Types of Recurrence:

Linear Homogenous: $T(n) = T(n-1) + T(n-2)$ →

Linear Non-Homogenous: $T(n) = 2T(n-1) + 1$

Divide & Conquer: $T(n) = 2T(n/2) + n$

1. Find characteristic eqn. (replace $T(n)$ w x^n)
2. Find roots of characteristic (r_1, r_2)
3. $T(n) = a_1 r_1^n + a_2 r_2^n$
4. Solve for a_1, a_2 using init. conditions

$T(n) = aT(n/b) + cn^d$ (break into a smaller problems, each of size n/b with cost cn^d to put together)	$O(n^d)$ if $a/b^d < 1$; $O(n^d \log n)$ if $a/b^d = 1$; $O(n^{\log_b a})$ if $a/b^d > 1$

Bernoulli Trial:

Experiment w/ exactly 2 outcomes - success, failure

$p(\text{success}) = p$, $p(\text{failure}) = q = 1-p$

Binomial Experiment: Repeat Bernoulli Trial n times, each trial has same p, q and all trials independent.

E_k : k successes occur. $p(E_k) = \binom{n}{k} p^k (1-p)^{n-k}$ (Binomial R.V. is # of successes)

Geometric R.V.: Repeat Bernoulli trial until success occurs

E_k : k trials needed; $p(E_k) = (1-p)^{k-1} p$

R.V.: Function from sample space to real numbers (eg: # of successes in any given outcome)

Stars + Bars: $\binom{\#\text{stars} + \#\text{bars}}{\#\text{bars}}$; # bars = # divisions - 1

bijection to bit string w/ 0s (stars), 1s (bars)

Counting / Probability:

- Experiment: Procedure that yields an outcome.
- Sample Space: Set of all possible outcomes $\boxed{S}$
- Event: Subset of sample space (set of outcomes) $\boxed{E}$
- PIE applies: $p(E_1 \cup E_2) = p(E_1) + p(E_2) - p(E_1 \cap E_2)$
- $p(E|F) = \frac{p(E \cap F)}{p(F)} = \frac{p(F|E)\,p(E)}{p(F)}$ BAYES

$p(E|F) = \frac{p(F|E)\,p(E)}{p(F|E)\,p(E) + p(F|\bar{E})\,p(\bar{E})}$

- $p(E) = p(E \cap F) + p(E \cap \bar{F})$

$p(E) = p(E|F)\,p(F) + p(E|\bar{F})\,p(\bar{F})$

- $p(E|F) + p(\bar{E}|F) = 1$

Independence:

- E, F independent iff $p(E \cap F) = p(E)\,p(F)$ iff $p(E|F) = p(E)$

Asymptotic Growth / Bounds

- f is $O(g)$ ⇒ f grows no faster than g
- $\exists k, \exists C$ s.t. $\forall n > k$, $f(n) \le Cg(n)$
- Formally, $O(g)$ is SET of all $f \le g$
- $\log n < n < n\log n < n^2 < 2^n < n!$
- Proving Big-O: Find witnesses C, k
- Disproving Big-O: Proof by Contradiction: Assume that $\forall n > k$, $f(n) \le Cg(n)$. Find an n big enough that makes this false
- $\Omega(g) \Rightarrow f(n) \ge Cg(n)\ \forall n > k$
- $\Theta(g) \Rightarrow C_1 g(n) \le f(n) \le C_2 g(n)$
- If $f_1 \in O(g_1)$, $f_2 \in O(g_2)$;

$(f_1 + f_2)(n) \in O(\max\{g_1, g_2\})$

$(f_1 \cdot f_2)(n) \in O(g_1(n) \cdot g_2(n))$

- If $f(n) \in O(g)$, $af(n) \in O(g)$

Proving NOT Big-O: $f(x) = \log(x) \cdot \log(x)$ NOT $O(\log x)$

Assume $f(x)$ is $O(\log x)$; so, $\log(x) \cdot \log(x) \le C\log(x)\ \forall x \ge k$

Restrict $x > \max(10, k)$ to ensure $\log(x) > 0$.

Then, $\log(x) \cdot \log(x) \le C\log(x)$
$\log(x) \le C$
$x \le 2^C$.

So, choosing $x = 2^C + 1$ will violate the inequality. If $2^C + 1 < k$, Simply choose $x = k+1$.

Thus, $f(x)$ is not $O(g(x))$ because $x = \max(2^C + 1, k+1)$ will always violate the inequality, proving our assumption false.

Things to Remember:

- Distinguishable objects in indistinguishable boxes is WACK; use CAREFUL case work and remember to divide as necessary.
  - Look @ Highlighted Cases
- Make sure sample space vs. event conditions clear
- Read the fucking problem
- CAREFUL + SLOW
- Try Alt ways of Counting / Smaller Cases + Crosscheck
- Expand out probabilities, double-check
- Careful w/ fractions in Big-O problems

Solve:

$f(n) = 6f(n-1) + 8f(n-2)$
$f(0) = 4$, $f(1) = 10$

Then, 1. $x^n = 6x^{n-1} + 8x^{n-2}$
$x^2 - 6x + 8 = 0$
2. $x = 2, 4$
3. $f(n) = a_1 2^n + a_2 4^n$
4. » $4 = a_1 2^0 + a_2 4^0$
$a_1 + a_2 = 4$
» $10 = a_1 2^1 + a_2 4^1$
$2a_1 + 4a_2 = 10$
» $a_1 = 3$, $a_2 = 1$
5. $f(n) = 3 \cdot 2^n + 4^n$

Permutations: $\frac{N!}{(N-r)!}$

Combinations: $\binom{N}{k} = \frac{N!}{(N-k)!\,k!}$

Stirling's: $N! \approx \sqrt{2\pi N}\left(\frac{N}{e}\right)^N$

Coefficient of k^{th} term of $(ax+by)^n$: $\binom{n}{k} a^{n-k} b^k \,(x^{n-k} y^k)$

Pascal's Identity: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$

Multinomial: $\binom{n}{k_1, k_2, k_3 \ldots} = \frac{n!}{k_1!\,k_2!\,k_3! \ldots}$

Prove $3n^2 + 8n + 5001$ is $O(n^2)$:

1. Consider $k = 5001$, $C = 4$
$f(n) = 3n^2 + 8n + 5001$
$\le 3n^2 + n^2$, $n \ge 5001$
$= 4n^2$

2. Consider $k = 1$, $C = 5012$
$f(n) = 3n^2 + 8n + 5001$
$\le 3n^2 + 8n^2 + 5001n^2$
$= 5012n^2$

E.V.:

Suppose you are purchasing a meal & you recieve one of 10 toys @ random. How long before collect all 10 toys?

