Introduction to Combinatorics
Lecture Notes

Ezra Guerrero
GuidEd by Stacy

August 5, 2025

Contents

Part I

Mini Unit 1

1 Why Proofs?

Mathematics is all about solving problems and searching for the truth. But, how can you be sure that you have solved a problem or found the truth? The way mathematicians have solved this is by writing **proofs**. Proofs lay out the steps needed to go **from** things we already know **to** some new statement that we want to show. Thus, the importance of proofs is that they guarantee that every step is logically sound; no lies are being told.

2 Sets of Numbers

In this section, we will talk about sets and numbers. These are the first mathematical objects for which we will write proofs.

2.1 Sets

Sets are one of the foundational blocks of formal mathematics. Simply put, we think of sets as collections of objects. An object that is part of our collection is called an **element** of the set. We care only about whether or not an object is an element of the set. We do not concern ourselves with giving the elements any ordering, nor do we allow the same element to be in the set more than once. Thus, we say that two sets are **equal** if they have exactly the same elements.

When writing sets explicitly, mathematicians use curly braces $\{\}$ and write the elements between the braces. For example, a mathematician would write the set containing the uppercase vowels as

$$\{A, E, I, O, U\}.$$

Suppose that we start with some set, which I will name S. What happens if we want to consider some elements of S, but not necessarily all of them? We can build a **subset**. A subset of S will be another set such that all the elements of the new set are also elements of S. For example, $\{A, E, O\}$ is a subset of the set $\{A, E, I, O, U\}$.

Warning! A common pitfall at this stage is confusing elements and subsets. An element is an object which belongs to the set. A subset is another set, which does not have to be an element of the original set. So, for example, A is an *element* of the set $\{A, E, I, O, U\}$, but $\{A\}$ (the set that contains A) is a *subset* of $\{A, E, I, O, U\}$.

2.2 Numbers

Sets are all well and good, but what are the sets that mathematicians work with the most? Our next example of a set is one of the most important: the **empty set**. The empty set is the set that contains no elements. This set is so important that mathematicians have a special symbol for it: $\emptyset$. The empty set is important for many reasons. For example, the empty set is a subset of every set. We will discuss this more in Section 3.2.

Now, we will discuss some more interesting sets that are actually non-empty. We are all familiar with the numbers $0, 1, 2, 3$, and so on. These are the numbers that we use to count. As you will soon learn, counting is the foundation of combinatorics, and knowing how to count is the most important skill to tackle combinatorics problems. So, it is no surprise that the set that contains the numbers we use to count is very important. This set is called the set of **natural numbers**, and contains $0, 1, 2, 3$, and so on to infinity.

If to this set we also add the *negative* numbers $-1, -2, -3$, and so on, we obtain the set of **integers**. This set contains all natural numbers and their negatives. In particular, notice that every natural number is also an integer. So, the set of natural numbers is a subset of the set of integers[1].

We can keep going! If we now add all numbers that can be written as a quotient of integers, we get the **rational numbers**. This set contains all integers and numbers of the form a/b, where both a and b are integers. Similarly to before, we can see that the set of integers is a subset of the set of rationals.

Finally, if we consider all numbers, fractions or not, we get the set of **real numbers**. These are all the numbers in the real number line. It contains all the rationals and also numbers such as π and e. The real numbers that are not rational numbers are called **irrational numbers**. Again, we see that the set of rational numbers isa subset of the set of real numbers.

In summary, we talked about the empty set, the naturals, the integers, the rationals, and the reals. Furthermore, these sets satisfy that

$$\begin{aligned} \emptyset \quad \text{is a subset of} \quad \substack{\text{the set of}\\ \text{natural numbers}} \quad \text{is a subset of} \quad \substack{\text{the set of}\\ \text{integers}} \\ \substack{\text{the set of}\\ \text{integers}} \quad \text{is a subset of} \quad \substack{\text{the set of}\\ \text{rational numbers}} \quad \text{is a subset of} \quad \substack{\text{the set of}\\ \text{real numbers}} \end{aligned} \tag{1}$$

3 Mathematical Statements

In this section we discuss mathematical statements, the things we write proofs for.

3.1 Axioms and Definitions

A mathematical statement is a statement saying something about mathematical objects. We have already encountered several mathematical statements. Here are some examples:

Example 1

The following are all mathematical statements:

(a) There is a set with no elements, called the empty set.

(b) The set of natural numbers is the set whose elements are $0, 1, 2, 3$, and so on.

(c) If a and b are integers, then a/b is an element of the set of rational numbers.

(d) The empty set is a subset of every set.

Now, as mathematicians, we are in search of **true** mathematical statements. All three statements above certainly seem to be true, but how can we know for sure? Remember, this is why we write proofs, to confidently say that things are true. In order to show some *new* statement is true, we must start with some other statement we *know* is true, and somehow deduce the new one. However, how did we know that other statement was true in the first place? To know this, we must have started with another statement that we knew was true to deduce this one. Continuing like this is unfeasible, so we need some statements that we declare to be true without further justification. These are **axioms**; statements that we declare to be true and can use without further justification. For example, consider statement (a) in Example 1. It certainly seems intuitive that we can talk about a set that has nothing in it. How could we possibly go about showing this? We do not have to! Mathematicians have declared this to be an axiom, so you can use that the empty set exists without proof.

[1] You just encountered your first proof

Warning! When actually writing down proofs, you generally do not have to go all the way down to the axioms. For example, the fact that $1 + 1 = 2$ is not an axiom, and it in fact has a proof that is hundreds of pages long. Does this mean that you should prove $1 + 1 = 2$ any time you want to use it in this course? No! All of us here know that $1 + 1 = 2$, so we can treat it as an axiom and use it without proof. This is generally the game when writing down proofs: we have to figure out when we have reduced things to statements that we all agree are true.

In a similar spirit to axioms, we have **definitions**. Definitions are mathematical statements in which we declare that some object has certain properties. For example, Section 2.2 is full of definitions. We *defined* the set of natural numbers to be the set that contains the numbers $0, 1, 2, 3$, and so on. Thus, statement (b) in Example 1 is a definition.

We also use definitions to prove statements. For example, look at statement (c) in Example 1. How can we prove it? We want to say something about the set of rational numbers, so we should go to its definition. From Section 2.2, we recall that the set of rational numbers is *defined* to contain all numbers of the form a/b where both a and b are integers. Since statement (c) starts with this assumption, it follows that it is true by the definition of rational numbers!

3.2 Theorems and Lemmas

If the only statements math had were axioms and definitions, then it would be very boring. Mathematicians are interested in showing important statements that are not as obvious as axioms. Such important statements are called **theorems** or **lemmas**. The distinction between theorems and lemmas is not super clear cut. What one mathematician may call a lemma, another could call a theorem. Generally, theorems are the most important statements we are trying to show. On the other hand, lemmas are statements that we use to prove theorems. They are stepping stools to get to our main result. Whether to call a statement a lemma or a theorem depends on what your end goal is. If the goal is to prove that statement, then usually we would call it a theorem. If the goal is to use the statement as a step in the proof of something else, then perhaps calling it a lemma is better. In any case, do not fixate too much on the difference, the more you encounter these words, the clearer their use will become.

As practice of everything we have discussed, we will prove statement (d) in Example 1:

Theorem 1: Empty Set is always a Subset

The empty set is a subset of every set.

Proof. Recall the definition of a subset: A set is a subset of another set S if every element of the set is also an element of S. Now, recall the definition of the empty set: The empty set is the set with no elements. Since the empty set has no elements, it is *vacuously* true that all of its elements are elements of the other set; it does not have any elements! Thus, the empty set always satisfies the definition of subset, so it is a subset of every set. $\square$

If this argument was confusing, the idea of vacuous truths will be expanded on in Section 6.2.

4 Mathematical Notation

Mathematicians, above all, are lazy. You may have noticed that these lecture notes have been very wordy, containing phrases such as "the set of natural numbers is s subset of the set of real numbers". Since we do not like to write a lot, mathematicians have created several **notations** to help us save space and effort, reducing wordiness in our proofs and making things more concise. We already encountered some pieces of notation before. We discovered that $\{\}$ is the notation we use to denote sets. We also discussed the notation $\emptyset$ for the empty set. In this section we introduce more notation.

Let S and T be sets and a be some object. Do not be scared by the use of letters, these are just place-holder names we use to talk about things more generally, instead of just using specific examples.

If a is an element of S, we say that a is *in* S or that S *contains* a. The notation for this is $a \in S$ or $S \ni a$. If a is not an element of S, we write $a \notin S$. For example, $1 \in \{0, 1, 2\}$ but $3 \notin \{0, 1, 2\}$.
If S and T are equal, we write $S = T$. If S is a subset of T, we write $S \subseteq T$ or $T \supseteq S$. For example, $\emptyset \subseteq \{1, 2, 3, 4\}$ and $\{1, 2\} \supseteq \{1\}$.

We also have notation for the number sets we introduced earlier. We denote the natural numbers by $\mathbb{N}$, the integers by $\mathbb{Z}$, the rational numbers by $\mathbb{Q}$, and the real numbers by $\mathbb{R}$. Thus, we can rewrite the long sentence (1) from Section 2.2 as

$$\emptyset \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}. \tag{2}$$

Look at how much nicer that is!

Sometimes, our statements will be of the form "for all x, y holds" or "there exists some x such that y holds". Since these types of statements occur frequently, we also have notation for the phrases "for all" and "there exists". We write for all as $\forall$ and there exists as $\exists$. For example, we can rewrite some of our statements about the empty set using this notation:

Example 2

- (Axiom) $\exists$ a set that contains no elements.
- (Theorem) $\forall$ sets S, we have $\emptyset \subseteq S$.

Warning! The purpose of notation is to make your writing more clear and concise. Do not use choose to use notation at the expense of clarity. For example, even though we can write the empty set axiom using notation as above, it is perhaps clearer to just write it out in full in English. The most important thing about writing proofs is to communicate your ideas across effectively. Notation helps with this, but only if it is not abused too much.

5 Logic

How do we actually go from known statements to new ones? In order to do this, we use logic.

5.1 Propositions

Propositions are stand-alone statements that can be **True** or **False**. For example, *"it will rain today"* is a proposition. It is true if it will rain today, and it is false if it will not.

We can create new propositions using certain logical operations. Our first operation is **negation**. It gives a proposition that is true exactly when the original proposition is false. For example, the negation of *"it will rain today"* is *"it will not rain today"*. Abstractly, if P is an arbitrary proposition, we write $\neg P$ for its negation. These are useful for proofs, as perhaps it is easier to show that P is true (resp. false) by showing that $\neg P$ is false (resp. true).
Our next operation is **conjunction**, more commonly called "and". Given two propositions P, Q, their conjunction $P \wedge Q$ is true if both P and Q are true, and false otherwise. For example, the conjunction of *"it will rain today"* and *"tomorrow will be sunny"* is the proposition *"it will rain today and tomorrow will be sunny"*.
Similarly, we can define **disjunction**, more commonly called "or". The disjunction $P \vee Q$ of P and Q is true if either P or Q are true, and false if both of them are false.

We can summarize these definitions using a truth table. A truth table lists the possible truth values of each proposition and the resulting operation. So far, our operations follow the following truth table:

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$
T	T	F	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	F

Our next logical building blocks give us the mathematical tools to move from known statements to new ones. Given two propositions P and Q, the proposition $P \implies Q$, read "P implies Q", is true if P being true means Q is true as well. That is, if $P \implies Q$ is true and we know that P is true, we can justifiably conclude that Q is true. We usually get propositions of the type $P \implies Q$ from definitions. For example, the definition of $\mathbb{Q}$ gives us:

$$a, b \in \mathbb{Z} \implies a/b \in \mathbb{Q}.$$

Hence, we can show that $2/3$ is a rational number from this. We know that 2 and 3 are integers and we know that the above implication is true by definition. Thus, we can justifiably conclude that $2/3$ is rational. Given two propositions P and Q, the proposition $P \iff Q$, read "P is equivalent to Q" or "P if and only if Q", is true if P and Q have the same truth value. That is, if we know $P \iff Q$ is true, then P being true means Q is true and P being false means Q is false. In fact, definitions are usually equivalences. The definition of $\mathbb{N}$ tells us that

$$a \in \mathbb{N} \iff a = 0, 1, 2, 3, \ldots$$

The truth tables of $\implies$ and $\iff$ are as follows:

P	Q	$P \implies Q$	$P \iff Q$
T	T	T	T
T	F	F	F
F	T	T	F
F	F	T	T

5.2 The Contrapositive

The power of thinking about statements in this framework is that we only care about their truth values. If two statements are **equivalent**, that is, $P \iff Q$, then we treat them as the same statement. This is great, as it allows us to change our problem to something we perhaps already know. For example, say we want to show Q and we know that $P \implies Q$ is true. Then, it suffices to show that P is true, so we have essentially changed our proof of Q into a proof of P, which is hopefully a simpler problem. This technique makes a lot of sense intuitively, and we can use our truth table framework to show why it works. Consider the truth table of $((P \implies Q) \wedge P) \implies Q$:

P	Q	$(P \implies Q) \wedge P$	$((P \implies Q) \wedge P) \implies Q$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

Notice how $((P \implies Q) \wedge P) \implies Q$ is always true[2]! This is our indication that we can use this bit of logic in our proof!

[2] A proposition that is always true is called a **tautology**.

There is another common technique we can use to change our problem into a simpler one. Suppose we want to prove the statement $P \implies Q$. The **contrapositive** of this statement is the statement $\neg Q \implies \neg P$. It turns out that $P \implies Q$ and its contrapositive are equivalent. Thus, if we want to show $P \implies Q$ is true, it suffices to show its contrapositive is true. We can use truth tables to understand why this works:

P	Q	$P \implies Q$	$\neg Q \implies \neg P$	$(P \implies Q) \iff (\neg Q \implies \neg P)$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

Again, observe how $(P \implies Q) \iff (\neg Q \implies \neg P)$ is always true. Hence, if we want to show an implication, we can equivalently show its contrapositive.

If you are ever unsure if a bit of logic in your proof is valid, you can always write down a truth table and check!

6 Quantifiers

In Section 4 we introduced $\forall$ and $\exists$. These symbols are unique as they allow us to build a statement that talks generally about the contents of a set rather than about the set itself. For this reason, we call them **quantifiers**; they talk about the quantity of elements in a set that satisfy some property.

6.1 Free and Bound Variables

When stating propositions with quantifiers, we will unavoidably need to use **variables**. Quantifiers allow us to range over elements of a set, so in order to represent said elements, we need a variable that represents them. When a proposition uses variables, we write that dependence using parentheses. For example, if a proposition P has one variable x, then we denote it by $P(x)$.

Example 3

The following are all propositions using (possibly no) variables:

(1) $P \colon \emptyset \subseteq \mathbb{N}$

(2) $Q(x) \colon x \in \mathbb{Q} \implies x \in \mathbb{Z}$;

(3) $R(x) \colon x \in \mathbb{Z} \implies x \in \mathbb{Q}$;

(4) $S \colon \forall x \in \mathbb{R}, (x \in \mathbb{Z} \implies (x+1) \in \mathbb{Z})$;

(5) $T(y) \colon \exists x \in \mathbb{N}.(y \in \mathbb{Q} \implies (x \cdot y) \in \mathbb{Z})$.

The keen reader may notice that something suspicious is going on. Last time, we said that propositions are either true or false. However, what happens when a proposition has variables? For example, consider $Q(x)$. When x is an integer, it is certainly true that $x \in \mathbb{Q}$ implies $x \in \mathbb{Z}$, as $x \in \mathbb{Z}$ is already true. However, if x is a number like $1/2$, then $x \in \mathbb{Q}$ but $x \notin \mathbb{Z}$, so the implication is false. So, what should the truth value of $Q(x)$ be? Should it be true since **there exists** one x for which it is true? Or should it be false since it does not hold true **for all** values of x?
You may have also noticed that S and $T(y)$ involve more variables than suggested by the name. We have written S without stating any dependence, but its formula involves x. Similarly, $T(y)$ is written as only

depending on y, while its formula includes both x and y.

To understand both of these issues, it is crucial to understand the difference between **free** and **bound** variables. When we include a variable in a proposition, it starts out initially as free. However, if we add a quantifier that uses that variable in front of our expression, the variable now becomes bound. When giving a name to a proposition, we write in parentheses exactly the variables that are free. This is because the proposition does not really depend on the bound variables! Once we have added a quantifier, we do not have a choice on what to do with the variable.
When a proposition has no free variables, it makes sense to talk about its truth value. If it has at least one free variable, then its truth value can depend on what value that variable takes on. Thus, we cannot assign $Q(x)$ a single truth value. However, if we bind its free variable, we get new propositions whose truth values we can talk about. In particular, $\exists x \in \mathbb{Q}.Q(x)$ is true, while $\forall x \in \mathbb{Q}, Q(x)$ is false.

Warning! Just because propositions with free variables have no well-defined truth value does not mean they are not useful or interesting. For example, a lot of problems take on the form of finding all values of x such that $P(x)$ is true! For such problems, it is often the case that $\forall x, P(x)$ is false and $\exists x.P(x)$ is true. But, the interesting question about the problem is exactly which x make this happen.

6.2 Domain of Quantification

When dealing with quantifiers, it is important to specify the **domain** over which we are quantifying. In other words, we have to agree on what the set that the variable ranges over actually is. Usually, the way we will do this is by explicitly writing the set in our notation: $\forall x \in S$ means we are quantifying over all elements of the set S. In cases where the domain of quantification is understood or not relevant to the discussion, we will often omit it. However, it is important to not forget it.

To see the importance of the domain of quantification, consider the following proposition:

$$\exists x.(0 < x < 1).$$

This is a very innocent looking statement, but what is its truth value? It depends on what values we are allowed to quantify over. If we quantify over real numbers, then the statement is definitely true, but if we quantify over integers, it is certainly false! Thus, we see that truth values can depend on our domain. Hence, we should not forget to include it explicitly if it is not clear what it should be.

Warning! One domain of quantification that can lend itself to confusion is the empty set! What does it mean to say $\forall x \in \emptyset$ or $\exists x \in \emptyset$? This is a weird question, but mathematicians have agreed on an answer. We declare that $\forall x \in \emptyset, P(x)$ is always true, and we call this situation a **vacuous truth**. The reasoning is that since $\emptyset$ has no elements, there is no x we can choose to make $P(x)$ false. So, we say that $\forall x \in \emptyset P(x)$ holds true vacuously. Similarly, we declare that $\exists x \in \emptyset.P(x)$ is always false. In this situation, there is no x we can choose to make $P(x)$ true, since there do not exist any $x \in \emptyset$.
Do not worry too much about this, as it is mostly a formal technicality. But, vacuous truths do show up from time to time, so it is worthwhile to justify to yourself why they should indeed be true.

6.3 The $\forall - \exists$ Duality

At first glance, the quantifiers $\forall$ and $\exists$ talk about two seemingly very unrelated quantities. “For all” asks whether a property holds for every single element of the set, while “exists” asks whether the property holds for at least one. However, it turns out that these two quantifiers are very similar under the hood. In fact, we can turn any instance of $\forall$ into a statement using just $\exists$s. We now show how this works:

Lemma 1: Duality

The following pairs of statements are equivalent:

- $\forall x \in S, P(x)$ is equivalent to $\neg(\exists x \in S.\neg P(x))$;
- $\exists x \in S.P(x)$ is equivalent to $\neg(\forall x \in S, \neg P(x))$.

Proof. Once we translate the symbols into English, this result is actually fairly intuitive! We start by breaking down the meaning of $\neg(\exists x \in S.\neg P(x))$. First, the statement $(\exists x \in S.\neg P(x))$ is true if and only if we can find some $x \in S$ such that $\neg P(x)$ holds. Put another way, it is true if and only if we can find some x such that $P(x)$ does not hold. However, if we can find such an x, that means that $P(x)$ does not hold for all $x \in S$! Thus, when we add the negation to the whole statement, we are saying that there does not exist an x such that $P(x)$ does not hold, i.e., for all $x \in S$, $P(x)$ must hold. This establishes the first equivalence. Showing the second equivalence is analogous to the first, so we leave it as an exercise for the reader to practice these trains of thought. $\square$

Once we have internalized what this duality is telling us, this lemma should become more intuitive. Essentially, each statement gives a different way of thinking about the quantifier; one way thinks about how things go right, while the other examines how things can go wrong. This is a very valuable way to think about approaching math problems. Usually, we can try to attack a problem in several ways. Sometimes a more fruitful approach will be to approach the problem directly, trying to see what things go right and how we can move forward from there. Other times, the more fruitful approach will be to attempt to try to make things go wrong, which can end up illustrating why the statement is true in the first place. This dichotomy in how to approach problems is similar to the duality discussed in this section. We will talk more about these approaches in Section 8.2.

This type of duality is more common in logic than one might initially think. As an exercise, try to show the following duality between disjunctions ($\wedge$) and conjunctions ($\vee$):

Lemma 2: De Morgan's Laws

The following pairs of statements are equivalent:

- $P \wedge Q$ is equivalent to $\neg(\neg P \vee \neg Q)$;
- $P \vee Q$ is equivalent to $\neg(\neg P \wedge \neg Q)$.

7 Proofs by (Counter)Example

In this section we talk about (dis)proving statements by (counter)example. This is one of the easiest ways to prove things, but it is also one of the easiest ways to write a proof that does not actually work!

7.1 Proof by Example

Proving things by example is probably one of the most intuitive proof techniques at our disposal. However, it is important to understand its limitations, as an incorrect proof by example is unsalvageable. If we want to prove a statement of the form $\exists x \in S.P(x)$, then it suffices to find one example $x \in S$ such that $P(x)$ is true. This is essentially the definition of $\exists$.

Example 4

Prove the following statements:

(1) $\exists n \in \mathbb{Z}.(n^2 - 5n + 6 = 0)$;

(2) $\exists q \in \mathbb{Q}.(100(q-1) \notin \mathbb{N} \wedge 100q \in \mathbb{N})$;

(3) $\forall x \in \mathbb{R}, x/3 \in \mathbb{Q}$.

Proof of (1). Consider $n = 3$. Since $3^2 - 5 \cdot 3 + 6 = 9 - 15 + 6 = 0$, we have exhibited an example $n \in \mathbb{Z}$ such that $n^2 - 5n + 6 = 0$. Hence, the statement is true. $\square$

Proof of (2). Consider $q = 99/100$. Observe that $100(99/100 - 1) = -1$, which is not in $\mathbb{N}$ since it is negative. Furthermore, $100q = 99$, which is in $\mathbb{N}$. Therefore, we have exhibited an example $q \in \mathbb{Q}$ such that $100(q-1) \notin \mathbb{N}$ and $100q \in \mathbb{N}$, so the statement is true. $\square$

Bogus Proof of (3). Consider $x = 1$. Since $1/3 \in \mathbb{Q}$, we have exhibited an example $x \in \mathbb{R}$ such that $x/3 \in \mathbb{Q}$, so the statement is true. $\square$

The proofs of statements (1) and (2) are completely valid. However, something is off with statement (3). In fact, statement (3) is false, so there must be something wrong with our proof. What is the problem? The problem is that proofs by example *only* work if we are working with $\exists$. As soon as our quantifier is $\forall$, a proof by example is completely bogus! This should make sense; if I ask you to prove there exists a brown dog and you show me one, I will be satisfied by your proof. However, if I want proof that *every* dog is brown, I should not be satisfied if you only show me a brown dog, as this gives no information about every other dog[3].

The moral of the story is that you should be careful with examples! If your whole proof is presenting one example where the statement holds, make sure that this is enough to prove the problem. Proofs by example only work if you have $\exists$, as $\exists$ essentially asks for an example. If you are working with $\forall$, proofs by example are completely invalid and you have to do more work.

7.2 Disproof by Counterexample

Does this mean that $\exists$ is somehow simpler than $\forall$? Not exactly! Just as we often try to prove statements, we also want to disprove statements sometimes. At the level of logic, proving and disproving are exactly the same thing: disproving P is the same as proving $\neg P$ and vice-versa. In light of the $\forall - \exists$ duality from section 6.3, it is hopefully not too surprising then that it is simple to disprove $\forall$ statements and more involved to disprove $\exists$ statements.

Explicitly, if we want to show that $\forall x \in S, P(x)$ is false, the it suffices to find one example $x \in S$ such that $P(x)$ is false. We usually call examples that show something is false **counterexamples**, to emphasize that they are falsifying the statement. Thus, just like to prove an $\exists$ statement we just have to give an example, to disprove a $\forall$ statement we just have to give a counterexample.

