Example 44. The set $\mathbb{Z}$ is countable. Consider the injection $f : \mathbb{Z} \to \mathbb{N}$:

$$f(x) = \begin{cases} 2^x & : x \geq 0 \\ 3^{|x|} & : x < 0 \end{cases} \tag{5}$$

Example 45. The set $\mathbb{Q}$ is countable. Consider the injection $g : \mathbb{Q} \to \mathbb{N}$:

$$g(p/q) = \begin{cases} 2^p 3^q & : p/q > 0 \\ 0 & : p/q = 0 \\ 5^{|p|} 7^{|q|} & : p/q < 0 \end{cases} \tag{6}$$

Remark: These functions are injections as prime factorization is unique, which we have from the Fundamental Theorem of Arithmetic.

An uncountable set will now be introduced.

Theorem 1.15. *The set $2^{\mathbb{N}}$ is uncountable.*

Proof. Suppose to the contrary that $2^{\mathbb{N}}$ is countable. Let $h : \mathbb{N} \to 2^{\mathbb{N}}$ be a bijection. As h is a bijection, every element of $2^{\mathbb{N}}$ is mapped. We achieve a contradiction by constructing an element not mapped by h. Define $S \in 2^{\mathbb{N}}$ by $i \in S$ if and only if $i \notin h(i)$. If $i \in h(i)$, then $i \notin S$, so $h(i) \neq S$. By similar argument, if $i \notin h(i)$, then $i \in S$, so $h(i) \neq i$. Therefore, S is not mapped by any element of $\mathbb{N}$. As our choice of h was arbitrary, no such bijection can exist. Therefore, $2^{\mathbb{N}}$ is uncountable. □

Remark: Observe that Russell's Paradox came up in the proof that $2^{\mathbb{N}}$ is uncountable. We can also use this construction to show that $\mathbb{R}$ is uncountable. More precisely, we show that $[0, 1]$ is uncountable. First, we write each $S \in 2^{\mathbb{N}}$ as an binary string $\omega_0\omega_1 \ldots$ where $\omega_i = 1$ iff $i \in S$. Recall this is a bijection. So we map each infinite binary string to $0.\omega_0\omega_1 \ldots \in [0, 1]$.

2 Automata Theory

Theoretical computer science is divided into three key areas: automata theory, computability theory, and complexity theory. The goal is to ascertain the power and limits of computation. In order to study these aspects, it is necessary to define precisely what constitutes a model of computation as well as what constitutes a computational problem. This is the purpose of automata theory. The computational models are automata, while the computational problems are formulated as formal languages. A common theme in theoretical computer science is the relation between computational models and the problems they solve. The Church-Turing thesis conjectures that no model of computation that is physically realizable is more powerful than the Turing Machine. In other words, the Church-Turing thesis conjectures that any problem that can be solved via computational means, can be solved by a Turing Machine. To this day, the Church-Turing thesis remains an open conjecture. For this reason, the notion of an algorithm is equated with a Turing Machine. In this section, the simplest class of automaton will be introduced- the finite state automaton, as well as the interplay with regular languages which are the computational problems finite state automata solve.

2.1 Regular Languages

In order to talk about regular languages, it is necessary to formally define a language.

Definition 48 (Alphabet)**.** An alphabet Σ is a finite set of symbols.

Example 46. Common alphabets include the binary alphabet $\{0, 1\}$, the English alphabet $\{A, B, \ldots, Z, a, b, \ldots, z\}$, and a standard deck of playing cards.

Definition 49 (Kleene Closure)**.** Let Σ be an alphabet. The Kleene closure of Σ, denoted Σ^*, is the set of all finite strings whose characters all belong to Σ. Formally, $\Sigma^* = \bigcup_{n \in \mathbb{N}} \Sigma^n$. The set $\Sigma^0 = \{\epsilon\}$, where ϵ is the empty string.

Definition 50 (Language)**.** Let Σ be an alphabet. A language $L \subset \Sigma^*$.

We now delve into regular languages, starting with a definition. This definition for regular languages is rather difficult to work with and offers little intuition or insights into computation. Kleenes Theorem (which will be discussed later) provides an alternative definition for regular languages which is much more intuitive and useful for studying computation. However, the definition of a regular language provides some nice syntax for regular expressions, which are useful in pattern matching.

Definition 51 (Regular Language)**.** Let Σ be an alphabet. The following are precisely the regular languages over Σ:

- The empty language $\emptyset$ is regular.
- For each $a \in \Sigma$, $\{a\}$ is regular.
- Let L_1, L_2 be regular languages over Σ. Then $L_1 \cup L_2, L_1 \cdot L_2$, and L_1^* are all regular.

Remark: The operation $\cdot$ is string concatenation. Formally, $L_1 \cdot L_2 = \{xy : x \in L_1, y \in L_2\}$.

A regular expression is a concise algebraic description of a corresponding regular language. The algebraic formulation also provides a powerful set of tools which will be leveraged throughout the course to prove languages are regular, derive properties of regular languages, and show certain collections of regular languages are decidable. The syntax for regular expressions will now be introduced.

Definition 52 (Regular Expression)**.** Let Σ be an alphabet. A regular expression is defined as follows:

- $\emptyset$ is a regular expression, and $L(\emptyset) = \emptyset$.
- ϵ is a regular expression, with $L(\epsilon) = \{\epsilon\}$.
- For each $a \in \Sigma$, $L(a) = \{a\}$.
- Let R_1, R_2 be regular expressions. Then:
  - $R_1 + R_2$ is a regular expression, with $L(R_1 + R_2) = L(R_1) \cup L(R_2)$.
  - $R_1 R_2$ is a regular expression, with $L(R_1 R_2) = L(R_1) \cdot L(R_2)$.
  - R_1^* is a regular expression, with $L(R_1^*) = (L(R_1))^*$.

Like the definition of regular languages, the definition of regular expressions is bulky and difficult to use. We provide a couple examples of regular expressions to develop some intuition.

Example 47. Let L_1 be the set of strings over $\Sigma = \{0, 1\}$ beginning with 01. We construct the regular expression $01\Sigma^* = 01(0 + 1)^*$.

Example 48. Let L_2 be the set of strings over $\Sigma = \{0, 1\}$ beginning with 0 and alternating between 0 and 1. We have two cases: a string ends with 0 or it ends with 1. Suppose the string ends with 0. Then we have the regular expression $0(10)^*$. If the string ends with 1, we have the regular expression $0(10)^*1$. These two cases are disjoint, so we add them: $0(10)^* + 0(10)^*1$.

Remark: Observe in Example 38 that we are applying the Rule of Sum. Rather than counting desired objects, we are listing them explicitly. Regular Expressions behave quite similarly to the ring of integers, with several important differences, which we will discuss shortly.

In-Class Exercise 1: Let L_1 be the language over $\Sigma = \{a, b\}$ where the number of a's is divisible by 3. **Answer:** $b^*(b^*ab^*ab^*ab^*)^*$.

In-Class Exercise 2: Let L_2 be the language over $\Sigma = \{0, 1\}$ where each string in L_2 contains both 00 and 11 as substrings. **Answer:** $(0 + 1)^*00(0 + 1)^*11(0 + 1)^* + (0 + 1)^*11(0 + 1)^*00(0 + 1)^*$.

2.2 Finite State Automata

The finite state automaton (or FSM) is the first model of computation we shall examine. We then introduce the notion of language acceptance, culminating with Kleene's Theorem which relates regular languages to finite state automata.

We begin with the definition of a deterministic finite state automaton. There are also non-deterministic finite state automata, both with and without ϵ transitions. These two models will be introduced later. They are also equivalent to the standard deterministic finite state automaton.

Definition 53 (Finite State Automaton (Deterministic))**.** A *Deterministic Finite State Automaton* or *DFA* is a five-tuple $(Q, \Sigma, \delta, q_0, F)$ where Q is the finite set of states, Σ is the alphabet, $\delta : Q \times \Sigma \to Q$ is the state transition function, q_0 is the initial state, and $F \subset Q$ is the set of accepting states.

A We now select a string $\omega \in \Sigma^*$ as the input string for the FSM. From the initial state, we transfer to another state in Q based on the first character in ω. The second character in ω is examined and another state transition is executed based on this second character and the current state. We repeat this for each character in the string. The state transitions are dictated by the state transition function δ associated with the machine. A string ω is said to be accepted by the finite state automaton if, when started on $q_0 with \omega$ as the input, the finite state automaton terminates on a state in F. The language of a finite state automaton M is defined as follows:

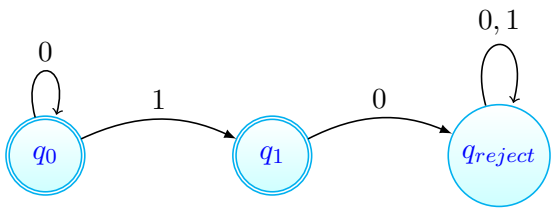
Definition 54 (Language of FSM)**.** Let M be a FSM. The language of M is the set of strings it accepts.

Let us consider an example of a DFA to develop some intuition.

Example 49. Let $\Sigma = \{0, 1\}$, and let $Q = \{q_0, q_1, q_{reject}\}$. We define $\delta(q_0, 0) = q_0, \delta(q_0, 1) = q_1, \delta(q_1, 1) = 1$, and $\delta(q_1, 0) = q_{reject}$. Finally, we have $\delta(q_{reject}, 0) = \delta(q_{reject}, 1) = q_{reject}$. We have the accepting set of states $F = \{q_0, q_1\}$. Observe that this finite state automata accepts the language 0^*1^*. We start at state q_0. For each 0 read in, we simply stay at state q_0. Then when we finish reading in 0s, we transition to q_1 if any 1s follow the sequence of 0s. At q_1, we simply eat away at the 1s. If a 0 is read after any 1s have been recognized, then we transition to a *trap* state or a *reject* state.

We represent FSMs pictorally using labeled directed graphs $G(V, E, L)$ where each vertex of V corresponds to the set of states Q. There is a directed edge $(q_i, q_j) \in E(G)$ if and only if there exists a transition $\delta(q_i, a) = q_j$ for some $a \in \Sigma \cup \{\epsilon\}$. The label function $L : E(G) \to 2^{\Sigma \cup \{\epsilon\}}$ maps $(q_i, q_j) \mapsto \{a \in \Sigma \cup \{\epsilon\} : \delta(q_i, a) = q_j\}$.

The FSM diagram for Example 39 is shown below:



Recall from the introduction that we are moving towards the notion of an algorithm. This is actually a good starting place. Observe that a finite state automaton has no memory beyond the current state. It also has no capabilities to write to memory. Conditional statements and loops can all be reduced to state transitions, so this is a good place to start.

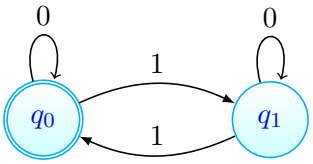
Consider the following algorithm to recognize binary strings with an even number of bits.

```
function evenParity(string ω):
    parity := 0
    for i := 0 to len(ω):
```

```
        parity := (party + ω_i) (mod 2)
    return parity == 0
```

So this algorithm accepts a binary string as input and examines each character. If it is a 1, then parity moves from $0 \to 1$ if it is 0, or from $1 \to 0$ if its current value is 1. So if there are an even number of 1s in ω, then parity will be 0. Otherwise, parity will be 1.

The following diagram models the algorithm as a finite state automaton. Here, we have $Q = \{q_0, q_1\}$ as our set of states with q_0 as the initial state. Observe in the algorithm above that parity only changes value when a 1 is processed. This is expressed in the finite state automata below, with the directed edges indicating that $\delta(q_i, \epsilon) = \delta(q_i, 0) = q_i, \delta(q_0, 1) = q_1$, and $\delta(q_1, 1) = q_0$. A string is accepted if and only if it has parity = 0, so $F = \{q_0\}$.



From this finite state automaton and algorithm above, it is relatively easy to guess that the corresponding regular expression is $(0^*10^*1)^*$. Consider 0^*10^*1. Recall that 0^* can have zero or more 0 characters. As we are starting on q_0 and $\delta(q_0, 0) = q_0, 0^*$ will leave the finite state automaton on state q_0. So then the 1 transitions the finite state automaton to state q_1. By similar analysis, the second 0^* term keeps the finite state automaton at state q_1, with the second 1 term sending the finite state automaton back to state q_0. The Kleene closure of 0^*10^*1 captures all such strings that will cause the finite state automaton to halt at the accepting state q_0.

In this case, the method of judicious guessing worked nicely. For more complicated finite state automata, there are algorithms to produce the corresponding regular expressions. We will explore one in particular, the Brzozowski Algebraic Method, later in this course. The standard algorithm in the course text is the State Reduction Method.

In-Class Exercise 3: Let L_1 be the language over $\Sigma = \{a, b\}$ where the number of a's is divisible by 3. Provide a FSM for L_1.

In-Class Exercise 4: Let L_2 be the language over $\Sigma = \{0, 1\}$ where each string in L_2 contains both the substrings 00 and 11.

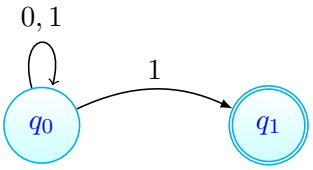
We briefly introduce NFAs and ϵ-NFAs prior to discussing Kleene's Theorem.

Definition 55 (Non-Deterministic Finite State Automata)**.** A *Non-Deterministic Finite State Automaton* or *NFA* is a five-tuple $(Q, \Sigma, \delta, q_0, F)$ where Q is the set of states, Σ is the alphabet, $\delta : Q \times \Sigma \to 2^Q$ is the transition function, q_0 is the initial state, and $F \subset Q$ is the set of accept states.

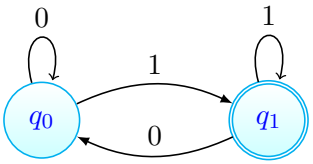
Remark: An ϵ-NFA is an NFA where the transition function is instead defined as $\delta : Q \times (\Sigma \cup \{\epsilon\}) \to 2^Q$ is the transition function. An NFA is said to accept a string ω if there exists a sequence of transitions terminating in accepting state. There may be multiple accepting sequences of transitions, as well as non-accepting transitions for NFAs. Observe as well that the other difference between the non-deterministic and deterministic finite state automata is that the non-deterministic variants transition function returns a subset of Q, while the deterministic variants transition function returns a single state. So we trivially have that a DFA is an NFA (ignoring the non-determinism). Similarly, an NFA is also an ϵ-NFA.

It is often easier to design efficient NFAs than DFAs. Consider an example below.

Example 50. Let L be the language given by $(0 + 1)^*1$. An NFA is given below. Observe that we only care about the last character being a 1. As $\delta(q_0, 1) = \{q_0, q_1\}$, the FSM is non-deterministic.



An equivalent DFA requires more thought in the design. We change state immediately upon reading a 1, then additional effort is required to ensure 1 is the last character of any valid string. At q_1, we transition to q_0 upon reading a 0, as that does not guarantee 1 is the last character of the string. If at q_1, we remain there upon reading in additional 1's.



We introduce one final definition before Kleene's Theorem.

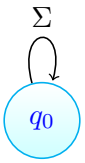
Definition 56 (Complete Computation)**.** Let M be a FSM and let $\omega \in \Sigma^*$. A *Complete Computation* of M on ω is a sequence $(s_i)_{i=1}^{|\omega|}$ where each $s_i \in Q$, each $\omega_i \in \Sigma \cup \{\epsilon\}$, $s_0 = q_0$, and $s_{i+1} \in \delta(s_i, \omega_i)$. The complete computation is *accepting* iff $s_m \in F$; otherwise, it is rejecting. M is said to accept ω if there exists a complete computation of M on ω that is accepting.

We now conclude this section with Kleene's Theorem, for which we provide a proof sketch.

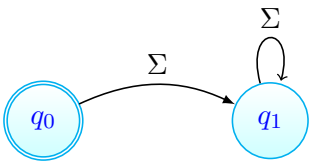
Theorem 2.1 (Kleene)**.** *A language L is regular if and only if it is accepted by some DFA.*

Proof Sketch. We first show that any regular language L is accepted by a DFA. The proof is by induction on $|L|$. When $L = 0$, a DFA with no accept states accepts L. Now suppose $|L| = 1$. There are two cases to consider: $L = \{\epsilon\}$ and $L = \{a\}$ for some $a \in \Sigma$. Suppose first $L = \{\epsilon\}$. We define a two-state DFA M_ϵ where $F = \{q_0\}$, and we transition from q_0 to q_1 upon reading in any character from Σ; after which, we remain at q_1.

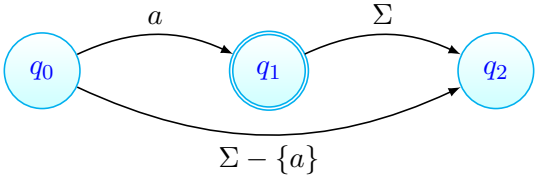
Now suppose $L = \{a\}$. We define a three-state DFA as follows with $F = \{q_1\}$. We have $\delta(q_0, a) = q_1$ and $\delta(q_1, x) = q_2$ for any $x \in \Sigma$. Now for any $y \in \Sigma - \{a\}$, we have $\delta(q_0, y) = q_2$.



A DFA to accept $L = \emptyset$.



A DFA to accept $L = \{\epsilon\}$.



A DFA to accept $L = \{a\}$, for some $a \in \Sigma$.

Now fix $n \in \mathbb{N}$ and suppose that for any regular language L with cardinality at most n, that L is accepted by some DFA. Let L_1, L_2 be regular languages with cardinalities at most n. We show that $L_1 \cup L_2, L_1L_2$, and L_1^* are all accepted by some DFA.

Lemma 2.1. *Let L_1, L_2 be regular languages accepted by DFAs $M_1 = (Q_1, \Sigma, \delta_1, q_{01}, F_1)$ and $M_2 = (Q_2, \Sigma, \delta_2, q_{02}, F_2)$ respectively. Then $L_1 \cup L_2$ is accepted by some DFA.*

Proof. We construct a DFA to accept $L_1 \cup L_2$. Let M be such a DFA, with $Q(M) = Q_1 \times Q_2$, $\Sigma(M) = \Sigma$, $\delta_M = \delta_1 \times \delta_2$, $q_0(M) = (q_{01}, q_{02})$, and $F(M) = (F_1 \times Q_2) \cup (Q_1 \times F_2)$. It suffices to show that $L(M) = L_1 \cup L_2$.

Let $\omega \in L(M)$. Then there is a complete accepting computation $\hat{\delta_M}(\omega) \in Q(M)$. Let $(q_{a_{|\omega|}}, q_{b_{|\omega|}})$ be the final state in $\hat{\delta_M}(\omega)$. If $q_{a_{|\omega|}} \in F_1$, then the projection of $\hat{\delta_M}$ into the first component is an accepting computation of M_1, so $\omega \in L_1$. Otherwise, $q_{b_{|\omega|}} \in F_2$ and the projection of $\hat{\delta_M}$ into the second component is an accepting computation of M_2. So $\omega \in L_2$.

Let $\omega \in L_1 \cup L_2$. Let $\hat{\delta_{M_1}}(\omega)$ and $\hat{\delta_{M_2}}(\omega)$ be complete computations of M_1 and M_2 respectively. One of these computations must be accepting, so $\hat{\delta_{M_1}} \times \hat{\delta_{M_2}}$ is an accepting complete computation of M. Thus, $\omega \in L(M)$. So $L(M) = L_1 \cup L_2$. □

Lemma 2.2. *Let L_1, L_2 be regular languages accepted by DFAs $M_1 = (Q_1, \Sigma, \delta_1, q_{01}, F_1)$ and $M_2 = (Q_2, \Sigma, \delta_2, q_{02}, F_2)$ respectively. Then L_1L_2 is accepted by some NFA.*

Proof. We construct an ϵ-NFA M to accept L_1L_2 as follows. Let $Q_M = Q_1 \cup Q_2$, $\Sigma_M = \Sigma$, $q_{0M} = q_{01}$, and $F_M = F_2$. We now construct $\delta_M = \delta_1 \cup \delta_2 \cup \{((q_i, \epsilon), q_{02}) : q_i \in F_1\}$. That is, we add an ϵ transition from each state of F_1 to the initial state of M_2. It suffices to show that $L(M) = L_1L_2$.

Let $\omega \in L(M)$. Then there exists an accepting complete computation $\hat{\delta_M}(\omega)$. By construction of M, $\hat{\delta_M}(\omega)$ contains some state $q_i \in F_1$ followed by q_{02}. So the string $\omega_1 \dots \omega_{i-1} \in L_1$ and $\omega_{i+1} \dots \omega_{|\omega|} \in L_2$. Conversely, let $x \in L_1, y \in L_2$, and let $\hat{\delta_{M_1}}(x)$ and $\hat{\delta_{M_2}}(y)$ be accepting complete computations of M_1 on x and M_2 on y respectively. Then $\hat{\delta_{M_1}}\hat{\delta_{M_2}}$ is a complete accepting computation of M_2, as $q_{|x|} \in \hat{\delta_{M_1}}$ has an ϵ-transition to q_{02} under δ_M. So $xy \in L(M)$. Thus, $L(M) = L_1L_2$. □

Lemma 2.3. *Let L be a regular language accepted by a FSM $M = (Q, \Sigma, \delta, q_0, F)$. Then L^* is accepted by some FSM.*

Proof. We construct an ϵ-NFA M^* to accept L^*. We modify M as follows to obtain M^*. Set $F_{M^*} = F_M \cup \{q_0\}$, and set $\delta_{M^*} = \delta_M \cup \{((q_i, \epsilon), q_0) : q_i \in F_M\}$. It suffices to show $L(M^*) = L^*$. Suppose $\omega \in L(M^*)$. Let $\hat{\delta_{M^*}}(\omega)$ be an accepting complete computation. Let $(a_i)_{i=1}^k$ be the indices in which q_0 is visited from an accepting state. Then for each $i \in [k-1]$, $\omega_{a_i} \dots \omega_{a_{i+1}-1} \in L$. So $\omega \in L^*$.

Conversely, suppose $\omega = \omega_1\omega_2\omega_3 \dots \omega_k \in L^*$. For each $i \in [k]$, let $\hat{\delta_M}(\omega_i)$ be an accepting complete computation. As there is an ϵ transition from each state in F to q_0 in M^*, the concatenation $\prod_{i=1}^k \hat{\delta_M}(\omega_i)$ is an accepting complete computation of M^*. So $\omega \in L(M^*)$. □

To complete the forward direction of the proof, it is necessary to show that ϵ-NFAs, NFAs, and DFAs are equally powerful. This will be shown in a subsequent section. In order to prove the converse, it suffices to exhibit an algorithm to convert a DFA to a regular expression, then argue the correctness of the algorithm. We present the Brzozowski Algebraic Method in a subsequent section. □

2.3 Algebraic Structure of Regular Languages

Understanding the algebraic structure of regular languages provides deep insights; which from a practical perspective, allow for the design of simpler regular expressions and finite state automata. Leveraging these machines also provides elegant and useful results in deciding certain collections of regular languages, which will be discussed in greater depth when we hit computability theory. Intuitively, the set of regular languages over the alphabet Σ has a very similar algebraic structure to the integers. This immediately translates into manipulating regular expressions, applying techniques such as factoring and distribution. We begin with the definition of a group, then continue on to other algebraic structures such as semi-groups, monoids, rings, and semi-rings. Ultimately, the algebra presented in this section will be subservient to deepening our understanding of regular languages. In a later section, the exposition of group theory will be broadened to include the basics of homomorphisms and group actions.

Definition 57 (Group)**.** A *Group* is a set of elements G with a closed binary operator $\star : G \times G \to G$ satisfying the following axioms:

1. Associativity: For every $g, h, k \in G$, $(g \star h) \star k = g \star (h \star k)$
2. Identity: There exists an element $1 \in G$ such that $1g = g1 = g$ for every $g \in G$.
3. Inverse: For every g, there exists a g^{-1} such that $gg^{-1} = g^{-1}g = 1$.

Remark: By convention, we drop the $\star$ operator and write $g \star h$ as gh, for a group is an abstraction over the operation of multiplication. When $\star$ is commutative, we write $g \star h$ as $g + h$ (explicitly using the $+$ symbol), with the identity labeled as 0. This is a convention which carries over to ring and field theory.

Example 51. The set of integers $\mathbb{Z}$ forms a group over addition. However, $\mathbb{Z}$ with the operation of multiplication fails to form a group.

Example 52. The real numbers $\mathbb{R}$ form a group over addition, and $\mathbb{R} - \{0\}$ forms a group over multiplication.

Example 53. The integers modulo $n > 1$, $\mathbb{Z}/n\mathbb{Z}$, forms a group over addition, and $\mathbb{Z}/n\mathbb{Z} - \{\overline{0}\}$ forms a group over multiplication precisely when n is a prime.

