MATH 55 Notes

Jad Damaj

Fall 2021

Contents

1 8/26/2021

1.1 Propositional Logic

Definition 1.1. A proposition is a statement that is either true or false but not both

Statement	Proposition?	Truth Value
$2+2=4$	yes	T
Wow	no	-
$x+5=7$	no	-
Pigs can fly	yes	F

- To be true or false a proposition must be specified precisely
- will define logical operators to combine propositions

Three main operators:

Definition 1.2. The negation of p is the proposition "it is not the case that p" denoted $\neg p$ or "not p". It has the opposite truth value of p.
$\neg$(pigs can fly) same as "pigs can't fly"

Truth Table:

p	$\neg p$
T	F
F	T

Definition 1.3. The conjunction of two propositions p and q is "p and q" denoted $p \wedge q$, it is true when both p and q are T, and false otherwise.

Truth Table:

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition 1.4. The disjunction of two propositions p and q is "p and q" denoted $p \vee q$ it is F if both p and q are F, otherwise it is T.

Truth Table:

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

- distinct from "exclusive or" which is closer to English.

Definition 1.5. The exclusive or, $p \oplus q$ is T when exactly one of p and q is T and F otherwise

Definition 1.6. The condition $p \to q$ is the proposition "if p then q". "p implies q", "q when p", "p is sufficient for q"
$p \to q$ is true if the following "contract" holds: if p is T then q must be T (if p is F, q can be either T or F).

Truth Table:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	F

Example 1.7. "if $2 + 2 = 4$ then $1 + 1 = 2$" T
"if $2 + 2 = 4$ then pigs can fly" F
"if pigs can fly then unicorn exist" T
"if pigs can fly then $2 + 2 = 4$" T

Related Operations:

1. Biconditional: $p \leftrightarrow$ "p if and only if q". T when p and q have the same truth value. Equivalent to $(p \to q) \wedge (q \to p)$

2. Converse of $p \to q$ is $q \to p$
   ex: "If you get a 100, you get an A" T
   conv: "if you get an A, you get a 100." F
   $p \to q$ not the same as $q \to p$

3. Contrapositive of $p \to q$ is $\neg q \to \neg p$
   ex: "If you get a 100, you get an A" T
   cont: "If you didn't get an A, you didn't get a 100" T
   $p \to q$ and $\neg q \to \neg p$ are logically equivalent. i.e. they have the same truth table:

p	q	$\neg p$	$\neg q$	$p \to q$	$\neg q \to \neg p$
T	T	F	F	T	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Definition 1.8. A compound proposition consists of logical operators applied to propositions or propositional variables.

- It's truth value can be mechanically determined from the truth value of its constituents

1.2 Logical Equivalence

Definition 1.9. Two propositions are logically equivalent if they have the same truth values, regardless of the values of the propositional variables in them. ex: $p \to q \equiv \neg p \lor q$

Example 1.10 (Knights and Knaves)**.** Two types of people: Knights, who always tell the truth, and Knaves, who always lie.
Alice and Bob are two people. Alice says "Bob is a knight", Bob says "the two are opposites"
Q) Figure out who is what.
p: Alice is a knight, q: Bob is a knight.
Statements equivalent to: $p \leftrightarrow q \quad q \leftrightarrow (p \land \neg q) \lor (\neg p \land q)$
Case 1: p is T. T $\leftrightarrow q$ so q is T. T $\leftrightarrow (p \land \neg q) \lor (\neg p \land q)$ so $T \leftrightarrow F$ which is a contradiction.
This means p is F so q is F as well. Thus, both are knaves.

2 8/31/2021

2.1 Logical Equivalence

Compound propositions $C_1 \equiv C_2$ if both have the same truth values for all values of their propositional variables

- $C_1 \equiv C_2$ is the same as $C_1 \leftrightarrow C_2 \equiv$ T
- C is a tautology if $C \equiv$ T eg. $(p \to q) \leftrightarrow (\neg q \to \neg p)$

- C is a contradiction of $C \equiv \mathrm{F}$ eg. $p \wedge \neg p$
- C is contingent otherwise.
- Some useful tautologies:
  - $((p \to q) \wedge p) \to q$
  - $p \to p \vee q$
  - $p \wedge q \to p$
  - $\neg(p \wedge q) \equiv \neg p \vee \neg q$
  - $\neg(p \vee q) \equiv \neg p \wedge \neq q$
- Use lots of these simple tautologies to derive more interesting ones

2.2 Propositional Functions

Want to be able to say things like "every integer is even or odd"

Definition 2.1. A propositional function is a statement that contains one or more variables from a domain which becomes a proposition when each of the variables is instantiated.

Example 2.2. $P(x) =$"x is even", domain = integers, $P(2) =$"2 is even" - proposition
$Q(x, y) =$"x¡y", domain = integers

Definition 2.3. The universal quantification of $P(x)$ is the statement "for every x in the domain, $P(x)$." Denoted $\forall x P(x)$, (eg. $\forall x$(x is even) domain= integers - F)

Definition 2.4. The existential quantification of $P(x)$ is the statement "there exists an x in the domain such that $P(x)$." Denoted $\exists x P(x)$, (eg. $\exists x$(x is even) domain= integers - T)

Example 2.5. $\exists x(x^2 = 2)$, domain=integers - F $\exists x(x^2 = 2)$, domain=$\mathbb{R}$ - T

- Can also specify a domain using conjugation: $\exists x$(x is an integer $\wedge x^2 = 2$), $\forall x$(x is an integer$\to$ x is even).
- a variable appearing in a quantifier is called bound. A statement where all variables are bound is a proposition.

Negation of Quantifies:

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

Example 2.6. "every integer is prime" = $\forall x$(x is prime), domain - integers
neg: "there is an integer that is composite" = $\exists x \neg$(x is prime), domain - integers

Definition 2.7. Two statements are logically equivalent if they have the same truth values for all values of the propositional variables in all domains.

Example 2.8 (Nesting of Quantifiers)**.**

- $\forall x \forall y(x + y = y + x)$ - "for any integer x, it is the case that for any integer y, $x + y = y + x$".
  $\forall x \forall y Q(x, y) \equiv \forall y \forall x Q(x, y)$
- $\exists x \exists y(x^2 + y^2 = 0) \equiv \exists y \exists x(x^2 + y^2 = 0)$
- $\forall x \exists y(y = x^2)$. "For every integer x, there is an integer y such that $y = x^2$."
  $\exists y \forall x(y = x^2)$. "There exists y such that for every integer x, $y = x^2$."
- $\forall x \exists y(y$ is strictly taller than $x)$, domain=the class, F - tallest person
  $\exists y \forall x(y$ is strictly taller than $x)$, domain=the class, F - tallest person not strictly taller than self
- $\neg(\exists x \forall y Q(x, y)) \equiv \forall x \neg(\forall y Q(x, y)) \equiv \forall x \exists y Q(x, y)$
- $\forall x \exists y((x \neq 0) \to xy = 1)$ domain-real numbers
  neg: $\exists x \forall y \neg((x \neq 0) \to xy = 1) \equiv \exists x \forall y((x \neq 0) \wedge xy \neq 1)$

2.3 Rules of Inference

Example 2.9. If it is raining the dog is wet
it is raining
$\therefore$ The dog is wet
Argument of the form:
$r \to w$
w
$\therefore r$ - "modus ponens"
This is valid because $(r \to w) \wedge w) \to w$ is a tautology.

Example 2.10. Consider the argument: $r \to w$
$\neg w$
$\therefore \neg r$
Valid since $(r \to w) \wedge \neg w) \to \neg r$ is a tautology

- Rules of inference are useful tautologies used to derive true propositions from known true properties.

Definition 2.11. An argument is a sequence of statements, the last of which is a conclusion. An argument is valid if each statement follows fro the previous ones and rules of inference.

Example 2.12. Claim: $p \wedge q \to p \vee q$ is a tautology.
Argument:

1. $p \wedge q \to p$ tautology
2. $p \to p \vee q$ tautology

3. $p \wedge q \to p \vee q$ hypothetical syllogism (tautology)

Rules of Inference for quantifiers:

- $\forall x P(x) \to P(c)$ for arbitrary c in domain: Universal Generalization
  $P(c)$ for arbitrary c in domain $\to \forall x P(x)$: Universal Instantiation

- $\exists x P(x) \to P(c)$ for some c in domain: Existential Generalization
  $P(c)$ for some c in domain $\to \exists x P(x)$: Existential Instantiation

Example 2.13. $\forall x(x$ is mortal$)$ $\therefore$ Nikhil is mortal
Nikhil is mortal $\therefore$ $\exists x(x$ is mortal$)$

Example 2.14 (Lewis Carol)**.** Informal Argument:

All Lions are fierce	$\forall x(L(x) \to F(x))$
Some lions don't drink coffee	$\exists x(L(x) \wedge \neg C(x))$
Some fierce creatures don't drink coffee	$\exists x(F(x) \wedge \neg C(x))$

Formal Argument: $L(x) =$"x is a lion", $F(x) =$"x is fierce", $C(x) =$"x drinks coffee" - domain: all creatures

1. $\exists x(L(x) \wedge \neg C(x))$	Premise
2. $L(a) \wedge \neg C(a)$	EI
3. $L(a)$	
4. $\neg C(a)$	
5. $\forall x(L(x) \to P(a))$	Premise
6. $L(a) \to F(a)$	UI
7. $F(a)$	from 3, 5
8. $F(a) \wedge \neg C(a)$	
9. $\exists x(F(x) \wedge \neg C(x))$	EI

3 9/2/2021

3.1 Proofs

- An argument is valid if every statement follows from the previous ones and rules of inference.

- A proof is a valid argument used to establish the truth of a statement.

Definition 3.1. An integer is even if there exists an integer k such that $n = 2k$. Formally, $\forall n(even(n) \leftrightarrow \exists k(n = 2k))$.

Definition 3.2. An integer is odd if $n = 2k + 1$ for some integer k. Formally, $\forall n(odd(n) \leftrightarrow \exists k(n - 2k + 1))$

Proposition 3.3. If an integer n is odd then n^2 is odd. Formally $\forall n(odd(n) \to odd(n^2))$

Regular Proof	Formal Proof
Assume n is odd. Observe that there is k such that $n = 2k+1$. So $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$. Thus n^2 is odd, as desired.	Assume n is an arbitrary integer Assume odd(n). $\exists k(n = 2k+1)$ by def $n = 2k+1$ for some k by EI $n^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ $n^2 = 2l+1$ for $l = 2k^2+2k$ $\exists l(n^2 = 2l+1)$ odd(n^2) by def odd(n) $\rightarrow$ odd(n^2) $\forall n(odd(n) \rightarrow odd(n^2))$

- There are many phrases in English with the same meaning. End: therefore, in conclusion, thus, it follows that. Beginning: Let x be an integer, suppose x is an integer.

Proposition 3.4. For every integer n if n^2 is odd then n is odd. Formally $\forall n(odd(n^2) \rightarrow odd(n))$

Regular Proof	Formal Proof
We will show the contrapositive.	$\forall n(odd(n^2) \rightarrow odd(n)) \equiv$ $\forall n(\neg odd(n) \rightarrow \neg odd(n^2)) \equiv$ $\forall n(even(n) \rightarrow even(n^2))$
Assume n is even. Choose k such that $n = 2k$. Observe that $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. Thus, n^2 is even.	Assume n is an integer Assume even(n) $\exists k(n = 2k)$ $n = 2k$ for some k $n^2 = 4k^2 = 2(2k^2)$ $n^2 = 2l$ for $l = 2k^2$ $\exists l(n^2 = 2l)$ even(n^2) even(n) $\rightarrow$ even(n^2) $\forall n(even(n) \rightarrow even(n^2))$

A proof should have two features:

- Clarity: should be precise enough that it can turned into a formal proof.
- Correctness: should be a valid argument.

Definition 3.5. A number x is rational if $x = \frac{p}{q}$ for some integers $p, q \neq 0$. Formally, rational(x) $\leftrightarrow \exists p \exists q(x = \frac{p}{q} \wedge q \neq 0)$.
A number if irrational if it is not rational. Formally, irrational(x) $\leftrightarrow \forall p \forall q(x \neq \frac{p}{q})$

- If $x = \frac{p}{q}$, we assume p and q have no common factors.

Proposition 3.6. $\sqrt{2}$ is irrational

Proof. Assume for contradiction $\sqrt{2}$ is rational. Choose $p, q \neq 0$ such that $\sqrt{2} = \frac{p}{q}$. Observe that $2 = \frac{p^2}{q^2}$ so $p^2 = 2q^2$ so p^2 is even. This means for some k, $p = 2k$ so notice that $q^2 = \frac{p^2}{2} = \frac{4k^2}{2} = 2k^2$ so q is even. Thus contradicts our assumption that p and q have no common factors since both are even. Thus, $\sqrt{2}$ is irrational. □

Summary:

Proof	Goal	Structure
Direct Proof	$p \to q$	Assume $p, \ldots, q$. Conclude $p \to q$
Proof by Contrapositive	$p \to q$	Assume $\neg q, \ldots, \neg p$. Conclude $\neg p \to \neg q \equiv p \to q$.
Proof by Contradiction	$p \to q$	Assume $p, \neg q, \ldots, q$ so $p \wedge \not{q} \to \mathrm{F} \equiv p \to q$

- A proof is a finite piece of reasoning which can establish the truth of infinitely many statements.
- A proof can convince any other person of the truth of a statement.

4 9/7/2021

4.1 Sets

Definition 4.1. A set is an unordered collection of objects, which are called elements. A set is said to contain its elements, denoted $x \in A$="x is an element of A", $x \notin A$="x is not an element of A"

Example 4.2. $A = \{1, 2, 3\}$ $\quad 1 \in a \quad 4 \notin a$
$\mathbb{Z}$ = set of all integers $\quad \mathbb{Z}_+$ = set of all positive integers $\quad \mathbb{R}$ = set of all real numbers

Two ways to specify a set:

1. Roster Notation: list out elements (eg. {granola, sushi, candy})
2. Set builder Notation: given a propositional function $P(x)$, $A = \{x : P(x)\}$ is the set of all x such that $P(x)$.
(eg. $E = \{x \in \mathbb{Z} : x \text{ is even}\}$, $O = \{x \in \mathbb{Z} : x \text{ is odd}\}$, $P = \{x \in \mathbb{Z} : x \text{ is prime}\}$)

Remark 4.3. We have not defined an "object". This called naive set theory.
Russel's Paradox: Consider the set of sets $A = \{x : x \notin x\}$
Case 1: Assume $A \in A$, by definition of A, $A \notin A$. Contradiction.
Case 2: Assume $A \notin A$, by definition of A, this impleis $A \in A$. Contradiction.

