

MATH 240: Discrete Structures

Anna Brandenberger, Binyuan Sun

May 9, 2018

This is a transcript of the lectures given by Prof. Ben Seamone during the winter semester of the 2017-2018 academic year (01-04 2018) for the Discrete Structures class (MATH 240). **Subjects covered** are: Mathematical foundations of logical thinking and reasoning; Mathematical language and proof techniques; Quantifiers; Induction; Elementary number theory; Modular arithmetic; Recurrence relations and asymptotics; Combinatorial enumeration; Functions and relations; Partially ordered sets and lattices; Introduction to graphs, digraphs and rooted trees.

1 Logic and Fundamentals

1.1 Propositional Logic

Basic Terms

Definition 1.1. A **proposition** or statement is something which can be verified as being either TRUE or FALSE.

Definition 1.2. A **sentence** is a formula consisting of

- **ATOMS:** simple propositions
- **CONNECTORS:** operations joining atoms

Sometimes parentheses are used to denote order of operations (if necessary.)

Definition 1.3. The three **connectors** are:

- **AND:** "P and Q" = $P \wedge Q$ (both are true)
- **OR:** "P or Q" = $P \vee Q$ (one or the other is true)
- **NOT:** "not P" = $\neg P$ (takes on the opposite truth value of P)

Definition 1.4. A sentence is a:

1. **Tautology** if it is always true.
2. **Contradiction** if it is always false.
3. **Contingency** otherwise.

Examples of propositions and non propositions:

Example

$x = 5$ YES

$x + y$ NO

"This statement is false." NO

P	Q	$P \wedge Q$	$P \vee Q$	$\neg P$
T	T	T	T	F
T	F	F	T	F
F	T	F	T	T
F	F	F	F	T

Table 1: Basic Truth Table

Order of operations:

1. Parentheses
2. \neg
3. \vee and \wedge
4. etc.

Example 1.1. Determine if each sentence is a tautology, contradiction or contingency.

1. $P \wedge \neg P$: Contradiction (c.f. Table 2).
2. $\neg(P \wedge Q) \vee (\neg P \vee Q)$: Tautology (c.f. Table 3).

CAN WE be more efficient in our logic? An **identity** is a statement that two sentences have the same truth values for the same truth values of their atoms.

SOME simple ones:¹

- Identity: $\begin{cases} P \wedge \mathbb{T} \equiv P \\ P \vee \mathbb{F} \equiv P \end{cases}$
- Idempotent: $\begin{cases} P \wedge P \equiv P \\ P \vee P \equiv P \end{cases}$
- Complement: $\begin{cases} P \wedge \neg P \equiv \mathbb{F} \\ P \vee \neg P \equiv \mathbb{T} \end{cases}$
- Double negation: $\neg(\neg P) \equiv P$
- DeMorgan's Laws: $\begin{cases} \neg(\neg P \vee \neg Q) \equiv P \wedge Q \\ \neg(\neg P \wedge \neg Q) \equiv P \vee Q \end{cases}$
- Associative: $\begin{cases} P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R \\ P \vee (Q \vee R) \equiv (P \vee Q) \vee R \end{cases}$
- Distributive: $\begin{cases} P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R) \\ P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R) \end{cases}$

Conditional Statements

Definition 1.5. "P implies Q" written $P \implies Q$.

Example 1.2. P = "the sun is shining", Q = "teeth are purple". The statement given is $P \implies Q$. To show this is false, you must show P is true and Q false.

$$\begin{aligned} \neg(P \implies Q) &\equiv P \wedge \neg Q \\ (P \implies Q) &\equiv \neg(P \wedge \neg Q) && \text{double negation} \\ &\equiv \neg P \vee \neg(\neg Q) && \text{DeMorgan's Law} \\ &\equiv \neg P \vee Q \end{aligned}$$

P	$\neg P$	$P \wedge \neg P$
T	F	F
F	T	F

Table 2: Table illustrating a Contradiction.

P	Q	$\neg P$	$P \wedge Q$	$\neg P \vee Q$	Final
T	T	F	T	T	T
T	F	F	F	F	T
F	T	T	F	T	T
F	F	T	F	T	T

Table 3: Table illustrating a Tautology.

¹ Use \mathbb{T} for a statement that is always true, \mathbb{F} for a statement that is always false.

Equivalent Phrasings to "P implies Q":

- "If P, then Q".
- "Q if P".
- "P only if Q".
- "Q whenever P".
- "Whenever Q, then also P."
- "P is sufficient for Q."
- "Q is necessary for P."

P	Q	$\neg P \vee Q$
T	T	T
T	F	F
F	T	T
F	F	T

Table 4: Table illustrating Example 1.2.

Examples 1.3. using identities:

1. Verify $P \Rightarrow (Q \vee \neg Q)$ is a tautology.

$$\begin{aligned} P \Rightarrow (Q \vee \neg Q) &\equiv P \Rightarrow \mathbb{T} && \text{("complement")} \\ &\equiv \neg P \vee \mathbb{T} && \text{("implies")} \\ &\equiv \mathbb{T} && \text{(identity)} \end{aligned}$$

2. Determine if the following sentence is a tautology, contradiction, or contingency.

$$\begin{aligned} [\neg P \vee (\neg P \wedge Q)] \wedge P &\equiv [\neg P \wedge P] \vee [(\neg P \wedge Q) \wedge P] \\ &\equiv \mathbb{F} \vee [\neg P \wedge P \wedge Q] \\ &\equiv \mathbb{F} \vee [\mathbb{F} \wedge Q] \\ &\equiv \mathbb{F} \vee \mathbb{F} \equiv \mathbb{F} \end{aligned}$$

Definition 1.6. The **contrapositive** of $P \Rightarrow Q$ is $\neg Q \Rightarrow \neg P$.

Proof. Show that $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$.

$$\begin{aligned} P \Rightarrow Q &\equiv \neg P \vee Q \\ &\equiv Q \vee \neg P \\ &\equiv \neg(\neg Q) \vee \neg P \\ &\equiv \neg Q \Rightarrow \neg P \end{aligned}$$

□

The **converse** of $P \Rightarrow Q$ is $Q \Rightarrow P$. In general $P \Rightarrow Q$ & its converse need not be related.

Biconditional Statements

Definition 1.7. $P \Leftrightarrow Q \equiv$ "P and Q are equivalent"

S = this shape is a square
R = this shape is a rectangle
 $S \Rightarrow R$ means if the shape is a square then it is a rectangle. $\neg R \Rightarrow \neg S$ means if the shape is not a rectangle then it is not a square.

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

Table 5: Table illustrating biconditional statements.

TWO NEW identities:

- $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$
- $P \Leftrightarrow Q \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$

AMBIGUOUS STATEMENTS:

1. $A \wedge B \vee C$
 $(A \wedge B) \vee C \equiv (A \vee C) \wedge (B \vee C)$
 $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$

Updated order of operations:

1. Parentheses
2. \neg
3. \vee and \wedge
4. \Rightarrow and \Leftrightarrow

2. $P \Rightarrow Q \Rightarrow R$

Check that:

$$(P \Rightarrow Q) \Rightarrow R \not\equiv P \Rightarrow (Q \Rightarrow R)$$

$$\neg(\neg P \vee Q) \vee R \not\equiv \neg P \vee (\neg Q \vee R)$$

PHRASING of \Leftrightarrow :

$$P \Leftrightarrow Q \equiv P \text{ if and only if } Q$$

$$\equiv P \text{ if } Q, \text{ and conversely}$$

$$\equiv P \text{ precisely when } Q$$

$$\equiv P \text{ is necessary and sufficient for } Q$$

$$\text{NECC: } Q \Rightarrow P, \text{ SUFF: } P \Rightarrow Q$$

A note: $P \equiv Q$ and $P \Leftrightarrow Q$ essentially mean the same thing.

Symbolization

Examples 1.4.

1. If you study then, then you will pass ²: $S \Rightarrow P$
2. The ground gets wet whenever it rains ³: $R \Rightarrow W$
3. The sun is out but it is raining ⁴: $S \wedge R$
4. You cannot scuba dive unless you have had lessons ⁵:
 $S \Rightarrow L \text{ or } \neg L \Rightarrow \neg S$
5. If you only study under pressure, then you do not learn ⁶:
 $(P \Leftrightarrow S) \Rightarrow \neg L$

² S: you study

P: you pass

³ W: the ground gets wet

R: it rains

⁴ W: the sun is out

R: it is raining

⁵ W: can scuba dive

R: had lessons

⁶ S: you study

P: you are under pressure

L: you learn

1.2 Predicate logic

Definition 1.8. We introduce two quantifiers:

1. \forall = "for all" = universal quantifier
2. \exists = "there exists" = "existential quantifier"

Predicates

Definition 1.9. A **predicate** is a sentence containing variables that is either true or false.

Examples 1.5. of symbolization:

1. Every even integer n greater than 2 can be expressed as the sum of two primes.

$$Z(n) = n \text{ is a positive integer}$$

$$P(n) = n \text{ is the sum of 2 primes}$$

$$\forall n(Z(n) \Rightarrow P(n))$$

Predicate logic = 1st order logic

Justification:

Consider a statement like: "Every positive integer is the sum of two primes".

To construct a truth table, we would need infinitely many columns (since this statement contains infinitely many atoms). So this can't be done in propositional logic.

2. "Not everything is about you"⁷: $\neg(\forall x Y(x))$

⁷ $Y(x)$ = "x is about you"

3. "When it rains, everything gets wet"⁸: $R \Rightarrow (\forall x W(x))$

⁸ R : "it rains"

$W(x)$: "x gets wet"

4. "Every person who wants wine gets asked for ID by the bartender"⁹: $\forall x(W(x) \Rightarrow I(x, b))$

⁹ $W(x)$ = x wants wine;

$I(x, y)$ = y asks x for ID;

b = the bartender

WE CAN USE equality to symbolize:

Example 1.6. "Sue is the only person who knows how this works":

$K(x)$: x knows how this works

$\forall x(K(x) \Rightarrow x = \text{Sue})$

WHEN USING multiple quantifiers, order matters (read L to R):

Example 1.7. $F(x, y)$ = "x and y are friends":

$\forall x \exists y F(x, y) \rightarrow$ every person has a friend

$\exists x \forall y F(x, y) \rightarrow$ someone is friends with everyone

FUNCTIONS, OR variables which depend on other variables are allowed.

Example 1.8. "Matt brings a friend":

$B(x, y)$: x brings y

$f(x)$: a friend of x

m : Matt

UPDATED ORDER OF OPERATIONS

1. Parentheses

2. \neg

3. \forall, \exists (L to R)

4. \wedge, \vee

5. $\Rightarrow, \Leftrightarrow$

Theorem 1.1. *Negation of predicates:*

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

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

Examples 1.9.

• "Not everything is about you".¹⁰

CLAIM: Everything is about you: $\forall x Y(x)$

NEGATION: There is a thing that is not about you: $\neg(\forall x Y(x)) \equiv \exists x \neg Y(x)$

¹⁰ $Y(x)$: x is about you

• "All cardinals are red".¹¹

CLAIM: $\forall x(C(x) \Rightarrow R(x))$

NEGATION: $\exists x \neg(C(x) \Rightarrow R(x))$

$\equiv \exists x \neg(\neg C(x) \vee R(x))$

$\equiv \exists x(C(x) \wedge \neg R(x))$

¹¹ $C(x)$: x is a cardinal

$R(x)$: x is red

• "There is an even number greater than three which is prime".¹²

CLAIM: $\exists x(E(x) \wedge G(x) \wedge P(x))$

NEGATION: $\forall x \neg((E(x) \wedge G(x) \wedge P(x)))$

$\equiv \forall x[\neg E(x) \vee \neg G(x) \vee \neg P(x)]$

¹² $E(x)$: x is even

$G(x)$: x is greater than 3

$P(x)$: x is prime

A SENTENCE OF the form $\forall x(P(x) \Rightarrow Q(x))$ is called vacuously true if $P(x)$ is $\text{F } \forall x$. This is because $P \Rightarrow Q$ is true whenever P is false. The rule holds because its never given a chance to fail.

Example 1.10. Every McGill prof with 200 years of experience is a great golfer.¹³

¹³ $M(x)$: McGill prof
 $O(x)$: 200 years of experience
 $G(x)$: great golfer

Proposition 1.2. To *disprove a claim* $\forall x(P(x) \Rightarrow Q(x))$, we show $\exists x$ for which $P(x) \wedge \neg Q(x)$ is true. This x is called a **counterexample** to the claim.

Arguments

Definition 1.10. Rule of inference

An **argument** is a finite collection of statements A_1, A_2, \dots, A_n (called predicate, or hypothesis) followed by statement B called the conclusion. An *argument is valid* if B is true whenever all A_1, A_2, \dots, A_n are true.

Proposition 1.3. To validate an argument:

1. Check a truth table (is B true when A_1, A_2, \dots, A_n are all true?)
2. Show $A_1 \wedge A_2 \wedge \dots \wedge A_n \Rightarrow B$ is a tautology

Some Rules of Inference (more posted on MyCourses)

1. Modus ponens
Arguments: $p \Rightarrow q$
Conclusion: $\frac{p}{q}$
2. Modus tollens
 $P \Rightarrow Q$
 $\frac{\neg Q}{\neg P}$

1.3 Set Definitions and Operations

Definition 1.11. A set is a collection of distinct objects, called elements or members.

NOTATION

$a \in S$ means a is an element of the set S
 $a \notin S$ means a is not an element of the set S

BASIC SETS

\mathbb{N} : the natural numbers
 \mathbb{Z} : the integers
 \mathbb{R} : the real numbers
 \emptyset : the empty set

WRITING DOWN SETS:

- list the elements, in any order inside $\{\}$
- if the elements follow a pattern, we sometimes use " \dots " to denote that the elements continues

Proposition 1.4. Set builder notation:
 $\{\text{element} \mid \text{rule the element obeys to be in the set}\}$

Theorem 1.5. Two sets are equal if and only if they either contain the same elements or are both empty.

Examples 1.13.

1. $\{x \in \mathbb{R} \mid x^2 - 3 = 0\} = \{\sqrt{3}, -\sqrt{3}\}$
2. $\{x \in \mathbb{N} \mid x^2 - 3 = 0\} = \emptyset$
3. $\{n \in \mathbb{Z} \mid n^2 + 1 = 0\} = \{x \mid x > 0 \wedge x < 0\}$
4. $\mathbb{Q} : \{\emptyset\} \stackrel{?}{=} \emptyset$ no! LHS contains an element \emptyset

Definition 1.12. We write $A \subseteq B$ and say A is a subset of B if every $x \in A$ also obeys $x \in B$.

Proposition 1.6. If $A \subseteq B$ & $A \neq B$, we can write as above and say A is a proper subset of B .

Examples 1.15.

- $$\begin{aligned} \{a, b\} &\in \{a, b, c\}? & F \\ \{a, b\} &\subseteq \{a, b, c\}? & T \\ \{a, b\} &\in \{a, b, \{a, b\}\}? & T \\ \{a, b\} &\subseteq \{a, b, \{a, b\}\}? & T \end{aligned}$$

Proposition 1.7. $A = B \Leftrightarrow A \subseteq B$ and $B \subseteq A$

Definition 1.13. \mathcal{U} = the universal set = the set containing everything (that we are interested in)

Venn diagrams

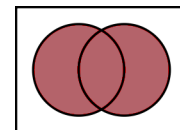
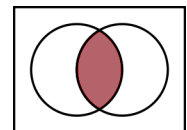
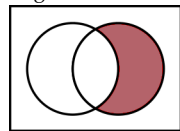
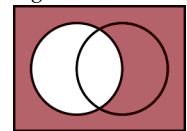
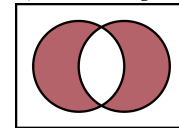
- UNION: $A \cup B = \{x \mid x \in A \vee x \in B\}$
- INTERSECTION: $A \cap B = \{x \mid x \in A \wedge x \in B\}$
- DIFFERENCE: $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$
- COMPLEMENT: $\overline{A} = \{x \mid x \notin A\} = \mathcal{U} \setminus A$
- SYMMETRIC DIFFERENCE: $A \oplus B = \{x \mid (x \in A \vee x \in B) \wedge x \notin A \cap B\}$
 $= \{x \mid x \in A \cup B \wedge x \notin A \cap B\}$

Examples 1.12.

1. \mathbb{Q} the rational numbers
 $\{\frac{m}{n} \mid m \in \mathbb{Z}, n \neq 0\}$
2. \mathbb{C} the complex numbers
 $\{a + bi \mid a \in \mathbb{R}, b \in \mathbb{R}, i^2 = -1\}$

Example 1.14. $\emptyset \subset X$ for every set X
 $\mathbb{N} \subseteq \mathbb{R} \subseteq \mathbb{C}$
 $\{1, 2\} \subseteq \{1, 2, \pi\}$

NOTATION $\{1, 2\} \not\subseteq \{1, 2\}$
 $\{1, 2\} \subset \{1, 2, \pi\}$


 Figure 1: $A \cup B$

 Figure 2: $A \cap B$

 Figure 3: $B \setminus A$

 Figure 4: \overline{A}

 Figure 5: $A \oplus B$

Definition 1.14. Power set of A : $\mathcal{P}(A) = \{B \mid B \subseteq A\}$

Example 1.16. $\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$

Proof Methods

Most statements to prove are of the form $P \Rightarrow Q$ or $P \Leftrightarrow Q$.