We defer formal proofs that these sets form groups under the given operations, until our group theory unit. The purpose of this section is purely intuitive. The next structure we introduce is a ring.

Definition 58 (Ring)**.** A ring is a three-tuple $(R, +, *)$, where $(R, +)$ forms an Abelian group, and $* : R \times R \to R$ is closed and associative. Additionally, multiplication distributes over addition: $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Remark: A ring with a commutative multiplication is known as a *commutative ring*, and a ring with a multiplicative identity 1 is known as a *ring with unity*. If $R - \{0\}$ forms an Abelian group over the operation of multiplication, then R is known as a field. Each of the above groups forms a ring over the normal operation of multiplication. However, only $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ and $\mathbb{Z}/p\mathbb{Z}$ (for p prime) are fields.

We now have some basic intuition about some common algeraic structures. Mathematicians focus heavily on groups, rings, and fields. Computer scientists tend to make greater use of monoids, semigroups, and posets (partially ordered sets). The set of regular languages over the alphabet Σ forms a semi-ring, which is a monoid over the addition operation (set union) and a semigroup over the multiplication operation (string concatenation). We formally define a monoid and semigroup, then proceed to discuss some intuitive relations between the semi-ring of regular languages and the ring of integers.

Definition 59 (Semigroup)**.** A *semigroup* is a two-tuple $(S, \odot)$ where $\odot$ is a closed, binary operator $\odot : S \times S \to S$.

Definition 60 (Monoid)**.** A *monoid* is a two-tuple $(M, \odot)$ that forms a semigroup, with identity.

Remark: A monoid with inverses is a group.

Definition 61 (Semi-Ring)**.** A *semi-ring* is a three-tuple $(R, +, *)$ is a commutative monoid over addition and a semigroup over multiplication. Furthermore, multiplication distributes over addition. That is, $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$ for all $a, b, c \in R$.

Recall the proof of the binomial theorem. We had a product $(x+y)^n$, and selected k of the factors to contribute an x term. This fixed the remaining $n-k$ terms to contribute a y, yielding the term $\binom{n}{k}x^k y^{n-k}$. Prior to rearranging and grouping common terms, the expansion yields strings of length n consisting solely of characters drawn from $\{x, y\}$. So the ith $(x+y)$ factor contributes either x or y (but not both) to character i in the string, just as with a regular expression. Each selection is independent; so by rule of product, we multiply. Since $\mathbb{Z}$ is a commutative ring, we can rearrange and group common terms. However, string concatenation is a non-commutative multiplication, so we cannot rearrange. However, the rule of sum and rule of product are clearly expressed in the regular expression algebra.

While commutativity of multiplication is one noticeable difference between the integers and regular languages, factoring and distribution remain the same. Recall the regular expression from Example 38, $0(10)^*0 + 0(10)^*1$. We can factor $0(10)^*$ to achieve an equivalent regular expression $0(10)^*(\epsilon + 1)$.

In-Class Exercise 5: Construct a regular expression over $\Sigma = \{a, b, c\}$ where the $n_b(\omega) + n_c(\omega) = 3$ (where $n_b(\omega)$ denotes the number of b's in ω), using exactly one term. **Answer:** $a^*(b+c)a^*(b+c)a^*(b+c)a^* = \left(\prod_{i=1}^{3} a^*(b+c)\right)a^*$. **Remark:** Notice how much cleaner this answer is than the full expansion.

2.4 DFAs, NFAs, and ϵ-NFAs

In this section, we show that DFAs, NFAs, and ϵ-NFAs are equally powerful. We know already that DFAs are no more powerful than NFAs, and that NFAs are no more powerful than ϵ-NFAs. The approach is to take the machine with weakly greater power and convert it to an equivalent machine of weakly less power. Note my use of weak ordering here. We begin with a procedure to convert NFAs to DFAs.

Recall that an NFA may have multiple complete computations for any given input string ω. Some, all, or none of these complete computations may be accepting. In order for the NFA to accept ω, at least one such complete computation must be accepting. The idea in converting an NFA to a DFA is to enumerate the possible computations for a given string. The power set of Q_{NFA} becomes the set of states for the DFA. In the NFA, a given state is selected non-deterministically in a transition. The DFA deterministically selects all possible states.

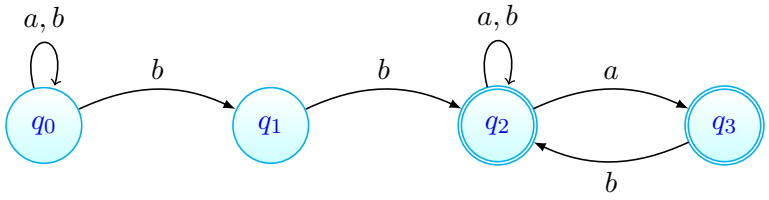
Definition 62 (NFA to DFA Algorithm)**.** Formally, we define the input and output:
INSTANCE: An NFA $N = (Q_N, \Sigma, \delta_N, q_0, F_N)$. Note that N is **not** an ϵ-NFA.
OUTPUT: A DFA $D = (Q_D, \Sigma, \delta_D, q_D, F_D\}$ such that $L(D) = L(N)$.

We construct D as follows:

- $Q_D = 2^{Q_N}$
- For each $S \in 2^{Q_N}$ and character $x \in \Sigma$, $\delta_D(S, x) = \bigcup_{s \in S} \delta_N(S, x)$
- $q_D = \{q_0\}$
- $F_D = \{S \in 2^{Q_N} : S \cap F_N \neq \emptyset\}$

Consider an example:

Example 54. We seek to convert the following NFA to a DFA.



The most methodical way to represent the DFA is by providing the transition table, noting the initial and accept states. We use the $\rightarrow$ symbol to denote the start state and the $\star$ symbol to denote accept states. The empty set is not included, because no transition leaves this state. Intuitively, the empty set is considered a trap state.

State	a	b
$\rightarrow \{q_0\}$	$\{q_0\}$	$\{q_0, q_1\}$
$\{q_0, q_1\}$	$\{q_0\}$	$\{q_0, q_1, q_2\}$
$\star\{q_0, q_2\}$	$\{q_0, q_2, q_3\}$	$\{q_0, q_1, q_2\}$
$\star\{q_0, q_3\}$	$\{q_0\}$	$\{q_0, q_1, q_2\}$
$\star\{q_1, q_2\}$	$\{q_2, q_3\}$	$\{q_2\}$
$\star\{q_1, q_3\}$	$\{q_0\}$	$\{q_0, q_1, q_2\}$
$\star\{q_2, q_3\}$	$\{q_2, q_3\}$	$\{q_2\}$
$\star\{q_0, q_1, q_2\}$	$\{q_0, q_2, q_3\}$	$\{q_0, q_1, q_2\}$
$\star\{q_0, q_1, q_3\}$	$\{q_0\}$	$\{q_0, q_1, q_2\}$
$\star\{q_0, q_2, q_3\}$	$\{q_0, q_2, q_3\}$	$\{q_0, q_1, q_2\}$
$\star\{q_1, q_2, q_3\}$	$\{q_2, q_3\}$	$\{q_2\}$
$\star\{q_0, q_1, q_2, q_3\}$	$\{q_0, q_2, q_3\}$	$\{q_0, q_1, q_2\}$

Dealing with an exponential number of states is tedious and bothersome. We can prune unreachable states after constructing the transition table, or we can only add states as they become necessary. In Example 44, only the states $\{q_0\}, \{q_0, q_1\}, \{q_0, q_1, q_2\}$, and $\{q_0, q_2, q_3\}$ are reachable from q_0. So we may restrict attention to those. A graph theory intuition regarding connected components and walks is useful here. If the graph is not connected, no path (and therefore, walk) exists between two vertices on separate components. We represent our FSMs pictorally as graphs, which allows us to easily apply the graph theory intuition.

We now prove the correctness of this algorithm.

Theorem 2.2. *Let $N = (Q_N, \Sigma, \delta_N, q_0, F_N)$ be an NFA. There exists a DFA D such that $L(N) = L(D)$.*

Proof. Let D be the DFA returned from the algorithm in Definition 50. It suffices to show that $L(N) = L(D)$. Let $\omega \in L(N)$. Then there is a complete accepting complete computation $\hat{\delta_N}(\omega) = (q_0, \ldots, q_k)$. Let $\hat{\delta_D}(\omega) = (p_0, \ldots, p_k)$ be the complete computation of D on ω. We show by induction that $q_i \in p_i$ for all $i \in \{0, \ldots, k\}$. When $i = 0$, $p_0 = \{q_0\}$, so the claim holds. Now fix h such that $0 < h < k$ and suppose that for each $i < h$, $q_i \in p_i$. We prove true for the $h + 1$ case. By construction:

$$p_{h+1} = \bigcup_{q \in p_h} \delta_N(q, \omega_{h+1}) \tag{7}$$

Since $q_i \in p_h$ and $q_{i+1} \in \delta_N(q_i, \omega_{h+1})$, we have $q_{i+1} \in \delta_D(q_i, \omega_{h+1})$. Since $\omega \in L(N)$, $q_k \in F_N$. We know that $q_k \in p_k$. By construction of D, $p_k \in F_D$. So $\omega \in L(D)$, which implies $L(N) \subset L(D)$.

Conversely, suppose $\omega \in L(D)$. Let $\hat{\delta_D}(\omega) = (p_1, \ldots, p_k)$ be an accepting complete computation of D on ω. We construct an accepting complete computation of N on ω. As $\omega \in L(D)$, $p_k \cap F_n \neq \emptyset$. Let $q_f \in p_k \cap F_n$. From (7), $q_f \in \delta_N(q, \omega_{k-1})$ for some $q \in p_{k-1}$. Let q_{k-1} be such a state. Iterating on this argument yields a sequence of states starting at q_0 and ending at q_f, which is a complete accepting computation of N on ω. So $\omega \in L(N)$, which implies $L(D) \subset L(N)$. $\square$

Example 55. In the worst case, the algorithm in Definition 50 requires an exponential number of cases. Consider an n state NFA where $\delta(q_0, 0) = \{q_0\}$, $\delta(q_0, 1) = \{q_0, q_1\}$; and for all $i \in [n-1]$, $\delta(q_i, 0) = \delta(q_i, 1) = \{q_{i+1}\}$. The only accept state is q_n.

We now discuss the procedure to convert an ϵ-NFA to an NFA without ϵ transitions. This shows that an ϵ-NFA is no more powerful than an NFA. We know already that an NFA is no more powerful than an ϵ-NFA, so our construction shows that an NFA and ϵ-NFA are equally powerful. The definition of the ϵ-closure will first be introduced.

Definition 63 (ϵ-Closure)**.** Let N be an ϵ-NFA and let $q \in Q$. The ϵ-closure of q, denoted ECLOSE(q) is defined recursively as follows. First, $q \in$ ECLOSE(q). Next, if the state $s \in$ ECLOSE(q) and there exists a state r such that $r \in \delta(s, \epsilon)$, then $r \in$ ECLOSE(q).

Intuitively, ECLOSE(q) is the set of states reachable from q using only ϵ transitions.

Definition 64 (ϵ-NFA to NFA Algorithm)**.** We begin with the instance and output statements:
INSTANCE: An ϵ-NFA $N = (Q_N, \Sigma, \delta, q_{0_N}, F)$.
OUTPUT: An NFA without ϵ transitions $M = (Q_M, \Sigma, \delta, q_{0_M}, F)$ such that $L(M) = L(N)$.

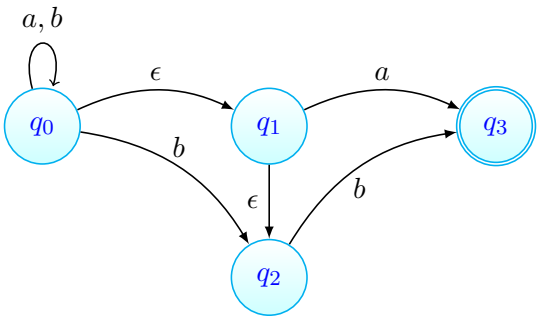
We construct M as follows:

```
if N has no ϵ transitions:
    return N

for each q ∈ Q_N:
    compute ECLOSE(q)
    for each pair s ∈ ECLOSE(q):
        if s ∈ F_N:
            F_N := F_N ∪ {q}

        for each ω ∈ Σ:
            if δ(s,ω) is defined:
                add transition δ(q,ω) := δ(s,ω)
                remove s from δ(q,ϵ)
return the modified N
```

Theorem 2.3. *The procedure in Definition 52 correctly constructs an NFA M with no ϵ transitions such that $L(M) = L(N)$.*

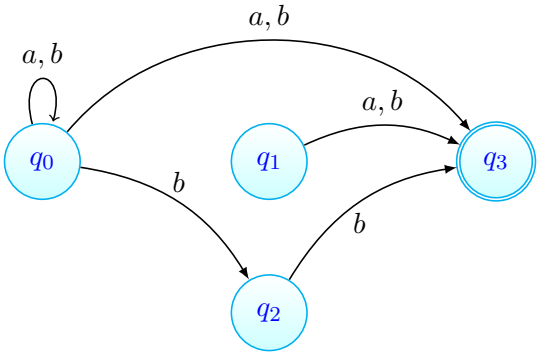
Proof. Discuss the proof strategy with students in class. Ask them why $L(N) \subset L(M)$, and why $L(M) \subset L(N)$. □

Example 56. Consider the following ϵ-NFA:



We begin by computing the ϵ-closure of each state. The only states with ϵ-transitions are q_0 and q_1, so we restrict attention to the ϵ-closures for these states. We have ECLOSE(q_1) = $\{q_1, q_2\}$ and ECLOSE(q_0) = $\{q_0\} \cup$ ECLOSE(q_1) = $\{q_0, q_1, q_2\}$. Since $\delta(q_2, b) = q_3$, we add the transitions $\delta(q_0, b) = \delta(q_1, b) = q_3$ and remove the ϵ transition $\delta(q_1, \epsilon) = q_2$.

We repeat this procedure for q_0. Since $\delta(q_1, a) = \delta(q_1, b) = q_3$. So we add the transitions $\delta(q_0, a) = \delta(q_0, b) = q_3$ and remove the transition $\delta(q_0, \epsilon) = q_1$. The final NFA is as follows:



2.5 DFAs to Regular Expressions- Brzozowski's Algebraic Method

In order to complete the proof of Kleene's Theorem, we must show that each finite state machine accepts a regular language. To do so, it suffices to provide an algorithm that converts a FSM to a corresponding regular expression. We exmaine the Brzozowski algebraic method. Intuitively, the Brzozowski Algebraic Method takes a finite state automata diagram (the directed graph) and constructs a system of linear equations to solve. Solving a subset of these equations will yield the regular expression for the finite state automata. I begin by defining some notation. Fix a FSM M. Let E_i denote the regular expression such that $L(E_i)$ contains strings ω such that when we run M on ω, it halts on q_i.

The system of equations consists of recursive definitions for each E_i, where the recursive definition consists of sums of $E_j R_{ji}$ products, where R_{ji} is a regular expression consisting of the union of single characters. That is, R_{ji} represents the selection of single transitiosn from state j to state i, or single edges (j, i) in the graph. So if $\delta(q_j, a) = \delta(q_j, b) = q_i$, then $R_{ji} = (a + b)$. In other words, E_j takes the finite state automata from state q_0 to q_j. Then R_{ji} is a regular expression describing strings that will take the finite state automata from state j to state i in exactly one step. That is, intuitively:

$$E_i = \sum_{j \in Q, \text{there exists a walk from state j to state i}} E_j R_{ji}$$

Note: Recall that addition when dealing with regular expressions is the set union operation.

Once we have the system of equations, then we solve them by backwards substitution just as in linear algebra and high school algebra.

We formalize our system of equations:

Definition 65 (Brzozowski Algebraic Method)**.** Let M be a DFA. Let $i, j \in Q$ and define $R_{ij} \subset (\Sigma \cup \{\epsilon\})$ where $R_{ij} = \{\omega : \delta(i, \omega) = j\}$. For each $i \in Q$, we define:

$$E_i = \sum_{q \in Q} E_q R_{qi} \tag{8}$$

The desired regular expression is the closed form sum of E_f, for each $f \in F$. In order to solve these equations, it is necessary to develop some machinery. More importantly, it is important to ensure this approach is sound. The immediate question to answer is whether E_q exists for each $q \in Q$? Intuitively, the answer is yes. Fix $q \in Q$. We take D, and construct a new DFA $D_q = (Q(D), \Sigma, \delta_D, q_{0_D}, F)$ where $F = \{q\}$. This is begging the question, though. We have shown that if a language is regular, then there exists a DFA that recognizes it.

The goal now is to show the converse: the language accepted by a FSM is regular. To this end, we introduce the notion of a derivative for regular expressions, which captures the suffix relation. The derivative of a regular expression returns a regular expression, so it is accepted by some FSM (which we have already proven in the forward direction of Kleene's Theorem). We view each R_{ij} as the sum of derivatives of each E_i. It then becomes necessary to show that a regular expression can be written as the sum of its derivatives. This implies the existence of a solution to the equations in Definition 53. With a high level view in mind, we proceed with the definition of a derivative.

Definition 66 (Derivative of Regular Expressions)**.** Let R be a regular expression and let $\omega \in \Sigma$. The derivative of R with respect to ω is $D_\omega R = \{t : \omega t \in L(R)\}$.

We next introduce the following function:

Definition 67. Let R be a regular expression, and define the function τ as follows:

$$\tau(R) = \begin{cases} \epsilon & : \epsilon \in L(R) \\ \emptyset & : \epsilon \notin L(R) \end{cases} \tag{9}$$

Note that $\emptyset R = R\emptyset = \emptyset$ (which a simple counting argument justifies). It is clear the following hold for τ:

- $\tau(\epsilon) = \tau(R^*) = \epsilon$
- $\tau(a) = \emptyset$ for all $a \in \Sigma$
- $\tau(\emptyset) = \emptyset$
- $\tau(P + Q) = \tau(P) + \tau(Q)$
- $\tau(PQ) = \tau(P)\tau(Q)$

Note that $\emptyset R = R\emptyset = \emptyset$, for any regular expression L. A simple counting argument for the cardinality of the concatenation of two languages justifies this.

Theorem 2.4. *Let $a \in \Sigma$ and let R be a regular expression. $D_a R$ is defined recursively as follows:*

$$D_a a = \epsilon \tag{10}$$
$$D_a b = \emptyset \text{ if } b \in (\Sigma - \{a\}) \cup \{\epsilon\} \cup \{\emptyset\} \tag{11}$$
$$D_a(P^*) = (D_a P)P^* \tag{12}$$
$$D_a(PQ) = (D_a P)Q + \tau(P)D_a Q \tag{13}$$

Proof Sketch. (10) and (11) follow immediately from Definition 54. (12) and (13) make excellent homework and test questions. Ask students for combinatorial intuition. □

The next two results allow us to show that the derivative of a regular expression is itself a regular expression. So regular languages are preserved under the derivative operator. This algebraic proof is more succinct than modifying a FSM to accept a given language.

Theorem 2.5. *Let $\omega \in \Sigma^*$ with $|\omega| = n$, and let R be a regular expression. $D_\omega R$ satisfies:*

$$D_\epsilon R = R \tag{14}$$
$$D_{\omega_1\omega_2} R = D_{\omega_2}(D_{\omega_1} R) \tag{15}$$
$$D_\omega R = D_{\omega_n}(D_{\omega_1 \ldots \omega_{n-1}} R) \tag{16}$$

Proof. This follows from the definition of the derivative and induction. We leave the details as an exercise for the reader. □

Theorem 2.6. *Let $s \in \Sigma^*$ and R be a regular expression. $D_s R$ is also a regular expression.*

Proof. The proof is by induction on $|s|$. When $|s| = 0$, $s = \epsilon$ and $D_s R = R$. If $|s| = 1$, Theorem 2.4 implies that $D_s R$ is a regular expression. Now suppose that if $|s| = k$ that $D_s R$ is a regular expression. We prove true for the $k + 1$ case. Let ω be a string of length $k + 1$. From Theorem 2.5, $D_\omega R = D_{\omega_{k+1}}(D_{\omega_1 \ldots \omega_k} R)$. By the inductive hypothesis, $(D_{\omega_1 \ldots \omega_k} R)$ is a regular expression, which we call P. We apply the inductive hypothesis to $D_{\omega_{k+1}} P$ to obtain the desired result. □

We introduce the next theorem, which is easily proven using a set-inclusion argument. This theorem does not quite imply the correctness of the system of equations for the Brzozowski Algebraic Method. However, a similar argument shows the correctness of the Brzozowski system of equations.

Theorem 2.7. *Let R be a regular expression. Then:*

$$R = \tau(R) + \sum_{a \in \Sigma} a(D_a R) \tag{17}$$

In order to solve the Brzozowski system of equations, we use the substitution approach from high school. Because the set of regular languages forms a semi-ring, we do not have inverses for set union or string concatenation. So elimination is not a viable approach here. Arden's Lemma, which is given below, provides a means to obtain closed form solutions for each equation in the system. We then substitute the closed form solution into the remaining equations and repeat the procedure.

Lemma 2.4 (Arden)**.** *Let α, β be regular expressions and R be a regular expression satisfying $R = \alpha + \beta R$. Then $R = \alpha(\beta^*)$.*

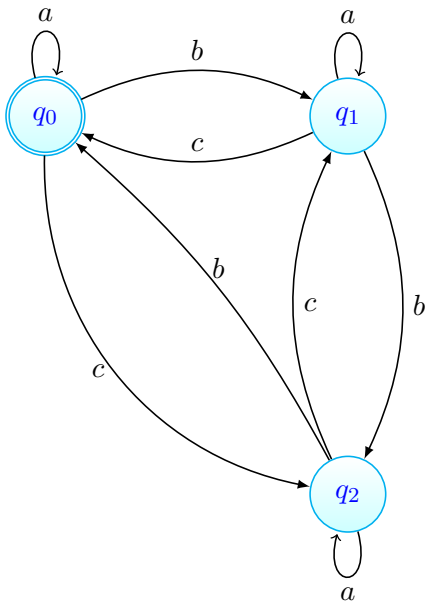
Remark: Arden's Lemma is analogous to homogenous first-order recurrence relations, which are of the form $a_0 = k$ and $a_n = ca_{n-1}$ where c, k are constants. The closed form solution for the recurrence is $a_n = kc^n$.

We now consider some examples of applying the Brzozowski Algebraic Method.

Example 57. We seek a regular expression over the alphabet $\Sigma = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ describing those integers whose value is 0 modulo 3.

In order to construct the finite state automata for this language, we take advantage of the fact that a number $n \equiv 0 \pmod 3$ if and only if the sum of n's digits are also divisible by 3. For example, we know $3|123$ because $1+2+3 = 6$, a multiple of 3. However, 125 is not divisible by 3 because $1+2+5 = 8$ is not a multiple of 3.

Now for simplicity, let's partition Σ into its equivalence classes $a = \{0, 3, 6, 9\}$ (values congruent to 0 mod 3), $b = \{1, 4, 7\}$ (values equivalent to 1 mod 3), and $c = \{2, 5, 8\}$ (values equivalent to 2 mod 3). Similarly, we let state q_0 represent a, state q_1 represent b, and state q_2 represent c. Thus, the finite state automata diagram is given below, with q_0 as the accepting halt state:



We consider the system of equations given by E_i, taking the FSM from state q_0 to q_i:

- $E_0 = \epsilon + E_0 a + E_1 c + E_2 b$

  If at q_0, transition to q_0 if we read in the empty string, or if we go from $q_0 \to q_0$ and read in a character in a; or if we go from $q_0 \to q_2$ and read in a character in c; or if we go from $q_0 \to q_2$ and read in a character from b.

- $E_1 = E_0b + E_1a + E_2c$

  To transition from $q_0 \to q_1$, we can go from $q_0 \to q_0$ and read in a character from b; go from $q_0 \to q_1$ and read in a character from a; or go from $q_0 \to q_2$ and read in a character from c.

- $E_2 = E_0c + E_1b + E_2a$

  To transition from $q_0 \to q_2$, we can go from $q_0 \to q_0$ and read a character from c; go from $q_0 \to q_0$ and read in a character from b; or go from $q_0 \to q_2$ and read in a character from a.

Since q_0 is the accepting halt state, only a closed form expression of E_0 is needed.

There are two steps which are employed. The first is to simplify a single equation, then to backwards substitute into a different equation. We repeat this process until we have the desired closed-form solution for the relevant E_i (in this case, just E_0). In order to simplify a variable, we apply Arden's Lemma, which states that $E = \alpha + E\beta = \alpha(\beta)^*$, where α, β are regular expressions.