Definition 4.4. A is equal to B if it has the same elements, formally $A = B \leftrightarrow \forall x(x \in A \leftrightarrow x \in B)$
(eg. $\{x \in \mathbb{Z}_+ : x \text{ is odd }\} = \{x \in \mathbb{Z}_+ : x \text{ is not even}\}$)

Definition 4.5. A set A is a subset of B if every element of A is an element of B, formally: $A \subseteq B \leftrightarrow \forall x(x \in A \rightarrow x \in B)$.
(eg. $\mathbb{Z}_+ \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{R}$, $\mathbb{R} \nsubseteq \mathbb{Z}$)

- If A is a set $A \subseteq A$
- $A = B \leftrightarrow A \subseteq B$ and $B \subseteq A$

Definition 4.6. The set with no elements is called the empty set, denoted $\emptyset = \{\}$

- For any set A, $\emptyset \subseteq A$

Definition 4.7. If A is a set, the power set of A is the set of all subsets of A, denoted $\mathcal{P}(A) = \{S : S \subseteq A\}$.
(eg. $\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$)

- If a set A has n elements, $\mathcal{P}(A)$ has 2^n elements.

Definition 4.8. If A has n elements for some nonnegative integer n, its has cardinality n and is finite, denoted $|A| = n$.

Proposition 4.9. If $A = B$ then $\mathcal{P}(A) = \mathcal{P}(B)$.

Proof. Assume $A = B$, we will show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ and $\mathcal{P}(B) \subseteq \mathcal{P}(A)$. Assume $S \in \mathcal{P}(A)$. By definition $S \subseteq A$, so since $A = B$ $S \subseteq B$ so $S \in \mathcal{P}(B)$. Proof of the other inclusion is the same with the roles of A and B reversed. □

Proposition 4.10. For sets A and B, if $\mathcal{P}(A) = \mathcal{P}(B)$ then $A = B$.

Proof. Assume $\mathcal{P}(A) = \mathcal{P}(B)$. We will show $A \subseteq B$ and $B \subseteq A$.
($\subseteq$) Assume $x \in A$. Observe that $\{x\} \in \mathcal{P}(A)$ so $\{x\}\mathcal{P}(B)$. By definition $\{x\} \subseteq B$ so $x \in B$
($\supseteq$) Proof is the same with the roles of A and B reversed. □

3 operations on sets (corresponding to $\wedge, \vee, \neg$)

1. Intersection: $A \cap B = \{x : x \in A \wedge x \in B\}$
2. Union: $A \cup B = \{x : x \in A \vee x \in B\}$
3. Complement (with respect to universe U): $\overline{A} = \{x \in U : x \notin A\}$
4. Set Difference: $A - B = \{x \in A : x \notin B\}$

Set Identities: Relations between sets which always hold

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $A - B = A \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$

Definition 4.11. The Cartesian product of A and B is the set of ordered pairs (a, b) such that $a \in A$ and $b \in B$ denoted $A \times B = \{(a, b) : a \in A \wedge b \in B\}$.

Example 4.12. $\mathbb{Z} \times \mathbb{Z}$ $\quad \mathbb{R} \times \mathbb{R} = \mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}$
$\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R} = \{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in \mathbb{R}\}$

4.2 Functions

Definition 4.13. If A and B are non empty sets, a function f from A to B is a rule that assigns exactly one element of B to every element of A. This assignment is denoted $f(a) = b$ for $a \in A, b \in B$. f is written as $f : A \to B$.

Example 4.14. $f : \mathbb{Z} \to \mathbb{Z}$ by $f(x) = x^2$
$g : \mathbb{R} \to \mathbb{R}_{\geq 0}$ by $g(x) = x^2$
$h : \mathbb{R} \to \mathbb{R}$ by $h(x) = e^x$
$p : A \to \mathcal{P}(A)$ by $p(a) = \{a\}$

Definition 4.15. $f : A \to B$ is onto/surjective if $\forall b \in B(\exists a \in A$ such that $f(a) = b\}$

Definition 4.16. If $S \subseteq A$ the image of S on f denoted $f[S] = \{b \in B : \exists a \in S$ such that $f(a) = b\} = \{f(s) : s \in S\}$. $f[A]$ is called the range of f.

5 9/9/2021

5.1 Functions

Definition 5.1. A function $f : A \to B$ is one-to-one/injective if $\forall a_1, a_2 \in A(f(a_1) = f(a_2) \to a_1 = a_2) \equiv \forall a_1, a_2 \in A(a_1 \neq a_2 \to f(a_1) \neq f(a_2))$

Definition 5.2. If $f : A \to B$ is a function and $S \subseteq B$ then $f^{-1}[S] = \{a \in A : f(a) \in S\}$.Observe that a function is onto if $\forall b \in B|f^{-1}[\{b\}]| \geq 1$ and it is one to one if $\forall b \in B|f^{-1}[\{b\}]| \leq 1$.

Example 5.3.

Function	One to One	Onto
$f : \mathbb{Z} \to \mathbb{Z} \quad f(x) = x^2$	No	No
$g : \mathbb{R} \to \mathbb{R}_{\geq 0} \quad g(x) = x^2$	No	Yes
$h : \mathbb{R} \to \mathbb{R}_{\geq 0} \quad h(x) = e^x$	Yes	Yes
$p : A \to \mathcal{P}(A) \quad p(a) = \{a\}$	Yes	No
$m : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \quad m(a, b) = b$	No	Yes

Definition 5.4. If $f : B \to C$ and $g : A \to C$ are functions, the function $f\dot{g} : A \to C$ denoted by $f\dot{g}(a) = f(g(a))$ is the composition of f and g. Note $f\dot{g} \neq g\dot{f}$ in general.

Definition 5.5. If $f : A \to B$ is one to one and onto it is called a bijection/one to one correspondence. If f is a bijection, for any $b \in B$ there is exactly one $a \in A$ such that $f(a) = b$.
$f^{-1}\dot{f}(a) = f^{-1}f(a)) = a \ \forall a \in A \quad f\dot{f}^{-1}(b) = f(f^{-1}(b)) = b \ \forall b \in B$

Example 5.6. $f : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ by $f(x) = \tan(x)$ is a bijection with $f^{-1}(x) = \arctan(x)$.

Proposition 5.7. For finite sets A and B, $|A| = |B|$ if and only if there is a bijection $f : A \to B$.

Proof. Assume $\rightarrow$) $|A| = |B|$. Let $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_n\}$. Observe that $f(a_n) = b_n$ is a bijection.
$\leftarrow$) Assume $|A| \neq |B|$. WLOG let $|A| < |B|$ so $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$ with $m < n$. Let $f : A \to B$ be an arbitrary function. We will show f is not onto. Since for each element in A there is exactly one element in B such that $f(a) = b$ so there can be at most n elements in B mapped to by f. Since $m > n$ there must be some $b \in B$ such that $b \notin f[A]$. □

5.2 Cardinality of Infinite Sets

Definition 5.8. The sets A and B have the same cardinality, denoted $|A| = |B|$ if there is a bijection $f : A \to B$.

Definition 5.9. An infinite sequence is a bijection from $\mathbb{Z}_+$ to a set A. It is said to "enumerate" the set. A set is countable if it is finite or $|\mathbb{Z}_+| = |A|$.

Example 5.10. Consider $\mathbb{Z}_+ \subseteq \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.
Claim: $\mathbb{Z}$ is countable.
Proof 1: Consider the sequence $0, 1, -1, 2, -2, \dots$ observe that each $n \in \mathbb{Z}$ appears once in the sequence. Thus $\mathbb{Z}$ is countable.

Proof 2: Consider the function $f : \mathbb{Z}_+ \to \mathbb{Z}$ by $f(n) = \begin{cases} \frac{n}{2} & \text{if even} \\ -\frac{n-1}{2} & \text{if odd} \end{cases}$.

Injective: Assume $n_1, n_2 \in \mathbb{Z}_+$ and $f(n_1) = f(n_2)$. Observe that they have the same sign so n_1 and n_2 are both odd or both even.
Case 1: n_1 and n_2 even. $\frac{n_1}{2} = \frac{n_2}{2}$ so $n_1 = n_2$.
Case2: n_1 and n_2 odd. $-\frac{n_1-1}{2} = -\frac{n_2-1}{2}$ so $n_1 - 1 = n_2 - 1$ so $n_1 = n_2$.
Onto: Assume $m \in \mathbb{Z}$ is an arbitrary integer. If $m > 0$, $f(2m) = m$, if $m \leq 0$, $f(-2m + 1) = m$.

Example 5.11. Consider $\mathbb{Z} \times \mathbb{Z} = \{(a, b) : a, b \in \mathbb{Z}\}$.
Claim: $\mathbb{Z} \times \mathbb{Z}$ is countable.

Proof: Consider the infinite array: $\begin{matrix} (1,1) & (1,2) & (1,3) & \cdots \\ (2,1) & (2,2) & (2,3) & \cdots \\ (3,1) & (3,2) & (3,3) & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{matrix}$

Consider the enumeration given by tracing out the diagonals. Let $D_i = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a + b = i\}$. Observe that in the list $D_1, D_2, D_3, \dots$ each (a, b) appears exactly once in D_s where $s = a + b$. So it is an enumeration.

Remark 5.12. It follows that if A and B are countable then so is $A \times B$

Example 5.13 (Cantor's Diagonal Argument)**.** Consider $(0, 1)$ where $x \in (0, 1)$ has digits $x = 0.x_1x_2x_2 \cdots$.
Claim: $(0, 1)$ is uncountable.
Proof: Assume $f : \mathbb{Z}_+ \to (0, 1)$ is a function. We will show f is not a bijection. Consider the set of decimal expansions:
$f(1) = 0.d_{11}d_{12}d_{13} \cdots$

$f(2) = 0.d_{21}d_{22}d_{23}\cdots$
$f(3) = 0.d_{31}d_{32}d_{33}\cdots$

Consider the following x defined by $x_i = \begin{cases} 4 & \text{if } d_{ii} = 5 \\ 5 & \text{if } d_{ii} \neq 5 \end{cases}$. Observe that by construction $f(n) \neq x$ for all n since they differ on the nth digit. Thus f is not onto.

6 9/11/2021

6.1 Division and Divisibility

Definition 6.1. If $a \neq 0$ and b are integers the then a divides b, denoted $a|b$ if there exists $k \in \mathbb{Z}$ such that $b = ka$. (ie. $\frac{b}{a}$ is an integer). eg. $3|9, 3 \not| 10, 3|0$

Theorem 6.2 (Basic Properties)**.**
1. If $a|b$ and $a|c$ then $a|b+c$ and $a|bc$
2. If $a|b$ and $b|c$ then $a|c$

Proof. Suppose $a, b \in \mathbb{Z}$ and $a|b, a|c$. Choose $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 a$ and $b = k_2 a$. Notice that $b + c = k_1 a + k_2 a = (k_1 + k_2)a$ so $a|b+c$ □

Theorem 6.3 ("Division Algorithm")**.** If $a \in \mathbb{Z}$ and $d \in \mathbb{Z}_+$ then there exists unique integers q and r satisfying $0 = dq + r$ and $0 \leq r < d$.

Proof. Existence: Given a choose minimal d such that $a - d_0 q \geq 0$. The existence of such a d guaranteed by well ordering property. Observe that $a = d_0 q + r$ with $0 \leq r < d$. If $r > d$ then $r - d > 0$ so there exists $r' > 0$ such that $r = r' + d$ so $a = d_0 q + r = d_0 q + r' + d$ so $a - (d_0 - 1)q \geq 0$ which contradicts the minimality of d_0. Thus, $0 \leq r < d$.
Uniqueness: Suppose $a = q_1 d + r_1 = q_2 d + r_2$ for some integers $a_1, a_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < d$. Assume WLOG $r_1 \geq r_2$. So $r_1 - r_2 = (a - q_1 d) - (a - q_2 d) = (q_2 - q_1)d$. Thus, $d|r_1 - r_2$. Since $d > r_1 > r_2$, $r_1 - r_2 = 0$ so $r_1 = r_2$. $q_1 = q_2$ follows. □

Notation: $a \text{div} d = q \quad a \text{mod} d = r$

6.2 Modular Arithmetic

Example 6.4. If you sleep at 11 pm for 8 hours, you wake up at 19pm. 19 mod 12 = 7 am.

Example 6.5. Number the days of the week $0 - 6$ starting on Sunday. Today is Tuesday(2), what day is it in 39 days?
$2 + 39 = 41 \text{mod} 7 = 6 \rightarrow$ Saturday

Definition 6.6. For integers a, b, a is congruent to b modulo m, denoted $a \equiv b (\text{mod} m)$ if $a \text{mod} m = b \text{mod} m$.

Proposition 6.7. $a \equiv b(\text{mod}m)$ if and only if $m|a-b$.

Proof. Suppose $\rightarrow$) $a \equiv b(\text{mod}m)$. $a = mq_1 + r$ and $b = mq_2 + r$ so $a - b = mq_1 + r - (mq_2 + r) = m(q_1 - q_2)$ so $m|a-b$.
$\leftarrow$) Suppose $m|a-b$. Let $a = mq_1 + r_1$ and $b = mq_2 + r_2$ by the division algorithm. We will show $r_1 = r_2$. Observe that $a - b = m(q_1 - q_2) + (r_1 - r_2)$ so $m|r_1 - r_2$. Since $m > r_1 \geq r_2$, $m > r_1 - r_2$ and so $r_1 - r_2 = 0$. □

Theorem 6.8 (Key Properties)**.** 1. If $a \equiv b(\text{mod}m)$ then $a\text{mod}m \equiv b\text{mod}m(\text{mod}m)$

2. If $a \equiv b(\text{mod}m)$ and $c \equiv d(\text{mod}m)$ then $a + c \equiv b + d(\text{mod}m)$ and $ac \equiv bd(\text{mod}m)$.

Proof. Assume $a \equiv b(\text{mod}m)$ and $c \equiv d(\text{mod}m)$. By proposition, $m|a-b$ so $(a-b) = km$ for some $k \in \mathbb{Z}$. This means $c(a+b) = ckm$ so $m|ca - cb$ so $ca \equiv cb(\text{mod}m)$. By the same argument, $cb \equiv db(\text{mod}m)$. Thus $ca \equiv cb \equiv db(\text{mod}m)$, as desired.

□

- can perform modulo m before doing arithmetic and it doesn't change the answer.

- can do algebra (addition, multiplication, substitution of equations) as usual.

Example 6.9. $36^2 \equiv 36 * 36 \equiv 36 * 1 \equiv 1 * 1 \equiv 1(\text{mod}7)$ since $36\text{mod}7 = 1$.

