Discrete Math Notes

1. Basic Truth Tables:

a	b	$a \vee b$	$a \wedge b$	$a \to b$	$a \leftrightarrow b$
T	T	T	T	T	T
T	F	T	F	F	F
F	T	T	F	T	F
F	F	F	F	T	T

2. Other ways of writing $a \to b$:
   1. If a then b
   2. If a, b
   3. b, if a
   4. a only if b
   5. a is sufficient for b
   6. b is necessary for a
   7. $\neg b \to a$ (contrapositive)
   8. $a \to b \equiv \neg p \vee Q$ Conditional
   9. $a \to b \equiv \neg(p \wedge \neg Q)$ Conditional

   * $b \to a$ is the converse of $a \to b$, but they aren't equivalent

3. Order of Operations when there are no brackets.
   1. not ($\neg$) — Do it first
   2. and ($\wedge$)
   3. or ($\vee$)
   4. $\forall / \exists$
   5. $\to / \leftrightarrow$ — Do it last

4. Logical Equivalences

Laws	"And"	"OR"
Commutative	$p \wedge q \Leftrightarrow q \wedge p$	$p \vee q \Leftrightarrow q \vee p$
Associative	$(p \wedge q) \wedge R \Leftrightarrow p \wedge (q \wedge R)$	$(p \vee q) \vee R \Leftrightarrow p \vee (q \vee R)$
Distributive	$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge T \Leftrightarrow p$	$p \vee F \Leftrightarrow p$
Negation	$p \wedge \neg p \Leftrightarrow F$	$p \vee \neg p \Leftrightarrow T$
Double Negative	$\neg(\neg p) = p$	← Same
Idempotent	$p \wedge p \Leftrightarrow p$	$p \vee p \Leftrightarrow p$
Universal Bound	$p \wedge F \Leftrightarrow F$	$p \vee T \Leftrightarrow T$

Law	"And"	"OR"
De Morgan's	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$	$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$
Absorption	$p \wedge (p \vee q) \Leftrightarrow p$	$p \vee (p \wedge q) \Leftrightarrow p$
Conditional	$\neg(p \rightarrow q) \Leftrightarrow p \wedge \neg q$	$p \rightarrow q \Leftrightarrow \neg p \vee q$
Biconditional	$p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$	

5. Predicates and Quantifers

$\forall$: for all

$\exists$: there exists

$\neg\forall = \exists$ and $\neg\exists = \forall$

If the quantifers are same throughout a statement, their order doesn't matter.

E.g. $S(x,y)$: x scares y

$D = \{$ All people $\}$

- $\exists x \in D, \exists y \in D, S(x,y) = \exists y \in D, \exists x \in D, S(x,y)$
- $\forall x \in D, \forall y \in D, S(x,y) = \forall y \in D, \forall x \in D, S(x,y)$

Since the same quantifer is used in each sentence, the order doesn't matter.

- $\exists x \in D, \forall y \in D, S(x,y) \neq \forall y \in D, \exists x \in D, S(x,y)$

Since there are different quantifers, the order does matter

6. Proofs

1. Direct Proofs

often follows this form: $\forall x \in D, P(x) \rightarrow Q(x)$

Let x be an arbitrary element of the domain.

Suppose $P(x)$ is true.

Use true sentences to prove $Q(x)$ is true

E.g. Prove for all real numbers x and y, if x and y are rational then xy is rational.

Suppose x and y are rational.

Let $x = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$

Let $y = \frac{c}{d}$, $c, d \in \mathbb{Z}$, $d \neq 0$

$x \cdot y = \left(\frac{a}{b}\right)\left(\frac{c}{d}\right)$

$= \frac{ac}{bd}$, $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$

∴ If x and y are rational, then xy is rational

QED

2. Proof Using Mod

Mod gives the remainder.

E.g. 16 mod 13 = 3

$a \equiv_n b$ means $a \bmod n = b \bmod n$

Division Theorem:

Let m and n be natural numbers. Then, there exists a quotient Q and remainder R such that $m = nQ + R$, $0 \leq R < n$

Theorem:

For all int a, b, and n with $n \geq 1$, $a \equiv_n b$ iff $n \mid (a-b)$

Proof.