We start by simplifying E_2 using Arden's Lemma: $E_2 = (E_0c + E_1b)a^*$.

We then substitute E_2 into E_1, giving us $E_1 = E_0b + E_1a + (E_0c + E_1b)(a)^*c = E_0(b + ca^*c) + E_1(c + ba^*c)$. By Arden's Lemma, we get $E_1 = E_0(b + ca^*c)(a + ba^*c)^*$

Substituting again, $E_0 = \epsilon + E_0a + E_0(b + ca^*c)(a + ba^*c)^*c + (E_0c + E_1b)a^*b$.

Expanding out, we get $E_0 = \epsilon + E_0a + E_0(b + ca^*c)(a + ba^*c)^*c + E_0ca^*b + E_0(b + ca^*c)(a + ba^*c)^*a^*b$.

Then factoring out: $E_0 = \epsilon + E_0(a + ca^*b + (b + ca^*c)(a + ba^*c)^*(c + ba^*b))$.

By Arden's Lemma, we have: $E_0 = (a+ca^*b+(b+ca^*c)(a+ba^*c)^*(c+ba^*b))^*$, a closed form regular expression for the integers mod 0 over Σ.

Example 58. Consider the DFA:

State	Set	a	b
Q_0	$\{q_0\}$	Q_1	Q_2
$\star Q_1$	$\{q_0, q_2\}$	Q_1	Q_2
Q_2	$\{q_1\}$	Q_0	Q_3
$\star Q_3$	$\{q_1, q_2\}$	Q_0	Q_3

The Brzozowski Equations are shown below. We leave it as an exercise for the reader to solve this system of equations.

- $E_0 = E_2a + E_3a + \epsilon$
- $E_1 = E_0a + E_1a$
- $E_2 = E_0b + E_1b$
- $E_3 = E_2b + E_3b$

2.6 Pumping Lemma for Regular Languages

So far, we have only examined languages which are regular. The Pumping Lemma for Regular Languages provides a non-deterministic test to determine if a language is not regular. We check if a language cannot be pumped. If this is the case, then it is not regular. However, there exist non-regular languages which satisfy the Pumping Lemma for Regular Languages. That is, the Pumping Lemma for Regular Languages is a necessary condition for a language to be regular. There are numerous Pumping Lemmas, including the Pumping Lemma for Context Free Languages and others in the literature for various classes of formal languages. So the Pumping Lemma for Regular Languages is a very natural result. We state it formally below.

Theorem 2.8 (Pumping Lemma for Regular Languages)**.** *Suppose L is a regular language. Then there exists a constant $p > 0$, depending only on L, such that for every string $\omega \in L$ with $|\omega| \geq p$, we can break w into three strings $w = xyz$ such that:*

- $|y| > 0$
- $|xy| \leq p$
- $xy^i z \in L$ *for all* $i \geq 0$

Proof. Let D be a DFA with p states accepting L, and let $\omega \in L$ such that $|\omega| \geq p$. We construct strings x, y, z satisfying the conclusions of the Pumping Lemma. Let $\hat{\delta}(\omega) = (q_0, \ldots, q_{|\omega|})$ be a complete accepting computation. As $|\omega| \geq p$, some state in the sequence $(q_0, \ldots, q_p)$ is repeated. Let $q_i = q_j$ with $i < j$ be repeated. Let $\omega_{i+1} \ldots \omega_j$ be the substring of ω taking the string from q_i to q_j. Let $x = \omega_1 \ldots \omega_i, y = \omega_{i+1} \ldots \omega_j$ and $z = \omega_{j+1} \ldots \omega_{|\omega|}$. So $|xy| \leq p$, $|y| > 0$ and $xy^k z \in L$ for every $k \geq 0$. □

We consider a couple examples to apply the Pumping Lemma for Regular Languages. In order to show a language is not regular, we pick one string and show that every decomposition of that string can be pumped to produce a new string not in the language. One strategy with pumping lemma proofs is to pick a sufficiently large string to minimize the number of cases to consider.

Proposition 2.1. *Let $L = \{0^n 1^n : n \in \mathbb{N}\}$. L is not regular.*

Proof. Suppose to the contrary that L is regular and let p be the pumping length. Let $\omega = 0^p 1^p$. By the Pumping Lemma for Regular Languages, there exist strings x, y, z such that $\omega = xyz$, $|xy| \leq p, |y| > 0$ and $xy^i z \in L$ for all $i \in \mathbb{N}$. Necessarily, $xy = 0^k$ for some $k \in [p]$, with y containing at least one 0. So $xy^0 z = xz$ has fewer 0's than 1's. Thus, $xz \notin L$, a contradiction. □

Proposition 2.2. *Let $L = \{0^n 1^{2n} 0^n : n \in \mathbb{N}\}$. L is not regular.*

Proof. Suppose to the contrary that L is regular and let p be the pumping length. Let $\omega = 0^p 1^{2p} 0^p$. By the Pumping Lemma for Regular Languages, let x, y, z be strings such that $\omega = xyz$, $|xy| \leq p$ and $|y| > 0$. Necessarily, xy contains only 0's and y contains at least one 0. So $xy^0 z = xz$, which contains fewer than p 0's followed by $1^{2p} 0^p$, so $xz \notin L$, a contradiction. □

We examine one final example, which is a non-regular language that satisfies the Pumping Lemma for Regular Languages.

Example 59. Let L be the following language:

$$L = \{uvwxy : u, y \in \{0,1,2,3\}^*; v, w, x \in \{0,1,2,3\} \text{ s.t}(v = w \text{ or } v = x \text{ or } x = w)\} \cup \tag{18}$$

$$\{w : w \in \{0,1,2,3\}^* \text{ and precisely } 1/7 \text{ of the characters are } 3\} \tag{19}$$

Let p be the pumping length, and let $s \in L$ be a string with $|s| \geq p$. As the alphabet has order 4, there is a duplicate character within the first five characters. The first duplicate pair is separated by at most three characters. We consider the following cases:

- If the first duplicate pair is separated by at most one character, we pump one of the first five characters not separating the duplicate pair. As $u \in \{0,1,2,3\}^*$, the resultant string is still in L.
- If the duplicate pair is separated by two or three characters, we pump two consecutive characters separating them. If we pump down, we obtain a substring with the duplicate pair separated by either zero or one characters. If we pump the separators ab up, then we have aba in the new string. In both cases, the pumped strings belong to L.

However, L is not regular, which we show in the next section.

2.7 Closure Properties

The idea of closure properties is another standard idea in automata theory. So what exactly does closure mean? Informally, it means if we take two elements in a set and do something to them, we get an element in the set. This section focuses on operations on which regular languages are closed; however, we also have closure in other mathematical operations. Consider the integers, which are closed over addition. This means that if we take two integers and add them, we get an integer back.

Similarly, if we take two real numbers and multiply them, the product is also a real number. The real numbers are not closed under the square root operation, however. Consider $\sqrt{-1} = i$, which is a complex number but not a real number. This is an important point to note- operations on which a set is closed will never give us an element outside of the set. So adding two real numbers will never give us a complex number of the form $a + bi$ where $b \neq 0$.

Now let us look at operations on which regular languages are closed. Let Σ be an alphabet and let $RE(\Sigma)$ be the set of regular languages over Σ. A binary operator is closed on the set $RE(\Sigma)$ if it is defined as: $\odot : RE(\Sigma) \times RE(\Sigma) \to RE(\Sigma)$. In other words, each of these operations takes either one or two (depending on the operation) regular languages and returns a regular language. Note that the list of operations including set union, set intersection, set complementation, concatenation, and Kleene closure is by no means an extensive or complete list of closure properties.

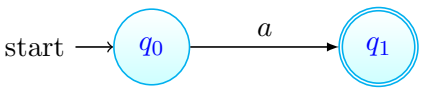
Recall from the definition of a regular language that if A and B are regular languages over the alphabet Σ, then $A \cup B$ is also regular. More formally, we can write $\cup : RE(\Sigma) \times RE(\Sigma) \to RE(\Sigma)$, which says that the set union operator takes two regular languages over a fixed alphabet Σ and returns a regular language over Σ. Similarly, string concatenation is a closed binary operator on $RE(\Sigma)$ where $A \cdot B = \{a \cdot b : a \in A, b \in B\}$. The set complementation and Kleene closure operations are closed, unary operators. Set complementation is defined as $- : RE(\Sigma) \to RE(\Sigma)$ where for a language $A \in RE(\Sigma)$, $\overline{A} = \Sigma^* \setminus A$. Similarly, the Kleene closure operator takes a regular language A and returns A^*.

Recall that the definition of a regular language provides for closure under the union, concatenation, and Kleene closure operations. The proof techniques rely on either modifying a regular expression or FSMs for the input languages. We have seen these techniques in the proof of Kleene's theorem. We begin with set complementation.

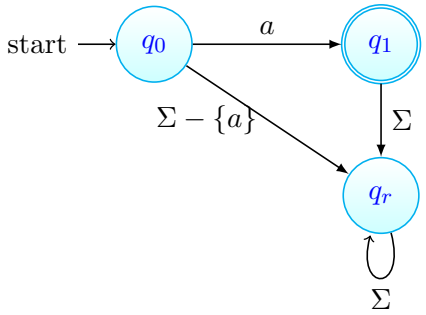
Proposition 2.3. *Let Σ be an alphabet. The set $RE(\Sigma)$ is closed under set complementation.*

Proof. Let L be a regular language, and let M be a DFA with a total transition function such that $L(M) = L$. We construct $\overline{M} = (Q_M, \Sigma, \delta_M, q_0, Q_M \setminus F_M)$. So $\omega \in \Sigma^*$ is not accepted by M if and only if ω is accepted by $\overline{M}$. So $\overline{L} = L(\overline{M})$, which implies that $\overline{L}$ is regular. □

Remark: It is important that the transition function is a total function; that is, it is fully defined. A partial transition function does not guarantee that this construction will accept $\overline{L}$. Consider the following FSM. The complement of this machine accepts precisely a.



However, if we fully define an equivalent machine (shown below), then the construction in the proof guarantees the complement machine accepts $\Sigma^* \setminus \{a\}$:



We now discuss the closure property of set intersection, for which two proofs are provided. The first proof leverages a product machine (similar to the construction of a product machine for the set union operation in the proof for Kleene's Theorem). The second proof uses existing closure properties, and so is much more succinct.

Proposition 2.4. *Let Σ be an alphabet. The set $RE(\Sigma)$ is closed under set intersection.*

Proof (Product Machine). Let L_1, L_2 be regular languages, and let M_1 and M_2 be fully defined DFAs that accept L_1 and L_2 respectively. We construct the product machine $M = (Q_1 \times Q_2, \Sigma, \delta_1 \times \delta_2, (q_{01}, q_{02}), F_1 \times F_2)$. A simple set containment argument shows that $L(M) = L_1 \cap L_2$. We leave the details as an exercise for the reader. □

Proof (Closure Properties). Let L_1, L_2 be regular languages. By DeMorgan's Law, we have $L_1 \cap L_2 = \overline{\overline{L_1} \cup \overline{L_2}}$. As regular languages are closed under union and complementation, we have that $L_1 \cap L_2$ is regular. □

We next introduce the set difference closure property for two regular languages. Like the proof for the closure under set intersection, the proof of closure under set complementation relies on existing closure properties.

Proposition 2.5. *Let L_1, L_2 be regular languages. $L_1 \setminus L_2$ is also regular.*

Proof. Recall that $L_1 \setminus L_2 = L_1 \cap \overline{L_2}$. As the set of regular languages is closed under intersection and complementation, $L_1 \setminus L_2$ is regular. □

We conclude with one final closure property before examining some examples of how to apply them.

Proposition 2.6. *Let L be a regular language, and let $L^R = \{\omega^R : \omega \in L\}$. We have L^R is regular.*

Proof. Let M be a DFA accepting L. We construct an ϵ-NFA M' to accept L^R as follows. The states of M' are $Q_M \cup \{q_0'\}$, where q_0' is the initial state of M'. We set $F' = \{q_0\}$, the initial state of M. Finally, for each transition $((q_i, s), q_j) \in \delta_M$, we add $((q_j, s), q_i) \in \delta_{M'}$. Finally, we add ϵ transitions from q_0' to each state $q_f \in F_M$. A simple set containment argument shows that $L(M') = L^R$, and we leave the details as an exercise for the reader. □

One application of closure properties is to show languages are or are not regular. To show a language fails to be regular, we operate on it with a regular language to obtain a known non-regular language. Consider the following example.

Example 60. Let $L = \{ww^R : w \in \{0,1\}^*\}$. Suppose to the contrary that L is regular. We Consider $L \cap 0^*1^*0^* = \{0^n1^{2n}0^n : n \in \mathbb{N}\}$. We know that $\{0^n1^{2n}0^n : n \in \mathbb{N}\}$ is not regular from Proposition 2.2 (recall from earlier this morning). As regular languages are closed under intersection, it follows that at least one of $0^*1^*0^*$ or L is not regular. Since $0^*1^*0^*$ is a regular expression, it follows that L is not regular.

The next example contains another non-regular language.

Example 61. Let $L = \{w :$ w contains an equal number of 0's and 1's $\}$. Consider $L \cap 0^*1^* = \{0^n1^n : n \in \mathbb{N}\}$. We know that $\{0^n1^n : n \in \mathbb{N}\}$ is not regular from Proposition 2.1. Since 0^*1^*, it follows that L is not regular.

We consider a third example.

Example 62. Let L be the language from Example 49 which satisfies the Pumping Lemma for Regular Languages.

$$L = \{uvwxy : u, y \in \{0,1,2,3\}^*; v, w, x \in \{0,1,2,3\} \text{ s.t}(v = w \text{ or } v = x \text{ or } x = w)\} \cup \tag{20}$$
$$\{w : w \in \{0,1,2,3\}^* \text{ and precisely } 1/7 \text{ of the characters are } 3\} \tag{21}$$

Consider:

$$L \cap (01(2+3))^* = \{w : w \in \{0,1,2,3\}^* \text{ and precisely } 1/7 \text{ of the characters are } 3\} \tag{22}$$

It is quite easy to apply the Pumping Lemma for Regular Languages to the language in (22), which implies that L is not regular.

We now use closure properties to show a language is regular.

Example 63. Let L be a regular language, and let $\overline{L}$ be its complement. Then $M = L \cdot \overline{L}$ is regular. As regular languages are closed under complementation, $\overline{L}$ is also regular. It follows that since regular languages are also closed under concatenation, that M is regular.

2.8 Converting from Regular Expressions to ϵ-NFA

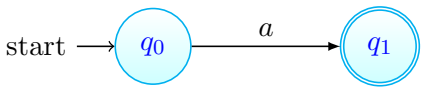
Regular expressions are important from a theoretical standpoint, in providing a concise description of regular languages. They are also of practical importance in pattern matching, with various programming languages providing regular expression libraries. These libraries construct FSMs from the regular expressions to validate input strings. One such algorithm is Thompson's Construction Algorithm. Formally:

Definition 68 (Thompson's Construction Algorithm)**.**

- **INSTANCE:** A regular expression R.
- **OUTPUT:** An ϵ-NFA N with precisely one final state such that $L(N) = L(R)$.

The algorithm is defined recursively as follows:

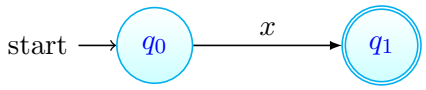
- Suppose $R = \emptyset$. Then we return a singe state FSM, which does not accept any string.
- Suppose $R = a$, where $a \in \Sigma \cup \{a\}$. We define a two-state machine as shown below:



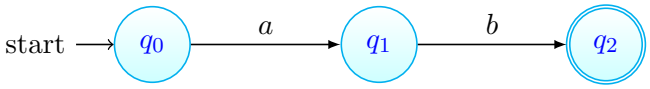
- Suppose $R = P + S$, where P and S are regular expressions. Let M_P and M_S be the ϵ-NFAs accepting P and S respectively, by applying Thompson's Construction Algorithm to P and S respectively. We define an ϵ-NFA to accept R as follows. We add an initial state q_R and the transitions $\delta(q_R, \epsilon) = \{q_P, q_S\}$, the initial states of R and S respectively. As M_R and M_S were obtained from Thompson's Construction Algorithm, they each have a single final state. We now add a new state q_{F_R} and transitions $\delta(q_{F_P}, \epsilon) = \delta(q_{F_P}, \epsilon) = \{q_{F_R}\}$, and set $F_R = \{q_{F_R}\}$.
- Suppose $R = PS$, where P and S are regular expressions. Let M_P and M_S be the ϵ-NFAs accepting P and S respectively, by applying Thompson's Construction Algorithm to P and S respectively. We construct an ϵ-NFA M_R to accept R. We begin by setting the final state of M_P is the initial state of M_S. Then $F_R = F_S$.
- Now consider R^*. Let M_R be the ϵ-NFA accepting R, by applying Thompson's Construction Algorithm to R. We construct an ϵ-NFA to accept R^* as follows: We add a new state initial state q_{R^*} and a new final state $q_{F_{R^*}}$. We then add the transitions $\delta(q_{R^*}, \epsilon) = \{q_R, q_{F_{R^*}}\}$ and $\delta(q_{F_R}, \epsilon) = \{q_R\}$.

Thompson's Construction Algorithm follows immediately from Kleene's Theorem. We actually could use the constructions given in this algorithm for the closure properties of union, concatenation, and Kleene closure in Kleene's Theorem. This is a case where a proof gives us an algorithm. As a result, we omit a formal proof of Thompson's Construction Algorithm, and we proceed with an example to illustrate the concept.

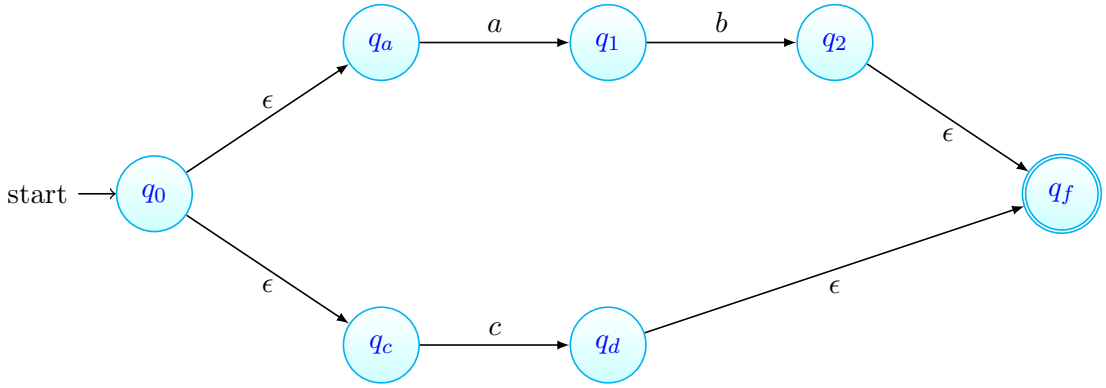
Example 64. Let $R = (ab + c)^*$ be a regular expression. We construct an ϵ-NFA recognizing R using Thompson's Construction Algorithm. Observe that our base cases are the regular expressions a, b and c. So for each $x \in \{a, b, c\}$, we construct the FSMs:



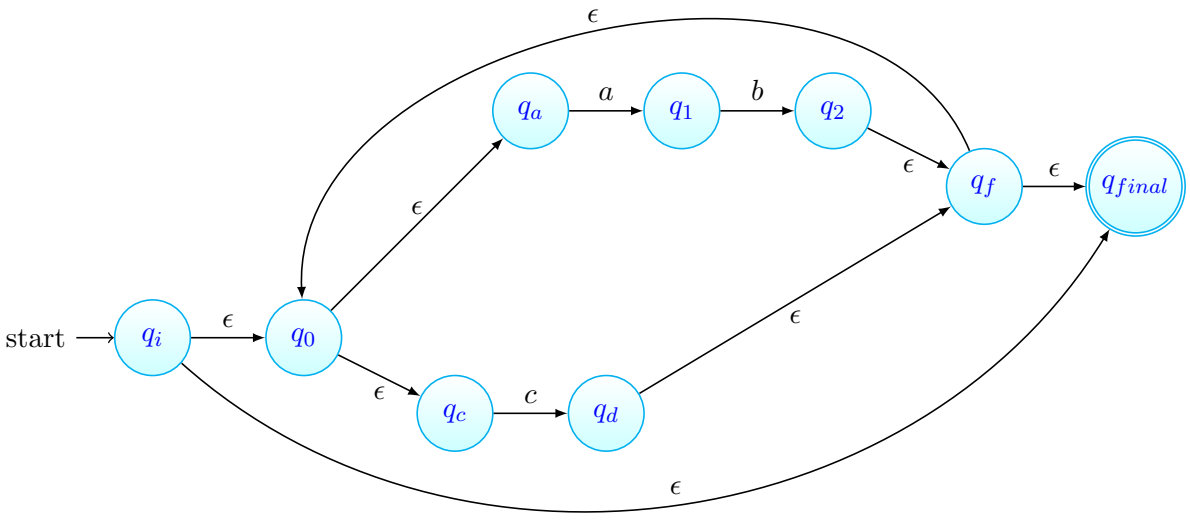
Now we apply the concatenation rule for ab to obtain:



Next, we apply the union rule for $ab + c$ to obtain:



Finally, we apply the Kleene closure step to $(ab + c)^*$ to obtain our final ϵ-NFA:



2.9 Myhill-Nerode and DFA Minimization

The Myhill-Nerode theorem is one of the most elegant and powerful results with respect to regular languages. It provides a characterization of regular languages, in addition to regular expressions and Kleene's theorem. Myhill-Nerode allows us to quickly test if a language is regular, and this test is deterministic. So we have a far more useful tool than the Pumping Lemma. Additionally, Myhill-Nerode implies an algorithm to minimize a DFA. The resultant DFA is not only *minimal*, in the sense that we cannot remove any states from it without affecting functionality; but it is also *minimum* as no DFA with fewer states that accepts the same language exists.

The intuition behind Myhill-Nerode is in the notion of distinguishing strings, with respect to a language as well as a finite state machine. We begin with the following definition.

Definition 69 (Distinguishable Strings)**.** Let L be a language over Σ. We say that two strings x, y are **distinguishable** w.r.t L if there exists a string z such that $xz \in L$ and $yz \notin L$ (or vice-versa).

Example 65. Let $L = \{0^n 1^n : n \in \mathbb{N}\}$. The strings $0, 00$ are distinguishable with respect to L. Take $z = 1$. However, 0110 and 10 are not distinguishable, because $xz \notin L$ and $yz \notin L$ for every non-empty string z.

Example 66. Let $L = (0+1)^*1(0+1)$. The strings 00 and 01 are distinguishable with respect to L, taking $z = 0$.

We obtain a straight-forward result immediately from the definition of Distinguishable Strings.

Lemma 2.5. *Let L be a regular language, and let M be a DFA such that $L(M) = L$. Let x, y be distinguishable strings with respect to L. Then $M(x)$ and $M(y)$ end on different states.*

Proof. Suppose to the contrary that $M(x)$ and $M(y)$ terminate on the same state q. Let z be a string such that (WLOG) $xz \in L$ but $yz \notin L$. As D is deterministic, $M(xz)$ and $M(yz)$ transition from q_0 to q and then from q to some state q' on input z. So xz, yz are both in L, or xz, yz are both not in L. This contradicts the assumption that x, y are distinguishable. □

Remark: The above proof fails when using NFAs rather than DFAs, as an NFA may have multiple computations for a given input string.

We now introduce the notion of a distinguishable set of strings.

Definition 70 (Distinguishable Set of Strings)**.** A set of strings $\{x_1, \ldots, x_k\}$ is distinguishable if every two distring strings x_i, x_j in the set are distinguishable.

This yields a lower bound on the number of states required to accept a regular language.

Lemma 2.6. *Suppose L is a language with a set of k distinguishable strings. Then every DFA accepting L must have at least k states.*

Proof. If L is not regular, no DFA exists and we are done. Let x_i, x_j be distinguishable strings. By Lemma 2.5, a DFA M run on x_i halts on a state q_i, while $M(x_j)$ halts on a different state q_j. So there are at least k states. □

We use Lemma 2.6 to show a language is in fact non-regular, by showing that for infinitely many $k \in \mathbb{N}$, there exists a set of k-distinguishable strings. Consider the following example.

Example 67. Recall that $L = \{0^n 1^n : n \in \mathbb{N}\}$ is not regular. Let $\in \mathbb{N}$, and consider $S_k = \{0^i : i \in [k]\}$. Each of these strings is distinguishable. For $i \in [k]$, $z = 1^i$ distinguishes 0^i from the other strings in S_k. So for every $k \in \mathbb{N}$, we need a minimum of k states for a DFA to accept L. Thus, no DFA exists to accept L, and we conclude that L is not regular.