6.3 Representation of Numbers

In decimal, the number $d_k d_{k-1} \cdots d_0$ with $d_i \in \{0, \ldots, a\}$ is equal to $a_0 + a_1 * 10 + \cdots + a_k * 10^k$

Proposition 6.10. Let $n \in \mathbb{Z}_+$ has digits $d_k d_{k-1} \cdots d_0$. Then $9|n$ if and only if $9|d_0 + d_1 + \cdots + d_k$.

Proof. Suppose $n = d_0 + d_1(10) + \cdots d_k(10)^k = \sum_{i=0}^{k} d_i 10^i$. Note $10 \equiv 1(\text{mod}9)$ so $10^i \equiv 1(\text{mod}9)$. Then $n \equiv \sum_{i=0}^{k} d_i 10^i \equiv \sum_{i=0}^{k} d_i(\text{mod}9)$. Thus $9|n$ if and only if $9|\sum_{i=0}^{k} d_i$ □

- In base b we write numbers as the sum of powers of b.

- $b = 2$ is called binary. eg $(101101)_2 = 1 * 2^0 + 0 * 2^2 + 1 * 2^2 + 1 * 2^2 + 1 * 2^3 + 0 * 2^4 + 1 * 2^5 = 45$

- How to convert to binary: divide by 2.
  $45 = 2*22+1, 22 = 2*11+0, 11 = 2*5+1, 5 = 2*2+1, 2 = 2*1+0, 1 = 2*0+1$ so $45 = (101101)_2$

7 9/16/2021

7.1 Representation of Numbers

Example 7.1. What is 5^{45}(mod 7)?
Step 1: $45 = 2^0 + 2^1 + 2^3 + 2^5$
Step 2: Express $5^{45} \equiv 5^{2^0+2^1+2^3+2^5} \equiv 5^{2^0}5^{2^1}5^{2^3}5^{2^5}$(mod7).
Step 3: Compute $5^{2^0}, 5^{2^1}, 5^{2^3}, 5^{2^5}$ by repeated squaring. $5 \equiv 5$(mod7), $5^2 \equiv 25 \equiv 4$(mod7), $5^{2^2} \equiv (5^2)^2 \equiv 4^2 \equiv 16 \equiv 2$(mod7), $(5^{2^3}) \equiv (5^{2^2})^2 \equiv 2^2 \equiv 4$(mod7), $5^{2^4} \equiv 4^2 \equiv 2$(mod7), $5^{2^5} \equiv 2^2 \equiv 4$(mod7).
Step 4: Plug in values from step 3. $5^{45} = 5 * 2 * 4 * 4 \equiv 6$(mod7).

Remark 7.2. Fast exponentiation is a key operation in cryptography.

7.2 Prime Numbers

Definition 7.3. An integer $p > 1$ is prime if it has no divisors other than 1 and itself. (Formally, p is prime $\leftrightarrow \forall k \in \mathbb{Z}_+(k|p \rightarrow k = 1 \vee k = p)$. An integer $c > 1$ is composite if it is not prime. i.e $c = ab$ for some integers $a, b \neq 1$.

Theorem 7.4 (Fundamental Theorem of Arithmetic)**.** Every integer $n > 1$ can be written uniquely as a product of primes $p_1, \dots, p_k$ listed in nondecreasing order.

Lemma 7.5. If $c > 1$ is composite, there is a prime p such that $p|c$.

Proof. Assume $c > 1$ is composite. Let $S = \{d \in \mathbb{Z}_+|d|c \text{ and} d > 1$. Notice $S \neq \emptyset$ since $c \in S$, also $S \subseteq \{2, \dots, c\}$. Let q be the smallest element of S. Observe that q is prime. If not, then we can choose a number $a \neq 1$, such that $a|q$. Since $q|c$, we have $a|c$ but $a < q$ which is a contradiction. □

Proof of Existence of FTA. If n is composite, Lemma 1 implies $n = p_1 n_1$ for some p_1 prime and $n_1 < n$. If n_1 is prime, we are done, otherwise let $n_1 = p_2 n_2$ for some p_2 prime and $n_2 < n_1$. If we repeat this process k times we obtain $n = p_1 p_2 \cdots p_k n_k$. Since $n_k < n_{k-1} < \cdots < n_1$, this process must terminate in T steps for some $T < n$. For that T, we have have $n = p_1 p_2 \cdots p_T n_T$ and n_T is prime, as desired. □

Theorem 7.6. (Euclid) There are infinitely many prime numbers.

Proof. Assume for contradiction there are finitely many primes $p_1, \dots, p_n$. Consider $q = p_1 p_2 \cdots p_n + 1$. Notice q is not prime since $q > p_j$ for $j = 1, \dots, n$. Thus q is composite so by Lemma 1 there is some p_j such that $p_j|q$. Notice $p_j|p_1 \cdots p_n$ so $p_j|q - 1$ so $p_j|1$ which is a contradiction. □

7.3 GCD

Definition 7.7. If a and b are integers, not both zero, then $\gcd(a, b)$ is the largest positive integer such that $d|a$ and $d|b$. eg. $\gcd(10, 36) = 2$

Euclidean Algorithm: much faster way to find $\gcd(a, b)$.

Lemma 7.8. If $a > b > 1$ and $a = bq + r$ with $0 \leq r < b$ then for every $d \in \mathbb{Z}_+, d|a$ and $d|b \leftrightarrow d|b$ and $d|r$. Or in other words, $\gcd(a, b) = \gcd(b, r)$.

Proof. $\rightarrow$) Assume $d|a$ and $d|b$. Then $d|a - bq = r$.
$\leftarrow$) Assume $d|b$ and $d|r$. Then $d|bq + r = a$ □

Example 7.9. Calculate $\gcd(252, 198)$.
Iteratively apply lemma 2 till $r = 0$. $252 = 1 * 198 + 54$ so $\gcd(252, 198) = \gcd(198, 54)$
$190 = 3 * 54 + 36$ so $\gcd(198, 54) = \gcd(54, 36)$
$54 = 1 * 36 + 18$ so $\gcd(54, 36)$=$\gcd(36, 18)$
$36 = 2 * 18 + 0$ so $\gcd(36, 18)$=$\gcd(18, 0) = 18$
Thus $\gcd(252, 198) = 18$
Observe that $18 = 54 - 1 * 36 = 54 - 1 * (198 - 3 * 54) = -1 * (198) + 4 * 54 = (-1) * 198 + 4 * (252 - 1 * 198) = -5 * 198 + 4 * 252$ so $18 = -5 * 198 + 4 * 252$

Remark 7.10. Using equations obtained in the Euclidean Algorithm, we can write $\gcd(a, b) = sa + tb$ for integers s, t

Theorem 7.11 (Bezout's Theorem)**.** IF a, b are integers, not both zero, there are $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = as + bt$.

Proof. Follows from Euclidean Algorithm □

Definition 7.12. Two integers a, b are relatively prime if $\gcd(a, b) = 1$.

Lemma 7.13. Euclid's Lemma If $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Proof. By Bezout's Theorem there are $s, t \in \mathbb{Z}$ such that $as + bt = 1$. Observe that $c = c * 1 = c(as + bt) = cas + cbt$. Since $a|a$ and $a|cbt$, $a|c$. □

8 9/21/2021

8.1 The Fundamental Theorem of Arithmetic

Well Ordering Property: If S is a nonempty subset of $\mathbb{Z}_+$, then S has a least element.

Proof of Existence of FTA. Let $S = \{n \in \mathbb{Z}_+ : n > 1, n$ can't be written as a product of prime numbers$\}$. Assume for contradiction $S \neq \emptyset$. By WOP, S has a least element q. If q is prime we are done, so assume q is not prime. By Lemma, there is a prime $p < q$ such that $p|q$ for some $k > 1$. Observe that $k \notin S$ since $k < q$ so $k = p_1 \cdots p_n$ for primes $p_1, \ldots, p_n$ so $q = p_1 \ldots, p_n p$ which is a contradiction since q was assumed to be in S. Thus S must be empty. □

Corollary 8.1 (Corollary of Euclid's Lemma)**.** If p is prime and $p|a_1 \cdots a_j$ then $p|a_j$ for some j.

Proof. Let $S = \{k \in \mathbb{Z}_+ : \exists p, \exists a_1, \dots, a_n$ such that $p|a_1 \cdots a_k$ and $p \not| a_j$ for $j \in \{1, \dots, k\}\}$. Assume for contradiction $S \neq \emptyset$. By WOP, S has a least element $k \in S$. Choose p prime, $a_1, \dots, a_k$ such that $p|a_1 \cdots a_k$ and $p \not| a_j$ for $j \in \{1, \dots, k\}$. Since $p \not| a_1$, $\gcd(a_1, p) = 1$ so by Euclid's Lemma, $p|a_2 \cdots, a_k$ and $p \not| a_2, \dots, p \not| a_k$ which implies $k - 1 \in S$. This contradicts the minimality of k so S must be empty. □

Proof of Uniqueness of FTA. Assume there is $n \geq 1$ such that $n = p_1 \cdots p_k = q_1 \cdots = q_l$ where $p_1, \dots, p_k, q_1, \dots, q_l$ are primes. Assume WLOG $p_i \neq q_j$ for all i, j (otherwise we could divide both sides by it). Notice that $p_1 | q_1 \cdots q_l$ and p_1 is prime so by the corollary $p_1 | q_j$ for some $j \in \{1, \dots, l\}$ since q_j is prime $p_1 = q_j$ which is a contradiction. □

8.2 Division Modulo m

Definition 8.2. If $a \not\equiv 0 (\text{mod } m)$ then $\overline{a} \in \mathbb{Z}$ is an inverse of a (mod m) if $a\overline{a} \equiv 1 (\text{mod } m)$.

Example 8.3. What is the inverse of $a = 5(\text{mod}7)$?
$\overline{a} = 3$ since $3 * 5 = 15 \equiv 1(\text{mod}7)$

Theorem 8.4. If $\gcd(a, m) = 1$, then a has a unique inverse $a^{-1} \in \{0, \dots, m - 1\}$

Proof. Existence: Assume $\gcd(a, m) = 1$. By Bezout's Theorem, there are $s, t \in \mathbb{Z}$ such that $as + mt = 1$. Thus $1 \equiv as + mt \equiv as + 0 \equiv a(s\text{mod}m)(\text{mod}m)$. Thus $s\text{mod}m \in \{0, \dots, m - 1\}$ is an inverse of $a(\text{mod}m)$.
Uniqueness: Suppose $sa \equiv 1(\text{mod}m)$ and $s'a \equiv 1(\text{mod}m)$. $s \equiv s(s'a) \equiv s'(sa) \equiv s'(\text{mod}m)$. □

Remark 8.5. If $\gcd(a, m) \neq 1$ then a does not have an inverse mod m.

Example 8.6. What is the inverse of $a = 5(\text{mod}7)$?
Step 1: Euclidean Algorithm: $7 = 1 * 5 + 2 \to 5 = 2 * 2 + 1 \to 2 = 2 * 1 + 0$ so $\gcd(5, 7)$ =1. $1 = 5 - 2(2) = 5 - 2(7 - 5) = 3(5) - 2(7)$ so $5^{-1} \equiv 3(\text{mod}7)$.
Step 2: Calculate $s(\text{mod}7)$: $s = 3$.

Remark 8.7. Can be used to solve the linear congruence $ax \equiv b(\text{mod}m)$ where $\gcd(a, m) = 1$. $x \equiv a^{-1}ax \equiv a^{-1}b(\text{mod}m)$.

8.3 Inverses Modulo a Prime

Theorem 8.8 (Fermat's Little Theorem)**.** If p is a prime and $a \not\equiv 0(\text{mod}p)$, then $a^{p-1} \equiv 1(\text{mod}p)$.

Proof. Assume p is prime and $p \not| a$. Consider the terms $a * 1, a * 2, \dots, a * (p-1) \in \mathbb{Z}$. Consider the remainders modulo p: $r_1 = a * 1(\text{mod} p), r_2 = a_2(\text{mod} p), \dots, r_{p-1} = a * (p-1)(\text{mod} p) \in \{0, \dots, p-1\}$.
Claim 1: $r_k \neq 0$ for every $k \in \{1, \dots, p-1\}$.
Proof: If $a * k \equiv 0(\text{mod} p)$, then $p|ak$. Since $\gcd(p, a) = 1$, $p|k$ which is a contradiction since $0 < k < p$.
Claim 2: $r_{k_1} \neq r_{k_2}$ when $k_1 \neq k_2$.
Proof: Assume WLOG $k_1 > k_2$. If $r_{k_1} = r_{k_2}$ then $ak_1 \equiv ak_2(\text{mod} p)$ so $p|ak_1 - ak_2$ so $p|a(k_1 - k_2)$ so $p|k_1 - k_2$ which is a contradiction since $0 < k_1 - k_2 < p$.
We will calculate the product $r_1 r_2 \cdots r_{p-1}$ in two different ways. $r_1 r_2 \cdots r_{p-1} = (p-1)!$ so all remainders are distinct so $r_1 r_2 \cdots r_{p-1} \equiv (p-1)!(\text{mod} p)$. Also, $r_1 r_2 \cdots r_{p-1} \equiv (a*1)(a*2) \cdots (a*(p-1)) \equiv a^{p-1}(p-1)!(\text{mod} p)$. Thus $a^{p-1}(p-1)! \equiv (p-1)!(\text{mod} p)$. Observe that $p \not| (p-1)!$ so $(p-1)!$ has an inverse modulo p. Multiplying on both sides by this inverse yields $a^{p-1} \equiv 1(\text{mod} p)$. □

9 9/23/2021

9.1 Chinese Remainder Theorem

Example 9.1. Solve the system of linear congruences:
$x \equiv 1(\text{mod } 3) \quad x \equiv 0(\text{mod } 5) \quad x \equiv 0(\text{mod } 7)$
Idea: $5 * 7 = 35$ solved last two equivalences. Observe $35 \equiv 2(\text{mod } 3)$ so multiplying by $2^{-1} \equiv 2(\text{mod} 3)$ yields $x = 70 \equiv 2^{-1} * 2 \equiv 1(\text{mod } 3)$ so 70 satisfies all three congruences.