1. $a \equiv_n b \rightarrow n \mid (a-b)$ $\quad n \mid (a-b)$ means $a - b = nq$, $q \in R$

$\forall a, b, n \in \mathbb{Z}$ with $n \geq 1$, $a \equiv_n b \rightarrow n \mid (a-b)$

$a \equiv_n b$ means $a \bmod n = b \bmod n$

By Division Theorem, $a = nq_1 + r_1$, $q_1, r_1 \in \mathbb{Z}$, $0 \leq r_1 < n$

$b = nq_2 + r_2$, $q_2, r_2 \in \mathbb{Z}$, $0 \leq r_2 < n$

Since $a \bmod n = b \bmod n$, $r_1 = r_2$

$a = nq_1 + r$

$b = nq_2 + r$

$a - b = nq_1 + r - (nq_2 + r)$

$= nq_1 + r - nq_2 - r$

$= nq_1 - nq_2$

$= n(q_1 - q_2)$

Since both q_1 and q_2 are int, their difference must also be an int. $\therefore \exists q = q_1 - q_2$

$\therefore a \equiv_n b \rightarrow n \mid (a-b)$

2. $n \mid (a-b) \rightarrow a \equiv_n b$

$\forall a, b, n \in \mathbb{Z}$, $n \mid (a-b) \rightarrow a \equiv_n b$ with $n \geq 1$

$a = nq_1 + r_1$, $q_1, r_1 \in \mathbb{Z}$, $0 \leq r_1 < n$

$b = nq_2 + r_2$, $q_2, r_2 \in \mathbb{Z}$, $0 \leq r_2 < n$

$a - b = nq_1 + r_1 - (nq_2 + r_2)$

$= nq_1 + r_1 - nq_2 - r_2$

$= n(q_1 - q_2) + (r_1 - r_2)$

However, since $n \mid (a-b)$, $a - b = nq$, $q \in \mathbb{R}$

This means $n(q_1 - q_2) + (r_1 - r_2) = nq$

Since $0 \leq r_1, r_2 < n$, the only way $n(q_1 - q_2) + (r_1 - r_2) = nq$ is if $r_1 - r_2 = 0$. So, $r_1 = r_2$

So, $n(q_1 - q_2) = nq$

Since both q_1 and q_2 are ints, their difference must also be an int.

$\therefore \exists q = (q_1 - q_2)$

$\therefore n \mid (a-b) \rightarrow a \equiv_n b$

QED

2. Indirect Proofs

Type 1. Proof by contradiction

Claim: P

Assume $\neg P$

Derive a false statement

Conclude the assumption is wrong, so P is true

E.g. Prove $\sqrt{2}$ is irrational

To solve this, we need to use the Fundamental Theorem of Arithmetic.

The Fundamental Theorem of Arithmetic states:

Any int greater than 1 is either a prime number or can be written as a unique product of prime numbers.

Proof:

Suppose that $\sqrt{2}$ is rational.

That means $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}$, $b \neq 0$

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2$$

However $2b^2$ will have an odd number of prime factors while a^2 will have an even number of prime numbers. This contradicts the FTA. $\therefore \sqrt{2}$ is irrational.

QED

Type 2. Proof by Contrapositive

Claim $\forall x \in D$, $P(x) \rightarrow Q(x)$

Let $x \in D$ be arbitrary

Assume $\neg Q(x)$

Derive $\neg P(x)$ so $\neg Q(x) \rightarrow \neg P(x)$

By the contrapositive, $P(x) \rightarrow Q(x)$

Conclude $\forall x \in D$, $P(x) \rightarrow Q(x)$

E.g. Prove that $\forall x \in \mathbb{Z}$, (x^2-6x+5) is even $\rightarrow$ x is odd

Assume that x is even.

Then, it can be written as $2k$, $k \in \mathbb{Z}$

$x^2 - 6x + 5$ is now $(2k)^2 - 6(2k) + 5$

$= 4k^2 - 12k + 5$

$4k^2 - 12k$ must be even because k is being multipled by an even number and an even int multiplied by another int will result in an even number. Then, since both $4k^2$ and $12k$ are even, their difference must be even because an even int subtracting an even int will result in an even int. Since $4k^2 - 12k$ is even, and is added to 5, $4k^2 - 12k + 5$ will be odd.

$\therefore$ If x is even, x^2-6x+5 is odd

Having proved the contrapositive, the original statement must be True.

