CIS-1600 - Notes

May 6, 2024

Contents

1 Module 1 **2**
- 1.1 Addition and Multiplication Rules . . . 2
  - 1.1.1 Addition Rule . . . 2
  - 1.1.2 Multiplication rule . . . 2
- 1.2 Parity-based proofs . . . 2
  - 1.2.1 Odd and Even . . . 2
- 1.3 Divisibility and Primes . . . 2
  - 1.3.1 Divisibility . . . 2
  - 1.3.2 Primes . . . 3
- 1.4 Subsets and Set-builder Notation . . . 3
  - 1.4.1 Sets and their elements . . . 3
  - 1.4.2 Subset and proper/strict subset . . . 3
  - 1.4.3 Empty Set . . . 3
  - 1.4.4 Standard sets of numbers . . . 3
  - 1.4.5 Set-builder notation . . . 3
- 1.5 Set Operations and Cardinality . . . 4
  - 1.5.1 Union . . . 4
  - 1.5.2 Intersection . . . 4
  - 1.5.3 Union and intersection of more than two sets . . . 4
  - 1.5.4 Disjoint and pairwise disjoint sets . . . 4
  - 1.5.5 Set Difference . . . 5
  - 1.5.6 Cardinality . . . 5
- 1.6 Powerset and Cartesian Product . . . 5
  - 1.6.1 Powerset . . . 5
  - 1.6.2 Sequence . . . 5
  - 1.6.3 Cartesian Product . . . 5

2 Module 2 **6**
- 2.1 Counting subsets . . . 6
  - 2.1.1 Cardinality of powerset . . . 6
- 2.2 Permutations . . . 6
- 2.3 Logical structure of statements . . . 6
  - 2.3.1 Logical connectives . . . 6
  - 2.3.2 Logic set-builder notation . . . 7
- 2.4 Implication, conditional and equivalence . . . 7
- 2.5 Symmetric difference . . . 7
- 2.6 Two basic proof patters . . . 7
  - 2.6.1 Proof pattern for implication . . . 7
  - 2.6.2 Proof pattern by cases . . . 7
- 2.7 Proofs regarding sets . . . 8
- 2.8 Combinations . . . 8
- 2.9 Predicates and Quantifiers . . . 8
  - 2.9.1 Predicates . . . 8
  - 2.9.2 Quantifiers . . . 8

3 Module 3 **10**
3.1 Stars and Bars . . . 10
3.2 Negating statements . . . 10
3.2.1 Negation of disjunction / conjunction . . . 10
3.2.2 Negation of quantifiers . . . 10
3.2.3 Negation of implication . . . 10
3.3 Converse and Contrapositive . . . 10
3.4 Truth tables . . . 11
3.5 Vacuous implications . . . 11
3.6 Prove by contrapositive . . . 11
3.7 Logical equivalence . . . 11
3.8 Proofs by contradiction . . . 11
3.8.1 Proofs by contradiction I . . . 11
3.8.2 Proofs by contradiction II . . . 11
3.9 Permutations . . . 12

4 Module 4 **13**
4.1 Binomial Theorem . . . 13
4.2 Combinatorial proofs . . . 13
4.3 Functions . . . 13
4.3.1 Set of all functions . . . 13
4.4 Integer intervals . . . 14
4.5 Surjections and injections . . . 14
4.5.1 Surjective functions . . . 14
4.5.2 Injective functions . . . 14
4.5.3 Surjection & injection rules . . . 14

5 Module 5 **16**
5.1 Bijections . . . 16
5.2 Counting surjections, injections, and bijections . . . 16
5.2.1 Counting injections . . . 16
5.2.2 Counting bijections . . . 16
5.2.3 Counting surjections . . . 16
5.3 Inclusion - Exclusion for Cardinality . . . 17
5.4 Derangements . . . 17
5.5 Pigeonhole Principle . . . 17
5.5.1 Example 1 . . . 17
5.5.2 Problem 2 . . . 18

6 Module 6 - Induction **19**
6.1 Ordinary Induction . . . 19
6.1.1 Good to memorize . . . 19
6.2 Strong Induction . . . 19
6.2.1 Triangular example . . . 19
6.3 Recurrence . . . 19
6.3.1 Recurrence relationship Problem 1 . . . 20
6.4 Fibonacci . . . 20

7 Probability **21**
7.1 Probability space . . . 21
7.2 Uniform space . . . 21
7.3 Bernoulli Trials . . . 21
7.4 Probability Properties . . . 21

8 Probability II **23**
8.1 PIE 23
8.2 Independence 23
8.3 Pairwise & Mutual Independence 23
8.4 Conditional Probability 24
8.5 Chain Rule 24

9 Expectations **25**
9.1 Random Variables 25
9.1.1 Uniform r.v. 25
9.1.2 Bernoulli r.v. 25
9.2 Expectations 26
9.3 LOE 26
9.4 Indicators 26

10 Probability III **27**
10.1 Variance 27
10.2 Binomial r.v. 27

11 Graph Theory I **28**
11.1 Terminology 28
11.1.1 Vertex degree 28
11.2 Special Graphs 28
11.2.1 Edgeless 28
11.2.2 Complete 29
11.2.3 Paths 29
11.2.4 Cycles 29
11.2.5 Grids 29
11.3 Walks and paths 30
11.4 Connected Components 30
11.5 Counting CCs 31

12 Module 12 **32**
12.1 Graph Isomorphism 32
12.2 Subgraphs 32
12.3 Counting paths 33
12.4 Subgraphs 33
12.5 Counting paths 33
12.5.1 Counting paths in cycles 33
12.6 Cycles 34
12.6.1 Counting cycles 34
12.7 Forests, Trees, Leaves 34
12.7.1 Trees and forests 34
12.7.2 Leaves 34
12.8 Properties of trees 35
12.8.1 Any edge is cut edge 35
12.8.2 Trees are maximally acyclic 35
12.8.3 Trees are unique-path connected 35

13 Module 13 **36**
13.1 Spanning Trees 36
13.1.1 Existence of spanning trees 36
13.2 Graph coloring 36
13.2.1 Definitions 36
13.2.2 Chromatic number of graphs 36
13.2.3 Bipartite graphs 37
13.2.4 Distance in a connected graph 38
13.3 Cliques and independent sets 38