Theorem 9.2 (Chinese Remainder Theorem)**.** If $m_1, \dots, m_k$ are pairwise relatively prime, the system of congruences $x \equiv a_1(\text{mod} m_1)$, $x \equiv a_2(\text{mod} m_2)$, $\dots$, $x \equiv a_k(\text{mod} m_k)$ has a unique solution in $\{0, \dots, M-1\}$ where $M = m_1 m_2 \cdots m_k$

Proof. Let $x = y_1 M_1 a_1 + y_2 M_2 a_2 + \cdots y_k M_k a_k$ where $M_i = M/m_i$ and $y_i \equiv M_i^{-1}(\text{mod} m_i)$. Observe that $x \equiv y_1 M_1 a_1 + y_2 M_2 a_2 + \cdots y_k M_k a_k \equiv y_i M_i a_i \equiv a_i(\text{mod} m_i)$ since $m_i | M_j$ for $i \neq j$, as desired. □

9.2 Cryptography

Public Key Encryption (RSA)

Goal: Send a message $M \in \{0, \dots, n-1\}$

Steps	Running Example
1. Key Generation: choose two large primes p, q and let $n = pq$. Choose $e \in \{0, \dots, n-1\}$ such that $\gcd(e, \phi) = 1$ where $\phi = (p-1)(q-1)$. “public key”=(n, e), “private key”=(n, p, q)	$p = 7$, $q = 11$, $n = 77$, $\phi = 6 * 10 = 60$, $e = 7$
2. Encryption: Message $M \in \{0, \dots, n-1\}$. “Cipher Text” - $C = M^e(\text{mod} n)$	m=2, $c \equiv 2^7 \equiv 51(\text{mod}77)$ so $c = 51$
3. Decryption: let d be $e^{-1}(\text{mod}\phi)$. Compute $\hat{M} \equiv C^d \text{mod} n$.	Use Bezout coefficients to get $d = 43$. $\hat{M} = 51^{43} \equiv 2(\text{mod}77)$

Theorem 9.3. For every integer M, $\hat{M} \equiv M$ in the above scheme.

Theorem 9.4. An algorithm which can recover M from C using only the public key can be used to factor integers efficiently (the only way to recover M from C is to know p, q).

Proof. Proof of Theorem 1 Observe that $\hat{M} \equiv C^d \equiv (M^e)^d \equiv M^{ed}$ and $ed \equiv 1(\text{mod}\phi)$ so $ed = k\phi + 1$ for some $k \in \mathbb{Z}$. So $\hat{M} \equiv M^{k(p-1)(q-1)+1}(\text{mod} n)$.
Claim: $M^{k(p-1)(q-1)+1} \equiv 1(\text{mod} pq)$.
Proof: Case 1: Assume $M \not\equiv 0(\text{mod} p)$ and $M \not\equiv 0(\text{mod} q)$. By FLT, $M^{p-1} \equiv 1(\text{mod} p)$ and $M^{q-1} \equiv 1(\text{mod} q)$. Thus $\hat{M} \equiv (M^{p-1})^{k(q-1)} M \equiv 1^{k(q-1)} M \equiv M(\text{mod} p)$. Similarly, $\hat{M} \equiv M(\text{mod} q)$.
Consider the system of congruences given by $x \equiv M(\text{mod} p)$ and $x \equiv M(\text{mod} q)$. $\hat{M}(\text{mod} pq)$ is a solution to the system. $M(\text{mod} pq)$ is also a solution to the system so by uniqueness of the Chinese remainder theorem $\hat{M} \equiv M(\text{mod} pq)$, as desired.
Case 2: $\hat{M} \equiv 0(\text{mod} p)$ or $\hat{M} \equiv 0(\text{mod} q)$. Follows similarly. □

10 9/30/2021

10.1 Induction

New inference rule for proving $\forall n \in \mathbb{Z}_+ P(n)$ where $P(n)$ is some propositional function.

- Rule: $P(1) \wedge \forall k \in \mathbb{Z}_+ P(n) \therefore \forall n \in \mathbb{Z}_+ (P(n))$
- Proof of “$\forall n \in \mathbb{Z}_+ P(n)$ ” by induction:
  We will proceed by induction.
  Basis Step: Prove $P(1)$
  Inductive Step: Assume $k \in \mathbb{Z}_+$ is arbitrary and assume $P(k)$. Show $P(k+1)$. Conclude $\forall n \in \mathbb{Z}_+ P(n)$.

Example 10.1. Let $P(n) = \sum_{i=0}^{k} 2^i = 2^{k+1} - 1$. Show for any $n \in \mathbb{Z}_+$ $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Basis Step: We will show $P(1)$. $2^0 + 2^1 = 3 = 2^2 - 1$
Inductive Step: Assume $k \in \mathbb{Z}_+$ is arbitrary. Assume $\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$. Observe that $\sum_{i=0}^{k+1} 2^i = \sum_{i=0}^{k} 2^i + 2^{k+1} + 2^{k+1} - 1 + s^{k+1} = 2^{k+2} - 1$. This concludes the inductive step.

Remark 10.2. Validty of induction follows from well ordering principle. Consider $S = \{n \in \mathbb{Z}_+ : P(n) \text{ is false } \}$.

Remark 10.3. Can't prove $\forall x \in \mathbb{R}_+(P(n))$ by induction since there is no “next” real number. There is no well ordering principle for $\mathbb{R}_+$

Example 10.4. Let S_n = sum for the first n odd positive integers. $S_n = \sum_{i=1}^{n} 2(i-1) + 1$

Attempt 1	Attempt 2
Claim: S_n is a perfect square	Claim: $S_n = n^2$
Proof: Let $P(n)$=“S_n is a perfect square”	Proof: Let $P(n)$=“$S_n = n^2$”
Basis: $P(1) = 1$ is a perfect square	Same
Induction: $\forall k \in \mathbb{Z}_+$ assume $P(k)$ is true. Observe $S_{n+1} = S_k + 2k + 1 = m^2 + 2k + 1$ for some m. Stuck because not necessarily true that S_{k+1} is a perfect square.	$\forall k \in \mathbb{Z}_+$ assume $P(k)$ is true. So $S_n = n^2$. Thus $S_{k+1} = S_k + 2k + 1 = k^2 + 2k + 1 = (k+1)^2$

Remark 10.5. Sometimes choosing a stronger inductive hypthesis may make the proof easier.

Example 10.6. Can you perfectly tile a 4x4 checkerboard with triominoes (3 tile shapes)?
No, since each trinominoe has 3 tiles and a 4x4 checkerboard has 16 tiles and $3 \not| 16$

Theorem 10.7. Any 2^n x 2^n with a square removed can be tiled with triominoes.

Proof. We will proceed by induction. Let $P(n)$ =“any 2^n x 2^n checkerboard with one tile removed can be tiled with triominoes”
Basis: For $n = 1$, one one such checkerboard and it can be tiled using the L shaped triominoe.
Induction: Assume true for $P(k)$. Consider $P(k+1)$. Observe that a 2^{n+1} x 2^{n+1} checkerboard can be split into 4 2^n x 2^n checkerboards. Let these boards be labeled B_1, B_2, B_3, B_4. Assume WLOG, B_1 is missing a tile, then by the inductive hypothesis it can be tiled using triominoes. Next, observe that B_2, B_3, and B_4 all meet at the center of the board. Removing the the tile adjacent to the center of each of these boards allows them to be tiled using the inductive hypothesis. Finally, adding back in an L shaped triominoe to fill in the three removed tiles completes the full tiling of the board. □

10.2 Strong Induction

Rule: $P(1) \wedge \forall k \in \mathbb{Z}_+((P(1) \wedge P(2) \wedge \cdots \wedge P(k) \to P(k+1)) \therefore \forall k \in \mathbb{Z}_+(P(k))$

- Follows from $Q(n) = P(1) \wedge P(2) \wedge P(n)$ and strong induction
- Proof of "$\forall n \in \mathbb{Z}_+ P(n)$ " by induction:
  We will proceed by strong induction.
  Basis Step: Prove $P(1)$
  Inductive Step: Assume $k \in \mathbb{Z}_+$ is arbitrary and assume $P(1), \dots, P(k)$. Show $P(k+1)$. Conclude $\forall n \in \mathbb{Z}_+ P(n)$.

Theorem 10.8. If $n \geq 2$ is an integer then it can be written as the product of primes.

Proof. Basis: 2 is a prime so $P(2)$ holds.
Induction: Assume $k \geq 2$. Assume $P(2), \dots, P(k)$. We will show $P(k+1)$.
Case 1: $k+1$ is prime. Then we are done and $P(k+1)$ is true.
Case 2: $k+1$ is composite. So $k+1 = ab$ for $2 \geq a, b, \leq k$. By our inductive hypothesis, there are primes $p_1, \dots, p_n$ and $q_1, \dots, q_n$ such that $a = p_1 \cdots p_n$ and $b = q_1 \cdots q_m$. So $k = ab = p_1 \cdots p_n q_1 \cdots q_m$ so $P(k+1)$ is true. □

11 10/5/2021

11.1 More Induction

Example 11.1 (Splitting Game with n stones)**.** Rules:

- Start with pile of n stones
- Split a pile of m stones into two piles of r and s stones with $m = r + s$. Get rs points.
- Repeat on subpiles until all the piles have one stone

Claim: For every, $n \geq 1$ every strategy for the splitting game has a score of $\frac{n(n-1)}{2}$

Proof. Let $P(n) =$"the splitting game with n stones has score $\frac{n(n-1)}{2}$" Base Case: If $n = 1$, score $= 0 = \frac{1(1-1)}{2}$
Inductive Step: Assume $k \geq 1$ and score$(i) = \frac{i(i-1)}{2}$ for all $i = 1, \dots, k$. Consider the game with $k+1$ stones and let the first split be $k+1 = r+s$ where $1 \leq r, s \leq k$. Notice the score is rs+score(s)+score(t). By our inductive hypothesis this is equal to $rs + \frac{r(r-1)}{2} + \frac{s(s-1)}{2} = \frac{2rs+r^2-r+s^2-s}{2} = \frac{(r+s)(r+s-1)}{2} = \frac{(k+1)k}{2}$ □

11.2 Recursive Definition (of functions)

Goal: Define functions $f : \mathbb{Z}_+ \cup \{0\} \to \mathbb{Z}_+$

Recursive Definition:

- Basis Step: Define $f(0), f(1), \ldots, f(b)$ for some finite b
- Recursive Step: For every integer, define $f(k+1)$ in terms of $f(0), f(1), \ldots, f(k)$

Example 11.2. Fibonacci Numbers $f : \mathbb{Z}_+ \cup \{0\} \to \mathbb{Z}_+$
Basis Step: Let $f(0) = 1, f(1) = 1$
Recursive Step: If $k \geq 1$, define $f(k+1) = f(k) + f(k-1)$

Example 11.3. (Invalid Definition)
$f(0) = 1, f(1) = 1, \quad f(k+1) = f(k+2) + f(k+3)$

Example 11.4. $f(0) = 1, \quad f(k+1) = \sqrt{1 + f(k)}$

Definition 11.5. Find $a, b > 0$such that $\frac{a}{b} = \frac{a+b}{b}$
Solve for $x = \frac{a}{b}$. $x = 1 + \frac{1}{x}$ so $x^2 - x + 1 = 0$ so $x = \frac{1 \pm \sqrt{5}}{2}$ so
$\frac{a}{b} = \frac{1+\sqrt{5}}{2} = \phi$: golden ratio

Theorem 11.6. If $n \geq 2$ then $f(n) \geq \phi^{n-1}$

Proof. We will proceed by induction
Basis Step: $P(2) =$ "$f(2) > \phi$" $= 2 > \frac{1+\sqrt{5}}{2} \approx 1.618$
$P(3) =$ "$f(3) > \phi^2$ " $= 3 > (\frac{1+\sqrt{5}}{2})^2$
Inductive Step: Assume $k \geq 3$, $f(i) \geq \phi^{i-1}$ for $i = 2, 3, \ldots, k$. Observe that $f(k+1) = f(k) + f(k-1) \geq \phi^{k-1} + \phi^{k-2} = \phi^{k-2}(\phi + 1) = \phi^{k-2}(\phi^2) = \phi^k$ □

11.3 Recursive Algorithms

Recursive algorithms solve problems by reducing it to a smaller instance of the same problem.

Example 11.7. Recall: Euclidean Algorithm for computing $\gcd(a, b)$ when $a \geq b \geq 0$ are integers.
Recursive Definition: let $S = \{(a, b) : a > b \geq 0 \quad a, b \in \mathbb{Z}\}$ Define function EA: $S \to \mathbb{Z}_+$
Basis Step: EA$(a, 0) = a$ for all a
Recursive Step: If $b \geq 0$, EA$(a, b) =$EA$(b, a\text{mod}b)$.

Theorem 11.8. If $(a, b) \in S$ then EA$(a, b) =$gcd(a, b)

Proof. We will proceed by induction. Let $P(n) =$"EA$(a, b) = \gcd(a, b)$ when $b \leq n$
Base Case: $\forall a \geq 1$ EA$(a, 0) =$gcd$(a, 0) = a$
Inductive Step: Assume $b = k + 1$ and $a > 1$. We will show EA$(a, b) =$gcd(a, b). Observe that EA$(a, b) =$EA$(b, a\text{mod}b)$.By our inductive hypothesis since a mod$b < b$, it is equal to gcd$(b, a\text{mod}b) =$gcd(a, b) □

12 10/7/2021

12.1 Counting Rules: Product

Goal: Count the number of objects with some specific property = find cardinality of $S = \{x|x \text{ has has property } p\}$.

Example 12.1. Bit strings of length 10. $S = \{(b_1, \dots, b_n)|b_i \in \{0, 1\}\}$
For each bit 2 choices so total $= c_1c_2 \cdots c_10 = 2^{10}$ bit strings

Example 12.2. Ordered pairs of 2 cards from a deck of 52.
$c_1 =$ 1st card, $c_2 =$ 2nd card. $c_1 = 52$, $c_2 = 51$ so $52 * 51$ total ways.

Product Rule: Suppose can object can be specified by a sequence of n choices $c_1, \dots, c_n$ and # of ways to make $c_i = n_i$, then the total # of objects is $n_1 * n_2 * \cdots * n_k$.

To count:

- Find a sequence of choices $c_1, \dots, c_n$ that uniquely specifying an object.
- Count the number of ways to make each c_i given previous choices
- Combine using product rule

Example 12.3. How many rankings of {Cal, Stanford, UCLA, USC}?
$4 * 3 * 2 * 1 = 24$ ways.

Definition 12.4. An ordering of n distinct objects is called a permutation.

Theorem 12.5. The number of permutations of n distinct objects is $n!$

12.2 Sum and Subtraction Rules

Sum Rule: If A, B are finite and $A \cap B = \emptyset$ then $|A \cup B| = |A| + |B|$.