Let X_k be # of purchases it takes to go from k to k+1 toys

$E(P) = E(X_0 + X_1 + \ldots + X_9) = E(X_0) + E(X_1) + \ldots + E(X_9)$

Each X_k is a geometric R.V. w/ $p(\text{success}) = 10-k/10$.

Thus, $E(X_n) = \frac{10}{10-k}$, and $E(P) = \frac{10}{10} + \frac{10}{9} + \ldots + \frac{10}{2} + \frac{10}{1}$

So, $E(P) = 10\left(1 + \frac{1}{2} + \ldots + \frac{1}{10}\right) \approx 30$

E.V.:

Suppose n couples in a room (2n people). Out of 2n people, m are chosen. What is expected # of couples chosen (both picked)?

$E(C) = E(C_1 + C_2 + C_3 + \ldots + C_n) = E(C_1) + E(C_2) + \ldots + E(C_n)$
$= n\,E(C_k)$

$p(C_k) = \frac{m}{2n} \cdot \frac{m-1}{2n-1} = E(C_k)$

$= \frac{n \cdot m(m-1)}{2n(2n-1)} = \boxed{\frac{m^2 - m}{4n-2}}$

Find a Recurrence Relation

- Can eat Ranch, Caesar, or Balsomic
- No Balsamic 2x in a row
- Caesar only follows Ranch

Case 1: Ranch on n'th day → $f(n-1)$

C2: Caesar on n^{th} day → $f(n-2)$

C3: Balsamic on n^{th} day ⇒ not Balsamic on $(n-1)^{th}$ day

C3.1: Caesar on n-1 → Ranch on n-2: $f(n-3)$

C3.2: Ranch on $(n-1)^{th}$ → Anything on (n-2): $f(n-2)$

So, $f(n) = f(n-1) + 2f(n-2) + f(n-3)$

IC: $f(0) = 1$, $f(1) = 2$, $f(2) = 4$

How many ways to put 6 employees in 3 identical offices (can have empty offices)? INDISTINGUISHABLE BOXES

1. 6-0-0: $\binom{6}{6} = 1$
2. 5-1-0: $\binom{6}{5} = 6$
3. 4-2-0: $\binom{6}{4} = 15$
4. 4-1-1: $\binom{6}{4} = 15$
5. 3-3-0: $\binom{6}{3}\frac{1}{2!} = 10$
6. 3-2-1: $\binom{6}{3}\binom{3}{2} = 60$
7. 2-2-2: $\binom{6}{2}\binom{4}{2}\frac{1}{3!} = 15$

TOTAL: 122

Proving Big-O: Prove $\log(5n^3)$ is $O(\log n)$

$\log(5n^3) \le C\log(n)$ $(\forall n \ge k)$

$3\log(n) + \log(5) \le C\log(n)$

$C = 3 + \log(5)/\log(n)$

Consider $C = 4$, $k = 5$

$\log(5n^3) \le 4\log(n)$, $n \ge 5$

$3\log(n) + \log(5) \le 3\log(n) + \log(n)$

$\log(5) \le \log(n)$

This is always true as $n \ge 5$; so, we have proven $\log(5n^3) \in O(\log n)$

Prove $f(n) = \frac{2n^5 - n^3 + 2}{3n^2 + 4n - 1}$ is $O(n^3)$

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

$\le \frac{2n^5 + 2}{3n^2 + 4n - 1}$

$\le \frac{2n^5 + 2}{3n^2}$, $\forall n \ge 1$ (as $4n - 1 > 0$)

$\le \frac{2n^5 + 2n^5}{3n^2}$

$\le \frac{4}{3}n^3 \le 2n^3$

$\boxed{C = 2;\ k = 1}$

- Bottom-Up Recursion instead of Top-Down
  » First day instead of n^{th} day

Buy Toilet Paper, Chicken, Egg, Bread everyday (one item)
- No TP 2 days in a row
- If Chicken, must buy eggs day after

Consider what he does on Day 1 (for n-day sequence)

Case 1: TP on day 1

1.1: C on day 2, E on day 3. No restrictions on day 4

1	2	3	4	–	n-1	n

(1–3 FIXED, n-3)

$a(n-3)$

1.2: E on day 2, Anything on day 3: $a(n-2)$

1.3: B on day 2, Anything on day 3: $a(n-2)$

Case 2: C on day 1. E on day 2, Anything on day 3: $a(n-2)$

Case 3: E on day 1. Anything on day 2: $a(n-1)$

Case 4: B on day 1. Anything on day 2: $a(n-1)$

TOTAL: $a(n) = 2a(n-1) + 3a(n-2) + a(n-3)$

$a(0) = 1$, $a(1) = 4$, $a(2) = 12$

Expected Value

Average of R.V. weighted by probability

$= \sum_{s \in S} p(s) \cdot X(s)$ — Average over all outcomes in sample space

$= \sum_r p(X = r) \cdot r$ — Average over possible values of R.V.

For geometric R.V., $E(X) = 1/p$

For binomial R.V., $E(X) = np$

Linearity of Expectation:

$E(X_1 + X_2) = E(X_1) + E(X_2)$

$E(aX + b) = a \cdot E(X) + b$

A country uses bronze coins with denominations of 1 peso, 2 pesos, and 5 pesos, silver coins of denominations of 2 pesos and 5 pesos, and uses gold coins with denominations of 5 pesos, and 10 pesos. Anton buys a candy bar from a vending machine, using the coins of this country, by putting one coin at a time into the vending machine.

