote $y = \bigcup x$.

Remark: For sets a, b, define $a \cup b := \bigcup \{a, b\}$.

5) (***Comprehension***) If $\varphi(z, w_1, w_2, \ldots, w_k)$ is a formula in L with free variables $z, w_1, w_2, \ldots, w_k$ and x is a set, and $a_1, a_2, \ldots, a_k$ are sets, then $\{y \in x : \varphi(y, a_1, a_2, \ldots, a_k)\}$ is a set.
$\forall x \forall a_1 \forall a_2 \cdots \forall a_k \exists z \left(y \in z \iff y \in x \wedge \varphi(y, a_1, a_2, \ldots, a_k)\right)$

A ***class*** is a collection of the form $X = \{x : \varphi(x)\}$.

6) (***Power set***) Let x be a set. There is a set y whose elements are subsets of x.
$a \subseteq b \overset{\text{def}}{\iff} (\forall z \; z \in a \implies z \in b)$
$\forall x \exists y \forall z \; z \subseteq x \iff x \in y$
We denote $y = P(x)$.

Cartesian product: Let X, Y be sets, $X \times Y := \{z \in P(P(X \cup Y)) : \exists x \in X \; \exists y \in Y \; z = (x, y)\}$

A ***relation*** from X to Y is a subset $R \subseteq X \times Y$
$(x, y) \in R \iff xRy$

A relation $R \subseteq X \times Y$ is a ***function*** $R : X \to Y$ if
$\forall x \in X \ \exists y \in Y (xRy \wedge \forall y' \in Y \ xRy' \implies y = y')$

7) (***Infinity***) There is an inductive set.
$\exists X \ \varnothing \in X \wedge \forall y \ y \in X \implies y \cup \{y\} \in X$

Theorem: There is a unique set **N** such that
1) **N** is inductive.
2) For every inductive set X, we have $\mathbf{N} \subseteq X$.

8) (***Replacement***) Let $\varphi(x, y)$ be a formula in L such that $\forall x \exists y \ \varphi(x, y) \wedge \exists y' \ \varphi(x, y') \implies y' = y$
Then $\varphi(x, y)$ is called a ***class function***.
If $\varphi(x, y)$ is a class function and X is a set , then there is a set Y containing exactly y's such that $\exists x \in X \ \varphi(x, y)$.

9) (***Foundation***) Every set x contains an $\in$-minimal element.
$\forall x \exists y (y \in x \wedge \forall z \ z \in x \implies z \notin y)$

Theorem: Let x be a set, then $x \notin x$.

10) (***Choice***) The following statements are equivalent.

1) For every two sets A and B, either $|A| \le |B|$ or $|B| \le |A|$.

2) For any relation $R \subseteq X \times Y$, there is a function $F \subseteq R$ such that $\text{dom}(F) = \text{dom}(R)$.

3) For every set A, there exists a function $F : P(A) \backslash \{\varnothing\} \to A$ such that
$\forall B \subseteq A, \ B \neq \varnothing \implies F(B) \in B$

4) For every set A of non-empty disjoint sets, $\exists C \subseteq \bigcup A$ such that $\forall a \in A, \ |a \cap C| = 1$.

5) (***Zorn's Lemma***) Let A be a set such that for every chain $B \subseteq A$ we have $\bigcup B \in A$. Then A has a maximal element.

A set C is a ***chain*** if $\forall x, y \in C, \ x \subseteq y \vee y \subseteq x$.
A ***maximal element*** of A is an element $m \in A$ such that $\forall a \in A, \ a \neq m \implies m \nsubseteq a$.

Construction of natural number using ZFC: $\begin{cases} 0 := \varnothing \\ s(n) := n \cup \{n\} \end{cases}$

For example:

$0 = \varnothing$
$1 = 0 \cup \{0\} = \{0\} = \{\varnothing\}$
$2 = 1 \cup \{1\} = \{0,1\} = \big\{\varnothing, \{\varnothing\}\big\}$
$3 = 2 \cup \{2\} = \{0,1,2\} = \big\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\big\}$

We define the order of natural numbers as follows:
$n \le m \iff n \subseteq m$
$n < m \iff n \in m$

- Cardinality

A set x is ***finite*** if there is an $n \in \mathbf{N}$ and a function $f : x \to n$ such that f is bijective. Denote $|x| = n$.

