1 Number Theory

1.1 FTA

$$n = p_1^{e_1} \cdots p_r^{e_r}$$

1.2 The Well-Ordering Property

$$\emptyset \neq S \subseteq \mathbb{N} \Rightarrow \min S \in S$$

1.3 Division Algorithm

$$a = bq + r \quad 0 \leq r < b \text{ for unique } q, r$$

1.4 Ideal of $\mathbb{Z}$

A nonempty set $I \subseteq \mathbb{Z}$ such that

$$a, b \in I \Rightarrow a + b \in I$$
$$a \in I, r \in \mathbb{Z} \Rightarrow ra \in I$$
$$I \text{ is an ideal of } \mathbb{Z} \Leftrightarrow I = d\mathbb{Z}$$
$$I_1 + I_2 = \{x + y : x \in I_1, y \in I_2\}$$
$$a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\mathbb{Z}$$

1.5 Great Common Divisor

$$\gcd(a, b) = as + bt$$

1.6 Euler's Phi Function

$$\Phi(n) = |\mathbb{Z}_n^*|, \forall n \in \mathbb{Z}^+$$

If $n = p_1^{e_1} \cdots p_r^{e_r}$, then

$$\Phi(n) = \Phi(p_1^{e_1}) \cdots \Phi(p_r^{e_r}) = n(1 - p_1^{-1}) \cdots (1 - p_r^{-1})$$

If $n = pq$, then

$$\Phi(n) = (p - 1)(q - 1)$$

1.7 The Set $\mathbb{Z}_n$ and $\mathbb{Z}_n^*$

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$$
$$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n : \gcd(a, n) = 1\}$$

1.8 Euler's Theorem

Let $n \geq 1$ and $\alpha \in \mathbb{Z}_n^*$, then $\alpha^{\Phi(n)} = 1$

1.9 Fermat's Little Theorem

If p is a prime and $\alpha \in \mathbb{Z}_p$, then $\alpha^{p-1} = 1$

1.10 Wilson's Theorem

If p is a prime, then $(p - 1)! \equiv -1 \pmod{p}$

2 Cryptography

2.1 RSA

$(pk, sk) \leftarrow \mathbf{Gen}(1^n)$:
Choose two n-bit primes $p \neq q$, $N = pq$
Choose e, d s.t. $0 \leq e, d < \Phi(N)$, $\gcd(e, \Phi(N)) = 1$
$d = e^{-1} \bmod \Phi(N)$
output $pk = (N, e), sk = (N, d)$

$c \leftarrow \mathbf{Enc}(pk, m)$:
output $c = m^e \bmod N, 0 \leq c < N$

$m \leftarrow \mathbf{Dec}(sk, c)$:
output $m = c^d \bmod N, 0 \leq m < N$

2.2 Arithmetic Operations

$$a = (a_{k-1} \cdots a_1 a_0)_2,\ b = (b_{l-1} \cdots b_1 b_0)_2$$
$$\ell(a) = \begin{cases} \lfloor \log_2(|a|) \rfloor + 1, & a \neq 0, \\ 1, & a = 0 \end{cases}$$
$$k = \ell(a), l = \ell(b)$$

Addition & Subtraction $a + b$ or $a - b$: $O(k)$
Multiplication $a * b$: $O(k^2)$
Division a/b: $O((k - l + 1) \cdot l)$
Arithmetic Module N $(a \pm b) \bmod N$: $O(\ell(N))$, $(ab) \bmod N$: $O(\ell(N)^2)$
Square-and-Multiply
Square $x_0 = a$

$$x_{k-1} = x_{k-2}^2 \bmod N = a^{2^{k-1}} \bmod N$$

Multiply $a^e \bmod N = (x_0^{e_0} \cdot x_1^{e_0} \cdots x_{k-1}^{e_0}) \bmod N$

2.3 EA

Compute $d = \gcd(a, b)$

2.4 EEA

Compute $d = \gcd(a, b) = as + bt$: $O(\ell(a)\ell(b))$

2.5 Prime Number Theorem

For $x \in \mathbb{R}^+, \pi(x) = \sum_{p \leq x}$ Numbers of primes

$$|\mathbb{P}_n| \geq \frac{2^n}{n \ln 2}(\frac{1}{2} + O(\frac{1}{n})) \text{ when } n \to \infty$$