Definition 71. Let L be a language. Define $\equiv_L \subset \Sigma^* \times \Sigma^*$. Two strings x, y are said to be **indistinguishable** w.r.t. L, which we denote $x \equiv_L y$, if for every $z \in \Sigma^*$, $xz \in L$ if and only if $yz \in L$.

Remark: $\equiv_L$ is an equivalence relation. Note as well that $\Sigma^*/\equiv_L$ denotes the set of equivalence classes of $\equiv_L$. We now prove the Myhill-Nerode theorem.

Theorem 2.9 (Myhill-Nerode)**.** *Let L be a language over Σ. If Σ^* has infinitely many equivalence classes with respect to $\equiv_L$, then L is not regular. Otherwise, L is regular and is accepted by a DFA M where $|Q_M| = |\Sigma^*/\equiv_L|$.*

Proof. If Σ^* has an infinite number of equivalence classes with respect to $\equiv_L$, then we pick a string from each equivalence class. This set of strings is distinguishable. So by Lemma 2.6, no DFA exists to accept L. This shows that if L is regular, then $\Sigma^*/\equiv_L$ is finite.

Conversely, suppose $|\Sigma^*/\equiv_L|$ is finite. We construct a DFA M where Q is the set of equivalence classes of $\equiv_L$, Σ is the alphabet, $q_0 = [\epsilon]$, and $[\omega] \in F$ iff $\omega \in L$. We define the transition function $\delta([x], a) = [xa]$ for any $a \in \Sigma$. It suffices to show that δ is well-defined (that is, it is uniquely determined for any representative of an equivalence class). For any two strings $x \equiv_L y$, $[x] = [y]$ as $\equiv_L$ is an equivalence relation. We now show that $[xa] = [ya]$. Since $x \equiv_L y$, x, y are indistinguishable. So $xaz \in L$ iff $yaz \in L$ for every string z. So $[xa] = [ya]$. So the DFA is well-defined.

Finally, we show that $L(M) = L$. Let $x = x_1 \dots x_n$ be an input string. We run M on x. The resulting computation is $([\epsilon], [x_1], \dots, [x_1 \dots x_n])$. By construction of M, $x \in L$ if and only if $[x_1 \dots x_n] \in F$. So the DFA works as desired and L is regular. □

The Myhill-Nerode Theorem provides us with a *quotient machine* to accept L, though not a procedure to compute this machine explicitly. We show this DFA is minimum and unique, then discuss a minimization algorithm. We begin by defining a second equivalence relation:

Definition 72 (Distinguishable States)**.** Let M be a DFA. Define $\equiv_M$ to be a relation on $\Sigma^* \times \Sigma^*$ such that $x \equiv_M y$ if and only if $M(x)$ and $M(y)$ halt on the same state of M.

Remark: Observe that $\equiv_M$ is a second equivalence relation.

Theorem 2.10. *The machine M constructed by the Myhill-Nerode Theorem is minimum and unique up to relabeling.*

Proof. We begin by showing that M is minimal. Let D be another DFA accepting $L(M)$. Let $q \in Q(D)$. Let:

$$S_q = \{\omega : D(w) \text{ halts on } q\} \tag{23}$$

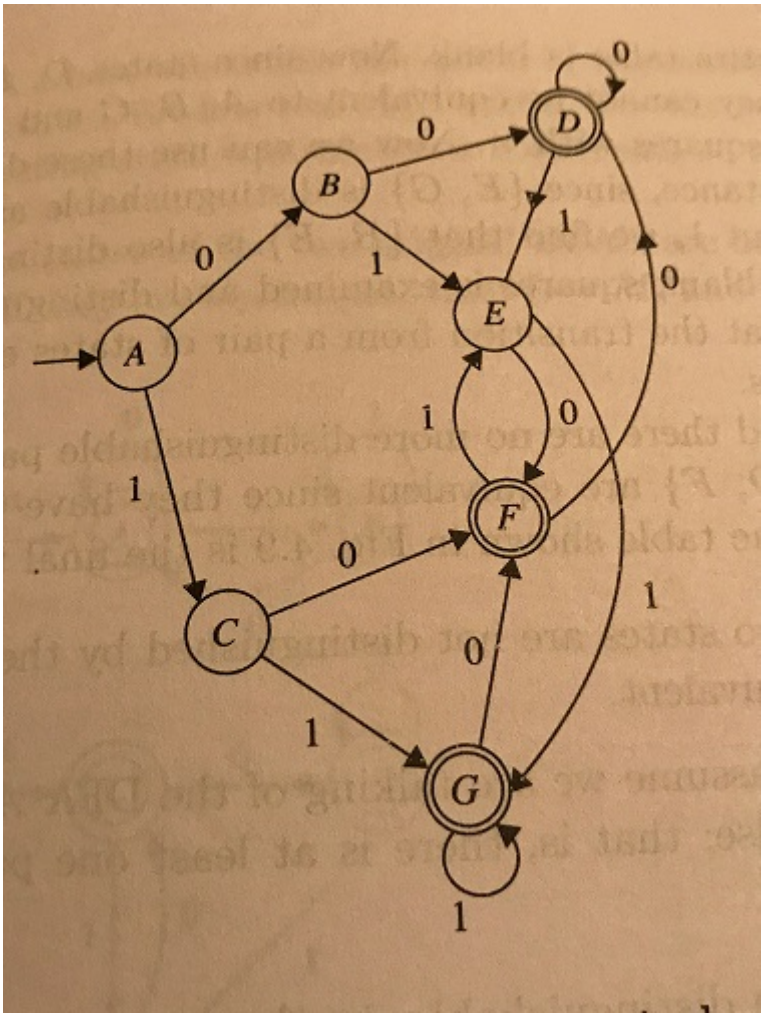
The strings in S_q are pairwise indistinguishable under $\equiv_L$. So $S_q \subset [x]$ for some $[x] \in Q(M)$. Thus, $|Q(D)| \geq |Q(M)|$.

We now show uniqueness. Suppose D has the same number of states as M but for some strings x, y, we have $x \equiv_D y$ but $x \not\equiv_M y$. Suppose M halts on state q when run on either x or y. Recall that $\equiv_M$ is the same relation as $\equiv_L$. So $[x]_M, [y]_M$ are distinct equivalence classes under $\equiv_M$. However, we have already shown that $S_q \subset [x]_M$, a contradiction. So M is the unique minimum DFA accepting L. □

Computing $\equiv_L$ outright is challenging given the fact that Σ^* is infinite. We instead deal with $\equiv_M$ for a DFA M, which partitions Σ^* as well. Consider two states q_i, q_j of a M. Recall that S_{q_i} and S_{q_j} contain the set of strings such that M halts on q_i and q_j respectively when simulated on an input from the respective set. If the strings in S_{q_i} and S_{q_j} are indistinguishable, then S_{q_i} and S_{q_j} are subsets of the same equivalence class under $\equiv_L$. Thus, we can consolidate S_{q_i} and S_{q_j} into a single state. We again run into the same problem of

determining which states of M are equivalent under $\equiv_L$. Instead, we deduce which states are not equivalent. This is done with a table-marking algorithm. We consider a $|Q| \times |Q|$ table, restricting attention to the bottom triangular half. The rows and columns correspond to states; and each cell is marked if and only if the two states are not equivalent. In each cell corresponding to a state in F and a state in $Q \setminus F$, we mark that cell. We then iterate until we mark no more states.

Example: We seek to minimize the following DFA:



We begin by noting that ϵ distinguishes the accept states and the non-accept states. So we mark the corresponding cells accordingly:

A						
	B					
		C				
X	X	X	D			
			X	E		
X	X	X		X	F	
X	X	X		X		G

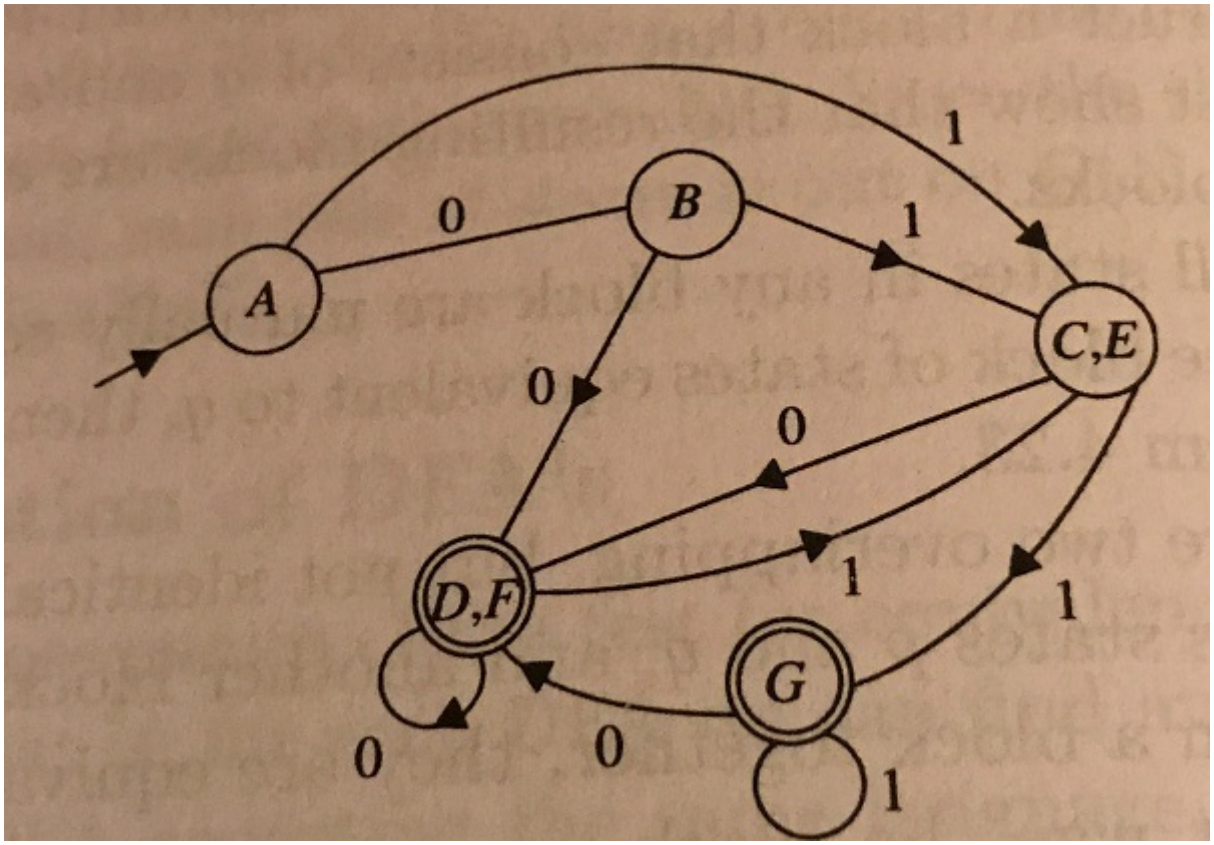
We now deduce as many distinguishable states as possible:

- B and E are distinguishable states, as $\delta(B, 1) = E$ and $\delta(E, 1) = G$. As E and G are distinguishable states, it follows that B and E are distinguished by 1.
- F and G are distinguished by 1.
- D and G are distinguished by 1.
- A and B are distinguished by 0.

- A and C are distinguished by 0.
- A and E are distinguished by 0.
- B and C are distinguished by 1.
- As $\delta(C, x) = \delta(E, x)$ for $x \in \{0, 1\}$, C and E are indistinguishable.
- As $\delta(D, x) = \delta(F, x)$ for $x \in \{0, 1\}$, D and F are indistinguishable.

A						
X	B					
X	X	C				
X	X	X	D			
X	X		X	E		
X	X	X		X	F	
X	X	X	X	X	X	G

The minimal DFA:



3 More Group Theory (Optional)

In mathematics, we have various number systems with intricate structures. The goal of Abstract Algebra is to examine the common properties and generalize them into abstract mathematical structures, such as groups, rings, fields, modules, and categories. We restrict attention to groups, which are algebraic structures with an abstract operation of multiplication. Group theory has deep applications to algebraic combinatorics and complexity theory, with the study of group actions. Informally, a group action is a dynamical process on some set, which partitions the set into equivalence classes known as orbits. We study the structures of these orbits, which provide deep combinatorial insights such as symmetries of mathematical objects like graphs. This section is intended to supplement a year long theory of computation sequence in which elementary group theory is necessary, as well as provide a stand alone introduction to algebra for the eager mathematics or theoretical computer science student.

3.1 Introductory Group Theory

3.1.1 Introduction to Groups

In this section, we define a group and introduce some basic results. Recall that a group is an algebraic structure that abstracts over the operation of multiplication. Formally, we define a group as follows.

Definition 73. A group is an ordered pair $(G, \star)$ where $\star : G \times G \to G$ satisfies the following axioms:

- **Associativity:** For every $a, b, c \in G$, $(a \star b) \star c = a \star (b \star c)$
- **Identity:** There exists an element $1 \in G$ such that $1 \star a = a \star 1 = a$ for every $a \in G$.
- **Inverses:** For every $a \in G$, there exists an $a^{-1} \in G$ such that $a \star a^{-1} = a^{-1} \star a = 1$.

Definition 74 (Abelian Group)**.** A group $(G, \star)$ is said to be Abelian if $\star$ commutes; that is, if $a \star b = b \star a$ for all $a, b \in G$.

We have several examples of groups, which should be familiar. All of these groups are Abelian. However, we will introduce several important non-Abelian groups in the subsequent sections, including the Dihedral group, the Symmetry group, and the Quaternion group. In general, assuming a group is Abelian is both dangerous and erroneous.

Example 68. The following sets form groups using the operation of addition: $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$.

Example 69. The following sets form groups using the operation of multiplication: $\mathbb{R} - \{0\}, \mathbb{Q} - \{0\}, \mathbb{C} - \{0\}$. Note that $\mathbb{Z} - \{0\}$ fails to form a group under multiplication, as it fails to satisfy the inverses axiom. There does not exist an integer x such that $2x = 1$.

Example 70. Vector spaces form groups under the operation of addition.

Let's examine the group axioms more closely. Individually, each of these axioms seem very reasonable. Let's consider associativity at a minimum. Such a structure is known as a semi-group.

Definition 75 (Semi-Group)**.** A *semi-group* is a two-tuple $(G, \star)$ where $\star : G \times G \to G$ is associative.

Example 71. Let Σ be a finite set, which we call an alphabet. Denote Σ^* as the set of all finite strings formed from letters in Σ, including the empty string ϵ. Σ^* with the operation operation of string concatenation $\odot : \Sigma^* \times \Sigma^* \to \Sigma^*$ forms a semi-group.

Example 72. $\mathbb{Z}^+$ forms a semi-group under addition. Recall that $0 \notin \mathbb{Z}^+$.

Associativity seems like a weak assumption, but it is quite important. Non-associative algebras are quite painful with which to work. Consider $\mathbb{R}^3$ with the cross-product operation. We show that this algebra does not contain an identity:

Proposition 3.1. *The algebra formed from $\mathbb{R}^3$ with the cross-product operation does not have an identity.*

Proof. Suppose to the contrary that there exists an identity $(x, y, z) \in \mathbb{R}^3$ for the cross-product operation. Let $(1, 1, 1)$ and (x, y, z) such that $(1, 1, 1) \times (x, y, z) = (1, 1, 1)$. Under the operation of the cross-product, we obtain:

$$z - y = 1 \tag{24}$$
$$z - x = 1 \tag{25}$$
$$x - y = 1 \tag{26}$$

So we obtain $z = y + 1$ and $z = x + 1$. However, $x = y + 1$ as well, so $x = z$, a contradiction. □

In Example 57, we have already seen an algebra without inverses as well. Imposing the identity axiom on top of the semi-group axioms gives us an algebraic structure known as a monoid.

Definition 76 (Monoid)**.** A *monoid* is an ordered pair $(G, \star)$ that forms a semi-group, and also satisfies the identity axiom of a group.

Example 73. Let S be a set, and let 2^S be the power set of S. The set union operation $\cup : 2^S \to 2^S$ forms a monoid.

Example 74. $\mathbb{N}$ forms a monoid under the operation of addition. Recall that $0 \in \mathbb{N}$.

Remark: Moving forward, we drop the $\star$ operator and simply write ab to denote $a \star b$. When the group is Abelian, we explicitly write $a + b$ to denote the group operation. This convention is from ring theory, in which we are dealing with two operations: addition (which forms an Abelian group) and multiplication (which forms a semi-group).

With some examples in mind, we develop some basic results about groups.

Proposition 3.2. *Let G be a group. Then:*

(A) The identity is unique.

(B) For each $a \in G$, a^{-1} is uniquely determined.

(C) $(a^{-1})^{-1} = a$ for all $a \in G$.

(D) $(ab)^{-1} = b^{-1}a^{-1}$

(E) For any $a_1, \ldots, a_n \in G$, $\prod_{i=1}^{n} a_i$ is independent of how the expression is parenthesized. (This is known as the generalized associative law).

Proof.

(A) Let $f, g \in G$ be identities. Then $fg = f$ since f is an identity, and $fg = g$ since g is an identity. So $f = g$ and the identity of G is unique.

(B) Fix $a \in G$ and let $x, y \in G$ such that $ax = ya = 1$. Then $y = y1 = y(ax)$. By associativity of the group operation, we have $y(ax) = (ya)x = 1x = x$. So $y = x = a^{-1}$, so a^{-1} is unique.

(C) Exchanging the role of a and a^{-1}, we have from the proof of (B) and the definition of an inverse that $a = (a^{-1})^{-1}$.

(D) We consider $abb^{-1}a^{-1} = a(bb^{-1})a^{-1}$ by associativity. By the group operation, $bb^{-1} = 1$, so $a(bb^{-1})a^{-1} = a(1)a^{-1} = aa^{-1} = 1$.

(E) The proof is by induction on n. When $n \leq 3$, the associativity axiom of the group yields the desired result. Now let $k \geq 3$; and suppose that for any $a_1, \ldots, a_k \in G$, $\prod_{i=1}^{k} a_i$ is uniquely determined, regardless of the parenthesization. Let $a_{k+1} \in G$ and consider $\prod_{i=1}^{k+1} a_i$. Any parenthesization of this product breaks it into two sub-products $\prod_{i=1}^{j} a_i$ and $\prod_{i=j+1}^{k+1} a_i$, each of which may be further parenthesized. As there are two non-empty products, each product has at most k terms. So by the inductive hypothesis, each subproduct is uniquely determined regardless of parenthesization. Let $x = \prod_{i=1}^{j} a_i$ and $y = \prod_{i=j+1}^{k+1} a_i$. We apply the inductive hypothesis again to xy to obtain the desired result.

□

We conclude this section with the definition of the *order* of a group and the definition of a subgroup.

Definition 77 (Order)**.** Let G be a group. We refer to $|G|$ as the *order of the group*. For any $g \in G$, we refer to $|g| = \min\{n \in \mathbb{Z}^+ : g^n = 1\}$ as the *order of the element* g. By convention, $|g| = \infty$ if no $n \in \mathbb{Z}^+$ satisfies $g^n = 1$.

Example 75. Let $G = \mathbb{Z}_6$ over addition. We have $|\mathbb{Z}_6| = 6$. The remainder class $\overline{3}$ has order 2 in G.

Example 76. Let $G = \mathbb{R}$ over addition. We have $|G| = \infty$ and $|g| = \infty$ for all $g \neq 0$. The order $|0| = 1$.

Definition 78 (Subgroup)**.** Let G be a group. We say that H is a subgroup of G if $H \subset G$ and H itself is a group. We denote the subgroup relation $H \leq G$.

Example 77. Let $G = \mathbb{Z}_6$ and $H = \{\overline{0}, \overline{3}\}$.

3.1.2 Dihedral Group

The Dihedral group is a common first example of a non-Abelian group, along with the Symmetry group. In some ways, the Dihedral group is more tangible than the Symmetry group, and we shall see the reason for this shortly. From a pedagogical perspective, intuition is a compelling argument to present the Dihedral group before the Symmetry group. In contrast, the Dihedral group is a subgroup of the Symmetry group; so mathematically, there is reason to present the Symmetry group first. Both orderings have merits and drawbacks. However, in keeping with Dummit and Foote as well as for the sake of intuition, we begin with the Dihedral group and follow up with the Symmetry group.

Standard algebra texts introduce the Dihedral group as the group of symmetries for the regular polygon on n vertices, where $n \geq 3$. The Dihedral group provides an algebraic construction to study the rotations and reflections of the regular polygon on n vertices. This provides a very poor intuition for what constitutes a symmetry, or why rotations and reflections qualify here. Formally, a symmetry is a function from a set to itself that preservs a certain property. More precisely, symmetries are automorphisms of a given structure. We begin with the definition of an isomorphism.

Definition 79 (Graph Isomorphism)**.** Let G, H be graphs. G and H are said to be *isomorphic*, denoted $G \cong H$, if there exists a bijection $\phi : V(G) \to V(H)$ such that $ij \in E(G) \implies \phi(i)\phi(j) \in E(H)$. The function ϕ is referred to as an *isomorphism*. The condition $ij \in E(G) \implies \phi(i)\phi(j) \in E(H)$ is referred to as the *homomorphism* condition. If $G = H$, then ϕ is a *graph automorphism*.

Remark: The Graph Isomorphism relation denotes that two graphs are, intuitively speaking, the same up to relabeling; this relation is an equivalence relation.

It is also important to note that Graph Homomorphisms, which for graphs G and H are maps $\phi : V(G) \to V(H)$ such that $ij \in E(G) \implies \phi(i)\phi(j) \in E(H)$, are of importance as well. They are also known as *colorings*, which are labelings of the vertices such that no two vertices use the same color. In particular, the chromatic number of a graph is defined as follows.

Definition 80 (Chromatic Number)**.** Let G be a graph. The *chromatic number* of G, denoted $\chi(G)$ is defined as:

$$\chi(G) = \min\{n \in \mathbb{N} : \text{there exists a homomorphism } \phi : V(G) \to V(K_n)\} \tag{27}$$

Determining the chromatic number of a graph is an $\mathcal{NP}$-Hard problem. We will discuss graph homomorphisms in greater detail at a later point, as well as group isomorphisms and group homomorphisms. For now, we proceed to discuss the Dihedral group.

Recall that the Dihedral group is the group of rotations and reflections of the regular polygon on n vertices (where $n \geq 3$). This geometric object is actually the cycle graph C_n, and the rotations and reflections are actually automorphisms. We start by intuiting the structure of the automorphisms for cycle graphs. As an automorphism preserves a vertex's neighbors, it is necessary that a vertex v_i can only map to a vertex with degree at least $\deg(v_i)$. As the cycle graph is 2-regular (all vertices have degree 2), there are no restrictions in terms of mapping a vertex v_i of higher degree to a vertex v_j of lower degree (as this would result in one of v_is adjacencies not being preserved). So lets start with v_1 and map $v_1 \mapsto v_i$ for some $i \in \{2, ..., n\}$.

In C_n, v_1 has neighbors v_2, v_n. So in the automorphism, $\phi(v_n)\phi(v_1), \phi(v_1)\phi(v_2) \in E(C_n)$. This leaves two options. Either preserve the sequence: $\phi(v_n) - \phi(v_1) - \phi(v_2)$ or swap the vertices v_n, v_2 under automorphism to get the sequence $\phi(v_2) - \phi(v_1) - \phi(v_n)$.

As an automorphism is an isomorphism, it must preserve adjacencies. So the sequence $\phi(v_2) - \phi(v_3) - ... - \phi(v_{n-1}) - \phi(v_n)$ must exist after mapping v_1. After fixing v_1, v_2 and v_n, there is only one option for each of $\phi(v_3)$ and $\phi(v_{n-1})$. This in terms fixes $\phi(v_4)$ and $\phi(v_{n-2})$, etc. In short, fixing a single vertex then choosing whether or not to reflect its adjacencies fixes the entire cycle under automorphism.

Conceptually, consider taking n pieces of rope and tying them together. The knots are analogous to the graph vertices. If each person holds a knot, shifting the people down by n positions is still an isomorphism. A single person can then grab the two incident pieces of rope to his or her knot, and flip those pieces around (the reflection operation). The same cycle structure on the rope remains.

So there are n such ways to permute a single vertex. Then there are two options: reflect its adjacencies or leave them be. This then fixes the cycle, and so the possible automorphisms are exhausted. By rule of product, we multiply $2 \cdot n$, which counts the number of automorphisms of C_n.

