Discrete Structures

Logic Operators/Symbols

Conjunction	AND	$\wedge$
Disjunction	OR	$\vee$
Exclusive disjunction	XOR	$\oplus$
Implication	IF/THEN	$\rightarrow$
Biconditional	IFF	$\Leftrightarrow$

p `[operator]` q

p	q	$\wedge$	$\vee$	$\oplus$	$\rightarrow$	$\Leftrightarrow$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

Precedence of Operators

$() \; \neg \; \wedge \; \vee \oplus \; \rightarrow \Leftrightarrow$

Laws of propositional logic

Idempotent laws	$p \vee p \equiv p$	$p \wedge p \equiv p$
Associative laws	$(p \vee q) \vee r \equiv p \vee (q \vee r)$	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$
Commutative laws	$p \vee q \equiv q \vee p$	$p \wedge q \equiv q \wedge p$
Distributive laws	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
Identity laws	$p \vee F \equiv p$	$p \wedge T \equiv p$
Domination laws	$p \wedge F \equiv F$	$p \vee T \equiv T$
Double negation law	$\neg\neg p \equiv p$	
Complement laws	$p \wedge \neg p \equiv F$ $\neg T \equiv F$	$p \vee \neg p \equiv T$ $\neg F \equiv T$
De Morgan's laws	$\neg(p \vee q) \equiv \neg p \wedge \neg q$	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Conditional identities	$p \rightarrow q \equiv \neg p \vee q$	$p \Leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Rules of inference

p $p \rightarrow q$ $\therefore q$	Modus ponens
$\neg q$ $p \rightarrow q$ $\therefore \neg p$	Modus tollens
p $\therefore p \vee q$	Addition
$p \wedge q$ $\therefore p$	Simplification
p q $\therefore p \wedge q$	Conjunction
$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	Disjunctive syllogism
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	Resolution

Tree Method

Negate conclusion.
Stack $\wedge$. Split $\vee$.

Quantifiers

$\forall$ universal
$\exists$ existential

Quantifiers: De Morgan's laws

$\neg\forall x P(x) \equiv \exists x \; \neg P(x)$
$\neg\exists x P(x) \equiv \forall x \; \neg P(x)$

Quantifiers: Rules of inference

AE = arbitrary element
PE = particular element

c is AE/PE $\forall x P(x)$ $\therefore P(c)$	Universal instantiation
c is AE $\forall x P(c)$ $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore c$ is $PE \wedge P(c)$	Existential instantiation*
c is AE/PE $\forall x P(c)$ $\therefore \exists P(x)$	Existential generalization

Set Symbols

Set of naturals	$\mathbb{N}$
Set of integers	$\mathbb{Z}$
Set of rationals	$\mathbb{Q}$
Set of real numbers	$\mathbb{R}$
Empty set	$\varnothing$
Universal set	U
Cardinality of a set	$\lvert S \rvert$

Naïve Set Theory

- A set is an unordered collection of objects, called members or elements.
- A set can be an element of another set.
- The empty set $\varnothing$ contains no elements.
- No set can contain itself as a member, either directly or indirectly.

Set Membership	$x \in S$	x is a member of S
Negation of set membership	$x \notin S$	$\neg(x \in S)$

Subset	$A \subseteq B$	$\forall x : (x \in A \Rightarrow x \in B)$
Proper Subset	$A \subset B$	$\forall x : (x \in A \Rightarrow x \in B) \wedge (\exists x : x \in B \wedge x \notin A)$

Set Operations

Intersection	$A \cap B$	$\{x : x \in A \text{ and } x \in B\}$
Union	$A \cup B$	$\{x : x \in A \text{ or } B \text{ or both}\}$
Difference	$A - B$	$\{x : x \in A \text{ and } x \notin B\}$
Symmetric difference	$A \oplus B$	$\{x : x \in A - B \text{ or } x \in B - A\}$
Complement	$\overline{A}$ A^C	$\{x : x \notin A\}$
Cartesian Product	$A \times B$	$\{(a, b) : (a \in A) \wedge (b \in B)\}$
Power Set	$P(S)$	$\{X : X \subseteq S\}$