2.6 Linear Congruence Equation

$$ax \equiv b \pmod{n}$$

2.7 CRT

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ \vdots \\ x \equiv b_k \pmod{n_k} \end{cases}$$

Let $N_i = n/n_i$ for every $i \in [k]$, $\exists s_i, t_i, N_i s_i + n_i t_i = 1$
Let $b = b_1 N_1 s_1 + \cdots + b_k N_k s_k$, then

$$x \equiv b \pmod{n}$$

2.8 DLOG & CDH

$f_{\text{DLOG}}(q, G, g; h) = \log_g h$, $f_{\text{CDH}}(q, G, g; A, B) = g^{ab}$

2.9 Diffie-Hellman Key Exchange

Alice: $a \leftarrow \mathbb{Z}_q, A = g^a$, send (q, G, g, A) to Bob
Bob: $b \leftarrow \mathbb{Z}_q, B = g^b$, send B to Alice; output $k = A^b$
Alice: output $k = B^a$

3 Group Theory

3.1 Group

Closure $\forall a, b \in G, a \star b \in G$
Associative $\forall a, b, c \in G, a \star (b \star c) = (a \star b) \star c$
Identity $\exists e \in G, \forall a \in G, a \star e = e \star a = a$
Inverse $\forall a \in G, \exists b \in G, a \star b = b \star a = e$
Commutative (Abelian Group) $\forall a, b \in G, a \star b = b \star a$

3.2 Field

$(\mathbb{F}, +, \cdot)$

3.3 Polynomial

Let $f(X) = f_t X^t + \cdots + f_1 X + f_0 \in \mathbb{Z}_p[X]$ and $\alpha \in \mathbb{Z}_p$, then $\exists q(X) = q_{t-1} X^{t-1} + \cdots + q_0 \in \mathbb{Z}_p[X]$ s.t.

$$f(X) = (X - \alpha)q(X) + f(\alpha)$$
$$q_{t-1} = f_t$$
$$q_{t-2} = f_{t-1} + f_t \alpha$$
$$\vdots$$
$$q_0 = f_1 + f_2 \alpha + \cdots + f_t \cdot \alpha^{t-2}$$

$f(X) \in \mathbb{Z}_p[X]$ has $\leq \deg(f)$ roots in $\mathbb{Z}_p$

3.4 Order

The order of a group G is the cardinality of G.
When $|G| < \infty, \forall a \in G$, the order of a is the least integer $l > 0$ s.t. $a^l = 1$ ($la = 0$ for additive group)
$\forall a \in G, a^{|G|} = 1$

3.5 Cyclic Group

Abelian group $(G, \cdot)$ is a cyclic group if $\exists g \in G$ s.t. $G = \langle g \rangle$

4 Combinatorics

4.1 Functions

Let $A, B \neq \emptyset$ be two sets. A function(map) $f : A \to B$ assigns a unique element $b \in B$ for all $a \in A$
injective $f(a) = f(b) \Rightarrow a = b$
surjective $f(A) = B$
bijective injective and surjective

4.2 Cantor's Diagonal Argument

$$|A| \neq |\mathbb{Z}^+|$$

4.3 Cantor's Theorem

Let A be any set, then $|A| < |\mathcal{P}(A)|$

4.4 The Halting Problem

There is no Turing machine computing

$$\mathbf{HALT}(P, I) = \begin{cases} \text{“halts”} & \text{if } P(I) \text{ halts;} \\ \text{“loops forever”} & \text{if } P(I) \text{ loops forever.} \end{cases}$$

4.5 Countable an Uncountable

A set A is countable if $|A| < \infty$ or $|A| = |\mathbb{Z}^+|$;
otherwise, it is said to be uncountable

4.6 Schröder-Bernstein Theorem

If $|A| \leq |B|$ and $|B \leq |A|$, then $|A| = |B|$
$\aleph_0 = |\mathbb{Z}^+| < |\mathcal{P}(\mathbb{Z}^+)| = 2^{\aleph_0} = |[0, 1)| = |(0, 1)| = |\mathbb{R}| = c$

4.7 Permutations of Set

An n-element set has $P(n, r) = \dfrac{n!}{(n - r)!}$ and has n^r different r-permutations with repetition.