Before introducing the Dihedral group formally, we begin with the notion of a group presentation. Rather than listing each of the group elements, which can be tedious and unweildy for large groups, a presentation provides a smaller collection of elements and their relations, which generate the group. Formally, we have:

Definition 81 (Group Presentation)**.** A presentation of a group G is $\langle x_1, \ldots, x_k : R_1, \ldots, R_n \rangle$ where $x_1, \ldots, x_k \in G$ are referred to as the *generators* and $R_1, \ldots, R_n$ are referred to as the *relations*.

We now introduce the Dihedral group.

Definition 82 (Dihedral Group)**.** Let $n \geq 3$. The *Dihedral group of order* $2n$, denoted D_{2n}, is given by the following presentation:

$$D_{2n} = \langle r, s : r^n = s^2 = 1, rs = sr^{-1} \rangle \tag{28}$$

Formally, $D_{2n} \cong Aut(C_n)$, where $Aut(C_n)$ is the automorphism group of the cycle graph C_n. The presentation of the Dihedral group captures the notions of rotation and reflection which have been discussed so far. Note that r and s are both bijections, and the group operation is function composition. The element r captures the notion of rotation. Notice $|r| = n$. The interpretation is that r rotates the cycle clockwise (or counter-clockwise, if preferred, so long as you are consistent) by one vertex, and so r^i states to rotate the cycle i spots clockwise. The element s then captures the notion of reflection. And so, looking back at the example above, s being present denotes flipping the order on the neighbors of the vertex being rotated. In a sense, s is an indicator. So let $j \in \{1, ..., n\}$ and consider the elements $r^j s \in D_{2n}$. The operation is function composition, so the elements are considered from right to left. So $r^j s$ says to first reflect the cycle along the vertex v_1. This is the *flipping the rope* step in the analogy above. The second step is to rotate each vertex by j elements clockwise.

The final relation in the presentation of D_{2n} provides sufficient information to compute the inverse of each element. The presentation states that $(rs)^2 = 1$, which implies that $rs = (rs)^{-1}$. Lets solve for the exact form of $(rs)^{-1}$. By the presentation of $D_{2n}, s^2 = 1$, which implies that $|s| \leq 2$. As $s \neq 1, |s| = 2$. So $rs \cdot s = r$. As $r^n = 1$, it follows that $r^{n-1} = r^{-1}$. Intuitively, r states to rotate the cycle by one element clockwise. So r^{-1} undoes this operation. Rotating one unit counter-clockwise will leave the cycle in the same state as rotating it $n - 1$ units clockwise. So $r^{-1} = r^{n-1}$. It follows that $rs = (rs)^{-1} = sr^{-1} = sr^{n-1}$. And so $(r^i s)^{-1} = sr^{-i} = sr^{n-i}$.

We conclude with a final remark about what is to come. The Dihedral group provides our first example of a group action. Intuitively, a group action is a dynamical process in which a group's elements are used to permute the elements of some set. We study the permutation structures which arise from the action, which provide deep combinatorial insights. Here, the Dihedral group acts on the cycle graph C_n by rotating and reflecting its vertices. This is a very tangible example of the dynamical process of a group action. We will formally introduce group actions later.

3.1.3 Symmetry Group

The Symmetry group is perhaps one of the most important groups, from the perspective of algebraic combinatorics. The Symmetry group captures all possible permutations on a given set. Certain subgroups of the Symmetry group provide extensive combinatorial information about the symmetries of other mathematical objects. We begin by formalizing the notion of a permutation.

Definition 83 (Permutation)**.** Let X be a set. A permutation is a bijection $\pi : X \to X$.

Formally, we define the Symmetry group as follows:

Definition 84 (Symmetry Group)**.** Let X be a set. The *Symmetry group* S_X is the set of all permutations $\pi : X \to X$ with the operation of function composition.

Remark: Recall that the composition of two bijections is itself a bijection. This provides for closure of the group operation. The identity map is a bijection, and so a permutation. This is the identity of the Symmetry group. In order to see that the Symmetry group is closed under inverses, it is helpful to think of a permutation as a series of swaps or transpositions. We simply undo each transposition to obtain the identity. Showing that every permutation can be written as the product of (not necessarily disjoint) two-cycles is an exercise left to the reader.

We first show how to write permutations in cycle notation. Formally, we have:

Definition 85 (Cycle)**.** A *cycle* is a sequence of integers which are cyclically permuted.

Definition 86 (Cycle Decomposition)**.** The *cycle decomposition* of a permutation π is a sequence of cycles where no two cycles contain the same elements. We refer to the cycle decomposition as a product of disjoint cycles, where each cycle is viewed as a permutation.

Theorem 3.1. *Every permutation π of a finite set X can be written as the product of disjoint cycles.*

The proof is constructive. We provide an algorithm to accomplish this. Intuitively, a cyclic permutation is simply a rotation. So we take an element $x \in X$ and see where x maps under π. We then repeat this for $\pi(x)$. The cycle is closed when $\pi^n(x) = x$. Formally, we take $(x, \pi(x), \pi^2(x), \ldots, \pi^n(x))$. We then remove the elements covered by this cycle and repeat for some remaining element in X. As X is finite and each iteration partitions at least one element into a cycle, the algorithm eventually terminates. The correctness follows from the fact that this construction provides a bijection between permutations and cycle decompositions. We leave the details of this to the reader, but it should be intuitively apparent. Let's consider a couple examples.

Example 78. Let σ be the permutation:

$$1 \mapsto 3 \quad 2 \mapsto 4 \quad 3 \mapsto 5 \quad 4 \mapsto 2 \quad 5 \mapsto 1 \tag{29}$$

Select 1. Under σ, we have $1 \mapsto \sigma(1) = 3$. Then $3 \mapsto \sigma(3) = 5$. Finally, $5 \mapsto \sigma(5) = 1$. So we have one cycle $(1, 3, 5)$. By similar analysis, we have $2 \mapsto 4$ and $4 \mapsto 2$, so the other cycle is $(2, 4)$. Thus, $\sigma = (1, 3, 5)(2, 4)$.

Example 79. Let τ be the permutation:

$$1 \mapsto 5 \quad 2 \mapsto 3 \quad 3 \mapsto 2 \quad 4 \mapsto 4 \quad 5 \mapsto 1 \tag{30}$$

Select 1. We have $1 \mapsto 5$, and then $5 \mapsto 1$. So we have the cycle $(1, 5)$. Similarly, we have the cycle $(2, 3)$. Since $4 \mapsto 4$, we have (4). By convention, we do not include cycles of length 1 which are fixed points. So $\tau = (1, 5)(2, 3)$.

In order to deal with the cycle representation in any meaningful way, we need a way to evaluate the composition of two permutations, which we call the **Cycle Decomposition Procedure**. We provide a second algorithm to take the product of two cycle decompositions and produce the product of disjoint cycles. Consider two permutations σ, τ and evaluate their product $\sigma\tau$, which is parsed from right to left as the operation is function composition. We view each cycle as a permutation and apply a similar procedure as above. We select an element x not covered in the final answer and follow it from right-to-left according to each cycle. When we reach the left most cycle, the element we end at is x's image under the product permutation. We then take x's image and repeat the procedure until we complete the cycle; that is, until we end back at x. We iterate again on some uncovered element until all elements belong to disjoint cycles. Let's consider an example:

Example 80. We consider the permutation

$$(1,2,3)(3,5)(3,4,5)(2,4)(1,3,4)(1,2,3,4,5) \tag{31}$$

We evaluate this permutation as follows:

- We begin by selecting 1 and opening a cycle (1. Under $(1,2,3,4,5)$ we see $1 \mapsto 2$. We then move to $(1,3,4)$, under which 2 is a fixed point. Then under $(2,4)$, $2 \mapsto 4$. Next, we see $4 \mapsto 5$ under $(3,4,5)$. Then $5 \mapsto 3$ under $(3,5)$, and $3 \mapsto 1$ under $(1,2,3)$. So 1 is a fixed point and we close the cycle: (1).
- Next, we select 2. Under $(1,2,3,4,5)$, $2 \mapsto 3$. We then see $3 \mapsto 4$ under $(1,3,4)$. Under $(2,4), 4 \mapsto 2$. The cycle $(3,4,5)$ fixes 2, as does $(3,5)$. So we finally have $2 \mapsto 3$, yielding $(2,3$.
- By similar analysis, we see $3 \mapsto 4 \mapsto 1 \mapsto 2$, so we close $(2,3)$.
- The only two uncovered elements are now 4 and 5. Selecting 4, we obtain $4 \mapsto 5 \mapsto 3 \mapsto 5$. So we have $(4,5$. Then we see $5 \mapsto 1 \mapsto 3 \mapsto 4$, so we close $(4,5)$.

Thus:

$$(1,2,3)(3,5)(3,4,5)(2,4)(1,3,4)(1,2,3,4,5) = (2,3)(4,5) \tag{32}$$

The Cycle Decomposition Algorithm provides us with a couple nice facts.

Theorem 3.2. *Let c_1, c_2 be disjoint cycles. Then $c_1c_2 = c_2c_1$.*

Proof. We apply the Cycle Decomposition algorithm to c_1c_2 starting with the elements in c_2, to obtain c_2c_1. □

Remark: This generalizes for any product of n disjoint cycles.

Theorem 3.3. *Let $(x_1, \ldots, x_n)$ be a cycle. Then $|(x_1, \ldots, x_n)| = n$.*

Proof. Consider $(x_1, \ldots, x_n)^n = \prod_{i=1}^{n}(x_1, \ldots, x_n)$. Applying the cycle decomposition algorithm, we see $x_1 \mapsto x_2 \mapsto \ldots \mapsto x_n \mapsto x_1$. We iterate on this procedure for each element in the cycle to obtain $\prod_{i=1}^{n}(x_1, \ldots, x_n) = (1)$, the identity permutation. So $|(x_1, \ldots, x_n)| \leq n$. Applying the cycle decomposition procedure to $(x_1, \ldots, x_n)^k$ for any $k \in [n-1]$, and we see $x_1 \mapsto x_k, x_2 \mapsto x_{k+1}, \ldots, x_n \mapsto x_{n+k+1}$ where the indices are taken modulo n. □

3.1.4 Quaternion Group

We write $Q_8 = \langle -1, i, j, k : (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1 \rangle$. Dummit and Foote includes the multiplications written explicitly on Page 36. The homework problems provide good exercises to familiarize oneself with an unfamiliar group and build up some maturity. The Quaternion group also comes up frequently in subsequent homework exercises in later sections.

3.1.5 Group Homomorphisms and Isomorphisms

In the exposition of the Dihedral group, we have already defined the notion of a graph isomorphism. Recall that a graph isomorphism is a bijection from the vertex sets of two graphs G and H, that preserves adjacencies. The group isomorphism is defined similarly. The one change is the notion of a homomorphism. While a graph homomorphism preserves adjacencies, a group homomorphism preserves the group operation. Formally:

Definition 87 (Group Homomorphism)**.** Let $(G, \star)$ and $(H, \diamond)$ be groups. A *group homomorphism* from G to H is a function $\phi : G \to H$ such that $\phi(x \star y) = \phi(x) \diamond \phi(y)$ for all $x, y \in G$. Omitting the formal operation symbols (as is convention), the homomorphism condition can be written as $\phi(xy) = \phi(x)\phi(y)$.

Example 81. Let $G = \mathbb{Z}_4$ and $H = \mathbb{Z}_2$. The function $\phi : \mathbb{Z}_4 \to \mathbb{Z}_2$ sending $\overline{0}_4$ and $\overline{2}_4$ to $\overline{0}_2$, and $\overline{1}_4$ and $\overline{3}_4$ to $\overline{1}_2$ is a homomorphism. We verify as follows. Let $\overline{x}_4, \overline{y}_4 \in \mathbb{Z}_4$. We have $\overline{x}_4 + \overline{y}_4 = \overline{x+y}_4$. We have $\overline{x+y}_2 = \overline{0}_2$ if and only if $\overline{x+y}_4 \in \{\overline{0}_4, \overline{2}_4\}$ if and only if $\overline{x}_4 + \overline{y}_4 \in \{\overline{0}_4, \overline{2}_4\}$. So ϕ is a homomorphism.

We now introduce the notion of a group isomorphism.

Definition 88 (Group Isomorphism)**.** Let G, H be groups. A *group isomorphism* is a bijection $\phi : G \to H$ that is also a group homomorphism. We say that $G \cong H$ (G is isomorphic to H) if there exists an isomorphism $\phi : G \to H$.

We consider a couple examples of group isomorphisms.

Example 82. Let G be a group. The identity map $\mathrm{id} : G \to G$ is an isomorphim.

Example 83. Let $\exp : \mathbb{R} \to \mathbb{R}^+$ be given by $x \mapsto e^x$. This map is a bijection, as we have a well-defined inverse function: the natural logarithm. We easily verify the homomorphism condition: $\exp(x+y) = e^{x+y} = e^x e^y$.

There are several important problems relating to group isomorphisms:

- Are two groups isomorphic?
- How many isomorphisms exist between two groups?
- Classify all groups of a given order.

In some cases, it is easy to decide if two groups are (not) isomorphic. In general, the group isomorphism problem is undecidable; no algorithm exists to decide if two arbitrary groups are isomorphic. In particular, if two groups $G \cong H$, the following necessary conditions hold:

- $|G| = |H|$
- G is Abelian if and only if H is Abelian
- $|x| = |\phi(x)|$ for every $x \in G$ and every isomorphism $\phi : G \to H$.

It is quite easy to verify that the isomorphism relation preserves commutativity. Consider an isomorphism $\phi : G \to H$ and let $a, b \in G$. If G is Abelian, then $ab = ba$. Applying the isomorphism, we have $\phi(a)\phi(b) = \phi(b)\phi(a)$. As ϕ is surjective, it follows that H is also Abelian.

Similarly, it is quite easy to verify that for any isomorphism ϕ that $|x| = |\phi(x)|$. We prove a couple lemmas.

Lemma 3.1. *Let G, H be groups and let $\phi : G \to H$ be a homomorphism. Then $\phi(1_G) = 1_H$.*

Proof. Recall that $\phi(1_G) = \phi(1_G \cdot 1_G)$. Applying the homomorphism, we obtain that $\phi(1_G) = \phi(1_G)\phi(1_G) = \phi(1_G) \cdot 1_H$. By cancellation, we obtain that $\phi(1_G) = 1_H$. □

With Lemma 3.1 in mind, we prove this next Lemma.

Lemma 3.2. *Let G, H be groups and let $\phi : G \to H$ be a homomorphism. Then $|x| \geq |\phi(x)|$.*

Proof. Let $n = |x|$. So $\phi(x^n) = \phi(x)^n = \phi(1_G) = 1_H$. Thus, $|\phi(x)| \leq n$. □

We now show that isomorphisms are closed under inverses.

Theorem 3.4. *Let G, H be groups and let $\phi : G \to H$ be an isomorphism. Then $\phi^{-1} : H \to G$ is also an isomorphism.*

Proof. An isomorphism is a bijection, so $\phi^{-1} : H \to G$ exists and is a function. It suffices to show that ϕ^{-1} is a function. Let $a, b \in G$ and $c, d \in H$ such that $\phi(a) = c$ and $\phi(b) = d$. So $\phi(ab) = \phi(a)\phi(b) = cd$. We apply ϕ^{-1} to obtain $\phi^{-1}(cd) = \phi^{-1}(\phi(a)\phi(b)) = \phi^{-1}(\phi(ab))$, with the last equality as ϕ is a homomorphism. So $\phi^{-1}(\phi(ab)) = ab$. Similarly, $\phi^{-1}(c)\phi^{-1}(d) = ab$. So ϕ^{-1} is a homomorphism, and therefore an isomorphism. □

We now use Lemma 3.2 and Theorem 3.4 to deduce that isomorphism preserves each element's order.

Theorem 3.5. *Let G, H be groups and let $\phi : G \to H$ be an isomorphism. Then $|x| = |\phi(x)|$ for all $x \in G$.*

Proof. We have $|x| \geq |\phi(x)|$ from Lemma 3.2. As ϕ^{-1} is an isomorphism, we interchange the role of x and $\phi(x)$ then apply Lemma 3.2 again to obtain $|\phi(x)| \geq |x|$. □

We conclude this section with a classification result. The proof of this theorem requires machinery we do not presently have; namely, Lagrange's Theorem which states that any subgroup H of a finite group G, $|H|$ divides $|G|$. I leave Lagrange's Theorem as a homework exercise as it pertains to group actions.

Theorem 3.6. *Every group of order 6 is either S_3 or $\mathbb{Z}_6$.*

3.1.6 Group Actions

The notion of a group action is one of the most powerful and useful notions from algebra. Intuitively, a group action is a discrete dynamical process on a set of elements that partitions the set. The structure and number of these equivalence classes provide important insights in algebra, combinatorics, and graph theory. We formalize the notion of a group action:

Definition 89 (Group Action)**.** Let G be a group and let A be a set. A *group action* is a function $\cdot : G \times A \to A$ (written $g \cdot a$ for all $g \in G$ and $a \in A$) satisfying:

1. $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and all $a \in A$.
2. $1 \cdot a = a$ for all $a \in A$

Before providing examples of group actions, we begin by proving Cayley's Theorem which yields that every group action has a permutation representation. That is, if the group G acts on the set A, G permutes A. Formally, we have:

Theorem 3.7 (Cayley's Theorem)**.** *Let G act on the set A. Then there exists a homomorphism from G into S_A. When $A = G$ (that is, when G is acting on itself), we have an isomorphism from G to a group of permutations.*

Proof. For each $g \in G$, we define the map $\sigma_g : A \to A$ by $\sigma_g(a) = g \cdot a$. We prove the following propositions.

Proposition 3.3. *For each $g \in G$, the function σ_g is a permutation. Furthremore, $\{\sigma_g : g \in G\}$ forms a group.*

Proof. It suffices to show that σ_g has a two-sided inverse. Consider $\sigma_{g^{-1}}$, which exists as G is a group. We have $(\sigma_{g^{-1}} \circ \sigma_g)(a) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = a$. So $\sigma_{g^{-1}} \circ \sigma_g = (1)$, the identity map. As g was arbitrary, we exchange g and g^{-1} to obtain that $\sigma_g \circ \sigma_{g^{-1}} = (1)$ as well. So σ_g has a two-sided inverse, and so it is a permutation. As G is a group, we have that $\{\sigma_g : g \in G\}$ is non-empty and forms a group as well. □

Proposition 3.3 gives us our desired subgroup of S_A. We construct a homomorphism $\phi : G \to S_A$, with $\phi(G) = \{\sigma_g : g \in G\}$. We refer to $\phi(G)$ as the *permutation representation* of the action. When G acts on itself; that is, when $G = A$, $G \cong \phi(G) \leq S_G$.

Proposition 3.4. *Define $\phi : G \to S_A$ by $g \mapsto \sigma_g$. This function ϕ is a homomorphism.*

Proof. Clearly, $\phi(G) = \{\sigma_g : g \in G\}$. We show that ϕ is a homomorphism. Let $g_1, g_2 \in G$. Consider $\phi(g_1 g_2)(a) = \sigma_{g_1 g_2}(a) = g_1 g_2 \cdot a = g_1 \cdot (g_2 \cdot a) = \sigma_{g_1}(\sigma_2(a)) = \phi(g_1)\phi(g_2)(a)$. So ϕ is a homomorphism. □

We conclude by showing $G \cong \phi(G)$ when $A = G$.

Proposition 3.5. *Suppose $G = A$. Then $G \cong \phi(G)$.*

Proof. Let ϕ be defined as in Proposition 3.3. The proof of Proposition 3.3 provides that ϕ is a surjective homomorphism. It suffices to show ϕ is injective. Let $g, h \in G$ such that $\phi(g) = \phi(h)$. So $\sigma_g = \sigma_h$, which implies that the permutations agree on all points in G. In particular, $\sigma_g(1) = \sigma_h(1) = g1 = h1 = g = h$. So ϕ is injective, and we conclude $G \cong \phi(G) \leq S_G$. □

□

We now consider several important examples of group actions:

Example 84. Let G be a group and let A be a set. The action in which $g \cdot a = a$ for all $g \in G$ and all $a \in A$ is known as the *trivial action*. In this case, $\sigma_g = (1)$ for all $g \in G$. The trivial action provides an example of why it is sufficient for G to act on itself in order to be isomorphic to a group of permutations.

Example 85. Let A be a set and let $G = S_A$. The action of S_A on A is given by $\sigma \cdot a = \sigma(a)$ for any permutation σ and element $a \in A$.

Example 86. Let $G = D_{2n}$ and let $A = V(C_n)$. D_{2n} acts on the vertices of C_n by rotation and reflection. In particular, $r = (1, 2, \ldots, n)$ and $s = \prod_{i=2}^{\lfloor n/2 \rfloor}(i, n - i + 1)$.

It turns out that it is not necessary for G to act on itself in order for the permutation representation of the action to be isomorphic to G. We introduce the notion of the kernel and a faithful action.

Definition 90 (Kernel of the Action)**.** Suppose G acts on a set A. The *kernel* of the action is defined as $\{g \in G : g \cdot a = a, \forall a \in A\}$.

Definition 91 (Faithful Action)**.** Suppose G acts on the set A. The action is said to be *faithful* if the kernel of the action is $\{1\}$.

In particular, if the action is faithful, then each permutation σ_g is unique. So $G \cong \phi(G)$.

One application of group actions is a nice, combinatorial proof of Fermat's Little Theorem. We have already given this proof with Theorem 1.14, but abstracted away the group action. We offer the same proof using the language of group actions below.

Theorem 3.8 (Fermat's Little Theorem)**.** *Let p be a prime number and let $a \in [p - 1]$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Let Λ be an alphabet of order p. Let $\mathbb{Z}_p \cong \langle (1, 2, \ldots, p) \rangle$ act on Λ^p by cyclic rotation. The *orbit* of a string $\omega \in \Lambda^p$, denoted

$$\mathcal{O}(\omega) = \{g \cdot \omega : g \in \mathbb{Z}_p\}$$

Consists of either a single string or p strings. Each orbit is an equivalence class under the action. There are a orbits with a single string, where each string is simply a single character repeated p times. So we partition the remaining $a^p - a$ strings into orbits containing p strings. So $p \big| (a^p - a)$, which implies $a^p \equiv a \pmod{p}$. □

Lagrange's Theorem is similarly proven. In fact, Fermat's Little Theorem is a special case of Lagrange's Theorem. We conclude by stating Lagrange's Theorem, but the proof is an exercise for homework.

Theorem 3.9 (Lagrange's Theorem)**.** *Let G be a finite group, and let $H \leq G$. Then the order of H divides the order of G.*

3.1.7 Algebraic Graph Theory- Cayley Graphs

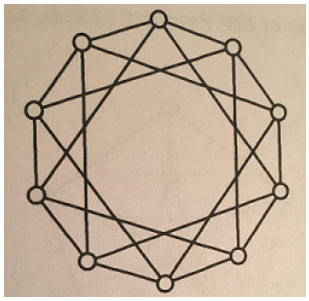
We introduce the notion of a Cayley Graph, which provides an intuitive approach to visualizing the structure of a group. Formally, we define the Cayley Graph as follows:

Definition 92 (Cayley Graph)**.** Let G be a group and let $C \subset G$ such that $1 \notin C$ and for every $x \in C$, $x^{-1} \in C$. The *Cayley Graph* with respect to G and C is denoted $X(G, C)$ where $V(X) = G$ and $ij \in E(X)$ if $ji^{-1} \in C$. We refer to C as the *Cayley set*.

We begin with an example of a Cayley graph- the Cycle graph.

Example 87. Let $G = \mathbb{Z}_n$, where the operation is addition. Let $C = \{\pm\overline{1}\}$. So the vertices of $X(G, C)$ are the congruence classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. We have an edge $\overline{ij}$ if and only if $\overline{j} - \overline{i} = \overline{1}$ or $\overline{j} - \overline{i} = \overline{n-1}$.

Example 88. The Cycle graph is in particular an *undirected circulant graph*. Let $G = \mathbb{Z}_n$, where the operation is addition. Let $C \subset \mathbb{Z}_n$ such that $0 \notin C$ and $\overline{x} \in C \implies -\overline{x} \in C$. The Cayley graph $X(G, C)$ is an undirected circulant graph. The complete graph K_n is a Cayley graph with $G = \mathbb{Z}_n$ and $C = \mathbb{Z}_n \setminus \{\overline{0}\}$. Similarly, the empty graph is a Cayley graph with $G = \mathbb{Z}_n$ and $C = \emptyset$. We illustrate below the case where $G = \mathbb{Z}_{10}$ with $C = \{\pm\overline{1}, \pm\overline{3}\}$.



We now develop some theory about Cayley Graphs.