English expressions of the conditional operation

$p \rightarrow q$	If p then q (If p, q) q if p p implies q q whenever p p only if q p is sufficient for q q is necessary for p
$q \rightarrow p$	p is necessary for q p whenever q
$\neg q \rightarrow p$	p unless q

	$p \rightarrow q$
Converse	$q \rightarrow p$
Contrapositive	$\neg q \rightarrow \neg p$
Inverse	$\neg p \rightarrow \neg q$

Set identities

Idempotent laws	$A \cup A = A$	$A \cap A = A$
Associative laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Commutative laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Distributive laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity laws	$A \cup \varnothing = A$	$A \cap U = A$
Domination laws	$A \cap \varnothing = \varnothing$	$A \cup U = U$
Double complement law	$\overline{\overline{A}} = A$	
Complement laws	$A \cap \overline{A} = \varnothing$ $\overline{U} = \varnothing$	$A \cup \overline{A} = U$ $\overline{\varnothing} = U$
De Morgan's laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$

Relations

A relation R from domain A to B is a subset of $A \times B$.
A relation R over a set A is a subset of $A \times A$.

Properties of Relations

Reflexive	$\forall x \in A : (x, x) \in R$
Anti-Reflexive	$\forall x \in A : (x, x) \notin R$
Symmetric	$\forall x, y \in A : (x, y) \in R \Leftrightarrow (y, x) \in R$
Anti-Symmetric	$\forall x, y \in A : ((x, y) \in R \wedge (y, x) \in R) \Rightarrow (x = y)$
Transitive	$\forall x, y, z \in A : ((x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$
Equivalence	Reflexive, symmetric, and transitive

Closure Functions

Reflexive closure	$r(R) : r(R) \supseteq R$	$r(R) = R \cup I$
Symmetric closure	$s(R) : s(R) \supseteq R$	$s(R) = R \cup R^{-}$
Transitive closure	$t(R) : t(R) \supseteq R$	$t(R) = R \cup R^{+}$

I is the identity. R^{-} is the inverse of R.

Composing relations

Given two relations $R : A \to B$, $S : B \to C$, the composition $S \circ R : A \to C$ is defined as
$\{((a, c) : a \in A \wedge c \in C) \wedge (\exists\, b \in B : (a, b) \in R \wedge (b, c) \in S)\}$

If R is a relation over a set A, then:
$R \circ R = R^2 = \{(a, b) : \exists x \in A(a, x) \in R \wedge (x, b) \in R\}$

$R \circ (R \circ R) = R^3 = \{(a, b) : \exists x, y \in A(a, x) \in R \wedge (x, y) \in R \wedge (y, b) \in R\}$

In general: $(a, b) \in R^k$ iff there is a sequence of k flights from a to b.

Theorem: For any relation R over a set $A, |A| = n$,
$R^{+} = R \cup R^2 \cup R^3 \cup \cdots \cup R^n$

Corollary: If R is reflexive, then $R^{+} = R^n$ since
$R \subseteq R^2 \subseteq R^3 \cdots \subseteq R^n$

Functions

A function f from a domain A to a target B is a relation such that every domain element is mapped to exactly one element in the target.

- A function $f : A \to B$ is *one-to-one (injective)* if
$\forall x_1, x_2 \in A : (x_1 \neq x_2) \Rightarrow f(x_1) \neq f(x_2)$
"Every domain element is mapped to a unique element in the target."

- A function $f : A \to B$ is *onto (surjective)* if
$\forall y \in B\ \exists\, x \in A : f(x) = y$
"Every element in the target is the target of at least one domain element."

- A function $f : A \to B$ is a *one-to-one correspondence (bijective)* if f is both injective and surjective.
"Every domain element is matched with exactly one element in the target, and vice versa."