Find a recurrence relation for the number of ways Anton can pay for a candy bar that costs n pesos, if the order in which he inserts the coins matters as does the type of coin (e.g., using a 2-peso bronze coin is different than using a 2-peso silver coin).

Solution: To find a recurrence for the total number of ways to pay for a candy bar that costs n pesos, it is necessary to consider the denomination, d, of the final coin used to pay, the number of coins of that denomination, and the number of ways to pay the first $n-d$ pesos.

Case 1: Final coin denomination is 1 peso.
There is one coin with denomination 1 and there are $f(n-1)$ ways to pay $n-1$ pesos.
Therefore, this case accounts for $1 \cdot f(n-1) = f(n-1)$ ways to pay n pesos.

Case 2: Final coin denomination is 2 pesos.
There are 2 coins with denomination 2 and there are $f(n-2)$ ways to pay $n-2$ pesos.
Therefore, this case accounts for $2f(n-2)$ ways to pay n pesos.

Case 3: Final coin denomination is 5 pesos.
There are 3 coins with denomination 5 and there are $f(n-5)$ ways to pay $n-5$ pesos.
Therefore, this case accounts for $3f(n-5)$ ways to pay n pesos.

Case 4: Final coin denomination is 10 pesos.
There is one coin with denomination 10 and there are $f(n-10)$ ways to pay $n-10$ pesos.
Therefore, this case accounts for $f(n-10)$ ways to pay n pesos.

Therefore, the final recurrence relation is $f(n) = f(n-1)+2f(n-2)+3f(n-5)+f(n-10)$.

Set Proof: Prove $A \times (B \cap C) = (A \times B) \cap (A \times C)$

Prove both subsets of each other.

First, lets prove that $A \times (B \cup C) \subseteq (A \times B) \cap (A \times C)$.

Let (x, y) be an arbitrary element of $A \times (B \cup C)$.

Then $x \in A$, $y \in (B \cap C)$ by definition of the Cartesian product.

As $y \in (B \cap C)$, by the definition of intersection, $[(y \in B) \wedge (y \in C)]$.

Thus as $x \in A$ and $y \in B$, $[(x, y) \in (A \times B)]$ by the definition of Cartesian Produ

Likewise, as $x \in A$ and $y \in C$, $[(x, y) \in (A \times C)]$ by the definition of Cartesian Product.

As $[((x,y) \in (A \times B)) \wedge ((x,y) \in (A \times C))]$, by the definition of intersection, $(x, y) \in (A \times B) \cap (A \times C)$. Thus, we have proven that any arbitrary element (x, y) of $A \times (B \cup C)$ is also in $((A \times B) \cap (A \times C))$.

Thus, $A \times (B \cup C) \subseteq (A \times B) \cap (A \times C)$.

Second, lets prove that $(A \times B) \cap (A \times C) \subseteq A \times (B \cup C)$.

Let (x, y) be an arbitrary element of $(A \times B) \cap (A \times C)$. By the definiton of intersection, $(x, y) \in (A \times B) \wedge (x, y) \in (A \times C)$.

By the definition of the Cartesian Product, we can conclude that $x \in A$ and $y \in B$ and $y \in C$. As $y \in B$ and $y \in C$, by the definition of intersection, $y \in B \cap C)$. Thus, as $x \in A$ and $y \in (B \cap C)$, by definition of the Cartesian product, $(x, y) \in [A \times (B \cap C)]$.

Thus we have proven any arbitrary element of $(A \times B) \cap (A \times C)$ is also in $A \times (B \cap C)$.

Thus, $[(A \times B) \cap (A \times C)] \subseteq [A \times (B \cap C)]$.

As both sets are subsets of each other, they must be equal.

ONTO/ONE-TO-ONE

a) $f : \mathbb{R} \to \mathbb{Z}$ with $f(x) = \lfloor x \rfloor$

- First, lets prove that $f(x)$ is $\boxed{\text{NOT one-to-one}}$. For a function f to be one one w/ domain $\mathbb{R}$, $\forall a, b \in \mathbb{R}\ (f(a) = f(b) \to a = b\}$. Negating this state
  $[\neg \forall a, b \in \mathbb{R}\ ((f(a) = f(b)) \to (a = b))] \equiv [\exists a, b \in \mathbb{R}\ ((f(a) = f(b)) \wedge (a \neq b))]$
  Consider $a = 0.1$ and $b = 0.2$, noting that $a, b \in \mathbb{R}$ (domain).
  Then $f(a) = \lfloor a \rfloor = \lfloor 0.1 \rfloor = 0$, and $f(b) = \lfloor b \rfloor = \lfloor 0.2 \rfloor = 0$.
  Thus $f(a) = f(b)$, but $a \neq b$; therefore f is not one-to-one.
- Now, let's prove that $\boxed{f \text{ is onto.}}$ For a function f to be onto w/ domain $\mathbb{R}$ codomain $\mathbb{Z}$, $[\forall b \in \mathbb{Z}, \exists a \in \mathbb{R}\ (f(a) = b)]$. Let b be an arbitrary codom element. Define $a = b + 0.1$, noting that $a \in \mathbb{R}$ and $b < a < b+1$.
  Then $f(a) = \lfloor b + 0.1 \rfloor = b$ (as $b < a < b+1$). Thus, as $f(a) = b$ fo an arbitrary codomain element b, f is onto.

b) $f : \mathbb{Z} \to \mathbb{Z}$ with $f(x) = 5 - 3x$.

- First, let's prove that $f(x)$ is one-to-one. For a function f to be one-to-one w/ $\forall a, b \in \mathbb{Z}, [(f(a) = f(b)) \to (a = b)]$. For arbitrary a, b, assume $f(a) = f(b)$

$$f(a) = f(b)$$
$$5 - 3a = 5 - 3b$$
$$-3a = -3b$$
$$a = b.$$

Thus, as $f(a) = f(b)$ implies $a = b$ for arbitrary a, b, we conclude that $f(x)$ is one-to-one.