Proposition 1.8. *Proof methods for $P \Rightarrow Q$:*

1. **Direct proof:** Assume P is true. Show Q is true, usually with some application of the transitive rule of inference.
2. **Contrapositive proof:** Prove the contrapositive ($\neg Q \Rightarrow \neg P$).

Set Identities (to be posted)

- **COMPLEMENT LAW:** $A \cup \bar{A} = U, \quad A \cap \bar{A} = \emptyset$
- **DEMORGAN:** $\overline{A \cup B} = \bar{A} \cap \bar{B}, \quad \overline{A \cap B} = \bar{A} \cup \bar{B}$
- **DISTRIBUTIVE:** $A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$
 $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Examples 1.17. $P \Rightarrow R_1 \Rightarrow R_2 \Rightarrow Q$

Example 1.18. Prove $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Recall: $X = Y \Leftrightarrow X \subseteq Y$ and $Y \subseteq X$.¹⁴

Proof.

1. Show $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

Let $x \in A \cap (B \cup C)$

$$\begin{aligned} &\Rightarrow x \in A \ \& \ x \in (B \cup C) \\ &\Rightarrow x \in A \ \& \ (x \in B \ || \ x \in C) \\ &\Rightarrow (x \in A \ \& \ x \in B) \ \text{or} \ (x \in A \ \& \ x \in C) \\ &\Rightarrow x \in A \cap B \ || \ x \in A \cap C \\ &\Rightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

2. Show $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$:

Let $y \in (A \cap B) \cup (A \cap C)$

Either $y \in A \cap B$ or $y \in A \cap C \Rightarrow y \in A$ and either $y \in B$ or $y \in C$

$$\begin{aligned} &\Rightarrow y \in (B \cup C) \\ &(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C) \\ &A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{aligned}$$

□

¹⁴ We must show each of the sets in the statement is contained in the other as a subset.

Definition 1.15. Another operation on sets is the **Cartesian product** of A and B denoted $A \times B = \{(a, b) \mid a \in A, b \in B\}$

Proposition 1.9. Two elements in $A \times B$ are equal precisely when they are in both coordinates: $(a_1, b_1) = (a_2, b_2) \Leftrightarrow a_1 = a_2 \text{ and } b_1 = b_2$

Example 1.20. Prove that $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$

Proof. $\Rightarrow x \in A$ and $y \in B \cup C$

If $y \in C$, then $(x, y) \in A \times C$; if $y \in B$, then $(x, y) \in A \times B$

So either $(x, y) \in A \times B$ or $(x, y) \in A \times C$

$\Rightarrow (x, y) \in (A \times B) \cup (A \times C)$

$\Rightarrow A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ \square

Example 1.19. $A = \{1, 2\}, B = \{3, 4\}$
 $A \times B = \{(1, 3), (2, 3), (1, 4), (2, 4)\}$
 $B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2)\}$

1.4 Relations and Equivalence Relations

Definition 1.16. A binary relation \mathcal{R} from A to B is a subset of $A \times B$.

Proposition 1.10. A binary relation on A is a subset of A^2 .

Using the example above, $R = \{(1, 3), (1, 4)\}$ is a binary relation from A to B (one of many).

Definition 1.17. Useful properties: Let R be a binary relation on A .

R is	Definition
reflexive	$\forall a \in A, (a, a) \in R$
symmetric	$(a, b) \in R \Rightarrow (b, a) \in R$
antisymmetric	$(a, b) \in R \text{ and } (b, a) \in R \Rightarrow a = b$
transitive	$(a, b), (b, c) \in R \Rightarrow (a, c) \in R$

Example 1.21.

$\{(x, y) | y = x^2\}$ is a bin. rel. on \mathbb{R} .
 $\{(x, y) | x = y^2\}$ is a bin. rel. on \mathbb{R} .
 $\{(m, n) | \frac{m}{n} \in \mathbb{Z}\}$ is a bin rel on \mathbb{Z} .

Example 1.22. Determine if the relation has any of the 4 properties defined above: $R = \{(x, y) \in \mathbb{R}^2 | x \leq y\}$

– **Reflexive:** $\forall x \in \mathbb{R}, x \leq x \Rightarrow (x, x) \in R$

– **Symmetric:** $(1, 2) \in R$ and $(2, 1) \notin R$

– **Antisymmetric:** If $(x, y) \in R$ and $(y, x) \in R$, then $x \leq y$ and $y \leq x \Rightarrow x = y$

– **Transitive:** If $(x, y), (y, z) \in R$, then $x \leq y \cap y \leq z \Rightarrow (x, z) \in R$ \square

Definition 1.18. A binary relation on A is a **partial order** on A if it is reflexive, antisymmetric, and transitive

Example 1.23. $R = \{(a, b) \in \mathbb{Z}^2 | a - b \text{ is even}\}$

– **Reflexive:** $\forall x \in \mathbb{Z}, a - a = 0 \text{ is even} \Rightarrow (a, a) \in R$

Note: n is even $\Leftrightarrow n = 2k$ for some $k \in \mathbb{Z}$

- **Symmetric:** $(a, b) \in R \Rightarrow a - b \text{ even} \Rightarrow b - a \text{ even} \Rightarrow (b, a) \in R$
- **Antisymmetric:** $(16, 8) \in R \ \& \ (8, 16) \in R$ but $16 \neq 8$
- **Transitive:** If $(a, b) \in R$ and $(b, c) \in R$, then
$$\begin{cases} a - b = 2k \\ b - c = 2l \end{cases}$$

 $\Rightarrow a - c = 2k + 2l = 2(k + l)$ is even.

Definition 1.19. A binary relation on A is an **equivalence relation** on A if it is reflexive, symmetric, and transitive.

Definition 1.20. A **total order** on A is a partial order R where $\forall a, b \in A$, either (a, b) or (b, a) is in R . (Linear order.)

Remark 1. Not every partial order is a total order.

Example 1.24. Let A be some set $R = \{(x, y) | x, y \in P(A), x \subseteq y\}$

Why is this not a total order?

$$A = \{1, 2, 3\}, \quad M = \{1\}, \quad N = \{2, 3\}$$

$$(x, y) \notin R \because M \not\subseteq N \wedge N \not\subseteq M$$

Show it is a partial order.

- **Reflexive:** $\forall x \subseteq A$, is $(x, x) \in R$?
- **Antisymmetric:** $(x, y) \in R \wedge (y, x) \in R$
 $\Rightarrow X \subseteq Y \wedge Y \subseteq X$
 $\Rightarrow X = Y$
- **Transitive:** $(X, Y) \in R, (Y, Z) \in R$
 $\Rightarrow X \subseteq Y, Y \subseteq Z$
 $\Rightarrow X \subseteq Z$
 $\Rightarrow (X, Z) \in R$

Equivalence Relations

Definition 1.21. We say a is related to b in a equivalent relation R if $(a, b) \in R$, denoted as follows:

Notation 1.11. a is related to b in a equivalent relation R :

$$a \mathcal{R} b \qquad a \sim_{\mathcal{R}} b \qquad a \sim b \text{ (if } \mathcal{R} \text{ is understood)}$$

Definition 1.22. If R is an equivalence relation, the **equivalence class** of an element $a \in R$ is denoted $[a]$ or \bar{a} , is $[a] = \{x | x \sim a\}$

Example 1.25. 1. Show $R = \{(x, y) \in \mathbb{Z}^2 | x - y = 3k \text{ for some } k \in \mathbb{Z}\}$ is an equivalence class.

Recall: Definition 1.19: an **equivalence relation** is a relation R which is:

- Reflexive
- Symmetric
- Transitive

2. What are $[0], [1], [2], [3]$?

1. R: $x - x = 0 \Rightarrow (x, x) \in R$

S: $x - y = 3k \Rightarrow y - x = 3k \Rightarrow (x, y) \in R \Rightarrow (y, x) \in R$

I: $(x, y) \in R, (y, z) \in R$

$\Rightarrow x - y = 3k, y - z = 3l \Rightarrow x - z = 3(k + l) \in \mathbb{Z} \Rightarrow (x, z) \in R$

2. $[0] = \{x | x \sim 0\} = \{x | x - 0 = 3k\} = \{x | x = 3k\} = \{\dots, -6, -3, 0, 3, 6, \dots\}$

$[1] = \{x | x \sim 1\} = \{x | x - 1 = 3k\} = \{x | x = 3k + 1, k \in \mathbb{Z}\}$

$[2] = \{x | x \sim 2\} = \{x | x - 2 = 3k\} = \{x | x = 3k + 2, k \in \mathbb{Z}\}$

$[3] = \{x | x \sim 3\} = \{x | x - 3 = 3k\} = \{x | x = 3k + 3, k \in \mathbb{Z}\} = \{x | x = 3(k + 1), k \in \mathbb{Z}\} = \{x | x = 3l, l \in \mathbb{Z}\} = [0]$

Theorem 1.12. Let $a \in A$, R an equivalence relation to A . For any $x \in A$, $[x] = [a] \Leftrightarrow x \sim a$.

Proof. (\Leftarrow) Suppose $[x] = [a] \therefore x \in [x] \Rightarrow x \in [a] \Rightarrow x \sim a$

(\Rightarrow) Suppose $x \sim a$, We will show $\underbrace{[x] \subseteq [a]}_{(a)}$ and $\underbrace{[a] \subseteq [x]}_{(b)}$

(a) Let $y \in [x] \Rightarrow y \sim x$.

Since $x \sim a$, by transitivity, $y \sim a \Rightarrow y \in [a] \Rightarrow [x] \subseteq [a]$

(b) $z \in [a]$

$\Rightarrow z \sim a$

$\Rightarrow z \sim x$ (since $x \sim a$)

$\Rightarrow z \in [x]$

$\Rightarrow [a] \subseteq [x]$

Together, this gives $[a] = [x]$ □

Theorem 1.13. Let $a, b \in A$, R an equivalence relation of A .

$[a] \neq [b] \Leftrightarrow [a] \cap [b] = \emptyset$

Proof. (\Rightarrow) If $[a] \cap [b] = \emptyset$ then since $a \in [a]$, $a \notin [b] \Rightarrow [a] \neq [b]$.

(\Leftarrow) We will prove the contrapositive: show $[a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$.

$[a] \cap [b] \neq \emptyset \Rightarrow \exists x, x \in [a] \cap x \in [b] \Rightarrow x \sim a \wedge x \sim b \Rightarrow [x] =$

$[a] \cap [x] = [b] \Rightarrow [a] = [b]$ □

To prove $P \Leftrightarrow Q$, prove $P \Rightarrow Q$ and $Q \Rightarrow P$

Recap: $P \Rightarrow Q$: Direct proof, Contrapositive (direct proof of $\neg Q \Rightarrow \neg P$)

$P \Leftrightarrow Q : P \Rightarrow Q \wedge Q \Rightarrow P, \quad P \Rightarrow Q \wedge \neg P \Rightarrow \neg Q, \quad [\neg Q \Rightarrow \neg P \wedge \neg P \Rightarrow \neg Q]$

1.5 Proof by Contradiction

PRINCIPLE: If your assumption leads, by logical steps, to something false (a contradiction), then the assumption must have been wrong and thus the opposite statement is right.

Following are some proofs using this method:

Theorem 1.14. $\sqrt{2} \notin \mathbb{Q}$

Proof. Suppose $\sqrt{2} \in \mathbb{Q}$

$$\Rightarrow \sqrt{2} = \frac{m}{n}, \quad m, n \in \mathbb{Q}$$

We may assume, without loss of generality (WLOG), that $\frac{m}{n}$ is in reduced form, i.e they share no common factors.

$$\begin{aligned} \sqrt{2} = \frac{m}{n} &\Rightarrow 2 = \frac{m^2}{n^2} \\ &\Rightarrow m^2 = 2n^2 \\ &\Rightarrow m \text{ is even} \Rightarrow m = 2k \text{ for some } k \in \mathbb{Z} \\ &\Rightarrow (2k)^2 = 2n^2 \Rightarrow 4k^2 = 2n^2 \Rightarrow 2k^2 = n^2 \\ &\Rightarrow n \text{ is even} \end{aligned}$$

$\Rightarrow m$ and n have a common factor of 2. $\Rightarrow \Leftarrow$

Thus our assumption $\sqrt{2} \in \mathbb{Q}$ was wrong. \square

Theorem 1.15. Fundamental Theorem of Arithmetic. Every $n \in \mathbb{N}$ can be written as a product of primes that is unique up to order.

Proof. given later (Section 2). \square

Theorem 1.16. There are infinitely many primes.

Proof. Suppose there are finitely many primes p_1, p_2, \dots, p_n

Let $q = p_1 p_2 \dots p_n + 1$. Theorem 1.15 (Fundamental Theorem of Algebra) states that q is divisible by some prime: WLOG, $p_1 \Rightarrow q = p_1 k$ for some $k \in \mathbb{Z}$.

$$\begin{aligned} q - p_1 p_2 \dots p_n &= 1 \\ p_1 k - p_1 p_2 \dots p_n &= 1 \\ \underbrace{p_1}_{\geq 2} \underbrace{(k - p_2 \dots p_n)}_{\in \mathbb{N}} &= 1 \quad \Rightarrow \Leftarrow \end{aligned}$$

Thus our assumption that there are finitely many primes was wrong. \square

Proposition 1.17. Proving Existential Statements ($\exists x P(x)$)

1. Give the example.
2. When you can't give the example, a "non constructive proof" can sometimes be found.

Example 1.26. 1. "There exists an even prime". It's 2.

2. "There is a real solution to $x^2 - x - 1 = 0$ ". It's $\frac{1 \pm \sqrt{5}}{2}$.

Example 1.27. "There are irrational numbers x, y such that $x^y \in \mathbb{Q}$."

Proof. We know $\sqrt{2} \notin \mathbb{Q}$.

Consider $\sqrt{2}^{\sqrt{2}}$.

If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, then $x = \sqrt{2}, y = \sqrt{2}$ is our example.

If $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$, then consider $\sqrt{2}^{\sqrt{2}}, y = \sqrt{2} : (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2 \in \mathbb{Q}$.

In either case, we have an example that proves such x, y exist. \square

2 Number Theory

2.1 Division

The study of properties of integers.

Theorem 2.1. Division AlgorithmIf $a, b \in \mathbb{Z}$, $b \neq 0$, then $\exists q, r \in \mathbb{Z}$ such that: $a = qb + r$, with $0 \leq r < |b|$.Furthermore, q and r are unique. t

The proof of this algorithm uses the following as main tool:

Lemma 2.2. Well Ordering Principle. If $A \subseteq \mathbb{N}$, then A has a smallest element.*Proof. of the Division Algorithm (Theorem 2.1)*Consider the case where $a, b > 0$. Look at the following multiples of b : $0, b, 2b, 3b, 4b, \dots$. There is some multiple of $b > a$. Let $B = \{kb | k \in \mathbb{N}, kb > a\}$ By the Well Ordering Principle (Lemma 2.2), B has a smallest element. Call it $(q+1)b$.

$$qb \leq a < (q+1)b$$

$$\text{Let } r = a - qb$$

Then

$$a = qb + r$$

And:

$$0 \leq a - qb < (q+1)b - qb$$

$$0 \leq r < b$$

WHAT ABOUT UNIQUENESS?

Assume $\exists q_1, q_2, r_1, r_2$ such that $a = q_1b + r_1$, $a = q_2b + r_2$. We will show $q_1 = q_2$ and $r_1 = r_2$, and so distinct solutions are impossible.

$$0 = (q_1 - q_2)b + (r_1 - r_2), (q_1 - q_2)b = r_2 - r_1.$$

But

$$0 \leq r_1 < b$$

$$-b < -r_2 \leq 0$$

$$\Rightarrow -b < r_1 - r_2 < b$$

Since $r_1 - r_2$ is a multiple of b , we have $r_1 - r_2 = (0)(b) \Rightarrow r_1 = r_2$ and $(q_1 - q_2)b = 0 \Rightarrow q_1 = q_2$. Therefore q and r are unique. \square **Definition 2.1.** b divides $a \Leftrightarrow \exists q$ such that $a = qb$. Write $b \mid a$ if b divides a and $b \nmid a$ if b does not divide a .**Proposition 2.3.** g is a divisor of a if $g \mid a$ and $g \mid b$ and if g is the largest such integer, we call g the greatest common divisor of a and b ; we write $g = \gcd(a, b)$.**Example 2.1.** $(2a)b = (2b)a \geq 2a > a$ A note about proving the remaining cases: you can use the $a > 0, b > 0$ case.

Let's prove some things about divisors.

Lemma 2.4. If $c \mid a$ and $c \mid b$ then, $c \mid xa + yb \forall x, y \in \mathbb{Z}$.

Proof. $\exists k, l \in \mathbb{Z}$ such that $a = kc, b = lc \Rightarrow xa + yb = x(kc) + y(lc) = (xk + yl)c \Rightarrow c \mid (xk + yl)c = c \mid (xa + yb)$ \square

Lemma 2.5. If $a = qb + r$, then $\gcd(a, b) = \gcd(b, r)$.