We write $|X| = |Y|$ or $X \sim Y$ if there exists a bijective function $f : X \to Y$
We write $|X| \leq |Y|$ if there exists a one-to-one function $f : X \to Y$.

Theorem:
1) $\forall x, x \sim x$
2) $\forall x, y, z\ x \sim y \wedge y \sim z \implies x \sim z$
3) $\forall x, y\ x \sim y \iff y \sim x$

A set X is ***countable*** if $|X| = |\mathbf{N}|$.

Theorem:
1) $|2\mathbf{N}| = |\mathbf{N}|$
2) $|\mathbf{P}| = |\mathbf{N}|$
3) $|\mathbf{Q}| = |\mathbf{N}|$
4) $|\mathbf{N} \times \mathbf{N}| = |\mathbf{N}|$
5) $|\mathbf{N}^k| = |\mathbf{N}|$

Theorem: Let $X = \{x_0, x_1, \ldots\}$ be a countable set whose every element x_i is also a countable set. Then $\bigcup X$ is also countable.

Cantor's Theorem: For every set A, $|P(A)| \neq |A|$.

Proof: Suppose $g : A \to P(A)$ is a bijection. $T := \{a \in A : a \notin g(a)\} \in P(A)$
$\forall a \in A, \begin{cases} a \notin g(a) \implies a \in T \implies g(a) \neq T \\ a \in g(a) \implies a \notin T \implies g(a) \neq T \end{cases}$. Therefore g is not onto.

Tarski's Fixed Point Theorem: Let X be a set and $h : P(X) \to P(X)$ such that $A \subseteq B \implies h(A) \subseteq h(B)$. Then there exists $C \subseteq X$ such that $h(C) = C$.

Schröder-Bernstein Theorem: $\begin{cases} |X| \leq |Y| \\ |Y| \leq |X| \end{cases} \implies |X| = |Y|$

- Real Number System

Decimal expansion of rational numbers: $0.a_1a_2\ldots a_n := \sum_{i=1}^{n} \frac{a_i}{10^i}$ or $0.a_1a_2\ldots := \sum_{i=1}^{\infty} \frac{a_i}{10^i}$

Three types of decimal expansions:
1) Terminating: [int] $. a_1a_2\ldots a_n$
2) Repeating: [int] $. a_1a_2\ldots a_na_1a_2\ldots a_n\ldots$
3) Mixed: [int] $. a_1a_2\ldots a_nb_1b_2\ldots b_mb_1b_2\ldots b_m\ldots$

Theorem: x is a terminating, repeating or mixed decimal expansion $\iff x \in \mathbf{Q}$

Let A be a set. An ***order*** on A is a relation $\cdot < \cdot \subseteq A \times A$ such that
1) $\forall a, b \in A$, we have exactly one of $a < b$ or $b < a$ or $a = b$
2) $\forall a, b, c \in A$, $a < b \wedge b < a \implies a < c$

Define $a \leq b \iff a < b \wedge a = b$

Let U be an ordered set and $A \subseteq U$. An element $b \in U$ is an ***upper-bound*** of A if $\forall a \in A,\ a \leq b$.
If there exists s such that $\begin{cases} s \in B \\ \forall s' \in B,\ s' \geq s \end{cases}$ then s is the ***supremum*** of A, denoted as $\sup A$.
If U is an ordered set, we say U has the ***least-upper-hound property*** if every non-empty subset $A \subseteq U$ that has an upper bound also has a supremum.

Theorem: If U is an ordered set,
then U has the least-upper-hound property $\iff$ U has the largest-lower-bound property.