Composition of functions

f and g are two functions, where $f : X \to Y$ and $g : Y \to Z$. The composition of g with f is the function $(g \circ f) : X \to Z$, such that $\forall x \in X, (g \circ f)(x) = g(f(x))$.
$f \circ g \circ h = (f \circ g) \circ h = f \circ (g \circ h) = f(g(h(x)))$
Identity function $(I_A : A \to A)$ is defined as $I_A(a) = a,\ \forall a \in A$.

Pigeonhole principle: If $k + 1$ pigeons occupy k pigeonholes, then at least two pigeons share a pigeonhole.
No function from a domain of size $k + 1$ to a target of size k is injective.

Well-ordering principle: Every non-empty subset of $\mathbb{N}$ has a least element.

Theorem: The pigeonhole principle is logically equivalent to the well-ordering principle.

Uncountability

- $|\mathbb{N}| = |\mathbb{Z}|$
- A set S is *countable* if there is an injective function $f : S \to \mathbb{N}$.
  - Every finite set is countable.
  - Every subset of $\mathbb{N}$ is countable.
- A set S is *countably infinite* if there is a bijective function $f : \mathbb{N} \to S$.
  - $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are countably infinite.
  - Theorem: If A, B are countable sets, then $A \times B$ is countable. ($\mathbb{N} \times \mathbb{N}$ is countable.)
- $\mathbb{R}$ is uncountable.
- If a finite set S has m elements, then $P(S)$ has $2^m > m$ elements.
  - $P(\mathbb{N})$ is infinite and not countable.
  - For every set S, $|S| < |P(S)|$.
- The Infinite Hierarchy of Infinite Sets:

N	$P(N)$	$P(P(N))$	$P(P(P(N)))$	$\cdots$
$\aleph_0$	$\aleph_1$	$\aleph_2$	$\aleph_3$	$\cdots$

$|P(N)| = |\mathbb{R}|$

Proofs

- Direct proofs
- Induction
  - **CLAIM:** $P(n)$
  - **BASIS:** $P(0)$ is true
  - **INDUCTIVE HYPOTHESIS:** For some $k \geq 0, P(k)$
  - **INDUCTIVE STEP:** $P(k) \Rightarrow P(k+1)$
- Strong Induction
  - **CLAIM:** $P(n)$
  - **BASE CASES:** $P(x_1), P(x_2), \cdots$ are true
  - **INDUCTIVE HYPOTHESIS:** $\forall i, 0 \leq i \leq k\ P(k)$
  - **INDUCTIVE STEP:** $(\forall i \leq k : P(i)) \Rightarrow P(k+1)$
- Contrapositive
  - Prove $p \to c$ by showing that $\neg\, c \to \neg\, p$.
- Contradiction
  - Prove t is true by first assuming $\neg\, t$ is true and reaching the conclusion $r \wedge \neg\, r$, for some proposition r.
- Proof by cases (e.g. When x is odd..., when x is even...)