4.8 Combinations of Set

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

of r-combinations of an n element set with repetition,
of natural number solutions of the equation
$x_1 + x_2 + \cdots + x_n = r$ are $\binom{n+r-1}{r}$

4.9 Multiset
$A = \{n_1 \cdot a_1, n_2 \cdot a_2, \ldots, n_k \cdot a_k\}$ is an $(n_1+n_2+\cdots n_k)$-multiset

4.10 Permutations of Multiset
A has exactly $\frac{(n_1+n_2+\cdots+n_k)!}{n_1!n_2!\cdots n_k!}$ permutations

4.11 Combination of Multiset
An r-subset(multiset) of A is r-combination of A

4.12 Shortest Path
of shortest paths from $(0,0)$ to (p,q) is $\frac{(p+q)!}{p!q!}$

4.13 T-Route
There is a T-route from $A=(a,\alpha)$ to $B=(b,\beta)$ only if
(1) $b > a$; (2) $b-a \geq |\beta-\alpha|$ (3) $2 \mid (b+\beta-a-\alpha)$

4.14 Numbers of T-Routes
of T-routes from $A=(a,\alpha)$ to $B=(b,\beta)$ is
$$\frac{(b-a)!}{(\frac{b-a}{2}+\frac{\beta-\alpha}{2})!(\frac{b-a}{2}-\frac{\beta-\alpha}{2})!}$$
# of T-routes that intersect the x-axis is
$$\frac{(b-a)!}{(\frac{b-a}{2}+\frac{\beta+\alpha}{2})!(\frac{b-a}{2}-\frac{\beta+\alpha}{2})!}$$

4.15 Solution of Bertrand's Ballot Problem
The sequence $x_1 x_2 \ldots x_{2n}$ is a ballot
The probability that A never trials B is $p_n = C_n / \binom{2n}{n}$

4.16 Catalan Number
of solutions of the equation system
$$\begin{cases} x_1 + x_2 + \cdots + x_{2n} = n \\ x_1 + x_2 + \cdots + x_i \leq i/2, i = 1, 2, \ldots, 2n-1 \\ x_i \in \{0,1\}, i = 1, 2, \ldots, 2n \end{cases}$$
$$C_n = \frac{(2n)!}{n!(n+1)!}$$

4.17 Inverse Binomial Transform
The binomial transform of $\{a_n\}_{n\geq s}$ is $\{b_n\}_{n\geq s}$ s.t.
$$b_n = \sum_{k=s}^{s} \binom{n}{k} a_k$$
The inverse binomial transform of $\{b_n\}_{n\geq s}$ is $\{a_n\}_{n\geq s}$ s.t.
$$a_n = \sum_{k=s}^{s} (-1)^{n-k} \binom{n}{k} b_k$$

4.18 Distribution Problems
Type 1 n labeled $\to$ k labeled: $|S| = k^n$
$n \to i$: $N_1 = \frac{n!}{n_1!n_2!\cdots n_k!}$

Type 2 n unlabeled $\to$ k labeled: $|S| = \binom{n+k-1}{n}$

Type 3 n labeled $\to$ k unlabeled: $|S| = \sum_{j=1}^{k} S_2(n,j)$

Type 4 n unlabeled $\to$ k unlabeled: $|S| = \sum_{j=1}^{k} p_j(n)$

4.19 Stirling number of the second kind $S_2(n,j)$
$$S_2(n,j) = \frac{1}{j!}\sum_{i=0}^{j-1}(-1)^i \binom{j}{i}(j-i)^n \text{ when } n \geq j \geq 1$$
$$S_2(n,j) = S_2(n-1,j-1) + jS_2(n-1,j)$$

