Discrete Math (CS2022) Notes

Christopher Myers

June 13, 2020

Contents

Discrete mathematics deals with discrete objects, or objects that are "separate" from each other in some way. This is opposed to continuous mathematics where there is no "gap" between data and the interval is continuous. For example, $f(x) = \sin x$ is a continuous function.

1 Logic

1.1 Propositions

Propositions are declarative statements that are either true or false. They cannot be both and they cannot be somewhere between, they are definitively one or the other. For example, 2 + 3 = 5 is a declarative statement, and it is true. 2 + X = 5, on the other hand, is declarative but is not determinable, so it is *not* a proposition.

These can be statements in written english, but those statements must follow the same rules. "It is sunny outside" counts as a proposition, but "please be quiet" does not, for instance.

Keep in mind that unproved or even unprovable statements can be propositions. Goldbach's conjecture (that every number is the sum of at least two primes), for instance, *is* a conjecture, but it hasn't been definitively proven either way.

1.2 Operations

Operations can be performed on propositions. The basic ones are negation ($\neg$), conjunction ($\wedge$, or "and"), and disjunction ($\vee$, or "or"). More will be added here over time.

- Negation $\neg$ - "not" (invert)
- Conjunction $\wedge$ - "and" (true if both are true)
- Disjunction $\vee$ - "or" (true if one is true)
- Exclusive or $\bigoplus$ - "xor" (true if one is true but not if both are)

There is an order of operations that can be applied in absence of parentheses, analogous to the order of operations for math. That order is $\neg, \wedge, \vee,$.

1.3 Conditional Statements

Conditional statements take one proposition and maps it to another. If the first proposition is true, the second is said to also be true. This can be phrased in multiple ways, such as "p is sufficient for q", "p only if q", "q is necessary for p", "q follows from p", "q when p", and "q unless not p" In such statements as $p \to q$, p is referred to as the premise, antecedent, or hypothesis, and q is referred to as the conclusion.

If you have a true premise and a true conclusion, the statement is true. If the premise is true but the conlusion is false, the statement is false. If instead the premise is false and the conclusion is true, the statement is true, as in the case where both premise and conclusion are true. In short, a false premise can lead to anything; the relationship between premise and conclusion goes in one direction only.

1.3.1 Operations on Statements

Given an implication $p \to q$, the converse is $q \to p$. The converse is *not* always true, but the contrapositive - $\neg q \to \neg p$ is always true. The inverse is just $\neg p \to \neg q$. Note that $p \to q$ is the same as $\neg p \vee q$.

1.4 De Morgan's Laws

De Morgan's Laws are two simple equivalencies: the negation of p or q is $\neg p \wedge \neg q$ and the negation of p and q is $\neg p \vee \neg q$.

1.5 Tautologies and Contradictions

There are some statements - tautologies - that are always true and denoted by **T**, and some statements that are always false - contradictions - and denoted by **F**. All other statements are contingencies. Some examples are below:

- $p \vee \neg p$ - Tautology
- $p \wedge \neg p$ - Contradiction
- $\neg(p \vee q) \equiv \neg p \wedge \neg q$
- $\neg p \rightarrow q \equiv p \vee q$

1.6 Existential Propositions

It is possible to write propositions that depend on a variable that are proper propositions so long as the value of a variable is defined. For example, for the proposition "x+2 is an even integer", x must be defined. For some x, P(x) is true, which is on its own a proposition. This can be

1.7 Predicates and Quantifiers

It is possible to write statements that take some variable and apply a conditional statement. For example, consider the line "All CS students must take discrete math." This would take the logical form of "If x is a CS student, then X must take discrete math," where the domain is over *all* CS students. Formally this is written as $\forall x(P(x) \rightarrow Q(x))$, or just $\forall x Q(x)$.

Note that there is a easy negation to the above statement: find at least one CS student that does *not* need to take discrete math. Formally, this is written as $\exists x \neg Q(x)$.

There can of course be statements that use multiple variables, for example $x + y = 17$ with a domain of all real numbers. A statement that could be evaluated would then be $\forall x \exists y P(x, y)$, or translated to English: "For all x there exists a y in which x+y=17." For another example, consider the sentence "All students in this class have read section 1.3"[1]. This would then be written as $\forall x(P(x) \rightarrow Q(x))$, or more briefly, $\forall x Q(x)$ where the domain is understood. The negation is then $\exists x \neg Q(x)$ while the negation of the first form is $\exists x(P(x) \wedge \neg Q(x))$

Inverting the order of "for all" and "there exists" does *not* yield an equivalent function - that is, $\forall x \exists y P(x, y) \neq \forall y \exists x P(x, y)$. For example, take the function $\frac{y}{x} = 0$. There is a y for every x that makes this yield 0, but there is NOT an x for every h that makes this zero... or maybe the other way around. It all has to do with dividing by zero. Something like that, anyways!