Theorem 3.10. *Let G be a group with $C \subset G$ as the Cayley set. Let $X(G, C)$ be the associated Cayley graph. For any $u, v \in G$, there exists a $\phi \in Aut(X(G, C))$ such that $\phi(u) = v$. (That is, every Cayley graph is vertex transitive).*

Proof. Let $u, v \in G$ such that $uv \in E(X)$. Then $vu^{-1} \in C$. Let $g \in G$ and define $\rho_g : x \mapsto xg$. Then $\rho_g(v)(\rho_g(u))^{-1} = vg(ug)^{-1} = vgg^{-1}u^{-1} = vu^{-1}$, so $\rho_g(u)\rho_g(v) \in E(X(G, C))$. Thus, $\rho_g \in \mathrm{Aut}(X(G, C))$. So $X(G, C)$ is vertex transitive. □

In order for a graph to be vertex-transitive, it is necessary for the graph to be regular (as isomorphism preserves vertex degree- an exercise for the reader to verify). The next lemma shows that a Caley graph $X(G, C)$ is in fact $|C|$-regular.

Lemma 3.3. *Let G be a group and with $C \subset G$ as the Cayley set. Let $X(G, C)$ be the associated Cayley graph. Then $X(G, C)$ is $|C|$-regular.*

Proof. Let $v \in G$ and $x \in C$. There exists a unique $u \in G$ such that $vu^{-1} = x$. In particular, $u = x^{-1}v$. So v has $|C|$ neighbors in $X(G, C)$. As our choice of v was arbitrary, we conclude that $X(G, C)$ is $|C|$-regular. □

We next show that a Cayley graph is connected if and only if its Cayley set generates the entire group. The idea is to think of each vertex in the path as a multiplication. So the edge xy in $X(G, C)$ is a multiplication by yx^{-1}. And so a path is a sequence of these multiplications, where the inverses in the interior of the expression cancel. Formally, we have:

Theorem 3.11. *Let G be a group and let C be the Cayley set. The Cayley graph $X(G, C)$ is connected if and only if $\langle C \rangle = G$.*

Proof. Suppose first that $X(G,C)$. Let $x_1, x_k \in G$. Let $x_1x_2\dots x_k$ be a shortest path from x_1 to x_k in G. By definition of the Cayley graph, $x_i^{-1}x_{i-1} \in C$ for each $i \in \{2,\dots,k\}$. Applying the multiplications: $(x_k^{-1}x_{k-1})(x_{k-1}^{-1}x_{k-2})\dots(x_2^{-1}x_1) = x_k^{-1}x_1 \in \langle C\rangle$. So C generates G.

We now show by contrapositive that $\langle C\rangle = G$ implies $X(G,C)$ is connected. Suppose $X(G,C)$ is not connected. Let $u, v \in X(G,C)$ such that no $u-v$ path exists in $X(G,C)$. Let y be the unique solution to $uy = v$. Then $y \notin \langle C\rangle$, so $\langle C\rangle \neq G$. □

With this in mind, we show that the Petersen graph is not a Cayley graph (though it is vertex-transitive, a fact that will be left for homework).

Theorem 3.12. *The Petersen Graph is not a Cayley Graph.*

Proof. Suppose to the contrary that the Petersen graph is a Cayley graph. There are two groups of order 10: $\mathbb{Z}_{10}$ and D_{10}. As the Petersen graph is 3-regular, we have that a Cayley set $C \subset G$ has three elements. So either one or all three elements are their own inverses. If $G = \mathbb{Z}_{10}$, then $C = \{\overline{a}, -\overline{a}, \overline{5}\}$. Observe that $(\overline{0}, \overline{a}, \overline{5+a}, \overline{5})$ forms a sequence of vertices that constitute a 4-cycle in $X(\mathbb{Z}_{10}, C)$. However, any pair of non-adjacent vertices in the Petersen graph share precisely one common neighbor, so the Petersen graph has no four-cycle. So the Petersen graph is not the Cayley graph of $\mathbb{Z}_{10}$.

Now suppose instead that $G = D_{10}$. C necessarily generates D_{10}, as the Petersen graph is connected. If C has precisely one element of order 2, then $C = \{r^i, r^{-i}, sr^j\}$ for some $i, j \in [4]$. In this case, 1 is adjacent to both r^i and sr^j in $X(G,C)$. However, r^i and sr^j are both adjacent to sr^{j+i}. We verify $sr^{j+i} \cdot r^{-j}s = r^{-i}sr^j \cdot r^{-j}s = r^{-i} \in C$, applying the fact $sr^i = r^{-i}s$ for all $i \in [5]$. Similarly, we consider $sr^{j+i}r^{-i} = sr^j \in C$. So we have a four-cycle in $X(G,C)$ consisting of $(1, r^i, sr^{j+i}, sr^j)$.

Suppose instead $C = \{sr^i, sr^j, sr^k\}$ for $m \in \{0,1\}$ and distinct $i, j, k \in \{0,1,2,3,4\}$. We have 1 is adjacent to each element of C in $X(G,C)$. The other two neighbors of sr^j are r^{i-j} and r^{k-j}. However, sr^k is also adjacent to r^{k-j}, creating a four-cycle in $X(G,C)$. So in this case, $X(G,C)$ is not isomorphic to the Petersen graph.

As we have exhausted all possibilities, we conclude that the Petersen graph is not a Cayley graph. □

We now provide some exposition on transpositions. A permutation of $[n]$ can be viewed as a directed graph with vertex set $[n]$, which is the disjoint union of directed cycles. Each directed cycle in the grpah corresponds to a cycle in the permutation's cycle decomposition. Furthermore, each permutation cycle can be decomposed as the product of transpositions, or 2-cycles. The transpositions are viewed as edges. We adapt this framing to study the Symmetry group from an algebraic standpoint.

Formally, let $\mathcal{T}$ be a set of transpositions. We define the graph T with vertex set $[n]$ and edge set

$$E(T) = \{ij : (ij) \in \mathcal{T}\} \tag{33}$$

We say that $\mathcal{T}$ is *generating set* if $S_n = \langle\mathcal{T}\rangle$, and $\mathcal{T}$ is *minimal* if for any $g \in \mathcal{T}$, $\mathcal{T} \setminus \{g\}$ is not a generating set. Note that T is not a Cayley graph, but it is useful in studying the Cayley graphs of S_n.

We begin with an analogous result to Theorem 3.5, for T rather than Cayley Graphs.

Lemma 3.4. *Let $\mathcal{T}$ be a set of transpositions from S_n. Then $\mathcal{T}$ is a generating set for S_n if and only if its graph T is connected.*

Proof. Let T be the graph of $\mathcal{T}$, and let $G = \langle\mathcal{T}\rangle$. Suppose $(1i), (ij) \in \mathcal{T}$. Then:

$$(ij)(1i)(ij) = (1j) \in G \tag{34}$$

By induction, if there exists a $1-k$ path in T, then $(1k) \in G$. It follows that for any x, y on the same component, then $(xy) \in G$. So the transpositions belonging to a certain component generate the symmetric

group on the vertices of that component. Thus, if T is connected, then $S_n = \langle \mathcal{T} \rangle$.

We next show that if $\langle \mathcal{T} \rangle = S_n$, then T is connected. This will be done by contrapositive. If T is not connected, then no transposition of $\mathcal{T}$ can map a vertex from one component to the other. So the components are the orbits of G acting on $[n]$. □

Lemma 3.2 is quite powerful. It implies that every minimal generating set $\mathcal{T}$ of transpositions has the same cardinality. In particular, the graph of any minimal generating set is a spanning tree, so every minimal generating set has $n-1$ transpositions. This allows us to answer the following questions:

1. Is a set of transpositions $\mathcal{T}$ of S_n a generating set?
2. Is a generating set of transpositions $\mathcal{T}$ of S_n minimal?
3. If a set of transpositions is a generating set, which transpositions can be removed while still generating S_n?
4. If a set of transpositions is not a generating set, which transpositions are missing?

In order to answer these questions, we reduce to the spanning tree problem and the connectivity problem. Question 1 is answered by Lemma 3.2- we simply check if the graph T corresponding to $\mathcal{T}$ is connected, which can be done using Tarjan's algorithm which runs in $O(|V| + |E|)$ time. In order to answer Question 2, Lemma 3.2 implies that it suffices to check if T is a spanning tree. So first, we first check if the graph T is connected. If so, it suffices to check if T has $n-1$ edges, as that is the characterization of a tree.

Using our theory of spanning trees, we easily answer Question 3 as well. We can construct a spanning tree by removing an edge from a cycle, then applying the procedure recursively to the subgraph. As the transpositions of $\mathcal{T}$ correspond to edges of T, this fact about spanning trees allows us to remove transpositions from $\mathcal{T}$ while allowing the modified $\mathcal{T}$ to generate S_n.

Finally, to answer Question 4, we simply select pairs of vertices from two components of T and add an edge $e = ij$, which corresponds to setting $\mathcal{T} := \mathcal{T} \cup \{(ij)\}$. We repeat the procedure for the modified $\mathcal{T}$ until it is connected.

We conclude with a final lemma, which relates the graph T for a set of transpositions $\mathcal{T}$ to the Cayley graph $X(S_n, \mathcal{T})$.

Lemma 3.5. *Let $\mathcal{T}$ be a non-empty set of transpositions from S_n, and let $g, h \in \mathcal{T}$. If the graph T of $\mathcal{T}$ contains no triangles, then g and h have exactly one common neighbor in the Cayley graph $X(S_n, \mathcal{T})$ if $gh \neq hg$ and exactly two common neigbors otherwise.*

Proof. The neighbors of g in $X(S_n, \mathcal{T})$ are of the form xg (as $gg^{-1}x^{-1} = x^{-1} \in \mathcal{T}$). So suppose $xg = yh$ is a common neighbor of g, h in $X(S_n, \mathcal{T})$. Observe that $xg = yh$ is equivalent to $yx = hg$ (recall that $g = g^{-1}$ and $h = h^{-1}$ since g, h are transpositions). Any solution to $yx = hg$ yields a common neighbor of g, h. (Again, we may easily verify that xg is a neighbor of G and yh is a neighbor of h).

Suppose that $gh = hg$. Then g and h are disjoint, so we have two common neighbors of g and h: $1, hg$. Suppose instead $hg \neq gh$. Then g, h are not disjoint. Without loss of generality, suppose $g = (1,3)$ and $h = (1,2)$. Then $hg = (1,2,3)$, which has three factorizations: $(1,2)(1,3) = (1,3)(2,3) = (2,3)(1,2)$. As there is no triangle in T, the graph of $\mathcal{T}$, $(2,3) \notin \mathcal{T}$. So $(1,2)(1,3)$ is the unique factorization of hg in $\mathcal{T}$, yielding (1) as the unique neighbor of g, h. □

3.2 Subgroups

One basic approach in studying the structure of a mathematical satisfying a set of axioms is to study subsets of the given object which satisfy the same axioms. A second basic method is to collapse a mathematical object onto a smaller object sharing the same structure. This collapsed structure is known as a *quotient*. Both

of these themes recur in algebra: in group theory with subgroups and quotient groups; in ring theory with subrings and quotient rings; in linear algebra with subspaces and quotient spaces of vector spaces; etc. A clear understanding of subgroups is required to study quotient groups, with the notion of a *normal subgroup*.

Definition 93 (Subgroup)**.** Let G be a group, and let $H \subset G$. H is said to be a *subgroup* of G if H is also a group. We denote the subgroup relation as $H \leq G$.

We begin with some examples of subgroups:

Example 89. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.

Example 90. The group of rotations $\langle r \rangle \leq D_{2n}$

Example 91. $D_{2n} \leq S_n$

Example 92. The set of even integers is a subgroup of $\mathbb{Z}$ with the operation of adddition.

We begin with the subgroup test, which allows us to verify a subset H of a group G is actually a subgroup without verifying the group axioms.

Proposition 3.6 (The Subgroup Criterion)**.** *Let G be a group, and let $H \subset G$. $H \leq G$ if and only if:*

1. *$H \neq \emptyset$*
2. *For all $x, y \in H$, $xy^{-1} \in H$*

Furthermore, if H is finite, then it suffices to check that H is non-empty and closed under multiplication.

Proof. If $H \leq G$, then conditions (1) and (2) follow immediately from the definition of a group. Conversely, suppose that H satisfies (1) and (2). Let $x \in H$ (such an x exists because H is non-empty). As H satisfies condition (2), we let $y = x$ to deduce that $xx^{-1} = 1 \in H$. As H contains the identity of G, we apply property (2) to obtain that $1x^{-1} = x^{-1} \in H$ for every $x \in H$. So H is closed under inverses. We next show that H is closed under product. Let $x, y^{-1} \in H$. Then by property (2) and the fact that $(y^{-1})^{-1} = y$, $xy \in H$. As the operation of G is associative, we conclude that H is a subgroup of G.

Now suppose that H is finite and closed under multiplication. Let $x \in H$. As H is closed under multiplication, $\langle x \rangle \subset H$. As H is finite, $x^{-1} \in \langle x \rangle$. So H is closed under inverses and $H \leq G$. □

Example 93. We use the subgroup criterion to verify that the set of even integers is a subgroup of $\mathbb{Z}$ over addition. We have that 0 is an even integer. Now let $2x, 2y$ be even integers where $x, y \in \mathbb{Z}$. We have $(2y)^{-1} = -2y$, so $2x(2y)^{-1} = 2x - 2y = 2(x - y)$. As $\mathbb{Z}$ is closed under addition and inverses, $x - y \in \mathbb{Z}$. So $2(x - y)$ is an even integer.

We explore several families of subgroups, which yield many important examples and insights in the study of group theory. Two important problems in group theory include studying (a) how "far away" a group is from being commutative; and (b) in a group homomorphism $\phi : G \to H$, which members of G map to 1_H? On the surface, these problems do not appear to be related. In fact, both these problems are closely related. We examine a specific class of group action known as the *action of conjugation*. Studying the kernels and stabilizers of these actions provide invaluable insights about the level of commutativity of for the given group. We begin by studying the commutativity of a group, with the centralizer, normalizer, and center of a group.

Definition 94 (Centralizer)**.** Let G be a group and let $A \subset G$ be non-empty. The *centralizer* of G is the set: $C_G(A) = \{g : ga = ag, \text{ for all } a \in A\}$. That is, $C_G(A)$ is the set of elements of G which commute with every element of A.

Remark: It is common to write $C_G(A) = \{g \in G : gag^{-1} = a, \text{ for all } a \in A\}$, which is equivalent to what is presented in the definition. We see the notation gag^{-1} again when discussing the normalizer, and more generally when discussing the action of conjugation. By convention, when $A = \{a\}$, we write $C_G(\{a\}) = C_G(a)$.

Proposition 3.7. *Let G be a group, and let A be a non-empty subset of G. Then $C_G(A) \leq G$.*

Proof. We appeal to the subgroup criterion. Clearly, $1 \in C_G(A)$, so $C_G(A) \neq \emptyset$. Now suppose $x, y \in C_G(A)$ and let $a \in A$. It follows that $xya = xay = axy$, as x, y commute with a. So $C_G(A)$ is closed under the group operation. Finally, if $g \in C_G(A)$ and $a \in A$, we have $gag^{-1} = a$, which is equivalent to $ag^{-1} = g^{-1}a$, so $C_G(A)$ is closed under inverses. So $C_G(A) \leq G$. □

Example 94. Let G be a group and let $a \in G$. Then $\langle a \rangle \leq C_G(a)$, as powers of a commute with a by associativity of the group operation.

Example 95. Let G be an Abelian group. Then $C_G(A) = G$ for any non-empty $A \subset G$.

Example 96. Recall Q_8, the Quaternion group of order 8. By inspection, we see that $C_{Q_8}(i) = \{\pm 1, \pm i\}$. Observe that $ij = k$ while $ji = -k$, so $j \notin C_{Q_8}(i)$. If we consider $-j$ instead, we see that $-ji = k$ while $i(-j) = k$, so $-j \notin C_{Q_8}(i)$. By similar argument, it can be verified that $\pm k \notin C_{Q_8}(i)$.

We could alternatively use Lagrange's Theorem to compute $C_{Q_8}(i)$. Recall that Lagrange's Theorem states that $|C_{Q_8}(i)|$ divides $|Q_8| = 8$. As $\langle i \rangle \leq C_{Q_8}(i)$, we have $|C_{Q_8}(i)| \in \{4, 8\}$. As $j \notin C_{Q_8}(i)$, $|C_{Q_8}(i)| \neq 8$. Therefore, $C_{Q_8}(i) = \langle i \rangle$.

We next introduce the notion of the *center* of a group, which is a special case of the centralizer. Formally:

Definition 95 (Center)**.** Let G be a group. The *center* of G is the set $Z(G) = \{g \in G : gx = xg, \text{ for all } x \in G\}$. That is, the center is the set of elements in G which commute with every element in G.

Remark: Observe that $Z(G) = C_G(G)$, so $Z(G) \leq G$. We also clearly have:

$$Z(G) = \bigcap_{g \in G} C_G(g)$$

The next subgroup we introduce is the normalizer, which is a generalization of the centralizer. Intuitively, the centralizer is the set of elements that commute with a non-empty $A \subset G$. However, the normalizer simply preserves the set A under this notion of conjugation. That is, if g is in the normalizer of A, then $x \in A$, there exists a $y \in A$ such that $gx = yg$. So the elements of A may map to each other rather than preserved by commutativity. Formally:

Definition 96 (Normalizer)**.** Let G be a group, and let $A \subset G$. The *normalizer* of A with respect to G is the set $N_G(A) = \{g \in G : gAg^{-1} = A\}$.

Clearly, $C_G(A) \leq N_G(A)$ for any non-empty $A \subset G$. We now compute the centralizer, center, and normalizer for D_8.

Example 97. If G is Abelian, $Z(G) = C_G(A) = N_G(A) = G$ for any non-empty $A \subset G$.

Example 98. Let $G = D_8$ and let $A = \langle r \rangle$. Clearly, $A \leq C_G(A)$. As $sr = r^{-1}s \neq rs$, $s \notin C_G(A)$. Now suppose some $sr^i \in C_G(A)$. Then $sr^i r^{-i} = s \in C_G(A)$, a contradiction. So $C_G(A) = A$.

Example 99. $N_{D_8}(\langle r \rangle) = D_8$. We consider:

$$s\langle r \rangle s = \{s1s, srs, sr^2s, sr^3s\} = \{1, r^{-1}, r^2, r^{-3}\}$$

As $N_{D_8}(\langle r \rangle)$ is a group, s is multiplied by each rotation. So we obtain $N_{D_8}(\langle r \rangle) = D_8$.

Example 100. $Z(D_8) = \{1, r^2\}$. As $Z(D_8) \leq C_{D_8}(\langle r \rangle)$, it suffices to show r and r^3 do not commute with some element of D_8. We have $rs = sr^{-1}$ by the presentation of D_8. Similarly, $r^3 s = sr^{-3}$. So $Z(D_8) = \{1, r^2\}$.

We next introduce the stabilizer of a group action, which is a special subgroup which contains elements of G that fix a specific element $a \in A$.

Definition 97 (Stabilizer)**.** Let G act on the set A. For each $a \in A$, the stabilizer $G_a = \{g \in G : g \cdot a = a\}$.

Remark: Clearly, the Kernel of the action is simply: $\bigcap_{a \in A} G_a$, which contains the set of all group elements g that fix every point in A.

We defined the kernel in the previous section on group actions. More generally, we define the kernel of a homomorphism as follows:

Definition 98 (Kernel of a Homomorhism)**.** Let $\phi : G \to H$ be a group homomorphism. We denote the *kernel* of the homomorphism ϕ as $\ker(\phi) = \phi^{-1}(1_H)$, or the set of elements in G which map to 1_H under ϕ.

Remark: Recall that the Kernel of a group action is the set of group elements which fix every element of A. We equivalently define the Kernel of a group action as $\ker(\phi) = \phi^{-1}((1))$, where $\phi : G \to S_A$ is the homomorphism defined in Cayley's theorem sending $g \mapsto \sigma_g$, a permutation. Both the Kernel and the Stabilizers are subgroups of G.

We now explore the relation between normalizers, centralizers, and centers, and the kernels and stabliziers of group actions. In particular, normalizers, and centers of groups are stabilizers of group actions. We begin with the action of conjugation.

Definition 99 (Action of Conjugation)**.** Let G be a group, and let A be a set. G acts on A by conjugation, by mapping $(g, a) \in G \times A$ to gag^{-1}.

Proposition 3.8. *Suppose G acts on 2^G by conjugation. Then $N_G(A) = G_A$, the stabilizer of A.*

Proof. Let $A \in 2^G$. Let $g \in G_A$. Then $gAg^{-1} = A$, so $g \in N_G(A)$ and $G_A \subset N_G(A)$. Conversely, let $h \in N_G(A)$. By definition of the normalizer, $hAh^{-1} = A$, so h fixes A. Thus, $h \in G_A$ and $N_G(A) \subset G_A$. □

Remark: It follows that the kernel of the action of G on 2^G by conjugation is $\bigcap_{A \subset G} N_G(A)$.

By similar analysis, we consider the action of $N_G(A)$ on the set A by conjugation. So for $g \in G$, we have:

$$g : a \mapsto gag^{-1}$$

By definition of $N_G(A)$, this maps $A \to A$. We observe that $C_G(A)$ is the kernel of this action. It follows from this that $C_G(A) \leq N_G(A)$. A little less obvious is that $Z(G)$ is the kernel of G acting on itself by conjugation.

Proposition 3.9. *Let G act on itself by conjugation. The kernel of this action Ker $= Z(G)$.*

Proof. Let $g \in$ Ker, and let $h \in G$. Then $ghg^{-1} = h$ by definition of the Kernel. So $gh = hg$, and $g \in Z(G)$. So Ker $\subset Z(G)$. Conversely, let $x \in Z(G)$. Then $xh = hx$ for all $h \in G$. So $xhx^{-1} = h$ for all $x \in$ Ker and $Z(G) \subset$ Ker. □

3.2.1 Cyclic Groups

In this section, we study cyclic groups, which are generated by a single element. The results in this section are number theoretic in nature. There is relatively little meat in this section, but the results are quite important for later. So it is important to spell out certain details. We begin with the definition of a cyclic group below.

Definition 100 (Cyclic Group)**.** A group G is said to be cyclic if $G = \langle x \rangle = \{x^n : n \in \mathbb{Z}\}$ for some $x \in G$.

Remark: As the elements of G are of the form x^n, associativity, closure under multiplication, and closure under inverses follows immediately. We have that $x^0 = 1$, so $G = \langle x \rangle$ is a group.

Recall from Section 3.1 that the order of an element x in a group is the least positive integer n such that $x^n = 1$. Equivocally, $|x| = |\langle x \rangle|$. We formalize this as follows.

Proposition 3.10. *If $H = \langle x \rangle$, then $|H| = |x|$. More specificially:*

1. *If $|H| = n < \infty$, then $x^n = 1$ and $1, x, \ldots, x^{n-1}$ are all distinct elements of H; and*
2. *If $|H| = \infty$, then $x^n \neq 1$ for all $n \neq 0$; and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$.*

Proof. Let $|x| = n$. We consider first when $n < \infty$. Let $a, b \in \{0, \ldots, n-1\}$ be distinct such that $x^a = x^b$. Then $x^{b-a} = x^0 = 1$, contradicting the fact that n is the minimum integer such that $x^n = 1$. So all the elements of $1, x, \ldots, x^{n-1}$ are unique. It suffices to show that $H = \{1, x, \ldots, x^{n-1}\}$. Consider x^t. By the Division Algorithm, $x^t = x^{nq+k}$ for some $q \in \mathbb{Z}$ and $k \in \{0, \ldots, n-1\}$. Then $x^t = (x^n)^q x^k = 1^q x^k = x^k \in \{1, \ldots, x^{n-1}\}$. So $|H| = |x|$.

Now suppose $|x| = \infty$. So no positive power of x is the identity. Now suppose $x^a = x^b$ for distinct integers a, b. Clearly, $x^{a-b} \neq x^0 = 1$; otherwise, we have a positive integer such that $x^n = 1$, a contradiction. So distinct powers of x are distinct elements of H, and we have $|H| = \infty$. □

Remark: Proposition 3.10 allows us to reduce powers of x based on their congruence classes modulo $|x|$. In particular, $\langle x \rangle \cong \mathbb{Z}_n$ when $|x| = n < \infty$. If $n = \infty$, then $\langle x \rangle \cong \mathbb{Z}$. In order to show this, we need a helpful lemma.

Proposition 3.11. *Let G be a group, and let $x \in G$. Suppose $x^m = x^n = 1$ for some $m, n \in \mathbb{Z}^+$. Then for $d = gcd(m, n)$, $x^d = 1$. In particuar, if $x^m = 1$ for some $m \in \mathbb{Z}$, then $|x|$ divides m.*

Proof. By the Euclidean Algorithm, we write $d = mr + ns$, for appropriately chosen integers r, s. So $x^d = x^{mr+ns} = (x^m)^r \cdot (x^n)^s = 1$.