14 Module 14 **39**
14.1 Directed graphs . . . 39
14.1.1 Directed walk . . . 39
14.1.2 Directed cycle . . . 39
14.1.3 Directed cycle . . . 40
14.2 Recheability and strong connectivity . . . 40
14.3 Reduced graphs . . . 40
14.4 DAGs . . . 40
14.5 Binary trees . . . 41

Chapter 1: Module 1

1.1 Addition and Multiplication Rules

1.1.1 Addition Rule

Theorem: For objects that can be classified into k distinct kinds, with the i-th kind having n_i objects, the total number of objects is

$$\sum_{i=1}^{k} n_i = n_1 + n_2 + \dots n_k$$

1.1.2 Multiplication rule

Theorem: For a procedure that can be broken down into k steps, where each step is independent of all other steps, and the $i-th$ step can be performed in n_i ways

$$\prod_{i=1}^{k} n_i = n_1 \times n_2 \times \dots n_k$$

1.2 Parity-based proofs

1.2.1 Odd and Even

Definition: An integer n is even when $n = 2k$ for *some* integer k

$$\{0, 2, 4 \dots\}$$

Definition: An integer n is odd when $n = 2k + 1$ for *some* integer k

$$\{1, 3, 5 \dots\}$$

1.3 Divisibility and Primes

1.3.1 Divisibility

Definition: The positive integer d is a divisor or factor of an integer n when $n = d \times k$ for some integer k

$$d \text{ is a divisor of } n \iff d \text{ divides } n \iff d|n$$

1.3.2 Primes

Definition: An integer p is a prime when p has exactly two positive factors, 1 and p and $p \geq 2$

1.4 Subsets and Set-builder Notation

1.4.1 Sets and their elements

Definition: A **set** is an unordered collection of distinct **elements**.

1.4.2 Subset and proper/strict subset

Definition: Set A is a subset of B when every element of A is also an element of B

$$A \subseteq B$$

Definition: A **strict** or **proper** subset is a subset that is not itself

$$A \subset B$$

1.4.3 Empty Set

Definition: The **empty set** $\emptyset$ has no elements

- The empty set is a subset of any set

$$\emptyset \subseteq A \text{ for any } A$$

- The empty set is a proper subset of any non-empty set

$$\emptyset \subset V \text{ for any non-empty set}$$

1.4.4 Standard sets of numbers

Integers: $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2 \ldots\}$Positive integers: $\mathbb{Z}^+ = \{\ldots, 1, 2 \ldots\}$Natural numbers $\mathbb{N} = \{0, 1, 2 \ldots\}$Rational num

1.4.5 Set-builder notation

A is the set containing those elements x that have the property $P(x)$

$$A = \{x|P(x)\}$$

B is the subset of X consisting of those elements x that have the property $P'(x)$

$$B = \{x \in X|P'(x)\}$$

1.5 Set Operations and Cardinality

1.5.1 Union

Definition: The union of two sets A and B is the set whose elements are elements of A or elements of B (including those who are elements of both)

$$A \cup B = \{x|x \in A \text{ or } x \in B\}$$

1.5.2 Intersection

Definition: The union of two sets A and B is the set whose elements are elements of both A and B

$$A \cap B = \{x|x \in A \text{ and } x \in B\}$$

1.5.3 Union and intersection of more than two sets

Definition: The union and intersection of sets $A_1, A_2, A_3, \ldots A_n$ are

$$A_1 \cup A_2 \cup \ldots A_n = \{x|x \in A_1 or x \in A_2 \ldots A_n\}$$

$$A_1 \cap A_2 \cap \ldots A_n = \{x|x \in A_1 and x \in A_2 \ldots A_n\}$$

1.5.4 Disjoint and pairwise disjoint sets

Definition: Two sets A and B are said to be disjoint when they have no elements in common.

$$A \cap B = \emptyset$$

Definition: $A_1, A_2, \ldots A_n$ are pairwise disjoint when A_i, A_j are disjoint for all $i, j \in \{1, 2, \ldots n\}, i \neq j$

Note that

some subsets are pairwise disjoint $\Rightarrow$ **their intersection is empty**

subsets have empty intersection $\not\Rightarrow$ subsets are pairwise disjoint

1.5.5 Set Difference

Definition: The difference of A, B is the set whose elements are elements of A but not elements of B.

$$A \setminus B = \{x | x \in A \text{ and} x \notin B\}$$

1.5.6 Cardinality

Definition:The **cardinality** of a finite set A is the number of elements in A

$$|\emptyset| = 0$$
$$|\{\emptyset, \{\emptyset\}\}| = 2$$
$$|A \cup B| = |A| + |B|, \text{ if A, B disjoint}$$

1.6 Powerset and Cartesian Product

1.6.1 Powerset

Definition: The powerset of A is the set whose elements are all the subsets of A

$$2^A = \{X | X \subseteq A\}$$

$$2^{\{\emptyset\}} = \{\emptyset\{\emptyset\}\}$$

1.6.2 Sequence

Definition: A **sequence** is an ordered collection of elements, with possible repetitions

A sequence is also referred to as a n-tuple where n is the length

1.6.3 Cartesian Product

The cartesian product or cross product of A and B is the set whose elements are pairs whose first component is an element of A and second component is an element of B

$$A \times B = \{(a, b) | a \in A \text{ and } b \in B\}$$

Note that

$$\text{If } A \subseteq B \text{ then } A \times B \subseteq B \times B$$

Chapter 2: Module 2

2.1 Counting subsets

2.1.1 Cardinality of powerset

The cardinality of the powerset 2^A is the number of subsets of A

$$|2^A| = 2^{|A|}$$

2.2 Permutations

Definition: Let A be a non-empty set with n elements

$$|A| = n$$

A **permutation** of A is an ordering of all elements of A without repetition

$$n!$$

A partial permutation of r out of n elements of A consists of picking r of the elements and ordering them without repetition

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

2.3 Logical structure of statements

2.3.1 Logical connectives

Connectives

- **conjunction**: $\quad$ "*and*" $\quad \wedge$
- **disjunction**: $\quad$ "*or*" $\quad \vee$
- **implication**: $\quad$ "$if - then$" $\quad \Rightarrow$
- **negation**: $\quad$ "*not*" $\quad \neg$