1.8 Rules of Inference

If you have a statement P and a statement $P \wedge (p \rightarrow Q))$, we can safely say that the whole statement implies Q. This is one rule of inference, called "modus ponens". More are listed below.

- $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg q$ – modus lollens (?)
- $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (q \rightarrow r)$ – syllogism
- $(p \vee q) \wedge (\neg p) \rightarrow q$
- $p \rightarrow p \vee q$
- $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

[1] According to knowledge of this statement, this is *false*

1.9 Theorems and Proofs

Theorems are propositions that can be shown to be true. They are distinct from propositions that are not yet shown to be true, called conjectures. The typical way to prove a theorem is to go through a series of propositions (each of which should be true) using axioms, definitions, etc. as tools to eventually prove the definition. For example, some time ago Euclid was able to create a system of geometry using only a few simple axioms, definitions, and a *lot* of deduction work.

Example 1 Prove that for every real number X, $x^2 - 4x + 17 \neq 0$

$$\begin{aligned} \forall x \exists R x^2 - 4x + 17 &\neq 0 \\ x^2 + 4x + 17 &= x^2 - 4x + 4 + 13 \\ &= (x-2)^2 + 13 \geq 13 \end{aligned}$$

When a theorem is completed, often a symbol in the form of a solid block or the word "Q.E.D." is written to signify that the proof is done.

There are different kinds of proofs and theorems - one such proof example is given above in the form of a simple algebraic theorem. Other kinds of theorems exist as well, such as existence theorems.

Example 2 - Proofs by contradiction Prove that $\sqrt{2}$ is irrational.

Start by supposing the opposite and trying to deduce a contradiction. Here, suppose that $\sqrt{2}$ is irrational. That would mean that, by definition, there must be some two numbers p and q whose quotient yields $\sqrt{2} : \frac{p}{q} = \sqrt{2}$. Assume that the fraction is reduced. A little algebra yields $2q^2 = p^2$, meaning that both p^2 is even and p is even. If you substitute p for 2k, you get $2q^2 = 4k^2$ and then $q^2 = 2q^2 \ldots$ this leads to the same conclusion that q is even and can be represented as 2l instead. So the final fraction is $\frac{2k}{2l}$ (or something like that anyways), which contradicts our orriginal assumption of a reduced fraction.

Example 2 Prove that there are an infinite number of primes (the sequence of numbers that are not divisible by any number other than themselves and one). This is an existence theorem. This can't be done constructively as it would require a complete list of primes.

Suppose there are a finite number of primes that take the form of a list $P1, P2, P3, \ldots Pk$. Let $m = P1, P2 \ldots Pk + 1$, formed by multiplying the last two together and adding one.

This is where the fundamental theorem of arithmetic is needed, which states that every number greater than one is either a prime or is a product of primes. We can determine that there is no Pi number of which m is a factor. Since all numbers must either be prime or must be a product of primes, this means that m is a prime. However, m must be prime in order to not contradict with the fundamental theorem and it must be nonprime in order to not contradict with our original supposition that there is a finite number of primes. Thus by contradiction there must be infinite primes.

2 Sets

A set is simply a collection of objects. A simple example of a set is the set of students in a lecture hall.

2.1 Notation

If x is an element in a set A, we can write it as $x \in a$. If it is not in A, we write it as $x \notin A$ (notation WIP). If A is a subset of B, write it as $A \subseteq B$. Also, $A \subset B \equiv (x \in A \rightarrow x \in B) \wedge (\exists x \in B \wedge x \notin A)$.

There are a number of special predefined sets, for example U, the universal set. The universal set is very context dependant; for example, when working with students in a lecture hall, U could be all students in the hall. The opposite then is ϕ, the empty set or the null set, and is a subset of every set: $\phi \subseteq A$ (phi is

contained in or equal to A). If $x \in \phi$, then $x \in A$. This can be fun to play around with - for instance, $\phi = \phi$, since phi is the empty set. So a set containing phi is empty.

Finally, there is such a thing as a power set or P(s) where s is a set. This is the set of all subsets of s, and its size grows very quickly as s expands – specifically, it expands with the rows on Pascal's triangle, or 2^m where m is the number of elements in s.