Number Theory

- **Divisibility Lemma**
  1. $a|b \Rightarrow \forall c : a|bc$
  2. $a|b \wedge b|c \Rightarrow a|c$
  3. $a|b \wedge a|c \Rightarrow \forall s, t \in \mathbb{Z} : a|(sb + tc)$
  4. $\forall c \neq 0 : a|b \Leftrightarrow ca|cb$
- **Division Theorem**
  $\forall n, d \in \mathbb{Z}$ where $d > 0, \exists$ a unique pair $q, r \in \mathbb{Z}$ such that $n = qd + r,\ 0 \leq r < d$.
- **GCD Theorem:** The smallest positive linear combination m of two integers a, b (at least one of which is non-zero) equals $g = gcd(a, b)$.
  Lemma: An integer is a linear combination of a, b if and only if it is a multiple of $gcd(a, b)$.
- **GCD Lemma**
  1. $\forall c \in \mathbb{Z} : (c|a \wedge c|b \Rightarrow c|gcd(a, b)$
  2. $\forall k > 0 : gcd(ka, kb) = k \cdot gcd(a, b)$
  3. $(gcd(a, b) = 1 \wedge gcd(a, c) = 1) \Rightarrow gcd(a, bc) = 1$
  4. $(a|bc \wedge gcd(a, b) = 1) \Rightarrow a|c$
  5. $gcd(a, b) = gcd(b, rem(a, b))$,
     where $rem(a, b)$ is the remainder on dividing a by b.
- **Fundamental Theorem of Arithmetic:** Every number greater than 1 is uniquely expressed as a product of primes. The natural number $p > 1$ is prime if $\forall n < p, gcd(n, p) = 1$.
- **Congruence modulo m**
  Definition: Integers a, b are congruent modulo m iff $m|a - b$.
  Notation: $a \equiv b\ (mod\ m)$
  Theorem: $a \equiv b\ (mod\ m) \Leftrightarrow rem(a, m) = rem(b, m)$
  Lemma: Congruence mod m is an equivalence relation.
  The following properties hold for every $m \in \mathbb{N}^+$
  1. $a \equiv a\ (mod\ m)$ - Reflexive
  2. $a \equiv b\ (mod\ m) \Rightarrow b \equiv a\ (mod\ m)$ - Commutative
  3. $a \equiv b\ (mod\ m) \wedge b \equiv c\ (mod\ m) \Rightarrow a \equiv c\ (mod\ m)$ - Transitive
- **Modular Arithmetic**
  Rules
  - $[x + y]\ mod\ m = [(x\ mod\ m) + (y\ mod\ m)]\ mod\ m$
  - $[x \cdot y]\ mod\ m = [(x\ mod\ m)(y\ mod\ m)]\ mod\ m$
  - $x^a\ mod\ m = (x\ mod\ m)^a$

  Lemma
  1. $a \equiv b\ (mod\ m) \Rightarrow a + c \equiv b + c\ (mod\ m)$
  2. $a \equiv b\ (mod\ m) \Rightarrow a \cdot c \equiv b \cdot c\ (mod\ m)$
  3. $a \equiv b\ (mod\ m) \wedge c \equiv d\ (mod\ m) \Rightarrow a + c \equiv b + d\ (mod\ m)$
  4. $a \equiv b\ (mod\ m) \wedge c \equiv d\ (mod\ m) \Rightarrow a \cdot c \equiv b \cdot d\ (mod\ m)$

  Theorem:
  If $a \cdot c \equiv b \cdot c\ (mod\ m)$ and $gcd(c, m) = 1$, then $a \equiv b\ (mod\ m)$
- **Modular inverses**
  Definition: If $a \cdot x \equiv 1\ (mod\ m)$ then we say that x is the inverse of a modulo m. (Note: $a, x \in \mathbb{Z}_m$)
  Notation: $x \equiv a^{-1}\ (mod\ m)$.
  $x \equiv a^{-1}\ (mod\ m)$ also means that $a \equiv x^{-1}\ (mod\ m)$
  Theorem: If $gcd(a, m) = 1$ then $a^{-1}\ (mod\ m)$ exists.
  Corollary: If m is prime then every non-zero element in $\mathbb{Z}_m$ has an inverse.
- **Fermat's Last Theorem:** There are no non-zero integer solutions to $a^n + b^n = c^n$ for $n \geq 3$.
- **Fermat's Little Theorem:** If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1\ (mod\ p)$
- **Euler's Totient Function**
  Definition: Euler's totient function $\Phi(n)$ = number of numbers in $[1, n]$ relatively prime to n.
  Lemma:
  1. If p is prime, then $\Phi(p) = p - 1$.
  2. If p, q are primes, then $\Phi(pq) = (p-1)(q-1) = \Phi(p)\Phi(q)$.
- **Euler's Generalization of Fermat's Little Theorem**
  If $gcd(a, n) = 1$ then $a^{\Phi(n)} \equiv 1\ (mod\ n)$.
- **Euclidean Algorithm**
  $gcd(a, b) = r_n$

y	x	r = y mod x
a	b	r_1
b	r_1	r_2
r_1	r_2	r_3
r_{n-2}	r_{n-1}	r_n
r_{n-1}	$\boldsymbol{r_n}$	0