Example 5

Disprove the following statements:

(1) $\forall x \in \mathbb{R}, x/3 \in \mathbb{Q}$;

(2) $\forall a \in \mathbb{N}, a/2 \in \mathbb{N}$;

(3) $\exists n \in \mathbb{Z}.(n^2 - 5n + 6 = 0)$.

[3] In fact, I have non-brown dogs back home.

Proof of (1). Consider $x = 3\pi$. Since $3\pi/3 = \pi$ is irrational, 3π is a counterexample to the statement, showing it is false. $\square$

Proof of (2). Consider $a = 1$. Since $1/2$ is not a natural number, 1 is a counterexample to the statement, showing it is false. $\square$

Bogus proof of (3). Consider $n = 0$. Since $0^2 - 5\cdot 0 + 6 = 6$ is nonzero, 0 is a counterexample to the statement, showing it is false. $\square$

Again, the proofs for statements (1) and (2) are completely valid, but the proof for statement (3) is incorrect. In fact, we already showed statement (3) is true in section 7.1. The problem lies in that we cannot disprove an $\exists$ statement using a single counterexample. This should also make sense; if I ask you to disprove that every dog is brown, you just have to show me a non-brown dog. But, if I ask you to disprove that there exists a brown dog, showing me a non-brown dog is not convincing, as it does not tell me anything about whether any other dog is brown.

These last two sections hopefully sound very similar. This is for good reason! The duality between our quantifiers tells us that, in some sense, a disproof by counterexample is the same as a proof by example, and vice-versa. Explicitly, to show $\forall x, P(x)$ is false, we want to show $\neg(\forall x, P(x))$ is true. Now, Lemma 1 tells us that $\neg(\forall x, P(x))$ is equivalent to $\exists x \in S. \neg P(x)$. We know that to prove an $\exists$ statement, it suffices to provide an example. An example for this statement is an $x \in S$ such that $\neg P(x)$ is true, that is, such that $P(x)$ is false. Hence, an example of $\neg P(x)$ is a counterexample of $P(x)$. This shows mathematically how these two types of proofs are secretly the same. The differences arise in how we think about the problem.

8 Proof by Contradiction

In this section we talk about soundness and proofs by contradiction.

8.1 Soundness

So far, we have developed a system to talk about mathematical statements and how to prove them. It would be right to wonder at this point if any of this makes sense. How can we be sure that the system we have set up does not allow for contradictory statements to be proven true? How can we guarantee that we cannot have two correct proofs, one showing a statement is true and one showing it is false? A system in which one cannot derive a false statement starting from a true one is called **sound**. We would certainly hope that mathematics is sound. However, as Gödel showed in 1931, we cannot prove starting from our axioms that these axioms do not reach contradictions. This may concern you, but do not be worried that mathematics is meaningless. Mathematicians have worked very hard to choose the axioms we start with and we have very good reason to believe that mathematics is sound. Nevertheless, it is my duty to inform you that we in fact have no proof.

That said, for the rest of this course we will assume that mathematics is sound. I advice you to follow this assumption for the rest of your life. So, if we start from a true statement and follow a valid train of logic, there is no way that we prove a false statement. In other words, true statements can only imply true statements. This certainly sounds reasonable, and we can sleep well at night assuming it.

8.2 Contradiction

That mathematics is sound allows us to use one of the most useful proof techniques mathematicians have devised: contradiction. As we just said, contradictions cannot occur in mathematics. This means that if we somehow show something false, one of our starting assumptions must be false. This is really powerful, as it gives us a way to prove things are false. Thus, a shift in perspective allows us to prove statements are true.

A true statement cannot imply a false one. Thus, if a statement implies something false, it must have been false to start with. Say we want to prove some statement, call it P, is true. In order to apply our observation above, we switch our perspective a little: instead of showing P is true, we will show that $\neg P$ is false. Thus, we start with the assumption that P is false. Then, we follow valid steps of logic to prove some statement we know is false. Since a true statement cannot imply a false one, this will mean that P cannot be false, so it must be true.

The idea behind this proof technique will become clearer with examples.

Theorem 2: Infinitude of primes

Prove that there are infinitely many primes.

Proof. Trying to show that there are infinitely many primes directly sounds complicated. However, we know how to work with the assumption that something is finite pretty well. This suggests contradiction will be a good idea.
Assume for the sake of contradiction that there are finitely many primes. Let $p_1, p_2, \ldots, p_n$ be the finite list of all primes. Now, consider the number $P = p_1 p_2 \cdots p_n + 1$. Since P is greater than 1, it must have prime divisors. This means that one of $p_1, \ldots, p_n$ must divide P evenly, since these are all the primes. However, observe that P/p_k is not an integer for any of the primes p_k. Therefore, none of the primes divide P evenly. This is not possible, so we have reached a contradiction. Therefore, our initial assumption that there are finitely many primes must be incorrect, so there are infinitely many primes. $\square$

Generally, proofs by contradiction work well when it is easy to explore how things can go wrong. In the problem above, it is not straightforward to think about how to show there are infinitely many primes. However, it is way more manageable to think about what would happen if there are finitely many primes. If there are finitely many, we can look at all of them and try to do things. Playing around we land on some number that cannot exist, which gives us the desired contradiction.

These kinds of situations work well with contradiction in general. For example, say you want to show $x \notin S$ for some specific x and some particular S that you have defined. Then, perhaps it is easier to start with the assumption that $x \in S$. Then, use the definitions of x and S to get some contradiction and be able to conclude what you wanted to show in the first place.

Proofs by contradiction will show up in this course frequently. As you get more experience with it, this technique will become second nature and you will be able to add it to your arsenal to tackle problems.

9 Philosophy

In this section, I talk about life and dramatically introduce induction. If you want to continue the math, go to section 10.

In section 8 we introduced proofs by contradiction. In these notes we will introduce arguably the most important proof technique for your mathematical journeys: induction. If this is your first introduction to induction, I am pleased to tell you that your life will irreversibly change for the better after learning it. I am not exaggerating when I say that if you study mathematics, you will use some type of induction for the rest of your life. It is undoubtedly one of the most useful and powerful proof techniques we have to our disposal.

Before introducing the concept, I want to give some thoughts about life:
Often in math class we hear the infamous question "Why is this useful?". Although knowing the Pythagorean theorem or the specifics of how to factor polynomials does not sound useful if you want to do things that do not involve triangles or polynomials, I think there is still usefulness to all we learn in math classes. Mathematics, at the end of the day, is about solving problems. In math class, we tackle specific problems. We work with fractions, triangles, linear equations, conic sections, matrices, calculus, etc. The most useful thing about math classes is not the specific problems that we solve, but rather the strategies that we learn to solve

said problems.

Real life has a lot of problems for us to solve. Although these problems are usually not about Gaussian elimination or the quadratic formula, what we have learned in math classes can help us tackle these problems[4]. When we were little, we were tasked with memorizing multiplication tables. We did not now it then, but this was one of our first problem solving techniques. Take a moment to think about how many problems you have solved by memorizing. In middle school, we were introduced to variables. We all complained that letters had invaded math! But, variables taught us about generalizing. Now we can talk about things more abstractly and refer to unknowns. Last time, we showed how to disprove things by counterexample. Take a moment to think about how many times one of your friends told you something that sounded false, so you disproved them with a counterexample. Maybe it was about some mechanic in a video-game, or maybe they told you there was no homework due tomorrow.

My message here is not that math gives you the recipe to solve all your problems. Real life is more complicated than mathematics. However, you should remember that math is about solving problems, and every problem you solve makes you a better problem solver. I do not think you will ever use induction to resolve a fight in your friend group. What I do know is that learning induction will make you a better mathematician. Being a better mathematician means being better at solving problems. And, hopefully, being better at solving problems makes your life better. Now, let us get on with the math.

10 Mathematical Induction

In this section we do all things induction.

10.1 Toppling Dominoes

The technique of mathematical induction is often compared to a long line of dominoes. We, the mathematicians, start by toppling the first domino in the line and each subsequent domino topples one by one until every domino has fallen. We use induction when we want to prove that some statement holds for every natural number. Thus, induction is our first technique allowing us to directly prove a $\forall$ statement is true. Our toy problem to show induction is the following:

Lemma 3: Powers of 2

Let n be a natural number. Then,

$$1 + 2 + 4 + \dots 2^n = 2^{n+1} - 1.$$

This lemma tells us that there is a simple formula for the sum of the first powers of two. This is a remarkable result that you will probably use often!

Now, for this problem it is not difficult to verify that the equation holds for any specific value of n. For example, for $n = 3$ we find that $1+2+4+8 = 15$ and $2^4-1 = 15$. However, as we discussed last time, a proof by example is invalid in this case. We have to show that this holds for every single natural number, not just one. The power of induction is that, after some work, we will essentially reduce the problem to a proof by example.

Here is the idea: We will show that the statement is true for some initial value of n, usually 0 or 1. Showing the problem is true for the initial value is the **base case** of our induction and it is crucial we never forget it. The base case is like toppling the first domino in the line, if we never topple it, the rest of the dominoes will never fall. Once we have established our base case, we state our **inductive hypothesis**. For this step, we will assume that we know that the problem holds for some specific value of n. This is like

[4] Now, most real life issues are not math problems for which you can find a single correct solution. But, sometimes these ways of thinking can help us get a better grasp of what is in front of us.

assuming that the first n dominoes have fallen. Next, we show that the $(n+1)$th domino also falls. The final **inductive step** of the induction is to show that, assuming the statement is true for n (inductive hypothesis), we can show that the statement is true for $n+1$.
If we follow these three steps, we will have a complete and correct proof by induction. To understand why it works, think about the dominoes. Our base case starts off the motion, and the inductive hypothesis and inductive step keep toppling the dominoes to the end. Since we know the statement is true when $n = 0$, the inductive step tells us it is true for $n = 1$. Now, we know the statement is true for $n = 1$, so the inductive step tells us it is true for $n = 2$, then $n = 3$, then $n = 4$, and so on.

It is crucial to have all three steps in an induction proof. Not showing the base case is like never toppling the first domino. Not specifying the inductive hypothesis is like having a domino missing from the line. Failing to prove the inductive step is as if a domino falls but does not hit the next one in line. In any case, not all dominoes topple and our proof is incorrect. So, let's summarize all three steps:

Proof by Induction

To successfully prove a statement is true for all $n = 0, 1, 2, \ldots$, we can follow these steps:

(1) **Base Case**: We first prove that the statement is true for $n = 0$.

(2) **Inductive Hypothesis**: We now assume that the statement is true for n.

(3) **Inductive Step**: Finally, we show that assuming the inductive hypothesis, we can prove the statement is true for $n + 1$.

We are now ready to prove Lemma 3 using induction.

Proof. We proceed by induction.

(1) **Base Case**: We show that the formula is true for $n = 0$. When $n = 0$, the left hand side equals 1 and the right hand side equals $2^1 - 1 = 1$. Since $1 = 1$, we have established our base case.

(2) **Inductive Hypothesis**: We assume that the statement holds for n. That is, we assume that

$$1 + 2 + \ldots + 2^n = 2^{n+1} - 1.$$

(3) **Inductive Step**: We now show that the statement is true for $n + 1$. That is, we want to prove that

$$1 + 2 + \ldots + 2^n + 2^{n+1} = 2^{n+2} - 1.$$

Observe that

$$\begin{aligned} 1 + 2 + \ldots + 2^n + 2^{n+1} &= (1 + 2 + \ldots + 2^n) + 2^{n+1} \\ &= (2^{n+1} - 1) + 2^{n+1} \\ &= (2^{n+1} + 2^{n+1}) - 1 \\ &= 2^{n+2} - 1, \end{aligned}$$

where we have used the inductive hypothesis to get the second line. This proves the inductive step, concluding the induction.

Thus, we conclude the statement is true for all natural numbers n. □

You may have noticed that the inductive step is the most involved step. This is usually the case with induction proofs. Just like with a line of dominoes the hardest part is aligning them so they keep falling, the hardest part of an induction hypothesis is showing the inductive step is true.

10.2 Horses

Hopefully sections 6.3, 7.2, and 8.2 have convinced you that sometimes the best way to understand something is to try to understand how it fails. Following this philosophy, we look at a completely bogus proof that seems to use induction. By understanding how things go wrong in this proof, we hope to enlighten how induction works and prevent its incorrect use.

Theorem 3: Monochromatic Horses

Let n be a positive integer. In every group of n horses, all horses are the same color.

Bogus Proof. We proceed by induction.

(1) **Base Case**: We show the statement is true for $n = 1$. Indeed, in every group of 1 horse, all horses have the same color, the color of the horse. This establishes our base case.

(2) **Inductive Hypothesis**: Suppose the statement holds for n. That is, in every group of n horses, all horses are the same color.

(3) **Inductive Step**: We now show the statement is true for $n + 1$. Suppose we have a group of $n + 1$ horses. Call two different horses Allison and Bob. The group of horses without Allison has n horses, so by the inductive hypothesis they are all the same color. The group of horses without Bob has n horses, so by the inductive hypothesis they are all the same color. Thus, the other $n - 1$ horses are the same color, and this color is the same as Allison's and Bob's color, so all $n + 1$ horses have the same color. This proves the inductive step, concluding the induction.

Thus, we conclude that in every group of n horses, all horses are the same color. □

Not all horses in the world are the same color, so something has gone terribly wrong. Does induction not work? Is mathematics inconsistent? Luckily, none of these is the issue. There is a mistake in our proof. Take a moment to try to spot it.

To find it, let's try to topple all the dominoes. The problem is not in our base case, as it is true that in every group of 1 horse, they all have the same color. So, let's try to use the inductive step to go to 2 horses. Since the theorem is not true for $n = 2$, hopefully this will show us what the mistake is! We have two horses, Allison and Bob. It is indeed true that the horses in the group without Allison are all the same color, and that this color is Bob's. After all, Bob is the only horse in the group without Allison. We can say something similar about the group without Bob. The problem then, is how we conclude that Allison's and Bob's color is the same! To do so, we talk about the "other" horses that are both in the group without Allison and the group without Bob. However, such horses do not exist for $n = 2$! Thus, our inductive step fails and mathematics is saved.

You may have noticed that the inductive step almost works. Is there perhaps some way to amend this and return chaos to mathematics? We know the inductive hypothesis works as long as we have more than 2 horses. Thus, one possible fix for our proof is to add $n = 2$ to our base case. If we do this, then we can start toppling our dominoes from $n = 2$ and our proof works. However, luckily for our horses, the case $n = 2$ is not true! It suffices to exhibit one pair of horses that are different colors to disprove it. So, lucky for us Theorem 3 remains false.
However, this idea can be useful for your proofs. If your inductive step works for all but some n, then you can still make your proof by induction work if you add those n to your base case. This is why it is important to include all three steps in your proof! All three contribute to a successful application of mathematical induction.

10.3 Strong Induction

Sometimes, our inductive hypothesis is not strong enough to complete the problem. If we think about our dominoes, we have toppled every domino up to n, but our inductive hypothesis is only using that the last domino has fallen. There is nothing stopping us from also using the information that previous dominoes have fallen. When we strengthen our inductive hypothesis to include more information, we usually call this **strong induction**. Really, the underlying idea is exactly the same, with the logic working out in exactly the same way. However, this name allows us to clearly communicate that our inductive hypothesis is assuming the statement holds for more values. Let us see this in action with some examples.

Theorem 4: Eating Chocolate

Let n be a positive integer. We have a $1 \times n$ chocolate bar, separated into 1×1 chocolate pieces. Every minute, we can eat any positive number of contiguous chocolate pieces from the left. There are 2^{n-1} ways to eat the chocolate bar.

For example, if we start with a 10×1 bar, the following are three different ways to eat it:

(a) The first minute we eat 7 pieces, leaving a 3×1 bar left over. The second minute we eat 2 pieces, leaving a 1×1 bar left over. The third minute we eat the last piece, finishing the bar.

(b) The first minute we eat 4 pieces, leaving a 6×1 bar left over. The second minute we eat the remaining 6 pieces, finishing the bar.

(c) The first minute we eat the whole bar.

The theorem is stating that, in this particular case, there are $2^9 = 512$ different ways to eat the bar. This seems hard to prove even for a specific n. Furthermore, using "weak" induction seems to be out of the picture, since depending on how many pieces we eat at the start, we end up with a differently sized bar. This is where strengthening our inductive hypothesis comes to the rescue.

Proof. We proceed by strong induction.

(1) **Base Case**: We show that the statement is true for $n = 1$. There is only one way to eat the bar: in the first minute we must eat the whole bar. Since $2^{1-1} = 1$, this establishes our base case.

(2) **Inductive Hypothesis**: Suppose that the statement holds for all $k \leq n$. That is, there are 2^{k-1} ways to eat a $k \times 1$ chocolate bar, where $k \leq n$.

(3) **Inductive Step**: We now show the statement is true for $n + 1$. In the first minute we eat m pieces, where $m = 1, \ldots, n + 1$. If $m = n + 1$, then we have eaten the whole bar. This gives 1 way to eat it. Otherwise, if $m < n+1$, we are left with a $(n+1-m) \times 1$ chocolate bar. Observe that $n+1-m \leq n$. Therefore, by the inductive hypothesis, we know there are exactly 2^{n-m} ways to eat the remaining chocolate bar. Hence, in total there are

$$1 + 1 + 2 + \ldots + 2^{n-1}$$

ways to eat the chocolate bar. The first 1 comes from eating the whole bar, and each power of two comes from some value of m. When $m = n$, the corresponding power is $2^0 = 1$ and when $m = 1$, the corresponding power is 2^{n-1}. From Lemma 1, we then observe we can simplify this as

$$1 + 2^n - 1 = 2^n.$$

This proves the inductive step, concluding the induction.

Thus, we conclude the statement is true for all positive integers n. □

When working with strong induction, we must pay extra attention to our base case. We must make sure that our inductive step works for every number that we did not include in our base case. To illustrate this, we tackle one last problem:

Theorem 5: Separating into Groups

Let n be an integer greater than 2. Show that we can divide a class of n students into groups consisting of 2 or 3 students each.

Proof. We proceed by induction.

(1) **Base Case**: We show that the statement is true for $n = 2, 3, 4$. For $n = 2$, we separate the students into one group of 2. For $n = 3$, we separate the students into one group of 3. For $n = 4$, we separate the students into two groups of 2. This establishes our base case.

(2) **Inductive Hypothesis**: Suppose that the statement holds for $n - 3$. That is, we can divide a class of $n - 3$ students into groups consisting of 2 or 3 students each.

(3) **Inductive Step**: We now show the statement is true for n. Separate 3 students into a group. Then, by the inductive hypothesis, the remaining $n - 3$ students can be separated into groups consisting of 2 or 3 students each. Thus, we have separated the whole class into such groups. This proves the inductive step, concluding the induction.

Thus, we conclude the statement is true for all integers n greater than 2. □

Warning! Notice the relationship between the base case, inductive hypothesis, and inductive step here. Why do we have to include $n = 3, 4$ in our base case? Observe that the inductive step does not work for $n < 5$. If $n = 4$ and we group 3 students together, we are left with 1 student and nothing to do. To avoid this problem, we include the problematic values as base cases. It is crucial we do this, else we cannot be sure we do not have a monochromatic horses situation!

What would have happened if in the inductive step, instead of separating 3 students we separate just 2? Then, we could make two changes. First, it is no longer necessary to include 4 in the base case, as the inductive step now reduces it to 2. Second, we should adjust our inductive hypothesis to assume the statement holds for $n-2$. Of course, in both cases we could go full strong induction and suppose the statement holds for all values less than n. However, since we only need one value, we can also opt for simplicity and just include the assumptions we need.

Part II
Mini Unit 2

11 Learning to Count

We will now learn how to count. You may think that you already know how to count. Was this not something we learned back in preschool? It turns out that we can count much better than what we were taught in preschool. From sections 12 through 19 we will learn some techniques to improve our counting and be able to count things like we never have before.

To understand why we need to learn how to count, recall this problem from Section 10.3:

Theorem 4: Eating Chocolate

Let n be a positive integer. We have a $1 \times n$ chocolate bar, separated into 1×1 chocolate pieces. Every minute, we can eat any positive number of contiguous chocolate pieces from the left. There are 2^{n-1} ways to eat the chocolate bar.

This is a counting problem! We have some setup and we want to **count** how many possible ways something can be done. Most combinatorics problems can be boiled down to counting in this way. Sometimes we want to count how many ways we can do something, sometimes we want to count how many of something there are. However, unlike this problem, we will not always be given the answer to the counting problem and be asked to show it is true. Often, we will have to come up with the answer ourselves. For example, we could have been asked "In how many ways can the chocolate bar be eaten?". How would we have got the 2^{n-1} answer? One way to go about this that you should always attempt is **trying small cases**. If we try the cases $n = 1, 2, 3$ it is not too complicated to see each has $1, 2, 4$ ways to eat the chocolate bar, respectively. From there, we may perhaps guess that the answer is 2^{n-1}. Once we have this guess, we can use induction to prove it is true. It turns out that there is another way to prove the answer is 2^{n-1}, without appealing to induction at all. We will see how this other method works in Section 16.2.

Now, let us learn how to count!

12 Choices

Our first technique to count things is **constructive counting**. The idea behind constructive counting is that in order to count how many of something there are, we try to construct the thing we are counting and keep track of the choices we had along the way. When doing this, we will see that there are two types of choices, each of which will lead to an arithmetic operation. **Disjunctive choices**, or choices that correspond to an **or**, lead to addition. **Conjunctive choices**, or choices that correspond to an **and**, lead to multiplication. In this section, we explain how this works.

12.1 Addition

Consider the following problem:

Example 6

Julia has several distinct shirts, which she organizes by colors. She has 3 shirts in her red cabinet, 7 shirts in her green cabinet, and 5 shirts in her blue cabinet. How many options does Julia have to pick from for the shirt she will use to school today?

This example, although simple, illustrates our first type of choice in constructive counting.

Solution. We claim the answer is $\boxed{15}$. We have to pick one shirt. We have three cases:

The shirt is red **OR** the shirt is green **OR** the shirt is blue.

Importantly, these ors are **exclusive**, we cannot have both that the shirt is red and that the shirt is green. In this situation, we say that the cases are **disjoint**.

Case 1: (The shirt is red) We have 3 red shirts, so there are 3 options to pick from this case.

Case 2: (The shirt is green) We have 7 green shirts, so there are 7 options to pick from in this case.

Case 3: (The shirt is blue) We have 5 blue shirts, so there are 5 options to pick from in this case.

The total number of options to pick from is the **sum** of the number of options in each disjoint case. Thus, Julia has $3 + 7 + 5 = 15$ options to pick from for her shirt. ☐

Now, we all agree that this proof is unnecessarily long, but I have written it in this way to illustrate the structure of **casework** proofs. First, we identify the different cases that we can break up the problem into. It is important that these cases cover all possibilities, otherwise we will **undercount**, or fail to count possibilities. In these lecture notes we will focus on problems where the cases are **disjoint**, so that no possibility can fall in more than one case at once. This is to avoid **overcounting**, or counting one possibility more than once. We handle non-disjoint cases and other types of overcounting in Sections 14 and 17.
Once we have broken up the problem into disjoint cases, we count the number of possibilities in each case. The point here is to break the problem up into cases that we do know how to count. Perhaps in each case we will use some counting technique[5], but the point is that we can count the number of possibilities in each case.
Now that we have counted the number of possibilities in each disjoint case, we appeal to the **additive principle**:

Additive Principle

The total number of possibilities is the sum of the number of possibilities in each disjoint case.

You should think of the additive principle as an axiom. Despite just assuming its truth, make sure that this makes intuitive sense to you! It certainly makes sense when looking at the shirt example, and any other application should feel equally intuitive.

Since in the above problem the separation into cases is very straightforward, we can be less explicit and shorten our solution.

Solution. We claim the answer is $\boxed{15}$. From the additive principle, where our cases are the color of the shirt, we see that there are $3 + 7 + 5 = 15$ ways to pick a shirt to wear to school today. □

Warning! If the cases that you are dividing your problem into are not obvious, make sure to state them explicitly. Remember, writing down proofs is a balance between clarity and conciseness and neither should be satisfied at the expense of the other. If it is clear what your casework is, you can be concise and not say it explicitly. If you need to write out explicitly what each case is and why they are disjoint, write it out!

Let us finish with one more example:

Example 7

Lily is going to the ice-cream shop. She has 3 options for the ice-cream flavor and 4 options for the toppings. She wants to eat an ice-cream with exactly one flavor and exactly one topping. How many possible ice-creams could Lily order?

Solution. We claim the answer is $\boxed{12}$. We do casework on the choice of topping. Since Lily wants exactly one topping, these are disjoint cases.

Case 1: (Topping 1) Lily has 3 options for the ice-cream flavor and she has already chosen her topping, so there are 3 possible ice-creams in this case.