Proof. If $a = b = 0$ or $b = r = 0$, then the gcd's are undefined. If $a \neq 0$, then $\gcd(a, 0) = a$. Let $g_1 = \gcd(a, b)$ and $g_2 = \gcd(b, r)$. $g_1 \mid a$ and $g_1 \mid b$.

$$\Rightarrow g_1 \mid a - qb$$

$$\Rightarrow g_1 \mid r$$

$$\Rightarrow g_1 \text{ divides } r \& b$$

$$\Rightarrow g_1 \leq g_2$$

$$\text{Similarly, } g_2 \mid b \text{ and } g_2 \mid r$$

$$\Rightarrow g_2 \mid qb + r \text{ (by lemma above)}$$

$$\Rightarrow g_2 \Rightarrow g_2 \leq g_1 \text{ (because } g_2 \mid a \& g_2 \mid b)$$

$$g_1 = g_2$$

\square

Proposition 2.6. Euclidean Algorithm

Suppose $a > b$ ($a, b \in \mathbb{N}$). Then write:

$$a = q_1b + r_1 \quad (0 \leq r_1 < b)$$

$$b = q_1r_1 + r_2 \quad (0 \leq r_2 < r_1)$$

$$r_1 = q_2r_2 + r_3 \quad (0 \leq r_3 < r_2)$$

and continue until the remainder becomes 0, $r_{k+1} = 0$. Then $r_k = \gcd(a, b)$

Proof.

DOES THIS TERMINATE?

This set has a smallest element by W.O.P., this is r_k .

DOES IT WORK?

By previous lemma,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \gcd(r_k, 0) = r_k$$

\square

Definition 2.2. $a, b \in \mathbb{N}$ are **relatively prime** if $\gcd(a, b) = 1$.

Example 2.4. Show 91 and 8 are relatively prime:

$$91 = 11(8) + 3$$

$$8 = 2(3) + 2$$

$$3 = 1(2) + 1$$

$$2 = 2(1) + 0$$

Example 2.2. $\underbrace{87}_a = 4(\underbrace{21}_b) + \underbrace{3}_r$

$$\gcd(a, b) = 3$$

$$\gcd(b, r) = 3$$

If $a \neq 0$ then $\gcd(a, 0) = a$.

Example 2.3. Find $\gcd(630, 196) = 14$

$$630 = 3(196) + 42$$

$$196 = 4(42) + 28$$

$$42 = 1(28) + 14$$

$$28 = 2(14) + 0$$

As a consequence of the Euclidean Algorithm, $\exists x, y$ such that $\gcd(a, b) = xa + yb$:

$$14 = (42) - 1(28)$$

$$= (42) - 1[196 - 4(42)]$$

$$= 5(42) - 1(196)$$

$$= [630 - 3(196)] - 1(196)$$

$$\Rightarrow 14 = 5(630) - 16(196)$$

Again, $\exists s, t \in \mathbb{Z}$ s.t. $91s + 8t = 1$

$$\begin{aligned}
 1 &= (3) - 1(2) \\
 &= 3 - 1(8 - 2(3)) \\
 &= 3(3) - 1(8) \\
 &= 3(91 - 11(8)) - 1(8) \\
 &= \underbrace{3}_s(91) - \underbrace{34}_t(8)
 \end{aligned}$$

Theorem 2.7. If a & b are relatively prime, then $\forall n \in \mathbb{N}$, $\exists x, y \in \mathbb{Z}$ s.t.

$$n = xa + yb$$

Proof.

$$\begin{aligned}
 \gcd(a, b) &= 1 \\
 \Rightarrow \exists s, t \quad sa + tb &= 1 \\
 \Rightarrow (sn)a + (tn)b &= n \\
 \Rightarrow xa + yb &= n \quad \square
 \end{aligned}$$

Corollary 2.8. If $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof.

$$\begin{aligned}
 &\exists x, y \text{ such that } ax + by = 1 \\
 &\Rightarrow c = cax + cby \\
 &\text{Since } a \mid a \text{ and } a \mid bc \\
 &a \mid a(xc) + bc(y) \Rightarrow a \mid c(ax + by) \\
 &\Rightarrow a \mid c \quad \square
 \end{aligned}$$

Definition 2.3. $p \in \mathbb{N}$ is called prime if $d \mid p \Rightarrow d = 1$ or p

Lemma 2.9. $\forall n \in \mathbb{N}, n \geq 2, \exists p \mid n, p$ prime.

Proof. Suppose n has no prime divisor. The set of all positive integers with no prime divisors would be non-empty. By WOP (Lemma 2.2), it has a smallest element. Call this m .¹⁵ Since $m \mid m$, m is not prime. Thus $\exists d, 1 < d < m$ such that $d \mid m$. By minimality of m , d has a prime divisor, say p . $p \mid d$ and $d \mid m$

$$\Rightarrow p \mid m \quad \Rightarrow \Leftarrow \quad \square$$

Lemma 2.10. If $n \in \mathbb{N}, n$ composite, $n \geq 2$, then $\exists p \in \mathbb{N}$ such that $p \mid n$, p prime and $p \leq \sqrt{n}$.

Proof. n composite $\Rightarrow n = ab$ for some $a, b \in \mathbb{N}$. WLOG, $a \leq b$.

Claim: $a \leq \sqrt{n}$.

If not, $a > \sqrt{n}$ and $b \geq a > \sqrt{n} \Rightarrow ab > \sqrt{n}\sqrt{n} = n \Rightarrow \Leftarrow$

$$\exists p \mid a, p \text{ prime} \Rightarrow p \leq a \leq \sqrt{n} \quad (\exists p \mid a, a \mid n \Rightarrow p \mid n) \quad \square$$

¹⁵ Note: This variation on a proof by contradiction uses a minimal counterexample

Lemma 2.11. $p \mid ab, p \text{ prime} \implies p \mid a \text{ or } p \mid b$

Proof. $p \mid a \implies$ done.

$$p \nmid a \implies \gcd(a, p) = 1 \implies p \mid b. \quad \square$$

Corollary 2.12. $p \mid a_1 \dots a_k \implies p \mid a_i \text{ for some } i$

Theorem 2.13. Fundamental Theorem of Arithmetic.

For an $n \in \mathbb{N}, n \geq 2, n = p_1 p_2 \dots p_k$ for some primes p_1, p_2, \dots, p_k .
This representation is unique.

Proof. Suppose $n = p_1 p_2 \dots p_k$ and $n = q_1 q_2 \dots q_l$ (all p_i, q_i prime).

$\implies p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$. Cancel any common prime factors. If there's anything left, p_i , then $p_i \mid q_i \implies p_i = q_i$. $\implies \Leftarrow$

The two representations must be identical. \square

2.2 Congruence and Modular Arithmetic

Definition 2.4. Let $n \in \mathbb{N}$. We say $a, b \in \mathbb{Z}$ are **congruent modulo n** iff $n \mid (a - b)$. We write $a \equiv b \pmod{n}$.

Example 2.5.

$$13 \equiv 83 \pmod{10}$$

$$736 \equiv -1044 \pmod{2}$$

Theorem 2.14. $R_n = \{(a, b) \in \mathbb{Z}^2 \mid n \mid (a - b)\}$ is an equivalence relation.

Proof. To be proved. \square

Lemma 2.15. For $n \in \mathbb{N}$ if $a = qn + r$ for some $q \in \mathbb{Z}, 0 \leq r < n$, then $a \sim r$.

Proof.

$$a = qn + r$$

$$\implies a - r = qn$$

$$\implies n \mid a - r$$

$$\implies (a, r) \in R_n \quad \square$$

Example 2.6. Find an integer $0 \leq k \leq 17$ such that

$$1. \quad 18 \equiv k \pmod{17}$$

$$\implies k \equiv 1 \pmod{17}$$

$$2. \quad -18 \equiv \quad \pmod{17}$$

$$-18 \equiv -1 \equiv 16 \pmod{17}$$

Corollary 2.16. $[a] = [r]$ in \mathcal{R}_n where r is the remainder of a after division by n .

Corollary 2.17. The equivalence classes of $\mathcal{R}_n = \{(a, b) \in \mathbb{Z}^2 \mid n \mid (a - b)\}$ are $[0], [1], \dots, [n - 1]$.

EQUIVALENT STATEMENTS:

1. $a \equiv b \pmod{n}$
2. $n \mid (a - b)$
3. $a - b \equiv 0 \pmod{n}$
4. $a \in [b] \in \mathcal{R}_n$
5. $b \in [a] \in \mathcal{R}_n$
6. $[a] = [b] \in \mathcal{R}_n$

Operations

Lemma 2.18. *If $a \equiv b \pmod{n}$ and $x \equiv y \pmod{n}$ then:*

1. $(a \pm x) \equiv (b \pm y) \pmod{n}$
2. $ax \equiv by \pmod{n}$

Proof.

1. $n \mid (a - b)$ and $n \mid (x - y)$
 $\Rightarrow n \mid (a \pm x) - (b \pm y)$
 $\Rightarrow (a \pm x) \equiv (b \pm y) \pmod{n}$
2. Note that $ax - by = ax - ay + ay - by = a(x - y) + y(x - y)$
 $\therefore n \mid (x - y) \wedge n \mid (a - b)$

$$\begin{aligned}
 &\Rightarrow n \mid [a(x - y) + y(a - b)] \\
 &= n \mid (ax - by) \\
 &= ax \equiv by \pmod{n}
 \end{aligned}$$

□

Example 2.7. Solve $\begin{cases} 2x + 3y \equiv 1 \pmod{6} \\ x + 3y \equiv 5 \pmod{6} \end{cases}$

$$\begin{aligned}
 3x + 6y &\equiv 6 \pmod{6} \\
 \Rightarrow 3x &\equiv 0 \pmod{6} \\
 \implies x = 0, 2, 4 \pmod{6} &\text{ are the possibilities.}
 \end{aligned}$$

$$\text{If } x \equiv 0 \pmod{6} \Rightarrow 3y \equiv 5 \pmod{6}$$

$$\text{But } 3 \nmid 3y - 5 \Rightarrow 6 \nmid 3y - 5$$

$$\text{So } 3y \not\equiv 5 \pmod{6} \quad \forall y \in \mathbb{Z}$$

If $x \equiv 2 \pmod{6} \Rightarrow 2 + 3y \equiv 5 \pmod{6}$

$$\Rightarrow 3y \equiv 3 \pmod{6}$$

$$\Rightarrow y \equiv 1 \pmod{2}$$

Check: $y \equiv 0, 1, 2, 3, 4, 5$

$$ka \equiv kb \pmod{kn} \Leftrightarrow a \equiv b \pmod{n}$$

If $x \equiv 4 \pmod{6} \Rightarrow 4 + 3y \equiv 5 \pmod{6}$

$$\Rightarrow 3y \equiv 1 \pmod{6}$$

$$\text{But } 3 \nmid 3y - 1 \Rightarrow 6 \nmid 3y - 1$$

So no solutions.

$$\Rightarrow \text{Final Solutions: } \begin{cases} x \equiv 2 \pmod{6} \\ y \equiv 1, 3, 5 \pmod{6} (y \equiv 1 \pmod{2}) \end{cases}$$

Proposition 2.19. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Proof.

$$ac \equiv bc \pmod{n}$$

$$\Rightarrow n \mid ac - bc$$

$$\Rightarrow n \mid c(a - b)$$

$$\Rightarrow n \mid a - b \text{ since } \gcd(c, n) = 1 \Rightarrow a \equiv b \pmod{n} \quad \square$$

Example 2.8. Solve $2x \equiv 1 \pmod{9}$

$$2x \equiv 1 \pmod{9}$$

$$\Rightarrow 2x \equiv 10 \pmod{9}$$

$$\text{since } \gcd(2, 9) = 1$$

$$\Rightarrow x \equiv 5 \pmod{9}$$

Theorem 2.20. Let $n \in \mathbb{N}, a \in \mathbb{Z}$. Then $\gcd(a, n) = 1 \Leftrightarrow \exists s \in \mathbb{Z}$ such that $sa \equiv 1 \pmod{n}$, where we call s the **multiplicative inverse**.

Proof.

$$(\Rightarrow) : \gcd(a, n) = 1 \Rightarrow \exists s, t \in \mathbb{Z} \text{ such that } sa + tn = 1$$

$$\Rightarrow n \mid (sa - 1)$$

$$\Rightarrow sa \equiv 1 \pmod{n}$$

$$(\Leftarrow) : \text{If } \exists s, sa \equiv 1 \pmod{n} \Rightarrow \exists q \text{ such that } sa - 1 = qn$$

$$\Rightarrow 1 = sa - qn$$

$$\text{If } \exists d \text{ s.t. } d \mid a \text{ and } d \mid n:$$

$$\Rightarrow d \mid 1 \Rightarrow \gcd(a, n) = 1 \quad \square$$

Example 2.9. Find the inverse of $91 \pmod{190}$.

$$\begin{array}{ll}
 190 = 2(91) + 8 & \text{Backtracking gives: } \dots \\
 91 = 11(8) + 3 & 1 = (71)(91) - (34)(190) \\
 8 = 2(3) + 2 & (71)(91) - 1 = \underbrace{(34)(190)}_{\equiv 0 \pmod{190}} \\
 3 = 1(2) + 1 & \Rightarrow (71)(91) \equiv 1 \pmod{190} \\
 2 = 2(1) + 0 & \Rightarrow 91^{-1} \equiv 71 \pmod{190} \\
 & \Leftrightarrow 71^{-1} \equiv 91 \pmod{190} \\
 & \text{since } 190 \mid (1 - (71)(91))
 \end{array}$$

Example 2.10. Find x such that $2x \equiv 1 \pmod{9}$ (cont. Example 2.8), aka find $2^{-1} \pmod{9}$.

$$\begin{aligned}
 9 &= 4(2) + 1 \Rightarrow 1 = 9 - 4(2) \\
 2 &= 2(1) + 0 \\
 \Rightarrow (-4)(2) &\equiv 1 \pmod{9} \\
 2^{-1} &\equiv -4 \equiv 5 \pmod{9}
 \end{aligned}$$

So:

Not using inverse:	Using inverse:
$2x \equiv 1 \pmod{9}$	$2x \equiv 1 \pmod{9}$
$\Rightarrow 10x \equiv 5 \pmod{9}$	$\Rightarrow x \equiv (1)(2^{-1}) \pmod{9}$
$\Rightarrow (1)x \equiv 5 \pmod{9}$	$\Rightarrow x \equiv 5 \pmod{9}$
$\Rightarrow x \equiv 5 \pmod{9}$	

Why no solutions for $g \nmid b$? (recall $g = \gcd(a, n)$)

$$\begin{aligned}
 ax &\equiv b \pmod{n} \\
 \Rightarrow ax - b &= kn \\
 \Rightarrow \underbrace{b}_{g \nmid b} &= \underbrace{ax - kn}_{\text{divisible by } g} \\
 &\Rightarrow \text{no solution.}
 \end{aligned}$$

SOLVING ALGORITHM ($ax \equiv b \pmod{n}$)

```

1  if  $\gcd(a, n) = 1$ 
2    find  $a^{-1} \pmod{n}$  backtracking from Euclidian Algorithm,
3    return  $x \equiv a^{-1}b \pmod{n}$ 
   // simplify to  $x = z \pmod{n}$ 
   // all solutions:  $x = z + nk, k \in \mathbb{Z}$ 
4  else  $\gcd(a, n) = g \neq 1$ 
5    if  $g \mid b$ 
6      return SOLVING ALGORITHM  $\left(\frac{a}{g}x \equiv \frac{b}{g} \pmod{\frac{n}{g}}\right)$ 
   // solution has  $g$  equivalence classes  $\pmod{n}$ 
   // i.e.  $x \equiv z + \frac{n}{g}k \pmod{n}$  where  $x < n$ 
7  else  $g \nmid b$ 
8    return no solution.

```

Example 2.11. Solve if possible:

1. $91x \equiv 10 \pmod{190}$

$\gcd(91, 190) = 1 \Rightarrow$ there is a solution. Use $91^{-1} \equiv 71 \pmod{190}$.

$$\begin{aligned} 91x &\equiv 10 \pmod{190} \\ \Rightarrow x &\equiv (10)(91^{-1}) \pmod{190} \\ &\equiv (10)(71) \pmod{190} \\ &\equiv 710 \pmod{190} \\ &\equiv 3(190) + 140 \pmod{190} \\ \Rightarrow x &\equiv 140 \pmod{190} \end{aligned}$$

2. $92x \equiv 10 \pmod{196}$

$\gcd(92, 196) = 4$ using Euclidian Algorithm.

$$\begin{aligned} 92 &= 2^2 \cdot 23 \\ 196 &= 2^2 \cdot 7^2 \end{aligned} \quad 4 \nmid 10 \Rightarrow \text{no solution}$$

3. $92x \equiv 12 \pmod{196}$

$\gcd(92, 196) = 4$: divide both sides of equation and modulus by 4.

$$23x \equiv 3 \pmod{49}$$

$$\gcd(23, 49) = 1$$

$\Rightarrow 23^{-1}$ exists. Using Euclidian Algorithm:

$49 = 2(23) + 3$	Backtracking:
$23 = 7(2) + 2$	$1 = 3 - 1(23 - 7(2))$
$3 = 1(2) + 1$	$= 8(2) - 1(23)$
$2 = 2(1) + 0$	$= 8(49 - 2(23)) - (23)$
$1 = 3 - 1(2)$	$= 8(49) - 17(23)$
	$1 \equiv \underbrace{8(49) - 17(23)}_{\equiv 0} \pmod{49}$
	$1 \equiv (-17)(23) \pmod{49}$
	$\Rightarrow 23^{-1} \equiv -17 \pmod{49}$
	$\equiv 32 \pmod{49}$

So:

$$\begin{aligned} 92x \equiv 12 \pmod{196} &\Leftrightarrow 23x \equiv 3 \pmod{49} \\ x &\equiv 3(23)^{-1} \pmod{49} \\ x &\equiv 3(32) \pmod{49} \\ \Leftrightarrow x &\equiv 96 \pmod{49} \\ \Leftrightarrow x &\equiv 47 \pmod{49} \end{aligned}$$

What if we wanted all solutions modulo 196?