2.2 Operations on Sets

Suppose there are two sets A and B. Their cartesian product $A \times B$ consists of $(a, b)|a \in A \wedge b \in B$. For example, for sets $A = 1, 2, 3$ and $B = a, b$, $A \times B = (1, a), (1, b), (2, a), (2, b), (3, a), (3, B)$. If you were to do $R \times R$, you would get the entire cartesian plane.

The union of two sets is just two sets merged into one: $A \cup B = x|x \in A \vee x \in B$. On a Venn diagram, both intersecting circles and their intersection should be shaded in. The intersection is then *only* the intersection on the venn diagram: $A \cap B = x|x \in A \wedge x \in B$. The complement of B relative to A is $A - B = x|x \in A \wedge x \notin B$. When viewing A in the universal set U, everything not in A would be defined as U-A, or the complement of A. Also since I don't know where this should go, $|A \cup B| = |A| + |B| - |A \cap B|$.

2.3 Logic and sets

There is a connection between sets and logic. A list of corresponding logic and set statements is below - logic on the left, sets on the right.

- $p = p$
- $\neg p = \bar{p}$
- $T = U$
- $F = \phi$
- p(x) is true $= x \in p$
- $p \to q = x \in p \to x \in q$
- $p \vee q = p \cup q$
- $p \wedge q = p \cap q$
- $p \bigoplus q = p \cup u - p \cap q$

Furthermore, proving logical equivalence between two logic statements is the same as proving equality of sets.

The net result of this is that set theory is really just logic in disguise. The same theorems work, the same principles hold, and similar operations can be performed.

2.4 Functions

A function is a rule mapping each $a \in A$ to an output in BL $f(a) = B$. For example, take A to be the set of students and B is the set of chairs. The function, then, would map one student per chair. Every value in B must have a corresponding unique value in A in much the same way as matheatical functions can only have one Y output per X.

2.4.1 Recurrence Functions

Recurrence functions, sometimes called recursive functions, rely on their past output values to generate new values. For example, the fibonacci sequence is a recurrence function where $f_n = f_{n-1} + f_{n-2}$. Alternatively, the factorial functin can be defined as $a_n = na_{n-1}$

2.5 Unification of circuits, sets, and logic

In circuits, current flows when a switch is closed. Switches can be configured in series where there is one after another – current flows iff all switches are closed. Alternatively, switches can be configured in parallel to create the equivalent of an and gate. Using these simple rules it is possible to construct a circuit to represent any kind of logic system or set rule. These are all logically equivalent – there are $\wedge$, $\vee$ & $\neg p$ in logic, $\cap$, $\cup$ & $\bar{A}$ in sets, and $a \cdot b$, $a + b$, and a' in circuits. Each system has its own special symbols too: F and T for logic, ϕ and U for sets, and 0 and 1 for circuits.

All of these behave similarly because they fall under the header of Boolean algebra, a system involving binary operations such as "and", "not", "or", plus the unary operations like the complement. These following axioms must be satisfied for any system to be considered a Boolean system:

1. $x \vee 0 = x$
2. $x \wedge 1 = x$
3. $x \vee \bar{x} = 1$
4. $x \wedge \bar{x} = 0$

Furthermore, commutativity ($x \wedge y = y \wedge x$), associativity ($x \vee (y \vee z) = (x \vee y) \vee z$), and distributivity ($x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$) must be satisfied. These axioms plus these requirements together form a complete specification for the fundamentals of Boolean algebra. Further identities may be derived from the above axioms.

As an aside, there is a principle of duality in these systems where, if you swap all "and"s and "or"s and you swap all 1's for 0's, you get an equivalent expression.

3 Number Theory

3.1 Divisibility

If a number A divides a number B (where A and B are integers), the result should also be an integer, implying that $B = Ak$ for some integer k. This is written as $A|B$. This immediately yields some properties: if A divides B and A divides C, then A is divided by B + C. Another one, If A divides B, then A divides BC for all integers C. Finally, if A divides B and B divides C, then A divides C (this is the transitive property).

When numbers do not divide evenly into one another, there is a remainder. For this case we have the division algorithm. If A is an integer and D is a positive integer, then there exists integers Q and R where R is $0 \leq R < d$, such that $A = DQ + R$. (No, this isn't a real algorithm). This just means that if you divide A and D, you get the quotient plus a remainder. For example, $\frac{-37}{8} = 8(-5) + 3$. In this case we would say that -37 is congruent to 3 mod 8. For another example. $13 \equiv 3 \mod 5$, because $13 - 3 = 2 \cdot 5$. Or, $23 \equiv 3 \mod 5$, and $13 \mod 5 = 23 \mod 5$.