Case 2: (Topping 2) Lily has 3 options for the ice-cream flavor and she has already chosen her topping, so there are 3 possible ice-creams in this case.

Case 3: (Topping 3) Lily has 3 options for the ice-cream flavor and she has already chosen her topping, so there are 3 possible ice-creams in this case.

Case 4: (Topping 4) Lily has 3 options for the ice-cream flavor and she has already chosen her topping, so there are 3 possible ice-creams in this case.

[5] Including, possibly, more casework.

By the additive principle, the total number of possible ice-creams is $3 + 3 + 3 + 3 = 12$. $\square$

12.2 Multiplication

You may have noticed that our last proof sounded very repetitive; every case was handled in exactly the same way. Because of this, we ended up adding the same number multiple times, getting an answer of $3 + 3 + 3 + 3 = 3 \cdot 4 = 12$. Furthermore, observe what would have happened if we had done our casework slightly differently. If we did casework on the flavor, then we would have had 3 cases, each with 4 options, one for each topping. Thus, we would have got an answer of $4+4+4 = 4 \cdot 3 = 12$. First of all, we should be glad both answers coincide. After all, how many options we have should not depend on how we count them. Furthermore, it is no coincidence that multiplication shows up here! To order an ice-cream,

Lily has to choose a flavor **AND** choose a topping.

The fact that we have to make both choices is an indication that multiplication arises! The other key fact here is that the choices are **independent**. We say that two choices are independent when the option picked for one does not change what possibilities we have for the other. For this problem, since the flavor of ice-cream we choose does not change the options for toppings that we have, and vice-versa, we see that these options are independent.

Then, the fact that we get a product as the answer exemplifies our next principle, which is a direct consequence of the additive principle:

Multiplicative Principle

If we have independent choices, then the total number of possibilities is the product of the number of possibilities for each choice.

As an exercise, prove the multiplicative principle from the additive principle. Doing it for two choices is an exercise in casework. To prove it holds for an arbitrary number of choices, you can practice your induction skills!

Using the multiplicative principle, we can shorten our proof of Example 7:

Solution. We claim the answer is $\boxed{12}$. Observe that the choice of flavor and the choice of topping are independent choices. Thus, by the multiplicative principle, the total number of possible ice-creams is $3 \cdot 4 = 12$. $\square$

With the power of the additive and multiplicative principle, you can now tackle a lot of counting problems!

Example 8

In the country of Principalia, every car must be issued a license plate, which consists of four characters. The first has to be a letter. The second can be either a letter or a numerical digit $(0-9)$. The third and fourth have to be numerical digits. How many different license plates can the Principalia government issue?

Solution. We claim the answer is $\boxed{93600}$. Observe that the choice of character for each of the four positions are independent choices. Therefore, by the multiplicative principle, the total number of license plates is the product of the number of options for each position. The first character must be a letter, so it has 26 options. The second character can be either a letter or a numerical digit, but it cannot be both. Thus, by the additive principle, it has $26 + 10 = 36$ options. Finally, the third and fourth characters must be numerical digits, so they each have 10 options. Thus, by the multiplicative principle, the number of different license plates is $26 \cdot 36 \cdot 10 \cdot 10 = 93600$. $\square$

Example 9

A binary string of length n is a sequence of n digits, each of which is either 0 or 1. For example, the binary strings of length 2 are $00, 01, 10, 11$. How many binary strings of length n are there?

Solution. We claim there are $\boxed{2^n}$ binary strings of length n. We imagine building a binary string, one choice of digit at a time. Observe that these choices are independent. Furthermore, each digit has exactly 2 options, either it is 0 or it is 1. Hence, by the multiplicative principle, there are

$$\underbrace{2 \cdot 2 \cdots 2}_{n \text{ times}} = 2^n$$

binary strings of length n. □

As an exercise, try to find an inductive proof of this fact!

Warning! Our guideline throughout this section has been that **OR** means additive principle and **AND** means multiplicative principle. It is important to not follow this blindly, but rather understand when OR and AND correspond to each principle. For example, consider a standard deck of 52 cards. It contains 26 black cards and 36 number cards.
How many cards are either black cards or number cards? The answer certainly cannot be $26 + 36 = 62$, since there are not that many cards in the deck. The problem here was that our casework was not disjoint; there are cards that are both black and number cards.
How many cards are black cards and number cards? Again, the answer certainly cannot be $26 \cdot 36 = 936$. The problem here is that we do not have any independent choices! Whether the card is a number card or not depends a lot on the choice of black card.
The lesson here is to not follow things blindly, but rather think about what the words and principles actually mean.

13 Permutations

Our tools so far allow us to tackle a great number of classic counting problems. In this section, we extend our tools to tackle another category of counting problems: permutations.

13.1 Dependent Choices

Consider the following two problems:

Example 10

(1) How many 4−digit numbers are there?

(2) How many 4−digit numbers with no repeated digits are there?

On the surface, these two problems are really similar. However, the extra restriction in Problem (2) will require an adjustment to our multiplicative principle.

Solution to (1). We claim the answer is $\boxed{9000}$. We look at the options each digit has. Observe that these are independent choices, so the multiplicative principle applies! Since the number has 4 digits, the first digit cannot be 0. Therefore, it has 9 options $(1 - 9)$. Digits two through four have no such restrictions, so they each have 10 options. Thus, by the multiplicative principle, there are $9 \cdot 10 \cdot 10 \cdot 10 = 9000$ four-digit numbers. □

How do things change for (2)? Observe that our choices are no longer independent! By adding the restriction that there are no repeated digits, the choice of digit in one position affects the number of options the other digits have. For example, if the first digit is 7, then the second digit no longer has 10 options. Rather, it can only be one of the digits that is not 7, so it has 9 options. Does this mean that our previous techniques are hopeless to tackle (2)? No! We just have to make a small adjustment to our multiplicative principle.

To understand how this will work, recall how we derived the multiplicative principle. We noticed that when our choices are independent, when doing casework on our first choice we ended up adding the same number multiple times, so we could simplify this to a multiplication. However, we can get this same behavior even if our choices are not independent!

Suppose we want to count how many $2-$digit numbers with no repeated digits there are. Again, the choices for each digit are not independent, as the choice of the first digit changes what the possible options for the second digit are. However, does this choice change **how many** options the second digit has? No matter what the first digit is, the second digit can be any digit other than the first. Thus, it will always have 9 options. Put another way, if we did casework on the value of the first digit, the second digit would always have 9 options. Those options would change depending on the first digit, but what we care about when counting are how many we have, not what they actually are. Therefore, we can still multiply! This works in general: even if our choices are dependent, if the number of options for one is the same regardless of the choice made for the other, we can still multiply. Thus, for this problem, we have 9 options for the first digit, which leaves 9 options for the second digit in every case, so there are $9 \cdot 9 = 81$ two-digit numbers with no repeated digits.

Solution to (2). We claim the answer is $\boxed{4536}$. We analyze how many options each digit has. The first digit can be any nonzero digit, so it has 9 options. The second digit can be any digit different from the first, so it also has 9 options. The third digit can be any digit different from the first and second, so it has 8 options. Finally, the fourth digit can be any digit different from the first, second, and third, so it has 7 options. Thus, there are $9 \cdot 9 \cdot 8 \cdot 7 = 4536$ four-digit numbers with no repeated digits. □

Warning! When we work with dependent choices, the order in which we consider our choices matters! For example, let's go back to the $2-$digit problem. Suppose we started by considering the options for the second digit. Since we have not yet chosen the first one, it has 10 options. How about the first digit? If we naively say that it can be any digit other than the second, we conclude that it has 9 options, so there should be $9 \cdot 10 = 90$ two-digit numbers with no repeated digits. However, this is not the same answer we got before. What went wrong? The problem is that the first digit has a different number of options depending on what we choose for the second digit. If the second digit is chosen to be 0, then the first digit can be any nonzero digit, so it has 9 options. However, if the second digit is chosen to be nonzero, then the first digit cannot be 0 nor can it be the choice for the second digit. So, it only has 8 choices. Hence, the correct computation for this method is $9 \cdot 1 + 8 \cdot 9 = 81$, coinciding with our previous computation. The plus sign here reflects that we have two cases, the second digit being zero or nonzero!

13.2 Books!

Let us put our ideas into practice with a classic problem:

Example 11

I have four different books that I want to arrange in my shelf. In how many orders can I put them?

A possible ordering of some objects is called a **permutation** of the objects. This problem is trying to count the number of permutations of four different books. We now have the tools to tackle this problem.

Solution. We claim the answer is $\boxed{24}$. The first book has 4 options: it can be any of the books I want to arrange. The second book has 3 options: it can be any of the remaining books. Similarly, since the third book cannot be the same as was placed first or second, it has 2 options. Lastly, the fourth book only has 1 option: the last remaining book. Thus, there are $4 \cdot 3 \cdot 2 \cdot 1 = 24$ orders in which I can put the books. □

It turns out that counting permutations of objects is a very common problem in combinatorics! Because of this, the answer to the problem gets a special notation.

Definition 1: Factorial

For n a positive integer, we define the number $n!$ (read "n factorial") to be product of the integers from n all the way down to 1. That is,

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1.$$

Furthermore, we define $0! = 1$.
Observe that $n! = n \cdot (n-1)!$ for all positive integers n.

What do we mean when we say that this is the answer to the permutation counting problem?

Theorem 6: Number of Permutations

Suppose you have n different books that you want to arrange in your shelf in a line. There are $n!$ ways to order them.

Proof. There are n options for the first book. Since the second book cannot be the one placed first, there are $n-1$ options for the second book. Similarly, there are $n-2$ options for the third book. We can continue this logic all the way down to the last book, which has only 1 option. Therefore, there are

$$n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1 = n!$$

ways to order the books. □

As an exercise, try to find an inductive proof of this statement!

Warning! Why does it make sense to define $0! = 1$? There are two motivations for this that I want to use to convince you that this is a good definition. First, we would like the formula $n! = n \cdot (n-1)!$ to hold for all n. If this is going to be true for $n = 1$, then we need $1 = 1! = 1 \cdot 0!$, so $0!$ should equal 1. Second, we should really think of the factorial as the answer to the permutation problem. What is the answer to the permutation problem when we have no objects? That is, in how many ways can we order 0 objects? The answer is 1, the empty ordering. We have no things to order, so having no things is the one way we have to order them!

14 Indistinguishability

So far we have been dealing with counting problems where all objects are different. However, we do not always want to consider all objects as distinct. For example, if we have some colored marbles, it is impossible to distinguish two marbles that are painted the same color. So, if we try to count permutations of these marbles, we want to consider orderings that switch the indistinguishable marbles as the same, since we do not have any way to distinguish them ourselves.
We already saw how addition and multiplication show up in counting. In this section, we will see how correcting for indistinguishability leads to division.

14.1 Permutations with Repetition

Consider the following problems:

Example 12

(1) There is one red marble, one green marble, one blue marble, and one yellow marble inside an urn. In how many ways can we arrange the four marbles in a line?

(2) There are two indistinguishable red marbles, one green marble, and one blue marble inside an urn. In how many ways can we arrange the four marbles in a line?

Solution to (1). We claim the answer is $\boxed{24}$. This is a permutation problem! We have four distinct objects and we want to count how many permutations of them there are. As we saw in Section 13.2, the answer is $4! = 24$. □

Solution to (2). We claim the answer is 12. Since two of the marbles are identical, simply counting the number of permutations will end up **overcounting** the number of permutations in this case. How do we know by how much we are overcounting? Suppose we had some way to distinguish the two red marbles; perhaps one is labeled with a 1 and the other is labeled with a 2. In this case, we do have $4! = 24$ permutations. How do these permutations relate to the original problem? In the permutations problem, swapping the positions of red marble 1 and red marble 2 gives a different permutation. But, in the problem where they are indistinguishable, swapping their positions looks the same, since we cannot tell them apart. Therefore, when counting the 24 permutations, we are counting each permutation in the original problem exactly twice. Hence, we can correct our counting by dividing by 2, as this is the number of times we are counting each **distinct** permutation. Thus, there are $24/2 = 12$ ways to arrange the four marbles in a line. □

Counting the number of permutations of some objects where some of them are indistinguishable is a problem called counting **permutations with repetition**. The repetition arises from the indistinguishable objects, which lead to each permutation being over-counted some number of times. The number of times we count each permutation is called its **multiplicity**. When all permutations have multiplicity 1, we do not have to correct anything, we have counted everything exactly once and our answer will be right. However, if all permutations have some common multiplicity greater than 1, we have to correct our computation. In this case, since they all have the same multiplicity, we can simply divide, correcting the overcounting and leading to the right answer.

Now, we shall see this in practice with the following theorem:

Theorem 7: Permutations with Repetition

How many permutations are there of n objects, where k of them are indistinguishable and the remaining $n - k$ are distinguishable?

Solution. We claim the answer is $n!/k!$. Again, let us begin by imagining that we can distinguish the k indistinguishable objects. In this case, we already know that the number of permutations is $n!$. However, as we have just discussed, these permutations will overcount the true answer. What is the multiplicity of each permutation when the k objects are indistinguishable? Observe that permuting the k objects yields an indistinguishable permutation! We know how many permutations of k objects there are: $k!$. Therefore, each indistinguishable permutation has multiplicity $k!$, one for each way to permute the k objects. Thus, to correct the overcounting we divide by $k!$, yields an answer of $n!/k!$. □

We can generalize this for more indistinguishable objects!

Theorem 8: General Permutations with Repetition

Suppose we have n objects, with n_1 of Type 1, n_2 of Type 2, and so on until n_k objects of Type k. All objects of the same type are indistinguishable and objects of different types can be distinguished. Then, the number of permutations of these objects is

$$\frac{n!}{n_1!n_2!\cdots n_k!}.$$

We leave this proof as an exercise to the reader. The idea is the same as Theorem 7, try to count the multiplicity of each permutation if we assumed the objects were indistinguishable.

With the theory in hand, we can now solve any permutation problem thrown at us.

Example 13

How many 5 digit numbers are there whose digits are $1, 1, 2, 2, 3$ in some order?

Proof. Solution We claim the answer is $\boxed{30}$. We are looking for permutations with repetition of the objects $1, 1, 2, 2, 3$. If the five digits were indistinguishable, we would have $5! = 120$ permutations. However, since the two 1s are indistinguishable, we have to divide by $2! = 2$. Furthermore, the two 2s are indistinguishable, so we have to divide by $2! = 2$ again. Thus, there are

$$\frac{5!}{2!2!} = \frac{120}{2 \cdot 2} = 30$$

five-digit numbers whose digits are $1, 1, 2, 2, 3$ in some order. $\square$

14.2 Combinations

Often in combinatorics, we are interested in selecting a subset of objects from some bigger set. For example, we may be trying to build a k person committee from a club with n people. Or, we could be considering a five-card poker hand drawn from the $52-$card deck. Any time we want to select a group of k things from a pool of n objects, we are asking a question about **combinations**. When we ask about combinations, we do not care about the order in which we choose the elements, only which elements we choose. For a committee, it does not matter what order we chose its members, only who is a member. For a poker hand, the order in which the cards show up is irrelevant, we only care about what cards we actually have.

How can we go about counting how many combinations there are? We can use our techniques from the previous section! We have already seen a situation where the order of objects does not matter, which is when the objects are indistinguishable. When working with combinations, the only distinction we want to make is whether we chose an object or not, so we can treat chosen objects as indistinguishable among each other and not chosen objects as indistinguishable among each other. Thus, we have translated our combination problem into one we already know how to solve!

Theorem 9: Combinations

The number of ways to choose k elements of an n element set is

$$\frac{n!}{k!(n-k)!}.$$

Proof. We can imagine picking the k elements as ordering the n elements in a straight line. We will choose the first k elements in the line and not choose the remaining $n-k$. We know that the number of permutations of n objects is $n!$. However, this overcounts our choices, since we do not care about the order of the chosen nor unchosen elements. We can order the k selected elements in $k!$ ways, while we can order the $n-k$ not selected elements in $(n-k)!$ ways. Thus, the multiplicity of each choice is $k!(n-k)!$. Hence, the number of ways to choose k elements of an n element set is

$$\frac{n!}{k!(n-k)!},$$

as claimed. □

This problem will show up a lot in several disguises! Any time you can boil down the problem to choosing k objects from a pool of n and you do not care about their order, you have a combination problem!

Example 14

(1) Let S be a set with n elements. How many subsets with k elements does it have?

(2) How many binary strings of length n have exactly k ones?

Solution to (1). To build a subset with k elements we have to choose k elements to belong in the subset. By the definition of sets, we do not care about the order of the elements in the set, so this is a combination problem. Thus, there are

$$\frac{n!}{k!(n-k)!}$$

$k-$element subsets of an $n-$element set. □

Solution to (2). We can phrase this as a combination problem! We have n positions and we want to choose k of them to have a one. The remaining $n-k$ positions will necessarily have a 0. We only care about which k positions we choose, not the order in which we choose them, so this is a combination problem. Thus, there are

$$\frac{n!}{k!(n-k)!}$$

binary strings of length n with exactly k ones. □

15 Applications of Combinations

Combinations are abundant in combinatorics. In this section we see some common applications of this idea.

15.1 Binomial Coefficients

The expression

$$\frac{n!}{k!(n-k)!}$$

shows up a lot in combinatorics, particularly because it is the answer to the combination problem. As such, we give it a special symbol, called the **binomial coefficient**:

Definition 2: Binomial Coefficients

For a positive integer n and a natural number $0 \leq k \leq n$, we define the binomial coefficient

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

We read this as "n choose k".

This allows us to simplify our notation when solving combination problems. Now we know the answer is simply the binomial coefficient!

Why is this symbol called a binomial coefficient? The reason is that it shows up when we expand the expression

$$(x+y)^n.$$

The term $x+y$ is called a binomial and the resulting expansion is called a **binomial expansion**. We can prove the following theorem using our counting techniques:

Theorem 10: Newton's Binomial Expansion

The following holds for all positive integers n and real numbers x, y:

$$(x+y)^n = \binom{n}{0}x^0y^n + \binom{n}{1}x^1y^{n-1} + \binom{n}{2}x^2y^{n-2} + \ldots + \binom{n}{n-1}x^{n-1}y^1 + \binom{n}{n}x^ny^0.$$

Proof. Although this may seem like an algebra problem, we can prove this using combinations! To understand how this works, let us begin by looking at the case $n = 2$:

$$\begin{aligned}(x+y)^2 &= (x+y)(x+y)\\ &= x^2 + xy + yx + y^2\\ &= x^2 + 2xy + y^2.\end{aligned}$$

We have three types of terms: terms of the form $x^2 = x^2y^0$, terms of the form $xy = x^1y^1$ and terms of the form $y^2 = x^0y^2$. How does each term arise from the expansion? When we multiply out $(x+y)(x+y)$, we choose one term from each $(x+y)$ factor. Thus, to get a x^2y^0 factor, we must choose two xs and zero ys. Similarly, to get a x^1y^1 factor, we must choose one x term and one y term. The 2 in front of the xy term in the final answer represents that there are 2 ways to do this: we pick an x from the first term and a y from the second, or we pick an x from the second term and a y from the first. Observe what we are doing! In order to count how many x^1y^1 terms we obtain, we choose one $(x+y)$ term for the x to come from and one $(x+y)$ term for the y to come from.

With these observations, we can now deal with the general case. Observe that we must pick one x and one y for each $(x+y)$ term, so the exponents of the variables must add up to n. We now count how many x^ky^{n-k} terms we obtain. In order to get such a term, we must choose k terms from which an x factor will come from. The remaining $n-k$ terms will contribute a factor of y. Thus, we want to **choose** k terms from the n we have available. This is a combination problem! So, the coefficient in front of the term x^ky^{n-k} is

$$\binom{n}{k}.$$

Adding up all terms from x^0y^n to x^ny^0, we get the desired equality. □

15.2 Stars and Bars

Another common problem in combinatorics is distributing things among a group. For example, we may want to distribute some slices of pizza among friends. Or, we could be distributing pieces of candy to children. Any time we want to distribute n objects among k people, we have a **distribution** problem. As it turns out, we can turn distribution problems into combination problems!

Example 15

You are a third grade teacher and want to distribute 20 star stickers among your top 5 performing students. Each of the students can get from 0 to 20 stars and you want to distribute all of the stickers. How many distributions of the star stickers are there?

There are many ways to distribute the stars with these conditions. For example, we could give one student all 20 stars and give 0 stars to all others. Or, we could give 4 stars to each of the 5 students. How can we possibly count these systematically? Here is an idea: imagine that we have all 20 stars in a line. How can we represent a distribution of stars? Imagine we place four bars somewhere between the stars. Then, we give the first student all stars to the left of the first bar, the second student the stars between the first and second bar, and so on, until the fifth student gets the stars to the right of the fourth bar. For example, the following illustrates giving all 5 students 4 stars:

$$\star\star\star\star/\star\star\star\star/\star\star\star\star/\star\star\star\star/\star\star\star\star,$$

while the following illustrates giving the first student 13 stars and giving the third 7:

$$\star\star\star\star\star\star\star\star\star\star\star\star\star//\star\star\star\star\star\star\star//.$$

This is now a combination problem! We have $20 + 4$ symbols and we want to choose 4 of them to be bars. Each of these combinations give us a distribution and vice-versa.

Solution. We claim the answer is $\boxed{10626}$. As we argued above, the problem is equivalent to choosing 4 symbols out of 24 available to be bars. This is a combination problem, so there are

$$\binom{24}{4} = 10626$$

distributions of star stickers among the students. □

We can use this strategy in general. If we want to distribute n objects among k people with similar restrictions, then we can think of lining up the n objects in a line and placing $k-1$ dividers between them. This turns the distribution problem into a combination problem which we know how to solve!

Theorem 11: Stars and Bars

Suppose we want to distribute n objects among k people. Each person can get from 0 to n objects and we want to distribute all objects. There are

$$\binom{n+k-1}{k-1}$$

possible distributions of the objects among the people.

We leave the proof as an exercise; the logic is the same as Example 15.

16 Changing Problem

Sometimes, the hardest part about a problem is realizing that you have already solved it before. In this section we study some ways to remove a problem's disguise and turn it into something we have already seen.

16.1 Complementary Counting

Consider the following problem:

Example 16

In your third grade class, you have to divide your 15 students into a group of 7 and a group of 8. However, Bob and Dylan are very talkative, so you want to place them in different groups. In how many ways can we separate the class into these two groups if Bob and Dylan cannot be in the same group?

Solution. We claim the answer is $\boxed{3432}$. We know how to count the number of ways to divide the class if we do not impose the Bob and Dylan restriction. Now, observe that either Bob and Dylan end up in the same group, or they do not end up in the same group, but not both. Thus, we have disjoint cases! By the additive principle, we know that the sum of the number of ways to separate the class in each case gives the total number of ways to separate the class. Since we know how to compute this total, we can count the number of ways Bob and Dylan end up in different groups by counting the number of ways they end up in the same group!

To count the total number of ways to separate the class without restriction, observe that we want to choose 7 students out of the 15 to form part of the smaller group. This is a combination problem, so we know there are $\binom{15}{7}$ ways to do this.

Next, we count the number of ways to separate the class when Bob and Dylan end up in the same group. We have two disjoint cases: they end up in the smaller group or they end up in the bigger group. If they end up in the smaller group, then we have to choose 5 students from the remaining 13 to comprise the rest of the small group. There are $\binom{13}{5}$ ways to do this. If they end up in the bigger group, then we have to choose 7 students from the remaining 13 to comprise the small group. There are $\binom{13}{7}$ ways to do this. Thus, there are

$$\binom{13}{5} + \binom{13}{7}$$

ways to separate the class such that Bob and Dylan end up in the same group. We want them to not be in the same group, so we subtract this from the total to see that there are

$$\binom{15}{7} - \left(\binom{13}{5} + \binom{13}{7}\right) = 3432$$

ways to separate the class where Bob and Dylan end up in different groups[6]. □

The strategy we just employed is called complementary counting, and it is a consequence of the additive principle. We imagine we want to count something, subject to some restrictions. Then, the additive principle tells us that the total count equals the count subject to the restrictions added to the count subject to the restrictions not holding. Sometimes, it is easier to count when the restrictions do not hold and we can use complementary counting to simplify our work. The essential idea boils down to

$$\begin{aligned} \text{what we want } + \text{ what we do not want } &= \text{ total} \\ \implies \text{what we want} &= \text{ total } - \text{ what we do not want }. \end{aligned}$$

16.2 Bijections

We have already seen bijections in these notes before. When we translated between permutations with repetition, combinations, and distributions, we were secretly using bijections. The idea behind bijections is to change what we are counting to some other problem that we already know how to deal with. To do this, we must ensure that both problems lead to the same number! How can we ensure this? A **bijection** or **one-to-one correspondence** between two sets is a way to assign to each element of the first set an element of the second such that

[6] It is safe to assume Bob and Dylan were not among the star sticker students.