QED

3. Proof by Cases/Exhaustion

Claim: $\forall x \in D$, $P(x) \rightarrow Q(x)$

Split the domain D into disjoint sets $S_1, S_2 \ldots S_k$ such that their union equals D.

For each set S_i, show $\forall x \in S_i$, $P(x) \rightarrow Q(x)$

Since the union of the sets is D, conclude that $\forall x \in D$, $P(x) \rightarrow Q(x)$.

E.g. Prove if $n \in \mathbb{Z}$, then $3n^2 + n + 14$ is even.

Case 1. n is even

let $n = 2k$, $k \in \mathbb{Z}$

$3(2k)^2 + (2k) + 14$

$= 3(4k^2) + 2k + 14$

$= 12k^2 + 2k + 14$

$= 2(6k^2 + k + 7)$

$\therefore 3n^2 + n + 14$ is even when n is odd

Case 2. n is odd

let $n = 2k+1$, $k \in \mathbb{Z}$

$3(2k+1)^2 + (2k+1) + 14$

$= 3(4k^2 + 4k + 1) + 2k + 15$

$= 12k^2 + 12k + 3 + 2k + 15$

$= 12k^2 + 14k + 18$

$= 2(6k^2 + 7k + 9)$

$\therefore 3n^2 + n + 14$ is even when n is odd.

$\therefore 3n^2 + n + 14$ is always even if $n \in \mathbb{Z}$.

QED

3. Pigeon Hole Principle

If n items are put in m containers, with n>m, then at least 1 container will contain more than 1 item.

E.g. Prove that if we were to select 7 distinct numbers from 1 to 11, that at least 2 numbers will add up to 12.

Let m be the number of pigeon holes.
Let n be the number of pigeons.

Since we are selecting 7 distinct numbers, n = 7.
{1, 11}, {2, 10}, {3, 9}, {4, 8}, {5, 7}, {6}
Let m = 6 to correspond with these 6 sets ↑.

Since we are selecting 7 numbers to go into the 6 sets, then at least 1 set will have 2 numbers. Since each set, except for the set that only contains 6, add up to 12, and we are guaranteed to have at least 1 set that contains 2 numbers, we are guaranteed to select at least 2 numbers that add up to 12.

QED

4. Proof By Induction.

1. Simple Induction

Format:

1. State the predicate

P(n): ...

2. Base Case

Prove that P(n) is true when n is its smallest possible value

3. Induction Hypothesis

Assume for any arbitrary k that P(k) holds.

4. Induction Step

Prove $P(k) \rightarrow P(k+1)$

E.g. Prove that $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$, $\forall n \in N$.

1. $P(n)$: $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$, $\forall n \in N$

2. Base Case

$n = 0$

$LS = \sum_{i=0}^{0} i$

$= 0$

$RS = \frac{0(0+1)}{2}$

$= 0$

$LS = RS$, as wanted

$\therefore$ The base case holds

3. Induction Hypothesis

Assume for any arbitrary k that $P(k)$ holds $\forall k \in N$.

4. Induction Step

Prove $P(k) \rightarrow P(k+1)$

WTS: $P(k+1) = \frac{(n+1)(n+2)}{2}$

$P(k+1) = P(k) + (n+1)$

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

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

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

$\therefore S(k) \rightarrow S(k+1)$

$\therefore S(k+1)$ holds $\forall k \in N$

QED

2. Strong Induction

Step 1. Define the Predicate

P(n): ....

Step 2. Base Cases

Unlike simple induction where you only proved the base case once, you have to do it multiple times for strong induction. Like simple induction, you start at the smallest possible value for n.

Step 3. Induction Hypothesis

Assume for any arbitrary k that P(k) holds.

Step 4. Induction Step

Prove $P(k) \rightarrow P(k+1)$

You have to use I.H. more than once.

E.g.

$$F(n) = \begin{cases} 0 & n=0 \\ 1 & n=1 \\ F(n-1) + F(n-2) & n \geq 2 \end{cases}$$

Prove that $\forall n \in N$, $F(n+2) = 1 + \sum_{i=0}^{n} F(i)$

1. $P(n)$: $F(n+2) = 1 + \sum_{i=0}^{n} F(i)$, $\forall n \in N$

2. Base Cases

$n=0$

LS

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

$= 1$

RS

$1 + \sum_{i=0}^{0} F(i)$

$= 1$ ⟶ LS = RS, as wanted

$n=1$

LS: $F(3) = F(2) + F(1)$
$= 1+1$
$= 2$

RS: $= 1 + \sum_{0}^{1} F(i)$
$= 1+1$
$= 2$

LS = RS, as wanted
∴ The base case holds.