- Second, let's prove that $f(x)$ is not onto. For a function f to be onto w/ domain $\mathbb{Z}$ codomain $\mathbb{Z}$, $[\forall b \in \mathbb{Z}\ \exists a \in \mathbb{Z}\ [f(a) = b]]$.
  Negating this statement, $\neg \forall b \in \mathbb{Z}, \exists a \in \mathbb{Z}\ [f(a) = b] \equiv \exists b \in \mathbb{Z}\ \forall a \in \mathbb{Z}\ [f(a) \neq b]$.
  Consider $b = 0$. Then for $f(x)$ to be onto, $f(a) = 0$ for some a in domain $\mathbb{Z}$

$$f(a) = 0$$
$$5 - 3a = 0$$
$$3a = 5$$
$$a = 5/3.$$

So for $f(a) = b$, $a = 5/3$; but $5/3$ is not in the domain $\mathbb{Z}$.
Thus there is no a-value in the domain such that $f(a) =$
thus $f(x)$ is not onto.

Suppose R_1, R_2 equivalence relations on set S. Then,

a) $R_1 \cup R_2$ is NOT nec. an equivalence relation (not nec. transitive)

b) $R_1 \cap R_2$ IS an equivalence relation

c) $R_1 \oplus R_2$ is NOT an equivalence relation (esp. not reflexive)

- K_n is bipartite only for $n = 2$ (not enough vertices w/ $n = 1$)
- C_n is defined for $n \geq 3$. C_n is bipartite iff n is even - otherwise not
- W_n is bipartite only for $n = 1$ ($W_1 = K_2$)
- Q_n is bipartite $\forall n \geq 1$ — division on even # of ones vs. odd # of ones (when vertices represented as bitstrings)
  Each vertex connects to all vertices w/ exactly one bit flipped

- Prove $2^n > n^2$ if $n > 5$.

Let $P(n)$: $2^n > n^2$

BASE CASE: LHS: $2^n = 2^5 = 32$
RHS: $n^2 = 5^2 = 25$
As LHS > RHS, $P(5)$ holds true

IS: Assume $P(k)$ is true: $2^k > k^2$.
We want to show $P(k+1)$ is true: $2^{k+1} > (k+1)^2$

$$
\begin{aligned}
2^{k+1} &= 2(2^k) \\
&> 2k^2 && \text{(By the IH)} \\
&= k^2 + k^2 \\
&> k^2 + 4k && \text{(As } k > 4) \\
&> k^2 + 2k + 1 && \text{(As } 2k > 1 \text{ as } k > 4) \\
&= (k+1)^2
\end{aligned}
$$

So, $P(k+1)$ holds true.

Thus, as $P(k) \to P(k+1)$ and $P(5)$ holds true, we have proved $P(n)$ is true for $n > 4$ by mathematical induction.

$f : \mathbb{Z} \to \mathbb{Z}^+$

a) one-to-one, not onto: $f(x) = 3x + 1$ for $x \geq 0$; $f(x) = -3x + 2$ for $x <$

b) onto, not one-to-one: $f(x) = |x| + 1$

c) bijective: $f(x) = -2x$ for $x < 0$

d) neither: $f(x) = x^2 + 1$

$f : \mathbb{N} \to \mathbb{N}$

a) One-to-one but not onto: $f(x) = x + 1$

b) Onto but not one-to-one: $f(x) = \begin{cases} 0 & \text{if } x \text{ is odd} \\ n/2 & \text{if } x \text{ is even} \end{cases}$

RELATION PROOF: Prove that if relation R over non-empty A is symmetric, transitive, and irreflexive, then R is empty.

Seeking a contradiction, suppose R is non-empty. So R has some element (a, b), $a, b \in A$. Since R is symmetric, $(b, a) \in R$. Since R is transitive, and $aRb \wedge bRa$, aRa. However, R is also irreflexive, so $\forall a \in A$, $a \not R a$. So, we have a contradiction as both aRa and $a \not R a$ cannot be true.
So, we disprove our initial assumption that R is non-empty.

① PROVE THAT $\sqrt{2}$ IS IRRATIONAL

Seeking contradiction, $\sqrt{2} = a/b$, $\gcd(a, b) = 1$

$\frac{a^2}{b^2} = 2 \to a^2 = 2b^2$. Thus a^2 is even.

Prove if a^2 is even then a is even by contrapositive

Then $a = 2k$; $(2k)^2 = 2b^2$; $b^2 = 2k^2$.

Same proof by contrapositive; b is even.

As a, b both even, $\gcd(a, b) \neq 1$ (CONTRADICTION)

Thus, $\sqrt{2}$ is not rational.

$L(x, y)$: x eats lunch w/ y
$C(x, y)$: x has class w/ y
$R(x, y)$: x is roommates w/ y
} UM Students

a) $\forall x \forall y\ [(C(x,y) \wedge R(x,y)) \to L(x,y)]$
Every pair of UM students that have a class w/ each other and are roommates, eat lunch together.

b) $\exists x \forall y\ [((x \neq y) \wedge C(x,y)) \to \neg L(x,y)]$
There is at least one UM student who does not have lunch w/ any of their classmates.

c) $\forall x \exists y\ [((x \neq y) \wedge C(x,y) \vee R(x,y)) \wedge \neg L(x,y)]$
For every UM student, there exists someone who they are either roommates or classmates with and they don't eat lunch with.

$I(x)$: x has internet connection
(x: students in class)

"Everyone except one student has an internet connection."