- We do not assign the same element to two different elements of the first set.
- Every element of the second set is assigned to some element of the first.

Let us think about why these conditions guarantee both sets will have the same number of elements. The first condition guarantees that the first set is no bigger than the second, as we do not repeat assignments in the second. The second condition guarantees that the first set is no smaller than the second, as everything in the second set must have some element assigned to it. Thus, when we have a bijection, we can count either the elements of the first set or the elements of the second set.

We saw already a bijection between distributions and combinations: Distributing n objects among k people is in bijection with choosing $k-1$ objects from a pool of $n+k-1$ things. We now recall how this bijection worked. To each distribution of objects, we assigned a visualization in which we have the n objects separated by $k-1$ dividers. Observe that this assignment is unique, if two distributions get the same visualization, then the distributions must have been the same. Furthermore, every visualization corresponds to a distribution. Given a visualization, we can reconstruct which distribution it gets assigned to. Thus, we have our bijection!

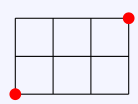
Here is a classic example of a bijection:

Theorem 12: Paths

You are located at the bottom left corner of a $n \times m$ grid. You want to reach the top right corner and are only allowed to move either one unit to the right or one unit up. There are

$$\binom{n+m}{n}$$

possible paths to do so.



Proof. Observe that in order to reach the top right corner, we must move to the right exactly m times and move up exactly n times. Therefore, we can assign to each valid path a sequence of letters U, R, where U denotes moving up and R denotes moving right. Observe that different paths get assigned different sequences. Furthermore, each sequence is assigned to some path, as given a sequence we can reconstruct which path it was assigned to. Hence, we have a bijection between the number of paths and the number of ways to order m Rs and n Us, where the Rs are indistinguishable and the Us are indistinguishable. Recall that this is given by

$$\frac{(m+n)!}{m!n!} = \binom{m+n}{n}.$$

□

Finally, we end this section fulfilling the promise made at the start of section 11.

Theorem 4: Eating Chocolate

Let n be a positive integer. We have a $1 \times n$ chocolate bar, separated into 1×1 chocolate pieces. Every minute, we can eat any positive number of contiguous chocolate pieces from the left. There are 2^{n-1} ways to eat the chocolate bar.

Proof. There is a bijection between the ways of eating the chocolate and binary strings of length $n-1$. Since there are 2^{n-1} of the latter, establishing this bijection proves the problem.

The bijection is as follows: for each piece of chocolate after the first one, write a 1 if after some time it is the first piece in the remaining bar and write a 0 otherwise. This gives each way of eating the bar a binary string of length $n-1$. Let us look at an example to see how this works. Suppose the chocolate bar has length 10. Then,

- Eating the whole bar the first minute gets assigned the string 000000000.
- Eating 3 pieces the first minute, 5 the second, and the remaining 2 the third minute gets assigned the string 001000010
- Eating one piece each minute gets assigned the string 111111111.

Observe that two different ways of eating the chocolate bar will be assigned to different strings. Furthermore, since the first piece must get eaten in the first minute, each string is assigned to some way of eating the chocolate bar, and we can reconstruct it from the string. Thus, we have our desired bijection. ☐

17 PIE

We already saw how to correct for overcounting for conjunctive choices. How about disjunctive choices? That is, how do we correct for when the cases in our casework are not disjoint?

We will explore this with some examples:

Example 17

There are 15 students in your third grade class. Of these students, 8 are in the math club, 6 are in the science club, and 4 are in both. How many students are in at least one of the two clubs?

Proof. Solution We claim there are 10 students in at least one of the two clubs. We can count the students directly, doing casework on whether a student is in the math club or in the science club. There are 8 students in the math club and 6 students in the science club, for a total of $6+8$ students. We are not done! This is where we have to be careful. Since our cases are not disjoint, we have counted some students more than once! Imagine one student, Pablo, is in both the math club and science club. How many times did we count Pablo above? We counted him once for the math club and once for the science club. Thus, we have overcounted Pablo! Since every student should be counted only once, we have to correct for overcounting. Thus, we should subtract the number of students that are in both clubs from our total. Thus, there are $6+8-4=10$ students in at least one club. ☐

The way we corrected for overcounting should feel very intuitive. We counted in each case, then realized that some people were counted twice, so we subtracted the number of people we counted too many times. This strategy, **including** each person once for each case and then **excluding** each person that was overcounted, is called the **Principle of Inclusion-Exclusion**. It is often abbreviated **PIE**.

We can generalize the story from Example 1 to be applicable in general. In order to write this in general, we introduce the **intersection** and **union** of sets:

Definition 3: Union, Intersection and Size

Given two sets A and B, we define

- their intersection $A \cap B$ as the set containing all elements that are both in A and in B;
- their union $A \cup B$ as the set containing all elements that are either in A or in B or both.

Furthermore, for a finite set S, we define $|S|$ to be the number of elements in S.

We say that two sets A and B are **disjoint** if $A \cap B = \emptyset$, ie, A and B have no elements in common. Observe that we can rephrase our additive principle in terms of sets:

Additive Principle (Sets)

If the finite sets A and B are disjoint, then

$$|A \cup B| = |A| + |B|.$$

Thus, we can interpret PIE as a generalization of the additive principle, suitable when the sets (cases) are not disjoint.

Theorem 13: Principle of Inclusion-Exclusion

For all finite sets A and B, we have

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

Proof. By definition, an element of $A \cup B$ must be either an element of A or an element of B or both. By definition, A has $|A|$ elements and B has $|B|$ elements, giving a total of $|A| + |B|$ elements. However, this double counts the elements that are both in A and B. In other words, it double counts the elements in $A \cap B$. Thus, the total number of elements of $A \cup B$ is $|A| + |B| - |A \cap B|$, as claimed. □

We can extend PIE to when we have more than two cases. Consider the following problem:

Example 18

In your third grade class, there are 15 students, all of which are in one of three clubs. Of these 15 students, 6 are in the math club, 5 are in the science club, and 7 are in the art club. Furthermore, there are 3 students that are both in the math and science club, 2 students both in the math and art club, and 1 student both in the science and art club. How many students are in all three clubs?

Solution. We claim the answer is $\boxed{3}$. Since we know all students are in at least one club, we count the students by their clubs. There are 6 students in math club, 5 in science and 7 in art, for a total of $6 + 5 + 7 = 18$ students. However, this overcounts the students that belong to at least two clubs. There are $3 + 2 + 1 = 6$ of these, leaving $18 - 6 = 12$ students. Where are the remaining 3 students? Think about the students that are in all three clubs. How many times have we counted them? We included them once in the math club, once in the science club, and once in the art club. Then, we excluded them once per pair when correcting our overcounting. Thus, we excluded them once when counting students in math and science, once when counting students in math and art, and once when counting students in science and art. Therefore, in total, we have counted them $3 - 3 = 0$ times! This explains the missing students in the above count. The $15 - 12 = 3$ remaining students must be in all three clubs. □

We can again express this in terms of sets!

Theorem 14: 3 Case PIE

For all finite sets A, B, and C, we have

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

We leave the proof as an exercise; follow the idea in Example 18.

18 Pigeonholes

Our next principle is one of the most intuitive statements in combinatorics. Despite its simplicity, it is also one of the most useful principles we have available to us:

Pigeonhole Principle

Suppose we have $n+1$ pigeons and n pigeonholes. If we distribute all pigeons among the pigeonholes, then some pigeonhole has at least 2 pigeons.

Although this statement sounds obvious, it is super useful to prove things! The key idea when using the pigeonhole principle is to identify what are the pigeons and what are the pigeonholes.

Example 19

Lucas has 20 socks in his drawer. Of these, 4 are red, 4 are green, 5 are blue, 4 are black, and 3 are white. Since the light of his room is off, Lucas will draw socks blindly from his drawer. How many socks does he have to draw to guarantee he has pulled two socks of the same color?

Solution. We claim the answer is $\boxed{5}$. We identify the socks as pigeons and the color of sock as the pigeonhole. Observe that we have 4 possible colors. Thus, by the pigeonhole principle, if we have 5 socks, there must be a color that has at least 2 socks. Hence, if Lucas draws 5 socks, he guarantees to pull two socks of the same color. □

Pigeonhole comes in various different flavors. All of them are variations on this idea that if we have too many pigeons, then some pigeonhole must have a lot of pigeonholes. Our first flavor is a generalization of the principle that allows us to show some pigeonhole has at least m pigeons, where m can be larger than 2. To do this, we introduce the notation $\lfloor x \rfloor$, read "floor of x". This symbol denotes the greatest integer that is less than or equal to x. For example, $\lfloor \pi \rfloor = 3$, $\lfloor 12.75 \rfloor = 12$, $\lfloor 7 \rfloor = 7$, and $\lfloor -2.3 \rfloor = -3$.

Theorem 15: Generalized Pigeonhole

Suppose we have n pigeons and k pigeonholes. If we distribute all pigeons among the pigeonholes, then some pigeonhole has at least

$$\left\lfloor \frac{n-1}{k} \right\rfloor + 1$$

pigeons.

Proof. Suppose for the sake of contradiction that no pigeonhole contains at least $\lfloor (n-1)/k \rfloor + 1$ pigeons. Then, each pigeonhole contains at most $\lfloor (n-1)/k \rfloor$ pigeons. By definition of $\lfloor x \rfloor$, we know that $\lfloor (n-1)/k \rfloor \leq (n-1)/k$. Thus, each of the k pigeonholes contains at most $(n-1)/k$ pigeons, so there are at most

$$k \cdot \frac{n-1}{k} = n-1$$

pigeons distributed. This contradicts that we distributed all pigeonholes, so our initial assumption must be false. Thus, some pigeonhole has at least $\lfloor (n-1)/k \rfloor + 1$ pigeons, as desired. □

Do not try to memorize this formula! Although useful, you should be able to derive it on the spot when trying to apply the pigeonhole principle. Simply try to think about how we can distribute the pigeons as evenly as possible, and come to a conclusion from there.

Our final flavor is when we have infinitely many pigeons.

Theorem 16: Infinite Pigeonhole

Suppose we have infinitely many pigeons and finitely many pigeonholes. If we distribute all pigeons among the pigeonholes, then some pigeonhole has infinitely many pigeons.

Proof. Suppose for the sake of contradiction that all pigeonholes had finitely many pigeons. Then, since there are finitely many pigeonholes, we distributed a finite number of pigeons. This contradicts that we distributed all infinitely many pigeons, so some pigeonhole must have infinitely many pigeons. □

Again, you do not really have to memorize this, as the principle at hand is very logical!

Example 20

Show that π contains one of the digits $0 - 9$ infinitely many times in its decimal expansion.

This is an application of infinite pigeonhole!

19 Combinatorial Identities

Now that we have a solid grasp of various counting techniques, we can use what we have learned so far to prove cool equations! We will be able to prove algebraic equations that are hard to manipulate by using our combinatorial technology. The idea here is **counting in two ways**. If we count the same thing in two different ways, the two answers that we get must be the same. Thus, we will get an equation related both counting methods. To understand how this works, we look at three examples of increasing difficulty:

Example 21

(1) Prove that

$$\binom{n}{k} = \binom{n}{n-k}.$$

(2) (Pascal's identity) Prove that

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

(3) Prove that

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}.$$

Proof of (1). We think about counting how many binary strings with exactly k ones there are. On the one hand, we have n positions and choose k positions to be ones. The remaining $n - k$ positions will be zeros. Thus, there are

$$\binom{n}{k}$$

ways to do this. On the other hand, we have n positions and choose $n - k$ positions to be zeros. The remaining k positions will be ones. Thus, there are

$$\binom{n}{n-k}$$

ways to do this. Since these count the same thing, it follows they must be equal, so

$$\binom{n}{k} = \binom{n}{n-k}.$$

□

Proof of (2). We think of building a $k+1$ person committee from a group of $n+1$ people. On the one hand, we simply choose $k+1$ people from the group of $n+1$, which we can do in

$$\binom{n+1}{k+1}$$

ways. On the other hand, consider singling out one person, Bob. Either Bob is in the committee or he is not and these choices are disjoint. If Bob is in the committee, then we still have to choose k people from the remaining n to complete it. There are

$$\binom{n}{k}$$

ways to do this. If Bob is not in the committee, then we have to choose $k+1$ people from the remaining n to form the committee. There are

$$\binom{n+1}{k+1}$$

ways to do this. Thus, by the additive principle, there are

$$\binom{n}{k} + \binom{n+1}{k+1}$$

ways to build a $k+1$ person committee from a group of $n+1$ people. Since we are counting the same thing, we conclude

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

□

Proof of (3). This is the trickiest so far. One way to approach this is to try to manufacture a counting problem whose answer is the more complicated side of the equation, then justify why the other side also solves it. Inspired by this approach, consider the following counting problem:
We have two groups of n people. In how many ways can we make two committees, each one made from each group of people, such that both committees have the same size?
On the one hand, we can do casework on the size of the committees. If the committees have 0 people, then we want to choose 0 people from the first group of n and 0 people from the second group of n. By the multiplicative principle, since these choices are independent, there are

$$\binom{n}{0} \cdot \binom{n}{0} = \binom{n}{0}^2$$

ways to do this. Similarly, if the committees have k people, a similar analysis tells us that there are

$$\binom{n}{k}^2$$

ways to create the committees. Hence, by the additive principle, the total number of ways to create the equal side committees is

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2.$$

On the other hand, observe that we can create the committees by choosing k people in the first group to belong to the committee and choosing $n-k$ people in the second group to not belong to the committee.

Doing this guarantees that both committees have the same number of people. Furthermore, we are choosing $k + (n - k) = n$ people from the big group of $2n$ when we do this. Therefore, we have

$$\binom{2n}{n}$$

ways to create the equal side committees. Since we are counting the same thing, it follows that

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}.$$

$\square$

Part III
Mini Unit 3

20 Why Graphs?

Graphs are a very useful tool to approach a lot of problems. There are many situations that you can model with graphs, so understanding how to work with them is very useful. Any time you are dealing with relationships between pairs of objects, you can phrase your problem as a graph. At a party, you can model how people greet each other with a graph. You can describe friend networks, public transportation, highways, data sets, etc. using graphs.

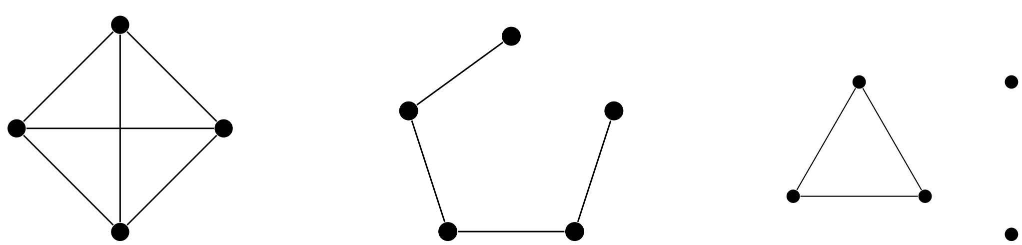
Graphs are easily one of the most applicable structures we will study in this course. They show up everywhere in computer science and mathematics. In fact, both Stacy and myself have recently engaged in graph-related research[7]! As such, I hope that you will learn a lot and have fun with this unit. Graphs can be scary at first, but they can also be fun to work with.

21 Graphs

In this section we discuss the basic definitions related to graphs.

21.1 Basic Definitions

In the figure below, we have three examples of graphs:



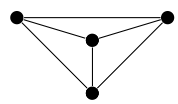
(a) (b) (c)

The purpose of a graph is to represent relationships between pairs of objects. We do this by representing each object with a **vertex** and drawing an **edge** between two vertices if they satisfy the relationship. For example, we can represent a group of 4 people who all know each other using graph (a). Graph (a) has 4 vertices, one for each person. Furthermore, observe that we have drawn an edge between every pair of

[7]Funny enough, our research also intersects with quantum mechanics.

vertices, signifying that evey pair of people know each other. The specific geometric layout of the vertices and edges is not important, we only care about the relationships that they encode. We will discuss this more in Section 21.3. As an exercise, try to come up with two situations that can be modeled with graphs (b) and (c), respectively.

Warning! Notice that the point of intersection of two edges is **not** a vertex of the graph. This is a geometric apparition, not combinatorial information. For graph (a), we could have just as well drawn it with no intersections:



Drawing a graph without intersecting edges is not always possible. Just remember, we only care about the actual vertices and edges, not intersection points or anything else that arises from the geometric layout.

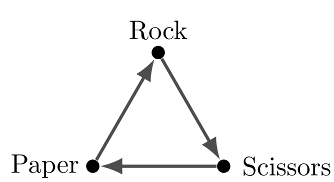
To talk about graphs abstractly, we have some common notation. Graphs themselves are commonly denoted by the letter G. The set of vertices of a graph is called its **vertex set**, and is usually denoted by V or V_G. Its size is called the **size** or **order** of G and is usually denoted by[8] $n, |G|, |V|$, or V. The set of edges of a graph is called its **edge set**, and is usually denoted by E or E_G. The number of edges is usually denoted by $m, k, |E|$, or E.

We say that two vertices v, w are **adjacent** if the graph has some edge connecting v and w. We also say that v and w are **neighbors**. Each edge has two **endpoints**, the two vertices that it connects. We say that an edge is **incident** on a vertex if that vertex is one of its endpoints.

There are many types of graphs that one can consider and which type of graph you are dealing with will depend on the application at hand. For this class, we will focus on simple graphs. What exactly makes a graph simple?

If some vertex is adjacent to itself, that means that there is some edge that connects the vertex with itself. Such an edge is called a **loop**. If there are two edges that have the exact same endpoints, we say that our graph is a **multigraph**. For this class, we will assume that a graph has no loops and is not a multigraph. Therefore, no edge can connect a vertex with itself and there is at most one edge between any pair of vertices.

Sometimes, the relationship that we are examining is directional. For example, a graph representing the game of rock, paper, scissors would look as follows:



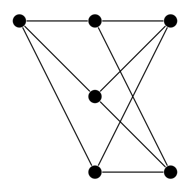
Here, we draw an edge from one vertex to the other if that option beats the other! Since beating is a one-sided relationship, we add an arrow to indicate this directionality. Rock beats scissors, but scissors does not beat rock. Graphs where the edges have a direction are called **directed graphs**. In this course, we will mostly focus on **simple graphs**, which are graphs that are not multigraphs, have no loops, and are not directed.

[8] Sometimes, V means both the set and the size of the set. This is an abuse of notation, which you will soon discover mathematicians love to do.

This is definitely not an exhaustive list! There are many different situations that lend themselves to thinking about graphs with different properties. For example, one type of graph that arises in computer science which we have not discussed above is a **weighted graph**. In a weighted graph, we additionally assign a number to each edge, called its **weight**. This weight can represent the strength of the relationship or the cost to move from one vertex to another. We will use weighted and directed graphs to tackle the stable matching problem in Section 24.1.

Warning! As you can tell, there are many different types of graphs we can work with depending on our objective. Sometimes, some of these adjectives will be written out explicitly. More often, you will only read the word "graph". So, always double check what definition of graph you are using to avoid any incorrect assumptions!

From now on, assume that every graph is simple unless otherwise stated. One of the most important notions in graph theory is the **degree** of a vertex. Simply put, the degree of a vertex is the number of edges incident to that vertex. In other words, the degree of a vertex is the number of edges connecting that vertex to other vertices. We denote the degree of a vertex v by $\deg(v)$. Observe that v has exactly $\deg(v)$ neighbors. We say that a graph is **regular** if every vertex has the same degree. More specifically, if every vertex has degree d, we say that the graph is $d-$**regular**. Below is an example of a $3-$regular graph:



Two particular examples of regular graphs are the **empty graph** and the **complete graph**. The empty graph on n vertices, denoted I_n, is the $0-$regular graph with n vertices. Thus, every vertex has degree 0. When a vertex has degree 0, we call it **isolated**, since it has no neighbors. The complete graph on n vertices, denoted K_n, is the $(n-1)-$ regular graph with n vertices. Thus, every vertex has degree $n-1$. Observe that this is the maximum degree a vertex can have in an $n-$vertex graph, since it only has $n-1$ possible neighbors. Thus, this graph has all possible edges between vertices.

I_5 K_5

Occasionally, we are interested in considering the relationships between a smaller group contained in the bigger group we are working with. For example, we may want to ask if in a party with 10 people subject to some restrictions, there exists a subset of 4 people who all know each other. We can phrase these questions using **subgraphs**. A subgraph H of a graph G is a graph formed by taking a subset of the vertices of G along with a subset of the edges connecting those vertices. We say the subgraph is **full** if we take all edges connecting those vertices. For example, I_5 is a subgraph of K_5, but it is not a full subgraph since we are omitting some edges. For the two graphs below, (b) is a full subgraph of (a).

(a) (b)

Our last definition of the section is a certain type of subgraph, called a **clique**. A $k-$**clique** is a complete subgraph on k vertices. That is, if the graph has k vertices with all edges between them, it has a $k-$clique. Finding $k-$cliques is a very well-studied problem in graph theory as it has applications to many real-world problems.

21.2 Paths

We can imagine a graph as a little town we can walk around in. Each vertex is a place we can go to and the edges are roads we can walk along. In fact,it may be the case that we are working with a graph that came from a situation like this! As such, we are interested in studying the different ways we have to move around a graph.

A **walk** is a sequence of vertices $(v_1, v_2, \ldots, v_k)$ such that consecutive vertices are adjacent. That is, there is always an edge between v_i and v_{i+1}. There are no restrictions on walks, we can use the same edge or pass through the same vertex as many times as we want. Alternatively, we can think of a walk as a sequence of edges $(e_1, e_2, \ldots, e_{k-1})$ such that consecutive edges share a common endpoint. A **trail** is a walk where we are not allowed to repeat edges. In other words, we do not want to backtrack and use the same edge more than once. However, note that we can still repeat vertices if we want. A **path** is a trail where we are not allowed to repeat vertices. Thus, in a path, every edge we use and every vertex we visit is different from all the edges we have used and all the vertices we have visited before, respectively. Finally, a **cycle** is a trail whose starting and ending vertices are the same and no other vertices are repeated. The **length** of a cycle is the number of edges that it uses. A graph is called **acyclic** if it has no cycles.

We say that a graph is **connected** if for every pair of vertices there is a path starting at one and ending at the other. Intuitively, this is saying that we can get to any vertex starting from any other. When a graph is not connected, we say it is **disconnected**. In such a case, we can talk about its **connected components**. A connected component is a connected full subgraph such that adding any other vertex necessarily makes it disconnected. Intuitively, each connected component is a connected piece of the graph that we cannot make any bigger. For example, graph (c) from the start of section 21.1 is disconnected and has 3 connected components.

We will talk more about paths, cycles, and connectedness in Section 26. As practice with these concepts, go through the graphs in these lecture notes. Which of these are acyclic? For those with cycles, what are the lengths of its cycles? Which of these are connected? For those that are disconnected, how many connected components does it have?

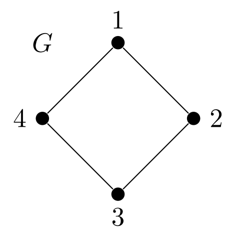
21.3 Graph Homomorphisms

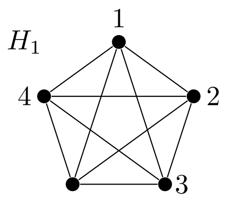
We can phrase a lot of relationships between graphs in terms of **graph homomorphisms**. This concept will encapsulate being a subgraph, having a clique, and two graphs being the same.

Definition 4: Graph Homomorphism

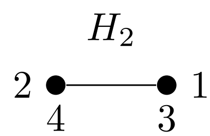
Let G and H be two graphs and let n be the order of G. Label the vertices of G using the integers $1, 2, \ldots, n$. Then, a graph homomorphism $G \to H$ is a way to distribute the n labels among the vertices of H such that if there is an edge between i and j in G, then there is an edge between i and j in H.
Observe that each vertex in H can get any number of labels; a vertex could get no labels, one label, or more than one label.

Below, (a) and (b) represent some graph homomorphisms and (c) shows a labeling that is not a graph homomorphism. Observe that G has a vertex between 1 and 2, but since H_3 has no loops, the labeling in (c) does not give an edge between 1 and 2 in H_3. Thus, (c) does not give a valid graph homomorphism.