For example, a letter l is either a vowel or a consonant can be expressed as

$$letter(l) \Rightarrow [(vowel(l) \wedge \neg consonant(l)) \vee (consonant(l) \wedge \neg vowel(l))]$$

$$letter(l) \Rightarrow [vowel(l) \wedge consonant(l)) \wedge \neg(vowel(l) \wedge consonant(l))]$$

2.3.2 Logic set-builder notation

If $P(x)$ is some logical statement about x, A is the set of elements that satisfies the logical statement

$$A = \{x | P(x)\}$$

2.4 Implication, conditional and equivalence

- **implication**: if P_1 then P_2 : $P_1 \Rightarrow P_2$
- **biconditional / equivalence**: if P_1 then P_2 and if P_2 then P_1

$$(P_1 \Rightarrow P_2) \vee (P_2 \Rightarrow P_1)$$

$$P_1 \iff P_2$$

2.5 Symmetric difference

The symmetric difference of two sets A, B is

$$A \triangle B = (A \setminus B) \cup (B \setminus)$$

$$A \triangle B = \{x | \, (x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)\}$$

2.6 Two basic proof patters

2.6.1 Proof pattern for implication

To prove that

$$P_1 \Rightarrow P_2$$

Proof pattern

1. assert premise P_1
2. logical / mathematical consequences
3. assert conclusion P_2

2.6.2 Proof pattern by cases

Assuming $P_1 \vee P_2$, to prove P_3
Proof pattern

Assert $P_1 \vee P_2$

Case 1: Assert P_1

- logical / mathematical consequences
- assert P_3

Case 2: Assert P_2

- logical / mathematical consequences
- assert P_3

P_3 proven assuming $P_1 \vee P_2$

2.7 Proofs regarding sets

To show $A = B$ for sets A, B, show that

- $A \subseteq B$
- $B \subseteq A$

2.8 Combinations

Let A be a non-empty set with n elements, and r be a natural number

A combination of r elements from the n elements of A is an **unordered** selection of r of the n elements of A

A combination is the same as a **subset** S of A of size r

The number of combinations is given by

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

2.9 Predicates and Quantifiers

2.9.1 Predicates

Predicates are undetermined logical statements because they contain variables whose values are not specified, e.g.

$$odd(p), vowel(l)$$

2.9.2 Quantifiers

Quantifiers include

- universal quantifiers, $\forall x$
- existential quantifiers, $\exists x$

For all positive integers there is a strictly bigger positive integer that is a prime

$$\forall x \in \mathbb{Z}^+ \exists y \in \mathbb{Z}^+ (y > x) \wedge prime(y)$$

Chapter 3: Module 3

3.1 Stars and Bars

Stars and bars are used to count the number of ways to distribute n **indistinguishable** objects into r distinguishable categories, given by

$$\binom{n+r-1}{r-1}$$

3.2 Negating statements

To disprove a statement P is to prove its negation $\neg P$

3.2.1 Negation of disjunction / conjunction

IMPT!!

the negation of disjunction is conjunction

$$\neg(P_1 \wedge P_2) = (\neg P_1) \vee (\neg P_2)$$

the negation of conjunction is disjunction

$$\neg(P_1 \vee P_2) = (\neg P_1) \wedge (\neg P_2)$$

3.2.2 Negation of quantifiers

the negation of universal is existential

$$\neg(\forall x P(x)) = \exists x \neg P(x)$$

the negation of existential is universal

$$\neg(\exists x P(x)) = \forall x \neg P(x)$$

3.2.3 Negation of implication

The negation of "if premise then conclusion" is premise and the negation of the conclusion

$$\neg(P_1 \Rightarrow P_2) = P_1 \wedge \neg P_2$$

3.3 Converse and Contrapositive

Given an implication

$$P_1 \Rightarrow P_2 \text{ (if } P_1 \text{ then } P_2\text{)}$$

The **converse** is

$$P_2 \Rightarrow P_1 \text{ (if } P_2 \text{ then } P_1\text{)}$$

The **contrapositive** is

$$\neg P_2 \Rightarrow \neg P_1 \text{ (if not } P_2 \text{ then not } P_1\text{)}$$

NOTE that the contrapositive is **logically equivalent** to the original implication

3.4 Truth tables

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

3.5 Vacuous implications

Note that is the premise is false then the implication is true, regardless of the conclusion.

False implies everything

Implications where premise is always false is said to **hold vacuously**

3.6 Prove by contrapositive

Instead of proving

$$p \Rightarrow q$$

we prove

$$\neg q \neg p$$

3.7 Logical equivalence

Two boolean expressions are **logically equivalent** if they yield the same truth value for the same truth assignments to their variables

$$
\begin{gathered}
p \Rightarrow q \equiv \neg q \Rightarrow \neg p \quad \text{Contrapositive} \\
p \vee q \Rightarrow r \equiv (p \Rightarrow r) \wedge (q \Rightarrow r) \quad \text{By-cases} \\
p \Rightarrow q \equiv \neg p \vee q \quad \text{Law of Implication} \\
\neg(p \Rightarrow q) \equiv p \wedge \neg q \quad \text{Disproving implication} \\
\neg(p \vee q) \equiv \neg p \wedge \neg q \quad \text{De Morgan's Law I} \\
\neg(p \wedge q) \equiv \neg p \vee \neg q \quad \text{De Morgan's Law II} \\
\neg\neg p \equiv p \quad \text{Law of Double Negation}
\end{gathered}
$$

3.8 Proofs by contradiction

3.8.1 Proofs by contradiction I

A statement P and $\neg P$ is called a contradiction, and is always false.

To prove P, we prove instead that if (not P) then C, where C is a contradiction.