Example 12.6. Count the number of two digit numbers whose numbers are either both odd or both even.
$S = A \cup B$ with $A = \{(a, b)| \text{ both even}\}$ and $A = \{(a, b)| \text{ both odd}\}$
$|A| = c_1c_2 = 4^2 = 16 \quad |B| = c_1c_2 = 5^2 = 25$ so $|A \cup B| = 16 + 25 = 41$

Subtraction Rule: If A and B are finite, $|A \cup B| = |A| + |B| - |A \cap B|$

Example 12.7. How many bit strings of length 5 are there with 00 at the end or 1 at the start?
$|A| = 2^3$, $|B| = 2^4$, $|A \cap B| = 2^2$ so $|A \cup B| = 2^3 + 2^4 - 2^2 = 20$

12.3 Division Rule

Example 12.8. How many ways set of 5 ordered cards from a set of 52?
number of options decreases by 1 for each choice so
# of ways $= 52 * 51 * 50 * 49 * 48 = \frac{52!}{47!}$

Definition 12.9. An ordered sequence of r objects is called an r-permutation. The number of r-permutations of n objects is $P(n,r) = \frac{n!}{(n-r)!}$

Example 12.10. How many unordered sets of 5 cards are there from a set of 52?
Observe that # ordered sets of 5 cards = # unordered sets * # ways to order 5 cards.
So # unordered sets of 5 cards $= \frac{\text{\# ordered set}}{\text{\# ways to order set of 5}} = \frac{52!}{5!47!}$

Definition 12.11. An unordered set of r objects from a collection of n objects is called an r-combination. # of r-combinations $= C(n,r) = \frac{P(n,r)}{r!} = \frac{n!}{(n-r)!r!}$

Division Rule: If $f : A \to B$ is m to one then $|B| = \frac{|A|}{m}$

13 10/12/2021

13.1 Binomial Theorem

Example 13.1. $(x+y)^2 = x^2 + 2xy + y^2$
Observe: $(x+y)^3 = (x \overset{s_1}{+} y)(x \overset{s_2}{+} y)(x \overset{s_3}{+} y) = xxx + xxy + xyx + xyy + yxx + yxy + yyx + yyy$ can be written $(x \text{ or } y)(x \text{ or } y)(x \text{ or } y)$. So # of terms before grouping $= 2^3 = 8$
Observe that: # of terms with 3 x's = 1
# of terms with 2 x's = 2-combinations of $\{s_1, s_2, s_3\} = C(2,3) = 3$
# of terms with 1 $x = C(3,1) = 3$
# of terms with 0 x's $= C(3,0) = 1$
After grouping, $(x+y)^3 = C(3,3)x^3 + C(3,2)x^2y + C(3,1)xy^2 + C(3,0)y^3 = x^3 + 3x^2y + 3xy^2 + y^3$.

Note: $\binom{n}{r} = C(n,r)$, "n choose r", binomial coefficient

Theorem 13.2. If $n \geq 1$, then $(x+y)^n = \binom{n}{n}x^n + \binom{n}{n-1}x^{n-1}y + \cdots + \binom{n}{0}y^n = \sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}$

Proof. Let $n \geq 1$ and $0 \leq r \leq n$. Observe that the coefficient of $x^r y^{n-r}$ in $\underbrace{(x+y)(x+y)\cdots(x+y)}_{n \text{ terms}}$ is the number of terms before grouping with exactly r x's = # of r-subsets of $\{1, \ldots, n\} = \binom{n}{r}$. □

13.2 Combinatorial Identities

Example 13.3. If $n \geq 1$, $0 \leq r \leq n$ then $\binom{n}{r} = \binom{n}{n-r}$

Proof 1 (Algebra). $\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n!}{(n-r)!r!} = \binom{n}{n-r}$ □

Proof 2 (Bijection). Let $A = \{S \subseteq \{1, \dots, n\} : |S| = r\}$, $B = \{S \subseteq \{1, \dots, n\} : |S| = n - r\}$. We know that $|A| = \binom{n}{r}, |B| = \binom{n}{n-r}$. Observe that $f : A \to B$ by $f(S) = \{1, \dots, n\} - S = \overline{S}$ is a bijection so $|A| = |B|$. Thus, $\binom{n}{r} = \binom{n}{n-r}$, as desired. □

Example 13.4. If $n \geq 1$, then $2^n = \binom{n}{n} + \binom{n}{n-1} + \cdots + \binom{n}{1} + \binom{n}{0} = \sum_{r=0}^{n} \binom{n}{r}$

Proof 1 (Algebra). Plug in $x = y = 1$ into the binomial theorem. □

Proof 2 (Counting in 2 ways). We will count all subsets of $\{1, \dots, n\}$ in two ways.
Method 1: A set $S \subseteq \{1, \dots n\}$ is uniquely determined by the choices $1 \in S?, 2 \in S?, \dots, n \in S?$. So there are 2^n ways.
Method 2: A set $S \subseteq \{1, \dots, n\}$ is uniquely determined by first choosing the size of the set in $0 \leq r \leq n$, then choose a subset S such that $|S| = r$. By the sum rule there is $\sum_{r=0}^{n} \binom{n}{r}$.
Thus, $2^n = \sum_{r=0}^{n} \binom{n}{r}$. □

Example 13.5. If $n \geq 1$ and $1 \leq r \leq n$ then $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$

Proof. We will choose an r-subset of $\{1, \dots, n\}$ in two different ways.
Method 1: $\binom{n}{r}$ ways by def.
Method 2: Observe that every r-subset of $\{1, \dots, n\}$ either contains 1 or not. Every r-subset of S that contains 1 can be determined by an $r - 1$ subset $T \subseteq \{2, \dots, n\}$ by taking $T \cup \{1\}$. Every subset that does not contain 1 is equivalent to an r-subset T of $\{2, \dots, n\}$ with $S + T$. So by sum rule, # of r-subsets = # of r-subsets with 1 + # of r-subsets without 1 = $\binom{n-1}{r-1} + \binom{n-1}{r}$ □

13.3 Permutations and Combinations with Repetitions

So far repetition has not been allowed.

Example 13.6. How many 7 digit permutations with repetition of the set $\{1, \dots, 9\}$?
Choices $c_1, c_2, \dots, c_7$ all have 10 options so 10^7 ways.

In general: There are n^r ways to choose an r-permutation of $\{1, \dots, n\}$.

14 10/14/2021

14.1 Permutations and Combinations with Repetitions

Example 14.1. How many different 5-scoop sundaes can be made from {mint, chocolate, vanilla}?
Idea: A sundae is completely determined by the number of scoops of each flavor. This is equivalent to depositing 5 indistinguishable tokens into 3 boxes. Letting the tokens be represented by 0s and the divisions between the boxes be represented by 1s, this is equivalent to bit strings of length 7 with 5 0s and 2 1s. Thus, there are $\binom{7}{2}$ ways.

Theorem 14.2.

1. The number of ways to place n indistinguishable objects into k boxes is $\binom{n+k-1}{k-1}$.

   Proof. Allocations are in bijection with $n+k-1$ bit strings with exactly $k-1$ 1's corresponding to the dividers between the k boxes. □

2. The number of n-combinations of r-objects with repetitions is $\binom{n+r-1}{r-1}$

   Proof. Such combinations are in bijection with the allocations of n indistinguishable objects into r boxes. □

14.2 Putting objects into boxes

Allocations of n objections into k boxes where order does not matter.

- If the objects are distinct there are n^k total ways.
- Variation: Case with ith box for $i = 1, \dots, k$ must have n_i objects

Example 14.3. How many ways are there to deal 4 hands of 5 cards from a deck of 52 cards?
Idea: 5 boxes, 52 objects. Process:

1. Choose H_1 $\binom{52}{5}$ ways
2. Choose H_2 $\binom{47}{5}$ ways
3. Choose H_3 $\binom{42}{5}$ ways
4. Choose H_4 $\binom{37}{5}$ ways
5. Choose remaining 32 $\binom{32}{32}$ ways

Total $= \binom{52}{5}\binom{47}{5}\binom{42}{5}\binom{37}{5}\binom{32}{32} = \frac{52!}{5!47!}\frac{47!}{5!42!}\frac{42!}{5!37!}\frac{37!}{5!32!}\frac{32!}{32!0!} = \frac{52!}{5!5!5!5!32!}$

- In general there are $\frac{n!}{n_1! \cdots n_k!}$ ways to put n distinguishable objects into k distinguishable boxes with n_i in the ith box (provided $n = n_1 + n_2 + \cdots + n_k$).

Example 14.4. How many distinct words can be made by rearranging ANAGRAM?
Make a token for each position $1, 2, \ldots, 7$. Make a box for each letter A, N, G, R, M. # of ways = # of allocations of $(3, 1, 1, 1, 1)$ tokens $= \frac{7!}{3!1!1!1!1!} = \frac{7!}{3!}$

Remark 14.5. If boxes are indistinguishable no closed formulas.

14.3 Pigeonhole Principle

Theorem 14.6. If $k \geq 1$ and $k + 1$ or more objects are placed into k boxes then there is a box that has two or more objects

Proof. We will show the contrapositive. Assume every box has at most one object. Then since there are k boxes, there are at most k objects. □

Example 14.7. In a group of 367 people, two people have the same birthday.

Proof. There are 367 people placed into 366 boxes corresponding to possible birthdays so two people are in the same box. □

Example 14.8. If 5 integers are chosen from $\{1, 2, \ldots, 8\}$ there are 2 that add up to 9.

Proof. Observe that $\{1, \ldots, 8\}$ can be partitioned into 4 sets: $\{1, 8\}, \{2, 7\}, \{3, 6\}, \{4, 5\}$. Since 5 integers are chosen, two must be in the same set so they add up to 9. □

Example 14.9 (Chinese Remainder Theorem with 2 integers)**.** Assume $\gcd(m, n) = 1$ and $0 < a < m$, $0 < b < n$. There is an integer x such that $x \equiv a (\text{mod } m)$, $x \equiv b (\text{mod } n)$.

Proof. Consider $a + 0 = a, a_1 = a + n, \ldots, a_{n-1} + (n - 1)m$. Notice that $a_i \equiv a (\text{mod } m)$ for $I \leq n - 1$.
Create $n - 1$ boxes by letting $B_i = \{x : x \equiv i (\text{mod } n)\}$. Assume $a_i \not\equiv b (\text{mod } m)$. Each $a_i \in B_j$ for some j. By the pigeonhole principle, there is some j, i_1, i_2 such that $a_{i_1} \equiv a_{i_2} \equiv j (\text{mod } n)$. This implies $n | (a_{i_1} - a_{i_2})$ so $n | (i_1 - i_2)m$. Since $\gcd(n, m) = 1$, $n | i_1 - i_2$ which is a contradiction since $i_1, i_2 < n$. □

- Generalized Pigeonhole Principle: If you put N object into k boxes then some box has at least $\lceil \frac{N}{k} \rceil$ objects.

15 10/19/2021

15.1 Recurrence Relations

A recurrence relation is simply a recursive definition of a sequence $(a_0, a_1, \ldots, a_n)$

Example 15.1. How many ways in the letter {L, A} are there to write 100 letters such that no 2 L's are adjacent?
Let $a_n = \#$ of strings of length n:
$a_1 = 2$ - A, L $\quad a_2 = 3$ - AA, AL, LA
Consider the process of determining a string of length n:

1. First letter A. Choose string of length $n-1$.

2. First letters LA. Choosing string of length $n-2$.

By sum rule, $a_n = a_{n-1} + a_{n-2}$.

Example 15.2. Suppose $x_0 * x_1 * x_2 * x_3$. How many ways to parenthesize?
Let C_n be the number of ways to $n+1$ vars.

1. Choose one of the n $*$'s to be the innermost multiplication. i.e. $\pi = \pi_1 * \pi_2$. Assume π_1, has $k+1$ vars and π_2 has $n-k$ vars.

2. Choose parenthesization for $\pi_1 = C_k$, $\pi_2 = C_{n-k-1}$

By sum rule, $C_n = C_0C_{n-1} + C_1C_{n-2} + \cdots + C_{n-2}C_1 + C_{n-1}C_0 = \sum_{k=0}^{n-1} C_kC_{n-k-1}$
$C_2 = C_0C_1 + C_1C_0 = 1 + 1 = 2$
$C_3 = C_0C_2 + C_1C_1 + C_2C_0 = 2 + 1 + 2 = 5$

15.2 Inclusion Exclusion

For finite sets A and B, $|A \cup B| = |A| + |B| - |A \cap B|$

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

	RH	LH
Elements that appear in exactly 1 set	1	1
Elements that appear in exactly 2 sets	1	2-1 = 1
Elements that appear in exactly 3 sets	1	3 - 3 + 1 = 1

Both sides equal so equality holds.

Theorem 15.3. If $A_1, \ldots, A_n$ are finite sets,

$$\begin{aligned}|A_1 \cup \cdots \cup A_n| &= |A_1| + \cdots + |A_n| - |A_1 \cap A_2| - |A_1 \cap A_3| - \cdots + (-1)|A_1 \cap \cdots \cap A_n| \\ &= \sum_{k=0}^{n} (-1)^{k-1} \sum_{S \subseteq [n], |S|=k} |\bigcap_{i \in S} A_i|\end{aligned}$$

Proof. Consider an arbitrary element a. Suppose a is in exactly r sets. Then a is counted exactly $\binom{r}{m}$ times by the summations involving m terms. So a is counted $\binom{r}{1} - \binom{1}{2} + \cdots + (-1)^{r+1}\binom{r}{r}$. Since $\binom{r}{0} - \binom{r}{1} + \binom{1}{2} + \cdots + (-1)^{r+1}\binom{r}{r} = 0$, $1 = \binom{r}{0} = \binom{r}{1} - \binom{1}{2} + \cdots + (-1)^{r+1}\binom{r}{r}$. Thus, each element is counted exactly once. □

16 10/21/2021

16.1 Inclusion Exclusion

Definition 16.1. A permutation $\pi = (\pi_1, \pi_2, \dots, \pi_2)$ of $[n]$ is a derangement if $pi_i \neq i$ for $i \leq n$.

Example 16.2 (Derangements)**.** Let $S_n = \{\pi : \pi \text{ is a permutation of } [n]\}$
$D_n = \{\pi \in S_n : \pi \text{ is a derangement}\}$
Let $A_1 = \{\pi \in S_n : \pi_i = i\}$ Observe that $D_n = S_n - (A_1 \cup A_2 \cup \cdots \cup A_n)$ so
$|D_n| = |S_n| - |A_1 \cup A_2 \cup \cdots \cup A_n|$

$$\begin{aligned}
|A_1 \cup \cdots \cup A_n| &= \sum_{k=0}^{n} (-1)^k \sum_{S \subset [n], |S|=k} |\bigcap_{i \in S} A_i| \\
&= \sum_{n=0}^{k} (-1)^k \sum_{S \subset [n], |S|=k} (n-k)! = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)! \\
&= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum (-1)^k \frac{1}{k!}
\end{aligned}$$

$|D_n| = n! - n! \sum_{k=0}^{n} (-1)^n \frac{1}{k!} = n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} - \cdots + (-1)^n \frac{1}{n!}) \approx \frac{n!}{e} \approx 0.37 * n!$

16.2 Probability

The process of reasoning of about uncertainty

Example 16.3. Suppose you flip 2 fair coins, what is the probability they are different?
Possible Outcomes: HH, HT, TH, TT Successful Outcomes: HT, TH
Probability of success $= \frac{\text{\# of successful outcomes}}{\text{\# of total outcomes}} = \frac{2}{4} = \frac{1}{2}$

Definition 16.4.