We now show that if $x^m = 1$, then $|x|$ divides m. If $m = 0$, then we are done. Now suppose $m \neq 0$. Let $d = \gcd(m, |x|)$. So $x^d = 1$. As $d \in [|x|]$ and $|x|$ is the least such positive integer that $x^m = 1$, it follows that $d = |x|$ and $|x|$ divides m. □

We now show that every cyclic group is isomorphic to either the integers or the integers modulo n, for some n. We first introduce the notion of a well-defined function, which we need for this next theorem.

Definition 101 (Well-Defined Function)**.** A map $\phi : X \to Y$ is well-defined if for every x, there exists a unique y such that $x \mapsto y$. Furthermore, if X is a set of equivalence classes, then for any two a, b in the same equivalence class, $\phi(a) = \phi(b)$.

Theorem 3.13. *Any two cyclic groups of the same order are isomorphic. In particular:*

1. *If $|\langle x \rangle| = |\langle y \rangle| = n < \infty$, then the map: $\phi : \langle x \rangle \to \langle y \rangle$ sending $x^k \mapsto y^k$ is a well-defined isomorphism.*
2. *If $\langle x \rangle$ has infinite order, then the map $\psi : \mathbb{Z} \to \langle x \rangle$ sending $k \mapsto x^k$ is a well-defined isomorphism.*

Proof. Let $\langle x \rangle, \langle y \rangle$ be cyclic groups of finite order n. We show that $x^k \mapsto y^k$ is a well-defined isomorphism. Let r, s be distinct positive integers such that $x^r = x^s$. In order for ϕ to be well-defined, it is necessary that $\phi(x^r) = \phi(x^s)$. As $x^{r-s} = 1$, we have by proposition 3.11 that n divides $r - s$. So $x^r = tn + s$. So:

$$\phi(x^r) = \phi(x^{tn+s}) \tag{35}$$
$$= y^{tn+s} \tag{36}$$
$$= (y^n)^t y^s \tag{37}$$
$$= y^s = \phi(x^s) \tag{38}$$

So ϕ is well-defined. By the laws of exponents, we have $\phi(x^a x^b) = y^{ab} = y^a y^b = \phi(x^a)\phi(x^b)$. So ϕ is a homomorphism. It follows that since y^k is the image of x^k under ϕ, that ϕ is surjective. As $|\langle x \rangle| = |\langle y \rangle| = n$, ϕ is injective. So ϕ is a homomorphism.

Now suppose $\langle x \rangle$ is infinite. We have from Proposition 3.10 that for any two distinct integers a, b that $x^a \neq x^b$. So ψ is well-defined and injective. It follows immediately from the rules of exponents that ψ is a homomorphism. It suffices to show ψ is surjective. Let $h \in \langle x \rangle$. Then $h = x^k$ for some $k \in \mathbb{Z}$. So k is the preimage of h under ψ, and we have ψ is surjective. So ψ is an isomorphism. □

We conclude this section with some additional results that are straight-forward to prove. This first proposition provides results for selecting generators of a cyclic group.

Proposition 3.12. *Let $H = \langle x \rangle$. If $|x| = \infty$, then $H = \langle x^a \rangle$ if and only if $a = \pm 1$. If $|x| = n < \infty$, then $H = \langle x^a \rangle$ if and only if $gcd(a, n) = 1$.*

Proof. Suppose that $|H| = \infty$. If $a = \pm 1$, then $H = \langle x^a \rangle$. Conversely, let $a \in \mathbb{Z}$ such that $H = \langle x^a \rangle$. If $a = \pm 1$, then we are done. So suppose to the contrary that there a is an integer other than ± 1 such that $H = \langle x^a \rangle$. Without loss of generality, suppose $a > 0$. Let $b \in \{-a+1, \ldots, -1, 1, \ldots, a-1\}$. No such integer k exists such that $ak = b$. So it is necessary that $a = \pm 1$.

We now consider the case in which $|H| = n < \infty$. We have $H = \langle x^a \rangle$ if and only if $|x^a| = |x|$. This occurs if and only if $|x^a| = \dfrac{n}{\gcd(n, a)} = n$, which is equivalent to $\gcd(a, n) = 1$. The Euler ϕ function counts the number of integers relatively prime to the input, so there are $\phi(n)$ members of H which individually generate H. □

We conclude this section with the following result.

Theorem 3.14. *Let $G = \langle x \rangle$. Then every subgroup of G is also cyclic.*

Proof. Let $H \leq G$. If $H = \{1\}$, we are done. Suppose $H \neq \{1\}$. Then there exists an element $x^a \in H$ where $a > 0$ (if we selected x^a with $a < 0$, then we obtain $x^{-a} \in H$ as H is closed under inverses, and so $-a > 0$). By Well-Ordering, there exists a least positive b such that $x^b \in H$. Clearly, $\langle x^b \rangle \leq H$. Now let $x^a \in H$. Then by the Division Algorithm, $x^a = x^{kb+r}$ for $k \in \mathbb{Z}$ and $0 \leq r < b$. So $x^r = x^a (x^b)^{-k}$. As $x^a, x^b \in H$, so is x^r. But since b is the least positive integer such that $x^b \in H$, then $r = 0$. So $H \leq \langle b \rangle$, and H is cyclic. □

3.2.2 Subgroups Generated By Subsets of a Group

In this section, we generalize the notion of a cyclic group. A cyclic group is generated by a single element. We examine subgroups which are generated by one or more elements of the group, rather than just a single element. The important result in this section is tht subgroups of a group G are closed under intersection.

Theorem 3.15. *Let G be a group, and let $\mathcal{A}$ be a collection of subgroups of G. Then the intersection of all the members of $\mathcal{A}$ is also a subgroup of G.*

Proof. We appeal to the subgroup criterion. Let:

$$K = \bigcap_{H \in \mathcal{A}} H$$

As each $H \in \mathcal{A}$ is a subgroup of G, $1 \in H$ for each $H \in \mathcal{A}$. So $1_H \in K$ and we have $K \neq \emptyset$. Now let x, y. As $x, y \in H$ for each $H \in \mathcal{A}$, we have xy^{-1} also in each $H \in \mathcal{A}$. So $xy^{-1} \in K$ and we are done. So $K \leq G$. □

We now examine precisely the construction of the subgroup generated by a set $A \subset G$. Formally, we have the proposition:

Proposition 3.13. *Let $A \subset G$. Then:*

$$\langle A \rangle = \bigcap_{A \subset H, H \leq G} H$$

Proof. Let $\mathcal{A} = \{H \leq G : A \subset H\}$. As $\langle A \rangle \in \mathcal{A}$, $\mathcal{A} \neq \emptyset$. Let

$$K = \bigcap_{H \in \mathcal{A}} H$$

Clearly, $A \subset K$. Since $K \leq G$ by Theorem 3.15, $\langle A \rangle \leq K$. As $\langle A \rangle$ is the unique minimal subgroup of G containing A, it follows that $\langle A \rangle \in \mathcal{A}$ and $K \leq \langle A \rangle$. □

3.2.3 Subgroup Poset and Lattice (Hasse) Diagram

The goal of this section is to provide another visual tool for studying the structure of the graph. While the Cayley Graph describes the intuitive notion of spanning of a subset of a group, the lattice (or Hasse) diagram depicts the subgroup relation using a directed graph. The lattice diagram and associated structure known as a poset are quite useful in studying the structure of a group. In the section on quotients, we see immediate benefit when studying the Fourth (or Lattice) Isomorphism Theorem. We begin with the definition of a poset.

Definition 102 (Partially Ordered Set (Poset))**.** A *partially ordered set* or *poset* is a pair $(S, \leq)$, where S is a set and $\leq$ is a binary relation on S satisfying the following properties:

- Reflexivity: $a \leq a$ for all $a \in S$.
- Anti-Symmetry: $a \leq b$ and $b \leq a$ implies that $a = b$.
- Transitivity: $a \leq b$ and $b \leq c$ implies that $a \leq c$.

Intuitively, a partial order behaves like the natural ordering on $\mathbb{Z}$. Consider $3, 4, 5 \in \mathbb{Z}$. We have $3 \leq 3$. More generally, $a \leq a$ for any $a \in \mathbb{Z}$. So reflexivity holds. Transitivity similarly holds, as is illustrated with the example that $3 \leq 4$ and $4 \leq 5$. We have $3 \leq 5$ as well. Anti-symmetry holds as well. We now consider some other examples of posets.

Example 101. The set of $\mathbb{Z}$ with the relation of divisibility forms a poset. Recall the divisibility relation $a \big| b$ if there exists an integer q such that $aq = b$.

Example 102. The Big-O relation is a partial order over the set of functions $\{f : \mathbb{N} \to \mathbb{N}\}$.

Example 103. Let S be a set. The subset relation $\subset$ is a partial order over 2^S.

Example 104. Let G be a group. Let $\mathcal{G} = \{H \leq G\}$. The subgroup relation forms a partial order over $\mathcal{G}$.

We now describe how to construct the Hasse Diagram for a poset. The vertices of the Hasse diagram are the elements of the poset S. There is a directed edge (i, j) if $i \leq j$ and there is no other element k such $i \leq k$ and $k \leq j$. In the poset of subgroups, the trivial subgroup $\{1\}$ is at the root of the Hasse diagram and the group G is at the top of the diagram. Careful placement of the elements of the poset can yield a simple and useful pictoral representation of the structure. A directed path along the Hasse diagram provides information on the transitivity relation. That is, the directed path H, J, K, M indicates that $H \leq J$, $J \leq K$, and $K \leq M$. So H is also a subgroup of K and M; and J is also a subgroup of M.

Let H, K be subgroups of G. We leverage the Hasse Diagram to find $H \cap K$. Additionally, the Hasse Diagram allows us to ascertain the *join* of H and K, denoted $\langle H, K \rangle$, which is the smallest possible subgroup containing H and K. Note that the elements of H and K are multiplied together. So $H \cup K$ is not necessarily the same set as $\langle H, K \rangle$. In fact, $H \cup K$ may not even form a group.

In order to find $H \cap K$, we find H and K in the Hasse Diagram. Then we enumerate all paths from 1 to H, as well as all paths from $1 \to K$. We examine all subgroups M that lie on some $1 \to H$ path and some $1 \to K$ path. The intersection $H \cap K$ is the subgroup M closest to both H and K. Similarly, if we start at H and K and enumerate the paths to G on the Hasse Diagram, the closest reachable subgroup from H and K is $\langle H, K \rangle$.

Ultimately, we are seeking to leverage visual intuition. We consider Hasse diagrams for $\mathbb{Z}_8$. Observe that the cyclic subgroups generated by $\overline{2}$ and $\overline{4}$ are isomorphic to $\mathbb{Z}_4$ and $\mathbb{Z}_2$ respectively. Here, the trivial subgroup $\{\overline{0}\}$ is at the bottom of the lattice diagram and is contained in each of the succeeding subgroups. We then see that $\langle \overline{4} \rangle \leq \langle \overline{2} \rangle$, and in turn that each of these are subgroups of $\mathbb{Z}_8$. If we consider the sublattice from $\{\overline{0}\}$ to $\langle \overline{2} \rangle$, then we have the lattice for $\mathbb{Z}_4$.

Example 105.

$$\begin{array}{c} \mathbb{Z}_8 = \langle \overline{1} \rangle \\ | \\ \langle \overline{2} \rangle \cong \mathbb{Z}_4 \\ | \\ \langle \overline{4} \rangle \cong \mathbb{Z}_2 \\ | \\ \langle \overline{8} \rangle = \{\overline{0}\} \end{array}$$

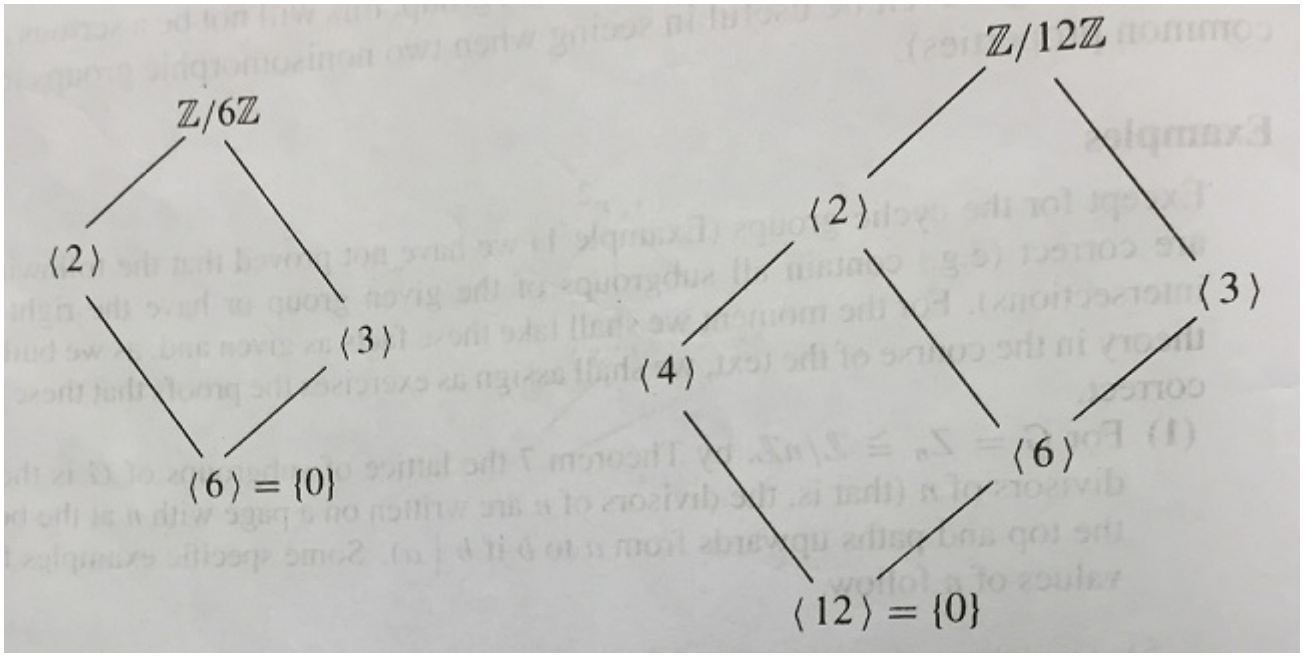
In particular, if p is prime, we see the lattice diagram of $\mathbb{Z}_{p^n}$ is:

Example 106.

$$\begin{array}{c} \mathbb{Z}_{p^n} = \langle \overline{1} \rangle \\ | \\ \langle \overline{p} \rangle \\ | \\ \langle \overline{p^2} \rangle \\ | \\ \langle \overline{p^3} \rangle \\ | \\ \vdots \\ | \\ \langle p^{n-1} \rangle \\ | \\ \{\overline{0}\} \end{array}$$

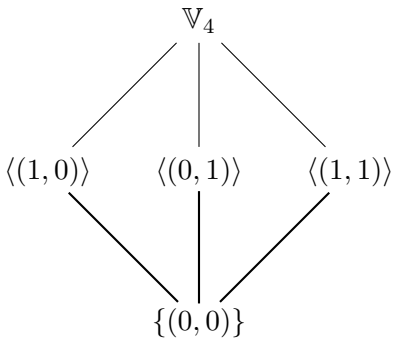
We now examine the Hasse diagrams of $\mathbb{Z}_6$ and $\mathbb{Z}_{12}$. Observe that in the lattice diagram of $\mathbb{Z}_{12}$, we have $\langle \overline{2} \rangle \cong \mathbb{Z}_6$. Similarly, $\langle \overline{4} \rangle$ in the lattice of $\mathbb{Z}_{12}$ corresponds to $\langle \overline{2} \rangle$ in the lattice of $\mathbb{Z}_6$. Following this pattern, we observe that the lattice of $\mathbb{Z}_6$ can be extracted from the lattice of $\mathbb{Z}_{12}$.

Example 107.



The next group we examine is the Klein group of order 4 (Viergruppe), which is denoted $\mathbb{V}_4$. Formally, $\mathbb{V}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. So there are three subgroups of order 2 and the trivial subgroup as the precise subgroups of $\mathbb{V}_4$. This yields the lattice:

Example 108.

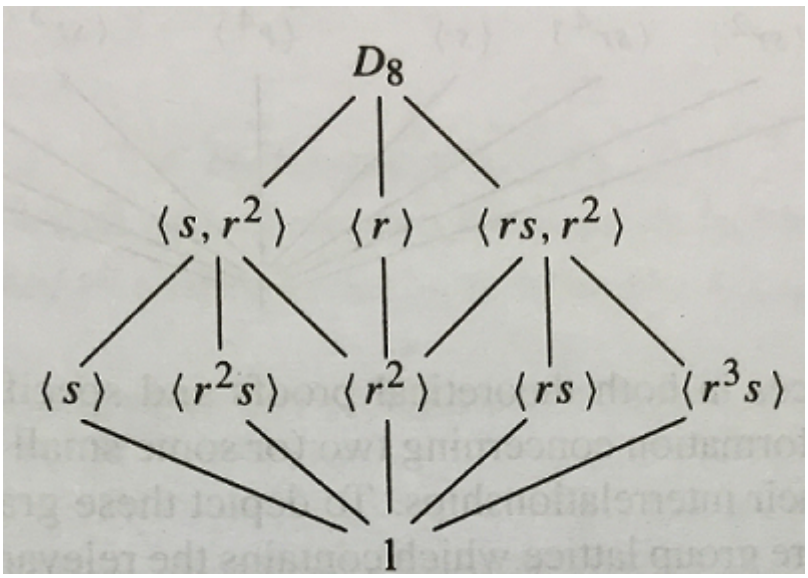


In fact, the two distinct groups of order 4 are $\mathbb{Z}_4$ and $\mathbb{V}_4$. It is easy to see that $\mathbb{V}_4 \ncong \mathbb{Z}_4$ by examining their lattices. It is not true in general that two groups with the same lattice structure are isomorphic. We will also see that $\mathbb{V}_4$ is isomorphic to a subgroup of D_8, and we will leverage the lattice of D_8 to obtain this result.

We now construct the lattice of D_8. Recall that Lagrange's Theorem states that if G is a finite group and $H \leq G$, then $|H|$ divides $|G|$. In $\mathbb{Z}_n$, we see that if q divides n, then $\mathbb{Z}_q \leq \mathbb{Z}_n$. In general, the converse of Lagrange's Theorem is not true. Furthermore, there could be many subgroups of a given order. In D_8, we have subgroups of order $1, 2$, and 4. We begin by enumerating the subgroups of order 2, then taking their joins to obtain all but one of the subgroups of order 4. The remaining subgroup of order four is $\langle r\rangle$, which only has $\langle r^2\rangle$ as an order 2 subgroup. Then the subgroups of order 4 all have directed edges to D_8 in the lattice. Recall that each reflection, which is of the form sr^i for $i \in \{0, \ldots, 3\}$, has order 2. Similarly, r^2 has order 2 as well. This yields the five subgroups of order 2 which are adjacent to $\{1\}$, the trivial subgroup.

It should be readily apparent that the three subgroups of order 4 specified in the lattice of D_8 below exist. What may not be as obvious is that these are precisely the three subgroups of order 4. There are precisely two distinct groups of order 4: $\mathbb{Z}_4$ and $\mathbb{V}_4$. It is clear that $\langle r\rangle \cong \mathbb{Z}_4$. Now $\mathbb{V}_4$ has three subgroups of order 2. We may check by exhaustion the joins of all $\binom{5}{3} = 10$ sets of three subgroups of order 2. The join of any three subgroups of order two which allows us to isolate r or r^3 results in a generating set for D_8. For example, $\langle r^2s, r^2, rs\rangle$ allows us to isolate r by multiplying $r^2s \cdot rs = r^2ssr^3 = r$. So $\langle r\rangle \leq \langle r^2s, r^2, rs\rangle$. Thus, $\langle r^2s, r^2, rs\rangle = D_8$.

Example 109.



The Hasse diagram, when combined with Lagrange's Theorem, provides a powerful tool to compute the center, normalizers, and centralizers for a given group. As each of these sets are subgroups of G, they are each vertices on the Hasse diagram. So finding a known subgroup of the center, centralizer, or normalizer, we can narrow

down candidates rather quickly. We consider an example.

Example 110. We seek to compute $C_{D_8}(s)$. Recall that $\langle s \rangle \leq C_{D_8}(s)$. Examining the lattice of D_8, our candidates for $C_{D_8}(s)$ are $\langle s, r^2 \rangle$ and D_8. We see that $r^2\langle s \rangle r^2 = \langle s \rangle$. However, $rs \neq sr$, so $C_{D_8}(s) \neq D_8$.

3.3 Quotient Groups

3.3.1 Introduction to Quotients

Recall in the exposition in the preliminaries that an equivalence relation partitions a set. We refer to this partitioning process as a *quotient*, denoted $S/\equiv$, where S is the set and $\equiv$ is the equivalence relation. We pronounce $S/\equiv$ as S modulo $\equiv$. Quotients appear throughout mathematics and theoretical computer science. In automata theory, we study quotient machines and quotient languages, with elegant results such as the Myhill-Nerode Theorem characterizing regular languages using quotients. The Myhill-Nerode theorem also provides an elegant algorithm to compute the quotient and yield a minimum DFA. Section 2.9 of these notes introduces the Myhill-Nerode theorem.

Quotients arise frequently in the study of algebra. In group theory, we study quotients of groups and the conditions upon which the quotient of two groups forms a group itself. In ring theory, we are interested in collapsing the structure to form a field. In fact, we take the ring $\mathbb{R}[x]$ of polynomials with real-valued coefficients and collapse these polynomials modulo $x^2 + 1$ to obtain a field isomorphic to $\mathbb{C}$. Similar constructions produce finite fields of interest in cryptography, such as the Rijndael field used in the AES-Cryptosystem.

In standard algebra texts, the study of group quotients is really restricted to the case when such quotients form a group. Formally, the elements of a group G are partitioned into equivalence classes called *cosets*. In order to partition one group G according to another group H, we use the orbit relation when H acts on G. This yields some interesting combinatorial results, as well as algebraic results in the study of quotient groups. In particular G/H forms a group when H is a *normal subgroup* of G. This means that H is the kernel of some group homomorphism with G in the domain. These ideas culminate to develop the notion of division, which intuitively speaking comes down to placing an equal number of cookies on each plate.

We begin by computing a couple quotients to illustrate the point. Using quotients of groups, we deduce that $P(n,r) = \frac{n!}{(n-r)!}$ is the correct formula for counting r-letter permutations from an n-letter set; and $\binom{n}{k} = \frac{n!}{r!(n-r)!}$ counts the number of k-element subsets from an n-element set. Recall that S_n is the group of all permutations, with order $n!$. In the mathematical preliminaries section, we considered equivalence classes of permutations in S_n according to whether the "first" r characters were the same. Intuitively, only the last r characters matter in a given permutation. Formally, $P(n,r) = |S_n/S_{n-r}|$. The equivalence classes are formalized by letting S_{n-r} act on S_n by postcomposition. So let $\pi \in S_n$ and $\tau \in S_{n-r}$. Then τ sends $\pi \mapsto \tau \circ \pi$. So the action of S_{n-r} on S_n partitions S_n into orbits each of order $(n-r)!$. So we have $P(n,r) = \frac{n!}{(n-r)!}$ orbits.

Example 111. Consider S_5/S_3. We compute the orbit of (13254). We see:

- $(1)(13254) = (13254)$. Combinatorially, this permutation corresponds to the string 43152.
- $(12)(13254) = (13)(254)$. Combinatorially, this permutation corresponds to the string 34152.
- $(13)(13254) = (3254)$. Combinatorially, this permutation corresponds to the string 13452.
- $(23)(13254) = (1254)$. Combinatorially, this permutation corresponds to the string 41352.
- $(123)(13254) = (254)$. Combinatorially, this permutation corresponds to the string 14352.
- $(132)(13254) = (12543)$. Combinatorially, this permutation corresponds to the string 31452.

So $\mathcal{O}((13254)) = \{(13254), (13)(254), (3254), (1254), (254), (12543)\}$.

By similar argument, we let S_r act on the orbits of S_n/S_{n-r} by postcomposition, which permutes the "last" r digits of the string. We note that the permutations in S_r are labeled using the set $[r]$, while the permutations of S_{n-r} are labeled using the digits $\{r+1,\ldots,n\}$. So the action of S_r on S_n/S_{n-r} does not interfere with the action of S_{n-r} on S_n. Formally, the action of S_r on S_n/S_{n-r} partitions the $\frac{n!}{(n-r)!}$ orbits of S_n/S_{n-r} into equivalence classes each of order $r!$. Intuitively, we are combining orbits of S_n/S_{n-r}. So there are $\frac{n!}{r!(n-r)!} = \binom{n}{r}$ subsets of order r from an n-element set.