- **Extended Euclidean Algorithm:** Expresses $gcd(a, b)$ as a linear combination of a and $b : gcd(a, b) = sa + tb$.
  $r = y\ mod\ x$
  $r = y - (y\ div\ x) \cdot x$ (div represents integer division)

  $r_1 = a - (a\ /\ b) \cdot b$
  $r_2 = b - (b\ /\ r_1) \cdot r_1$
  $r_3 = r_1 - (r_1\ /\ r_2) \cdot r_2$
  ...
  $r_n = r_{n-2} - (r_{n-2}\ /\ r_{n-1}) \cdot r_{n-1}$

  Rewrite $r_{n-2} - (r_{n-2}\ /\ r_{n-1}) \cdot r_{n-1} \rightarrow sa + tb$.
- **Chinese Remainder Theorem**
  If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, the system:
  $$\begin{aligned} x &\equiv a_1\ (mod\ m_1) \\ x &\equiv a_2\ (mod\ m_2) \\ &\cdots \\ x &\equiv a_n\ (mod\ m_n) \end{aligned}$$
  has a *unique* solution modulo $m = m_1 \cdot m_2 \cdots m_n$.
  To solve, construct:
  - $m = m_1 \cdot m_2 \cdots m_n$
  - $M_i = \frac{m}{m_i}$
  - $y_i \equiv M_i^{-1}\ (mod\ m_i)$
  - $X_i = a_i y_i M_i$

  Then: $x \equiv X_1 + X_2 + \cdots X_n\ (mod\ m)$
- **RSA Cryptosystem**
  1. Select two large prime numbers, p and q.
  2. Compute $N = pq$ and $\Phi = (p-1)(q-1)$.
  3. Find integer $e \rightarrow gcd(e, \Phi) = 1$.
  4. Compute integer $d \rightarrow (ed\ mod\ \Phi) = 1$.
  5. Public (encryption) key: N and e.
  6. Private (decryption) key: d.

  $c = m^e\ mod\ N$ (encryption)
  $m = c^d\ mod\ N$ (decryption)
  Validity of the RSA cryptosystem:
  $$\begin{aligned} &c^d\ mod\ N \\ &= (m^e\ mod\ N)^d\ mod\ N \\ &= m^{e \cdot d}\ mod\ N \\ &= m^{1+k\Phi}\ mod\ N \\ &= (m \cdot m^{k\Phi})\ mod\ N \\ &= (m \cdot 1)\ mod\ N \\ &= m \end{aligned}$$

Exponent rules

$$a^m \cdot a^n = a^{m+n}$$
$$\frac{a^m}{a^n} = a^{m-n}$$
$$(a^m)^n = a^{mn}$$
$$(ab)^m = a^m b^m$$