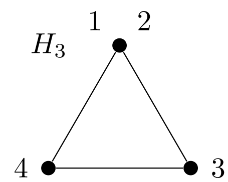




$G \to H_1$



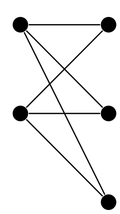
$G \to H_2$



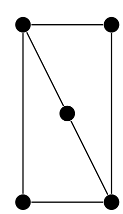
~~$G \to H_3$~~

As claimed before, we can rethink some notions in terms of graph homomorphisms. We say that a graph homomorphism $G \to H$ is **injective** if every vertex of H receives **at most one** label. Furthermore, we say that $G \to H$ is **full** if an edge between i and j in H implies an edge between i and j in G. For example, $G \to H_1$ above is injective but not full, while $G \to H_2$ is not injective but is full. If a graph homomorphism is both full and injective, we call it **fully injective**. Then, G is a subgraph of H if and only if there is an injective homomorphism $G \to H$. Furthermore, G is a full subgraph of H if and only if there is a fully injective homomorphism $G \to H$. These results are immediate from the definitions; as an exercise, prove them!
Since injective homomorphisms capture the notion of a subgraph, we can conclude that a graph G has a $k-$clique if and only if there is an injective homomorphism $K_k \to G$. Observe that such a homomorphism is also necessarily full. We will discover that colorings are related to homomorphisms $G \to K_k$ in Section 23.1.

We conclude with a discussion on when two graphs are the same. Consider the following two graphs:



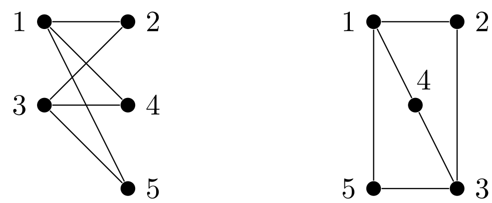
G_1



G_2

At first glance, these two graphs look different. However, it turns out that these graphs represent the same information, just laid out differently geometrically. Play around with moving the vertex and edge layout geometrically and try to convince yourself that these graphs indeed "are the same"! How can we say this formally? What we want to say that the two graphs have "the same" vertices and "the same" connections between vertices.
We can use graph homomorphisms to state this! We say that a graph homomorphism $G \to H$ is **surjective** if every vertex of H receives **at least one** label. If a graph homomorphism is both injective and surjective, we say it is **bijective**. Observe that a bijective graph homomorphism implies that the vertices of G and H can both be labeled using the integers $1, 2, \ldots, n$, so they must have the same number of vertices. So, should two graphs be considered "the same" if there is a bijective graph homomorphism between them? No! It could be the case that H has more edges than G. For example, there is a bijective graph homomorphism

$I_5 \to K_5$, but these graphs are certainly different. In order to ensure the edges also add up, we add the condition that the graph homomorphism be full. Then, there is an edge between i and j in G if and only if there is an edge between i and j in H. With all of these conditions, we will ensure that vertices are in one-to-one correspondence, edges are in one-to-one correspondence, and the relationships between vertices and edges is respected.
We call a fully bijective graph homomorphism $G \to H$ an **isomorphism** between G and H and say that G and H are **isomorphic**. This is the meaning of being "the same" in graph theory. We can now show that G_1 and G_2 above are isomorphic. Indeed, we have the following isomorphism:



$G_1 \to G_2$

We leave it as an exercise to verify that this is a full, injective, and surjective graph homomorphism.

22 Counting Edges

In this section we count edges and prove the powerful Handshake Lemma.

22.1 The Local-Global Principle

After so many definitions, we are finally going to prove some things about graphs! We are going to explore how we can use information about the degree of each vertex to deduce things about the number of edges and vice-versa.
We are trying to relate a **local** notion, the degree of each vertex, with a **global** property of the graph, the total number of edges. The degree of a vertex only gives us local information about what is going on near that vertex. We know that it has this many neighbors, but we do not get any information beyond that. The total number of edges gives us information about the totality of the graph. We know the graph as a whole has this many edges, but we do not get any specific information about where those edges are. Looking for these types of **local-global relationships** is a very common theme in combinatorics[9].
The words local and global here are more of an intuition than a mathematically precise statement. The key sentiment is that we have two quantities of very different natures. One gives more precise information in a small piece of our problem and the other gives broad information about the whole problem. Both types of information are valuable to understand the situation we are studying. Often, many interesting results describe how we can connect these two.

Identifying whether a problem is more local or global can help us solve it. Perhaps we have a problem that asks us to show some global property, but all our observations have been of a local nature. If we keep working locally, we will inevitably get stuck. At that point, we should ask ourselves: How can we paste together our local information to obtain the global picture? Thinking about how we can transform our local information into global data could be the key step we are missing to finish off the problem!

22.2 Handshakes

The specific local-global result that we are going to prove is the celebrated Handshake Lemma:

[9] And also geometry/topology!

Lemma 4: The Handshake Lemma

Let G be a graph with vertices $v_1, v_2, \ldots, v_n$ and E total edges. Then,

$$\deg(v_1) + \deg(v_2) + \ldots + \deg(v_n) = 2 \cdot E.$$

This is called the Handshake lemma because it is usually phrased in terms of handshakes at a party. If you have n people at a party and sum up how many handshakes each person gives, you get double the total number of handshakes!

Proof. We prove this by counting the size of the set

$$\{(v, e) \mid v \text{ is an endpoint of } e\}$$

in two different ways. On the one hand, we can do casework on the vertex. How many pairs of the form (v_j, e) do we have? The edge e has to be incident at v_j, so by definition, there are $\deg(v_j)$ such edges. Hence, the set has $\deg(v_j)$ pairs of the form (v_j, e). Since the choices of vertex are disjoint, the additive principle tells us the size of the set is

$$\deg(v_1) + \deg(v_2) + \ldots + \deg(v_n).$$

On the other hand, we can obtain a pair in the set by first choosing the edge e and then choosing the vertex v. We have E choices for the edge and no matter which edge we choose, we have 2 choices for v: the edge's two endpoints. Hence, the multiplicative principle tells us the size of the set is

$$2 \cdot E.$$

Since both quantities count the size of the set, they must be equal. $\square$

We can use this to count the total number of edges in some common graphs. For example, we can now count the total number of edges in the complete graph on n vertices, K_n. Recall that in this graph, every vertex has degree $n-1$. Therefore, the Handshake lemma tells us that

$$2 \cdot E = \underbrace{(n-1) + (n-1) + \ldots + (n-1)}_{n \text{ times}} = n \cdot (n-1).$$

Thus, K_n has $n(n-1)/2$ edges. You may recognize this number as $\binom{n}{2}$. Is this a coincidence? No! Indeed, notice that we could have counted the total number of edges in a different way. Each edge corresponds to a pair of vertices: its two endpoints. Therefore, for the complete graph, counting the number of edges is the same as counting the number of pairs of vertices. We know from Section 14.2 that this is $\binom{n}{2}$, agreeing with our previous computation.
We can use the same idea to count the number of edges of any regular graph. Suppose G is a $d-$regular graph with n vertices. Then, the Handshake lemma tells us that

$$2 \cdot E = \underbrace{d + d + \ldots + d}_{n \text{ times}} = n \cdot d.$$

Thus, G has $nd/2$ edges.

The Handshake lemma is a really powerful result that shows up frequently in graph theory problems. Make sure you understand how it works and play around with some graphs to get a feel for it!

23 Coloring

In this section we discuss concepts related to coloring vertices or edges of a graph.

23.1 Chromatic Number

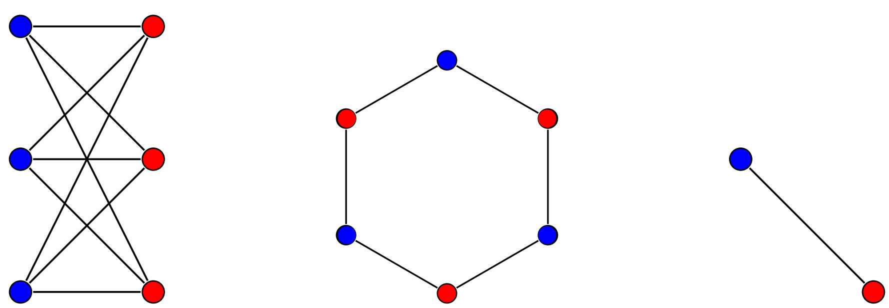
An interesting question we can ask about graphs is how we can color its vertices subject to some restrictions. Specifically, we will try to color the vertices of a graph such that no two adjacent vertices have the same color.

We say that a graph is $k-$colorable if we can color each vertex in one of k colors such that no two adjacent vertices have the same color. Now, note that if we allow ourselves to use sufficiently many colors, we can always color the vertices. Namely, if our graph, G, has n vertices, it is certainly $n-$colorable, as we can assign each vertex a different color and guarantee no adjacent vertices have the same color. So, we are interested in finding the **smallest** k such that G is $k-$colorable. This smallest k is called the **chromatic number** of G and it tells us the least number of colors we need to successfully color G. We denote the chromatic number of G by[10] $\chi(G)$.

How small can the chromatic number get? First of all, we always need at least one color, else we cannot color the vertices. Thus, $\chi(G) \geq 1$. What graphs have $\chi(G) = 1$? Observe that any two adjacent vertices must have different colors. So, if any two vertices are adjacent, we must have at least two colors. Since $\chi(G) = 1$ means that we only need one color, it follows that no two vertices are adjacent. Thus, our graph has no edges! Hence, if $\chi(G) = 1$ it follows that G must be an empty graph. Indeed, notice that if we color all vertices of an empty graph the same color, no two adjacent vertices have the same color.

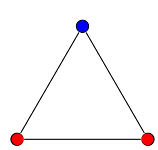
If G has at least one edge, we just argued that $\chi(G) > 1$. When can we get $\chi(G) = 2$? We call a $2-$colorable graph **bipartite**. The name can be explained by the following alternative definition: A graph is bipartite if we can partition its vertex set into two groups such that the endpoints of any edge lie in different groups. Bipartite and $2-$colorable coincide because the two colors precisely specify the two groups! As an exercise, prove that a graph is bipartite if and only if it is $2-$colorable.

Empty graphs are always bipartite! Since they are $1-$colorable, they are certainly $2-$colorable as well. Alternatively, we can also observe that partitioning the vertices into any two groups gives a valid bipartite partition, as there are no edges at all. Below are some more interesting examples of bipartite graphs:



Some example bipartite graphs.

Is every graph bipartite? It turns out that the answer is no. We can see this with the example of the complete graph K_3:



[10]Pronounced "kai" as in kite.

We show it is not 2−colorable. Suppose for the sake of contradiction that it were, and let blue and red be the two colors we are using. Consider one vertex and assume without loss of generality that it is colored blue. Then, since the other two vertices are adjacent to this blue vertex, they must be colored red. However, these two red vertices are adjacent, breaking the coloring restriction. This is the desired contradiction, so K_3 is not 2−colorable. We conclude that $\chi(K_3) > 2$. Since K_3 has 3 vertices, we also know that $\chi(K_3) \leq 3$, so $\chi(K_3) = 3$. Furthermore, note that if G has K_3 as a subgraph[11] then it can also not be bipartite! In fact, this is something that we can say more generally. If G is a subgraph of H, then $\chi(G) \leq \chi(H)$.

What exactly went wrong with K_3? To answer this question, let's take a look at **cycle graphs**. The cycle graph on n vertices, C_n, is the connected 2−regular graph with n vertices. Equivalently, you can think of a regular n−gon, whose vertices are vertices of the graph and whose edges are edges of the graph. Which cycle graphs are bipartite? It is straightforward to see C_n is bipartite when n is even. There is an example of this above. Is C_n bipartite when n is odd? Looking at the example of the triangle, you might conjecture that it is not. Indeed, we can show that C_n is bipartite if and only if n is even. We leave this as an exerciese.

In particular, we can conclude that if a graph has an odd cycle, it cannot be bipartite. We can show something even stronger. If a graph does not have any odd cycles, it must be bipartite. The key idea behind the proof is to try to color the graph. You will find that the only restriction to coloring it naively are odd cycles, so if there are not any, we can color successfully!
In summary, we can relate 2−colorability and cycle length with the following theorem:

Theorem 17: Bipartite graphs have no odd cycles

A graph G is bipartite if and only if it contains no cycles of odd length.

This settles our discussion of $\chi(G) = 2$. What can we say about higher chromatic numbers? One question is how big the chromatic number can get. We already said that $\chi(G) \leq n$, where n is the order of G. Can we do any better? It turns out that we cannot, at least not in general. In fact, our triangle example above illustrates why.

Lemma 5: Chromatic Number of Complete Graph

For any positive integer n we have

$$\chi(K_n) = n.$$

Proof. Since K_n has n vertices, we know that $\chi(K_n) \leq n$. We now show $\chi(K_n) \geq n$, which will establish the desired equality. Suppose for the sake of contradiction that $\chi(K_n) = c < n$. Then, we can color K_n using c colors such that no two adjacent vertices have the same color. Consider any vertex v of K_n. Observe that its $n-1$ neighbors must all be a different color than v. Therefore, we have $c - 1 < n - 1$ available colors for these $n-1$ vertices. By the pigeonhole principle, two vertices must have the same color, but since the graph is complete, they are adjacent. This violates the coloring restriction, contradicting that we can color K_n with less than n colors. So, $\chi(K_n) \geq n$, as claimed. □

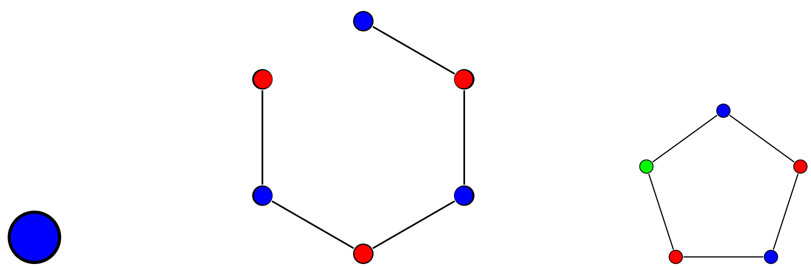
It is clear that what increased the chromatic number above was the huge degree of each vertex. So, it is reasonable to ask if smaller degrees lead to smaller chromatic number. Let's analyze a couple of examples to understand what we can say.

- Suppose that every vertex of G has degree at most 0. Then, every vertex is isolated, so G is an empty graph. Hence, $\chi(G) = 1$.
- Suppose that every vertex of G has degree at most 1. Then, a vertex is either isolated or is incident to exactly one edge. Observe that the other endpoint of this edge cannot have any more neighbors, since

[11] We also say G has a 3−clique or **triangle**.

its degree is also at most 1. Thus, G consists of isolated points and disjoint edges. In particular, G has no cycles, so it has no cycles of odd length. The theorem above then guarantees that $\chi(G) \leq 2$.

- Suppose that every vertex of G has degree at most 2. Then, every vertex has at most 2 neighbors. So, a connected component of G looks like an isolated vertex, a path of length at least 1, or a cycle of length of length at least 3.



Some possible connected components of a graph whose vertices have degree ≤ 2.

It is not hard to see that all of these options can be colored using only 3 colors. From our theorem above, we also do not expect to be able to do better, since odd length cycles cannot be $2-$colored. Hence, we conclude that $\chi(G) \leq 3$ and do not expect a better bound.

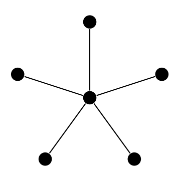
In fact, if every vertex has degree at most d, the best bound we can hope for is $\chi(G) \leq d+1$, since the complete graph K_{d+1} satisfies that every vertex has degree at most d and $\chi(G) = d+1$. It is an amazing fact that we can actually guarantee this bound!

Theorem 18: Maximum Degree and Colorability

Suppose that every vertex of G has degree at most d. Then, $\chi(G) \leq d+1$.

In order to prove this, we will use induction on the number of vertices of the graph. We discuss induction on graphs in Section 25.1, so we postpone the proof of this theorem until then.

Warning! Be careful not to assume the converse is true! Namely, it is **not** true that if $\chi(G) \leq d+1$, then every vertex of G has degree at most d. For example, the star graph below is bipartite, so its chromatic number is 2. However, observe that the central vertex has degree greater than 1.



We conclude this section by interpreting coloring in terms of graph homomorphisms. First, recall that a graph is $1-$colorable if and only if it is an empty graph. We can rephrase this using graph homomorphisms into the one vertex graph K_1. If there is a graph homomorphism $G \to K_1$, it must be the case that the single vertex in K_1 receives all the labels. However, recall that an edge between i and j in G would imply an edge between i and j in K_1. However, since K_1 has no loops, its has no edges. Thus, G cannot have any edge. So, a graph homomorphism $G \to K_1$ implies that G is empty. This works more generally:

Lemma 6: Colorings are Graph Homomorphisms

A graph G is $k-$colorable if and only if there exists a graph homomorphism $G \to K_k$.

Proof. The key idea is that we can think of each vertex of K_k as a color. Then, we color each vertex in G according to which vertex of K_k received its label. We now show this more formally.
Suppose that we have a graph homomorphism $G \to K_k$. Color G according to where the label of each vertex gets sent. Thus, color vertices sent to the same vertex of K_k the same color and vertices sent to different vertices of K_k different colors. Since K_k has k vertices, we will use at most k colors. Furthermore, if two vertices are adjacent in G, that means there is an edge between them. Thus, there is an edge between their corresponding labels in K_k. Therefore, their labels get sent to different vertices, so they are colored differently. Hence, adjacent vertices do not have the same color, so G is $k-$colorable.
Conversely, suppose that G is $k-$colorable. We use the colors to create a graph homomorphism to K_k. Assign to each vertex of K_k one of the k colors. Then, assign the label of each vertex of G to the vertex in K_k corresponding to the color we have painted the vertex. Since adjacent vertices are colored differently, if there is an edge between i and j in G, then i and j are different vertices in K_k, so there is an edge between them. Hence, we have constructed a graph homomorphism $G \to K_k$. □

Try to unwrap what this lemma is saying for bipartite graphs! Working out this specific example will give you a better feel for things.

Recall that if G is a subgraph of H, then $\chi(G) \leq \chi(H)$. Furthermore, recall from Section 21.3 that G is a subgraph of H if and only if there is an injective graph homomorphism $G \to H$. As it turns out, we can relax this condition a little and get a more general result!

Lemma 7: Graph Homomorphisms Increase Chromatic Number

If there is a graph homomorphism $G \to H$, then $\chi(G) \leq \chi(H)$.

Proof. Suppose that we have a graph homomorphism $G \to H$ and a $k-$coloring of H. We show that G can also be $k-$colored. Observe that this is enough to conclude $\chi(G) \leq \chi(H)$.
We color the vertex with label i in G the same color as the color of the vertex with label i in H. Since H is $k-$colored, this uses at most k colors. Furthermore, if two vertices are adjacent in G, their labels get assigned adjacent vertices in H. Since H is $k-$colored, these vertices must have different colors, so the two adjacent vertices in G also have different colors. Thus, we have colored G with k colors such that no two adjacent vertices are colored the same, as desired. □

As a specific use of this result, we can now show some results on whether graph homomorphisms between certain graphs exist. For example, since $\chi(C_6) = 2$ and $\chi(C_5) = 3$, the above lemma implies that there **does not exist** any graph homomorphism $C_5 \to C_6$. On the other hand, as an exercise, write down a graph homomorphism $C_6 \to C_5$.

23.2 Ramsey Theory

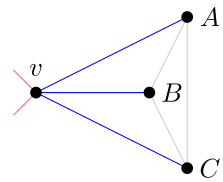
Instead of coloring vertices, we can also color edges. This is motivated by thinking about situations where there is more than one type of relationship between every pair of objects. For example, consider the following classic problem:

Example 22

In a certain group of 6 students, every pair of people are either friends or enemies. Show that we can choose 3 of them such that either they are all friends or they are all enemies.

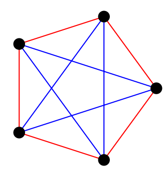
Proof. We can visualize the problem using graphs. In particular, consider a complete graph K_6 where we color an edge blue if the two people are friends and we color an edge red if the two people are enemies. Then, we want to prove that we can find a **monochromatic** triangle. That is, a $3-$clique whose edges are all the same color.
Consider a vertex v in the K_6. Since it is incident to 5 edges colored in 2 colors, the (generalized) pigeonhole

principle implies that there must be three edges of the same color. Without loss of generality, suppose they are all blue. Let A, B, and C be the three neighbors of v corresponding to these edges.



Now, observe that if any of the edges between A, B, and C are blue, we have a monochromatic blue triangle. Otherwise, all three edges are red and A, B, C is a monochromatic red triangle. In any case, we must have a monochromatic triangle, as desired. $\square$

This is the prototypical example of the type of problem studied in **Ramsey Theory**. In Ramsey Theory, we color the edges of a complete graph in various colors and try to figure out what we can say about monochromatic cliques in the graph. Specifically, we want to find the least number of vertices such that colorings guarantee a clique of some color. The above example tells us that, if we use two colors, we need at most 6 vertices to guarantee a monochromatic triangle. We cannot do better. The following K_5 does not have any monochromatic triangle:



Definition 5: Ramsey Numbers

The Ramsey number $R(n_1, n_2, \ldots, n_k)$ is the minimum number of vertices, n, needed to guarantee that if we color the edges of K_n using k colors, then there is either a monochromatic n_1-clique of color 1 or a monochromatic n_2-clique of color 2 or $\ldots$ or a monochromatic n_k-clique of color k.

In particular, $R(m, n)$ is the minimum number of vertices needed to guarantee that we can either find a blue $m-$clique or a red $n-$clique if we color using only blue and red. Additionally,

$$R(\underbrace{3, 3, \ldots, 3}_{k \text{ times}})$$

is the minimum number of vertices needed to guarantee a monochromatic triangle if we color using k colors. Our work above showed that $R(3, 3) = 6$. It is not terribly hard to show that $R(3, 3, 3) = 17$. In fact, you can use a similar idea to the above example to prove $R(3, 3, 3) \leq 17$. However, Ramsey numbers are absurdly hard to compute in practice. We do not even know the exact value of $R(5, 5)$. Furthermore, our best bounds for the values of the Ramsey numbers are not that good either. We have been able to show that

$$2^{n/2} \leq R(n, n) \leq 4^n,$$

but our best bounds are not much better than this. However, look at how bad these bounds are! When $n = 3$, we have $2\sqrt{2} \leq R(3, 3) \leq 64$. Recall we know $R(3, 3) = 6$.

It is truly amazing how such a complicated problem can arise from as simple an idea as coloring edges of a graph. The fact that this problem is so hard is not included here to discourage you. Rather, hopefully you are inspired to go learn more about Ramsey theory. Who knows, maybe you will be the first to compute $R(5, 5)$.

24 Matching

In this section we discuss concepts related to matching up vertices using edges of a graph.

24.1 Gale-Shapley

We will now use graphs to tackle a problem that arises in real life! Along the way, we will introduce the Gale-Shapley algorithm and show that it gives us a way to solve the problem. For this section only, we work with a directed, weighted graph.

The Stable Matching Problem

Let n be a positive integer. Suppose that we have n companies and n prospective employees. Each employee has ranked the companies by how much they want to work there. After reviewing all resumes, each company has ranked the employees by how much they want to employ them. Each company will hire exactly one employee. In an ideal world, once the hiring process is over, everyone is satisfied. In particular, we do not want there to be a company and an employee that would have both been happier if they ended up together instead of the actual result of hiring. Is it always possible to match the companies and employees to guarantee this does not happen?

We can phrase this in terms of a bipartite, directed, weighted graph. We will have $2n$ vertices, one group of n for the companies and one group of n for the employees. Then, for each company, we will have a directed edge into each employee, with the weight assigned to each edge representing how much the company wants to hire the employee. Similarly, each employee will have a directed edge into each company, with the weight assigned to each edge representing how much the employee want to work at the company.
This graph is bipartite since all edges connect companies to employees or vice-versa. It is directed because each edge has a direction and weighted because we assign a weight to its edge. Our goal is to find a **stable matching**. A matching is simply a way to pair up companies with employees. A matching is **unstable** if we can find a company C and an employee E that are not paired up such that C would prefer to hire E than their current employee and E would prefer to work at C than at their current company. A matching is **stable** if it is not unstable.

In 1962, Gale and Shapley provided an algorithm that always allows us to find a stable matching. In particular, their algorithm shows that a stable matching always exists. Furthermore, by adjusting the algorithm, we can decide who gets the better end of the stick, companies or employees. We now see how this works.

Theorem 19: The Gale-Shapley Algorithm

We prove every directed, weighted, bipartite graph with equal number of vertices in each part has a stable matching given by the following algorithm:
While the matching has not been completed, we repeatedly follow these steps:

1. A company that does not have a hired employee sends a job offer to their highest ranked employee that has not yet rejected them.

2. If the employee has the company ranked above the job offer they currently accepted (or have no offer at all), they accept the offer, rejecting any previous offers made.