3.8.2 Proofs by contradiction II

To prove if P then Q, we can instead prove if P and not Q then C

$$p \Rightarrow q \equiv p \wedge \neg q \Rightarrow F$$

3.9 Permutations

The number of permutations of a multiset is

$$\frac{n_{total}!}{n_1!n_2!\dots n_k!}$$

Chapter 4: Module 4

4.1 Binomial Theorem

The binomial coefficient is

$$\binom{n}{r}$$

The binomial theorem states that for any real a, b, and any natural number n,

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \ldots \binom{n}{n}b^n = \sum_{i=0}^{n}\binom{n}{i}a^{n-i}b^i$$

4.2 Combinatorial proofs

A combinatorial identity

$$\binom{n}{r} = \binom{n}{n-r}$$

Pascal's identity

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

4.3 Functions

Definition A function or a mapping denoted $f : A \to B$ consists of

- set A, called **domain**
- set B, called **codomain**
- a mapping, or a way of associating **every** element of domain with a unique element of the codomain

$$x \in A, f(x) \in B$$

The **range** of a function $f : B \to B$ is

$$Ran(f) = \{y | y \in B \wedge \exists x \in A \; y = f(x)\}$$

Note that

$$Ran(f) \subseteq B$$

4.3.1 Set of all functions

Given two sets A, B, the set

$$\{f | f : A \to B\} \text{ is denoted by} B^A$$

If $|A| = r$ and $|B| = n$, then the number of different functions with domain A and codomain B is

$$|B^A| = |B|^{|A|} = n^r$$

If $|A| = |B| = |C| = n$, how many functions are there with domain B^A and codomain 2^C?

Such functions map functions in B^A to the superset of C

$$|2^{C^{B^A}}| = |2^C|^{|B^A|} = 2^{n^{n^n}} = 2^{n^{n+1}}$$

4.4 Integer intervals

Definition: An integer interval $[m \dots n]$ $(m < n\ )$ is the set of all integers that lay between m, n inclusive

$$[m \dots n] = \{k \in \mathbb{Z} | m \leq m \leq n\}$$

4.5 Surjections and injections

4.5.1 Surjective functions

Definition: A function $f : A \to B$ is surjective if $Ran(f) = B$, or that for every $y \in B$ there exists $x \in A$ such that $y = f(x)$

Method of proof:

- show that for every $y \in B$, there is some $x \in A$ such that $f(x) = y$

4.5.2 Injective functions

A function $f : A \to B$ is injective if it maps distinct elements to distinct elements, i.e.

$$\text{for every } x_1 \neq x_2 \text{ in the domain we have } f(x_1) \neq f(x_2)$$

or

$$\text{for every } x_1, x_2 \in A, f(x_1) = f(x_2) \implies x_1 = x_2$$

Method of proof:

- show that for every $x_1 \neq n_2$ then $f(x_1) \neq f(x_2)$
- show that for every x_1, x_2, $f(x_1) = f(x_2) \implies x_1 = x_2$

4.5.3 Surjection & injection rules

Surjection rule

Variant 1: if we can define a surjective function with domain A and codomain B then

$$|A| \geq |B|$$

Variant 2: if we can define a function $f : A \to B$ then

$$|A| \geq |Ran(f)|$$

Variant 3 If $f : A \to B$ then $f' : A \to Ran(f)$ where $f'(x) = f(x)$ is surjective

Injection rule :
Variant 1 If we ca define an injective function with domain A and codomain B then

$$|A| \leq |B|$$

Chapter 5: Module 5

5.1 Bijections

Definition: A function $f : A \to B$ is bijective if it is both injective and surjective. It is also called a **bijection** or **one-one** correspondence.

Bijection rule:
Variant 1: if we can define a bijective function with domain A and codomain B then

$$|A| = |B|$$

Variant 2: If we cna define an injective function $f : A \to B$ then

$$|A| = |Ran(f)|$$

Variant 3: If $f : A \to B$ is injective then $f' : A \to Ran(f)$ where $f'(x) = f(x)$ is bijective.

5.2 Counting surjections, injections, and bijections

5.2.1 Counting injections

For A, B $|A| = r$, $|B| = n$, for $r > n$, the number of injections is

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

5.2.2 Counting bijections

For A, B, $|A| = |B| = n$, the number of bijections is

$$n!$$

5.2.3 Counting surjections

For A, B, there are only surjections when $|A| \geq |B|$. In the case $|B| = 2$, the number of surjections is the total number of functions minus the number of functions that are not surjections.

$$|B^A| - |F_0 \cup F_1|$$

where

$$|B^A| = n^r = 2^r$$

$$|F_0| = |\{f : A \to \{0,1\} | 0 \notin Ran(f)\}| = 1$$

$$|F_1| = |\{f : A \to \{0,1\} | 1 \notin Ran(f)\}| = 1$$

Hence the answer is

$$2^r - 2$$

5.3 Inclusion - Exclusion for Cardinality

For any A, B,

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

For three sets,

$$\begin{aligned}|A \cup B \cup C| &= |A| + |B| + |C| \\ &- |A \cap B| - |B \cap C| - |A \cap C| \\ &+ |A \cap B \cap C|\end{aligned}$$

5.4 Derangements

The number of derangements for n items is

$$n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

5.5 Pigeonhole Principle

Pigeonhole Principle: Let $f : A \to B$ be a function. If $|A| > |B|$ then there exist at least two elements, $x_1, x_2 \in A$ such that $x_1 \neq x_2$ but $f(x_1) = f(x_2)$

i.e. if $|A| > |B|$ then f is not injective

Generalized Pigenhole Principle: Let $f : A \to B$ and $k \in \mathbb{Z}^+$. If $|A| > k|B|$ then there exist at least $k + 1$ pairwise distinct elements that f maps onto the same element in B.

r objects into n boxes. For any integer k such that

$$r > kn$$

There is at least a box containing at least $k + 1$ objects

5.5.1 Example 1

Sums of consecutive subsequences

Problem: Given any sequence n integers show that we can always pick some subsequence which appear in consecutive positions in the sequence and whose sum is a multiple of n.

Solution: Let

$$x_1 \ldots x_n$$

be the sequence of n integers.

Consider the following n sums

$$\begin{aligned}
s_1 &= x_1 \\
s_2 &= x_1 + x_2 \\
&\vdots \\
s_n &= x_1 + x_2 + \ldots + x_n
\end{aligned}$$

Case 1: some $s_i \in \{s_1 \ldots s_n\}$ is divisible by n, then we are done

Case 2: none of s_i is divisible by n.

Let r_i be the remainder of the integer division s_i by n for $i \in [1 \ldots n]$, each $r_i \neq 0$.