4.20 Partitions of Integers
For $n \in \mathbb{Z}^+$, $p_j(n+j) = \sum_{k=1}^{j} p_k(n)$,
$$p_k(n) = p_{k-1}(n-1) + p_k(n-k)$$

4.21 Characteristic Roots
Characteristic equation: $r^k - c_1 r^{n-1} - c_2 r^{n-2} - \cdots - c_k = 0$

4.22 LHRR
$a_n = \sum_{i=1}^{k} c_i a_{n-i}$, where $n \geq k, \{c_i\}_{i=1}^{k}$ are constants, $c_k \neq 0$

No multiple roots $\{r_1, \ldots, r_k\}$: $x_n = \sum_{j=1}^{k} \alpha_j r_j^n$

Multiple roots $\{m_1 \cdot r_1, \ldots m_t \cdot r_t\}$: $x_n = \sum_{j=1}^{t}(\sum_{\ell=0}^{m_j-1} \alpha_{j,\ell} n^\ell) r_j^n$

4.23 LNRR
$a_n = \sum_{i=0}^{k} c_i a_{n-i} + F(n), \{c_i\}_{i=1}^{k}$ are constants, $c_k, F(n) \neq 0$

Particular Solutions
$F(n) = (f_l n^l + \cdots + f_1 n + f_0) s^n = f(n) s^n$
s: a root of characteristic equation, m: multiplication of s
$$x_n = (p_l n^l + \cdots + p_1 n + p_0) s^n n^m$$
General Solutions
Particular solution of LNRR + General solution of the associated LHRR

4.24 Generating Function
$$A(x) = \sum_{r=0}^{\infty} a_r x^r, B(x) = \sum_{r=0}^{\infty} b_r x^r$$
$$A(x) \pm B(x) = \sum_{r=0}^{\infty}(a_r \pm b_r)x^r, A(x) \cdot B(x) = \sum_{r=0}^{\infty}(\sum_{j=0}^{r} a_j b_{r-j}) x^r$$
$A(x)$ has an inverse iff $a_0 \neq 0$.

4.25 $(1+\alpha x)^u$
The extended binomial coefficient
$$\binom{u}{n} = \begin{cases} u(u-1)\cdots(u-n+1)/n! & n > 0 \\ 1 & n = 0 \end{cases}$$
Let x be a real number with $|x| < 1$,
$$(1+x)^u = \sum_{r=0}^{\infty} \binom{u}{r} x^r$$

4.26 Counting Combinations with GFs
$a_r = |\{(r_1, \ldots, r_n) : r_i \in R_i, r_1 + \cdots + r_n = r\}|$
$$\sum_{r=0}^{\infty} a_r x^r = \prod_{i=1}^{n} \sum_{r_i \in R_i} x^{r_i}$$

4.27 Counting Permutations with GFs
$a_r = \sum_{r_1 \in R_1, \ldots, r_n \in R_n, r_1+\cdots r_n = r} \frac{r!}{r_1! \cdots r_n!}$
$$\sum_{r=0}^{\infty} \frac{a_r}{r!} x^r = \prod_{i=1}^{n} \sum_{r_i \in R_i} \frac{x^{r_n}}{r_n!}$$

4.28 Partial Fraction Decomposition
Let $Q(x), P(x)$ be two polynomial s.t. $\deg(Q) > \deg(P)$. If $Q(x) = (1-r_1 x)^{m_1} \cdots (1-r_t x)^{m_t}$ for distinct non-zero numbers $r_1, \ldots, r_t$ and integers $m_1, \ldots, m_t \geq 1$, then there exist unique coefficients $\{\alpha_{j,u} : j \in [t], u \in [m_j]\}$ such that
$$\frac{P(x)}{Q(x)} = \sum_{j=1}^{t}\sum_{u=1}^{m_j} \frac{\alpha_{j,u}}{(1-r_j x)^u}$$

4.29 Principle of IE
Let S be a finite set, $A_1, A_2, A_n \subseteq S$, then
$$|\bigcup_{i=1}^{n} A_i| = \sum_{t=1}^{n}(-1)^{t-1} \sum_{1 \leq i_1 < \cdots < i_t \leq n} |A_{i_1} \cap \cdots \cap A_{i_t}|$$
$$|\bigcap_{i=1}^{n} A_i| = \sum_{t=1}^{n}(-1)^{t-1} \sum_{1 \leq i_1 < \cdots < i_t \leq n} |A_{i_1} \cup \cdots \cup A_{i_t}|$$

4.30 Cover
A cover of a finite set A is a family $\{A_1, A_2, \ldots A_n\}$ of subsets of A such that $\bigcup_{i=1}^{n} A_i = A$.