Construction of $\mathbf{R}$: ***Dedekind cut***

A ***cut*** is a subset $A \subseteq \mathbf{Q}$ such that

1) $A \neq \varnothing,\ A \neq \mathbf{Q}$
2) $a \in A,\ a' \in \mathbf{Q},\ a' < a \implies a' \in A$
3) A does not have a maximum

The definition of the set of ***real numbers*** using dedekind cut $\mathbf{R} := \{A \subseteq \mathbf{Q} : A \text{ is a cut}\}$

Theorem: $\mathbf{R} = \{\text{all decimal representations}\}$

We define the order of real numbers: $a \leq b \iff a \subseteq b$

Theorem: $\sup A = \bigcup A$

Theorem: ($\mathbf{Q}$ is ***dense*** on $\mathbf{R}$) $\forall x, y \in \mathbf{R},\ x < y \implies \exists z \in \mathbf{Q},\ x < z < y$

Theorem: $|[a,b]| = |(a,b)|$

Proof: Pick $X = \{x_1, x_2, \dots\} \subseteq (a,b)$.

$$\varphi(t) := \begin{cases} x_1 & t = a \\ x_2 & t = b \\ x_{i+2} & t = x_i \\ t & \text{otherwise} \end{cases}, \text{ hence } \varphi : [a,b] \to (a,b) \text{ is bijective.}$$

Theorem: $|(a,b)| = |(0,1)|$

Theorem: $|\mathbf{R}| = |(0,1)|$

Theorem: $|\mathbf{R}| = |P(\mathbf{N})|$

VI. Probability Theory

- Probability Space

Paradoxical probability problems: ***Monty Hall Problem***, ***Sleeping Beauty***, ***Cancer Test***

The set of ***extended real numbers***: $\overline{\mathbf{R}} := \mathbf{R} \cup \{+\infty, -\infty\}$

The set of ***positive extended real numbers***: $\overline{\mathbf{R}^+} := [0, +\infty) \cup \{+\infty\}$

Let A be a set and $E \subseteq P(A)$, $\mu : E \to \overline{\mathbf{R}^+}$. We say (A, E, μ) is a ***measure space*** if:

1) $\varnothing \in E,\ \mu(\varnothing) = 0$
2) $X_1, X_2, \dots \in E \implies \bigcup_{i=1}^{\infty} X_i \in E$
3) $\forall i \neq j,\ X_i \cap X_i = \varnothing \implies \mu\left(\bigcup_{i=1}^{\infty} X_i\right) = \sum_{i=1}^{\infty} \mu(X_i)$
4) $X \in E \implies A \backslash X \in E$

Lebesgue measure: For every segment from a to b, the measure μ is $b-a$.

Probability function is a function $P : E \to [0,1]$

We say (S, E, P) is a ***probability space*** if

1) $\varnothing \in E,\ S \in E$
2) $X_1, X_2, \ldots \in E \implies \bigcup_{i=1}^{\infty} X_i \in E$
3) $X \in E \implies A \backslash X \in E$
4) $P(S) = 1$
5) $\forall i \neq j, X_i \cap X_i = \varnothing \implies P\left(\bigcup_{i=1}^{\infty} X_i\right) = \sum_{i=1}^{\infty} P(X_i)$

Conditional probability: $P(A \mid B) = \dfrac{P(A \cap B)}{P(B)}$

We say A and B are ***independent events*** iff $P(A \mid B) = P(A)$, or equivalently, $P(A \cap B) = P(A) \cdot P(B)$.

We say $E_1, E_2, \cdots, E_n$ are independent events iff $\begin{cases} P(E_{i_1} \cap E_{i_2}) = P(E_{i_1}) \cdot P(E_{i_2}) \\ P(E_{i_1} \cap E_{i_2} \cap E_{i_3}) = P(E_{i_1}) \cdot P(E_{i_2}) \cdot P(E_{i_3}) \\ \vdots \\ P(\bigcap_{j=1}^{n} E_{i_j}) = \prod_{j=1}^{n} P(E_{i_j}) \end{cases}$.

- Real Random Variable

A ***real random variable*** is a function $X : S \to \mathbf{R}$ such that $\forall \alpha = (-\infty, a], X^{-1}(\alpha)$ is an event.

Define $P(X \leq a) = P(\{s \in S : X(s) \leq a\})$

We say X is a ***discrete random variable*** if range(X) is either finite or countable.

Suppose X is discrete and range$(X) = \{x_1, x_2, \ldots, x_n\}$.