Induction Hypothesis
Assume for any arbitrary k that $P(k)$ holds $\forall k \in \mathbb{N}$.

Induction Step
Prove $P(k) \rightarrow P(k+1)$
WTS: $F(n+2) = F(n+1) + F(n)$

$$F(n+1) = 1 + \sum_{i=0}^{n-1} F(i) \quad \text{(By IH)}$$

$$F(n) = 1 + \sum_{i=0}^{n-2} F(i) \quad \text{(By I.H)}$$

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

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

$$= 2 + \sum_{i=0}^{n-1} [F(i) + F(i-1)] + F(0)$$

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

$$= 1 + F(0) + F(1) \ldots + F(n)$$

$$= 1 + \sum_{i=0}^{n} F(i)$$

QED

When to use Simple Induction V.S. when to use Strong Induction

Generally, use Strong Induction when there is a piece-wise function, like in the Fibanocci question. However, you can still use strong induction if there is no piecewise function.

Summation Laws

1. $\sum_{i=s}^{n} c \cdot f(i) = c \sum_{i=s}^{n} f(i)$, c is a constant

2. $\sum_{i=s}^{n} f(i) \pm \sum_{i=s}^{n} g(i) = \sum_{i=s}^{n} (f(i) \pm g(i))$

3. $\sum_{i=s}^{n} f(i) = \sum_{i=s+p}^{n+p} f(i-p)$, p is an integer

Well Ordering Principle

Any non-empty set of natural numbers contains a smallest element.

Proof that induction proofs are valid.

Suppose you just used induction to prove something. Assume that there is a set, C, that contains all false cases. $C \in N$. Let a be the smallest element in C. We know that a is greater than the base case because the base case holds true. That means a-1 is greater or equal to the base case and is not part of C. That means a-1 holds true for the induction proof. Since we know $P(k) \rightarrow P(k+1)$, $P(a-1) \rightarrow P(a)$. That means a holds true for the induction proof and $a \notin C$. This means our supposition is wrong, so the induction proof must be right.

QED

The Sum Rule:

If an operation can be performed in n different ways, each having x_i possible outcomes, then the total number of possible outcomes is $\sum_{i=0}^{n} x_i$.

If the question has "or", you will generally use the sum rule.

The Product Rule

If an operation takes k steps and the first step can be performed in x_1 ways and the second step can be performed in x_2 ways and so on, the whole operation can be performed in $\prod_{i=1}^{k} x_i = x_1 \cdot x_2 \dots \cdot x_k$

If the question has "and", you will generally use the product rule.

Combinations:

- Order doesn't matter
- $C(n,r) = \frac{n!}{(n-r)!\,r!} = \frac{P(n,r)}{r!}$

Permutations:

- Order matters
- $P(n,r) = \frac{n!}{(n-r)!}$

Counting with Reptition

Given n objects with r_1 of type 1, r_2 of type 2 and r_m of type m, where $r_1 + r_2 + \dots r_m = n$, the number of arrangements is $\frac{n!}{r_1!\, r_2!\, r_3! \dots r_m!}$

E.g. How many ways can you arrange these letters?
a, a, b, a, c, b, c, a, d, e, f

There are 11 letters, so $n=11$
There are 4 a's.
There are 2 b's
There are 2 c's.