$\exists x \neg I(x) \wedge \forall y\ (x \neq y \to I(y))$

Set Identities:

- $A \cap U = A$, $A \cup \emptyset = A$ — Identity Laws
- $A \cup U = U$, $A \cap \emptyset = \emptyset$ — Domination Laws
- $A \cup A = A$, $A \cap A = A$ — Idempotent Laws
- $\overline{(\overline{A})} = A$ — Complementation Law
- $A \cup B = B \cup A$, $A \cap B = B \cap A$ — Commutative Laws
- $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$ — Associative Law
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ — Distributive Law
- $\overline{A \cap B} = \bar{A} \cup \bar{B}$, $\overline{A \cup B} = \bar{A} \cap \bar{B}$ — DeMorgan's Laws
- $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$ — Absorption Laws
- $A \cup \bar{A} = U$, $A \cap \bar{A} = \emptyset$ — Complement Laws
- $A - B = A \cap \bar{B}$ — Set Minus

To prove $A = B$:
Show $A \subseteq B$, $B \subseteq A$.
Pick arbitrary element in A, show in B.

Set: Unordered, no duplicates

Defined by MEMBERSHIP ($\in$)
$S = \{x \mid x \equiv 1 \pmod 2 \ \wedge \ \text{Prime}(x)\}$

$\mathbb{N}$: Naturals, $0 \to \infty$ — $\cup$: Union
$\mathbb{Z}$: Integers, $-\infty \to \infty$ — $\cap$: Intersection
$\mathbb{Q}$: Rationals — $\bar{S}$: Complement
$\mathbb{R}$: Reals — $S - T$: Minus

$S \subseteq T$: S subset of T — $S \oplus T$: $S \cup T - S \cap T$ (XOR / Symmetric Difference)
$S \subset T$: $S \subseteq T \wedge S \neq T$
$S \cap T = \emptyset$: S, T disjoint

Power Set: Set of all subsets of S (Size 2^n)

Cardinality: # of elements (recall no repeats)

PIE: $|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$
[ALTERNATE SIGNS]

Cartesian Product: $A \times B$ (ORDERED)
Set of all tuples (a, b); $a \in A$, $b \in B$.
$|A| = x$, $|B| = y \to |A \times B| = xy$

One-to-One Proof: $f(x): \mathbb{R} \to \mathbb{R}$
$f(x) = 2x + 4$.

One-to-One: $\forall a, b \in A\ [f(a) = f(b) \to a = b]$.
Let a, b be arbitrary domain elements such that $f(a) = f(b)$. Then, $2a + 4 = 2b + 4$, $2a = 2b$, $a = b$.
So, $(f(b) = f(a)) \to (b = a)$. As a, b arbitrary, $\forall a, b \in A\ [f(b) = f(a) \to b = a]$. So, $f(x)$ is one-to-one by definition.

Proof of NOT One-to-One:
$\neg(\forall a, b \in A\ [f(b) = f(a) \to b = a])$
$\equiv \exists a, b \in A\ [(f(b) = f(a)) \wedge (b \neq a)]$
So, find 2 inputs $(a, b \in A)$ such that $f(a) = f(b)$ but $a \neq b$.

Proof of NOT Onto:
$\neg(\forall b \in B\ \exists a \in A\ [f(a) = b])$
$\exists b \in B\ \neg \exists a \in A\ f(a) = b$
$\exists b \in B\ \forall a \in A,\ f(a) \neq b$

So, find a $b \in B$ such that no a exists for $f(a) = b$.

Onto Proof: $f: \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 4$.

Onto: $\forall b \in B, \exists a \in A\ [f(a) = b]$
Let b be an arbitrary codomain element.
Define $a = \frac{b-4}{2}$. Then, $f(a) = 2a + 4 = 2\left(\frac{b-4}{2}\right) + 4 = b - 4 + 4 = b$.
Note a is Domain element.
[Do side work to arrive @ this defn. of a]
So, $\exists a \in \mathbb{R}\ [f(a) = b]$. As b was arbitrary, $\forall b \in B, \exists a \in A\ [f(a) = b]$, so f is onto.

$h = g \circ f = g(f(x))$; if $f: A \to B$ and $g: B \to C$,
* Output of f must be subset of domain of g | $g \circ f: A \to C$
$(f_1 + f_2)(x) = f_1(x) + f_2(x)$ — $f_1, f_2: S \to \mathbb{R}$
$(f_1 f_2)(x) = f_1(x)\, f_2(x)$,

If $f: A \to B$ one-to-one, $|A| \leq |B|$
If $f: A \to B$ onto, $|A| \geq |B|$
If $f: A \to B$ bijection, $|A| = |B|$

Assume for ∞ sets; prove for finite

Schroeder-Bernstein Thm:
$(|A| \leq |B|) \wedge (|B| \leq |A|) \to |A| = |B|$.

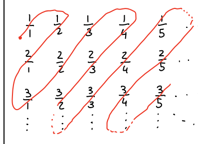
So, to demonstrate $|A| = |B|$:
Prove: $[f_1: A \to B$ is 1-1 OR $g_1: B \to A$ is onto$]$ $|A| \leq |B|$
AND
$[f_1: A \to B$ is onto OR $g_1: B \to A$ is 1-1$]$ $|B| \leq |A|$

DOMAIN, CODOMAIN MATTER!!

∞ Set Cardinality
Set S is countable iff $|S| \leq |\mathbb{Z}^+|$
- one-to-one $f: S \to \mathbb{Z}^+$
- onto $f: \mathbb{Z}^+ \to S$
- all finite sets countable

} can list elements in some order

$\mathbb{Z}, \mathbb{N}, \mathbb{Z}^+ \times \mathbb{Z}^+, \mathbb{Q}$ — cardinality $= \aleph_0$ (aleph null)



(onto, not one-to-one)
Similar for $\mathbb{Z}^+ \times \mathbb{Z}^+$

$f: \mathbb{Z} \to \mathbb{Z}^+$
$f(x) = \begin{cases} 2x + 1 & x \geq 0 \\ -2x & x < 0 \end{cases}$

- Diagonalization Proof ($\mathbb{R}$ uncountable)
$[0, 1] \subseteq \mathbb{R}$, so $|[0, 1]| \leq \mathbb{R}$.
For contradiction, assume $[0, 1]$ countable. Then $\exists$ onto $f: \mathbb{Z}^+ \to [0, 1]$.
List $[0, 1]$ out in a table in arbitrary order.