1. An experiment is a well defined procedure within a set of possible outcomes. An outcome is a complete description of the result of an experiment.
2. The set of all outcomes is the sample space.
3. An outcome is a subset of the sample space.
4. The probability of E, denoted $\mathbb{P}(E)$, is $\mathbb{P}(E) = \frac{|E|}{|S|}$

Two assumptions of classical probability:

- S is finite.
- All outcomes are equally likely.

Example 16.5. Flip 10 fair coins. What is the probability of getting exactly 5 H?
Sample Space $S = \{(s_1, \ldots, s_n) : s \in \{\text{H}, \text{T}\}\} = \{\text{H}, \text{T}\}^{10} \quad |S| = 2^{10}$
Event $E = \{(s_1, \ldots, s_n) : 5 \text{ of } s_i = \text{H}\} \quad |E| = \binom{10}{5}$
$\mathbb{P}(E) = \frac{|E|}{|S|} = \frac{\binom{10}{5}}{2^{10}} = \frac{252}{1024} \approx 25\%$

Example 16.6. A flush is 5 cards of the same suit. What is the probability of a flush in poker?
Sample Space $S = \{H \subseteq [52] : |H| = 5\} \quad |S| = \binom{52}{5}$
Event $E = E_D \cup E_H \cup E_S \cup E_C$ where $E_D = \{H \subset S : \text{all cards in } H \text{ have suit } D\}$
$|E| = 4 * \binom{13}{5}$
$\mathbb{P}(E) = \frac{|E|}{|S|} = \frac{4 * \binom{13}{5}}{\binom{52}{5}} \approx \frac{2}{1000}$

In general choose S so that:

- It has all relevant features to express E.
- Counting is easy.

Example 16.7. What is the probability that two people in a group of 40 have the same birthday?
Experiment: Assign each person a birthday in $\{1, \ldots, 365\}$ uniformly and randomly.
Sample space $S = \{1, \ldots, 365\}^{30} \quad |S| = 365^{30}$
Event $E = \{(s_1, s_2, \ldots, s_{30}) : \exists i \neq j \text{ s.t. } s_i = s_j\}$
Note: $\mathbb{P}(E) + \mathbb{P}(S - E) = 1$ so $\mathbb{P}(\overline{E}) = 1 - \mathbb{P}(E)$
$\overline{E} = \{(s_1, \ldots, s_{30} : s_i \in [365] \text{ all distinct}\} \quad |E| = P(365, 30) = \frac{365!}{335!}$
$\mathbb{P}(E) = 1 - \frac{365!}{335! * 365^{30}} \geq 90\%$

16.3 Probability Theory

Motivation: What if all events not equally likely.

Definition 16.8. A probability space consists of a sample space S with a probability distribution $p : S \to R$ satisying:

1. $p(s) \in [0, 1] \ \forall s \in S$
2. $\sum_{s \in S} p(s) = 1$

Example 16.9 (Monty Hall Problem)**.** 1. Car placed behind 1 of 3 doors at random. Goats behind other 2.

2. Choose door at random.

3. Monty opens one of other doors revealing a goat.
Q) Should you switch or not? A) Yes

Sample Space $S = \{(\text{car,you,monty}) : \text{car,you,monty} \in \{1, 2, 3\}$ monty$\neq$car,

monty$\neq$you}
Event $E = \{$(car,you,monty) : you=car$\}$
Consider to possible choices: You chose the car initially or you chose a goat initially:

- If you chose the car initially and you switch the the remaining door, you will lose.
- If you chose the goat initially and you switch to the remaining door, you will win since Monty must reveal a door with a goat.

Thus, by switching you win with 2/3 probability as opposed to 1/3 without switching.

17 10/26/2021

17.1 Conditional Probability

Given probabilities for some events $E_1, E_2, \dots, E_n$, what can we say about $\mathbb{P}(F)$?

- Sum Rule: For any two events: $\mathbb{P}(E \cup F) = \mathbb{P}(E) + \mathbb{P}(F) - \mathbb{P}(E \cap F)$
- Special Case: If $E \cap F = \emptyset$, then $\mathbb{P}(E \cup F) = \mathbb{P}(E) + \mathbb{P}(F)$
- Complement: $\mathbb{P}(E) + \mathbb{P}(\overline{E}) = 1 = \mathbb{P}(S)$

Definition 17.1. If E, F are events and $\mathbb{P}(F) > 0$, then the probability of E given F is defined as $\mathbb{P}(E|F) = \frac{\mathbb{P}(E \cap F)}{\mathbb{F}}$

Example 17.2. Expt = pick a random person in the US. $S = \{1, \dots, 3 * 10^6\}$
$C =$ person is a Cal student $\quad |C| = 30 * 10^3$
$B =$ person lives in Berkeley $\quad |C| = 200 * 10^3$
$B \cap C =$ person is Cal student and lives in Berkeley $\quad |B \cap C| = 20 * 10^3$
$\mathbb{P}(C|B) = \frac{\mathbb{P}(B \cap C)}{\mathbb{P}(B)} = \frac{20*10^3/300*10^6}{200*10^3/300*10^6} = \frac{1}{5}$
$\mathbb{P}(B|C) = \frac{\mathbb{P}(B \cap C)}{\mathbb{P}(C)} = \frac{20*10^3/300*10^6}{30*10^3/300*10^6} = \frac{1}{5} = \frac{2}{3}$

- Product Rule: $\mathbb{P}(E \cap F) = \mathbb{P}(E|F)\mathbb{P}(F)$
- More Generally: $\mathbb{P}(E \cap F \cap G) = \mathbb{P}(E|F \cap G)\mathbb{P}(F|G)\mathbb{P}(G)$

Proposition 17.3 (Law of Total Probability)**.** $\mathbb{P}(E) = \mathbb{P}(E|F)\mathbb{P}(F) + \mathbb{P}(E|\overline{F})\mathbb{P}(\overline{F})$

Proof. Note that $(E \cap F) \cap (E \cap \overline{F}) = \emptyset$

$$\begin{aligned} \mathbb{P}(E) &= \mathbb{P}((E \cap F) \cup (E \cap \overline{F}) \\ &= \mathbb{P}(E \cap F) + \mathbb{P}(E \cap \overline{F}) \\ &= \mathbb{P}(E|F)\mathbb{P}(F) + \mathbb{P}(E|\overline{F})\mathbb{P}(\overline{F}) \end{aligned}$$

□

Theorem 17.4 (Bayes' Rule)**.**

$$\mathbb{P}(E|F) = \frac{\mathbb{P}(F|E)\mathbb{P}(E)}{\mathbb{P}(F)}$$

Proof. $\mathbb{P}(E \cap F) = \mathbb{P}(E|F)\mathbb{P}(F) = \mathbb{P}(F|E)\mathbb{P}(E)$ by def of conditional probability, so Bayes' Rule follows. □

Example 17.5 (Medical Testing - Prostate Cancer PSA Test)**.** The NIH states the following:

1. If a patient has PC, the test is positive 80% of the time
2. If a patient does not have PC, the test is positive 10% of the time
3. 0.16% of men have PC

Q1) What is the likelihood of testing positive?
Q2) If someone tests positive what is the likelihood they have PC?
Expt: C = chosen person has PC T = person test positive.
By assumption 1) $\mathbb{P}(T|C) = 0.8$ 2) $\mathbb{P}(T|\overline{C}) = 0.1$ 3) $\mathbb{P}(C) = 0.0016$

A1) $\mathbb{P}(T) = \mathbb{P}(T|C)\mathbb{P}(C) + \mathbb{P}(T|\overline{C})\mathbb{P}(\overline{C})$
$= (0.8)(0.0016) + (0.1)(0.9984) \approx 0.10$

A2) $\mathbb{P}(C|T) = \frac{\mathbb{P}(T|C)\mathbb{P}(T)}{\mathbb{P}(T)} = \frac{(0.8)(0.0016)}{(0.10)} \approx 1.3\%$

17.2 Independence

Definition 17.6. Events E, F are independent if $\mathbb{P}(E \cap F) = \mathbb{P}(E)\mathbb{P}(F)$ or equivalently, $\mathbb{P}(E|F) = \mathbb{P}(E)$, $\mathbb{P}(F|E) = \mathbb{P}(F)$.

Example 17.7. Expt: Flip 2 coins.
H_1= 1rst coin heads. H_2= 2cnd coin heads.
$\mathbb{P})(H_1 \cap H_2) = \frac{1}{4} = \frac{1}{2} * \frac{1}{2} = \mathbb{P}(H_1)\mathbb{P}(H_2)$ so the events are independent.

Example 17.8. Expt: Roll 1 die.
$E_1 = \{$roll a 1 $\}$ $E_2 = \{$roll a 2 $\}$
$\mathbb{P}(E_1 \cap E_2) = 0 \neq \frac{1}{36} = \mathbb{P}(E_1)\mathbb{P}(E_2)$ so the events are dependent.

18 10/28/2021

18.1 Independence

Example 18.1. Expt = Flip 3 independent fair coins. $S = \{H, T\}^3$
$E_1 = \{S :$ first coin is $H\}$ $E_{odd} = \{S :$ odd number of heads$\}$
Are E_1 and E_{odd} independent?
$\mathbb{P}(E_1) = 1/2$
$\mathbb{P}(E_{odd}) = \mathbb{P}($exactly one head$) = \mathbb{P}($exactly 3 heads$) = 1/8 + 1/8 = 1/4$
$\mathbb{P}(E_1 \cap E_{odd}) = \mathbb{P}(E_1 \cap$ 1 H$) + \mathbb{P}(E_1 \cap$ 3 H$) = 1/8 + 1/8 = 1/4$
$\mathbb{P}(E_1)\mathbb{P}(E_{odd}) = \mathbb{P}(E_1 \cap E_{odd})$ so the events are independent.

18.2 Random Variables

Definition 18.2. A random variable on a probability space is a function $X : S \to \mathbb{R}$

Definition 18.3. The expectation of a random variable X on S is

$$\mathbb{E}X = \sum_{s \in S} p(s)X(s)$$

Equivalently: $\mathbb{E}X = \sum_{r \in S(X)} r\mathbb{P}(X = r)$

Example 18.4. Flip 3 independent biased coins with $\mathbb{P}(\mathrm{H}) = q, q \in [0, 1]$. What is the average number of heads?
$S = \{\mathrm{H}, \mathrm{T}\}^3 \quad p(s) = q^{\#\mathrm{H}}(1 - q)^{\#\mathrm{T}}$ so
$\mathbb{E}X = 0 * (1 - q)^3 + 1 * 3 * q(1 - q)^2 + 2 * 3 * q^2(1 - q) + 3 * q^3$
if $q = 1/3$, $\mathbb{E}X = 3 * (1/3)(4/9) + 2 * 3 * (1/9)(2/3) + 3(1/27) = (27/27) = 1$

Example 18.5 (Bernoulli Trials)**.** Flip n independent biased coins with $\mathbb{P}(\text{heads}) = q$, $\mathbb{P}(\text{tails}) = 1 - q$.
Let $X = \#$ of heads $\in \{0, 1, \ldots, n\} \quad \mathbb{P}(x = k) = \binom{n}{k} q^k (1 - q)^{n-k}$
Notice $\sum_{k=0}^{n} \binom{n}{k} q^k (1 - q)^{n-k} = 1$ by the binomial theorem

$$\begin{aligned} \mathbb{E}X &= \sum_{k=1}^{n} k \binom{n}{k} q^k (1 - q)^{n-k} = \sum_{k=1}^{n} \frac{kn!}{k!(n - k)!} q^k (1 - q)^{n-k} \\ &= qn \sum_{k=1}^{n} \frac{(n - 1)!}{(k - 1)!(n - 1 - (k - 1))!} q^{k-1} (1 - q)^{n-1-(k-1)} = qn \end{aligned}$$

18.3 Linearity of Expectation

Can add two random variables $X_1 : S \to \mathbb{R}$, $X_2 : S \to \mathbb{R}$ by defining $(X_1 + X_2)(s) = X_1(s) + X_2(s)$

Proposition 18.6. If X_1, X_2 are random variables on S then $\mathbb{E}(X_1 + X_2) = \mathbb{E}X_1 + \mathbb{E}X_2$.