4.31 Pigeonhole Principle
Let A be a set with $\geq N$ elements. Let $\{A_1, A_2, \ldots, A_n\}$ be a cover of A, then $\exists k \in [n], |A_k| \geq \lceil N/n \rceil$.

5 Propositional Logic

5.1 Logical Operators

p	$\neg p$
T	F
F	T

p	q	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

5.2 From Natural Language to WFFs

Introduce symbols $p, q, r, \dots$ to represent simple propositions
Connect the symbols with logical connecitves to obtain WFFs

5.3 Type of WFFs

Tautology: truth value is **T** for all truth assignment
Contradiction: truth value is **F** for all truth assignment
Contingency: neither tautology or contradiction
Satisfiable: is true for at least one truth assignment

5.4 Proving $A \equiv B$

(1) $A^{-1}(\mathbf{T}) = B^{-1}(\mathbf{T})$ (2) $A^{-1}(\mathbf{F}) = B^{-1}(\mathbf{F})$
(3) $A \leftrightarrow B$ is a tautology

5.5 Logical Equivalences

$P \vee Q \equiv Q \vee P$	Commutative Laws
$P \wedge Q \equiv Q \wedge P$	
$P \vee (Q \vee R) \equiv (P \vee Q) \vee R$	Associative Laws
$P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R$	
$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$	Distributive Laws
$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$	
$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$	De Morgan's Laws
$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$	
$P \vee (P \wedge Q) \equiv P$	Absorption Laws
$P \wedge (P \vee Q) \equiv P$	
$P \to Q \equiv \neg P \vee Q$	Laws Involving
$P \to Q \equiv \neg Q \to \neg P$	Implication
$(P \to R) \wedge (Q \to R) \equiv (P \vee Q) \to R$	$\to$
$P \to (Q \to R) \equiv (P \wedge Q) \to R$	
$P \to (Q \to R) \equiv Q \to (P \to R)$	
$P \leftrightarrow Q \equiv (P \to Q) \wedge (Q \to P)$	Laws Involving
$P \leftrightarrow Q \equiv (\neg P \vee Q) \wedge (P \vee \neg Q)$	Bi-Implication
$P \leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$	$\leftrightarrow$
$P \leftrightarrow Q \equiv \neg P \leftrightarrow \neg Q$	

5.6 Proving $A \Rightarrow B$

(1) $A^{-1}(\mathbf{T}) \subseteq B^{-1}(\mathbf{T})$
(2) $B^{-1}(\mathbf{F}) \subseteq A^{-1}(\mathbf{F})$
(3) $A \to B$ is a tautology
(4) $A \wedge \neg B$ is a contradiction

5.7 Argument

Conclusion: the final propositions
Premises: all the other propositions
Valid: the truth of premises implies that of the conclusion
Proof: valid and establishes the truth of a conclusion

5.8 Building Arguments

Premise: Introduce the given formulas $P_1, \dots, P_n$ in the process of constructing proofs
Conclusion: Quote the intermediate formula that have been deducted.
Rule of replacement: Replace a formula with a logically equivalent formula.
Rule of Inference: Deduct a new formula with a tautological implication.
Rule of substitution: Deduct a formula from a tautology.