Every solution is $x = 47 + 49k, k \in \mathbb{Z}$

For $k = 0, 1, 2, 3$: $x = 47, 96, 145, 194$.

These correspond to the solution's equivalence classes mod 196.

$$x \equiv 47, 96, 145, 194 \pmod{196}$$

Theorem 2.21. *Fermat's Little Theorem: If p is a prime and a is any integer, then $a^{p-1} \equiv 1 \pmod{p}$. [A consequence $a^p \equiv a \pmod{p}$] We can use this to quickly simplify large powers \pmod{p} .*

Proof. Later (posted). □

Example 2.12. Find $2^{39674} \pmod{523}$

We can check 523 is prime.

Rewrite 39674 by dividing by 522: $39674 = 76(522) + 2$.

$$\begin{aligned} 2^{39674} &\equiv 2^{(76)(522)+2} \pmod{523} \\ &\equiv (\underbrace{2^{522}}_{\equiv 1 \text{ by FLT}})^{76} * 2^2 \pmod{523} \\ &\equiv (1)^{76} 4 \pmod{523} \equiv 4 \pmod{523} \end{aligned}$$

Example 2.13.

$$\begin{aligned} 4762^{5377} \pmod{13} &\equiv [336(13) + 4]^{5367} \\ &\equiv 4^{5367} \pmod{13} \\ &\equiv 4^{(447)(12)+3} \pmod{13} \\ &\equiv (\underbrace{(4)^{12}}_{\equiv 1 \text{ by FLT}})^{447} * 4^3 \pmod{13} \\ &\equiv 64 \pmod{13} \\ &\equiv 12 \pmod{13} \end{aligned}$$

Example 2.14. Show $x^{97} - x - 1 \equiv 0 \pmod{97}$ has no solution.

$$\begin{aligned} x^{97} &\equiv x \pmod{97} \quad (\text{FLT}) \\ x - x + 1 &\equiv 0 \pmod{97} \implies 1 \equiv 0 \pmod{97} \\ 1 &\not\equiv 0 \pmod{97} \implies \text{no solution} \end{aligned}$$

SIMPLIFYING ALGORITHM ($a^x \pmod{p}$)

```

1  if p prime
2    Rewrite  $x = q(p-1) + r$ 
   //  $q \in \mathbb{Z}, 0 \leq r < p$ 
3  return  $a^x \equiv a^{q(p-1)+r}$ 
       $\equiv (a^{p-1})^q a^r \pmod{p}$ 
       $\equiv a^r \pmod{p}$ 

```

END OF MATERIAL FOR MIDTERM 1

2.3 RSA Encryption

Notes posted.

3 Combinatorics

3.1 Proof by Induction

Definition 3.1. Induction is used to prove a statement $S(n)$ is true for all $n \in \mathbb{N}$ by proving:

1. Base case: $S(1)$ true,
2. Inductive step: $S(n) \Rightarrow S(n+1)$.

WHY DOES this work — ? $S(1) \Rightarrow S(2) \Rightarrow S(3) \Rightarrow \dots$

Example 3.1. Prove $1 + 2 + 3 + \dots + (n-1) + n = \frac{n(n+1)}{2}$ for $n \in \mathbb{N}$

Proof. Base Case: $n = 1$: $1 = \frac{(1)(2)}{2} \checkmark$

Inductive Step: Assume $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ (hypothesis).

Show $1 + 2 + \dots + (n+1) = \frac{(n+1)(n+2)}{2}$

$$\begin{aligned} 1 + 2 + \dots + (n) + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left(\frac{n}{2} + 1\right) \\ &= \frac{(n+1)(n+2)}{2} \end{aligned} \quad \square$$

Example 3.3. Prove $\sum_{i=0}^n (i)(i!) = (n+1)! - 1$

Note: this is a statement taking $n \geq 0$ (an integer) as the variable.

Proof. Base case: $n = 0$ $\sum_{i=0}^n (i)(i!) = 0 \checkmark$

Inductive step: Assume $\sum_{i=0}^n (i)(i!) = (n+1)! - 1$

Show $\Rightarrow \sum_{i=0}^{n+1} (i)(i!) = (n+2)! - 1$

$$\begin{aligned} \sum_{i=0}^{n+1} (i)(i!) &= \sum_{i=0}^n (i)(i!) + (n+1)(n+1)! \\ &= [(n+1)! - 1] + (n+1)(n+1)! \\ &= (n+1)! [1 + (n+1)] - 1 \\ &= (n+1)!(n+2) - 1 \\ &= (n+2)! - 1 \end{aligned} \quad \square$$

Glorified counting. How do we count?

Example 3.2. Prove that the sum of odd integers $\sum_{i=1}^n (2i-1) = n^2$.

$$\begin{aligned} 1 &= 1 \\ 1 + 3 &= 4 \\ 1 + 3 + 5 &= 9 \\ 1 + 3 + 5 + 7 &= 16 \end{aligned}$$

Proof. Base case: $n = 1$: $\sum_{i=1}^n (2i-1) = 1$

Inductive step :

Assume $\sum_{i=1}^n (2i-1) = n^2$

Show $\Rightarrow \sum_{i=1}^{n+1} (2i-1) = (n+1)^2$

$$\begin{aligned} \sum_{i=1}^n (2i-1) &= n^2 = \sum_{i=1}^n (2i-1) \\ &= n^2 + [2(n+1) + 1] \\ &= n^2 + 2n + 1 \\ &= (n+1)^2 \end{aligned} \quad \square$$

Example 3.4. $n! \geq 2^n \forall n \geq 4$.

Proof. Base case: $n = 4$: $24 > 16 \checkmark$

Inductive step: Assume $n! \geq 2^n$

$$\begin{aligned} (n+1)! &= (n!)(n+1) > (n!)(2) \\ &= (n!)(n+1) > (2^n)(2) = 2^{n+1} \end{aligned} \quad \square$$

Example 3.5. Prove $5 \mid 8^n - 3^n$ for all $n \geq 0$.


Proof. Base case: $n = 0$: $5 \mid 8^0 - 3^0 \checkmark$

Inductive Step: Assume $5 \mid 8^n - 3^n$

$$\begin{aligned} 8^{n+1} - 3^{n+1} &= 8(8^n) - 3(3^n) \\ &= (5+3)(8^n) - 3(3^n) \\ &= 5(8^n) + 3(8^n - 3^n) \end{aligned}$$

$$5 \mid 5(8^n) \wedge 5 \mid 3(8^n - 3^n)$$

$$\Rightarrow 5 \mid 8^{n+1} - 3^{n+1} \quad \square$$

Example 3.6. Call a rotation of  a "tromino". Take a $(2^n \times 2^n)$ checkerboard ($n \geq 1$) and delete any tile (square). Prove you can tile it with trominos.

Proof.

Base Case: $n = 1$:

With a square removed from a (2×2) board, the remaining part is exactly one tromino piece. ✓

Inductive Step: Assume true for n , show true for $n + 1$:

Consider a $(2^{n+1} \times 2^{n+1})$ board. Place a tromino in the middle (one block covered - i.e. removed - in 3 of the 4 quadrants). Remove one block from the fourth quadrant. Now each of the 4 $2^n \times 2^n$ boards can be tiled (by Inductive Hypothesis).

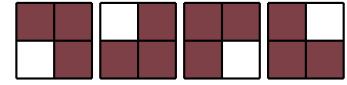


Figure 6: Base case.

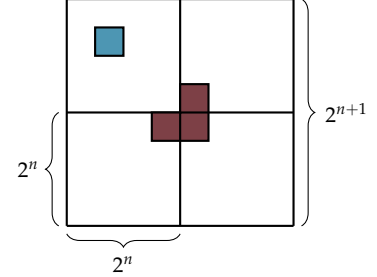


Figure 7: Inductive step.

□

Example 3.7. Prove that a set with n elements has 2^n subsets.

Proof. Base case: $n = 0$: \emptyset has 1 subset, $1 = 2^0$. ✓

Inductive Step: Assume true for n . Let A be a set with $n + 1$ elements (write $|A| = n + 1$). Let $x \in A, B = A \setminus \{x\}$. B has 2^n subset by IH.

For each $X \subseteq B$, X and $\cup\{x\}$ are distinct subsets of A .

$\Rightarrow 2^n + 2^n = 2(2^n) = 2^{n+1}$ subsets.

□

Common Mistakes

1. *Finding incorrect patterns.*

CLAIM: $n^2 + n + 41$ is prime for all $n \leq 0$. The proof works until $n = 39$ but at $n = 40, 40^2 + 40 + 41 = 41^2$

2. *Forgetting the base case.*

CLAIM: $n(n + 1)$ is odd for all $n \geq 1$.

Assume true for n .

$$(n + 1)(n + 2) = \underbrace{n(n + 1)}_{\text{odd}} + \underbrace{2(n + 1)}_{\text{even}} \therefore \text{ODD}$$

BUT THIS IS FALSE: We forgot the base case: $n = 1 \Rightarrow (1)(2) = 2$ ~~ODD~~

3. *Making an unstated (wrong) assumption.*

CLAIM: All cows are the same colour.

Let C_n denote a set of n cows.

Base case: $n = 1$: Any set of 1 cow has uniform colour.

Inductive Step: Assume true for any C_n . Look at $\{c_1, c_2, \dots, c_{n+1}\}$.

By IH, $\{c_1, c_2, \dots, c_n\}$ all have same colour. By IH, $\{c_1, c_2, \dots, c_{n+1}\}$ all have same colour.

PROBLEM: $S(1) \not\Rightarrow S(2)$ because $\{c_1\} \cap \{c_2\} = \emptyset$ (the two sets share no common cow when $n = 2$).

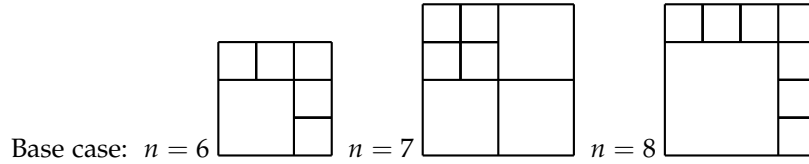
We have base case $n = 1$ but the statement is false when $n = 2$.

Definition 3.2. Strong Induction is a variation of induction in which we assume that the statement holds for all values preceding n , i.e. one proves:

1. $S(1)$ true
2. $(S(1) \wedge S(2) \wedge \dots \wedge S(n)) \Rightarrow S(n+1)$

Example 3.8. Prove that any square can be partitioned into $n \geq 6$ non-empty squares.

Proof.



Inductive Step: Assume true for all integers $k, 6 \leq k \leq n$ ($n \geq 8$).

Show true for $n+1$. By I.H., true for $n-2$. Take one square and quarter it, giving $(n-2) - 1 + 4 = n+1$. \square

Example 3.10. Prove every $n \in \mathbb{N}$ can be written as

$$n = a_0 2^0 + a_1 2^1 + \dots + a_k 2^k$$

for some $k \in \mathbb{N} \cup \{0\}$, where $a_i \in \{0, 1\} \forall i$.

Proof. Base case: $n = 1 \Rightarrow 1 = (1)2^0 \checkmark$

Inductive Step: Assume true for all $1 \leq k \leq n-1$, prove true for n :

1. If n is odd, $n-1$ is even. Thus $n-1 = (0)2^0 + a_1 2^1 + \dots + a_k 2^k$ for some k (by I.H.) $\Rightarrow n = 1(2)^0 + a_1 2^1 + \dots + a_k 2^k$.
2. If n is even, look at $\frac{n}{2}$. $\frac{n}{2} = a_0 2^0 + \dots + a_k 2^k$ by (I.H.) $\Rightarrow n = a_0 2^1 + \dots + a_k 2^{k+1}$. \square

Example 3.9. Prove that for any $n \geq 18$, $\exists x, y, \in \mathbb{N} \cup \{0\}$ s.t.

$$n = 4x + 7y$$

Proof. Base case: $n = 18, 19, 20, 21$

$$18 = 4(1) + 7(2)$$

$$19 = 4(3) + 7(1)$$

$$20 = 4(5) + 7(0)$$

$$21 = 4(0) + 7(3)$$

I.H. Assume true $\forall 18 \leq k \leq n$, ($n \geq 21$)

By I.H. $\exists x, y, \in \mathbb{N} \cup \{0\}$ s.t. $n-3 = 4x + 7y \Rightarrow n+1 = 4(x+1) + 7y$. \square

i.e. every n can be written in binary.

3.2 Recursion

Definition 3.3. A sequence $\{a_1, a_2, \dots\}$ is a **recurrence relation** if a_n is a function of $\{a_1, a_2, \dots, a_{n-1}\}$.

NOTATION: The first term can be for any $k \geq 0$. A finite number of **initial values** must be given.

Example 3.11. Let $a_0 = 1$, $a_n = na_{n-1}$, $n \geq 1$. Prove $a_n = n!$

Proof. Base case: $n = 0 \checkmark$

Inductive Step: Assume $a_n = n!$

$$\Rightarrow a_{n+1} = (n+1)a_n = (n+1)n! = (n+1)! \quad \square$$

Example 3.12. Let $a_1 = 1$, $a_n = \sqrt{6 + a_{n-1}}$, $n \geq 2$. Prove $a_n < 3$.

Proof. Base case : $n = 1 \Rightarrow a_1 = 1 < 3$.

Inductive Step: Assume true for n ($a_n < 3$) \checkmark .

$$\begin{aligned} a_{n+1} &= \sqrt{6 + a_n} \\ &< \sqrt{6 + 3} = 3 \end{aligned} \quad \square$$

Definition 3.4. Fibonacci numbers.

$$f_1 = 1, f_2 = 1, \quad f_n = f_{n-1} + f_{n-2}, \quad (n \geq 3)$$

Example 3.14. How many subsets of $\{1, 2, 3, \dots, n\}$ contain no consecutive integers? Let S denote the number of such subsets from $\{1, \dots, n\}$.

$$S_n = (\# \text{ with } n) + (\# \text{ without } n) = S_{n-2} + S_{n-1}$$

S_{n-2} because because if n is in the set, $n-1$ is not and we are counting subsets from $\{1, \dots, n-2\}$; and S_{n-1} because if n is not in, then we count subsets from $\{1, \dots, n-1\}$. $\Rightarrow S_n$ is f_{n+2} .

Some proofs about $\{f_n\}_{n=1}^\infty$

Theorem 3.1. $f_1 + f_2 + \dots + f_n = f_{n+2} - 1$

Proof. Base case: $n = 1 \Rightarrow f_1 = f_3 - 1 = 2 - 1 \checkmark$

Inductive Step: Assume true for n . Want $f_1 + f_2 + \dots + f_n + f_{n+1} = f_{n+3} - 1$

$$\begin{aligned} \boxed{f_1 + f_2 + \dots + f_n} + f_{n+1} &= \boxed{f_{n+2} - 1} + f_{n+1} \\ &= f_{n+3} - 1 \end{aligned} \quad \square$$

$$\begin{aligned} a_0 &= 1 \\ a_1 &= (1)a_2 = 1 \\ a_2 &= (2)a_1 = 2(1) \\ a_3 &= (3)a_2 = (3)(2)(1) \end{aligned}$$

Example 3.13. Prove $a_n = (n+1)2^n$

$$\text{where } \begin{cases} a_0 = 1 \\ a_1 = 4 \\ a_n = 4a_{n-1} - 4a_{n-2}, \quad n \geq 2 \end{cases}$$

Proof. Base cases: $n = 0, 1$.

$$n = 0: (1) = (0+1)2^0$$

$$n = 1: (4) = (1+1)2^1$$

Inductive Step: Assume true for all k , $1 \leq k \leq n$.

$$\begin{aligned} a_{n+1} &= 4a_n - 4a_{n-1} \\ &= 4(n+1)2^n - 4(n)2^{n-1} \\ &= 4 \cdot 2^{n-1} [2(n+1) - n] \\ &= 2^{n+1} (n+2) \end{aligned} \quad \square$$

$$n = 1: \{1\}, \quad 2: \emptyset, \{1\}$$

$$n = 2: \{1, 2\}, \quad 3: \emptyset, \{1\}, \{2\}$$

$$n = 3: \{1, 2, 3\}, \quad 5: \emptyset, \{1\}, \{2\}, \{1, 3\}$$

Theorem 3.2. $P(n) : f_{n+1}f_n + f_nf_{n-1} = f_{2n}$
 $Q(n) : f_n^2 + f_{n-1}^2 = f_{2n-1}$

Proof. For now, omit base cases: computation.