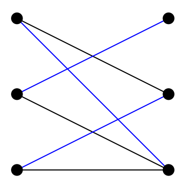
Once every company is matched up with an employee, the algorithm terminates.

Proof. First, how do we know that the algorithm will eventually end? Observe that each company makes at most n job offers, since they do not repeat offers once they have been rejected. Hence, at most $n \cdot n = n^2$ job offers will be made in total. So, after at most n^2 iterations, the algorithm must have ended. Now, we just have to show that the matching we are left with in the end is stable. Suppose for the sake of contradiction that it is unstable. Then, we can find a company C and an employee E such that C ranks E above their match and E ranks C above their match. Since C ranks E above their match, they must have sent a job offer to E before they sent a job offer to their match. If E accepted, then when E's match sent an offer, E would have rejected them, as they are ranked lower than C. If instead, E rejected, that means they had an offer from a company they ranked better than C. Again, they would not have accepted their match, as their matched is ranked lower than C. This is the desired contradiction, so the matching we end up with must be stable! ☐

This version of the algorithm favors companies over employees. This is because companies hold the power of sending offers. By sending the offers in order, the companies guarantee they will get the best ranked employee they possibly could have got from a stable matching. If we modified the algorithm so employees send the offers and companies accept or reject, then employees will be favored. By holding the power to send offers, employees can guarantee they will get the best ranked company they possibly could have got.

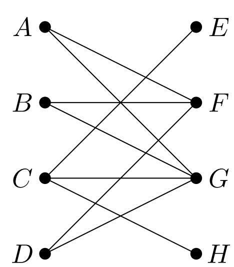
24.2 Hall's Marriage Lemma

We will cover one last matching result in this section. We return to unweighted simple graphs. Again, we are working with a bipartite graph where each of the groups has the same number of vertices, n. Our question now is whether we can find a **perfect matching**. In this context, a perfect matching is a set of n edges whose endpoints are all distinct. In other words, we want n disjoint edges such that every every vertex is the endpoint of exactly one edge. For example, a perfect matching in the bipartite graph below is marked by the blue edges:



A bipartite graph with a perfect matching.

We want to determine when such a perfect matching exists. First, we note that perfect matchings will not always exist. For example, if our bipartite graph has no edges, there is no way to choose edges to match vertices. The following is a more interesting counterexample:



At first glance, it may be hard to spot why there can be no perfect matching. However, observe that both E and H have degree 1. Therefore, in a perfect matching, they have to be matched to their unique neighbor. But, in this case, their unique neighbor is C for both! We cannot match C to both E and H, so there is no perfect matching.

The problem in both kinds of counterexamples was that some group of vertices had "too little" neighbors. We can formalize this as follows:

Definition 6: Hall's Condition

Let G be a bipartite graph with an equal number of vertices in each group. For X a set of vertices of G, let $N(X)$ be the set of vertices that are adjacent to some vertex in X. Observe that if X contains vertices in only one group, $N(X)$ only contains vertices in the other.
We say that G satisfies **Hall's condition** if for every subset of vertices, X, satisfying that all vertices are in one group, we have that

$$|X| \leq |N(X)|.$$

Essentially, we are saying that a graph satisfies this condition if whenever we take k vertices on one side, they have at least k neighbors on the other side. It should be clear why this condition is necessary to have a perfect matching. If we found k vertices on one side with less than k neighbors, pigeonhole tells us we will not be able to find a perfect matching. The magic of this condition is that it is also sufficient! That is, if a graph satisfies Hall's condition, then we will be able to find a perfect matching.

Theorem 20: Hall's Marriage Theorem

A bipartite graph G with an equal number of vertices in each group has a perfect matching if and only if it satisfies Hall's condition.

25 Induction on Graphs

In this section, we show how to perform induction on graphs and a common error to avoid.

25.1 Removing a Vertex

One way to prove things about graphs is by inducting on the number of vertices the graph has. As usual with induction proofs, the trickiest step will be the inductive step. This is especially tricky with graphs, as we have to track both vertex and edge information. However, it is still possible to do this if we are smart about how we reduce to the induction hypothesis.

Induction on Graphs Template

Say we want to prove that if some graph G satisfies property P, then it must also satisfy property Q. A proof by induction on the number of vertices of the graph will, in general, be as follows:

(1) **Base Case**: We first establish any necessary base cases. This is usually showing that Property P implies Property Q for graphs with $1, 2$, and sometimes 3 vertices. Since there are not that many graphs with so little vertices, this step should be straightforward.

(2) **Inductive Hypothesis**: Sometimes just assuming property P implies property Q when G has $n-1$ vertices is enough. For other problems, we may have to assume P implies Q for all $k < n$.

(3) **Inductive Step**: This is usually where we have to be clever. We start with some arbitrary graph G with n vertices that satisfies Property P. Then, we make some smart choice for a vertex v of G. Then, we use our choice of v to argue that the subgraph G' obtained by deleting v and all its incident edges also satisfies Property P. Since G' has $n-1$ vertices, the inductive hypothesis applies, so G' has property Q. Then, we argue that adding back v and its edges still preserves property Q. This will conclude the induction.

Oftentimes, the hardest part of the problem is to find the right choice of v. We need some vertex such that removing it and adding it back plays nicely with the properties we want to show. Sometimes, any choice of v will work.

We now use induction to prove the following theorem from Section 23.1:

Theorem 18: Maximum Degree and Colorability

Suppose that every vertex of G has degree at most d. Then, $\chi(G) \leq d+1$.

Proof. We proceed by induction on the number of vertices of G.

(1) **Base Case**: Our base case is $|G| = 1$. If G only has one vertex, its degree is 0. Thus, its degree is at most d. Furthermore, clearly $\chi(G) = 1 \leq d+1$. Hence, the statement holds for $|G| = 1$, establishing our base case.

(2) **Inductive Hypothesis**: Assume that if $|G| = n-1$ and every vertex has degree at most d, then $\chi(G) \leq d+1$.

(3) **Inductive Step**: Let G be an arbitrary graph with $|G| = n$ and every vertex with degree at most d. Let v be any vertex of G. Consider the subgraph G' obtained by removing v and all its incident edges. Since we only remove edges, we can only possibly decrease the degree of the vertices in G'. Therefore, every vertex of G' has degree at most d. Furthermore, $|G'| = n-1$, so by the inductive hypothesis we know that $\chi(G') \leq d+1$. Thus, we can color G' using $d+1$ colors. Given such a coloring, color G exactly the same as G'. The only vertex left to color is v. However, since $\deg(v) \leq d$, it follows that v is adjacent to at most d vertices. Since we have $d+1$ colors available, there is at least one color that is not adjacent to v. Hence, if we paint v that color, we obtain a $(d+1)-$coloring of G. Thus, $\chi(G) \leq d+1$, which concludes the induction.

□

Induction on graphs is especially powerful when we can guarantee our graph has **leaves**. A leaf is a vertex of degree exactly 1. Leaves are good for induction because removing a leaf also removes exactly one edge, so the changes to the graph are easier to handle. Let's look at this in action:

Lemma 8: Connected Graphs have Edges

If G is a connected graph with n vertices, then G has at least $n-1$ edges.

Proof. We proceed by induction on n.

(1) **Base Case:** Our base case is $n = 1$. In this case, G has one vertex and no edges. Observe that G is connected, since every pair of vertices has a path connecting them[12]. Furthermore, $0 = 1 - 1$, so the statement holds. This establishes our base case.

(2) **Inductive Hypothesis**: Suppose that if G is a connected graph with $n-1$ vertices, then G has at least $n-2$ edges.

(3) **Inductive Step**: Let G be an arbitrary connected graph with n vertices. If every vertex of G has degree at least 2, then by the Handshake lemma we know that

$$E \geq \frac{1}{2}\left(\underbrace{2+2+\ldots+2}_{n \text{ times}}\right) = n,$$

so G has at least n edges and the statement is true. Otherwise, we may assume there is some vertex of degree at most 1. Observe that if such a vertex had degree 0, it would be isolated, which prevents

[12]Here, there are no pairs! Hence, this is one of the vacuous truths we introduced in Section 6.2

G from being connected. Thus, we may assume G has a leaf v. Consider the subgraph G' obtained by deleting v and its incident edge. Since G is connected, for every pair of vertices u, w in G' there is a path in G connecting them. Now, observe that such a path could not pass through v, as that would require backtracking through its incident edge, which a path is not allowed to do. Hence, when we remove v, such a path still exists. In other words, u, w are connected by a path in G', so G' is a connected graph. Furthermore, we know it has $n-1$ vertices, so by the induction hypothesis, it has at least $n-2$ edges. Then, since G is obtained from G' by adding back a vertex and an edge, it follows that G has at least $(n-2)+1 = n-1$ edges. This concludes the induction.

□

We wrap up this section by looking at one more example of induction on graphs:

Lemma 9: Too many Edges give Cycles

Let $n \geq 3$ be an integer. If G is a connected graph with n vertices and n edges, then G contains exactly one cycle.

Proof. We proceed by induction on n.

(1) **Base Case**: Our base case is $n = 3$. If G is a connected graph with 3 vertices and 3 edges, then G must be C_3, which, as a cycle graph, contains exactly one cycle. This establishes the base case.

(2) **Inductive Hypothesis**: Suppose that if G is a connected graph with $n-1$ vertices and $n-1$ edges, then G contains exactly one cycle.

(3) **Inductive Step**: If every vertex of G has degree at least 2, then by the Handshake Lemma, every vertex has degree exactly 2. Thus, G is a connected $2-$regular graph, so it is isomorphic to C_n. This contains exactly one cycle, so the statement is true. Otherwise, we can find a leaf v of G. Consider the subgraph G' obtained by deleting v and its incident edge. As argued before, G' is connected. Furthermore, observe that G has $n-1$ vertices and $n-1$ edges. Thus, by the inductive hypothesis, G' contains exactly one cycle. When we add back v and its edge, no new cycles can be created, so G also contains exactly one cycle. This concludes the induction.

□

25.2 Build-Up Error

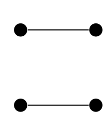
Warning!

When doing induction on graphs, there is one common pitfall we must strive to avoid at all costs. Consider the following false proposition:

Too Connected

If every vertex of a graph has positive degree, then the graph is connected.

Observe that the converse is true, if a graph is connected, then every vertex has positive degree. However, we must not fall for any logical traps! This statement is false. For example, the graph below has every vertex with positive degree, but it is not connected.



Since the statement is false, there must be an error in the following induction proof:

Bogus Proof. We proceed by induction on the number of vertices of the graph.

(1) **Base Case**: Our base cases are one vertex and two vertices. A one-vertex graph cannot have any vertex of positive degree, so the statement is true vacuously. If in a two vertex graph every vertex has positive degree, then there is an edge between the two vertices, so the graph is connected. This establishes our base case.

(2) **Inductive Hypothesis**: Assume that if a graph has $n-1$ vertices and all of its vertices have positive degree, then the graph is connected.

(3) **Inductive Step**: Consider a graph with $n-1$ vertices such that all its vertices have positive degree. By the inductive hypothesis, it is connected. Now, add a vertex, v, to obtain a n vertex graph. Since we assume every vertex has positive degree, there must be an edge incident to v. This edge connects v to the rest of the graph, so the graph is connected. This proves the inductive step, which concludes the induction.

□

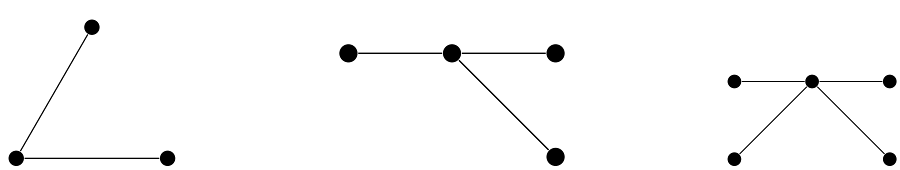
As usual with wrong proofs by induction, the problem is in the inductive step. Observe that we are not following our template. Instead of starting with a graph with n vertices and reducing to less vertices, we start with a graph with $n-1$ vertices and build up to a graph with n vertices. Why is this wrong? This does not work because not every graph with n vertices satisfying the property can be built up from a graph with $n-1$ vertices satisfying the property. Indeed, consider our counterexample above. If we remove a vertex from it, we end up with an isolated vertex, violating the positive degree condition. If we want to build it up from a smaller graph, we would have to go to $n-2$ vertices. However, in such a case, the inductive step does not work.

It is crucial to avoid the build-up error when doing our induction proofs. We often think of graphs as built up from smaller graphs and this intuition can be helpful for some problems. However, it is important to avoid a build-up induction proof. When proving things for all graphs, we have to make sure we consider arbitrary graphs, not just graphs we can build up from smaller cases. So, when you apply this technique, always follow the template: start with an arbitrary graph, find a way to remove a vertex smartly, and then argue why the induction step works. Doing this will ensure you do not fall for the build-up error and all your induction proofs will work.

26 Trees

In this section we discuss trees, probably the most important types of graphs we will study.

Recall that a graph is called **acyclic** if it does not have any cycles. Then, a **tree** is an acyclic, connected graph. Below we have some examples:



Some example trees.

Trees are, in some sense, the simplest possible connected graphs. Recall from Section 25.1 two key facts:

1. If a graph is connected, it has at least $n-1$ edges.
2. If a connected graph has n edges, then it has a cycle.

Trees are right in the middle of these behaviors. They have enough edges to be connected, but not enough to contain cycles. In particular, this gives us our first important result about trees:

Lemma 10: Tree Edge Count

Let T be a tree with n vertices. Then, T has exactly $n-1$ edges.

Try to prove this using induction on n.

In particular, this shows that trees are **minimally connected** and **maximally acyclic**. What do we mean by minimally connected? Since a tree has the minimum number of edges required to be connected, removing any edge from the tree disconnects the graph. Thus, in this sense, trees are the smallest connected graph. Similarly, since adding an edge to the tree would make it have a cycle, trees are the biggest connected graphs without cycles.

Suppose we start with an arbitrary connected graph. In general, it will not be a tree, since it could have cycles. However, observe that if we remove an edge from a cycle, the graph stays connected[13]. Thus, we can remove some edges from the graph until we remove all cycles. When we do this, we end up with a tree as a subgraph of the graph. Such a tree is called a **spanning tree** of the graph. More explicitly, a spanning tree of G is a subgraph of G that is a tree and contains all vertices of G.

Trees are especially susceptible to proofs by induction, as they always have leafs. In fact, trees always have at least two leaves! You will prove this fact and some other fun facts about trees in your pset.

Part IV
Mini Unit 4

27 Algebra

In this section, we will learn some useful algebra facts that will help us solve some combinatorics problems more easily.

27.1 Geometric Series

Recall the following lemma from Section 10:

Lemma 3: Powers of 2

Let n be a natural number. Then,

$$1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1.$$

We saw how to prove this by induction, but how could we have obtained the right hand side to begin with? For example, can we find a similar simplification for the following sum?

$$1 + 3 + 9 + \ldots + 3^n.$$

This type of sum is called a **geometric series**. Let's break this name down. A **sequence** of numbers is an ordered list of numbers. In a sequence, numbers can occur more than once and order matters. For example,

[13] Prove this from the definition of connectedness!

the sequences $(1, 2, 3)$ and $(1, 3, 2)$ are different. Sequences can be either finite or infinite. Abstractly, we denote the sequence whose $n-$th term is the number a_n by

$$(a_k)_{k=\text{start}}^{\text{end}},$$

where "start" and "end" are the first and last index of our sequence. For example,

$$(2k+1)_{k=0}^{4}$$

is the sequence $(1, 3, 5, 7, 9)$, while

$$(2^k)_{k=0}^{\infty}$$

is the sequence of all powers of two.

The **series** of a sequence is the sum of the elements of the sequence. So, for example, the series of $(1, 3, 5, 7, 9)$ is $1 + 3 + 5 + 7 + 9 = 16$. Above, we saw that the series of the sequence $(2^k)_{k=0}^{n}$ is $1 + \ldots + 2^n = 2^{n+1} - 1$. We have to be more careful when our sequence is infinite. For example, what is the series of $(2^k)_{k=0}^{\infty}$? We know that if we cut it off at some finite n we get $2^{n+1} - 1$. So, as we get to higher and higher n, the value of the series keeps growing and growing, exploding off to infinity. When a series explodes off to infinity we say that it **diverges** and call it a **divergent series**. When the value of a series is some finite number, we say that it **converges** and call it a **convergent series**. Observe that if the series is finite, it always converges.

A sequence is called **geometric** if the ratio between consecutive terms is always the same. That is, there exists some number r such that $a_{k+1} = ra_k$ for all k. This r is called the **common ratio** of the geometric sequence. For example, the sequence of all powers of two is a geometric sequence with common ratio 2. A **geometric series** is the series of some geometric sequence. Computing the values of geometric series is a problem that arises often in mathematics, so it would be convenient if we had some formula to compute it.

Theorem 21: Geometric Series Formula

For all real numbers a, r with $r \neq 1$, we have that

$$a + ar + ar^2 + \ldots + ar^n = \frac{ar^{n+1} - a}{r - 1}.$$

Proof. The key idea behind this result is to exploit the relationship between the terms of a geometric sequence. Let $S = a + ar + ar^2 + \ldots + ar^n$. Then, $rS = ar + ar^2 + \ldots + ar^n + ar^{n+1}$. Observe how similar S and rS are. In fact, S and rS share all terms but the first in S and the last in rS. Therefore, we expect a lot of simplification if we subtract them. We get that

$$\begin{aligned} rS - S &= (\cancel{ar} + \cancel{ar^2} + \ldots + \cancel{ar^n} + ar^{n+1}) \\ &\quad - (a + \cancel{ar} + \cancel{ar^2} + \ldots + \cancel{ar^n}) \\ (r-1)S &= ar^{n+1} - a \\ S &= \frac{ar^{n+1} - a}{r - 1}, \end{aligned}$$

as claimed. □

This formula allows us to prove Lemma 3 more easily. We have a geometric series with start term $a = 1$ and common ratio $r = 2$, so our formula gives

$$1 + 2 + \ldots + 2^n = \frac{1 \cdot 2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$

We can now find a closed form for $1+3+\ldots+3^n$. In this case, we have a geometric series with start term $a=1$ and common ratio $r=3$. Then, our formula gives

$$1+3+\ldots+3^n=\frac{3^{n+1}-1}{3-1}=\frac{1}{2}(3^{n+1}-1).$$

What happens when our geometric is infinite? We already argued that the series of powers of 2 diverges. Similarly, when we look at the series of all powers of 3, as we take more and more terms, the value of the series grows and grows, exploding off to infinity, so the series diverges. In general, when $|r|>1$, we will have a divergent geometric series. We can see this from our formula above. If $|r|>1$, then as n gets larger and larger, r^{n+1} will also get larger and larger, so the term ar^{n+1} explodes off to infinity and the series diverges. What happens when $r=1$ or $r=-1$? If $r=1$, then our geometric series is of the form

$$a+a+a+\ldots,$$

which clearly diverges. When $r=-1$, our geometric series is of the form

$$a-a+a-a+\ldots$$

Here, if we cut off our sum at some specific term, we will either get a or 0 and as we add each term, the series alternates between these values. Although in this case the value of the series does not explode off to infinity, since the series does not "decide" between a and 0, we still say the series diverges. There simply is no logical value to give the series as we take it to be infinite.

Finally, what happens when $|r|<1$? In this case, r^{n+1} becomes smaller and smaller as n gets large, getting closer and closer to 0. For example, if $r=\frac{1}{2}$, already at $n=9$ we have $|r^{n+1}|<0.001$. Thus, it makes sense to say that when we take the series to be infinite, the r^{n+1} term will vanish to 0. Thus, for $|r|<1$, we should have

$$a+ar+ar^2+\ldots=\frac{0-a}{r-1}=\frac{a}{1-r}.$$

The most famous example is when $a=r=\frac{1}{2}$. In this case, we get

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\ldots=\frac{\frac{1}{2}}{1-\frac{1}{2}}=\frac{\frac{1}{2}}{\frac{1}{2}}=1.$$

Although the discussion when the series is infinite was a little informal, the results that we got are correct! In order to formalize them we need the tools of calculus, which we will not get into here. However, now you have the formulas necessary to compute any geometric series, finite or infinite.

27.2 Functions

Functions may seem a little abstract when we are first introduced to them. However, it is a concept that we have been secretly using throughout this course. Simply put, functions are a way to mathematically formalize the concept of assigning things to objects. The set up is the following: we start with two sets A and B. Our goal is to assign to each element of A exactly one element of B. For example, A could be a set of pigeons and B a set of pigeonholes and we want to put each pigeon in exactly one pigeonhole. Or A could be $\mathbb{R}$ and B could be $\mathbb{Z}$ and we want to assign to each real number exactly one integer. A **function**, f, is exactly such an assignment, where each element of A gets assigned exactly one element of B. We say that f is a function **from** A **to** B and write $f\colon A\to B$. The set A is called the **domain** of f and the set B is called its **codomain**. Finally, if $a\in A$, we denote by $f(a)\in B$ the element that f assigns to A in B.

We have already dealt with functions several times in this course, even if we did not explicitly refer to them as such. For example, back in Section 16.2 we discussed bijections. We did this to switch our problem from counting the elements of A to counting the elements of B. These bijections were functions $A\to B$ that satisfied some more properties. We just encountered another example of a function last section, when we defined sequences! We can think of a sequence of real numbers

$$(a_k)_{k=m}^n$$

as a function $f\colon \{m, m+1, m+2, \ldots, n\} \to \mathbb{R}$, where $a_k = f(k)$. Similarly, an infinite sequence of real numbers is a function $f\colon \mathbb{N} \to \mathbb{R}$. Functions show up all the time in math, even if they are often hidden behind the scenes.

27.3 Polynomials

In this section, we concern ourselves with a specific type of functions $\mathbb{R} \to \mathbb{R}$, called polynomials. These are, in some sense, the simplest possible functions assigning real numbers to real numbers.

Given a real number x, what operations can we do on x and still get a real number? One option is to forget about x entirely and just give any real number a. This gives us a function $f\colon \mathbb{R} \to \mathbb{R}$, called a **constant** function. This function takes in any real number and assigns it to the real number a. Thus, we can describe it by the formula

$$f(x) = a,$$

where we think of x as representing an arbitrary real number. There are more interesting operations we can do on real numbers. For example, if we start with x, we could instead multiply it by a and get ax. This gives another function, given by the formula

$$f(x) = ax.$$

Another thing we can do is first multiply x by itself, or square it, to get the real number x^2. This gives another function, given by the formula

$$f(x) = x^2.$$

If instead of squaring, we took a third, fourth, or $n-$th power, we get more functions. Furthermore, observe that we can multiply by any real number after taking the $n-$th power. Thus, for any $n \in \mathbb{N}$ and any $a \in \mathbb{R}$, we get a function $f\colon \mathbb{R} \to \mathbb{R}$ given by the formula

$$f(x) = ax^n.$$

Such a tern ax^n is called a **monomial**. Its exponent n is called the **degree** of the monomial and the number a in front of the x^n is called its **coefficient**. However, we do not need to stop at a single term in our function. We can add up several monomials together. A **polynomial** is a function $P\colon \mathbb{R} \to \mathbb{R}$ given by a formula

$$P(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,$$

where n is a natural number and $(a_0, \ldots, a_n)$ is a sequence of real numbers. The **degree** of P is the maximum exponent of all its monomials, which according to the formula above would be n. The sequence $(a_0, \ldots, a_n)$ is called the **coefficients** of P. The coefficient a_0 is called the constant coefficient of the polynomial. The coefficient a_n is called the leading coefficient of the polynomial and, unless $P(x) = 0$, it is always non-zero. When the leading coefficient is 1, we call P **monic**.

We have specific names for polynomials of low degree. We already saw that polynomials of degree 0 are called **constant polynomials**. Polynomials of degree 1 are called **linear**[14]. Degree 2 polynomials are called **quadratic**, degree 3 **cubic**, degree 4 **quartic**, and degree 5 polynomials are called **quintic**. There is no need to give specific names to higher degree polynomials, as we do not often deal with them in practice.

Warning! The case of $P(x) = 0$ deserves some attention. Even though it is a constant polynomial, there are several reason why we do not want to say it has degree 0. For example, it technically does not have any

[14]If you were to graph them, you obtain a line.

monomials at all, since we have not added anything at all. There are more reasons that you will learn as you study more about polynomials, however we do not get into them here. Because of these reasons, we say that the degree of $P(x) = 0$ is either undefined or $-\infty$.