6 Predicate Logic

6.1 From Natural Language to WFFs

$\forall x(P(x) \to Q(x))$ $\exists x(P(x) \wedge Q(x))$

6.2 Type of WFFs

A WFF is **logically valid** if it is **T** in every interpretation
A WFF is **unsatisfiable** if it is **F** in every interpretation
A WFF is **satisfiable** if it is **T** in some interpretation

6.3 Proving $A \equiv B$

(1) $A \leftrightarrow B$ is logically valid
(2) $A \to B$ and $B \to A$ are both logically valid

6.4 De Morgan's Laws for Quantifiers

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

6.5 Distributive Laws for Quantifiers

$\forall x(P(x) \wedge Q(x)) \equiv \forall x P(x) \wedge \forall x Q(x)$
$\exists x(P(x) \vee Q(x)) \equiv \exists x P(x) \vee \exists x Q(x)$

6.6 Proving $A \Rightarrow B$

(1) $A \to B$ is logically valid
(2) $A \wedge \neg B$ is unsatisfiable

6.7 Rules of Substitution

$(P) \wedge (Q) \Rightarrow P \wedge Q$	Conjunction
$P \wedge Q \Rightarrow P$	Simplification
$P \Rightarrow P \vee Q$	Addition
$P \wedge (P \to Q) \Rightarrow Q$	Modus Ponens
$\neg Q \wedge (P \to Q) \Rightarrow \neg P$	Modus Tollens
$\neg P \wedge (P \vee Q) \Rightarrow Q$	Disjunctive Syllogism
$(P \to Q) \wedge (Q \to R) \Rightarrow (P \to R)$	Hypothetical Syllogism
$(P \vee Q) \wedge (\neg P \vee R) \Rightarrow Q \vee R$	Resolution
$P \Rightarrow Q \to R \equiv P \wedge Q \Rightarrow R$	Conclusion Premise

6.8 Tautological Implications

$\forall x P(x) \vee \forall x Q(x) \Rightarrow \forall x(P(x) \vee Q(x))$
$\exists x(P(x) \wedge Q(x)) \Rightarrow \exists x P(x) \wedge \exists x Q(x)$
$\forall x(P(x) \to Q(x)) \Rightarrow \forall x P(x) \to \forall x Q(x)$
$\forall x(P(x) \to Q(x)) \Rightarrow \exists x P(x) \to \exists x Q(x)$
$\forall x(P(x) \leftrightarrow Q(x)) \Rightarrow \forall x P(x) \leftrightarrow \forall x Q(x)$
$\exists x(P(x) \leftrightarrow Q(x)) \Rightarrow \exists x P(x) \leftrightarrow \exists x Q(x)$
$\forall x(P(x) \to Q(x)) \wedge \forall x(Q(x) \to R(x)) \Rightarrow \forall x(P(x) \to R(x))$
$\forall x(P(x) \to Q(x)) \wedge P(a) \Rightarrow Q(a)$

6.9 Building Arguments

The same as propositional logic

6.10 Rules of Inference for $\forall, \exists$

$\forall x P(x) \Rightarrow P(a)$	Universal Instantiation
$P(a) \Rightarrow \forall x P(x)$	Universal Generalization
$\exists x P(x) \Rightarrow P(a)$	Existential Instantiation
$P(a) \Rightarrow \exists x P(x)$	Existential Generalization

7 Graph

7.1 Types of Graph

Type	Edges	Multiple Edges	Loops
Simple graph	undirected	No	No
Multigraph	undirected	Yes	No
Pseudograph	undirected	Yes	Yes
Simple directed graph	directed	No	No
Directed multigraph	directed	Yes	Yes
Mixed graph	both	Yes	Yes

7.2 Special Simple Graph

Complete Graph K_n
Cycle C_n
Wheel W_n
n**-Cubes** Q_n

7.3 Matrix

Adjacency Matrix $A = (a_{ij})$,

$$a_{ij} = \begin{cases} 1, & (v_i, v_j) \in E \\ 0, & (v_i, v_j) \notin E \end{cases}$$

Incidence Matrix $B = (b_{ij})$,

$$b_{ij} = \begin{cases} 1, & \text{if } e_j \text{ is incident with } v_i \\ 0, & \text{otherwise} \end{cases}$$