3.1.1 Mod properties

Below are a few useful mod properties:

- If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$
- $b \mod (d \mod m) \equiv bd \mod m$
- $(b \mod m)^2 = b^2 \mod m$
- If $a \equiv b(\mod m)$ then $ac \equiv bc(\mod m)$. From this we can infer that $a - b = km$, and that $ac - bc = (kc)m$. Note that the converse is not true.

Example 1 Calculate $5^{11} \mod 17$

$$
\begin{aligned}
5^{11} &= 5^8 5^2 5^2 \\
11 &= 2^3 + 2^1 + 2^0 \\
5 \mod 17 &= 5 \\
5^2 \mod 17 &= 8 \\
5^4 \mod 17 &= 8^2 \mod 17 = 13 \\
5^8 \mod 17 &= 13^2 \mod 17 = 16 \\
5^{11} \mod 17 &= 16 \cdot 40 \mod 17 \\
&= 16 \cdot 6 \mod 17 \\
&= 96 \mod 17 \\
&= 11
\end{aligned}
$$

Example 1 Given three consecutive intergers $a, a+1, a+2$, prove that one of them is divisible by three.

First, divide A by three to see what you get: $a = 3q + r$, following the division algorithm. That means that R must be 0, 1, or 2. If $r = 0$, then A is divisible by three. If $r = 1$, then $a + 2$ must be divisible by three, and the same goes for $r = 2$ and $a + 1$. This all follows from doing simple arithmetic on the division algorithm.

3.2 Bases for Integers

Integers can have different bases. For instance, if you take the number 312, it can be represented as $3 * 10^2 + 1 * 10^1 + 2 * 10^0$. The general theorem is that if you take b as a positive integer greater than or equal to two, and given a positive integer n, n can be written as $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^0$. This is called the "base b expansion of n".

Change-of-base can be performed with relative ease, although a calculator might be wanted. For example, $312_{10} = 470_8$. These calculations can be performed in various ways, one of which is by using the base expansion method. [2].

Example 1 Convert 2159_{10} to binary, octal, and hexadecimal.

- Binary: 1000 0110 1111
- Hexadecimal: 86F
- Octal: 4157

3.3 Greatest Common Divisor

Let A and B be integers. The greatest common divisor of A and B is a number D such that D divides A and D divides B ($d|a, d|b$) such that D is the greatest possible number. This is written as $d = gcd(a, b)$. For example, $gcd(28, 70) = 24$.

Random aside: Take the lemma that if $a = bq + r$ and $a \geq b$, then $gcd(a, b) = d$. That also equals $gcd(b, r) = d'$, i.e. $d = d'$.

[2]Note that it might be worthwhile to become proficient at some kinds of bases, notably binary and hexadecimal

Example 1 Compute $gcd(207, 81)$.

$$\begin{aligned} gcd(207, 81) &= gcd(81, 45) \\ 207 &= 2 * 81 + 45 \\ 81 &= 45 + 36 \\ 45 &= 36 + 9 \\ 36 &= 4 \cdot 9 \\ &= 9 \end{aligned}$$

The above works because the lemma mentioned earlier is just repeated over and over again until a zero is obtained for one of the arguments to *gcd*. This is called the euclidean algorithm, and it is designed to find the greatest common divisor of two numbers.

The algorithm works on $gcd(a, b)$ where $a \geq b$ by first taking $a = bq + r \ldots$

$$\begin{aligned} a &= bq + r = gcd(a, b) \\ r_0 &= r_1 q_2 + r_2 = gcd(r_0, r_1) \\ r_1 &= r_2 q_2 + r_3 = gcd(r1, r2) \\ &\ldots \\ &= r_{n-2} = r_{n-1} q_{n-1} + r_n \end{aligned}$$

At some point this terminates at zero and a result is obtained.

Note that if the two numbers A and B have no common factors, they are called "relatively prime".

3.4 Least Common Multiple

The least common multiple is the smallest number that is divisible by two numbers A and B. Read it as "least (common multiple)", i.e. it is the common multiple with the lowest value. For example, the LCM of 3 and 4 is 12.

3.5 Modular Math

If $sa \equiv 1 \mod b$, s is said to be the multiplicative inverse of a.