$z \in \mathbb{Z}^+$	$x \in [0,1]$	D_1	D_2	D_3	D_4
1	0	0	0	0	...
2	0.12	1	2	0	...
3	½	5	0	0	...
4	$\frac{1}{\pi}$	3	1	8	...

Then, shift diagonal numbers up 1 ($9 \to 0$).
So, every row disagrees w/ diagonal on one digit; but diagonal num $\in \mathbb{R}$.

$\mathbb{R}$, Power set of ∞ S, Set f of $\mathbb{N} \to \{0, 1\}$ all uncountable ($\aleph_1$)

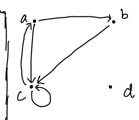
Functions: Map from Set D to Set C
- EVERY elem in D has ONE elem in C
- Range: Mapped part of Codomain
- ONTO (SURJECTIVE): Every elem in C mapped to
$\forall b \in B, \exists a \in A\ [f(a) = b]$; $f: A \to B$
- ONE-TO-ONE (INJECTIVE):
$\forall a, b \in A\ [f(a) = f(b) \to a = b]$
Can have unmapped elements in CoDomain
- Bijective: BOTH (One-to-one correspondence) ← IMPORTANT
 - Implies inverse exists

Relations (xRy, $R(x,y)$, x related to y)
Binary relation between D, C: $R \subseteq D \times C$.
R is a SET of tuples (ordered).
Properties on relations on $S \times S$: SET OPS APPLY
- Reflexive: $\forall x,\ xRx$
- Symmetric: $\forall x, y,\ xRy \leftrightarrow yRx$
- Antisymmetric: $\forall x, y,\ (xRy \wedge yRx) \to x = y$
- Transitive: $\forall x, y, z,\ (xRy \wedge yRz) \to xRz$
- Asymmetric: $\forall x, y\ (xRy \to \neg yRx)$
- Irreflexive: $\forall x,\ \neg xRx$

→ Asymmetric = (Antisymmetric ∧ Irreflexive)
> Symmetric ∧ Antisymmetric: Only self-loops
→ Sym ∧ Asym ∧ Antisym : $\emptyset$

xRy representations:

x\y	a	b	c	d
a	0	1	1	0
b	0	0	1	0
c	1	0	1	0
d	0	0	0	0



$R = \{(a, b), (a, c), (b, c), (c, c), (c, a)\}$

- Reflexive: main diagonal all 1s
- Symmetric: Symmetry across main diagonal
- Antisymmetric: No 2 1s across from main diagonal (except diagonal itself)
- Irreflexive: main diagonal all 0s
- Graphs:
 - Reflexive: Self-loop @ each vertex
 - Symmetric: Directed edges in pairs
- Composition: $R \subseteq A \times B$, $S \subseteq B \times C$
$a(S \circ R)c$ iff $\exists b \in B\ (aRb \wedge bRc)$
On bipartite graph, is there path from a to c
- $R^2 = R \circ R$; $R^3 = R \circ R^2 = R \circ R \circ R$, etc.
 - R^n is all nodes you can reach w/ EXACTLY n moves
 - R^* (transitive closure) $= R \cup R^2 \cup R^3 \cup \ldots$ (reachability region)
 - If $R^* \subseteq R$, R is transitive

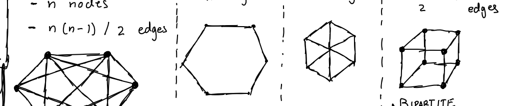
Closure (min relation satisfying prop):
- Reflexive, Transitive, Symmetric
- Iteratively find violation → fix violation
- Can only ADD to relation
- Reflexive: $MAT_R \cup$ Identity Mat
- Symm: $MAT_R \cup MAT_R'$

Graphs:
- $G = (V, E)$
Tuple of set of Vertices & set of edges (tuples)
- Differentiating Graphs
 - Directed Edges?
 - Multiple Edges b/w nodes?
 - Loops?
- NOTE: "ALLOWED TO" have loops and actually having loops diff. Differentiate on ALLOWED behavior.

- In-Degree $= \deg^-(v)$ − incoming
- Out-Degree $= \deg^+(v)$ − outgoing
- $2|E| = \sum_{v \in V} \deg(v)$
- $|E| = \sum_{v \in V} \deg^+(v) = \sum_{v} \deg^-(v)$

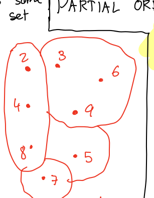
- Simple Graphs: Undirected, no multiple edges, no loops
- $e = \{u, v\}$ in Undirected;
- $e = (u, v)$ in Directed.
- Degree: # of edge ends on a vertex (loops counted 2x)
- Subgraph of $G = (V, E)$: $H = (V', E')$, $V' \subseteq V \wedge E' \subseteq E$
- $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$
Union $G_1 \cup G_2 = (V_1 \cup V_2,\ E_1 \cup E_2)$

Types of Graphs
- K_n (Complete) − all nodes connected
 - n nodes
 - $n(n-1)/2$ edges
- C_n (Cycle)
 - n nodes
 - n edges
- W_n (Wheel)
 - $(n+1)$ nodes
 - $2n$ edges
- Q_n (Hypercube)
 - 2^n nodes
 - $\frac{n 2^n}{2} = n 2^{n-1}$ edges



- Bipartite

Equivalence Relation: − set to some set
- Reflexive, Symmetric, Transitive (iff)
- $x = y$; $p \equiv q$; $\frac{a}{b} = \frac{c}{d}$; etc.
- Leads to EQUIVALENCE CLASSES
- EQ CLASS $[a]_R = \{b \in S : aRb\}$
- eq classes partition graph
 - disjoint classes, form whole graph
- ANY partition of S is equivalence class



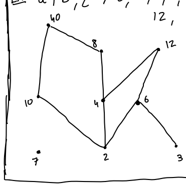
Same largest prime divisor

Partial Orders: Ranks elements (Some could be incomparable)
- Reflexive
- Antisymmetric
- Transitive

- Eg: $a \mid b$ over $\{1, 2, 3, 4, 5, 6\}$ (a divides b)
→ $(\{1, 2, 3, 4\}, \leq)$