One interesting question we can ask about polynomials is when they assign a real number to 0. Given a polynomial $P(x)$, we call r a **root** or **zero** of the polynomial if $P(r) = 0$. Constant polynomials teach us that roots do not always exist. For example, if $P(x) = 3$, what r satisfies $P(r) = 0$? None of them, since $P(r) = 3 \neq 0$. However, linear polynomials teach us that roots can exist. If $P(x) = a_1x + a_0$, when do we have $P(r) = 0$? We can solve the equation for r explicitly:

$$\begin{aligned} 0 &= P(r) \\ 0 &= a_1 \cdot r + a_0 \\ -a_0 &= a_1 \cdot r \\ -\frac{a_0}{a_1} &= r. \end{aligned}$$

Observe that since P has degree 1, we must have that $a_1 \neq 0$, so we can always do that last division. Thus, $a_1x + a_0$ always has exactly one root and it equals $-a_0/a_1$. We will study roots of quadratic polynomials in the next section. The case for cubic and quartic polynomials is a little more complicated, but there are still explicit formulas for the roots. Once we get to quintic polynomials and beyond, however, we can show that there is no explicit formula that gives the roots of a general polynomial of degree at least 5. This is a famous problem called the unsolvability of the quintic and its proof involves the tools of Galois Theory.

27.4 The Quadratic Formula

We now look to find a general formula for the roots of a quadratic polynomial. We start by analyzing the simplest type of quadratic polynomials: those of the form $x^2 - a$. We can explicitly solve for the roots in this case. We want $r^2 - a = 0$, so $r^2 = a$. Now, if a is nonnegative, we can just take square roots and conclude that $r = \pm\sqrt{a}$. If a is negative however, there is no real number such that $r^2 = a$. Thus, if $a < 0$, the polynomial $x^2 - a$ has no real roots[15]. Thus, we have three things that can happen when dealing with $x^2 - a$. If $a < 0$, there are no real roots. If $a = 0$, we have exactly one real root, $r = 0$. If $a > 0$, we have exactly two real roots, $r = \pm\sqrt{a}$. Furthermore, note that when we have real roots ($a \geq 0$), we can rewrite our polynomial:

$$x^2 - a = (x - \sqrt{a})(x + \sqrt{a}).$$

Check this explicitly by expanding out the right hand side.

We use the $x^2 - a$ example to solve for the roots of more general quadratic polynomials. In order to do this, we will use the following identity:

$$(x - b)^2 = x^2 - 2b \cdot x + b^2.$$

Check this explicitly by multiplying out the left hand side. This identity is useful because it will allow us to reduce to the case of taking square roots.

Example 23

Find the roots of $x^2 - 2x - 3$.

Solution. We claim the roots are 3 and -1. We recognize from the identity above that $x^2 - 2x + 1 = (x-1)^2$. Therefore,

$$x^2 - 2x - 3 = (x^2 - 2x + 1) - 4 = (x - 1)^2 - 4.$$

[15]Once you learn about complex numbers, you will be able to take square roots of negative numbers. We do not deal with complex numbers in this course.

Hence, r is a root of $x^2 - 2x + 3$ if and only if it is a root of $(x-1)^2 - 4$. Thus, we want

$$\begin{aligned}(r-1)^2 - 4 &= 0 \\ (r-1)^2 &= 4 \\ r - 1 &= \pm 2 \\ r &= 1 \pm 2,\end{aligned}$$

so $r = 3$ or $r = -1$, as desired. □

This technique of finding how to rewrite a quadratic polynomial using an expression of the form $(x-b)^2$ is called **completing the square**. As you just saw, it is really helpful to find roots of quadratic polynomials. In fact, it will allow us to give a formula for the roots of any quadratic polynomial:

Theorem 22: Quadratic Formula

Let a, b, c be real numbers with $a \neq 0$. Then, if $b^2 - 4ac \geq 0$, the roots of the quadratic polynomial $ax^2 + bx + c$ are given by

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

If $b^2 - 4ac < 0$, then the polynomial has no real roots.

Proof. We want to solve the equation $ar^2 + br + c = 0$ for r. We begin by dividing by a, which we can do since a is nonzero. Thus, we want

$$r^2 + \frac{b}{a} \cdot r + \frac{c}{a} = 0.$$

We attempt to complete the square. Comparing $(x - B)^2 = x^2 - 2B \cdot x + B^2$ with the above expression, we see that in order to match the coefficients in front of x, we need $B = -\frac{b}{2a}$. Observe that

$$\left(r + \frac{b}{2a}\right)^2 = r^2 + \frac{b}{a} \cdot r + \frac{b^2}{4a^2}.$$

Hence, we get

$$\begin{aligned} r^2 + \frac{b}{a} \cdot r + \frac{c}{a} &= 0 \\ \left(r^2 + \frac{b}{a} \cdot r + \frac{b^2}{4a^2}\right) + \frac{c}{a} - \frac{b^2}{4a^2} &= 0 \\ \left(r + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2} &= 0 \\ \left(r + \frac{b}{2a}\right)^2 &= \frac{b^2 - 4ac}{4a^2}. \end{aligned}$$

If $b^2 - 4ac < 0$, the right hand side is negative, so it cannot possibly be the square of a real number. Thus, if $b^2 - 4ac < 0$, the polynomial has no real roots. If $b^2 - 4ac \geq 0$, then

$$\begin{aligned} r + \frac{b}{2a} &= \pm \frac{\sqrt{b^2 - 4ac}}{2a} \\ r &= \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}, \end{aligned}$$

as claimed. □

We conclude this section with an observation on the roots of a quadratic polynomial. If r_1, r_2 are the real roots of $ax^2 + bx + c$, then

$$ax^2 + bx + c = a(x - r_1)(x - r_2).$$

Try to prove this yourself!

27.5 Partial Fraction Decomposition

Sometimes, when dealing with functions, we will end up with a polynomial in the denominator. Ideally, we would like these polynomials to be as simple as possible, in order to make things easier to work with. However, sometimes we will end up with quadratic or higher degree polynomials in the denominator. We will see how to transform a quadratic polynomial in the denominator to a sum of fractions with linear polynomials in the denominators. Our technique, called **partial fraction decomposition**, works more generally, but we will only use quadratic polynomials in this course.

Our first example is

$$\frac{1}{x(x-1)}.$$

We wish to rewrite this as a sum of fractions with something simpler in the denominator. Since our denominator is a product of two linear factors, x and $x-1$, we are hopeful that we can write

$$\frac{1}{x(x-1)} = \frac{A}{x} + \frac{B}{x-1}$$

for some constants A and B. To find A and B, we assume the above equality is true and clear denominators. Then,

$$1 = A(x-1) + Bx.$$

This should hold for all values of x, so we can pick some convenient ones that eliminate one of A or B. If we plug in $x = 1$ above, we see that $1 = B$. Similarly, plugging in $x = 1$ we get $1 = -A$, so $A = -1$. Hence, we see that

$$\frac{1}{x(x-1)} = \frac{1}{x-1} - \frac{1}{x},$$

and you can combine the fractions on the right to check this explicitly.

This method works more generally. Namely, let's decompose:

$$\frac{1}{(x-a)(x-b)},$$

when $a \neq b$. We guess that

$$\frac{1}{(x-a)(x-b)} = \frac{A}{x-a} + \frac{B}{x-b},$$

which after clearing denominators becomes

$$1 = A(x-b) + B(x-a).$$

Then, plugging in $x = a$ gives $1 = A(a-b)$, so $A = 1/(a-b)$ and plugging in $x = b$ gives $1 = B(b-a)$, so $B = 1/(b-a)$. Thus, we see that

$$\frac{1}{(x-a)(x-b)} = \frac{1}{a-b}\left(\frac{1}{x-a} - \frac{1}{x-b}\right).$$

We can apply the same method when our numerator is different from 1 or even depends on x. Lastly, if our denominator is not already written as a product, we can use the previous section to discover how to rewrite it. This technique will work as long as the polynomial has two different real roots. If it does not have any, we do not have linear factors to divide it in. If it has only one root, a similar technique works, but we have to be more careful. We do not go into these details as we will not need them.

27.6 Power Series

Power series are a sort of formal generalization of polynomials. A **power series** in x is a possibly infinite sum of monomials of the form $a_k x^k$. In the case when the sum is finite, we recover polynomials. Thus, every polynomial is a power series, although not every power series is a polynomial. We cannot always think of a power series as a function $\mathbb{R} \to \mathbb{R}$. However, the utility of power functions comes from being able to manipulate them like "infinite" polynomials even if they no longer represent functions. Power series show up all the time in calculus, physics, and complex analysis. We will see a cool combinatorial use for them in Section 30.1.

As a teaser for the power of power series, we see how they relate to geometric series. Consider the power series

$$1 + x + x^2 + x^3 + \ldots$$

Observe that each term is the previous term multiplied by x. Therefore, this is really just an infinite geometric series with start term $a = 1$ and common ratio $r = x$. Our formula for the geometric series tell us that

$$1 + x + x^2 + \ldots = \frac{1}{1-x}.$$

You may worry about using our formula blindly here. Are we not supposed to have —x—¡1 in order for our formula to apply? You would be right to worry, as if we were to plug in $x = 2$ above, we get the absurd equation

$$1 + 2 + 4 + 8 + \ldots = -1.$$

However, the power behind power series is that we can pretend that we are working with an x such that the above formula makes sense. We do not have to pick a specific value of x, we can just manipulate our power series as if things worked out and get mathematically valid results from this. We will see how to use this for combinatorics in Section 30.2.

28 The Fibonacci Numbers

In this section we introduce the Fibonacci Sequence and showcase some cool identities involving its terms.

The Fibonacci sequence is one of the most famous sequences in mathematics. Its first ten terms are given below:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$$

Observe that each term in the sequence is given by the sum of the previous two. For example, $13 = 8+5$. Let F_n denote the $n-$th Fibonacci number, where we start indexing with $n = 0$. Thus, $F_0 = 0, F_1 = 1, F_2 = 1$, and so on. Using this notation, our observation tells us that

$$F_n = F_{n-1} + F_{n-2} \tag{3}$$

for all $n \geq 2$. As we will see in the next section, the Fibonacci sequence are our first example of recursively defined sequences. One of our most powerful tools when dealing with recursive sequences is (strong) induction.

Lemma 11: Sum of Fibonacci

Let n be a natural number. Then,

$$F_0 + F_1 + \ldots + F_n = F_{n+2} - 1.$$

Proof. We proceed by induction on n.

(1) **Base Case**: For $n = 0$, we have $F_0 = 0$ and $F_{0+2} - 1 = F_2 - 1 = 1 - 1 = 0$. Thus, the equation is true for $n = 0$, establishing our base case.

(2) **Inductive Hypothesis**: Suppose that

$$F_0 + \ldots + F_{n-1} = F_{n+1} - 1.$$

(3) **Inductive Step**: Observe that

$$\begin{aligned} F_0 + \ldots + F_{n-1} + F_n &= (F_0 + \ldots + F_{n-1}) + F_n \\ &= F_{n+1} - 1 + F_n \\ &= (F_n + F_{n+1}) - 1 \\ &= F_{n+2} - 1, \end{aligned}$$

where we have used the inductive hypothesis for the second equality and the defining equation (3) for the last equality. This concludes the induction.

□

Warning! Working with recursive sequences leads us to emphasize the importance of the base case when doing induction! Indeed, observe that the equation $F_n = F_{n-1} + F_{n-2}$ is not enough to define the Fibonacci sequence. If we started with $L_0 = 2$ and $L_1 = 1$ and followed the same equation $L_n = L_{n-1} + L_{n-2}$, we obtain instead the Lucas numbers:

$$2, 1, 3, 4, 7, 11, 18, 29, \ldots$$

Observe that the inductive step in the above proof only uses the defining equation and not any specific values. However, some results we will prove for Fibonacci numbers are not true for Lucas numbers! Thus, we must never forget the base case, as it will decide whether or not statements are true!

As an exercise, prove the following identity:

$$F_1 + F_3 + F_5 + \ldots + F_{2n-1} = F_{2n}.$$

We continue showcasing the power of induction to deal with the Fibonacci numbers with two more cool identities:

Lemma 12: Sum of Squares of Fibonacci

Let n be a natural number. Then,

$$F_0^2 + F_1^2 + \ldots + F_n^2 = F_n F_{n+1}.$$

Proof. We proceed by induction on n.

(1) **Base Case**: When $n = 0$, we have $F_0^2 = 0$ and $F_0 F_1 = 0 \cdot 1 = 0$, so the equation is true for $n = 0$, establishing our base case.

(2) **Inductive Hypothesis**: Suppose that

$$F_0^2 + \ldots + F_{n-1}^2 = F_{n-1} F_n.$$

(3) **Inductive Step**: Observe that

$$\begin{aligned} F_0^2 + \ldots + F_{n-1}^2 + F_n^2 &= (F_0^2 + \ldots + F_{n-1}^2) + F_n^2 \\ &= F_{n-1} F_n + F_n^2 \\ &= F_n (F_{n-1} + F_n) \\ &= F_n F_{n+1}, \end{aligned}$$

where we have used the inductive hypothesis for the second equality and equation (3) for the last equality. This concludes the induction.

$\square$

Lemma 13: Cassini's Identity

Let n be a positive integer. Then,

$$F_n^2 - F_{n-1}F_{n+1} = (-1)^{n-1}.$$

Proof. We proceed by induction on n.

(1) **Base Case**: When $n = 1$, we have $F_1^2 - F_0F_2 = 1^2 - 0 \cdot 2 = 1$ and $(-1)^{n-1} = (-1)^0 = 1$. Thus, the equation is true for $n = 1$, establishing our base case.

(2) **Inductive Hypothesis**: Suppose that

$$F_{n-1}^2 - F_{n-2}F_n = (-1)^{n-2}.$$

(3) **Inductive Step**: Observe that

$$\begin{aligned}
F_n^2 - F_{n-1}F_{n+1} &= F_n^2 - F_{n-1}(F_n + F_{n-1}) \\
&= F_n^2 - F_{n-1}F_n - F_{n-1}^2 \\
&= F_n(F_n - F_{n-1}) - F_{n-1}^2 \\
&= F_nF_{n-2} - F_{n-1}^2 \\
&= (-1)(F_{n-1}^2 - F_nF_{n-2}) \\
&= (-1) \cdot (-1)^{n-2} \\
&= (-1)^{n-1},
\end{aligned}$$

where we repeatedly used equation (3) and the inductive hypothesis. This concludes the induction.

$\square$

Hopefully these proofs have convinced you that the Fibonacci sequence is pretty cool. The Fibonacci sequence shows up often and unexpectedly in all sorts of places, including math, computer science, and even nature! To give you a taste of why we are taking a look at it, we conclude this section with a combinatorics problem where the Fibonacci numbers unexpectedly show up.

Example 24

Let n be a natural number. We have a bathroom floor in the shape of a rectangle with dimensions $2 \times n$. We wish to tile the floor using tiles of dimensions 2×1 or 1×2. In how many ways can we tile the floor, if we have to cover every square with a tile and the tiles cannot overlap?

When trying out these types of problems, it is always a good idea to try out small cases! When $n = 0$, we have no squares to cover, so we can tile the floor in exactly one way: do nothing. When $n = 1$, we have to cover a 2×1 rectangle. The only way to do so with our pieces is by placing one 2×1 tile. When $n = 2$, we have two possible tilings: we use two 2×1 tiles or two 1×2 tiles. Finally, let's look at $n = 3$. In this case, we can either do three 2×1 tiles, or one 2×1 tile and two 1×2 tiles. In this second case we have two options: we either place the 2×1 all the way to the left or all the way to the right. Thus, our sequence of answers so far looks like $1, 1, 2, 3$. So far, this looks like the Fibonacci sequence! It is at this point that we attempt to prove that it actually is. For this problem, we will be successful!

Solution. We claim the answer is F_{n+1}. We proceed by induction on n.

(1) **Base Case**: By trying out small cases above, we have already shown our base case. In particular, for $n = 0$ we know there are $1 = F_1$ ways to tile the floor and for $n = 1$ there are F_2 ways. This establishes our base case.

(2) **Inductive Hypothesis**: We assume that there are F_{n-1} ways to tile a $2 \times (n-2)$ floor and F_n ways to tile a $2 \times (n-1)$ floor.

(3) **Inductive Step**: We do casework on the orientation of the tile covering the bottom left square. If this tile is a 2×1, then after placing it we want to tile the $2 \times (n-1)$ rectangle remaining to the right. From the inductive hypothesis, we know that there are F_n ways to do this. If this tile is a 1×2, then the only tile that can cover the top left square must also be a 1×2. Thus, the left-most 2×2 square is covered, so it remains to tile the remaining $2 \times (n-2)$ rectangle. BY the inductive hypothesis, we know that there are F_{n-1} ways to do this. Thus, by the additive principle, there are $F_n + F_{n-1} = F_{n+1}$ ways to tile the bathroom floor.

□

29 Recursion

In this section we introduce recursive sequences and how to find closed forms for their terms.

29.1 Sequences

We were already introduced to sequences in the last section, by looking at the Fibonacci numbers. Sequences are abundant in combinatorics. When trying to count some quantity that depends on n, we naturally get a sequence defined by the answer for each n. We saw this in Example 24 above, where the answer for each n corresponded to the (shifted) Fibonacci sequence. For other problems, the sequence may be different, but we are still interested in finding an explicit value for each n. The sequences that occur in combinatorics are often recursive in nature. As such, we take this time to study them more in depth.

A **recursive sequence** $(a_k)_{k=0}^{\infty}$ is a sequence such that the term a_n is defined by the previous terms $a_0, a_1, \ldots, a_{n-1}$. It is not necessary to use all terms. For example, the Fibonacci sequence is a recursive sequence. The term F_n is defined by the terms F_{n-1} and F_{n-2}. Recursive sequences arise naturally when a problem can be decomposed into smaller instances of the same problem. We saw this in Example 24. We could solve the problem for n from the solutions for $n-1$ and $n-2$. Thus, this gave us a **recursive formula**

$$a_n = a_{n-1} + a_{n-2},$$

which we recognize coincides with the formula for the Fibonacci numbers. After checking the initial terms coincided, we could use induction to show the solution to the problem was precisely the Fibonacci sequence!

We now showcase some problems that show how recursive series show up when solving combinatorics problems[16]:

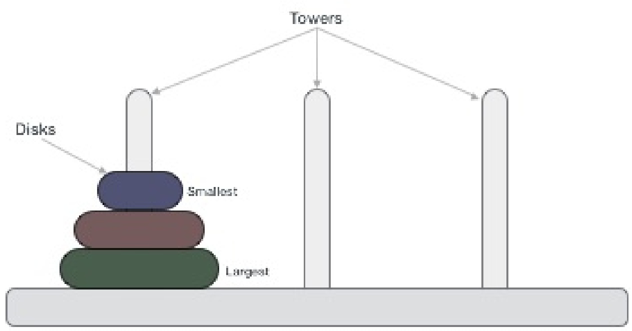
Example 25 (Towers of Hanoi)

Let n be a natural number. We have three towers in a line and n disks of different radii, initially placed such that the n disks are all on the leftmost tower, ordered in size so that the smallest disk is at the top and the largest at the bottom. A move consists in moving the topmost disk of a tower to a different tower, subject to the restriction that we cannot place a disk on top of a smaller disk. What is the least number of moves needed to end up with all n disks piled up in the rightmost tower?

I recommend that you try playing[17] with the problem before reading its solution. You can try several n at the following website: Towers of Hanoi.

[16] Image obtained from tutorialspoint.com

[17] The good thing about combinatorics is that some problems are games you can entertain yourself with.



The Towers of Hanoi Problem for $n = 3$.

Solution. Let H_n be the solution to the problem for n. We show $H_n = 2^n - 1$.
In order to move all the disks to the rightmost tower, we must at some point move the largest disk to the right. However, the only way to do this is if the largest disk has no disk on top of it and there is no other disk in the rightmost tower. Therefore, the remaining $n-1$ disks must have been moved to the second tower. Observe that this process is analogous to the problem for $n-1$, so this first step takes at least H_{n-1} moves. Then, we move the largest disk to the right, which takes 1 move. Finally, we must move the $n-1$ disks from the second tower to the third. Again, this is analogous to the $n-1$ problem, so it takes at least H_{n-1} moves. In fact, by doing the optimal solution for the $n-1$ disks, we know the whole process will take $H_{n-1} + 1 + H_{n-1}$ moves and we cannot do any better. Therefore, we conclude that

$$H_n = 2H_{n-1} + 1.$$

We have obtained a recursive formula! In order for this formula to give us the value of H_n, we need to know some initial term. In our case, we want to figure out what H_0 is. If we have no disks, we need no moves to move them all to the rightmost tower, so $H_0 = 0$. Armed with this knowledge, we can now conclude by induction on n.

(1) **Base Case**: When $n = 0$ we get $H_0 = 0$ and $2^0 - 1 = 0$, so $H_0 = 2^0 - 1$, establishing our base case.

(2) **Inductive Hypothesis**: Assume that $H_{n-1} = 2^{n-1} - 1$.

(3) **Inductive Step**: We have that

$$H_n = 2H_{n-1} + 1 = 2(2^{n-1} - 1) + 1 = 2^n - 2 + 1 = 2^n - 1,$$

where we used the inductive hypothesis and the recursive formula. This concludes our induction.

□

Look at how easy the induction was when we phrased things using a recursive sequence! The key idea in this type of problem is to use our combinatorics techniques to obtain the recursive formula. Then, we can use algebra to obtain the answer for each n.

You may be wondering how we knew the answer was going to be $2^n - 1$. After all, at first glance there is not really anything from $H_n = 2H_{n-1} + 1$ that suggests this formula will be true. One way we could have reached the $2^n - 1$ number is by trying small cases. We already saw $n = 0$ yields 0. Then, if we only have one disk, we only need 1 move: we just move it to the right. The case for two disks is a little more involved, but it is straightforward to see we need 3 moves. After finding that three disks require 7 moves, the pattern starts to manifest itself: $0, 1, 3, 7$. These are all one less than a power of 2. With this, we might conjecture that the answer is $2^n - 1$ and we know for sure once we run the induction and see that everything checks out.

The following problem shows that finding such a neat formula is not always that easy:

Example 26

Call a sequence of integers *good* if it only contains the integers $1, 2,$ and 3. For example, $(1, 2, 1, 2, 3, 2, 3)$ is good, but $(1, 2, 5, 2, 1)$ is not. Let C_n be the number of good sequences of length n that do not contain two consecutive 3's nor a 1 followed by a 3. Find a recursive formula for C_n.

Let's start by analyzing small cases. There is only one good sequence of length 0: the empty sequence. It certainly does not contain two consecutive 3's nor a 1 followed by a 3, so $C_0 = 1$. Similarly, we see that all good sequences of length 1 are valid, so $C_1 = 3$. Next, all good sequences of length 2 except for $(3, 3)$ and $(1, 3)$ are valid, so we have $C_2 = 3^2 - 2 = 7$. If our sequence has length 3, we can do casework on the last term. If it is 1 or 2, there are no restrictions on the other two terms other than that they cannot be $(3, 3)$ nor $(1, 3)$, which gives us $7 \cdot 2 = 14$ valid sequences. If the last term is 3, then the second must be 2 and the first can be any of $1, 2, 3$. Thus, we get 3 valid sequences. By the additive principle, $C_3 = 17$. What is the pattern here?

$$1, 3, 7, 17, \ldots$$

Whatever it is, it is certainly much harder to guess than for the previous example. We conclude this section by finding a recursive formula for this sequence. We give an explicit formula of C_n in the next section, using the tools we develop there.

Solution. We claim $C_n = 2C_{n-1} + C_{n-2}$. We model our approach from the case work we did to calculate C_3. We do casework on the last term of the sequence. If the last term is 1 or 2, our restrictions do not impose anything on the first $n - 1$ terms, other than following the restrictions themselves. Thus, we want a sequence of length $n - 1$ following the restrictions. We know that there are C_{n-1} such sequences. Since we had two options for the last digit, the multiplicative principle tells us that, in this case, there are $2C_{n-1}$ sequences. If the last term is 3, then the second-to-last term cannot be 1 nor 3. Therefore, it must be 2. However, no more restrictions are imposed on the remaining $n - 2$ terms. Thus, we have C_{n-2} sequences in this case. Thus, the additive principle tells us that

$$C_n = 2C_{n-1} + C_{n-2},$$

as claimed. □

29.2 Closed Forms

Recursive formulas are nice and useful, but oftentimes what we are really after is the **closed form** of the sequence. The closed form of a sequence is a formula that gives each term without using any other terms of the sequence. It is explicitly **not recursive**. For example, we saw above that the sequence $(H_n)_{n=0}^{\infty}$ that satisfies $H_0 = 0$ and

$$H_n = 2H_{n-1} + 1,$$

has the closed form

$$H_n = 2^n - 1.$$

In an ideal world, we can extract the closed form for a sequence from its recursive formula and the initial values. In this section we see how to do this for some recursive formulas.