If $a \equiv b \mod m$, then $ac \equiv bc \mod m$. The converse, $ac \equiv bc \mod m \rightarrow a \equiv b \mod m$, does not hold true. For example, $12 \equiv 20 \mod 8$ and $3 \cdot 4 \equiv 5 \cdot 4 \mod 8$, but $3 \not\equiv 5 \mod 8$. The c's can be cancelled in the case where $gcd(m, c) = 1$ (i.e. M and C are relatively prime).

If P is a prime, then $2^{p-1} \equiv 1 \mod p$. The converse is not true: $2^{340} \equiv 1 \mod 341$. 341 is not actually prime, it's $11 \cdot 31$. This is involved with a theorem called Fermat's Little Theorem, which says that if $gcd(a, p) = 1$ where P is a prime and P does not divide A, then $a^{p-1} \equiv 1 \mod p$. This is just a generalization of the earlier statement for any base A. It also implies that $a^p \equiv a \mod p$.

Fermat's Little Theorem is useful for some power calculations:

$$\begin{aligned} 5^{14} \mod 11 &=? \\ 14 &= 11 + 3 \\ 5^{14} &= 5^{11} 5^3 \\ &\equiv 5 \cdot 125(\mod 11) \\ &= 5 \cdot 4(\mod 11) \\ &= 9 \mod 11 \end{aligned}$$

Another example:

$$\begin{aligned} 9^{222}(\mod 11) &=? \\ 9^{222} &= 9^{10^2} \cdot 9^2 \\ &\equiv 9^2(\mod 11) \\ &\equiv 4(\mod 11) \end{aligned}$$

3.6 Prime Numbers

According to the fundamental theorem of arithmetic, every integer greater than one is either a prime or a product of primes (a composite number). If N is a composite number, then it has a prime factor less than or equal to $\sqrt{n}$.

Example 1 Take the number $n = 149$ and figure out possible prime factors. Right from the start all numbers greater than 12 can be eliminated, leaving primes 3, 5, 7, and 11. As it turns out, this number has no prime factors, so it itself must be a prime.

There is an interesting function $2^n - 1$ that has a habit of generating prime numbers as long as n is prime. It is not true for all primes (notably 11), but otherwise the primes generated by this formula are called Mersenne primes. The largest known Mersenne prime is is $2^{74,207,281} - 1$.

3.6.1 Twin Primes

Many things about prime numbers are not known, most notably the idea behind twin primes. These are primes that come in pairs with at most one number between them. For example, 3 and 5, 11 and 13, or 17 and 19. The conjecture for this is that there are infinitely many twin primes. This has not yet been proven.

3.6.2 Goldbach Conjecture

The Goldbach conjecture claims that every even number is the sum of two primes. For example, 74 = 37 + 37 or 71 + 3.

4 Cryptography

4.1 RSA

RSA is a cryptography scheme invented sometime in the 1970s, dependent on the fact that very large numbers are hard to factor.

Suppose that there are three players: Alice, Bob, and Eve, where Alice and Bob are people trying to communicate, and Eve is an eavesdropper. Alice starts by picking two very large prime numbers P and Q(think thousands of digits) and multiplies them together to form N. She also picks a number E that is relatively prime to $(p-1)(q-1)$ at her choosing. Alice sends her numbers N and E to Bob, but realistically she could send them to anybody in the world - this is her public key.

To send a message to Alice, Bob must use Alice's public key. He takes a message and encodes it using some scheme (often done in blocks at a time) and forms a message M as a number. Bob sends $m^e \mod n$ as a number to Alice.

To decrypt the message, Alice finds a number D such that $ed \equiv 1 \mod (p-1)(q-1)$ where D is the inverse of E. As it turns out, D is easy to find out as she already has access to P and Q: $ed-1 = k(p-1)(q-1)$, or $ed = 1 + k(p-1)(q-1)$. Alice takes $M^{ed} \mod n$, which equals $M^{1+k(p-1)(q-1)}$. A little simplification yields $M^{(p-1)k(q-1)} = M$. This whole procedure might be lost somewhere here (these are bad RSA notes...) so here's an example:

Example 1 Take $p = 11, q = 13$, $n = 143$ with $(p-1)(q-1) = 10 \cdot 12 = 120$, and $e = 7$. The numbers n and e are sent to him (143 and 7). Suppose Bob wants to encode a message $M = 09\ldots$

$$\begin{aligned} M^e &= 9^7 \\ 9^7 \mod n &= 9^7 \mod 143 \\ &= 48 \end{aligned}$$

So this number 48 is now sent out to Alice. To decrypt the number, Alice must find the inverse of e, d, such that $ed \equiv 1 \mod (p-1)(q-1)$.