- Tuple (Set, operator) − poset
- Total Order iff poset ∧ all elem comparable
- Hasse Diagrams
 - Height indicates order
 - Implied edges (transitive) omitted
 - No self-loops
 - For total order, straight line

Ex: $a \mid b$, $\{2, 3, 4, 6, 7, 8, 12, 40\}$



- Minimal: No elem smaller (Some incomparable)
- Maximal: No elem bigger ("...")
- Minimum: Unique − comparable to AND less than everything else.
- Maximum: Unique − comparable to AND greater than everything else.
- For subset A of S, upper bound for A is $x \in S$ s.t. $\forall a \in A$, $a \leq x$.
 x COULD BE IN A
- Similar for lower bound
 - Not necessarily just 2 elems
- LUB: Least Upper Bound
- GLB: Greatest Lower Bound

- Minimal, Maximal exist if set is finite
- Minimum, Maximum not nec. $\exists$. (doesn't have to be total order for them to exist tho)

Topological Sort
- Convert partial order into total order
- Starting from bottom, output any minimal element in S
- $\prec$: ordering symbol for orders

Strict Poset
- Irreflexive instead of reflexive
($\succ$, not $\geq$)

Bipartite
- If G can have vertices partitioned into disjoint V_1, V_2 such that every edge connects vertex in V_1, vertex in V_2.
(V_1, V_2): Bipartition
- Simple graph bipartite iff it is two-colorable (no adj. vertices have same color).
- 2-colorable iff all cycles have even length

Induction: To prove $P(n)$ true for all $n \in \mathbb{N}$:
- Prove $P(1)$
- Prove $P(n) \to P(n-1)$ $\forall n \in \mathbb{N}$
- ALWAYS WORK IN ONE DIRECTION FROM LHS = RHS
- Induction works when set WELL-ORDERED
- Set S well-ordered iff for all non-empty $A \subseteq S$, A has a LEAST ELEMENT according to some order $\prec$
- For ex, reals⁺ not well-ordered

Strong Induction
- To prove $P(n)$:
- Prove Base Case(s): $P(1), P(2) \ldots$
- Prove Inductive Step: $(P(1) \wedge P(2) \wedge \ldots P(k-1)) \to P(k)$
- Can use ALL previous results

Induction Template:
Inductive Step: Assume $P(k)$: [...] for some $k \geq n_0$.
Want to show $P(k+1)$: [...].
[Show $P(k+1)$ using assumption for $P(k)$. Remember only work from one side]
Base Case: $P(n_0)$: [...]
[Prove $P(n_0)$ holds]
By mathematical induction, $P(n)$ is true for all $n \geq n_0$

Strong Induction Template:
Inductive Step: Assume $P(j)$: [...] true for $n_0 \leq j < k$
Want to show $P(k)$: [...].
[Show $P(k)$ using assumption for $P(j)$, $n_0 \leq j < k$. Remember only work from one side]
Base Case: $P(n_0)$ . . . (and others)
[Prove $P(n_0)$, etc. hold]
By strong induction, $P(n)$ is true for all $n \geq n_0$

Exam Reminders:
- Define $P(k)$ properly
- $[a]$: equivalence class of a
- READ THE QUESTION
- Asymmetric vs. Antisymm, $\in$ vs. $\subseteq$ } CAREFUL
- DEFINE EVERYTHING
- JUSTIFY STEPS when solving onto / one-to-one / induction
- Conclusions important

Logical Equivalence Laws

1. $p \wedge T \equiv p$, $p \vee F \equiv p$ — Identity Laws
2. $p \vee T \equiv T$, $p \wedge F \equiv F$ — Domination Laws
3. $p \vee p \equiv p$, $p \wedge p \equiv p$ — Idempotent Laws
4. $\neg(\neg p) \equiv p$ — Double Negation
5. $p \vee q \equiv q \vee p$, $p \wedge q \equiv q \wedge p$ — Commutative
6. $(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ — Associative
7. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ — Distributive
8. $\neg(p \wedge q) \equiv \neg p \vee \neg q$, $\neg(p \vee q) \equiv \neg p \wedge \neg q$ — DeMorgan's
9. $p \vee (p \wedge q) \equiv p$, $p \wedge (p \vee q) \equiv p$ — Absorption
10. $p \vee \neg p \equiv T$, $p \wedge \neg p \equiv F$ — Negation
11. $\neg \forall x\, P(x) \equiv \exists x\, \neg P(x)$, $\neg \exists x\, P(x) \equiv \forall x\, \neg P(x)$ — De Morgans (Quantifiers)
12. $p \rightarrow q \equiv \neg p \vee q$ — Implication Breakout
13. $p \rightarrow q \equiv \neg q \rightarrow \neg p$ — Contrapositives

Natural Deduction Rules:

5 intro rules

- $\wedge$-intro: $\dfrac{p,\ q}{p \wedge q}$
- $\vee$-intro: $\dfrac{p}{p \vee q}$ / $\dfrac{q}{p \vee q}$
- $\rightarrow$-intro: $\dfrac{\boxed{p \ \vdots\ q}}{p \rightarrow q}$
- $\leftrightarrow$-intro: $\dfrac{\boxed{p \ \vdots\ q}\ \boxed{q \ \vdots\ p}}{p \leftrightarrow q}$
- $\neg$-intro: $\dfrac{\boxed{p \ \vdots\ F}}{\neg p}$

7 elim rules

- $\wedge$-elim: $\dfrac{p \wedge q}{p}$ / $\dfrac{p \wedge q}{q}$
- $\vee$-elim: $\dfrac{\boxed{p \ \vdots\ r}\ \boxed{q \ \vdots\ r}\ \ p \vee q}{r}$
- $\rightarrow$-elim: $\dfrac{p,\ p \rightarrow q}{q}$
- $\leftrightarrow$-elim: $\dfrac{p \leftrightarrow q,\ p}{q}$ / $\dfrac{p \leftrightarrow q,\ q}{p}$
- $\neg$-elim: $\dfrac{p,\ \neg p}{F}$
- $\neg\neg$-elim: $\dfrac{\neg\neg p}{p}$
- F-elim: $\dfrac{F}{p}$