We define the ***expectation*** $E[X] := \sum_{i=1}^{n} x_i \cdot P(X = x_i)$.

Theorem: $E[aX + bY + c] = aE[X] + bE[Y] + c$

- Markov Chain

Let Q be a finite set and $\forall i$, range$(X_i) \subseteq Q$. We say $X_0, X_1, X_2, \ldots$ is a ***Markov chain*** if $\forall n, \forall q_0, q_1, \ldots, q_n \in Q,\ P(X_n = q_n \mid X_{n-1} = q_{n-1}) = P(X_n = q_n \mid X_i = q_i, \forall i < n)$

Markov chain $C = (G, \pi, v_0)$ where $G = (V, E)$ is a directed graph and $\pi : E \to (0,1]$ such that $\forall u \in V, \sum_{v \in N(u)} \pi(u, v) = 1$.

Denote X_i: the vertex we're at at time i. Let $w = e_0 e_1 \cdots e_n$ be a finite walk on G.

$\text{Ext}(w) = \{\overline{w} \in E^\infty : \overline{w}$ is an infinite walk in G and w is a prefix of $\overline{w}\}$, define $P(\text{Ext}(w)) = \prod_{i=1}^{n-1} \pi(e_i)$

We have the probability space (S, F, P) for C, where S is the set of infinite walks on G starting at v_0.

We have a ***target set*** $T \subseteq V$ on our Markov chain.

$\Diamond T = \{\overline{w} : \exists i \ \ \overline{w}[i] \in T\}$, $A = \{w : w$ is a finite walk on G and the last vertex of w is in $T\}$

$\text{Ext}(w)$ is an event for every $w \in A$, and A is finite or countable.

Hence $\bigcup_{w \in A} \text{Ext}(w) = \Diamond T$ is an event. We call it a ***reachability event***.

Denote $\alpha[v, T]$ as the probability of reaching T if the walk starts at v.

Theorem: $\alpha[v, T] = \sum_{u \in N(v)} \pi(v, u) \cdot \alpha[u, T]$

Büchi set: $\text{Büchi}(T) = \Box \Diamond T = \{\overline{w} : \overline{w}$ is an infinite walk on $G, \exists i_0 < i_1 < \cdots \forall j, \overline{w}[i_j] \in T\}$

Theorem: $\text{Büchi}(T)$ is an event.

Proof: $A_k := \{w : w$ is a finite walk that visits T at least k times$\}$ is an event.

$B_k := \bigcup_{w \in A_k} \text{Ext}(w) = \{w : w$ is an infinite walk that visits T at least k times$\}$ is an event.

Hence $\text{Büchi}(T) = \bigcap_{i=1}^{\infty} B_i$ is an event.

Theorem: If $\pi(u, v) = q > 0$, then $P\left(\Diamond v \,|\, \text{Büchi}(u)\right) = 1$

Theorem: If $\pi(u, v) = q > 0$, then $P\left(\text{Büchi}(v) \,|\, \text{Büchi}(u)\right) = 1$

Theorem: If G is strongly connected, then $P\left(\text{Büchi}(v)\right) = 1 \ \forall v \in G$

Proof: Since $P(A \,|\, B) = 1 = \dfrac{P(A \cap B)}{P(B)} \implies P(A \cap B) = P(B) \implies P(A) \geq P(B)$

We have $P\left(\text{Büchi}(v)\right) \geq P\left(\text{Büchi}(u)\right)$. Therefore $P\left(\text{Büchi}(v)\right) = 1 \ \forall v \in G$.

Suppose G is not strongly connected, then it must be a DAG with each vertex being an SCC.

Bottom strongly conncected component (***BSCC***) is an SCC without any outgoing edges.

Theorem: $P\left(\text{Büchi}(v)\right) = \begin{cases} 0 & \text{if } u \text{ is not in a BSCC} \\ P\left(\Diamond T\right) & \text{if } u \in T \text{ and } T \text{ is a BSCC} \end{cases}$

VII. Game Theory

- Nim Games

We focus on games that are turn-based, finite, impartial, and have standard winning condition.

We can turn every state of such games into a vertex of a DAG $G = (V, E)$.