$$\begin{aligned} 7d &\equiv 1 \mod 120 \\ 120 &= 7 \cdot 17 + 1 \\ (-17)7 - 1 &\equiv -120 = (-1)(120) \\ -17 &\equiv 103 \mod 120 \\ d &= 103 \\ M^{ed} \mod n &= M \\ 48^{103} \mod 143 &= 9 \end{aligned}$$

Alice has managed to recover the original message M of 09. As supplementary material, to find the inverse of one number mod another is to use the division algorithm. In the above algorithm, it involved taking 120 and dividing by 7. That yielded a remainder of 1... or in the above example, $7x - 1 = 120k$ The above solution involved multiplying though to get a +1 on the left side as a positive number is needed for the inverse. No, this doesn't make sense either, but the exam will need the GCD function and the ability to express a GCD as a linear combination of the two parameters put into the GCD function.

5 Induction

Mathematical induction is the process of proving something using mathematical induction. This isn't the kind of induction where you notice a pattern and draw a (not necessarily true) conclusion based on it.

Take the "dominoes" approach to the problem. When the first domino falls, the next falls, then the one afterwards, and so on. Likewise in math, if you can set up a chain of interconnected propositions, if you can prove one, the rest will follow.

For example, if there is a statement P(n) about positive integers that needs proving, a viable approach is to prove that P(1) is true, then show that whenever P(k) is true, P(k+1) is true. If these hold up, you can say that P(n) is true for all positive integers n by proof by induction.

Example 1 Prove that the sum of all positive integers N yields $\frac{n(n+1)}{2}$. Call this P(n).

First prove that P(1) is true. It is, so we move on to show that if P(k) is true, P(k+1) is true. Once that's done, 1 can be our first k, so P(k) is proven. That specific proof will not be shown.

Example 2 Take some odd integers $1 + 3 + 5 + \cdots + (2n-1)$. Prove that the sum of these numbers is n^2.

Start with the statement that P(1)=1, which verifies. Then move on to P(k), which would be $1 + 3 + 5 + \cdots + (2k-1) = k^2$, and P(k+1), or $1 + 3 + \cdots + (2k-1) + (2k+1) = (k+1)^2$ An alternative way of visualizing this is to expand in shells outward from the corner of a square; the first shell has 1 cell, the second has 3, the third has 5, etc., and the outermost shells form a shell.

5.1 Strong Induction

The strong form of induction is to first find a statement of P(n) about some integer. Find a base case of P that is true, $P(n_0)$. Assume that P(n) is true for integers less than k but greater than or equal to n_0. This form of induction follows the "dominoes" analogy - if you can set up a chain of "dominoes" (statements), you only need to knock over one. In other words, if you can show that P(k) follows, then P(n) is true for all integers n. Keep in mind that this only works for discrete integers, not real numbers or rational numbers. Note the disctinction bewteen this and simple induction: $P(< k) \rightarrow P(k)$, not $P(k) \rightarrow P(k+1)$. In other words, the strong form of induction relies on multiple bases instead of just one.

Example 3 Prove the fundamental theorem of arithmetic, that any integer greater than 1 is either a prime or a product of primes.

The base case of this should be $n = 2$. If n in P(n) is a prime, no further proof is needed; otherwise, it must be proved that n is a product of two positive integers, and that each of them is less than n. By the inductive hypothesis, A and B are either primes or products of primes, implying that n is a product of primes. That's actually it - nothing more needs to be proven.

Example 4 Take a convex n-gon (a polygon with n sides where it is impossible to draw a line between two points within the polygon that crosses an edge). If you add up the angles of a triangle, the result is 180. If you add up the angles of a quadrilateral, the sum is 360. For an n-gon, prove that the sum of the degrees is $180(n-2)$. This is a statement about integers n, or $P(n)$, so induction can be applied to it (no, this isn't the fun electrical kind).

Assume that this result holds for integers less than n where $n \geq 3$. Start by splitting a given n-gon into two smaller polygons, one with $(n-q)+1$ sides and the second having $q+1$. The result holds for these two polygons holds - by the inductive hypothesis, the angle sums are $180(n-q-2)$ and $180(q-1)$. The n-gon on its own, however, has an angle sum equal to the two sections of it added together, or $100(n-q-1+q-1) = 180(n-2)$. This has yielded the original hypothesis using strong induction.

6 Counting

6.1 Basic Principles

6.1.1 Multiplication Principle

If there is an event that can be performed in n_1 ways and another independent event that can be performed in n_2 ways, then the number of ways for those events to happen together (note the *and*) is $n_1 \cdot n_2$. For example, with a bitstring of length 5, there are 2^5 different possibilities.