There are $n - 1$ possible non-zero remainders.

There are a total of n items in r_i. By PHP, with $r_1 \ldots r_n$ n pigeons and $n - 1$ pigeonholes, there exists distinct p, q such that $r_p = r_q$.

$$\begin{aligned}
s_p &= kn + r_p \\
s_q &= ln + r_q
\end{aligned}$$

WLOG assuming $p < q$,

$$s_q - s_p = (l - k)n$$

5.5.2 Problem 2

Theorem: In any group of 6 facebook users, there are 3 that are pairwise friends or 3 that are pairwise strangers.

Proof: Let $A, B, \ldots F$ be six users.

Each $B \ldots F$ is either friends with A or not.

Apply PHP, assign 5 users into two categories, since $5 > 22$, at least one category has 3 users.

WLOG, let these 3 be B, C, D. Consider two cases.

Case 1: B, C, D strangers with A.

1.1 B, C, D pairwise friends, done
1.2 B, C, D not pairwise friends, hence at least 2 are strangers. Say B, C, then, A, B, C pairwise strangers.

Case 2: By symmetry.

Chapter 6: Module 6 - Induction

6.1 Ordinary Induction

General case: to show that $P(n) \forall n \in \mathbb{N}$

Proof pattern:
BC: Show $P(0)$
IS: Let k be an arbitrary natural number, assume **IH** that $P(k)$ is true, show $P(k+1)$.

Variant case: to show that $P(n) \forall n > n_0$ **Proof pattern**:
BC: Show $P(n_0)$
IS: Let k be an arbitrary natural number $k \geq n_0$, assume **IH** that $P(k)$ is true, show $P(k+1)$.

6.1.1 Good to memorize

$$\sum_{i=1}^{n} q^n = q^0 + q^1 + \dots q^n = \begin{cases} \frac{q^{n+1}-1}{q-1} & \text{if } q \neq 1 \\ n+1 & \text{if } q = 1 \end{cases}$$

6.2 Strong Induction

Let $n_0 \in \mathbb{N}$ and let $P(n)$ be a predicated defined on all $n \in \mathbb{N}, n \geq n_0$.

Proof pattern

BC: Show $P(n_0)$

IS: Let $k \in \mathbb{N}$ such that $k \geq n_0$, let $j \in [n_0 \dots k]$, assume $P(j)$, show that $P(k+1)$

6.2.1 Triangular example

Prove by strong induction that if a polygon with 4 or more sides is triangulated then at least two of the triangles formed are exterior.

6.3 Recurrence

Solving recurrence relations

- Guessing the solution for $C(n)$
- Analyzing recurrence tree
- Telescoping method

6.3.1 Recurrence relationship Problem 1

What is the largest number of pieces of pizza that can be made with n distinct straight cuts?

6.4 Fibonacci

The Fibnacci sequence is defined by

$$
\begin{aligned}
&F_0 = 0 \\
&F_1 = 1 \\
&F_n = F_{n-1} + F_{n-2} \text{ for } n \geq 2
\end{aligned}
$$

Chapter 7: Probability

7.1 Probability space

A **probability space** (Ω, Pr) consists of

- a finite non-empty set Ω of outcomes
- a probability distribution function

$$Pr : \Omega \to [0, 1]$$

  that associates with each outcome $\omega \in \Omega$ its probability $Pr[\omega]$ such that

$$\sum_{\omega \in \Omega} Pr[\omega] = 1$$

An event is a subset of the space of all outcomes $E \subseteq \Omega$.

$$Pr[E] = \sum_{\omega \in E} Pr[\omega]$$

7.2 Uniform space

A probability space (Ω, Pr) is uniform if all the outcomes have the same probability.

Denote $n = |\Omega|$, then for each $\omega \in \Omega$,

$$Pr[\omega] = \frac{1}{n}$$

For any event

$$Pr[E] = \frac{|E|}{|\Omega|}$$

7.3 Bernoulli Trials

A **Bernoulli trial** corresponds to a probability space with two outcomes, with probability of success p and probability of failure $1 - p$

7.4 Probability Properties

Property 0

$$Pr[E] \geq 0$$

Property 1

$$Pr[\Omega] = 1$$

Property 2: If A, B disjoint then

$$Pr[A \cup B] = Pr[A] + Pr[B]$$

If $A_1 \dots A_n$ pairwise disjoint then

$$Pr[A_1 \cup \dots A_n] = Pr[A_1] + \dots Pr[A_n]$$

Property 3: If $A \subseteq B$ then

$$Pr[A] \leq Pr[B]$$

Property 4

$$Pr[\overline{E}] = 1 - Pr[E]$$

Property 5

$$Pr[\emptyset] = 0$$

Property 6

$$Pr[A \cup B] = Pr[A] + Pr[B] - Pr[A \cap B]$$

Property 7

$$Pr[A \cup B] \leq Pr[A] + Pr[B]$$

$$Pr[A_1 \cup \dots A_n] \leq Pr[A_1] + \dots Pr[A_n]$$

Chapter 8: Probability II

8.1 PIE

For any events $A, B, C \subseteq \Omega$

$$\begin{aligned} Pr[A \cup B \cup C] &= Pr[A] + Pr[B] + Pr[C] \\ &- Pr[A \cap B] - Pr[B \cap C] - Pr[C \cap A] \\ &= Pr[A \cap B \cap C] \end{aligned}$$

8.2 Independence

Two events $A, B \subseteq \Omega$ are independent, we write $A \perp B$, when

$$Pr[A \cap B] = Pr[A] \times Pr[B]$$

Property 1: If $Pr[A] = 0$ then $A \perp B$ for any B. $\emptyset \perp E$ for any E.