Quantifier Rules

- $\forall$-elim: $\dfrac{\forall P(x)}{P(t)}$
- $\exists$-intro: $\dfrac{P(t)}{\exists x\, P(x)}$
- $\forall$-intro: $\dfrac{\boxed{x_0 \ \vdots\ P(x_0)}}{\forall x\, P(x)}$
- $\exists$-elim: $\dfrac{\exists x\, P(x),\ \boxed{x_0\ \ P(x_0) \ \vdots\ q}}{q}$

Things to Remember:

- Do $\forall$-elim inside correct assumption box w/ some variable name that's needed
- Check line numbers — make sure to include ALL necessary citations for each step of natural deduction
- 2 Assumption Boxes will never end on the same line
- Distributive law WORKS BOTH WAYS
- For proof by contradiction for $p \rightarrow q$, assume p is true and q is false; then show that p is false based on q being true, creating contradiction.
- Check Work!! ✗

Table 7

1. $p \rightarrow q \equiv \neg p \vee q$
2. $p \rightarrow q \equiv \neg q \rightarrow \neg p$
3. $p \vee q \equiv \neg p \rightarrow q$
4. $p \wedge q \equiv \neg(p \rightarrow \neg q)$
5. $\neg(p \rightarrow q) \equiv p \wedge \neg q$
6. $(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$
7. $(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$
8. $(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$
9. $(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Proofs with Words

- Direct
- Casework
- Contrapositive
- Counter example
- Contradiction

- Cite definitions all the time – make explicit
- Say @ start what kind of proof it is
- "Seeking a contradiction, assume ..."
- "Let x be an arbitrary integer..."
- To prove $a \equiv b \equiv c$, prove CYCLE: $a \rightarrow b$, $b \rightarrow c$, $c \rightarrow a$.
- When proving rational / irrational, set $x = p/q$, with $\gcd(p,q) = 1$. For other things too, say "first instance of" or other specific to create contradiction later.

1. When proving logical equivalences, do NOT write both sides of equation.

- Edge / 0 cases in proofs
- For equivalent, must be able to start at any / get to any.

Modular Arithmetic

- $a \equiv b \pmod m \rightarrow a - b = m \cdot k,\ k \in \mathbb{Z}$
- m unique (mod m) values
- Addition, Subtraction, Multiplication normal; Division hard
- $a^{-1}(a) \equiv 1 \bmod m$
  - → if a^{-1} exists, is unique (a, m relatively prime)
  - → otherwise, 0 or MULTIPLE SOLS

- Proposition: Statement abt world w/ truth value
  - paradox / not well-defined ⇒ not a prop
  - every prop has negation
- Predicate: Statement w/ unspecified variables that becomes proposition once defined
  - Can define variables OR put $\forall$ / $\exists$
- Quantifiers: order matters when different!

- Tautology: A compound prop that is always true
- Contradiction: A compound prop that is always false
- Satisfiable: A compound prop that has a possible assignment of truth values to make it True.
- Consistent System: System specifications do not contain conflicting requirements that could be used to derive contradiction.

FME ($3^{26} \bmod 15$)

$3^{26} = (3^{13})^2$ | $3^3 \equiv -3 \bmod 15$

$3^{13} = 3 \cdot 3^{12}$ | $3^6 \equiv (-3)^2 \bmod 15 \equiv -6$

$3^{12} = (3^6)^2$ | $3^{12} \equiv (-6)^2 \bmod 15 \equiv 6$

$3^6 = (3^3)^2$ | $3^{13} \equiv 3 \bmod 15$

$3^{26} = 3^2 \bmod 15 \equiv \boxed{9}$

- if p then q
- p only if q
- q unless not p
- q whenever p

- if p, q
- q if p
- q when p
- p implies q

- p is sufficient for q
- q follows from p
- q is necessary for p
- a necessary condition for p is q

- A sufficient condition for q is p

p	q	p→q
T	T	T
T	F	F
F	T	T
F	F	T

be careful inside quantifiers of F → F case!!

$p \leftrightarrow q \equiv p \equiv q$

$\wedge$: and $\vee$: or $\oplus$: XOR ($\neg \leftrightarrow$)   but $\equiv$ and

Extended Euclidean Algo

- $59x \equiv 3 \bmod 73$

$\gcd(73, 59)$ | $73 - 59 = 14$
$\gcd(59, 14)$ | $59 - 4(14) = 3$
$\gcd(14, 3)$ | $14 - 4 \cdot 3 = 2$
$\gcd(3, 2)$ | $3 - 2 = 1$
$\gcd(2, 1)$

$3 - 2 = 1$
$3 - (14 - 4 \cdot 3) = 1$
$5 \cdot 3 - 14 = 1$
$5(59 - 4(14)) - 14 = 1$
$5 \cdot 59 - 21 \cdot 14 = 1$
$5 \cdot 59 - 21(73 - 59) = 1$
$26 \cdot 59 - 21 \cdot 73 = 1$

$(26 \cdot 59 - \cancel{21 \cdot 73}) \bmod 73 \equiv 1 \bmod 73$

$26 \cdot 59 \bmod 73 \equiv 1 \bmod 73$

$26(59)x \equiv 26(3) \bmod 73$

$x \equiv 78 \bmod 73$

$\boxed{x \equiv 5 \bmod 73}$

if-then with $\forall$ to talk about some of domain

and with $\exists$ to talk about some of domain

$S(x)$: student in class $C(x)$: studied calculus

Every student in this class has studied calculus $\forall x (S(x) \rightarrow C(x))$

Some student in this class has studied calculus $\exists x (S(x) \wedge C(x))$

Logic Puzzles: Write down 2^n truth table of possibilities, see which consistent.

$\exists y \forall(x)\ P(x,y) \rightarrow \forall x \exists y\ P(x,y)$

restrictive; single y to satisfy each x value

not as restrictive; can have diff y for each x-val