The first month of class is about Proofs and Asymptotic Analysis. This will provide you with a set of tools to learn about formal algorithmic analysis, which will provide solid grounding about how best to implement them.

1 | What is an Algorithm?

- Recipe for doing something: a set of steps to solve a particular problem or questions
- Bad Algorithms…
  - are wrong
  - are wrong sometimes (on edge cases) — this is worse
  - are slow as hell
  - gets stuck and try to test the halting problem

2 | Utility of Proofs and Asymptotic Analysis

Proofs test whether or not an algorithm is mathematically correct (it won't be wrong). **Asymptotic analysis** test how long its going to take.

3 | Proofs by Example, Counterexample

This could only be used in specific times when the statements are worded correctly. For instance:

"All Taylor Swift songs are awesome."

This statement **cannot** be *proved* by example, but it **can** be *disproved* by counterexample. By thinking about one counter-example, we can show that not all Tayler Swift songs are awesome.

On the other hand:

"At least one Taylor Swift songs are awesome."

This statement **can** be *proved* by example, but it **cannot** be *disproved* by counterexample. By thinking about one example, we can show that one Tayler Swift song is awesome.

3.1 | Example 1

For all non-negative integers n,

$$n^2 + n + 41 \tag{1}$$

results in a prime number.

For $n = 40$, the result is *not* prime! We could see that this is false. Hence, how did this work?

1. To *disprove* some statement, find *one* counterexample
2. To *prove* some statement, prove for *all possible cases* by…

(a) Dividing into sub-cases, and proving each cases
(b) Prove exhaustively the space of cases

3.2 | **Example 2**

For any group of 6 statements, exists a group of exactly 3 students that are all friends with each other OR strangers with each other.

In any group of 6 individuals, take an individual, Paul. Paul, in a group of 6, has 5 relationships.

WLOG, say Paul is friends with all three of them. We could say WLOG because, say he is friends with only 2 out of his five relationships, then he will have 3 strangers and we just flip the proof. Vise versa.

- Case 1: exists at least 1 pair of friends in the group of 3
- Case 2: no pair of friends in the group of 3

For Case 1, Paul are friends with both people that are also given to be friends. Therefore, there exists a friendship group of 3.

Fore Case 2, though Paul friends with all three of them, the three are all strangers with each other. Therefore, there exists a strangership group of 3.

4 | **Proofs by Contradiction**

"Try something, and see if that works." If you try something, and it doesn't work, then you know that what you tried is wrong and the case is disproved.

1. State the proof is by contradiction
2. Assume the logical negation of the hypothesis is true
   (a) Formally state that the opposite is true
   (b) Its not always clear what the exactly the opposite case is
3. Work until you reach a contradiction: "because of the fact that we reached a contradiction with the assumption, it means that the assumption is false"

4.1 | **Example**

Proof that the $\sqrt{2}$ is irrational

The proof is by contradiction.

Assume, for the purposes of contradiction, that $\sqrt{2}$ is rational. By definition of rationality, a rational number can be expressed as a fraction, which is a ratio of two integers in lowest terms.

If $\sqrt{2}$ is rational, then we have some

$$\sqrt{2} = \frac{a}{b}, a, b \in \mathbb{I} \tag{2}$$

at the lowest terms a, b.

We will then perform some algebra:

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

By the fact that b^2 is multiplied by 2 to equate to a^2, we know that a^2 is even. We can't square an odd number to get an even number, so we know that a is even.

If a is even, we know that a could be written as some $a = 2k$. Therefore, we could claim that $2b^2 = (2k)^2$. Therefore:

- $2b^2 = 4k^2$
- $b^2 = 2k$

By the fact that k is multiplied by 2 to equate to b^2, we know that b^2 is even. We can't square an odd number to get an even number, so we know that b is even.

So a, b are both even. Yet, we defined a and b is the lowest terms, and there must exist something in the lowest, irreducible terms a and b to make a fraction. Yet, a and b, under our setup, is always divisible both by 2.

CONTRADICTION.

Therefore, $\sqrt{2}$ must be irrational.

5 | Proof by (Weak) Induction

Kind of a big deal. It's super powerful and the basis of most proofs.

We prove the base case, and prove the next statement is true given the first statement is true, and prove that any one statement proves the next state, we could prove the statement is true for the whole space.