7.4 Handshaking Theorem

Let $G = (V, E)$ be an undirected graph, then
$2|E| = \sum_{v \in V} \deg(v)$ and $|\{v \in V : \deg(v) \text{ is odd}\}|$ is even
Let $G = (V, E)$ be an directed graph, then

$$\sum_{v \in V} \deg^-(v) = \sum_{v \in V} \deg^+(v) = |E|$$

7.5 Hall's Theroem

A bipartite graph $G = (X \cup Y, E)$ has a complete matching from X to Y iff $|N(A)| \geq |A|$ for any $A \subseteq X$

7.6 Connected Component

$v \in V$ is a cut vertex if $G - v$ has more connected components than G
$e \in E$ is a cut edge/bridge if $G - e$ has more connected components than G
$\kappa(G)$ is the minimum number of vertices whose removal disconnect G or results in K_1

$\lambda(G)$ is the minimum size of edge cuts of G

7.7 Connectivity

$0 \le \kappa(G), \lambda(G) \le n-1$
$\kappa(G) = \lambda(G) = 0$ iff G is disconnected or $G = K_1$
$\kappa(G) = \lambda(G) = n-1$ iff $G = K_n (n \ge 2)$
A simple graph $G = (V, E)$ is called **k-connected** if $\kappa(G) \ge k$
G is disconnected or $|V| = 1$: $\lambda(G) = 0$
G is connected and $|V| > 1$: $\lambda(G)$ is the minimum size of edge cuts of G
$\kappa(G) \le \lambda(G) \le \delta(G) = \min_{v \in V} \deg(V)$
Strongly connected $\exists$ path from any u to any v
Weakly connected is connected if remove all directions

7.8 Paths and Isomorphism

The existence of a simple circuit of length k, $k \ge 3$ is an isomorphism invariant for simple graphs

7.9 Counting Paths Between Vertices

The number of different paths of length $l \ge 1$ from v_i to v_j equals the (i, j) entry of the matrix A^r

7.10 Euler Paths and Circuits

Euler Path a simple path that traverses every edge of G
Euler Circuits a simple circuit that ...
Let $G = (V, E)$ be a connected multigraph of order ≥ 2
Then G has an Euler circuit iff $2 \mid \deg(x)$ for every $x \in V$
Let $G = (V, E)$ be a connected multigraph of order ≥ 2.
Then G has an Euler path (not Euler circuit) iff G has exactly 2 vertices of odd degree.

7.11 Hamilton Paths and Circuits

Hamilton Paths a simple path that ... every vertex once
Hamilton Circuits a simple circuit that ...
If G has a vertex of degree 1, then G cannot have a Hamilton circuit.
If G has a vertex of degree 2, then a Hamilton circuit of G traverses both edges.

7.11.1 Ore's Theorem

Let $G = (V, E)$ be a simple graph of order $n \ge 3$
If $\deg(u) + \deg(v) \ge n$ for all $\{u, v\} \notin E$, then G has a Hamilton circuit.

7.11.2 Dirac's Theorem

Let $G = (V, E)$ be a simple graph of order $n \ge 3$
If $\deg(u) \ge n/2$ for every $u \in V$, then G has a Hamilton circuit.

7.12 Djikstra's Algorithm

7.13 Euler's Formula

$r = e - v + 2$ or $V + E - F = 2$
$|V(G)| - |E(G)| + |R(G)| = p + 1$
If every region has degree $\ge l$ in a planar representation of G, then

$$|E(G)| \le \frac{l}{l-2}(|V(G)| - 2)$$

If $|V(G)| \ge 3$, then $|E(G)| \le 3|V(G)| - 6$
A connected planar simple graph has a vertex of degree ≤ 5
If $|V(G)| \ge 3$ and there is no circuits of length 3 in G, then $|E(G)| \le 2|V(G)| - 4$

7.14 Kuratowski's Theorem

A graph G is **nonplanar** iff it has a subgraph homeomorphic to $K_{3,3}$ or K_5

7.15 Dual Graph

A planar graph is said **self-dual** if it is isomorphic to its dual
A self-dual graph with v vertices has $2v - 2$ edges