6.1.2 Addition Principle

If there are two sets A and B that are disjoint, the cardinality of their union is just their combined cardinalities. Or in mathematical notation, $|A \cup B| = |A| + |B|$.

6.1.3 Principle of Inclusion and Exclusion

$|A \cup B| = |A| + |B| - |A \cap B|$. In plain english, if there are two intersecting sets A and B, the cardinality of their union is equivalent to their combined cardinalities minus the cardinality of their intersection.

6.2 Pigeonhole principle

If there are 10 pigeons and 9 holes, there must be at least two pigeons in at least one hole. In a set context, if $|A|, |B|$ and there is a function $f : A \rightarrow B$, then two values of A must be mapped onto B.

Example 1 For a given series of consecutive terms of lenth n, there is a sum divisible by m. To prove it, take the sums $a_1, a_1 + a_2, a_2 + a_3 \ldots$. The claim is then $\exists k, l \leq m$ such that $a_{k+1} + a_{k+2} + \cdots + a_l = qm$. If any of the formed sums is divisible by m, done. Now assume that none of the sums is divisible by m, so dividing by m will yield remainder $1, 2, \ldots, m-1$. There are $m-1$ possible remainders for m expressions, so by the pigeonhole principle, two of the sums must have the same remainder. Now suppose there are the sums $a_1 + a_2 + \cdots + a_k = q_1 m + r$ and $a_1 + a_{2r} + \cdots + a_k + a_{k+1} + \cdots + a_l = q_2 m + r$; this is just an expression of the two equal remainders. If you subtract the two, you get $(q_2 m + r) - (q_1 m + r) = (q_2 - q_1)m$, meaning that m divides the earlier sum $a_{k+1} + \cdots + a_l$.

6.3 Combinations and Permutationos

6.3.1 Permutations

Take a set S with n objects and call it an n-set. An R permutation of an n-set is an ordered arrangment of r objetcs from the n-set. $P(n, r)$ is then the number of r-permutations of an n-set. The formula can be expressed as $P(n, r) = \frac{n!}{(n-r)!}$

Example 1 Find the number of ways there are to order the 26 letters of the alphabet such that no two vowels are consecutive.

One way is to take the 21 consonants and find their permutations, which is just 21!. Now take the number of spaces between the consonants plus a space on each side for a value of 22 - 22 places to put the 5 vowels. Calculate P(22, 5) or the number of ways to select 5 spaces from 22 other spaces. The complete answer is then $21! \cdot P(22, 5)$ or just $\frac{21!22!}{17!}$

6.3.2 Combinations

Combinations are like permutations but where order does not matter. The formal definition is that an r-combination of an n-set is an unordered set of r objects from n objects. This is denoted by C(n,r) where n is the size of the set and r is the number of elements selected (often verbalized as "n choose r"). Permutations can actually be expressed in terms of combinations, using the form $C(n, r)r!$. The formula is just $C(n, r) = \frac{n!}{r!(n-r)!}$.

There are some useful properties to combinations:

- $C(n, k) = C(n, n-k)$.
- $C(n, k) = C(n-1, k-1) + C(n-1, k)$.
- $C(n, 0) + C(n, 1) + \cdots + C(n, n) = 2^n$

6.4 Binomial Theorem

Under binomial theorem, two numbers are taken and raised to a power, $(x + y)^n$, where the challenge is to expand the statement. Binomial theorem is intertwined with combinations and Pascal's triangle, whose values are given both by a simple adding rule and by taking combinations of the row and column value. The general formula for a binomial expansion is $(x + y)^n = \sum_{k=0}^{n} C(n, k) x^{n-k} y^k$.

6.5 Recurrence Relations

Recurrence relations (sometimes called recursive functions) are relations that involve the last number output by the function and some starting base condition. For example, the Fibonacci sequence can be represented by $a_n = a_{n-1} + a_{n-2}, a_1 = 1, a_2 = 1$.

One example of where recurrence relations arise is the Tower of Hanoi. The tower starts with a peg that has circular rings lined up around it, rings that grow smaller as hight increases. There are two more pegs that are empty. The challenge is to move the rings to the center peg under the condition that a smaller ring may never be underneath a larger ring.

Assuming there are N rings, the trick is to take $n-1$ rings to the third peg, move the largest ring on the original ring to the second ring, then repeat until all rings are moved. If it takes h_n steps to move n rings, then it takes h_{n-1} steps to move $n-1$ rings. So, here are the steps:

1. Move n-1 rings from peg 1 to peg three in h_{n-1} steps.
2. Move the bottom ring from peg 1 to peg 2 in one step.
3. Move the $n-1$ rings on peg three to peg 2 in h_{n-1} steps.