Property 2: $\Omega \perp E$ for any E

Property 3: If $A \perp B$ then

$$Pr[A \cup B] = 1 - (1 - Pr[A])(1 - Pr[B])$$

Property 4: The following are equivalent

- $A \perp B$
- $\overline{A} \perp B$
- $A \perp \overline{B}$
- $\overline{A} \perp \overline{B}$

8.3 Pairwise & Mutual Independence

$A_1 \dots A_n$ pairwise independent when for any $1 \leq i \leq j \leq n$, $A_i \perp A_j$

$A_1 \dots A_n$ mutually independent when for any $\{i_1, \dots i_k\} \subset [1 \dots n]$,

$$Pr[A_{i_1} \cap \dots A_{i_k}] = Pr[A_{i_1}] \dots Pr[A_{i_k}]$$

Note that

mutual independence $\implies$ **pairwise independence**

But the converse is not true

8.4 Conditional Probability

$$Pr[E|U] = \frac{Pr[E \cap U]}{Pr[U]}$$

8.5 Chain Rule

for any A, B, C

$$Pr[A \cap B \cap C] = Pr[A] \times Pr[B|A] \times Pr[C|A \cap B]$$

Chapter 9: Expectations

9.1 Random Variables

A r.v. on (Ω, Pr) is a function $X : \Omega \to \mathbb{R}$.

The values taken by X is

$$Val(X) = \{x \in \mathbb{R} | \exists \omega \in \Omega X(\omega) = x\}$$

The distribution of a random variable X is the function

$$f : Val(X) \to [0, 1] \text{ where } f(x) = Pr[X = x]$$

Note that

$$\sum_{x \in Val(X)} Pr[X = x] = 1$$

Also

$$\sum x \in Val(X) Pr[X = x] = 1$$

9.1.1 Uniform r.v.

Let $v_1 \dots v_n$ be n distinct values of $\mathbb{R}$.

$U : \Omega \to \mathbb{R}$ is uniform within these values when

$$Val(U) = \{v_1, \dots v_n\}$$

And the corresponding distribution

$$f : \{v_1, \dots v_n\} \to [0, 1], f(v_i) = \frac{1}{n}$$

9.1.2 Bernoulli r.v.

Given (Ω, Pr), an r.v. $X : \Omega \to \mathbb{R}$ with

$$Val(X) = \{0, 1\}$$

and

$$Pr[X = 1] = p$$

is called Bernouli r.v.

9.2 Expectations

The expectation is

$$E[X] = \sum_{x \in Val(X)} x \cdot Pr[X = x] = \sum_{\omega \in \Omega} X(\omega) \cdot Pr[\omega]$$

9.3 LOE

$$E[c_1 X_1 + \dots c_n X_n] = c_1 E[X_1] + \dots c_n E[X_n]$$

9.4 Indicators

Let A be an event in (Ω, Pr), the indicator r.v. of A is

$$I_A() = \begin{cases} 1 \text{ if } \omega \in A \\ 0 \text{ if } \omega \notin A \end{cases}$$

Chapter 10: Probability III

10.1 Variance

The variance of r.v. X is

$$Var[X] = E[(X - \mu)^2] = E[X^2] - E[X]^2$$

10.2 Binomial r.v.

A A r.v. $B : \Omega \to \mathbb{R}$ is binomial with parameters $n \in \mathbb{N}$ and $p \in [0, 1]$ when

$$Val(B) = [0 \ldots n]$$

and for any $k \in [0 \ldots n]$

$$Pr[B = k] = \binom{n}{k} p^k (1 - p)^{n-k}$$

Expectation: np
Variance: $np(1 - p)$

Chapter 11: Graph Theory I

11.1 Terminology

A undirected graph is a pair

$$G = (V, E)$$

Where V is a finite non-empty set of vertices

$E2^V$ is a finite and possibly empty set of edges.

11.1.1 Vertex degree

Definition: The degree of a vertex, $deg(u)$ is the number of neighbors of u.

Handshaking Lemma: the sum of degrees of all nodes in a graph is twice the number of edges

$$\sum_{v \in V} deg(v) = 2|E|$$

Proposition: In any graph, there are an even number of vertices of odd degree

Proof: Consider $V = V_e \cup V_o$, $V_e \cap V_o = \emptyset$.

$$\sum_{v \in V} deg(v) = \sum_{v \in V_e} deg(v) + \sum_{v \in V_o} deg(v)$$

11.2 Special Graphs

11.2.1 Edgeless

An **edgeless** graph is $G = (V, E)$ where

$$E = \emptyset$$

$$|E| = 0$$

11.2.2 Complete

A **complete** graph is

$$K_n = (V, E) \text{ where } n \geq 1$$
$$|V| = n$$
$$|E| = \binom{n}{2}$$

11.2.3 Paths

A path graph is denoted

$$P_n = (V, E)$$

where

$$|V| = n$$

Note that for a path graph,

$$|E| = n - 1$$

Note that for $n \geq 3$

$$|\{v \in V : deg(v) = 1\}| = 2$$
$$|\{v \in V : deg(v) = 2\}| = n - 2$$

11.2.4 Cycles

A cycle is denoted

$$C_n = (V, E) \text{ for } n \geq 3$$

Note that

$$\forall v \in V, deg(v) = 2$$
$$C_n \implies \text{ all vertices have degree two}$$

but the converse is not true

11.2.5 Grids

A grid has m rows and n columns

When $m, n \geq 3$,

$$|\{v \in V : deg(v) = 2\}| = 4$$
$$|\{v \in V : deg(v) = 3 \vee deg(v) = 4\}| = m \times n - 4$$

Note that the number of edges

$$|E_{horizontal}| = m(n - 1)$$
$$|E_{vertial}| = n(m - 1)$$

$$|E| = m(n - 1) + n(m - 1)2mn - m - n$$

11.3 Walks and paths

Definition: A walk is a non-empty sequence of vertices consecutively linked by edges

$$u_0, u_1 \dots u_k$$

such that

$$u_0 - u_1 - \dots u_k$$

We say that

- u_0, u_k are the endpoints of the walk
- u_0, u_k are connected by this walk
- the length of the walk is k (there are $k+1$ nodes)

Note that a single vertex is a walk of length 0

Definition: A path is a walk with all vertices distinct.

Proposition: When there is a walk from u_0 to u_n of length $n \geq 3$, and $u_0 \neq u_n$, then there exists vertices $v_1 \dots v_m$ such that $u_0 - v_1 - \dots v_m - u_n$ is a path of length $\leq n$

Alternatively, there exists a path whose sequence of nodes and edges are a subsequence of the sequence of nodes and edges in the walk.

11.4 Connected Components

Definition: two vertices u, v of graph $G = (V, E)$ are said to be **connected** if there exists some walk with endpoints u, v.