A state v is W if when we start at v, Player 1 wins. A state v is L if when we start at v, Player 2 wins.

We should have $W \sqcup L = V$.

G should have the following rules:

1) If v has no outgoing edges then $v \in L$
2) If $\exists u$ such that $(v, u) \in E$ and $u \in L$, then $v \in W$
3) If $\forall u$ such that $(v, u) \in E$ and $u \in W$, then $v \in L$

Nim game: We have n numbers $a_1, a_2, \dots, a_n \in \mathbf{N}$ and each player can choose a number and decrease it in their turn. The player who cannot make any move loses, and the other player wins.

Theorem: $L = \left\{ (a_1, a_2, \dots, a_n) : \bigoplus_{i=1}^{n} \left(a_i\right)_2 = 0 \right\}, W = \left\{ (a_1, a_2, \dots, a_n) : \bigoplus_{i=1}^{n} \left(a_i\right)_2 \neq 0 \right\}$

Proof: Check that

$$\bigoplus_{i=1}^{n} \left(a_i\right)_2 = 0 \implies \forall k, \forall a'_k < a_k, \left(\bigoplus_{i \neq k} \left(a_i\right)_2 \right) \oplus \left(a'_k\right)_2 \neq 0$$

$$\bigoplus_{i=1}^{n} \left(a_i\right)_2 \neq 0 \implies \exists k, \exists a'_k < a_k, \left(\bigoplus_{i \neq k} \left(a_i\right)_2 \right) \oplus \left(a'_k\right)_2 = 0$$

Denote $G_n := (V, E)$ where $V = \{1,2,\dots,n\}$ and $E = \{(i, j) : i > j\}$.

Theorem: For any Nim game $(a_1, a_2, \dots, a_n)$, we are playing on the graph $G_{a_1} \times G_{a_2} \times \cdots \times G_{a_n}$.

Every number in $(a_1, a_2, \dots, a_n)$ is also called a ***nimber***.

For any G_i, we assign a nimber to every $v \in G_i$ based on the following rules:

1) If v has no outgoing edges, then $\text{nim}(v) = 0$.
2) If v has edges to $u_1, u_2, \dots, u_k$, then let $\text{nim}(v) = \min\{i : i \in \mathbf{N}, i \neq \text{nim}(u_1), \text{nim}(u_2), \dots, \text{nim}(u_k)\}$.

Sprague-Grundy Theorem: For every finite impartial turn-based game, we have

$$L = \left\{ (v_1, v_2, \dots, v_n) : \bigoplus_{i=1}^{n} \left(\text{nim}(v_i)\right)_2 = 0 \right\}, W = \left\{ (v_1, v_2, \dots, v_n) : \bigoplus_{i=1}^{n} \left(\text{nim}(v_i)\right)_2 \neq 0 \right\}$$

- One-Shot Games

A ***one-shot game*** with n players consists of

1) a set S_i of ***strategies*** for player i
2) a set of ***payoff functions*** $u_i : S_1 \times S_2 \times \cdots \times S_n \to \mathbf{R}$

Each player i chooses a strategy $s_i \in S_i$ and the ***outcome*** is $s = (s_1, s_2, \dots, s_n)$

Every player is ***rational***, in other word, only interested in maximizing $u_i(s)$.

Prisoner's dilemma:

(p_1, p_2)	confess	silent
confess	(4,4)	(1,5)
silent	(5,1)	(2,2)

Denote $s_{\neg i} = (s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_n)$.

We say a strategy $s_i \in S_i$ is ***dominant*** if $\forall s_{\neg i} \forall s'_i,\ u_i(s_i, s_{\neg i}) \geq u_i(s'_i, s_{\neg i})$.

An outcome $s = (s_1, s_2, \ldots, s_n)$ is a ***pure Nash equilibrium*** if $\forall i\ \forall s_i' \in S_i,\ u_i(s_i, s_{\neg i}) \geq u_i(s_i', s_{\neg i})$.

Remark: Dominant strategy and pure Nash equilibrium sometimes don't exist.

A ***mixed strategy*** for player i is a probability function $\delta_i : S_i \to [0,1]$.