7.16 Graph Coloring

Let $G = (V, E)$ be a simple graph
$1 \le \mathcal{X}(G) \le |V|$
$\mathcal{X}(G) = 1$ iff $E = \emptyset$
$\mathcal{X}(G) = 2$ iff G is bipartite and $|E| \ge 1$
$\mathcal{X}(K_n) = n$
$\mathcal{X}(G) \ge n$ if G has a subgraph isomorphic to K_n
$\mathcal{X}(C_n) = 2$ if $2 \mid n$; $\mathcal{X}(C_n) = 3$ if $2 \mid (n-1)$;
$\mathcal{X}(G) \le \Delta(G) + 1$, where $\Delta(G) = \max\{\deg(v) : v \in V\}$

7.17 4-coloring Theorem

The chromatic number of a simple planar graph is ≤ 4.

7.18 5-coloring Theroem

We use induction on the number of vertices of the graph. Every graph with five or fewer vertices can be colored with five or fewer colors, because each vertex can get a different color. That takes care of the basis case(s). So we assume that all graphs with k vertices can be 5-colored and consider a graph G with $k+1$ vertices. By Corollary 2 in Section 10.7 in textbook, G has a vertex v with degree at most 5. Remove v to form the graph G'. Because G' has only k vertices, we 5-color it by the inductive hypothesis. If the neighbors of v do not use all five colors, then we can 5-color G by assigning to v a color not used by any of its neighbors. The difficulty arises if v has five neighbors, and each has a different color in the 5-coloring of G'. Suppose that the neighbors of v, when considered in clockwise order around v, are a, b, c, m, and p. (This order is determined by the clockwise order of the curves representing the edges incident to v.) Suppose that the colors of the neighbors are azure, blue, chartreuse, magenta, and purple, respectively. Consider the azure-chartreuse subgraph (i.e., the vertices in G colored azure or chartreuse and all the edges between them). If a and c are not in the same component of this graph, then in the component containing a we can interchange these two colors (make the azure vertices chartreuse and vice versa), and G' will still be properly colored. That makes a chartreuse, so we can now color v azure, and G has been properly colored. If a and c are in the same component, then there is a path of vertices alternately colored azure and chartreuse joining a and c. This path together with edges (a, v) and (v, c) divides the plane into two regions, with b in one of them and m in the other. If we now interchange blue and magenta on all the vertices in the same region as b, we will still have a proper coloring of G', but now blue is available for v. In this case, too, we have found a proper coloring of G. This completes the inductive step, and the theorem is proved.

7.19 Tree

A tree is a connected undirected graph with no simple circuits
An undirected graph is a tree iff there is a unique simple path between any two of its Vertices

7.20 Properties of Tree

A tree with n vertices has $n-1$ edges
A full m-ary tree with
1) n vertices has $i = (n-1)/m$ internal vertices and $\ell = ((m-1)n+1)/m$ leaves
2) i internal vertices has $n = mi + 1$ vertices and $\ell = (m-1)i + 1$ leaves
3) ℓ leaves has $n = (m\ell - 1)/(m-1)$ vertices and $i = (\ell - 1)/(m-1)$ internal vertices

7.21 Balanced m-ary tree

A rooted m-ary tree of height h is **balanced** if all leaves are at levels h or $h-1$
There are at most m^h leaves in an m-ary tree of height h
If an m-ary tree of height h has l leaves, then $h \ge \lceil \log_m l \rceil$.
If the m-ary tree is full and balanced, then $h = \lceil \log_m l \rceil$

7.22 Tree Traversals

7.22.1 Preorder traveral algorithm

Step 1: Visit r
Step $n+1$: Visit T_n

7.22.2 Inorder traveral algorithm

Step 1: Visit T_1
Step 2: Visit r
Step $n+2$: Visit T_{n+1}

7.22.3 Postorder traveral algorithm

Step n: Visit T_n
Step $n+1$: Visit r

7.23 Spanning Trees

Let G be a simple graph. A **spanning tree** of G is a subgraph of G that is a tree containing every vertex of G.
A simple graph is connected iff it has a spanning tree.

7.24 Search

Depth-First Search & Breadth-First Search