Note that connectivity is

- transitive
- reflexive
- symmetric

A **CC** of $G = (V, E)$ is a set of vertices $C \subseteq V$ such that

- any two vertices in C are connected
- there is no strictly bigger set of vertices $C \subset C' \subseteq V$ such that any two vertices in C' are also connected

C is a maximally connected set of vertices in G

Proposition: any two distinct CCs are disjoint

Definition: A **connected graph** is a graph with exactly one connected component

$$|CC| = 1$$

11.5 Counting CCs

Proposition: For any graph $G = (V, E)$

$$|V| - |E| \leq |CC| \leq |V|$$

Proposition: For any graph $G = (V, E)$

$$|V| - |CC| \leq |E| \leq \binom{n}{2}$$

Chapter 12: Module 12

12.1 Graph Isomorphism

Definition: Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a bijection $\beta : V_1 \to V_2$ such that for any $u_1, v_1 \in V_1$,

$$u_1 - v_1 \in E_1 \iff \beta(u_1) - \beta(u_2) \in E_2$$

Proposition: any two complete graphs are isomorphic iff

$$|V_1| = |V_2|$$

Proposition: any two cycle graphs are isomorphic iff

$$|V_1| = |V_2|$$

Proposition: any two path graphs are isomorphic iff

$$|V_1| = |V_2|$$

Proposition: any two $m \times n$ grids are isomorphic, and they are isomorphic to any $n \times m$ grids as well

A path graph on n vertices is a graph isomorphic to P_n

A path graph of length l is a graph isomorphic to P_{l+1}

12.2 Subgraphs

Definition: A graph $G_1 = (V_1, E_1)$ is a subgraph of $G_2 = (V_2, E_2)$ when

$$V_1 \subseteq V_2$$

$$E_1 \subseteq E_2$$

Definition: Given $G = (V, E)$ and $V' \subseteq V$, there is a subgraph G' induced by V' where

$$G' = (V', E')$$

and E' consists of all edges of G whose endpoints are both in V'.

12.3 Counting paths

Definition: Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are isomorphic if there is a bijection $\beta : V_1 \to V_2$ such that for any $u_1, v_1 \in V_1$,

$$u_1 - v_1 \in E_1 \iff \beta(u_1) - \beta(u_2) \in E_2$$

Proposition: any two complete graphs are isomorphic iff

$$|V_1| = |V_2|$$

Proposition: any two cycle graphs are isomorphic iff

$$|V_1| = |V_2|$$

Proposition: any two path graphs are isomorphic iff

$$|V_1| = |V_2|$$

Proposition: any two $m \times n$ grids are isomorphic, and they are isomorphic to any $n \times m$ grids as well

A path graph on n vertices is a graph isomorphic to P_n

A path graph of length l is a graph isomorphic to P_{l+1}

12.4 Subgraphs

Definition: A graph $G_1 = (V_1, E_1)$ is a subgraph of $G_2 = (V_2, E_2)$ when

$$V_1 \subseteq V_2$$

$$E_1 \subseteq E_2$$

Definition: Given $G = (V, E)$ and $V' \subseteq V$, there is a subgraph G' induced by V' where

$$G' = (V', E')$$

and E' consists of all edges of G whose endpoints are both in V'.

12.5 Counting paths

Counting paths of length n in a graph is the same as counting the number of subgraphs that are path graphs on $n + 1$ vertices.

12.5.1 Counting paths in cycles

Each vertex in C_n is uniquely associated with a path of length 2, there is a bijection from the set of vertices to the set of all P_2

12.6 Cycles

Definition: A closed walk is a walk in which the first and last vertex are the same.

Definition: A cycle is a closed walk of length at least 3 in which all nodes are pairwise distinct, except for first and the last.

12.6.1 Counting cycles

In a connected graph,
Counting cycles of length 3 : any 3 vertices form a distinct cycle.

Counting cycles of length 4 : any 4 vertices form 3 distinct cycles
Counting cycles of length 5 :

- choose 5 nodes
- starting from node 1, pick 2 adjacent edges, let end points be u, v
- pick a path of length 3 from u to v, not going through node 1

12.7 Forests, Trees, Leaves

12.7.1 Trees and forests

Definition: A graph that is both acyclic and connected is a **tree**.

An acyclic graph is a forests since each connected component in an acyclic graph is a tree.

Proposition: If $G = (V, E)$ is a tree then

$$|E| = |V| - 1$$

Any tree with n vertices has $n - 1$ edges.

Proof: by induction on the number of vertices.

12.7.2 Leaves

Definition: A leaf is a node with degree 1.

Proposition: Every tree with edges has at least once leaf.

Proof: Consider the set of paths, by Well Ordering Principle, there exists a path of maximum length. Claim that the end points of this maximum path are leaves. Suppose towards a contradiction that they are not then the path can be extended by 1 since there are no cycles.

Proposition: Removing a leaf from a tree results in a tree.

Proof: Resulting graph is still acyclic and connected

12.8 Properties of trees

12.8.1 Any edge is cut edge

Proposition: Removing any edge from a tree disconnects tree.

Proof: prove using the property that **tree with n vertices has $n-1$ edges**. Removing an edge results in graph not being a tree. Graph is still acyclic, hence it must be disconnected.

12.8.2 Trees are maximally acyclic

Proposition: Adding an edge between **any** two non-adjacent vertices in a tree creates a cycle.

Proof: Any two vertices are connected. Adding an edge creates two distinct paths.

12.8.3 Trees are unique-path connected

Proposition: Any two distinct vertices of a tree are connected by a unique path.

Proof: Prove by contradiction, using lemma below

Proposition: Adding an edge to an acyclic graph creates at most one cycle.

Proposition: Any graph such that two distinct vertices are connected by a unique path must be a tree.

Chapter 13: Module 13

13.1 Spanning Trees

Definition: A spanning subgraph of $G = (V, E)$ is a subgraph whose vertex set is V.

A spanning tree of a connected graph G is a spanning subgraph that is a tree.

A spanning forest of a graph G consist of a spanning tree for each CC of G.

13.1.1 Existence of spanning trees

Proposition: Every connected graph has a spanning tree.

Proposition: Removing a cut edge increases the number of connected components by exactly one.