Assume $P(n)$ and $Q(n)$ true, \implies Prove $Q(n+1)$ true.

$$\begin{aligned} f_{n+1}^2 + f_n^2 &= (f_n + f_{n-1})^2 + f_n^2 \\ &= f_n^2 + 2f_nf_{n-1} + f_{n-1}^2 + f_n^2 \\ &= (f_n^2 + f_{n-1}^2) + f_nf_{n-1} + f_nf_{n-1} + f_n^2 \\ &= f_{2n-1} + f_nf_{n-1} + f_n(f_{n-1} + f_n) \\ &= f_{2n-1} + f_nf_{n-1} + f_nf_{n+1} \\ &= f_{2n-1} + f_{2n} = f_{2n+1} \end{aligned}$$

$P(n+1)$ true?

$$\begin{aligned} f_{n+2}f_{n+1} + f_{n+1}f_n &= (f_{n+1} + f_n)f_{n+1} + (f_n + f_{n-1})f_n \\ &= f_{n+1}^2 + f_nf_{n+1} + f_n^2 + f_nf_{n-1} \\ &= \underbrace{f_{n+1}^2 + f_n^2}_{Q(n+1)} + \underbrace{f_nf_{n+1} + f_nf_{n-1}}_{P(n)} \\ &= f_{2n+1} + f_{2n} \\ &= f_{2n+2} \end{aligned}$$

□

3.3 Solving Recurrence Relations

Definition 3.5. The characteristic polynomial of $a_n = ra_{n-1} + sa_{n-2}$ is $x^2 - rx - s$. Its roots α, β are the characteristic roots of the relation.

Theorem 3.3. Consider $a_n = ra_{n-1} + sa_{n-2}$ with specified a_0, a_1 . If $x^2 - rx - s$ has 2 distinct roots α, β then

$$a_n = c_1\alpha^n + c_2\beta^n$$

where c_1 and c_2 solve $a_0 = c_1 + c_2$, $a_1 = c_1\alpha + c_2\beta$.

Example 3.15. Consider $a_n = a_{n-1} + 2a_{n-2}$, $a_0 = 2, a_1 = 1$

$$a_0 = 2 \quad a_1 = 1 \quad a_2 = 5 \quad a_3 = 7 \quad a_4 = 17$$

$$a_5 = 31 \quad a_6 = 65 \quad a_7 = 127$$

...

$$a_n = 2^n + (-1)^n ?$$

We could prove this by induction, but we would rather have a method more rigorous than "guess and check".

Proof. Show $a_n = c_1\alpha^n + c_2\beta^n$ solves the relation $a_n = ra_{n-1} + sa_{n-2}$

$$\begin{aligned} c_1\alpha^n + c_2\beta^n &= r[c_1\alpha^{n-1} + c_2\beta^{n-1}] + s[c_1\alpha^{n-2} + c_2\beta^{n-2}] \\ c_1\alpha^n - rc_1\alpha^{n-1} - sc_1\alpha^{n-2} &= -c_2\beta^n - rc_2\beta^{n-1} - s\beta^{n-2} \\ c_1\alpha^{n-2}[\alpha^2 - r\alpha - s] &= -c_2\beta^{n-2}[\beta^2 - r\beta - s] \\ 0 &= 0 \quad \checkmark \\ a_n &= c_1\alpha^n + c_2\beta^n \\ n = 0 : \quad a_0 &= c_1 + c_2 \\ n = 1 : \quad a_1 &= c_1\alpha + c_2\beta \end{aligned}$$

□

Example 3.16. (Back to Example 3.15) $a_n = a_{n-1} + 2a_{n-2}$
 $\Rightarrow x^2 - x - 2 = 0 = (x+1)(x-2) \Rightarrow \text{let } \alpha = 2, \beta = -1$

$$a_n = c_1 2^n + c_2 (-1)^n$$

$$n = 0: a_0 = c_1 + c_2 \Rightarrow 2 = c_1 + c_2$$

$$n = 1: a_1 = 2c_1 - c_2 \Rightarrow 1 = 2c_1 - c_2$$

$$\Rightarrow c_1 = 1, c_2 = 1 \Rightarrow a_n = 2^n + (-1)^n$$

WHAT ABOUT relations of the form $a_n = ra_{n-1} + sa_{n-2} + ta_{n-3}$ (or higher "order")? — Look at a characteristic polynomial whose degree is equal to the order of the recurrence.

Example 3.18. $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$, $a_0 = 2, a_1 = 5, a_2 = 15$

C.P. $x^3 - 6x^2 + 11x - 6$ has three roots: $\alpha = 1, \beta = 2, \gamma = 3$

$$\Rightarrow a_n = c_1^n + c_2(2)^n + c_3(3)^n$$

$$n = 0: 2 = c_1 + c_2 + c_3$$

$$n = 1: 5 = c_1 + 2c_2 + 3c_3$$

$$n = 2: 15 = c_1 + 4c_2 + 9c_3$$

$$\text{Solve } \begin{bmatrix} 1 & 1 & 1 & 2 \\ 1 & 2 & 3 & 5 \\ 1 & 4 & 9 & 15 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 2 \end{bmatrix} \Rightarrow \begin{cases} c_1 = 1 \\ c_2 = -1 \\ c_3 = 2 \end{cases}$$

$$\Rightarrow a_n = 1 - 2^n + 2(3^n)$$

Theorem 3.4. The recurrence relation $a_n = ra_{n-1} + sa_{n-2} + f(n)$ has solution $p_n + q_n$ where p_n is a particular solution of the recurrence (ignoring initial conditions) and q_n is the general solution to $a_n = ra_{n-1} + sa_{n-2}$, where constants c_1, c_2 in q_n are found from initial conditions.

Example 3.19. $a_n = 2a_{n-1} + 3a_{n-2} + 5^n \Rightarrow \text{guess } p_n = c5^n$

$$c5^n = 2c5^{n-1} + 3c5^{n-2} + 5^n$$

$$25c = 10c + 3c + 25 \Rightarrow p_n = \frac{25}{12}(5^n)$$

$$12c = 25 \Rightarrow c = \frac{25}{12}$$

$$a_n = 2a_{n-1} + 3a_{n-2}$$

$$x^2 - 2x - 3 = 0$$

$$(x-3)(x+1) = 0$$

$$\alpha = 3, \beta = -1$$

$$q_n = c_1 3^n + c_2 (-1)^n$$

$$\Rightarrow p_n + q_n = \frac{25}{12}(5^n) + c_1 3^n + c_2 (-1)^n$$

Example 3.17. Fibonacci sequence

$$f_n = f_{n-1} + f_{n-2}, f_0 = 0, f_1 = 1$$

Characteristic polynomial: $x^2 - x - 1$

$$x = \frac{1 \pm \sqrt{1+4}}{2} = \frac{1 \pm \sqrt{5}}{2}$$

$$\Rightarrow \alpha = \frac{1 + \sqrt{5}}{2}, \beta = \frac{1 - \sqrt{5}}{2}$$

$$f_n = c_1 \left(\frac{1 + \sqrt{5}}{2}\right)^n + c_2 \left(\frac{1 - \sqrt{5}}{2}\right)^n$$

$$\Rightarrow c_1 = \frac{1}{\sqrt{5}}, c_2 = -\frac{1}{\sqrt{5}}$$

$$\Rightarrow f_n = \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2}\right)^n$$

Note: the method for finding p_n is the equivalent of the constant coefficient method for finding a particular solution to a homogeneous second order ODE, i.e. guess a solution.

Solve for c_1 and c_2 :

$$\begin{aligned} n=0: \quad -2 &= \frac{25}{12} + c_1 + c_2 \\ n=1: \quad 1 &= \frac{125}{12} + 3c_1 - c_2 \end{aligned} \Rightarrow \begin{cases} c_1 = -\frac{27}{8} \\ c_2 = -\frac{17}{24} \end{cases}$$

$$a_n = \frac{25}{12}(5^n) - \frac{27}{8}(3^n) - \frac{17}{24}(-1)^n$$

Example 3.20. $a_n = 2a_{n-1} + 3a_{n-2} + 5n$, $a_0 = 0, a_1 = 1$

As above, $q_n = c_1 3^n + c_2 (-1)^n$

Guess $p_n = An + B$

$$An + B = 2A(n-1) + 2B + 3A(n-2) + 3B + 5n$$

$$0 = (-2-6)A + (-1+2+3)B + (-n+2n+3n)A + 5n$$

$$= 4B - 8A + 4An + 5n = (4B - 8A) + (4A + 5)n$$

$$4A + 5 = 0 \Rightarrow A = -\frac{5}{4}$$

$$4B - 8A = 0 \Rightarrow B = -\frac{5}{2}$$

$$p_n = -\frac{5}{4}n - \frac{5}{2}$$

$$a_n = -\frac{5}{4}n - \frac{5}{2} + c_1 3^n + c_2 (-1)^n$$

$$\begin{aligned} n=0: \quad 0 &= -\frac{5}{2} + c_1 + c_2 \\ n=1: \quad 1 &= -\frac{5}{2} - \frac{5}{4} + 3c_1 - c_2 \end{aligned} \Rightarrow \begin{cases} c_1 = \frac{29}{16} \\ c_2 = \frac{11}{16} \end{cases}$$

$$\Rightarrow a_n = -\frac{5}{4}n - \frac{5}{2} + \frac{29}{16}3^n + \frac{11}{16}(-1)^n$$

3.4 Functions

A function f from X to Y , written $f : X \rightarrow Y$ is a binary relation $f \subset X \times Y$ such that for every $x \in X$, there is at most one $y \in Y$ such that $(x, y) \in f$. Since y is unique for x we can write $y = f(x)$.

Definition 3.6. A surjection is a relation where $\forall y \in Y \exists x \in X$ s.t. $y = f(x)$. (f is "onto".)

Definition 3.7. An injection is a relation where $\forall y \in Y \exists$ at most one $x \in X$ s.t. $y = f(x)$. (f is "one to one".)

Definition 3.8. A bijection is a relation where $\forall y \in Y \exists! x \in X$ s.t. $y = f(x)$. (f is both surjective and injective.)

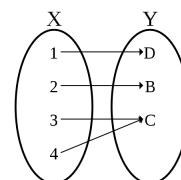


Figure 8: Surjective (non injective) map.

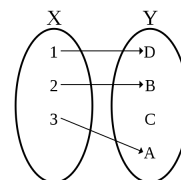


Figure 9: Injective (non surjective) map.

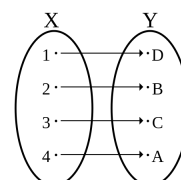


Figure 10: Bijective map.

RELATION TO COUNTING: Recall $|x|$ denotes the cardinality of X (the number of elements)

1. \exists a surjection, $f : X \rightarrow Y \Leftrightarrow |X| \geq |Y|$
2. \exists an injection, $f : X \rightarrow Y$ using every element of $X \Leftrightarrow |X| \leq |Y|$
3. \exists a bijection, $f : X \rightarrow Y \Leftrightarrow |X| = |Y|$

3.5 Counting

PRINCIPLES OF COUNTING:

1. $|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{i=1}^n |A_i|$
if each pair (A_i, A_j) is disjoint ($A_i \cap A_j = \emptyset$)
2. $|A_1 \times A_2 \times \cdots \times A_n| = \prod_{i=1}^n |A_i|$

Example 3.21. How many 4 digits number have no repeated digits?

Answer. The tasks are to choose each digit: $9 \times 9 \times 8 \times 7 = 4536$.
Since the first digit can't be 0.

Example 3.22. How many 4 digit even numbers have no repeated digits?

Answer. We split into 2 cases:

1. Last digit is 0: $9 \times 8 \times 7 \times 1 = 504$
2. Last digit is not 0: $8 \times 8 \times 7 \times 4 = 1792$

Total: 2296.

SOME QUESTIONS:

1. How many functions are there from an n -set to a k -set? (" m -set" = set with m elements)
Sequence of events: let $|X| = n, |Y| = k$. For each $x \in X$, choose $y \in Y$ such that $y = f(x)$.
Number of functions: $\underbrace{k \times k \times \cdots \times k}_{n \text{ times}} = k^n$.
2. How many subsets of an n -set are there?
Sequence of events: take each element and decide to put it in the subset or not: n tasks with 2 possibilities each.
Number of subsets: $\underbrace{2 \times 2 \times \cdots \times 2}_{n \text{ times}} = 2^n$.

Counting objects/structures.

TRANSLATED PRINCIPLES OF COUNTING:
 A_i : ways in which a task can be done.

1. The number of ways which a collection of tasks can be done if no two sets of ways of completing the tasks overlap is the sum of ways of the numbers of ways each task can be done.
2. The number of ways a sequence of tasks can be done is the product of the number of ways each task can be done.

3. How many bijections are there from an n -set to itself?
 1st element has n possible functions values. 2nd element has $n - 1$
 (since it's a bijection). Etc.
 Number of bijections: $(n)(n - 1)(n - 1) \dots (2)(1) = n!$

Definition 3.9. A **permutation** of an n -set is an ordering of its elements. This is precisely the same as a bijection, so there are $n!$ permutations of an n -set.

$X = \{1, 2, 3, 4\}$
 BIJ: $\{(1, 4), (2, 1), (3, 2), (4, 3)\}$
 PERM: 4123

Example 3.23. How many ways can you choose a president, vice president, treasurer, secretary from a group of 7 people?

$$P(7, 4) = \frac{7!}{3!} = 840$$

Definition 3.10. A **k -permutation** of an n -set X is a choice of k elements of X in some order. There are $P(n, k)$ such k -permutations:

4. $P(n, k) = (n)(n - 1) \dots (n - k + 1) = \frac{n!}{(n - k)!}$
5. How many subset of size k does an n -set have?
 Count the number of k -permutations again = $(\# \text{ of } k\text{-subsets})(k!)$
 $P(n, k) = \frac{n!}{(n - k)!} = (\# \text{ of } k\text{-subsets})(k!)$
 $\Rightarrow \text{number of } k\text{-subsets} = \frac{n!}{k!(n - k)!}$

Definition 3.11. $C(n, k) = \binom{n}{k} = \frac{n!}{k!(n - k)!}$ pronounced " n choose k "

Proposition 3.5. $\binom{n}{k} = \binom{n}{n - k}$

Proof. 1. $\binom{n}{n - k} = \frac{n!}{(n - k)!(n - (n - k))!} = \frac{n!}{(n - k)!k!} = \binom{n}{k}$

2. Choosing k elements to be in your set is equivalent to choosing the $n - k$ elements in its complement. \square

3.6 The Binomial Theorem

Theorem 3.6. The Binomial Theorem says that if $n \geq 1$ is an integer,

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$$

where $\binom{n}{k}$ are called binomial coefficients.

Proof. For a positive integer n , what is the coefficient of $x^k y^{n-k}$ in $(x + y)^n$? $(x + y)(x + y) \dots (x + y)$

How many ways can we choose k x 's from the n factors and $n - k$ y 's, choosing one variable from each factor? We only need to count the number of ways to choose x 's (get y 's for free). Thus the coefficient of $x^k y^{n-k}$ is $\binom{n}{k}$. \square

Lemma 3.7. $\sum_{k=0}^n \binom{n}{k} = 2^n$.

Proof. Two methods:

Binomial Theorem: Let $x = y = 1$:

$$(x + y)^n = 2^n = \sum_{k=0}^n \binom{n}{k} (1)(1)$$

Combinatorially:

$$2^n = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n-1} + \binom{n}{n}$$

where 2^n is the number of subsets of an n -set, and $\binom{n}{i}$ is the number of subsets with cardinality i . \square

Lemma 3.8. An n -set, $n \geq 1$, has the same number of even subsets as odd subsets.

Proof. Combinatorially: Fix some element x .

$$\begin{array}{l} \# \text{ odd subsets with } x = \# \text{ even without } x \\ \# \text{ odd subsets without } x = \# \text{ even with } x \\ \hline \# \text{ odd} = \# \text{ even} \end{array}$$

Binomial Theorem: Pick $x = -1, y = 1$.

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

$$\begin{aligned} 0 &= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \binom{n}{4} - \cdots \\ \binom{n}{1} + \binom{n}{3} + \cdots &= \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots \end{aligned} \quad \square$$

Lemma 3.9. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

Proof. $\binom{n}{k}$ is the number of subsets of size k . Define some k . $\binom{n-1}{k}$ is the number of such subsets without x , and $\binom{n-1}{k-1}$ is the number of such subsets including x . \square

Lemma 3.10. $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$

Proof. Rewrite what we want to prove:

$$\begin{aligned}\binom{2n}{n} &= \binom{n}{0}\binom{n}{0} + \binom{n}{1}\binom{n}{1} + \binom{n}{2}\binom{n}{2} + \cdots \\ &= \binom{2n}{n} = \binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{k}\binom{n}{n-k} + \cdots\end{aligned}$$

$$\{1, \dots, 2n\} = \{1, \dots, n\} \cup \{1, \dots, n\}$$

$\binom{2n}{n}$: number of n -subsets

$\binom{n}{k}\binom{n}{n-k}$: number of ways to choose k elements from $\{1, \dots, n\}$ and the rest from $\{n+1, \dots, 2n\}$. \square

Repetitions

1. IF ORDER MATTERS:

Proposition 3.11. Let a_1, a_2, \dots, a_n be a set of elements that can be decomposed into K subsets of elements that are repeated i_k times ($1 \leq k \leq K$), i.e. each subset has size i_k , $\sum i_k = n$. The number of permutations is $\frac{n!}{\prod_{k=1}^K i_k!}$.

Example 3.24. How many anagrams of EASY are there? 4!