Proof.

$$\begin{aligned} \mathbb{E}(X_1 + X_2) &= \sum_{s \in S} p(s)(X_1 + X_2)(s) = \sum_{s \in S} p(s)(X_1)(s) + p(s)X_2(s) \\ &= \sum_{s \in S} p(s)(X_1)(s) + \sum_{s \in S} p(s)X_2(s) \\ &= \mathbb{E}X_1 + \mathbb{E}X_2 \end{aligned}$$

□

Example 18.7 (Bernoulli Trials)**.** Consider the alternate calculation of the expected value of n Bernoulli trials.
Let $X_1 = \begin{cases} 1 \text{ if } i \text{ is H} \\ 0 \text{ if } i \text{ is T} \end{cases}$ for $i = 1, \dots, n$ Let $X = \#$ of heads
$\mathbb{E}X_i = 0 * \mathbb{P}(X_i = 0) + 1 * \mathbb{P}(X_i = 1) = q$
Observe $X = X_1 + \cdots + X_n$ so by linearity of expectation,
$\mathbb{E}X = \mathbb{E}\big(\sum_{i=1}^n X_i\big) = \sum_{i=1}^n \mathbb{E}X_i = qn$

Example 18.8. Let π = permutation of $\{1, \dots, n\}$. What is the expected number of fixed points?
$S = \{\pi : \pi is a permutation of [n]\}$ p is uniform
Let $X : S \to \mathbb{R}$ be $X(\pi) = \#$ of fixed points
Let $X_i = \begin{cases} 1 \text{ if } \pi_i = i \\ 0 \text{ if } \pi_i \neq i \end{cases}$ $\mathbb{E}X_i = \mathbb{P}(\pi_i = i) = \frac{(n-1)!}{n!} = \frac{1}{n}$
Observe that $\mathbb{E}X = \mathbb{E}(X_1 + \cdots + X_n) = \mathbb{E}X_1 + \cdots + \mathbb{E}X_n$, so $\mathbb{E}X = n * \frac{1}{n} = 1$

19 11/2/2021

19.1 Linearity of Expectation

Example 19.1. Suppose that I throw n (independent) balls into n bins. $\mathbb{P}$(Ball i lands in bin j) $= \frac{1}{n}$.
How many bins remain empty on average?
Let $X_i = \begin{cases} 1 \text{ if bin } i \text{ is not empty} \\ 0 \text{ otherwise} \end{cases}$ for $i = 1, 2, \dots, n$
total # empty bins $X = X_1 + X_2 + \cdots + X_n$

$$\begin{aligned} \mathbb{E}X_i &= \mathbb{P}(\text{Bin } i \text{ empty}) \\ &= \mathbb{P}(\text{Ball } 1 \notin \text{Bin } i \cap \text{Ball } 2 \notin \text{Bin } i \cap \cdots \cap \text{Ball } n \notin \text{Bin } i) \\ &= \mathbb{P}(\text{Ball } 1 \notin \text{Bin } i) \cdots \mathbb{P}(\text{Ball } n \notin \text{Bin } i) \\ &= (1 - \frac{1}{n})(1 - \frac{1}{n}) \cdots (1 - \frac{1}{n}) = (1 - \frac{1}{n})^n \end{aligned}$$

So $\mathbb{E}X = n(1 - \frac{1}{n})^n \approx \frac{n}{e} \approx 37\%$

19.2 Distribution

Definition 19.2. Given a probability space S and a random variable $X : S \to S$, the distribution of X is the set $\{(r, P(X = r) | r \in X(S)\}$

Example 19.3 (Bernoulli Distribution)**.** $S = \{\text{H}, \text{T}\}$ $p(\text{H}) = q \in [0, 1]$
$X(S) = \begin{cases} 1 \text{ if } S = \text{H} \\ 0 \text{ if } S = \text{ T} \end{cases}$ Distribution: $\{(0, 1 - q), (1, q)\}$

Example 19.4 (Binomial Distribution)**.** Expt: Flip n coins with bias q.
$X =$ total # of heads $\quad \mathbb{P}(X = k) = \binom{n}{k} q^k (1-q)^{n-k}$ for $k = 0, \ldots, n$

Example 19.5 (Geometric Distribution)**.** Expt: Flip a coin with bias q repeatedly until it lands H.
$S = \{\mathrm{H}, \mathrm{HT}, \mathrm{HHT}, \ldots, \mathrm{T}^m\mathrm{H}, \ldots\}$
$\mathbb{P}(\mathrm{T}^m\mathrm{H}) = (1-q)^m q$ because coins flips are independent
$\sum_{m=0}^{\infty} \mathbb{P}(\mathrm{T}^m\mathrm{H}) = \sum_{m=0}^{\infty} q(1-q)^m = q * \frac{1}{1-(1-q)} = 1$
Let $X : S \to R \quad X = \#$ of flips until lands on heads so $X(\mathrm{T}^m\mathrm{H}) = m + 1$
$\mathbb{E}X = 1q + 2q(1-q) + 3q(1-q)^2 + \cdots = \sum_{m=0}^{\infty} (m+1)q(1-q)^m$
Consider $\frac{1}{q} = \sum_{m=0}^{\infty} (1-q)^m$
Differentiating both sides yields: $-\frac{1}{q^2} = (-1) \sum_{m=1}^{\infty} m(1-q)^{m-1}$
so $\frac{1}{q} = \sum_{m=1}^{\infty} mq(1-q)^{m-1} = \sum_{m=0}^{\infty} (m+1)q(1-q)^m$
Thus, $\mathbb{E}X = \frac{1}{q}$

20 11/9/2021

20.1 Algebra and Independence of Random Variables

Definition 20.1. Two random variables $X, Y : S \to S$ are independent if $\forall r_1, r_2 \in \mathbb{R}\mathbb{P}(X = r_1 \text{ and } Y = r_2) = \mathbb{P}(X = r_1)\mathbb{P}(Y = r_2)$

Example 20.2. Event: roll two independent dice.
$X = \#$ on first die $\quad Y = \#$ on second die
$\forall r_1, r_2 \in \{1, \ldots, 6\}\mathbb{P}(X = r_1 \text{ and } Y = r_2) = \frac{1}{36} = \mathbb{P}(X = r_1)\mathbb{P}(Y = r_2)$
However, $X, Z = 1_{\{\text{1rst die 1}\}}$ are not independent since,
$\mathbb{P}(X = 1 \text{ and } Z = 1) = \frac{1}{6} \neq \frac{1}{6} * \frac{1}{6} = \mathbb{P}(X = 1)\mathbb{P}(Z = 1)$

Theorem 20.3. If $X, Y : S \to \mathbb{R}$ are independent random variables, then $\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$.

Proof. See book. □

- Independence allows us to decompose complicated random variables into simpler ones.

20.2 Variance

Variance is a way to measure how spread out the range of a random variable is.

Definition 20.4. If $V : S \to \mathbb{R}$ is a random variable and $\mathbb{E}(X) = \mu$, then the variance of X is $V(X) = \mathbb{E}(X - \mu)^2$.

Example 20.5. Let $X = 0$ and let $Y = \begin{cases} 1 \text{ if } s = \mathrm{H} \\ -1 \text{ if } s = \mathrm{T} \end{cases}$

	$\mathbb{E}$	V
X	$\mathbb{E}(X) = 0$	$V(X) = \mathbb{E}(X - 0(=)^2 = \mathbb{E}(X)^2 = 0$
Y	$\mathbb{E}(Y) = \frac{1}{2}(1) + \frac{1}{2}(-1) = 0$	$V(Y) = \mathbb{E}(Y - 0)^2 = \mathbb{E}(Y)^2 = \frac{1}{2}(1)^2 + \frac{1}{2}(-1)^2 = 1$

Example 20.6. Expt: Flip a biased coin with $p(\mathrm{H}) = q \in [0,1]$, $p(\mathrm{T}) = 1-q$.
Let $X = \begin{cases} 1 \text{ if H} \\ 0 \text{ if T} \end{cases} \qquad \mu_X = \mathbb{E}(X) = q$
$V(X) = \mathbb{E}(X-\mu_X)^2 = (1-q)(0-q)^2 + q(1-q)^2 = q(1-q)(q+(1-q)) = q(1-q)$
Q) What value of q maximizes $V(X)$? A)$q = \frac{1}{2} \to V(X) = \frac{1}{4}$
Q) What value of q minimizes $V(X)$? A)$q = 0, 1 \to V(X) = 0$

Remark 20.7. Suppose $\mathbb{E}(X) = \mu$

$$\begin{aligned} V(X) &= \mathbb{E}(X-\mu)^2 = \mathbb{E}(X^2 - 2\mu X - \mu^2) = \mathbb{E}X^2 - 2\mu\mathbb{E}X + \mu^2 = \mathbb{E}X^2 - 2\mu^2 + \mu^2 \\ &= \mathbb{E}X^2 - \mu^2 \end{aligned}$$

Remark 20.8. $\sqrt{V(X)}$ standard deviation of X.

Theorem 20.9 (Bienayme's Identity)**.** If X and Y are independent random variables, then $V(X+Y) = V(X) + V(Y)$.

Proof. Let $\mu_X = \mathbb{E}X$ and $\mu_Y = \mathbb{E}Y$, so $\mu_X + \mu_Y = \mathbb{E}(X+Y)$

$$\begin{aligned} V(X+Y) &= \mathbb{E}(X+Y-\mu_X-\mu_Y)^2 = \mathbb{E}(X+Y)^2 - (\mu_X+\mu_Y)^2 \\ &= \mathbb{E}X^2 + \mathbb{E}Y^2 + 2\mathbb{E}XY - \mu_X^2 - \mu_Y^2 - 2\mu_X\mu_Y \\ &= \mathbb{E}X^2 + \mathbb{E}Y^2 + 2\mu_X\mu_Y - \mu_X^2 - \mu_Y^2 - 2\mu_X\mu_Y \\ &= \mathbb{E}X^2 + \mathbb{E}Y^2 - \mu_X^2 - \mu_Y^2 \\ &= V(X) + V(Y) \end{aligned}$$

□

Remark 20.10. If $X_1, \dots, X_n$ are pairwise independent then $V(X_1 + \cdots + X_n) = V(X_1) + V(X_2) + \cdots + V(X_n)$.

Example 20.11. Suppose you are given a coin with bias $q \in [0,1]$. How do you estimate q?
Flip n times to see how many heads. Let $X = \#$ of heads.
Let $\hat{q} = \frac{X}{n}$. Will show $V(\frac{X}{n})$ gets really small as n gets really big.
Let $X_i = \begin{cases} 1 \text{ if } i\text{th flip H} \\ 0 \text{ otherwise} \end{cases}$. $X = X_1 + X_2 + \cdots + X_n$ so
$\mathbb{E}X = \mathbb{E}X_1 + \mathbb{E}X_2 + \cdots + \mathbb{E}X_n = qn$ so $\mathbb{E}\frac{X}{n} = q$.
Observe that X_i, X_j are independent for $\forall I \neq j$
so $V(\frac{X}{n}) = V(\frac{X_1}{n}) + V(\frac{X_2}{n}) + \cdots + V(\frac{X_n}{n})$
$V(\frac{X_i}{n}) = \mathbb{E}(\frac{X_i}{n} - \mathbb{E}\frac{X_i}{n})^2 = \frac{1}{n^2}\mathbb{E}(X_i - \mathbb{E}X_i)^2 = \frac{q(1-q)}{n^2}$
so $V(X) = n * \frac{q(1-q)}{n^2} = \frac{q(1-q)}{n} \leq \frac{1/4}{n} = \frac{1}{4n}$

21 11/16/2021

21.1 Markov and Chebyshev's Inequalities

Example 21.1. Expt: Choose a student at random. $Y =$ midterm 2 score. Given $\mathbb{E}Y = 80$. What can we say about $\mathbb{P}(Y \geq 90)$?

$$\begin{aligned}\mathbb{E}Y &= \sum_{r \in \text{Ran}(Y)} r\mathbb{P}(Y = r) = \sum_{r \geq 90} r\mathbb{P}(Y = r) + \sum_{r < 90} r\mathbb{P}(Y = r)\\ &\geq \sum_{r \geq 90} r\mathbb{P}(Y = r) + 0\\ &\geq 90 \sum_{r \geq 90} \mathbb{P}(y = r) = 90\mathbb{P}(Y \geq 90)\end{aligned}$$

So, $\mathbb{E}Y \geq 90\mathbb{P}(Y \geq 90)$. Thus, $P(Y \geq 90) \leq \frac{\mathbb{E}Y}{90} = \frac{80}{90} = \frac{8}{9}$

Theorem 21.2 (Markov's Inequality)**.** *If Y is a nonnegative random variable, then for every $t > 0$, $\mathbb{P}(Y \geq t) \leq \frac{\mathbb{E}(Y)}{t}$*

Remark 21.3. No information gained for $t < \mathbb{E}Y$

Remark 21.4. Need $Y \geq 0$ otherwise false in general.

Theorem 21.5 (Chebyshev's Inequality)**.** *If X is a random variable and $\mathbb{E}X = \mu$, $t > 0$ then $\mathbb{P}(|X - \mu| \geq t) \leq \frac{V(X)}{t^2}$*

Proof. Given X, $\mathbb{E}X = \mu$, Let $Y = (X - \mu)^2$.
Notice that $\mathbb{E}Y = \mathbb{E}(X - \mu)^2 = V(X)$
By Markov's Inequality $\mathbb{P}(Y \geq t^2) \leq \frac{V(X)}{t^2}$
$\mathbb{P}(Y \geq t^2) = \mathbb{P}(|X - \mu|^2 \geq t^2) = \mathbb{P}(|X - \mu| \geq t) \leq \frac{V(X)}{t^2}$ □

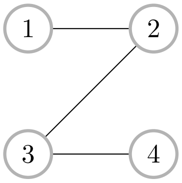
Example 21.6. Consider the experiment from example 1.
Given that $V(Y) = 400$, $\mathbb{P}(|Y - 80| \geq 25) \leq \frac{400}{625} = \frac{16}{25}$

21.2 Graph Theory

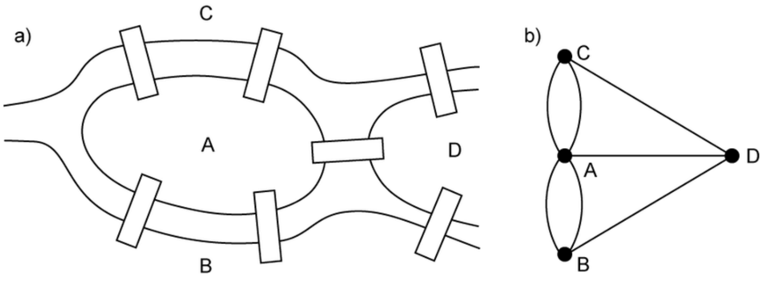
Graph: Mathematical object that models pairwise relationships

Definition 21.7. A graph $G = (V, E)$ is a pair of sets V, called the set of vertices, E called to the set edges such that E is a set of unordered pair of elements in V. ie. $E \subseteq \{S : S \subseteq V, |S| = 2\}$

Example 21.8. $V = \{1, 2, 4, 4\}$, $E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$
Picture: labeled points = vertices lines = edges



Example 21.9 (Bridges of Konigsburg)**.** Puzzle: Can we walk from A to A crossing each bridge exactly once?



Can translate image to a graph: $V = \{A, B, C, D\}$,
$E = \{\{A, C\}, \{A, C\}, \{C, D\}, \{A, D\}, \{A, B\}, \{A, B\}, \{B, D\}\}$
Euler: This is impossible

Proof. Assume for contradiction that such a walk is possible. Consider vertex D. Assume the walker enters and exits D exactly $k \geq 1$ times. Observe that every time D is entered/exited, 2 edges incident are crossed. D is incident to 3 edges so if all edges are crossed in the walk $3 = 2k$, which is impossible. □

Terminology:

- If $e = \{a, b\} \in E$ then a is adjacent to b, e is incident to a and b, and a and b are endpoints of e.
- If $G = (V, E)$ has no repeated edges it is called a simple graph.
- If G has repeated edges it is called a multigraph.

22 11/18/21

22.1 Terminology

Definition 22.1. A path of length n in G is a sequence of edges $e_1, e_2, \ldots, e_n$ such that there exists vertices $x_0, x_1, \ldots, x_n \in V$ such that $e_i = \{x_{i-1}, x_i\}$ for all $i = 1, 2, \ldots, n$. Equivalently, sequence of pairs of vertices $\{x_0, x_1\}, \{x_1, x_2\}, \ldots, \{x_{n-1}, x_n\}$. A path is simple if no edge is repeated. A path is a circuit if $x_0 = x_n$

Definition 22.2. A circuit C is Eulerian if every edge is traversed once.