Consider a sequence $(a_n)_{n=0}^{\infty}$ such that $a_0 = a$ and $a_n = 2a_{n-1}$. Can we find a closed form for a_n? Computing for small values, we see that $a_1 = 2a_0 = 2a, a_2 = 2a_1 = 4a, a_3 = 2a_2 = 8a$, and so on. From these examples, it seems that $a_n = 2^n \cdot a$. We can prove this using induction! The proof is fairly straightforward, so we omit it, but make sure that you know how to replicate it.

This is the first technique we have for finding closed forms. We compute the first few values of the sequence and guess what the closed form is. Then, we can use induction to prove that our guess is correct. This is how we have been rolling so far, and it worked for this sequence and the Towers of Hanoi. However, once the closed form becomes more complicated, it can be almost impossible to guess. For example, we currently have no idea what the closed form of C_n from Example 26 is. Furthermore, I challenge you to guess the closed form of the Fibonacci numbers! If you have not seen it before, it is really hard to guess.

So, we need a more universal method to find closed forms. We will show how to do this for recursive formulas of the form

$$a_n = A \cdot a_{n-1} + B \cdot a_{n-2},$$

where[18] $A^2 + 4B > 0$. This covers many of the sequences you will encounter when solving combinatorics problems and we will be able to find the closed form for C_n and the Fibonacci numbers.

Our method is inspired by our answer for $a_n = 2a_{n-1}$. Observe we can generalize this: if $a_0 = a$ and $a_n = ra_{n-1}$, then the closed form for a_n is $a_n = ar^n$. Thus, when we only have one term in the recursive formula, we get some sort of exponential behavior, depending on the coefficient present. When we add dependence on a_{n-2}, we expect things to change a little. However, we still expect some sort of exponential behavior. This expectation will allow us to make an educated guess for the closed form, which will turn out to give us the answers we search for.

Let $(a_n)_{n=0}^{\infty}$ be a sequence such that $a_n = A \cdot a_{n-1} + B \cdot a_{n-2}$. We guess[19] that there is some constant λ such that $a_n = \lambda^n$. If our guess is true, what are the possible values that λ can take on? We can substitute into the recursive formula:

$$\begin{aligned}
a_n &= A \cdot a_{n-1} + B \cdot a_{n-2} \\
\lambda^n &= A \cdot \lambda^{n-1} + B \cdot \lambda^{n-2} \\
\lambda^2 &= A\lambda + B \\
\lambda^2 - A\lambda - B &= 0,
\end{aligned}$$

where we divided by λ^{n-2} to get the third equality. Thus, we see that if $a_n = \lambda^n$, then we must have that λ is a root of the quadratic polynomial $x^2 - Ax - B$. We know we can find the roots of the quadratic polynomial by using the quadratic formula. It will have real roots as long as $A^2 + 4B \geq 0$ and it will have two different roots if $A^2 + 4B > 0$. Thus, we assume from now on that $A^2 + 4B > 0$. We get

$$\lambda = \frac{A \pm \sqrt{A^2 + 4B}}{2}.$$

We see that there are two possible values for λ. We call them λ_+ and λ_-, where λ_+ corresponds to taking $+$ in front of the square root above and λ_- corresponds to taking $-$. What we have concluded is that if we set $a_n = \lambda_\pm^n$, then the sequence will satisfy the formula $a_n = A \cdot a_{n-1} + B \cdot a_{n-2}$. Furthermore, note that this is still true if we set $a_n = C\lambda_+^n + D\lambda_-^n$. We have:

$$\begin{aligned}
A \cdot a_{n-1} + B \cdot a_{n-2} &= A(C\lambda_+^{n-1} + D\lambda_-^{n-1}) + B(C\lambda_+^{n-2} + D\lambda_-^{n-2}) \\
&= C\lambda_+^{n-2}(A\lambda_+ + B) + D\lambda_-^{n-2}(A\lambda_- + B) \\
&= C\lambda_+^{n-2} \cdot \lambda_+^2 + D\lambda_-^{n-2} \cdot \lambda_-^2 \\
&= C\lambda_+^n + D\lambda_-^n \\
&= a_n.
\end{aligned}$$

How do we choose C and D? They will depend on what values the sequence starts with. Namely, if we know a_0 and a_1 explicitly, we can use them to solve for C and D. An example will illustrate how to do this in practice:

[18] We can generalize this method to the case $A^2 + 4B = 0$ and even to formulas with dependence on more terms. However, for this course, we will only focus on the simplest possible case.

[19] This type of educated guess is often called an **ansatz** and it is a common way to solve these types of equations. When you learn about differential equations, this term will come up again.

Example 27

Let $(a_n)_{n=0}^{\infty}$ be a sequence such that $a_0 = 3, a_1 = 5$ and $a_n = 2a_{n-1} + 3a_{n-2}$. Find a closed form for a_n.

Solution. Guessing a solution $a_n = \lambda^n$, we see that λ has to be a root of

$$\lambda^2 - 2\lambda - 3.$$

Using the quadratic formula, we see that

$$\lambda_{\pm} = \frac{2 \pm \sqrt{4+12}}{2} = 1 \pm 2,$$

so that $\lambda_+ = 3$ and $\lambda_- = -1$. Therefore, we know

$$a_n = C \cdot 3^n + D \cdot (-1)^n,$$

for some constants C and D. We use a_0 and a_1 to compute C and D. Plugging in $n = 0$, we see that

$$3 = a_0 = C \cdot 3^0 + D \cdot (-1)^0 = C + D.$$

Plugging in $n = 1$, we see that

$$5 = a_1 = C \cdot 3^1 + D \cdot (-1)^2 = 3C - D.$$

Adding both equations, $8 = 4C$, so $C = 2$. Substituting back in the first equation, we get $D = 1$. Therefore,

$$a_n = 2 \cdot 3^n + (-1)^n.$$

To double check our answer, we can use induction to prove this closed form satisfies the initial terms and the recursive formula. □

We conclude by finding closed forms for C_n and F_n. Recall that the sequence $(C_n)_{n=0}^{\infty}$ satisfied the recursive formula

$$C_n = 2C_{n-1} + C_{n-2}.$$

Therefore, if we guess $C_n = \lambda^n$, we know λ has to be a root of

$$\lambda^2 - 2\lambda - \lambda.$$

Using the quadratic formula, we get that

$$\lambda_{\pm} = \frac{2 \pm \sqrt{4+4}}{2} = 1 \pm \sqrt{2}.$$

Hence, we know that

$$C_n = C(1+\sqrt{2})^n + D(1-\sqrt{2})^n$$

for some constants C and D. Recall that we computed $C_0 = 1$ and $C_1 = 3$. These values give the system of equations

$$\begin{cases} 1 &= C + D \\ 3 &= C(1+\sqrt{2}) + D(1-\sqrt{2}). \end{cases}$$

Solving this system gives $C = (1+\sqrt{2})/2$ and $D = (1-\sqrt{2})/2$. Therefore, the closed form of C_n is

$$C_n = \frac{1}{2}\left((1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\right).$$

This is certainly not obvious from computing the starting terms of the sequence!

Theorem 23: The Binet Formula

Let
$$\varphi = \frac{1+\sqrt{5}}{2}, \phi = \frac{1-\sqrt{5}}{2}.$$
Then, the closed form of the Fibonacci numbers is
$$F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - \phi^n\right).$$

The number φ is called the **golden ratio** and shows up everywhere the Fibonacci sequence appears. It is a very important constant and you can even find it in nature!

Proof. Recall the Fibonacci sequence satisfies the recursive formula
$$F_n = F_{n-1} + F_{n-2}.$$
Therefore, if we guess $F_n = \lambda^n$, we see λ must be a root of the quadratic polynomial
$$\lambda^2 - \lambda - 1.$$
Using the quadratic formula, the roots are
$$\lambda_{\pm} = \frac{1 \pm \sqrt{5}}{2},$$
so $\lambda_+ = \varphi$ and $\lambda_- = \phi$. Thus,
$$F_n = C\varphi^n + D\phi^n$$
for some constants C and D. Recall that $F_0 = 0$ and $F_1 = 1$. The first term gives us
$$0 = C + D,$$
so $C = -D$. The second term gives us
$$1 = C(\varphi - \phi) = C\sqrt{5},$$
so $C = 1/\sqrt{5}$. Thus,
$$F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - \phi^n\right),$$
as claimed. □

As an exercise, try to prove this formula by induction!

30 Generating Functions

In this section, we introduce generating functions and see how to use them to solve combinatorics problems and find closed forms of recursive sequences.

30.1 Counting Problems

Given a sequence $(a_k)_{k=0}^{\infty}$, we define the **generating function** of the sequence to be the power series
$$A(x) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + a_3 \cdot x^3 + \dots$$

If the sequence is finite, then this power series is a polynomial! For example, if our sequence is defined by

$$b_k = \binom{n}{k},$$

the generating function is

$$B(x) = \binom{n}{0} + \binom{n}{1}x + \ldots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n.$$

Interestingly, recall that Newton's Binomial theorem tells us that $B(x) = (x+1)^n$. As we will see soon, this is no coincidence!

Another example is the generating function of the Fibonacci numbers:

$$F(x) = 0 + x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + \ldots$$

There does not seem to be any clear pattern. In the next section, we will find a more explicit expression for the generating function.

Generating functions can be helpful to solve combinatorics problems. It turns out that polynomial multiplication perfectly encapsulates the additive principle in some cases. This is best illustrated by an example.

Example 28

There are three urns in a house. One has 3 red balls, another has 3 green balls, and the third has 2 pink balls. Balls of the same color are indistinguishable. In how many ways can we grab 5 balls from the urns?

Of course, it is not too complicated to simply list out all possibilities. In fact, here they are, listed out in a table: So, there are 9 ways to do this. However, generating functions can do all the busy work for us.

Red	Green	Pink
0	3	2
1	2	2
1	3	1
2	1	2
2	2	1
2	3	0
3	0	2
3	1	1
3	2	0

We illustrate how in the proof below:

Solution. We represent the possibilities for each urn with a generating function. Namely, each urn has a sequence given by the number of ways to pick n balls. Namely, for the urn with red balls, we have the sequence $(r_n)_{n=0}^{\infty}$ where r_n denotes the number of ways to pick n balls from the red urn. Since the balls are indistinguishable and there are three of them, $r_0 = r_1 = r_2 = r_3 = 1$ and $r_n = 0$ for $n \neq 0, 1, 2, 3$. Thus, the generating function for the red urn is

$$R(x) = 1 + x + x^2 + x^3.$$

Similarly, the generating function for the green urn is

$$G(x) = 1 + x + x^2 + x^3$$

and the generating function for the pink urn is

$$P(x) = 1 + x + x^2.$$

It turns out that grabbing balls from all urns is perfectly encapsulated by the product:

$$\begin{aligned} R(x)G(x)P(x) &= (1 + x + x^2 + x^3)(1 + x + x^2 + x^3)(1 + x + x^2) \\ &= 1 + 3x + 6x^2 + 9x^3 + 10x^4 + \boxed{9x^5} + 6x^6 + 3x^7 + x^8. \end{aligned}$$

In particular, the number of ways to grab 5 balls from the urns is given by the coefficient in front of x^5. We read off the coefficient 9, so there are 9 ways to grab 5 balls from the urns. $\square$

Red	Green	Pink	x^5 term
0	3	2	$1 \cdot x^3 \cdot x^2$
1	2	2	$x \cdot x^2 \cdot x^2$
1	3	1	$x \cdot x^3 \cdot x$
2	1	2	$x^2 \cdot x \cdot x^2$
2	2	1	$x^2 \cdot x^2 \cdot x$
2	3	0	$x^2 \cdot x^3 \cdot 1$
3	0	2	$x^3 \cdot 1 \cdot x^2$
3	1	1	$x^3 \cdot x \cdot x$
3	2	0	$x^3 \cdot x^2 \cdot 1$

Terms corresponding to each way to pick 5 balls.

Why did this work? Let's track how we got the $9x^5$ term in the above expansion. When we multiply out the polynomials, each term comes from multiplying one monomial from each factor. Thus, we see that the $9x^5$ term comes from adding

$$1 \cdot x^3 \cdot x^2 + x \cdot x^2 \cdot x^2 + x \cdot x^3 \cdot x + x^2 \cdot x \cdot x^2 + x^2 \cdot x^2 \cdot x + x^2 \cdot x^3 \cdot 1 + x^3 \cdot 1 \cdot x^2 + x^3 \cdot x \cdot x + x^3 \cdot x^2 \cdot 1.$$

Each of these terms corresponds to one of the possibilities we listed above! Thus, multiplying polynomials automatically did all the casework for us.

This idea works in general. If we can separate our problem into categories or cases, then computing generating functions can be productive. We find the generating function for each category, then multiply them together to see how to combine them.

Let's look at the above problem if the balls are distinguishable.

Example 29

There are three urns in a house. One has 3 red balls, another has 3 green balls, and the third has 2 pink balls. All balls are distinguishable. In how many ways can we grab 5 balls from the urns?

On the one hand, since colors do not matter for this problem, we know the answer should be $\binom{8}{5}$. Let's see how to get this with generating functions:

Solution. There are $\binom{3}{k}$ ways to choose k red balls. Therefore, the generating function for the red urn is

$$R(x) = \binom{3}{0} + \binom{3}{1}x + \binom{3}{2}x^2 + \binom{3}{3}x^3 = (x+1)^3.$$

Similarly, the generating function for the green urn is

$$G(x) = (1+x)^3$$

and the generating function for the pink urn is

$$P(x) = (1+x)^2.$$

We want the x^5 coefficient of $R(x)G(x)P(x) = (1+x)^8$. The Binomial Theorem tells us it is $\binom{8}{5}$. $\square$

We can phrase our combinatorial proof of the binomial theorem using generating functions. Let b_k be the number of size k subsets of an n element set. On the one hand, we know $b_k = \binom{n}{k}$, so the generating function is

$$B(x) = \binom{n}{0} + \binom{n}{1}x + \ldots + \binom{n}{n}x^n.$$

On the other hand, a subset is given by choosing whether or not to include each element. There is one way to include an element and one way to exclude it, so the generating function for each element is $1+x$. Since we have n elements,the generating function is

$$B(x) = (1+x)^n.$$

Generally, any counting problem that can be solved with generating functions can be solved without them. However, generating functions provide a shortcut which can make things easier to think about. One particular type of problem where generating functions are especially helpful are distributions. Before doing so, however, we make note of the following neat algebraic fact:

Theorem 24: Powers of Infinite Series

The coefficient of x^k in $(1+x+x^2+x^3+\ldots)^n$ is $\binom{n+k-1}{n-1}$. In other words,

$$\left(\sum_{k=0}^{\infty} x^k\right)^n = \sum_{k=0}^{\infty} \binom{n+k-1}{n-1} x^k.$$

Proof. We proceed by induction on n.

(1) **Base Case**: Observe that the coefficient of x^k in $(1+x+x^2+\ldots)^1$ is 1. Furthermore, $\binom{1+k-1}{1-1} = \binom{k}{0} = 1$, so the statement is true when $n=1$. This establishes our base case.

(2) **Inductive Hypothesis**: Suppose that

$$\left(\sum_{k=0}^{\infty} x^k\right)^n = \sum_{k=0}^{\infty} \binom{n+k-1}{n-1} x^k.$$

(3) **Inductive Step**: Observe that

$$\begin{aligned}
\left(\sum_{k=0}^{\infty} x^k\right)^{n+1} &= \left(\sum_{k=0}^{\infty} x^k\right)^n \cdot (1+x+x^2+\ldots) \\
&= \left(\sum_{k=0}^{\infty} \binom{n+k-1}{n-1} x^k\right) \cdot (1+x+x^2+\ldots) \\
&= \sum_{k=0}^{\infty} \left(\binom{n+k-1}{n-1} + \binom{n+k-2}{n-1} + \ldots + \binom{n+k-1}{n-1}\right) x^k \\
&= \sum_{k=0}^{\infty} \binom{n+k}{n} x^k,
\end{aligned}$$

where we have used the inductive hypothesis and the Hockey-stick Identity, which you proved in Pset 2. This concludes the induction.

□

Now, we are ready to tackle all kinds of distribution problems using generating functions. We start with a classic problem.

Example 30

In how many ways can we distribute 20 identical pieces of candy to 4 children, where each children can get any number (including zero) of pieces of candy?

We know from Section 15 that the answer is $\binom{23}{3}$. Let's obtain this answer with generating functions.

Solution. Each children can get any number of candy, so their generating function is given by

$$1 + x + x^2 + x^3 + \ldots$$

You may argue that each children can only get up to 20 pieces of candy, since there are not any more. However, it is okay to extend the generating function up to infinity. When we consider the x^{20} term, any terms where some child gets more than 20 pieces will not contribute anyway.
Since there are 4 children, the total generating function is

$$(1 + x + x^2 + \ldots)^4$$

and we want to extract the x^{20} coefficient. The theorem above asserts that this coefficient is

$$\binom{4 + 20 - 1}{4 - 1} = \binom{23}{3},$$

as expected. □

The power series $1 + x + x^2 + \ldots$ is interesting because it is also a geometric series. From the geometric series formula, we can rewrite and say that

$$1 + x + x^2 + \ldots = \frac{1}{1 - x}.$$

This is justified by the fact that

$$(1 - x)(1 + x + x^2 + \ldots) = 1.$$

So, in some sense, the generating function for giving candy to one child is the function

$$\frac{1}{1 - x}.$$

Even though we no longer have a power series, geometric series give us a way to think of the above function as a power series, so it still represents a generating function. Changing between both representations will prove to be useful algebraically.

Generating functions help simplify casework when our conditions are more complicated.

Example 31

We have 50 identical pieces of candy we want to distribute among 5 kids. Two kids want at most one piece of candy, a third wants any number of candy, a fourth wants an odd number of candy, and the last wants an even number of candy. In how many ways can we distribute the candy?

Solution. This is certainly harder to count with our previous techniques! We use generating functions. Since the first two kids want at most one piece of candy, their generating functions are

$$1 + x$$

The generating function for the third kid is

$$1 + x + x^2 + \ldots = \frac{1}{1-x}.$$

The fifth kid wants only even numbers, giving a generating function

$$1 + x^2 + x^4 + \ldots$$

Observe this is a geometric series as well! Thus, it equals

$$\frac{1}{1-x^2}.$$

The fourth kid wants only odd numbers, so their generating function is

$$x + x^3 + x^5 + \ldots = \frac{x}{1-x^2}.$$

Thus, the total generating function is

$$(1+x)(1+x)\left(\frac{1}{1-x}\right)\left(\frac{1}{1-x^2}\right)\left(\frac{x}{1-x^2}\right) = \frac{x(1+x)^2}{(1-x)(1-x^2)^2}.$$

Now, recall[20] that $(1-x^2) = (1-x)(1+x)$. Therefore,

$$\frac{(1+x)^2}{(1-x^2)^2} = \frac{\cancel{(1+x)^2}}{(1-x)^2\cancel{(1+x)^2}} = \frac{1}{(1-x)^2}.$$

Thus, the total generating function is

$$\frac{x}{(1-x)^3}.$$

We want to find the coefficient of x^{50}, which is the same as finding the coefficient of x^{49} in $\frac{1}{(1-x)^3}$. From our theorem, we know this is

$$\binom{3+49-1}{3-1} = \binom{51}{2}.$$

□

30.2 Closed Forms

Generating functions can also help us find the closed forms of recursive sequences. We show the technique with two examples:

Example 32

Let $(a_n)_{n=0}^{\infty}$ be the sequence such that $a_0 = 0, a_1 = -1$ and $10a_n = 3a_{n-1} + a_{n-2}$. Find a closed form for a_n.

[20] If you have never seen this, this is the moment to prove it!

Solution. We use the generating function

$$A(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 \dots$$

Now, we can do a similar trick as for geometric series. We will exploit the relationship between terms to simplify matters. In particular, we have

$$3xA(x) = 0 + 3a_0x + 3a_1x^2 + 3a_2x^3 + 3a_3x^4 \dots$$

and

$$x^2A(x) = 0 + 0 + a_0x^2 + a_1x^3 + a_2x^4 + \dots$$

Therefore,

$$\begin{aligned}
(x^2+3x)A(x) &= 0 + 3a_0x + (3a_1+a_0)x^2 + (3a_2+a_1)x^3 + (3a_3+a_2)x^4 + \dots \\
(x^2+3x)A(x) &= 3a_0x + 10a_2x^2 + 10a_3x^3 + 10a_4x^4 + \dots \\
(x^2+3x)A(x) &= 3a_0x + 10A(x) - 10a_0 - 10a_1x \\
(x^2+3x-10)A(x) &= (3a_0 - 10a_1)x + 10a_0 \\
(x^2+3x-10)A(x) &= 10x \\
A(x) &= \frac{10x}{x^2+3x-10}.
\end{aligned}$$

We have a more explicit form for the generating function! With this, we are almost done. However, we do not know how to deal with quadratic polynomials in the denominator. We do, however, know what to do if the denominator is linear. Thus, we look to do a partial fraction decomposition. Observe that $x^2+3x-10 = (x-2)(x+5)$. Therefore, we search for constants A and B such that

$$\begin{aligned}
\frac{10x}{(x-2)(x+5)} &= \frac{A}{x-2} + \frac{B}{x+5} \\
10x &= A(x+5) + B(x-2).
\end{aligned}$$

Plugging in $x = 2$, we see $A = 20/7$ and plugging in $x = -5$ we get $B = 50/7$. Thus,

$$A(x) = \frac{20/7}{x-2} + \frac{50/7}{x+5}.$$

We want to interpret the linear polynomial in the denominator as a geometric series. For example,

$$\frac{1}{x-2} = -\frac{1}{2}\left(\frac{1}{1-x/2}\right) = -\frac{1}{2}\left(1 + \frac{x}{2} + \frac{x^2}{4} + \dots\right),$$

so that the coefficient of x^k in $\frac{1}{x-2}$ is $-\frac{1}{2^{k+1}}$. Similarly,

$$\frac{1}{x+5} = \frac{1}{5}(1 + x/5) = \frac{1}{5}\left(1 - \frac{x}{5} + \frac{x^2}{25} - \dots\right),$$

so that the coefficient of x^k in $\frac{1}{x+5}$ is $\frac{(-1)^k}{5^{k+1}}$. Thus,

$$A(x) = \sum_{k=0}^{\infty}\left(\frac{(-1)^k 50}{7 \cdot 5^{k+1}} - \frac{20}{7 \cdot 2^{k+1}}\right)x^k.$$

Since $A(x)$ is the generating function, we deduce that

$$a_n = \frac{10}{7}\left(\frac{(-1)^n}{5^n} - \frac{1}{2^n}\right).$$

□

As an exercise, try to prove this using the techniques we developed in Section 29.2.

We finish with a generating function proof of the Binet Formula.

Theorem 23: The Binet Formula

Let

$$\varphi = \frac{1+\sqrt{5}}{2}, \phi = \frac{1-\sqrt{5}}{2}.$$

Then, the closed form of the Fibonacci numbers is

$$F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - \phi^n\right).$$

Proof. Let $F(x)$ be the generating function of the Fibonacci numbers. Then, observe that

$$(1-x-x^2)F(x) = x + \sum_{k=2}^{\infty}(F_k - F_{k-1} - F_{k-2})x^k = x,$$

so

$$F(x) = \frac{x}{1-x-x^2}.$$

Now, observe[21] that $1-x-x^2 = (\varphi^{-1}-x)(x-\phi^{-1})$. Then, we need A, B such that

$$\begin{aligned}\frac{x}{(\varphi^{-1}-x)(x-\phi^{-1})} &= \frac{A}{\varphi^{-1}-x} + \frac{B}{x-\phi^{-1}} \\ x &= A(x-\phi^{-1}) + B(\varphi^{-1}-x).\end{aligned}$$

Plugging in $x = \varphi^{-1}$, we get $A = \varphi^{-1}/\sqrt{5}$ and plugging in $x = \phi^{-1}$, we get $B = \phi^{-1}/\sqrt{5}$. Thus,

$$F(x) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\varphi x} - \frac{1}{1-\phi x}\right).$$

Expanding out the geometric series, we see

$$F(x) = \frac{1}{\sqrt{5}}\left(\sum_{k=0}^{\infty}(\varphi^k - \phi^k)x^k\right)$$

from which we read off that

$$F_n = \frac{1}{\sqrt{5}}(\varphi^n - \phi^n).$$

□

[21] The easiest way to see this is the quadratic formula and the fact that $\varphi^{-1} = \varphi - 1$