What about CHEESE? Not 6! since we have repetition.

If we take $C_1H_1E_1E_2S_1E_3$ we get $6! = (\# \text{ of anagrams of CHEESE})(3!)$,
 $\Rightarrow \# \text{ of anagrams of CHEESE} = \frac{6!}{3!}$

For MISSISSIPPI, $\# \text{ of anagrams} = \frac{11!}{(1!)(4!)(4!)(2!)}$

2. IF ORDER DOESN'T MATTER:

Proposition 3.12. "Balls & Boxes": The number of ways one can distribute k identical balls between n boxes corresponds to a binary string of length $n+k-1$ with $n-1$ 1's & k 0's, i.e. $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$.

Example 3.25. Jim's Morton's offers 30 kinds of Jimbits. How many ways can you choose a dozen?

Answer. $\binom{30+12-1}{29}$

Example 3.27. How many non-negative integers solutions are there to the equation: $x_1 + x_2 + x_3 = 48$?

Answer. 48 balls, 3 boxes: $\binom{48+3-1}{3} = 1225$

What if we impose $x_1 \geq 2$ and $x_3 \geq 5$?

Answer. Let $y_1 = x_1 - 2$, $y_2 = x_2$, $y_3 = x_3 - 5$
 $\binom{41+3-1}{2} = 903$

Visualize "Balls & Boxes" as choosing the positions for the $n-1$ separations between boxes, between $n-1+k$ possible positions (positions include elements and separation lines).

Example 3.26. A sandwich shop offers 3 kinds of bread, 4 kinds of meat and 10 kinds of toppings.

(a) How many possibilities are there if each sandwich has 1 bread, 1 meat and 3 toppings ?

Answer. Number of possible sandwiches: $\binom{3}{1} \times \binom{4}{1} \times \binom{10}{3} = 1440$

How many platters?

Answer. 1440 boxes, 20 balls.
 $\binom{1440+20-1}{20} \approx 6.89 \times 10^{44}$

(b) What if you may now use at most 1 bread, 2 meats and any of toppings?

Answer. Number of possible sandwiches: $\binom{3}{1} \times [\binom{4}{0} + \binom{4}{1} + \binom{4}{2}] \times 2^{10} = 33972$

Number of platters: $\binom{33782+20-1}{20} \approx 1.55 \times 10^{72}$

Example 3.28. How many (non-negative) solutions are there to the equation: $x_1 x_2 x_3 = 48$?

Answer. Notice $48 = 2 \times 2 \times 2 \times 2 \times 3$. So we distribute four 2's to three boxes, and distribute one 3 to three boxes. $\binom{4+3-1}{2} \times 3 = 45$.

Counting Elements in Sets

i.e. How to count the amount of elements in sets $|A_1 \cup A_2 \cup \dots \cup A_n|$ if these sets are not disjoint?

$$n = 2: |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

$$n = 3: |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Theorem 3.13. Principle of Inclusion-Exclusion (PIE).

If A_1, A_2, \dots, A_n are finite sets, then:

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{\substack{S \subseteq [n] \\ S \neq \emptyset}} (-1)^{|S|-1} \left| \bigcap_{i \in S} A_i \right|$$

Proof. Must show every $x \in A_1 \cup \dots \cup A_n$ is counted exactly once on the RHS. Say x appears in k of the sets $A_1 \cup \dots \cup A_n$. x is counted in collections of 1 set k times, of 2 sets $\binom{k}{2}$ times, of 3 sets $\binom{k}{3}$ times, ...

So x counted $\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \dots + (-1)^{k-1} \binom{k}{k}$ times in total.

Recall

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \binom{n}{4} + \dots = 0$$

Therefore we take

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \dots + (-1)^{k-1} \binom{k}{k} = 1$$

so each x is counted once. \square

Example 3.30. n people put their phones in a box. If every person takes a phone out, how likely is it that no one gets their phone back? The number of permutations of $[n]$ (or bijections from $[n] \rightarrow [n]$) where no element is mapped to itself is denoted D_n , they are called derangements.

Let A_i = Set of permutations which map i to itself.

$$\begin{aligned} D_n &= |\overline{A_1} \cap \overline{A_2} \cap \dots \cap \overline{A_n}| \\ &= |\overline{A_1 \cup A_2 \cup \dots \cup A_n}| \\ &= n! - |A_1 \cup A_2 \cup \dots \cup A_n| \end{aligned}$$

Example 3.29. 40 students: where 10 in ANTH, 22 in BIOL, 16 in COMP; 6 in A&B, 8 in B&C, 4 in A&C; and 2 in all. How many students are not enrolled in ANY of the 3 courses?

i.e. first find how many in at least one:

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3| \\ &= (10 + 22 + 16) - (6 + 8 + 4) + 2 = 32 \end{aligned}$$

\therefore There are $40 - 32 = 8$ students in none of the courses.

Here $[n]$ represents $\{1, \dots, n\}$.

However,

$$\begin{aligned}
 |S| &= A_1 \cup A_2 \cup \dots \cup A_n \\
 &= (|A_1| + |A_2| + \dots) - (|A_1 \cap A_2| + |A_1 \cap A_3| + \dots) + \dots \\
 &= n \cdot (n-1)! - \binom{n}{2}(n-2)! + \binom{n}{3}(n-3)! + \dots + (-1)^{n-1} \binom{n}{n}(n-n)! \\
 &= n! - \frac{n!}{2!} + \frac{n!}{3!} + \dots + (-1)^{n-1} \frac{n!}{n!} \\
 &= n! \left(1 - \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{(-1)^{n-1}}{n!} \right) \\
 D_n &= n! - n! \left(1 - \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{(-1)^{n-1}}{n!} \right) \\
 &= n! \left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right) \\
 &= n! \left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + \frac{(-1)^n}{n!} \right) \\
 &= n! \sum_{k=0}^n \frac{(-1)^k}{k!}
 \end{aligned}$$

So calculating the probability:

Recall $e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$ $x \in \mathbb{R}$

$$\begin{aligned}
 \mathbb{P}(\text{a permutation is a derangement}) &= \frac{D_n}{\# \text{ permutations}} = \frac{D_n}{n!} \\
 &= \sum_{k=0}^n \frac{(-1)^k}{k!} = e^{-1}
 \end{aligned}$$

So, as $n \rightarrow \infty$, $\mathbb{P} \approx e^{-1} \approx 0.36788$, and $D_n \approx \frac{n!}{e}$.

Theorem 3.14. Pigeon Hole Principle (PHP). *If one distributes $> n$ objects to n boxes, some box has more than one object.*

Example 3.31. 22 soccer players on a field measuring $42m \times 98m$. Show there are two players no more than $20m$ apart.

Answer. Cut the field into 21 boxes of size 14×14 m . There are 21 boxes and 22 players, therefore 2 players must be in the same square by PHP. $d \leq \sqrt{14^2 + 14^2} = \sqrt{196 + 196} < \sqrt{400} = \sqrt{400} = 20$.

Example 3.32. Let S be a set of 9 points in \mathbb{R}^3 each with integer coordinates. Show $\exists p_i, p_j \in S$ such that the midpoint of $\overline{p_1 p_2}$ has integer coordinates.

Answer. Let $p_i = (x_i, y_i, z_i)$, $p_j = (x_j, y_j, z_j)$.

Want $\frac{x_i + x_j}{2}, \frac{y_i + y_j}{2}, \frac{z_i + z_j}{2} \in \mathbb{Z} \Leftrightarrow x_i + x_j, y_i + y_j, z_i + z_j$ even.

The possible parity combinations are shown in Table 6.

x	y	z
E	E	E
E	E	O
E	O	E
O	E	E
E	O	O
O	E	O
O	O	E
O	O	O

Table 6: Table for Example 3.32

8 parity combinations, 9 points \Rightarrow 2 have same parity, i.e.

$$x_i \equiv x_j \pmod{2} \quad y_i \equiv y_j \pmod{2} \quad z_i \equiv z_j \pmod{2}$$

Therefore $x_i + x_j$, $y_i + y_j$, $z_i + z_j$ are all even.

Example 3.33. Show that if $n + 1$ numbers are chosen from $[2n]$, then there are

(a) 2 which differ by 1:

Answer. Boxes: $\{1, 2\}, \{3, 4\}, \{5, 6\}, \dots, \{2n - 1, 2n\}$
 n boxes, $n + 1$ choices, therefore 2 integers in same box by PHP
 which differ by 1.

(b) 2 which sum to $2n + 1$:

Answer. Boxes: $\{1, 2n\}, \{2, 2n - 1\}, \{3, 2n - 2\}, \dots$
 Each pair sums to $2n + 1$. 2 of the $n + 1$ choices lie in one box by PHP.

Proposition 3.15. Strong version of PHP: If one has $m > n$, m objects, n boxes, then some box receives $\geq \lceil \frac{m}{n} \rceil$ objects.

Example 3.34. 16 students, in 18 chairs. Show there are 6 consecutive occupied seats.

Answer. Split into 3 blocks of 6 chairs. Distribute 16 people across 3 boxes therefore the same box must get $\geq \lceil \frac{16}{3} \rceil = 6$ people.

Example 3.35. A student has 37 days to prepare for an exam. If she studies no more than 60 hours, but at least 1 hour each day, show there is some set of consecutive days over which she studied exactly 13 hours (whole hours each day).

Answer. Let s_i = number of hours studied on day i . Let $a_i = s_1 + s_2 + \dots + s_i$ (number of hours studied from day 1 to day i).

$$1 \leq a_1 < a_2 < \dots < a_{37} \leq 60$$

$$14 \leq a_1 + 13 < a_2 + 13 < \dots < a_{37} + 13 \leq 73$$

Consider the list $a_1, a_2, \dots, a_{37}, a_1 + 13, a_2 + 13, \dots, a_{37} + 13$. There are 74 integers between 1 and 73 therefore 2 must be the same. $\Rightarrow i, j$ s.t.
 $a_i = a_j + 13 \Leftrightarrow a_i - a_j = 13 \Leftrightarrow s_{j+1} + s_{j+2} + \dots + s_i = 13$

4 Graph Theory

4.1 Introduction

Definition 4.1. A **graph** G is a pair (V, E) where V is a set (whose elements are the vertices of the graph) and E is a set of unordered pairs of elements of V (called the edges of G).

We often write $V(G)$ and $E(G)$ for the vertices/edges if $G = (V, E)$. Also, for brevity, we write $uv \in E(G)$ for the edge $\{u, v\}$.

Example 4.1. $V = \{v_1, v_2, v_3, v_4\}$
 $E = \{v_1v_2, v_1v_3, v_1v_4, v_2v_3, v_2v_4, v_3v_4\}$

USES OF GRAPHS:

1. **Routing problems:** V = locations, E = direct passage between locations.
2. **Social networks:** V = users, E = friends.
3. **Scheduling:** V = events, E = pairs of events which cannot coincide.

Definition 4.2. Given $v \in V(G)$ and $e \in E(G)$, if $v \in e$, then we say that e is **incident** to v . If $uv \in E(G)$, we say that u and v are **adjacent** (neighbours).

Definition 4.3. The **neighbourhood** of $v \in V(G)$ is:

$$N(v) = \{u \mid uv \in E(G)\}$$

Definition 4.4. The **degree** of $v \in V(G)$ in G is $d(v) = |N(v)|$. We can also write this as $\deg(v)$, or $N_G(v)$, $d_G(v)$ which make it clear to which graph one is referring. In general, $0 \leq \deg_G(v) \leq |V(G)| - 1$

Definition 4.5. The **degree sequence** of G is a list of the degrees (in increasing order).

Theorem 4.1. If G is a graph, then $\exists u, v \in V(G)$ s.t. $d(u) = d(v)$.

Proof. Case 1: Suppose $\deg(u) \neq 0 \forall u \in V(G)$. Let $|V(G)| = n$. Then $1 \leq \deg(n) \leq n - 1$. There are n vertices and $n - 1$ possible degrees. By PHP, two vertices have the same degree.

Case 2: $\exists u$ s.t. $\deg(u) = 0$. Then $0 \leq \deg(n) \leq n - 2$. $n - 1$ possible degrees & n vertices, so 2 must have the same degree by PHP. \square

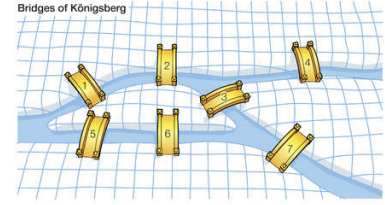


Figure 11: **Bridges of Königsberg:** can you start anywhere in the city, cross every bridge exactly once and finish where you started?

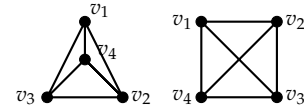


Figure 12: These two figures represent identical graphs (the one in Exercise 4.1).

Graphs are often represented pictorially where $V(G)$ is a set of points or dots, and each edge is a segment or curve between points; but a drawing of a graph is not the graph itself.

Lemma 4.2. Handshaking Lemma. says that in any graph G , there are an even number of vertices with odd degree.

Theorem 4.3. If G is a graph, then $\sum_{v \in V(G)} \deg(v) = 2|E(G)|$

Proof. Count the number of pairs (v, e) such that e is incident to v . Each vertex v appears $\deg(v)$ times in the set of pairs. Each edge appears exactly twice.

$$\sum_{v \in V(G)} \deg(v) = \sum_{e \in E(G)} 2 = 2|E(G)| \quad \square$$

Proof. of Handshaking Lemma (Lemma 4.2).

$$\sum_{\substack{v \in V(G) \\ \deg(v) \text{ odd}}} \deg(v) + \underbrace{\sum_{\substack{v \in V(G) \\ \deg(v) \text{ even}}} \deg(v)}_{\text{even}} = \underbrace{2|E(G)|}_{\text{even}} \quad \square$$

SPECIAL GRAPHS:

- empty graph: $E(G) = \emptyset$
- complete graph: $E(G) =$ all possible pairs:
 - denoted K_n if $|V(G)| = n$
 - $|E(K_n)| = \binom{n}{2}$ [in general, $0 \leq |E(G)| \leq \binom{n}{2}$]
- complete bipartite graph $K_{m,n}$ where :
 - $V(K_{m,n}) = \{u_1, \dots, u_m, v_1, \dots, v_n\}$
 - $E(K_{m,n}) = \{u_i v_j | 1 \leq i \leq m, 1 \leq j \leq n\}$
 - $\implies |V(K_{m,n})| = m + n$
 - $\implies |E(K_{m,n})| = m \cdot n$
- Path P_n : $V(P_n) = \{v_1, \dots, v_n\}, E(P_n) = \{v_1 v_2, v_2 v_3, \dots, v_{n-1} v_n\}$
 $\implies |E(P_n)| = n - 1$
- Cycle C_n : $V(C_n) = \{v_1, \dots, v_n\}$
 $E(C_n) = \{v_1 v_2, v_2 v_3, \dots, v_{n-1} v_n, v_n v_1\}$
 $\implies |E(C_n)| = n$

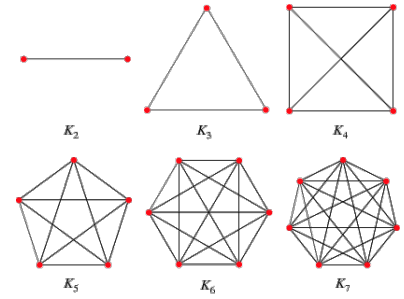


Figure 13: Complete Graphs.

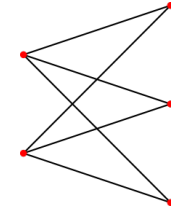


Figure 14: $K_{2,3}$.

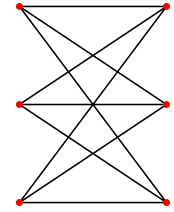


Figure 15: $K_{3,3}$.

Definition 4.6. We say H is a **subgraph** of G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$. Equivalent: obtain H from G by deleting edges and/or vertices. Note that when we delete $v \in V(G)$, we delete all incident edges as well. If $V(H) = V(G)$ we say that H is a **spanning subgraph**.

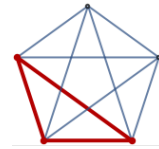


Figure 16: The red part is a subgraph of the entire graph.

Definition 4.7. A **walk** in G is a sequence of vertices $v_0, v_1, v_2, \dots, v_k$ where $v_{i-1}v_i \in E(G) \forall 1 \leq i \leq k$.

A **path** in a graph is a walk with no repeated vertices. A **closed walk** is a walk where $v_0 = v_k$: v_0 and v_k are the ends of a walk.

A closed path is a **cycle**.

Definition 4.8. A graph is **connected** if $\forall u, v \in V(G)$ there is a walk with ends u and v . The maximal connected subgraphs of G are called its **connected components**.

Definition 4.9. A **multigraph** M is a set (of vertices) $V(M)$ and a list of unordered pairs of vertices where repetition is allowed (i.e. $vv \in E(M)$).

Definition 4.10. An **Eulerian walk** in a graph (or multigraph M) is a closed walk which uses every edge exactly once. If G has an Eulerian walk, we call G **Eulerian**.

Theorem 4.4. (*Euler, 1736*). G is Eulerian if and only if it is connected and all vertices have even degree.

Proof.

$(\Rightarrow) \forall v \in V(G)$, the number of times an Eulerian walk enters v equals the number of times it exits v . $\Rightarrow \deg(v) = k + k = 2k$ for some k .