Graph Theory

- **Vertex:** Node
  - **Adjacent vertices:** Two vertices with an edge between them.
  - Vertices A and B are the **endpoints** of edge $\{A, B\}$. The edge $\{A, B\}$ is **incident** to vertices A and B.
  - Vertex A is a **neighbor** to vertex B if $\{A, B\}$ or $\{B, A\}$ exists.
- **Degree of a vertex:** The number of edges incident to a vertex (the number of neighbors a vertex has).
  - **Total degree:** The sum of the degrees of all of the vertices.
  - **Outdegree of $v(deg^+(v))$:** # of outgoing edges; edges with v as initial node.
  - **Indegree of $v(deg^-(v))$:** # of incoming edges; edges with v as end node.
- **Edge:** A set of two nodes; a line connecting two nodes together.
  - **Undirected edge:** $\bullet - - - - - \bullet$
  - **Directed edge:** $\bullet - - - \rightarrow \bullet$
  - **Parallel edges:** Multiple edges between the same pair of vertices.
  - **Self-loop:** An edge between a vertex and itself.
- **Walk:** A sequence of alternating vertices and edges that starts and ends with a vertex.
  - **Open walk:** First and last vertices are not the same.
  - **Closed walk:** First and last vertices are the same.
  - **Length of a walk:** The number of edges in the walk.
- **Trail:** A walk in which no edge is repeated.
- **Circuit:** A closed walk in which no edge is repeated.
- **Path:** A trail in which no vertex is repeated.
- **Cycle:** A circuit of length ≤ 1 with the same first and last vertices and no repeated vertex.
- **Eulerian Trail/Circuit:** A trail/circuit that traverses every edge exactly once.
- **Undirected graph:** Edges are unordered pairs of vertices.
- **Directed graph:** Edges are ordered pairs of vertices.
  - $G = (V, E)$
    - V is a set of vertices.
    - $E \subseteq V \times V$ is a set of directed edges, where each edge is an ordered pair $(u, v) : u, v \in V$.
  - $\sum_{v \in V} deg^{+/-}(v) = |E|$
  - $\sum_{v \in V} deg(v) = 2 \cdot |E|$
- **Simple graph:** A graph that does not have parallel edges or self-loops.
- **Regular graph:** All vertices have the same degree.
  - ***D*-regular graph:** All vertices have degree d.
- **Strongly connected graph:** A directed graph where there is a directed path from every node to every other node.
- **Directed Acyclic Graph (DAG):** A directed graph with no cycles.
  - If $G = (V, E)$ is a DAG, then G has a node with indegree 0 and has a topological ordering.
- **K_n :** A complete graph on n vertices. A complete graph has an edge between every pair of vertices.
- **C_n :** A cycle on n vertices; well-defined only for $n \geq 3$.
- **$K_{n,m}$:** A graph on $n + m$ vertices. The vertices are divided into 2 sets: one with m vertices and one with n vertices. There are no edges between vertices in the same set, but there is an edge between every vertex in one set and every vertex in another set.
- **Eulerian Circuits/Trails**
  An undirected graph G has an Euler circuit iff it is connected and every vertex in G has even degree.
  An undirected graph G has an Euler trail iff G is connected and has exactly two vertices with odd degree.
- **Trees**
  Tree: A connected acyclic graph.
  Leaves of a tree: Vertices with degree 1.
  Observations:
  1. Every connected subgraph of a tree T is also a tree.
  2. There is a unique path between every pair of vertices.
  3. Adding an edge between any two nonadjacent vertices in a tree creates a cycle.
  4. Removing any tree edge disconnects some pair of vertices.
  5. Every tree with at least two vertices contains at least two leaves.
  6. Every tree with n vertices has $n - 1$ edges.

  Full binary trees
  - Every vertex is either a leaf or has exactly 2 children.
  - THEOREM: A full binary tree has n leaves and $n - 1$ non-leaves.
  - LEMMA: Some two siblings are both leaves.
- **Map Coloring**
  - Four-Color Theorem: At most 4 colors are required to color a map such that no adjacent regions share the same color.
  - For maps with non-contiguous states, 5 colors may be necessary.
- **Planar Graphs:** A graph is planar if it can be drawn on the plane without crossing edges.
  1. Each edge lies once on the boundary of 2 regions, or twice on the boundary of 1 region.
  2. Therefore, X = sum of the # of edges of every region boundary $= 2m$.
  3. Also, since each region has 3 or more bounding edges, if the number of vertices is at least 3: $X \geq 3r$.
  4. Therefore, $2m \geq 3r$ for every connected planar graph with at least 3 vertices.
  5. In general, if every cycle has length c or greater, than $2m \geq cr$.

  - **Euler's Formula**
    Theorem: For every connected planar graph with n vertices, m edges, and r regions: $n - m + r = 2$.
    Corollary: The number of regions in all drawings of a planar graph is invariant.
  - **Planar graphs have few edges**
    Theorem: For every connected graph G with $n \geq 3$ vertices: $m \leq 3n - 6$.
    Corollary 1: K_5 is not planar.
    Corollary 2: $K_{3,3}$ is not planar.
  - **Five-Color Theorem:** Every planar graph can be colored with 5 or fewer colors.