Definition 22.3. A graph $G = (V, E)$ is connected if for every pair of distinct vertices $x, y \in V$, there is a path from x to y in G.

Example 22.4. Connected Graphs:

Theorem 22.5. If G is a connected graph and G has an Eulerian circuit, then $\deg(v)$ is even for every $v \in V$.

Proof. Assume G is connected. Let $C = \{x_0, x_1\}, \{x_1, x_2\}, \ldots, \{x_{n-1}, x_n\}$ be an Eulerian circuit of G. If $|V| = 1$, we are done. Otherwise, let v be any vertex other than x_0. Assume C visits v exactly $k \geq 1$ times. In each visit, C uses a pair of edges incident to v. Because C is Eulerian, these k pairs of edges are disjoint and every edge incident to v is in a pair. Thus, the edges incident to V can be partitioned into k pairs so $\deg(v)$=$2k$, as desired.
For the first vertex x_0, repeat the same argument for all edges incident to x_0 other than e_1 and e_n. Thus, you can partition all other edges incident to x_0 into pairs. Adding back e_1, e_n you can partition all edges incident to x_0 into pairs. □

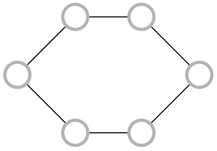
Lemma 22.6 (Handshaking Lemma)**.** For any graph $G = (V, E)$, $\sum_{v \in V} \deg(v) = 2|E|$.

Proof. Let $A = \{(e, v) : e \text{ is incident with } v\}$. We will count A into two ways:
Method 1: Choose $e \in E$ then choose $v \in V$ that is incident with e. $2|E|$ ways.
Method 2: Choose $v \in V$ then choose $e \in E$ incident with v. By sum rule, $\sum_{v \in V} \deg(v)$ total ways.
Thus, $\sum_{v \in V} \deg(v) = 2|E|$. □

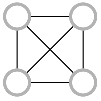
Corollary 22.7. In a graph, the number of vertices with ood degree is even.

22.2 Examples of Graphs

Example 22.8 (Cycle Graph)**.** $V = \{1, \ldots, n\}$,
$E = \{\{x, y\} : x - y \equiv 1 (\text{mod } n)\}$ $n = 6$:



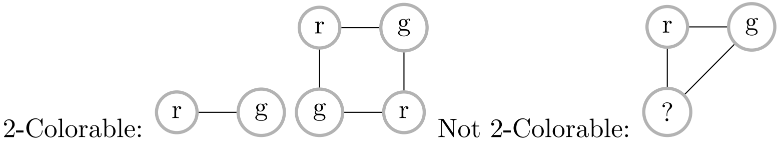
Example 22.9 (Complete Graph)**.** $V = \{1, \ldots, n\}$, $E = \{S \subseteq V : |S| = 2\}$ $n = 4$:



22.3 2-Colorings

Definition 22.10. $G = (V, E)$ is 2-colorable if there is a function $f : V \to \{$red, green$\}$ such that every edge $\{x, y\} \in E$ satisfies $f(x) \neq f(y)$.

Example 22.11. Consider the following example of 2-colorable and not 2-colorable graphs:



Remark 22.12. A graph with n vertices has 2^n colorings.

Theorem 22.13. A connected graph G is 2-colorable if and only if it does not contain a circuit if odd length.

Proof. $\rightarrow$) We will show the contrapositive. Assume G has a circuit $C = \{x_1, x_2\} \ldots, \{x_n, x_1\}$ where n is odd. Suppose $f : V \to \{\text{red}, \text{green}\}$ is a two-coloring of G. Assume WLOG, $f(x_1)$ =red. Observe that each edge must be incident with two different colors so $f(x_2)$ =green, $f(x_3)$ =red, $\ldots$, $f(x_i) = \begin{cases} \text{greem if } i \text{ even} \\ \text{red if } i \text{ odd} \end{cases}$. Thus $f(x_n) = f(x_1)$ =red so f is not 2-colorable.

$\leftarrow$) Assume G is connected and has no odd circuit. We will consider a coloring of $G, f : V \to \{\text{r}, \text{g}\}$. Let $v \in V$ be an arbitrary vertex. Let $f(v)$ =red. For every $y \in V$, define dist(v, y)= length of shortest path from v to y in G, dist: $V \times V \to \mathbb{Z}_+$. Define $f(x) = \begin{cases} \text{r if dist}(v, x) \text{ is even} \\ \text{g if dist}(v, x) \text{ is odd} \end{cases}$.

Claim: f is a valid 2-coloring

Proof: Assume for contradiction $f(a) = f(b)$ for some $\{a, b\} \in E$. Let $P(a)$ be the shortest path from v to a and let $P(b)$ be the shortest path from v to b. Let $C = P(a), \{a, b\}, P(b)$. C is a circuit of length dist(v, a) + dist$(v, b) + 1$. Notice dist(v, a) + dist(v, b) is even since the distances are both even or both odd since $f(a) = f(b)$ so C is an odd circuit, which contradicts our assumption. □

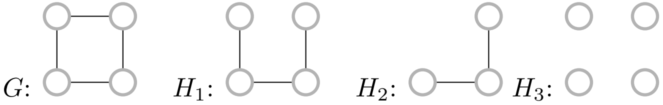
Remark 22.14. We could have used any path from x to y to define $f(y)$ but we would have to prove they are either all even or all odd.

23 11/23/2021

23.1 Subgraphs

Definition 23.1. A graph $H = (W, F)$ is a subgraph of $G = (V, E)$ if $W \subseteq V$ and $F \subseteq E$.

Example 23.2. Consider the following graph G and its subgraphs:



Common ways to create subgraphs:

1. Delete a vertex and all edges incident to it. If $x \in V, H = (V - \{x\}, \{e \in E : x \notin E\})$. (eg. H_2)
2. Delete an edge. If $e \in E, H = (V, \{E\} - \{x\})$. (eg. H_1, H_3)

- If $W = V$, then H is called a spanning subgraph. (eg. H_1, H_3)
- Q) If G has m edges, how many spanning subgraphs does G have?
  A) 2^m, corresponding to $\mathcal{P}(E)$.

23.2 Trees

Definition 23.3. A cycle is a simple circuit. A graph is acyclic if it does not have a cycle as a subgraph.

Definition 23.4. A tree is a connected cyclic graph.

Theorem 23.5. A graph G is a tree if and only if every pair of distinct vertices in G is connected by a unique simple path.

Proof. $\rightarrow$)We show the contrapositive. Assume x, y are vertices in G such that x and y are not connected by a unique simple graph.
Case 1: They are not connected by a a simple path. Then G is not connected so it is not a tree.
Case 2: There are two distinct simple paths $\pi_1 : x = V_0, V_1, V_2, \dots, V_n = y, \pi_2 : x = W_0, W_1, \dots, W_l = y$. Let s be the first index such that $V_t \neq W_j$ for some j. Now $\pi_1' = V_s, \dots, V_t$ and $\pi_2' = W_s, \dots, W_j$, and π_1',π_2' do not have any common vertices except at the endpoints. Now $V_s, \dots, V_t = W_s, W_{s-1}, \dots, W_s$ is a simple cycle, so G is not a tree, as desired.
$\leftarrow$)We show the contrapositive. Assume G is not a graph.
Case 1: G is not connected. Then there is some pair x, y of vertices not connected by a path in G.
Case 2: Assume G has a cycle C. Let $\{x, y\}$ be any edge in C. There are two distinct simple paths between x and y: x, y and $C - \{x, y\}$ □

Definition 23.6. A spanning tree of a graph G is a spanning subgraph which is a tree.

Theorem 23.7. A graph G is connected if and only if it contains a spanning tree.

Proof. $\leftarrow$) Assume T is a spanning tree of G. Let x, y be distinct in G. Since T is connected, there is a path π from x to y in T. So π is also a path in G since T is a subgraph of G. Thus, G is connected.
$\rightarrow$)We will proceed by induction on the number of edges.
Base Case: $P(1)$ is true since there is only 1 connected graph with 1 edge.
Inductive Step: Assume $P(k)$. Let G be a connected graph of with $k+1$ edges. If G is acylclic, we are done since G is its own spanning tree. Otherwise, let C be a cycle in G. Choose an arbitrary vertex $\{x, y\}$ in C. Let $G' = G - \{x, y\}$.

For every pair of distinct vertices a, b in G', there is a path from a to b in G' obtained by taking a path from a to b in G and replacing every occurrence of x, y by $C - \{x, y\}$. Since G' is connected and has k edges, it has a spanning tree T. T is also a spanning tree of G since G and G' have the same vertices. □

Definition 23.8. A degree one vertex of a spanning tree is called a leaf.

Theorem 23.9. Every tree T with $|V| \geq 2$ has at least one leaf.

Proof. Let x_0 be an arbitrary vertex of T. Let x_1 be a vertex incident to x_0. Inductively define a path $x_0, x_1, x_2, \ldots,$ where x_{i+1} is incident to x_i and distinct from $x_1, x_2, \ldots, x_{i-1}$. This process must terminate at some simple path $x_0, x_1, \ldots, x_k$ so either x_k is a leaf or x_k is adjacent to x_i for some $i < k$. The latter case is impossible since $x_i, x_{i+1}, \ldots, x_k, x_i$ would be a cycle in T. □

Theorem 23.10. A tree on n vertices has $n - 1$ edges.

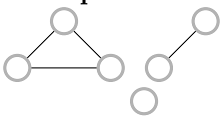
Proof. We will proceed by induction on n.
Base Case: $P(1)$ is true since it is a single vertex.
Inductive Step: Assume $P(k)$ is true. Let T be a tree with $k + 1$ edges. Let x be a leaf of T. Let $T' = T - \{x\}$. T' is acyclic since T is acyclic. If $x, y \in T'$, there is a path from x to y in T which does not visit x. This path lies in T' so T' is connected. By induction, T' has $k - 1$ edges. T has one more edge since x is a leaf of T so T has k edges, as desired. □

24 11/30/21

24.1 Connected Components

Definition 24.1. A connected component of $G = (V, E)$ is a maximally connected subgraph of $H \subseteq G$ (adding any edges or vertices to H would make it disconnected or not a subgraph.)

Example 24.2. Graph with 3 connected components:



Remark 24.3.

- Every graph is a disjoint union of its connected components.
- There are not edges between two distinct connected components.
- G is connected if it has one connected component.

24.2 Euler's Theorem

Theorem 24.4. If G is a connected multigraph with at least 2 vertices and $\deg(v)$ is even for all $v \in G$. Then G has an Eulerian circuit.

Lemma 24.5. If $G = (V, E)$ is a multigraph with $\deg(v) \geq 2$ for all $v \in V$ then G contains a simple circuit.

Proof. We will show the contrapositive. Assume g is acyclic. Let $G_1, , \ldots, G_n$ be the connected components of G. $G_1, \ldots, G_k$ are acyclic so they are trees. If some G_i has ≥ 2 vertices, it must have a leaf l and $\deg(l) = 1$ in G. Otherwise all connected component have only vertex and it has a degree of 0 in G. □

Proof of Theorem. We will proceed by induction on the number of edges.
Base Case: for $m = 2$, there is only one graph that satisfies the conditions and it has an eulerian circuit.
Inductive Step: Assume the statement is true for $2, \ldots, m$. Let G be a connected graph with $|V| \geq 2$ and $|E| = m + 1$. Notice $\deg(v) \geq 2$ since G is connected so by the lemma, G has a circuit simple circuit C. If C is an eulerian circuit we are done. Otherwise, let $H = G - E_C = (V, E - E_C)$ be the subgraph obtained by removing the edges of C. Let $H_1, \ldots, H_k$ be the connected components of H with ≥ 2 vertices. Observe the following:

1. Each H_i is connected with ≥ 2 vertices.
2. Each vertices in H_i, has even degree since C removes an even number of edges incident to each vertex in G and the degree of all vertices in G was assumed to be even.
3. H_i has $\leq m + 1 - |C| \leq m - 1$ edges.

So by the inductive hypothesis, each have an eulerian path C_i.
Claim: $\forall v = 1, \ldots, k$ there is a vertex $s_i \in H_i$ such that $s_i \in H_i \cap C$
Let C' be C with the first occurrence of s_i replaced with C_i for $i = 1, \ldots, k$. Now C' is an eulerian circuit if G since it is a circuit with all edges of $G = H \cup H_1 \cup \ldots \cup H_k$ exactly once. □

24.3 k-coloring

Definition 24.6. A $k-$coloring of $G = (V, E)$ is a function $f : V \to \{1, \ldots, k\}$ such that $\forall x, y \in V(\{x, y\} \in E \to f(x) \neq f(y))$. The minimum such k such that G is k colorable is called its chromatic number.

Example 24.7. For K_n, the complete graph on n vertices, $X(K_n) = n$.
For any tree T, it is acylic so it contains no odd cycles so $X(T) = 2$.

25 12/2/2021

25.1 k-coloring

Theorem 25.1. If G is a graph with maximum degree D then $X(G) \leq D+1$

Remark 25.2. $X(G)$ not always $D+1$

Remark 25.3. This is sharp for the complete graph $X(K_D) = D$

Proof of Theorem. We will proceed by induction on the number of vertices.
Base Case: $P(1)$ is a single node with degree 0 and it is 1 colorable.
Inductive Step: Let G be a graph on $k+1$ vertices with maximum degree D. Let x_0 be an arbitrary vertex of G. Let $x_1, \ldots, x_m$ be its neighbors. Let $G' = G - \{x_0\}$. G' has k vertices and max $\deg(G') \leq$ max $\deg(G) = D$. By the inductive hypothesis, there is a coloring $f' : V \to \{1, \ldots, k\}$ with $k = D+1$. Extend f' to a function $f : V \to \{1, \ldots, k\}$ by $f(y) = \begin{cases} f'(y) \text{ if } y \neq x_0 \\ \text{first } c \text{ in } \{1, \ldots, l\} - \{f'(x_1), \ldots, f'(x_m)\} \end{cases}$. This set is nonempty because $m \leq k$. f is a valid coloring of $G' \cup \{x_0, x_1\} \cup \ldots \cup \{x_0, x_m\}$ so it is a valid coloring of G. □

25.2 Planar Graphs

Definition 25.4. A graph G is planar if it can be in the plane with vertices corresponding to points and edges corresponding to curves such that no two curves cross.

Example 25.5. Every map is a planar graph

Theorem 25.6. (60's) Every planar graph is 4-colorable.

Proof. Proof by induction with 1936 base cases- done by computer. □

Remark 25.7. 5-color theorem is much easier.