(\Leftarrow) Suppose G is connected and $\deg(v)$ even $\forall v \in V(G)$. Let W be a *longest* walk in G with no repeated edges $W = v_0, v_1, \dots, v_k$.

Suppose W is not Eulerian.

Claim: W is closed.

Proof. Suppose it is not.

\Rightarrow we used odd number of edges incident to v_k

$\Rightarrow \exists$ an unused edge incident v_k

\Rightarrow we can extend W by 1. $\Rightarrow \Leftarrow$ with maximality of W . \square

So there is some edge in $E(G)$ not used by W . Because G is connected, there must be an edge uv_i not used by W for some $0 \leq i \leq k$. This contradicts maximality of W : $u, v_i, v_{i+1}, \dots, v_k = v_0, v_1, \dots, v_i$ is longer. $\Rightarrow \Leftarrow$. So G is Eulerian. \square

Definition 4.11. A path in G is **Hamiltonian** if it has $|V(G)|$ vertices (it "spans" G). A Hamiltonian cycle is a cycle in G with $|V(G)|$ vertices. A graph is Hamiltonian if it has a Hamiltonian cycle.

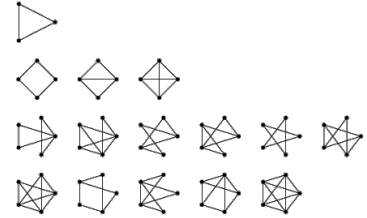


Figure 17: Connected components. Note that a single vertex is a connected component.

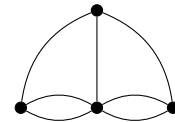
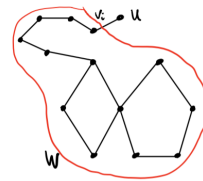


Figure 18: We can recall the Königsberg problem: V are land masses and E are bridges.



This result (Theorem 4.4) holds for multigraphs as well. Note that $\deg(v)$ counts a "loop" (edge between the same node) $w \in E(M)$ twice.

Finding Hamiltonian cycles, as a rule, is difficult (unless $P = NP$:').

Are there sufficient conditions for G to be Hamiltonian?

Theorem 4.5. (Bondy & Chvátal, 1972). *If $\deg(u) + \deg(v) \geq |V(G)|$ $\forall u, v \in V(G)$, then G is Hamiltonian $\Leftrightarrow G + uv$ is Hamiltonian where $uv \notin E(G)$.*

Proof. Show G is Hamiltonian $\Leftrightarrow G + uv$ is Hamiltonian where $uv \notin E(G)$.

(\Rightarrow) Trivial.

(\Leftarrow) If G is Hamiltonian, then done. Now suppose G is not Hamiltonian. $\Rightarrow \exists$ a Hamiltonian path from u to v in G , say P (Figure 19).

Let S be the neighbors of u which lie on P . Let T be the vertices which follow neighbors of v on P . $|S| + |T| \geq |V(G)|$

By PHP, there must be some vertex in $S \cap T$, say v_i .

$\Rightarrow v_i, v_{i+1}, \dots, v, v_{i-1}, v_{i-2}, \dots, v_1, u, v_i$ is a Hamiltonian cycle of G . \square

Theorem 4.6. (Ore, 1960). *If $d(u) + d(v) \geq |V(G)| \forall u, v \in V(G)$ nonadjacent, then G is Hamiltonian. This leads straightforwardly to (Dirac, 1952): If $\deg_G(v) \geq \frac{|V(G)|}{2}$ then G is Hamiltonian.*

Proof. By adding edges to the graph and applying Theorem 4.5 repeatedly, we get a complete graph, which is Hamiltonian. By the "iff" statements, G is Hamiltonian as well. \square

4.2 Trees

Definition 4.12. A graph is a **tree** if it is connected and has no cycles. A **leaf** of a graph is a vertex of degree 1.

Theorem 4.7. *If $\deg(v) \geq 2 \forall v \in V(G)$, then G contains a cycle.*

Proof. Let P be a maximal path in G : $P = v_0, v_1, v_2, \dots, v_k, v$

Since it has $\deg(v) \geq 2$, it has some neighbor other than v_k . By the maximality of P , this neighbor must be in P , say v_i . Thus $v_i v_{i+1} \dots v_k v v_i$ is a cycle. \square

Corollary 4.8. *Every tree has a leaf.*

Proof. Contrapositive proof. Left to the reader. \square

Theorem 4.9. *A connected graph is a tree if and only if there is a unique path between any 2 vertices.*

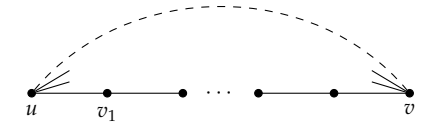
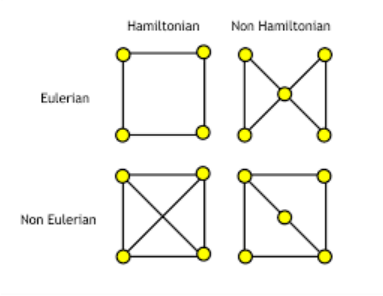


Figure 19: Hamiltonian path P .

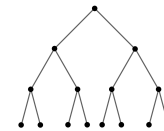
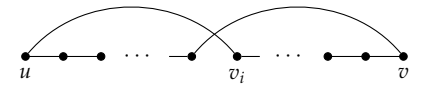


Figure 20: Binary tree. (Any k -ary $K_{1,t}$ is also a tree.)

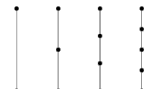


Figure 21: Any path P_n is a tree.

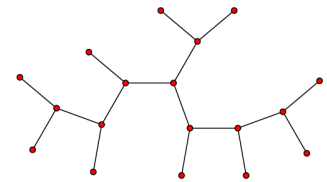


Figure 22: A general tree.

Proof. (\Rightarrow) Since it is connected, there is at least one path between any two vertices. To prove uniqueness, suppose P_1 and P_2 are distinct uv -paths. Let v_i be the last vertex P_1 and P_2 have in common aside from v . Let v_j be the next vertex in P_1 shared with P_2 . The subpaths of P_1 and P_2 from v_i to v_j together thus form a cycle.

$\Rightarrow \Leftarrow$

(\Leftarrow) Let G be a connected graph that is not a tree. The G has a cycle, C. If $u, v \in V(C)$, then there are ≥ 2 uv -paths. \square

Theorem 4.10. Every tree on ≥ 2 vertices has at least 2 leaves.

Proof. by induction, on the number of vertices.

Base: $n = 2$: the tree on two nodes has 2 leaves.

I.H.: Assume true for $n - 1$ vertices. Let T be an arbitrary tree with n vertices. Let x be a leaf of T , let $T' = T - x$. T' has $n - 1$ vertices, and is a tree because we are removing one node from T , a tree.

If $u, v \in V(T')$, then there exists a unique path in T' between them (the unique path in T could not contain x since $\deg(x) = 1$).

Then T' has ≥ 2 leaves, say y, z . Since $\deg(x) = 1$, x is adjacent to at most one of y and z .

Then x and at least one of y, z are leaves in T . \square

Theorem 4.11. A connected graph is a tree \Leftrightarrow the deletion of any edge disconnects the graph.

Proof. c.f. textbook (LPV). \square

Theorem 4.12. An n -vertex tree has $n - 1$ edges.

Proof. Base: $n = 1$: one node, zero edges.

I.H.: Assume true for $n - 1$ vertices. Let T be an n -vertex tree, and let x be a leaf. By the I.H., $T - x$ has $n - 2$ edges (because it is an $(n - 1)$ -vertex tree). Then T must have $n - 1$ edges. \square

Theorem 4.13. Adding an edge to a tree creates exactly one cycle.

Proof. Let u, v be non-adjacent vertices. There exists a uv -path, say $P = uv_1 \dots v_k v$. Thus adding uv creates a cycle. Now we must prove that it creates exactly one. Suppose there are more than one.

Any cycle created must contain the edge uv . (Otherwise there is a cycle in the original tree $\Rightarrow \Leftarrow$). But then deleting uv from these cycles gives distinct uv -paths in the tree, contradicting uniqueness (Theorem 4.9). \square

Added clarification: we can let the alleged two cycles created by adding uv be $(u, v, \dots, a, b, \dots, u)$ and $(u, v, \dots, x, y, \dots, u)$.

Removing uv , we get two paths from v to u : $(v, \dots, a, b, \dots, u)$ and $(v, \dots, x, y, \dots, u)$. $\Rightarrow \Leftarrow$ with path uniqueness.

Definition 4.13. A **spanning tree** of a graph G is a subgraph T such that $V(T) = V(G)$ and T is a tree.

Theorem 4.14. *Every connected graph has a spanning tree.*

Proof. Base: Trivially true for $n = 1$.

I.H.: Assume true for $|V(G)| = n - 1$.

Delete any vertex v from our graph, which does not disconnect it.¹⁶ The resulting $(n - 1)$ -vertex graph has a spanning tree. Add the edge vx to the tree for any $x \in N(v)$. The resulting subgraph:

- uses every vertex
- is connected
- contains no cycles (any cycle would contain v which has degree 1 in the subgraph). \square

¹⁶ **Exercise:** Prove that any connected graph has a vertex whose deletion does not disconnect the graph.

Counting Trees

Theorem 4.15. Cayley's Theorem. *There are n^{n-2} different trees on n labelled vertices.*

Proof.

- See LPV for proof using bijection between trees and "Prufer codes".
- c.f. Kirchhoff's Theorem, using linear algebra. \square

THERE IS NO theorem for the number of unlabelled trees on n vertices. However, we can find bounds.

Let T_n denote the number of unlabelled n -vertex trees.

$$n^{n-2} \leq n! T_n \tag{1}$$

$$\frac{n^{n-2}}{n!} \leq T_n$$

$$T_n \leq \binom{2n-2}{n-1} \tag{2}$$

Start at root, draw the tree so that no edges cross and vertices at distance i from root are at level i . Walk around the edges and record \mathcal{D} if you move down 1 edge and \mathcal{U} if you move up one edge. Thus the code has length $2|E(T)| = 2(n - 1)$ and has $n - 1$ \mathcal{U} 's and $n - 1$ \mathcal{D} 's, yielding a code that looks like $UUDUDDUU \dots$

Thus the number of combinations of codes is $\binom{2n-2}{n-1}$.

Some trees are counted more than once, but each tree is counted at least once.

$$\implies T_n \leq \binom{2n-2}{n-1}$$

Using Stirling's Approximation, we can say that for large n ,

$$\frac{e^n}{\sqrt{2\pi n^{5/2}}} \leq T_n \leq \frac{4^{n-1}}{\sqrt{2\pi n - 1}}$$

Stirling's Approximation:

$$\lim_{n \rightarrow \infty} \frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} = 1$$

4.3 Graph Colouring

Cliques and Independent Sets

Definition 4.14. Some more terminology:

$\Delta(G)$ = maximum degree of vertices in G

$\delta(G)$ = minimum degree of vertices in G

G is d -regular if $\deg_G(v) = d \forall v \in V(G)$

(G is regular if it is d -regular for some d .)

Definition 4.15. A **clique** in a graph G is a set $X \subseteq V(G)$ such that $uv \in E(G) \forall u, v \in X, u \neq v$, i.e. X is a complete subgraph of G .

The **clique number** of G is $\omega(G)$ = size of largest clique in G .

Definition 4.16. An **independent set** (or stable set) is a set $X \subseteq V(G)$ such that $uv \notin E(G) \forall u, v \in X$, i.e. X is an empty subgraph of G .

The **independence number** of G is $\alpha(G)$ = size of largest independent set in G .

Definition 4.17. A **proper vertex k -colouring** is a map $c : V(G) \rightarrow [k]$ such that if $uv \in E(G)$ then $c(u) \neq c(v)$. The **chromatic number** of G is $\chi(G)$ = the smallest k for which a proper vertex k -colouring exists.

Example 4.2.

G	δ	Δ	ω	α	χ
P_n	1	2	2	$\lceil \frac{n}{2} \rceil$	2
C_n	2	2	3 if $n = 3$ 2 otherw.	$\lfloor \frac{n}{2} \rfloor$	2 if n even 3 if n odd
K_n	$n - 1$	$n - 1$	n	1	n
$K_{m,n}$	m	n	2	n	2

Definition 4.18. A graph is **bipartite** if $V(G)$ can be partitioned into two independent sets.

Proper vertex k -colourings partition $V(G)$ into k independent sets.

G is bipartite $\Leftrightarrow \chi(G) \leq 2$

Theorem 4.16. G is bipartite $\Leftrightarrow G$ contains no odd cycles.

Lemma 4.17. *If H is a subgraph of G , then $\chi(H) \leq \chi(G)$.*

Proof. If c is a proper k -coloring of G , then $\forall u, v \in V(H)$ which are adjacent, $c(u) \neq c(v)$, so c is a proper k -colouring of H . \square

Lemma 4.18. *Every closed odd walk of a graph contains an odd cycle (length = number of edges).*

Proof. by strong induction on the length of the walk r .

Base: $r = 3$

The only closed walk of length 3 is a cycle of length 3.



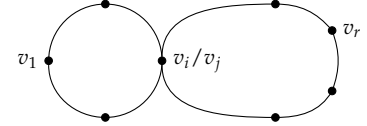
I.H. Assume true for all odd integers less than $r = 2t + 1$.

Take a close walk of length r : $v_0, v_1, \dots, v_{r-1}, v_r = v_0$

If there are no repeated vertices (other than $v_0 = v_r$), then this is an odd cycle.

If there are repeated vertices, i.e. $\exists i, j$ such that $v_i = v_j$ and $0 \leq i < j < r$. Let $W_1 = v_0, v_1, \dots, v_i, v_{j+1}, \dots, v_r$ and $W_2 = v_i, v_{i+1}, \dots, v_j$.

W_1 and W_2 together form the original odd closed walk. Since $|W_1| < |W|$ and $|W_2| < |W|$ and each of the two walks is a closed walk, the induction hypothesis guarantees that whichever of W_1 or W_2 has odd length contains an odd cycle. This must be a cycle of W as well. \square



Proof. of Theorem 4.16: G is bipartite $\Leftrightarrow G$ contains no odd cycles.

(\Rightarrow) If G has an odd cycle C , then $3 = \chi(C) \leq \chi(G) \Rightarrow G$ is not bipartite. $\Rightarrow \Leftarrow$

(\Leftarrow) Suppose G has no odd cycles. Let $u \in V(G)$. Now define

$$X = \{x \in V(G) \mid u \text{ and } x \text{ have even distance}\}$$

$$Y = \{y \in V(G) \mid u \text{ and } y \text{ have odd distance}\}$$

We must show any two vertices in X (or in Y) are nonadjacent.

Suppose not. Let $x, x' \in X$ and $xx' \in E(G)$. By construction there is an even length path from u to x say P and from u to x' say P' .

Then P with xx' with P' is a closed walk of odd length in G , $\Rightarrow G$ has an odd cycle. $\Rightarrow \Leftarrow$

Similarly, if $y, y' \in Y$ and $yy' \in E(G)$, then we get a closed odd walk from the odd uy -path, yy' and the odd uy' -path. $\Rightarrow \Leftarrow$ \square

"distance" is the length of the shortest path between vertices.

Note: $u \in X$ since u is at distance 0 from itself.

General colorings LOWER BOUNDS ON \mathcal{G}

Recall that $\chi(G) \geq \chi(H) \forall$ subgraph H of G . If H is the largest complete subgraph, then:

$$\chi(G) \geq \omega(G)$$

Since a proper k -colouring partitions $V(G)$ into independent sets,

$$\chi(G) \geq \frac{|V(G)|}{\alpha(G)}$$

To see this, let $C_i = \{v \in V(G) | c(v) = i\}$ for some proper $\chi(G)$ -colouring, then:

$$|V(G)| = \sum_{i=1}^{\chi(G)} |C_i| \leq \sum_{i=1}^{\chi(G)} \alpha(G) = \chi(G)\alpha(G)$$

UPPER BOUNDS ON $\chi(G)$

GREEDY COLOURING ALGORITHM ($G = (V, E)$)

- 1 order $V(G)$ arbitrarily v_1, v_2, \dots, v_n
- 2 colour $V(G)$ in this order assigning $c(v_i)$ the smallest colour not yet assigned to its neighbours.

This algorithm **doesn't** guarantee the optimal colouring. At any vertex, the max number of forbidden colours is its degree. So the greedy algorithm gives: $\chi(G) \leq \Delta(G) + 1$.

Theorem 4.19. *Brook's Theorem (1941). If G is not complete or an odd cycle, then $\chi(G) \leq \Delta(G)$.*

Proof. Beyond the scope of this course. □

Theorem 4.20. *If G is not regular, then $\chi(G) \leq \Delta(G)$.*

Proof. by algorithm:

BFS (BREADTH FIRST SEARCH) ALGORITHM ($G = (V, E)$)

- 1 Insert any vertex into a first-in-first-out (FIFO) queue Q .
- 2 **while** $Q \neq \emptyset$
- 3 Remove the next vertex x from Q and mark it "visited".
- 4 Place any neighbors of x which are not yet marked "visited" into the queue (and ignore other neighbors).

OUTPUT: ordering of $V(G)$ in the order they are marked visited.