Δ_i is the set of mixed strategies of player i, and the outcome is $s = (s_1, s_2, \ldots, s_n)$ where $s_i \sim \delta_i$.

Every player is ***rational***, in other word, only interested in maximizing $E[u_i(s)]$.

We say $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in \Delta_1 \times \Delta_2 \times \cdots \times \Delta_n$ is a ***Nash Equilibrium*** if
$\forall i\ \forall \sigma_i',\ E[u_i(\sigma_i, \sigma_{\neg i})] \geq E[u_i(\sigma_i', \sigma_{\neg i})]$

Nash's Theorem: Any n-player game in which every S_i is finite has a mixed Nash equilibrium.

- Two-player Infinite-duration Games

An ***arena*** is a directed finite graph $G = (V, E, V_1, V_2)$ such that $\forall v \in V$, outdegree$(v) \geq 1$ and $V_1 \sqcup V_2 = V$

A ***two-player infinite-duration game*** is an arena $G = (V, E, V_1, V_2)$ and a starting vertex $v_0 \in V$

A ***strategy*** for player i is a funtion $\sigma_i : V^n \times V_i \to V$

An ***outcome*** is an infinite walk on G starting at v_0.

Denote O as the set of all outcomes. If σ_1, σ_2 are strategies for players, then $o(\sigma_1, \sigma_2) \in O$ is the corresponding outcome.

An ***objective*** for player i is a set $\mathrm{Obj}_i \subseteq O$.

A ***zero-sum game*** is a game that satisfies $\mathrm{Obj}_1 \sqcup \mathrm{Obj}_2 = O$

A game G is ***determined*** if for every starting vertex v_0, either p_1 or p_2 has a winning strategy.

A ***reachability game*** is a game such that: $\begin{cases} \mathrm{Obj}_1 = \Diamond T = \{\overline{w} \in O : \exists i\ \ \overline{w}[i] \in T\} \\ \mathrm{Obj}_2 = \Box(T^C) = \{\overline{w} \in O : \forall i\ \ \overline{w}[i] \in T^C\} \end{cases}$

Denote Win_i as the set of initial states from which player i has a winning strategy.

We need an algorithm that:
Input: An arena $G = (V, E, V_1, V_2)$ and a target set $T \subseteq V$
Output: $\mathrm{Win}_1, \mathrm{Win}_2$

which goes as follows: $\begin{cases} T_0 := T \\ T_{i+1} := T_i \cup \{v \in V_1 : \exists (v, u) \in E, u \in T_i\} \cup \{v \in V_2 : \forall (v, u) \in E, u \in T_i\} \end{cases}$

Theorem: $\begin{cases} \mathrm{Win}_1 = \bigcup T_i \\ \mathrm{Win}_2 = V \backslash \left(\bigcup T_i\right) \end{cases}$

Define $\mathrm{Attr}_1(T) := \bigcup T_i$

A ***Büchi game*** is a game such that $\begin{cases} \text{Obj}_1 = \text{Büchi}(T) = \square \lozenge T = \{\overline{w} \in O : \exists i_1 < i_2 < \cdots \forall j, \overline{w}[i_j] \in T\} \\ \text{Obj}_1 = \text{coBüchi}(T^C) = \lozenge \square T^C = \{\overline{w} \in O : \exists i,\ \forall j > i,\ \overline{w}[j] \in T^C\} \end{cases}$

We need an algorithm that:

Input: An arena $G = (V, E, V_1, V_2)$ and a target set $T \subseteq V$

Output: $\text{Win}_1, \text{Win}_2$

which goes as follows: $\begin{cases} G_0 := G & G_i := G_{i-1} - C_i \\ A_1 := \text{Attr}_1(T, G_0) & A_{i+1} := \text{Attr}_1(T, G_i) \\ C_1 := \text{Attr}_2(A_1^C, G_0) & C_{i+1} := \text{Attr}_2(A_{i+1}^C, G_i) \end{cases}$

Theorem: $\begin{cases} \text{Win}_1 = V \setminus \left(\bigcup C_i\right) \\ \text{Win}_2 = \bigcup C_i \end{cases}$