13.2 Graph coloring

13.2.1 Definitions

Definition: For $G = (V, E)$ and some $k \in \mathbb{Z}+$, a **k-coloring** of G is a function $f : V \to [1 \ldots k]$

Definition: A coloring is **proper** when

$$\forall (u - v) \in E, f(u) \neq f(v)$$

Definition: A graph is k-colorable if it admits a proper k coloring. k-colorable implies j-colorable for $j > k$.

Definition: The smallest k such that G is k-colorable is called the **chromatic number** of G, denoted $\chi(G)$

13.2.2 Chromatic number of graphs

Proposition: Only edgeless graphs are 1-colorable

$$\chi(G) = 1 \iff E = \emptyset$$

Proposition: path graphs are 2-colorable

$$\forall n \geq 2, \chi(P_n) = 2$$

Proposition: Word graphs are 2 or 3 colorable depending on the parity of number of indices

$$\chi(C_n) = \begin{cases} 2 \text{ if } even(n) \\ 3 \text{ if } odd(n) \end{cases}$$

Proposition: Connected graphs are n-colorable.

$$\chi(K_n) = n$$

Proof: prove by contradiction that if K_n is m-colorable for some $m < n$, then at least 2 vertices have the same color, but the two vertices are adjacent.

13.2.3 Bipartite graphs

Definition: 2-colorable graphs are called **bipartite**.

Proposition: Every path graph is bipartite.

Proposition: Every cycle graph with even number of vertices is bipartite.

Proposition: Every tree is bipartite.

Proof: By induction on the number of vertices

Proposition: A graph is **bipartite** iff it does not contain a cycle of odd length.

Proposition: If S is a subgraph of G then

$$\chi(S) \leq \chi(G)$$

Or, every subgraph of a bipartite graph is bipartite.

13.2.4 Distance in a connected graph

Definition: The distance between two vertices $u, v \in V$, denoted $d(u, v)$ is the length of the shortest path from u to v.

- $d(u, u) = 0$
- $d(u, v) = d(v, u)$
- $d(u, v) \leq d(u, w) + d(w, v)$

13.3 Cliques and independent sets

Definition: A **clique** of G denotes the complete subgraph of G or a subset of $V' \subseteq V$ such that it induces a complete subgraph.

A **clique** is a subset of vertices such that any two are adjacent.

Definition: A **independent set** is a subset of vertices $V' \subseteq V$ such that no two vertices are adjacent.

Proposition: A graph is k-colorable if its set of vertices can be partitioned into k independent sets.

Proposition: The complement of $G = (V, E)$ is $\overline{G} = (V, \overline{E})$ where

$$\overline{E} = \{(u, v) : u, v \in V \wedge u \neq v \wedge (u, v) \notin E\}$$

Proposition: A subset $V' \subseteq V$ is a clique in G iff it is an independent set in $\overline{G}$.

Chapter 14: Module 14

14.1 Directed graphs

Definition: A directed graph $G = (V, E)$ consists of a non empty set of vertices and a set $E \subseteq V \times V$ of directed edges which are ordered pair of vertices.

Definition: u, v are neighbors when $u \to v$ and $v \to u$

Definition: The degree of a node is the sum of its out-degree and in-degree.

out-degree: number of successors, denoted $out(u)$
in-degree: number of predecessors, denoted $in(u)$

Proposition: the sum of out-degrees for all vertices equals the sum of all in-degrees and equals the number of edges.

$$\sum_{v \in V} out(v) = \sum_{v \in V} in(v) = |E|$$

$$\sum_{v \in V} deg(v) = 2|E|$$

14.1.1 Directed walk

Definition: A **directed walk** of length k is a non-empty sequence $u_0, u_1 \ldots u_k$ such that $u_0 \to u_1 \ldots u_k$.

A **directed path** is a directed walk with no repeated vertices.

14.1.2 Directed cycle

Definition: A **directed cycle** is a closed walk $u_0 \to u_k \to u_0$, of length $k + 1$.

A **directed path** is a directed walk with no repeated vertices.

14.1.3 Directed cycle

Definition: A **directed cycle** is a closed walk $u_0 \to u_k \to u_0$, of length $k+1$.

14.2 Recheability and strong connectivity

Definition: A vertex v is reachable from u if there is a walk from u to v.

Reachability is

- reflexive
- transitive

Definition: Two vertices are strongly connected when u is reachable from v and v is reachable from u.

Strong connectivity is

- reflexive
- transitive
- symmetric

Definition: The maximally strongly connected set of vertices are called **strongly connected components**.

Proposition: Any two distinct SCCs are disjoint.

SCCs determine a partition of the vertices (but not the edges).

14.3 Reduced graphs

Definition: Given $G = (V, E)$, the **reduced graph** has as vertices the SCCs of G and edges as pairs (S_1, S_2) where $S_1 \neq S_2$, and $u_1 \in S_1, u_2 \in S_2$ such that $u_1 \to u_2 \in E$

Proposition: the **reduced graph** has no directed cycles.

14.4 DAGs

Definition: A DAG is a digraph with no directed cycles

Definition: A **topological sort** of a digraph is a sequence σ in which every vertex appears exactly once such that for any $u \to v \in V$ in the graph, u appears in σ before v.

Definition: If a graph has a topological sort then

- the first vertex is a source and the last is a sink
- the digraph is a DAG

Proposition: Every DAG has at least once source and at least one sink.

Proof: Consider the directed path of maximum length, p, which goes from u to v. Prove by contradiction that if $in(u) \geq 1$, there is some edge $w \to u$, and consider two cases ($w \in p$ or $w \notin p$)

Proposition: Every DAG has at least one topological sort.

14.5 Binary trees

Definition: A **rooted tree** is a pair (T, r) where $T = (V, E)$ is a tree and $r \in V$ is designated as a root.

Proposition: Any edge of a rooted tree is traversed in the **same direction** by all unique paths from the root to each of the other vertices.

Definition: A **complete binary tree** of height h is a rooted tree in which every non-leaf node has two children and all leaves are at a distance h from r.

Proposition: A binary tree of height h has maximum of $2^{h+1} - 1$ nodes among which 2^h are leaves. The maximum is attained for the complete binary tree of height h.