Choose a vertex v_1 whose degree is NOT $\Delta(G)$: $\deg(v_1) \leq \Delta(G) - 1$. (We can do this since the graph is not regular.)

Now run BFS with v_1 as the initial vertex, yielding an ordering of $V(G)$: $v_1, v_2, \dots, v_{n-1}, v_n$.

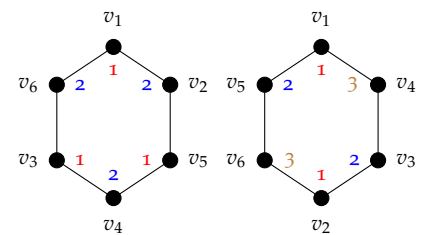


Figure 23: Left is an optimal coloring, right is non optimal. So the output depends on node ordering.

We can build a "BFS" tree, but we don't need it here.

Every v_i , $i \geq 2$ has a neighbour v_j with $j < i$ because for v_i to get placed in the queue, we must have already visited some neighbour v_j . We then colour the vertices in reverse order v_n, \dots, v_1 .

For $2 \leq i \leq n$, when we colour v_i , at least one of its neighbours has yet to be coloured (v_j from discussion above), which means that AT MOST $\deg(v_i) - 1$ colours have been used on the neighbours of v_i while greedily colouring, \Rightarrow at most $\Delta(G) - 1$ forbidden colours at every step, since $\deg(v_1) \leq \Delta(G) - 1$. \Rightarrow if we have $\Delta(G)$ colours, there will always be an available colour: $\therefore \chi(G) \leq \Delta(G)$ \square

4.4 Planar Graphs

Definition 4.19. A graph is **planar** if it can be drawn in the Euclidian plane so that the edges do not cross (only meet at vertices).

K_5 seems like it cannot be planar since there are vertices that cannot be joined without crossing other edges. But proofs along these lines require the Jordan Curve Theorem which will not be touched in Math 240. We will use an alternate proof.

Definition 4.20. Given a plane drawing G^* of a planar graph G , we define a **face** to be a maximal region bounded by edges.

Theorem 4.21. Euler's Formula.

If G^* is a plane drawing of a connected planar graph G with M vertices, $|E|$ edges, and $|F|$ faces, then: $|V| - |E| + |F| = 2$.

Proof. By induction on $|E|$.

Base: $|F| = 1$. If $|F| = 1$, then G^* has no cycles $\Rightarrow G$ is a tree $\Rightarrow |E| = |V| - 1$ and $|V| - |E| + |F| = |V| - (|V| - 1) + 1 = 2$

I.H.: Suppose true for $|F| = k - 1$.

Let G^* have $k \geq 2$ faces. Since G is not a tree, it has a cycle C .

Let e be an edge of C . Consider $G - e$. It is still planar. It is also still connected any walk that used e can be modified by replacing e with $C - e$. Thus e touches 2 faces since its deletion doesn't disconnect G^* (or G). Therefore deleting e merges the 2 faces into 1. By induction, the new graph with $|V'|, |E'|, |F'|$ satisfies

$$\begin{aligned} |V'| - |E'| + |F'| &= 2 \\ \Rightarrow |V| - (|E| - 1) + (|F| - 1) &= 2 \\ \Rightarrow |V| - |E| + |F| &= 2 \end{aligned} \quad \square$$

This means that $|F|$ is invariant for a graph G : the number of faces does not depend on its drawing.

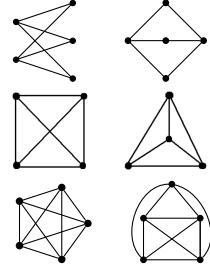


Figure 24: $K_{2,3}$ and K_4 have planar representations. K_5 seems like it does not.

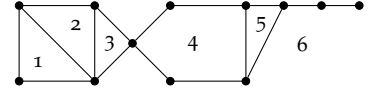


Figure 25: Example of a planar graph. Every drawing has an unbounded face called the outer face.

Note: The vertices of any face in a drawing can be made to be the vertices of the outer face.

Note: Each edge touches at most 2 faces. If an edge touches exactly one face, deleting it disconnects the graph.

Proofs are omitted since they use topology.

Theorem 4.22. If G is a connected planar graph, with $|V| \geq 3$, then

$$|E| \leq 3|V| - 6$$

Proof. Count the number of pairs (e, f) where e touches f . Call this number T . Since each edge touches at most 2 faces, $T \leq 2|E|$. But every face touches at least 3 edges (no self-touching edge or 2 edges with 2 vertices).

$$\begin{aligned} T &\geq 3|F| \\ 3|F| &\leq T \leq 2|E| \\ |F| &\leq \frac{2}{3}|E| \\ \Rightarrow 2 &= |V| - |E| + |F| \leq |V| - |E| + \frac{2}{3}|E| \\ \Rightarrow \frac{1}{3}|E| &\leq |V| - 2 \\ |E| &\leq 3|V| - 6 \quad \square \end{aligned}$$

Note: $K_{3,3}$ is also non-planar. But it satisfies the above property.

Theorem 4.23. Kuratowski (1930). G planar $\Leftrightarrow G$ has no K_5 or $K_{3,3}$ subdivision.

Definition 4.21. A **minor** of G is a graph obtained by deleting vertices, deleting edges or contracting edges (Figure 26).

Example 4.3. Show K_5 is non-planar:

$$\begin{aligned} |V| &= 5 \\ |E| &= \binom{5}{2} = 10 \\ 10 &\not\leq 3(5) - 6 = 9 \end{aligned}$$

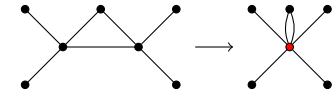


Figure 26: Edge contraction.

Theorem 4.24. Wagner (1937). G planar $\Leftrightarrow G$ has no K_5 or $K_{3,3}$ minor.

Proof. Beyond the scope of this course. ;-; □

Theorem 4.25. If G is planar with no triangles $\Rightarrow |E(G)| \leq 2|V(G)| - 4$.

Proof. Count pairs (e, f) where edge e touches face f . Let T be the number of such pairs.

$$\begin{aligned} 4|F| &\leq T \leq 2|E| \\ |F| &\leq \frac{1}{2}|E| \\ \Rightarrow 2 &= |V| - |E| + |F| \leq |V| - |E| + \frac{1}{2}|E| \\ \Rightarrow |E| &\leq 2|V| - 4 \quad \square \end{aligned}$$

Example 4.4. $K_{3,3}$ is bipartite \Rightarrow no odd cycles \Rightarrow no triangles.

$K_{3,3}$ planar $\Rightarrow 9 \leq 2(6) - 4 = 8$.

Contradiction, implying $K_{3,3}$ non-planar.

Theorem 4.26. Every planar graph is 4-colourable ($\chi(G) \leq 4$).

Proof. Appel and Haken, 1976. No human readable proof exists. \square

Theorem 4.27. Every planar graph is 5-colourable.

Lemma 4.28. If G is planar, then $\delta(G) \leq 5$.

Proof. Suppose $\delta(G) \geq 6$, so $\deg(v) \geq 6 \forall v \in V(G)$.

$$\begin{aligned} \sum_{v \in V(G)} \deg(v) &= 2|E| \\ \Rightarrow 6|V| &\leq 2|E| \\ \Rightarrow |E| &\geq 3|V| \quad \Leftrightarrow \text{since } |E| \leq 3|V| - 6 \quad \square \end{aligned}$$

Proof. of Theorem 4.27, by induction on $|V(G)|$.

Base: Trivial if $|V(G)| \leq 5$.

I.H.: Assume true for $|V(G)| = n - 1$ and let G be a planar graph with n vertices. We know $\exists v \in V(G)$ with $\deg(v) \leq 5$ (by Lemma 4.28).

Case 1: $\deg(v) \leq 4$. Delete v and 5-colour $V(G - v)$ by induction.

At most 4 colours are used on the neighbours. of v , so there is an available colour for v .

Case 2: $\deg(v) = 5$. Delete v and 5-colour $V(G - v)$ If 4 or fewer colours are used on the neighbours of v then we have a colour available for v .

If each neighbour of v got a distinct colour:

Let $N(v) = \{x_1, x_2, x_3, x_4, x_5\}$. Say $c(x_i) = i$. Let G_{13} be the subgraph of G consisting of all vertices coloured 1 or 3 and all edges of G between them.

If x_1 and x_3 are not in the same connected component of G_{13} , then we take the component of G_{13} containing x_1 and "flip" the colours of its vertices (3 to 1 and 1 to 3: Figure 27). This is still a proper colouring of $G - v$ and now we can colour v with 1.

If x_1 and x_3 are in the same connected component: then there is a path P_{13} in G_{13} from x_1 to x_3 (whose vertices are all coloured 1 or 3). $P_{13} \cup \{x_1v, x_3v\}$ form a closed curve. One of x_2 and x_4 lies inside and one lies outside. Look at the subgraph of $G - v$ with vertices coloured 2 and 4. x_2 and x_4 cannot be in the same connected component, or else there is an x_2x_4 -path with vertices coloured 2 and 4 which intersects $P_{13} \cup \{x_1v, x_3v\}$. So we take the component of G_{24} containing x_2 and swap colours 2 and 4.

This leaves the colour 2 available for v . \square

Proof. Alternate: see LPV p. 208-209. \square

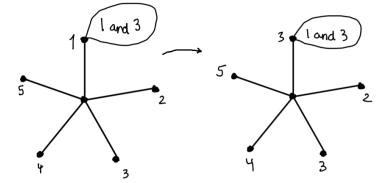


Figure 27: If x_1 and x_3 are not in the same connected component, flip all vertices coloured 1 and 3.

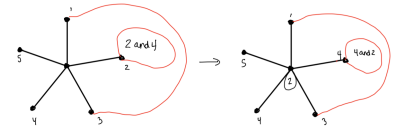


Figure 28: If x_1 and x_3 are in the same connected component, flip the colour of x_2 (and connected components).

4.5 Weighted Graphs

Definition 4.22. A **weighted graph** is a graph G and a function $w : E(G) \rightarrow \mathbb{R}$ where $w(e)$ is the weight of e .

Notation 4.29. If H is a subgraph of G , we use $w(H) = \sum_{e \in E(H)} w(e)$.

TYPES OF PROBLEMS we might wish to solve:

1. Find a uv -path P where $w(P)$ is minimum.
c.f. Dijkstra's Algorithm.
2. Find a spanning tree T with $w(T)$ minimum.
c.f. Kruskal's Algorithm and Prim's Algorithm.
3. Find a spanning closed walk W such that $w(W)$ is minimum.
c.f. Traveling Salesman Problem (difficult, but one can find W such that $w(W) \leq \frac{3}{2}w(W_{\text{optimal}})$).

DIJKSTRA'S ALGORITHM(G): find minimum weight uv -path.

- 1 Assign label $(-, 0)$ to u
// The elements in the tuple (a, b) are a : the preceding vertex;
// b : the weight of the minimum path from u .
- 2 if v is unlabelled
- 3 if \exists no unlabelled vertex adjacent to a labelled vertex
- 4 **return** no path.
- 5 **else for** each $xy \in E(G)$ s.t. x labelled (t, W) and y unlabelled
- 6 compute $W + w(xy)$
- 7 choose xy pair with minimum $W + w(xy)$
- 8 label y $(x, W + w(xy))$
- 9 **else** (v is labelled)
- 10 **return** the path iteratively obtained by taking v , the vertex from its label, the vertex from that vertex label, etc. (i.e. by backtracking)

A BRIEF INTRO TO COMPLEXITY ANALYSIS: here we have two types of steps - comparison and addition. At the k th iteration, we have labelled k vertices. Thus there are $\leq k(n - k)$ additions.

Fact: to find the smallest (or largest) element from a set of size t , we need $\leq t - 1$ comparisons. Therefore, $\leq k(n - k) - 1$ comparisons to choose xy . The worst case number of steps:

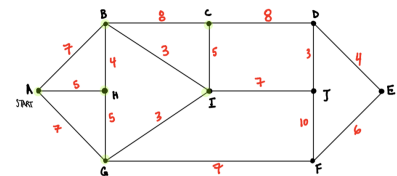


Figure 29: Minimum weight path for this graph is AGFE.

Recall:

$$\sum_{k=1}^t k = \frac{t(t+1)}{2}$$

$$\sum_{k=1}^t k^2 = \frac{t(t+1)(2t+1)}{6}$$

$$\begin{aligned}
& \sum_{k=1}^{n-1} [k(n-k) + k(n-k) - 1] \\
&= \sum_{k=1}^{n-1} 2nk - \sum_{k=1}^{n-1} 2k^2 - \sum_{k=1}^{n-1} 1 \\
&= 2n \frac{n(n-1)}{2} - 2 \frac{(n-1)(n)(2n-1)}{6} - (n-1) \\
&= \frac{1}{3}n^3 - \frac{4}{3}n + 1
\end{aligned}$$

KRUSKAL'S ALGORITHM(G): find minimum weight spanning tree.

G is a connected weight graph.

- 1 Find edge with minimum weight e_1 .
- 2 $k \leftarrow 1$
- 3 **while** $k < n$
- 4 **if** $\exists e \in E(G)$ such that $\{e\} \cup \{e_1, \dots, e_k\}$ has no cycle
- 5 Set e_{k+1} as the unused edge having least weight
which does not make a cycle.
- 6 $k \leftarrow k + 1$
- 7 **else return** e_1, e_2, \dots, e_k and exit.

Proof. Let T_k be the output. $T_k = \{e_1, \dots, e_k\}$ satisfies the following:

- has no cycle: by construction.
- is spanning: if $v \notin V(T_k)$ then any edge incident to v could still be added (and the algorithm would not have stopped).
- is connected: let $v, w \in V(G)$. Since G is connected, $\exists vw$ -path in G , say P_{vw} . If P_{vw} is in T_k , then done.
Else, let $e \in E(P_{vw}) \setminus E(T_k)$. Adding e to T_k creates a cycle. If $e = xy$, then T_k has an xy -path, P_{xy} . Take the path and replace the edge xy with P_{xy} (contained in T_k to get a new vw -walk with fewer edges not in T_k).
By iterating a finite number of times, we get a vw -walk in G , all of whose edges are in T_k , therefore T_k is connected.

We must now prove that the algorithm outputs the *minimum weight* spanning tree: Let $T_{opt} = MWST$ (and suppose $w(T_k) > w(T_{opt})$)¹⁷.

$T_k = e_1, e_2, \dots, e_{n-1}$ in the order added. Let e_k be the first edge which is in T_k and T_{opt} . *Claim:* There is an edge in T_{opt} , say e , such that $T = (T_{opt} - e) + e_k$ is a spanning tree. (To be proved in an assignment.)

¹⁷ No need, we didn't end up using contradiction.

$$\begin{aligned} &\implies w(T) \geq w(T_{opt}) \\ \implies \cancel{w(T_{opt})} - w(e) + w(e_k) &\geq \cancel{w(T_{opt})} \\ \implies w(e_k) &\geq w(e) \end{aligned}$$

If $k = 1$, then $w(e_1)$ was edge with minimum weight: $w(e_1) = w(e)$.

If $k > 1$, by choice of k , $e_1, e_2, \dots, e_{k-1} \in E(T_{opt})$, so the tree

$\{e_1, e_2, \dots, e_{k-1}\} \cup \{e\} \subseteq E(T_{opt}) \Rightarrow$ forms no cycles.

Since the algorithm chose e_k over e , $w(e_k) \leq w(e) \Rightarrow w(e_k) = w(e) \Rightarrow w(T) = w(T_{opt})$. And T shares more edges with T_k than T_{opt} did. Call $T = T'_{opt}$. If $T_k = T'_{opt}$, done. If not, repeat argument to get T''_{opt} which has minimum weight and more edges in common with T_k than T'_{opt} did, and so on. Eventually we stop when we get to $T_k \Rightarrow w(T_{opt}) = w(T'_{opt}) = w(T''_{opt}) = \dots = w(T_k)$. \square

TRAVELING SALESPERSON PROBLEM: given n points (vertices) to visit and a weight to each pair, i.e. a weighted complete graph, find a minimum weight Hamiltonian cycle C_{opt} .

If the Triangle-Inequality is satisfied: $w(xy) + w(yz) \geq w(xz) \forall x, y, z$, then we can find a spanning closed walk W with $w(W) \leq 2w(C_{opt})$.

TSP ALGORITHM(G)

- 1 Take a MWST.
- 2 Make a walk by starting at a root and walking down, then up until you can walk down again, etc. Call the walk W .

Proof. As seen in Figure 30, $w(W) = 2w(T_{opt})$. Also notice that removing any edge from C_{opt} gives a spanning tree (Hamiltonian path).

$$\begin{aligned} w(W) &= 2w(T_{opt}) \\ &\leq 2w(C_{opt} - e) \\ &\leq 2w(C_{opt}) \end{aligned}$$

□

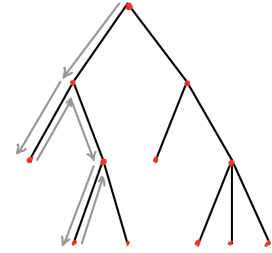


Figure 30: Example of the walk W in gray on the MWST.

Notes

- LPV stands for the textbook by L. Lovász, J. Pelikán and K. Vesztergombi: *Discrete Mathematics: Elementary and Beyond*.
- Thanks to Suleman Malik for Figures 27 to 30.