This means that $h_n = 2hn - 1 + 1$ where h_n is the number of steps it takes to move all the rings to peg 2. Note that since this is a recurrence relation and recurrence relations require initial conditions, the initial conditions for Tower of Hanoi is $h_1 = 1$. If you're lucky, a regular formula can be derived from a recurrence relation. In this case, the formula is $2^n - 1$.

6.5.1 Solving Recurrence Relations

Recurrence relations may be viewed in the form of $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$. This is said to be a linear homogeneous recurrence relation because it is a linear combination and it is homogeneous. The goal, then, is to look for a solution of the form $a_n = r^n$ where R is a scalar. Why? Because we can.

$$\begin{aligned} c_1 r_{n-1} + \cdots + c_k r^{n-k} &= r_n \\ r^{n=k}(r_k - c_1 r^{k-1} - \cdots - c_k) &= 0 \\ r_k - c_1 r^{k-1} - \cdots - c_k &= 0 \end{aligned}$$

This is the characteristic equation with roots $r_1, r_2, \ldots, r_k$. It requires that if R is solution the equation must be satisfied.

Example 1 - Distinct Roots Something like this may happen: $a_n = 5a_{n-1} - 6a_{n-2}, a_0 = 1, a_1 = 1$. The characteristic equation is then $r^2 - 5r + 6 = 0$. Now just solve for the roots! Factoring this yields $r_1 = 3, r_2 = 2$. Solutions to this problem are then $r = 3^n$ and $r = 2^n$. The general solution is a linear combination of the two solutions, or $a_n = \alpha_1 3^n + \beta 2^n$ for some constants alpha and beta where $1 = a_0 = \alpha + \beta$ and $1 = a_1 = 3\alpha + 2\beta$. The actual solution is then $a_n = 2^{n+1} - 3^n$.

Example 2

$$\begin{aligned} a_n &= 5a_{n-1} - 6a_{n-2} \\ r^n &= 5r^{n-1} - 6r^{n=2} \\ 0 &= r^{n-2}(r^2 - 5r + 6) \end{aligned}$$

The above equation (the characteristic equation) must be satisfied if the equation is to be solved. Its roots are obviously just 3 and 2. Solutions are then 3^n and 2^n, but we also need a general solution that is a linear combintion of the two, in the form of $a_n = \alpha 3^n + \beta 2^n$.

$$\begin{aligned} n = 0 : 1 = a_0 &= \alpha + \beta \\ n = 1 : 1 = a_1 &= 3\alpha + 2\beta \end{aligned}$$

There are two solutions and two unknowns that must be solved for (α and β). After a little bit of algebra (not shown here), the result is $a_n = -(3^n) + 2(2^n)$ or just $a_n = 2^{n+1} - 3^n$.

Example 3 Find a formula for the nth Fibonacci number, where the relation is defined by $a_n = a_{n-1} + a_{n-2}, a_1 = 1, a_2 = 1$. The characteristic equation is just $r^2 - r - 1 = 0$. This equation does not factor nicely, so use the quadratic fomula to solve: $\frac{1+\sqrt{1+4}}{2}$. The roots are then $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$. The first is the golden ratio and the second is some variation of it, represented by ϕ and $\bar{\phi}$ repectively. To solve for a general relation, solve $f_n = \alpha\phi^n + \beta\bar{\phi}^n$. Take $n = 0$, yielding $f_0 = 0\ldots$

$$
\begin{aligned}
0 = f_0 &= \alpha + \beta \\
1 = f_1 &= \alpha\phi + \beta\bar{\phi} \\
0 &= \alpha\phi + \beta\phi \\
1 &= \beta(\bar{\phi} - \phi) \\
1 &= \beta(-\sqrt{5}) \\
\beta &= -\frac{1}{\sqrt{5}} \\
\alpha &= \frac{1}{\sqrt{5}} \\
f_n &= \frac{1}{\sqrt{5}}\phi^n - \frac{1}{\sqrt{5}}\bar{\phi}^n \\
&= \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n)
\end{aligned}
$$

7 Graph Theory

Graphs consist of vertices with edges between them. Graphs can represent many different things - for example, computers as the vertices and connections between them as the nodes. If two objects (vertices) are related, an edge is put between them; otherwise, there is no edge. The degree for any given vertex is the number of edges it has. The sum of the degrees is then just twice the number of edges.