1. State the proof is by induction
2. State your inductive hypothesis, $P(n) \rightarrow P(n+1)$. (This is often the same as what you are trying to prove.)
    - Show that, we aim to prove that, given one statement, the next is true
3. Prove your base case!
    - A lot of proofs goes wrong here
    - It some cases, we have more than one base case!
4. Assume $P(n)$ is true. Show this implies that $P(n+1)$.
5. Invoke the Principle of Induction! "By induction it must be true for all n"

5.1 | Example

Proof:

$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2} \tag{3}$$

1. The proof is by induction

2. $P(n)$ is, for all positive integers, $1+2+3+\ldots+n=\frac{n(n+1)}{2}$
3. Set our base case $n=1$.
4. $1=\frac{1(1+1)}{2}=1$, therefore, base case proven
5. Assume $P(n)$ is true, that $1+2+3+\ldots+n=\frac{n(n+1)}{2}$. To prove $P(n+1)$, we take $n=n+1$
   (a) Prove $1+2+3+\ldots+n+n+1=\frac{(n+1)(n+2)}{2}$
   (b) We know a fact about the first bit of this, that $1+2+3+\ldots+n=\frac{n(n+1)}{2}$, meaning we could say that: $\frac{n(n+1)}{2}+n+1=\frac{(n+1)(n+2)}{2}$
   (c) And now, we multiply $(n+1)$ by two and divide by two to have common denominators
   (d) $\frac{n(n+1)}{2}+\frac{2(n+1)}{2}=\frac{(n+1)(n+2)}{2}$
   (e) $\frac{(n+2)(n+1)}{2}=\frac{(n+1)(n+2)}{2}$, which is shown
6. By the inductive principle, we have proven the base cases and inductive step. It must be true for all n.

5.2 | Common Errors

1. The step right after base case does not induce ($P(0) \not\to P(1)$). This is usually not a problem with the inductive step, but instead is that $P(0)$ is not the right base case that could possibly lead to the next step.
2. The inductive step does not apply in some n. This is usually ($P(1) \not\to P(2)$)
3. Sometimes, we might need multiple base cases to be proven.

6 | Proof by (Strong) Induction

Weak induction's inductive step: show $P(n) \to P(n+1)$.

Strong induction' inductive step: show $[P(1), P(2), P(3), \ldots, P(n)] \to P(n+1)$

Everything else pretty much stays the same.

6.1 | Example

Proof:

Any group of students ≥ 12 can be split into groups of 4 and 5.

1. The proof is by strong induction
2. Set our base case $n=(12,13,14,15)$
3. Prove our base cases:
   (a) $P(12)=4+4+4$
   (b) $P(13)=4+4+5$
   (c) $P(14)=4+5+5$
   (d) $P(15)=5+5+5$

4. Inductive step: (weak induction can't work — knowing that a group can be split into 4,5 does not do anything to tell us about group+1). However! We do strong induction:
   (a) Assume $P(n-3)$ is true. We know that we could add $n+4$ to arrive $P(n+1)$ to build a group of 4. Therefore, if given $P(n-3)$, then $P(n+1)$ is true.
   (b) For every case $P(n>15)$, we can just $(n-3)$ and back-propergate until you get to one of the base cases
5. Induction!

7 | Mixing and Matching Proofs

7.1 | Proof by Casing Contradictions

Proof:

There are infinite number of positive prime numbers.

1. The proof is by contradiction
2. Assume for the purposes of contradiction that there is an finite number of prime numbers $p_1, p_2, p_3, \ldots, p_n = S$.
3. Consider the following number: $p_1 \times p_2 \times p_3 \cdots \times p_n + 1 = p'$. There are two cases:
   (a) Case 1: p' is prime => CONTRADICTION! all the primes are in S and $p' > p_n$
   (b) Case 2: p' is not prime => it must be divisible by some p_i, we could see that p' is not divisible for any of p_i as dividing by any prime values will result in ($p_1 \times \cdots p_{i-1} \times p_{i+1} \cdots \times p_n + \frac{1}{p_i}$), which is not an integer. CONTRADICTION
   (c) The two cases exhaustively cover the cases.
4. Therefore, our assumption must be false and we reached a contradiction

7.2 | Proof by Inducting Cases

Define: An *n-team tournament* is an event with n teams where each team plays every other team and either win or looses (no ties).

Proof:

In every n-team tournament, there is a chain of n teams such that T_1 beats T_2 beats T_3 … beats T_n.

1. The proof is by induction
2. $P(n)$ in every n-team tournament, there is a chain of n teams such that T_1 beats T_2 beats T_3 … beats T_n
3. Base cases
   (a) $P(2)$, T_1 beats T_2
   (b) $P(2)$, T_2 beats T_1
4. Inductive step: $P(n) : T_1 > T_2 > T_3 \ldots T_n$

(a) In an $P(n+1)$ team tournament, there is a chain of n teams beating each other, so here is now two cases

(b) Case 1: T_{n+1} beats someone

i. If $T_{n+1} > [T_1 > T_2, \ldots, T_n]$

ii. If $T_1 > T_{n+1} > [T_2, \ldots, T_n]$

iii. If $T_1 > T_2 > T_{n+1} > [T_3, \ldots, T_n]$

iv. We can continue this chain all the way down, we must slot them in somewhere. No matter where they slot in, we could create a chain of $n+1$ teams

(c) Case 2: T_{n+1} loses to everybody: then, they lost to T_n, so they would just go at the end of the chain

(d) The two cases exhaustively cover the cases.

5. Induction.