So, answer = $\frac{11!}{2!\,2!\,4!}$

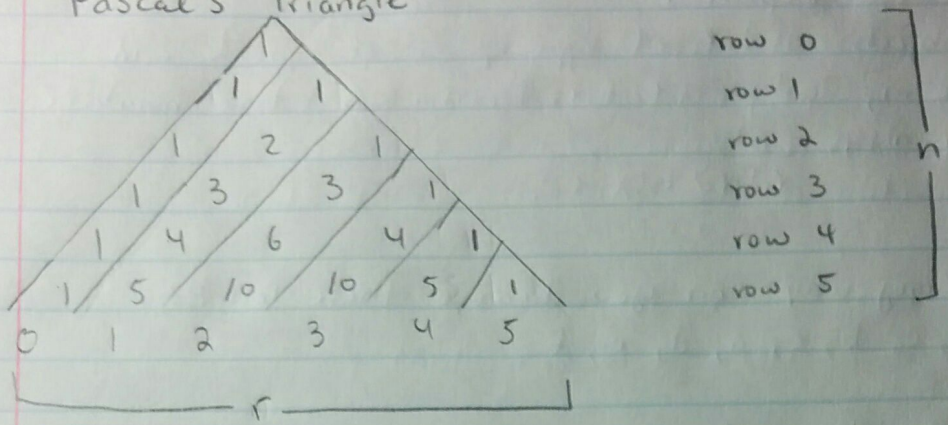
Selection with Reptition

If there are n choices, there are $n-1$ partitions, and you will have $C(r+n-1, n-1)$ or $C(r+n-1, r)$ ways of arranging it.

E.g. If there are plain, sesame seed and poppy seed bagels, how many ways can you select 6 bagels?
$r=6$
$n=3$
So, there are 2 partitions
In total, there are $C(8,2)$ or $C(8,6)$ ways of selecting the six bagels.

E.g. Same scenario as above, but this time, you must select a plain bagel.
Since you have to select a plain bagel, subtract that from the total numbers of bagels. $r=6-1=5$
$n=3$, so 2 partitions
$C(7,2)$ or $C(7,5)$

Pascal's Triangle



- The n, r^{th} element is $C(n,r)$
  E.g. in row 4, the 6 is the 2nd element
  $C(4,2) = 6$

- Each row gives the coefficient of a binomial expansion.
  E.g. In row 2, the numbers are 1, 2, 1
  $(a+b)^2 = (1)a^2 + 2ab + (1)b^2$

- Each row sums to 2^n.
  E.g. In row 3, the sum is 8. $2^3 = 8$

- Each row is a power of 11.
  $1 = 11^0$ (row 0)
  $11 = 11^1$ (row 1)
  $121 = 11^2$ (row 2)

The number of ways to distribute r identical objects in n distinct boxes with at least one object in each box is $C(r-1, n-1)$.

Probability

- An experiment is a clearly defined procedure that results in one of a possible set of outcomes.

- A sample space of a random experiment is a set S that includes all possible outcomes of the experiment.

- A compound event is a subset of S consisting of several elementary events.

$$\text{Probability} = \frac{|E|}{|S|}$$

E.g. What's the probability of throwing a 1 on a fair die?

$|E| = 1$

$|S| = 6$

$\text{Prob} = \frac{1}{6}$

- The sum of all probabilities in the sample space must be 1.

- $P(A \cup B) = P(A) + P(B) - P(A \cap B)$ (Sum Rule)

- 2 events, E and F are complementary if $P(E) = 1 - P(F)$.

- When the probability of event E depends on a previous event F happening, we denote this as $P(E|F)$.

- Product Rule:
If E and F are 2 events in an experiment then the probability of both E and F occuring is:

$$P(E \cap F) = P(F) \cdot P(E|F)$$
$$= P(E) \cdot P(F|E)$$

- If $P(E|F) = P(E)$, then the events are independent. In that case, $P(E \cap F) = P(E) \cdot P(F)$

- Bayes' Rule
Let A and B be events in the same sample space. If neither $P(A)$ nor $P(B)$ are 0, then:

$$P(B|A) = P(A|B)\left(\frac{P(B)}{P(A)}\right)$$

- Total Probability Theorem:
Let S be a sample space with disjoint union of events E_1, E_2, ... E_n with positive probabilities and let $A \subseteq S$.
Then:

$$P(A) = \sum_{i=1}^{n} P(A|E_i) \cdot P(E_i)$$

- Modular Properties
This is related to mod, not to probability.

1. $a \equiv_n b \iff a \bmod n = b \bmod n$
2. $a \bmod n \iff a = nq + r,\ q, r \in \mathbb{Z},\ 0 \leq r < n$
3. $a \equiv_n b \wedge b \equiv_n c \rightarrow a \equiv_n c$
4. $a \equiv_n b \iff n \mid (a-b)$
5. $a \equiv_n b \iff ac \equiv_n bc$, c is a constant