Example 112. Recall the example of S_5/S_3 above. We let S_2 act on S_5/S_3. So the following permutations belong to the same orbit:

$$\{(13254),(13)(254),(3254),(1254),(254),(12543),(1324),(13)(24),(324),(124),(24),(1243)\}$$

So while the string (13254) corresponds to the string 43152, the permutation (1324) corresponds to the string 43125. So the action of S_2 on the orbits of S_5/S_3 permutes the last two digits of a given string.

3.3.2 Normal Subgroups and Quotient Groups

We transition from talking about quotients of sets modulo equivalence relations to developing some intuition about quotient groups, where G/H forms a group. Intuitively, the study of quotient groups is closely tied to the study of homomorphisms. Recall a group homomorphism is a function $\phi : G \to K$ where G and K are groups. Let $H := \ker(\phi)$. Let $a, b \in K$. Intuitively, in a quotient group, we consider $\phi^{-1}(a)$ equivocal to a and $\phi^{-1}(b)$ equivocal to b. That is, $\phi^{-1}(a)$ behaves in G/H just as a behaves in H. That is, the operation of K provides a natural multiplication operation in G/H where multiply orbits by selecting a representative of each orbit, multiplying the representatives and taking the resultant orbit. Using this intuition, we see that $G/H \cong \phi(G)$, which indicates that in the action of H on G, the orbits of this action can be treated equivalently as the range of ϕ. This result is known as the First Isomorphism Theorem, which we will formally prove. Each orbit corresponds to some non-empty preimage of an element in K. It is common in the study of quotients for the orbits or cosets to be referred to as *fibers*. That is, $\phi^{-1}(a)$ is the *fiber above* $a \in K$.

Now consider a group G acting on a set A. In general, the orbits are not invariant when G acts by left multiplication on A vs. right multiplication. In quotient groups, it does not matter if the action is left multiplication or right multiplication. We formalize this as follows.

Proposition 3.14. *Let $\phi : G \to H$ be a group homomorphism with kernel K. Let $X \in G/K$ be the fiber above a; that is, $X = \phi^{-1}(a)$. Then for any $u \in X$, we have $X = \{uk : k \in K\} = \{ku : k \in K\}$.*

Proof. Let $u \in X$. Define $uK = \{uk : k \in K\}$ and $Ku = \{ku : k \in K\}$. We show $uK \subset X$ first. Let $uk \in uK$. Then $\phi(uk) = \phi(u)\phi(k)$ as ϕ is a homomorphism. As $k \in K$, $\phi(k) = 1_H$. So $\phi(u)\phi(k) = \phi(u) = a$. So $uK \subset X$. We now show that $X \subset uK$. Let $g \in X$ and let $k = u^{-1}g$. Observe that $k \in K$, as $\phi(k) = \phi(u^{-1})\phi(g) = a^{-1} \cdot a = 1_H$. So we have $g = uk \in uK$. So $\phi(g) = a$ and $g \in X$. So $X = uK$.

By similar argument, we deduce that $X = Ku$. The details are left to the reader. □

Remark: As the orbit relation is an equivalence relation, each equivalence class can be described by selecting an arbitrary representative. For any $N \leq G$, $gN = \{gn : n \in N\}$ and $Ng = \{ng : n \in N\}$. We refer to gN as the *left coset* and Ng as the *right coset*. If G is an Abelian group, then we write gN as $g + N$; and Ng as $N + g$. By Proposition 4.1, if N is the kernel of some homomorphism, we have that $gN = Ng$.

The first big result in the study of quotient groups is the First Isomorphism Theorem, which we mentioned above. The important result is that $G/\ker(\phi) \cong \phi(G)$ for a group homomorphism $\phi : G \to H$. It is easy to verify that $\phi(G) \leq H$ using the subgroup criterion- an exercise left for the reader. Showing that $G/\ker(\phi)$ forms a group takes some work. Constructing an isomorphism from $G/\ker(\phi)$ to $\phi(G)$ is relatively straight-forward. The desired isomorphism is rather obvious. However, the devil is in the details. Whenever we deal with functions on cosets, we must show that the desired function is well-defined. That is, the function is determined for all inputs, and that all members of an equivalence class behave in the expected manner. If a and b belong to

the same coset, then it is necessary for a well-defined function f that $f(a) = f(b)$.

We begin by showing $G/\ker(\phi)$ forms a group. We have already discussed the importance of having a well-defined operation. The second part of this proof shows that the desired operation forms a group. A good strategy when dealing with quotient groups is to take elements from the quotient group, work in the parent group, apply the homomorphism, then project back into the quotient group. This is precisely what we do below. Furthermore, we note that the desired isomorphism (sending $X = \phi^{-1}(a) \in G/K$ to $a \in \phi(G)$) to prove the First Isomorphism Theorem follows is contained (though not explicitly mentioned) in the proof of this next result.

Theorem 3.16. *Let $\phi : G \to H$ be a group homomorphism with kernel K. Then the operation on G/K sending $aK \cdot bK = (ab)K$ is well-defined.*

Proof. Let $X, Y \in G/K$ and let $Z = XY \in G/K$. Suppose $X = \phi^{-1}(a)$ and $Y = \phi^{-1}(b)$ for some $a, b \in \phi(G)$. Then by the definition of the operation, $Z = \phi^{-1}(ab)$. Let $u \in X, v \in Y$ be representatives of X and Y respectively. It suffices to show $uv \in Z$. We have $uv \in Z$ if and only if $uv \in \phi^{-1}(ab)$ if and only if $\phi(uv) = ab$. Applying the homomorphism, $\phi(uv) = ab$ is equivalent to $\phi(u)\phi(v) = ab$. Thus, $uv \in Z$, so $Z = abK$. So the operation is well-defined. □

We now have most of the machinery we need to prove the First Isomorphism Theorem. We want a couple more results first, though, to provide more intuition about the structure of a quotient group. First, we show that the cosets or orbits of an action form a partition of the group. Then we formalize the notion of a normal subgroup. The machinery we build up makes the proof of the First Isomorphism Theorem rather trivial. Remember that our goal is to show that the cosets of G/K behave the same way as the elements of $\phi(G)$, for a group homomorphism $\phi : G \to H$.

Proposition 3.15. *Let G be a group, and let $N \leq G$. The set of left cosets in G/N forms a partition of G. Furthermore, for any $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$. In particular, $uN = vN$ if and only if u, v are representatives of the same coset.*

Proof. As $N \leq G$, $1 \in N$. So for all $g \in G$, $g \cdot 1 \in gN$. It follows that:

$$G = \bigcup_{g \in G} gN$$

We now show that any two distinct left-cosets are disjoint. Let $uN, vN \in G/N$ be distinct cosets. Suppose to the contrary that $uN \cap vN \neq \emptyset$. Let $x = un = vm \in uN \cap vN$, with $m, n \in N$. As N is a group, $mn^{-1} \in N$. So for any $t \in N$, $ut = vmn^{-1}t = v(mn^{-1}t) \in vN$. So $u \in vN$ and $uN \subset vN$. Interchanging the roles of u and v, we obtain that $vN \subset uN$ and we have $uN = vN$. It follows that $uN = vN$ if and only if $uv^{-1} \in N$ if and only if u, v are representatives of the same coset. □

Remark: In particular, Proposition 3.15 verifies that the action of N on G by right multiplication (the left-coset relation) forms an equivalence relation on G.

We now introduce the notion of a normal subgroup.

Definition 103 (Normal Subgroup)**.** Let G be a group, and let $N \leq G$. We refer to gng^{-1} as the *conjugate* of n by g. The set $gNg^{-1} = \{gng^{-1} : n \in N\}$ is referred to as the *conjugate* of N by g. The element of $g \in G$ is said to *normalize* N if $gNg^{-1} = N$. N is said to be a *normal subgroup* in G if $gNg^{-1} = N$ for all $g \in G$. We denote N to be a normal subgroup of G as $N \trianglelefteq G$.

Intuitively, it is easy to see why a normal subgroup N is the kernel of some homomorphism ϕ. We let G act on N by conjugation. Then for any $g \in G$ and $n \in N$, we consider gng^{-1} and apply ϕ. As $n \in N = \ker(\phi)$, we have $\phi(gng^{-1}) = \phi(g)\phi(n)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = 1$. We next explore several characterizations of a normal subgroup.

Proposition 3.16. *Let G be a group, and let $N \leq G$. We have the following conditions:*

1. *The operation on the left cosets sending $uN \cdot vN = (uv)N$ is well-defined if and only if $gNg^{-1} \subset N$ for all $g \in G$.*

2. *If the above operation is well-defined, then it makes the set of left-cosets of G/N into a group. The identity of this group is the coset N, and the inverse of gN is $g^{-1}N$.*

Proof. We prove statement (1) first. Suppose the operation is well-defined on G/N. We observe that $g^{-1}N = (nN \cdot g^{-1}N) = (ng^{-1})N$ for any $g \in G$ and $n \in N$. As $N \leq G$, $ng^{-1} \in (ng^{-1})N$. So $g^{-1}n_1 = ng^{-1}$ for some $n_1 \in N$. Thus, $n_1 = gng^{-1}$. As our choice of g and n were arbitrary, we deduce that $gNg^{-1} \subset N$ for all $g \in G$.

Conversely, suppose $gNg^{-1} \subset N$ for all $g \in G$. Let $u, u_1 \in uN$ and $v, v_1 \in vN$. We write $u_1 = un$ and $v_1 = vm$ for some $m, n \in N$. It suffices to show $u_1v_1 \in (uv)N$. Observe that $u_1v_1 = unvm = u(vv^{-1})nvm$. By associativity, we rewrite $uv(v^{-1}nv)m$. As $gNg^{-1} \subset N$ for all g, we have $v^{-1}nv = n_1$ for some $n_1 \in N$. So $(uv)(v^{-1}nv)m = (uv)(n_1m)$. As $N \leq G$, $n_1m \in N$. So $u_1v_1 \in (uv)N$, completing the proof of (1).

We now prove statement (2). Suppose the operation on G/N sending $uN \cdot vN = (uv)N$is well-defined. We show G/N forms a group. Let $uN, vN, wN \in G/N$. Then $(uN \cdot vN) \cdot wN = uvN \cdot wN = uvwN = uN \cdot (vwN) = uN \cdot (vN \cdot wN)$. So G/N is associative. Let $g \in G$. Observe that $1N = N$; and so, $1N \cdot gN = 1gN = gN$; and $gN \cdot 1N = g1N = gN$. So N is the identity. We see immediately that $(gN)^{-1} = g^{-1}N$. So G/N forms a group. □

We next show that normal subgroups are precisely the kernels of group homomorphisms.

Proposition 3.17. *Let G be a group, and let $N \leq G$. We have $N \trianglelefteq G$ if and only if there exists a group H and group homomorphism $\phi : G \to H$ for which N is the kernel.*

Proof. Suppose first N is the kernel of ϕ. Let G act on N by conjugation. Then $\phi(gNg^{-1}) = \phi(g)\phi(N)\phi(g^{-1}) = \phi(g)\phi(g^{-1}) = 1_H$. So $gNg^{-1} \subset G$. Let $g \in G$. The map $\sigma_g : N \to N$ sending $n \mapsto gng^{-1}$ is an injection, as $gn_1g^{-1} = gn_2g^{-1} \implies n_1 = n_2$ by cancellation of the g and g^{-1} terms. Furthermore, the map $gn^{-1}g^{-1}$ is a two-sided inverse of gng^{-1}, so $gNg^{-1} = N$, and we have $N \trianglelefteq G$.

Conversely, suppose $N \trianglelefteq G$. We construct a group homomorphism π for which N is the kernel. By Proposition 3.16, G/N forms a group under the operation sending $uN \cdot vN = (uv)N$. We define the map $\pi : G \to G/N$ sending $g \mapsto gN$. Now let $g, h \in G$. So $\pi(gh) = (gh)N$. By the operation in G/N, $(gh)N = gN \cdot hN = \pi(g)\pi(h)$. So π is a homomorphism. We have $\ker(\pi) = \{g \in G : \pi(g) = 1N\} = \{g \in G : gN = 1N\}$. As $1N = N$, $\ker(\pi) = \{g \in G : gN = N\} = N$. □

We summarize our characterizations of normal subgroups with the next theorem. We have proven most of these equivalences above. The rest are left as exercises for the reader.

Theorem 3.17. *Let G be a group, and let $N \leq G$. The following are equivalent.*

1. *$N \trianglelefteq G$.*

2. *$N_G(N) = G$.*

3. *$gN = Ng$ for all $g \in G$.*

4. *The operation on the left cosets described in Theorem 3.16 forms a group.*

5. *$gNg^{-1} \subset N$ for all $g \in G$.*

6. *N is the kernel of some group homomorphism $\phi : G \to H$.*

We conclude with the First Isomorphism Theorem.

Theorem 3.18 (First Isomorphism Theorem)**.** *Let $\phi : G \to H$ be a group homomorphism. Then $ker(\phi) \trianglelefteq G$ and $G/ker(\phi) \cong \phi(G)$.*

Proof. By Proposition 3.17, we have $\ker(\phi) \trianglelefteq G$. Let $N := \ker(\phi)$. By Proposition 3.16, G/N forms a group. We construct an isomorphism $\pi : G/N \to \phi(G)$ sending $gN \mapsto \phi(g)$. We first show this map is well-defined. Let $g, h \in gN$. As $gN = \phi^{-1}(a)$ for some $a \in H$, we have $\phi(gN) = \phi(g)\phi(N) = a$, as $\phi(g) = a$ and $\phi(N) = 1$. By similar argument, $\phi(hN) = a$. So π is well-defined.

We now show π is an isomorphism. As $G/N = \{\phi^{-1}(a) : a \in \phi(G)\}$, π is surjective. Now suppose $\pi(gN) = \pi(hN) = a$. Then $gN = hN = \phi^{-1}(a)$ and π is injective. Finally, consider $\pi(gN \cdot hN) = \phi(gN \cdot hN)$. As ϕ is a homomorphism, $\phi(gN \cdot hN) = \phi(gN)\phi(hN) = \pi(gN) \cdot \pi(hN)$. So π is a homomorphism. Therefore, π is an isomorphism. □

3.3.3 More on Cosets and Lagrange's Theorem

In this section, we explore some applications of Lagrange's Theorem. In particular, we are able to quickly determine the number of cosets in a quotient, when it is finite. We then examine more subtle results concerning quotients of groups G/H where H is not normal in G. We recall the statement of Lagrange's Theorem below.

Theorem 3.19 (Lagrange's Theorem)**.** *Let G be a finite group, and let $H \leq G$. Then $|H|$ divides $|G|$.*

The proof of Lagrange's Theorem was relegated to a homework assignment. Intuitively, the proof is analogous to the proof of Fermat's Little Theorem. We let H act on G by left multiplication, which partitions the elements of G into orbits of order $|H|$. So $|H|$ divides $|G|$, and we have $\dfrac{|G|}{|H|}$ orbits in G/H. In fact, Lagrange's Theorem implies Fermat's Little Theorem.

Theorem 3.20 (Fermat's Little Theorem)**.** *Let p be prime and let $a \in [p-1]$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. There are $p-1$ elements in the multiplicative group $\mathbb{Z}_p^\times$. By Lagrange's Theorem, $|\overline{a}| = |\langle \overline{a} \rangle|$ divides $p-1$ for every $\overline{a} \in \mathbb{Z}_p^\times$. Let $|\overline{a}| = q$, and $p - 1 = kq$. Then $|\overline{a}|^{p-1} = |\overline{a}^q|^k = \overline{1}^k = \overline{1}$. So $a^{p-1} \equiv 1 \pmod{p}$. □

Remark: More generally, in $\mathbb{Z}_n$ where n is not necessarily prime, $|\mathbb{Z}_n^\times| = \phi(n)$, where ϕ is Euler's totient function. Note that $\phi(n) = |\{a : a \in [n-1], \gcd(a, n) = 1\}|$. The Euler-Fermat Theorem states that $a^{\phi(n)} \equiv 1 \pmod{n}$. So the Euler-Fermat Theorem generalizes and implies Fermat's Little Theorem. The proof is identical to Fermat's Little Theorem, substituting $p-1$ for $\phi(n)$. Note that if for any prime p, $\phi(p) = p - 1$.

We introduce formal notion for the order of a quotient of groups G/H. Note that we do not assume G/H forms a group.

Definition 104 (Index)**.** Let G be a group, and let $H \leq G$. The *index* of H in G, denoted $[G : H]$ is the number of left cosets in G/H. If G and H are finite, $[G : H] = \dfrac{|G|}{|H|}$. If G is infinite, then $\frac{|G|}{|H|}$ does not make sense. However, an infinite group may have a subgroup of finite index. For example, $[\mathbb{Z} : \{0\}] = \infty$ but $[\mathbb{Z} : \langle n \rangle] = n$ for every integer $n > 0$.

We now derive a couple easy consequences of Lagrange's Theorem.

Proposition 3.18. *Let G be a finite group, and let $x \in G$. Then $|x|$ divides $|G|$. Furthermore, $x^{|G|} = 1$ for all $x \in G$.*

Proof. Recall that $|x| = |\langle x \rangle|$. So by Lagrange's Theorem, $|x|$ divides $|G|$. Let $|x| = k$ and $|G| = kq$, for some integer q. Then $x^{|G|} = (|x|^k)^q = 1^q = 1$. □

Proposition 3.19. *If G is a group of prime order p, then $G \cong \mathbb{Z}_p$.*

Proof. Let $H \leq G$. By Lagrange's Theorem, $|H| = 1$ or $|H| = p$. As the identity is the unique element of order 1 and $p > 1$, there exists an element x of order p in G. So $G = \langle x \rangle \cong \mathbb{Z}_p$. □

The converse of Lagrange's Theorem states that if G is a finite group and k divides $|G|$, then G contains a subgroup of order k. In general, the full converse of Lagrange's Theorem does not hold. In particular, $A_4 \leq S_4$, the group of permutations of even order, has no subgroup of order 3 while $|A_4| = 12$. However, Cauchy's Theorem provides a nice partial converse: for every prime divisor p of $|G|$, where G is a finite group, there exists a subgroup of order p in G. Algebra texts introduce Cauchy's Theorem and prove it by induction for Abelian groups. This restricted case is then used to prove the Sylow theorems, which allow us to leverage combinatorial techniques to study the structure of finite groups. The Sylow theorems are then used to prove Cauchy's Theorem in its full generality. We offer an alternative and far more elegant proof of Cauchy's Theorem, which is accredited to James H. McKay. In his proof, McKay uses group actions and combinatorial techniques to prove Cauchy's Theorem, which resembles the necklace-counting (group action) proof of Fermat's Little Theorem we offered in these notes as well as the proof of Lagrange's Theorem relegated to the homework.

Theorem 3.21 (Cauchy's Theorem)**.** *Let G be a finite group, and let p be a prime divisor of $|G|$. Then G contains a subgroup of order p.*

Proof. Let:

$$\mathcal{G} = \{(x_1, \ldots, x_p) \in G^p : \prod_{i=1}^{p} x_i = 1\}.$$

The first $p-1$ elements of any tuple in $\mathcal{G}$ may be chosen freely from G. This fixes:

$$x_p = (\prod_{i=1}^{p-1} x_i)^{-1}$$

By rule of product, $|\mathcal{G}| = |G|^{p-1}$. As $\prod_{i=1}^{j} x_i$ and $\prod_{i=j+1}^{p} x_i$ are inverses for any $j \in [p]$, $\mathcal{G}$ is closed under cyclic rotations. Let $\mathbb{Z}_p \cong \langle (1, 2, \ldots, p) \rangle \leq S_p$ act on $\mathcal{G}$ by cyclic rotation. Each orbit has order 1 or order p, as p is prime. We have $|\mathcal{G}| = |G|^{p-1} = k + pd$, where k is the number of orbits of order 1 and d is the number of orbits of order p. As p divides $|G|$, p also divides $|G|^{p-1}$. Clearly, p divides pd, so p must divide k. The tuple consisting of all 1's is in $\mathcal{G}$, so $k > 0$. As $p > 1$ and since p divides k, there must exist a tuple in $\mathcal{G}$ consisting of all x terms for some $x \in G$. So $x^p = 1$ and we have a subgroup of order p in G. □

We conclude by examining another method for constructing subgroups: the concatenation of two subgroups. Recall that we can form subgroups by taking joins, intersections, and under certain conditions quotients of groups. Recall that the concatenation of two sets H and K is the set $HK = \{hk : h \in H, k \in K\}$. When H and K are subgroups of a group G, we evaluate each hk term using the group operation of G and retain the distinct elements. The question arises of when $HK \leq G$. This occurs precisely when $HK = KH$. So it suffices that either $H \trianglelefteq G$ or $K \trianglelefteq G$. However, we can relax this condition. It really suffices that $H \leq N_G(K)$. We begin by determining $|HK|$ in the finite case, using a bijective argument. When HK/K and $H/(H \cap K)$ form groups, the bijection we construct.

Proposition 3.20. *Let G be a group, and let $H, K \leq G$ be finite. Then: $|HK| = \dfrac{|H| \cdot |K|}{|H \cap K|}$.*

Proof. We define $f : H \times K \to HK$ sending $f(h, k) = hk$. Clearly, $|H \times K| = |H| \cdot |K|$. So it suffices to show there exist exactly $H \cap K$ preimages.

Observe that f is surjective, so $f^{-1}(hk) \neq \emptyset$ for all $hk \in HK$. Let $S = \{f^{-1}(hk) : hk \in HK\}$. As f is surjective, $|S| = |HK|$. We define a map $\phi : S \to H/(H \cap K)$ sending $f^{-1}(hk) \mapsto h(H \cap K)$. It suffices to show ϕ is a bijection. Clearly, ϕ is surjective. We now show that ϕ is injective. Suppose $f^{-1}(hk) \neq f^{-1}(h1k_1)$.

Then for every $g \in H \cap K$, $h \neq h_1 g$. So $h(H \cap K) \neq h_1(H \cap K)$, and ϕ is injective. So ϕ is a bijection and the result follows. $\square$

Remark: Let $G = S_3$, $H = \langle (1,2) \rangle$, and $K = \langle (1,3) \rangle$. Then $|H| = |K| = 2$ and $|H \cap K| = 1$. However, by Lagrange's Theorem, $HK \not\leq G$ as $|HK| = 4$, which does not divide $|S_3| = 6$. It follows that $S_3 = \langle (1,2), (1,3) \rangle$. Observe as well that when $HK \leq G$, f is a homomorphism with kernel $H \cap K$. In this case, the First Isomorphism Theorem implies the desired result. The bijective proof presented here provides only the desired combinatorial result.

We now examine conditions in which $HK \leq G$. Observe that:

$$HK = \bigcup_{h \in H} hK$$

In order for a set of cosets to form a group, it is sufficient and necessary that $hK = Kh$ for all $h \in H$. So it stands to reason that $HK = KH$ needs to hold. Another way to see this is that if $hk \in HK$, we need $(hk)^{-1} = k^{-1}h^{-1} \in HK$ as well. Observe that $k^{-1}h^{-1} \in KH$. So if $HK = KH$, then $k^{-1}h^{-1} \in HK$ and we have closure under inverses. We formalize this result below.

Proposition 3.21. *Let G be a group, and let $H, K \leq G$. We have $HK \leq G$ if and only if $HK = KH$.*

Proof. Suppose first $HK = KH$. We show $HK \leq G$. As $H, K \leq G$, we have $1 \in HK$. So $HK \neq \emptyset$. Now let $a, b \in HK$ where $a = h_1 k_1$ and $b = h_2 k_2$, $h_1, h_2 \in H$ and $k_1, k_2 \in K$. As $HK = KH$, $k_2 h_2 \in HK$. As H and K are groups, $k_2^{-1} h_2^{-1} \in HK$. In order for $ab^{-1} \in HK$, we need $h_1 k_1 k_2^{-1} h_2^{-1} \in HK$. As $HK = KH$, there exist $k_3 \in K$ and $h_3 \in H$ such that $h_3 k_3 = k_1 k_2^{-1} h_2$. So $h_1 k_1 k_2^{-1} h_2^{-1} = h_1 h_3 k_3 \in HK$ and $HK \leq G$.

Conversely, suppose $HK \leq G$. As H and K are subgroups of HK, we have $KH \subset HK$. In order to show $HK \subset KH$, it suffices to show that for every $hk \in HK$, $(hk)^{-1} \in KH$ (as groups are closed under inverses). Let $hk \in HK$. As HK is a group, $(hk)^{-1} = k^{-1}h^{-1} \in HK$. By definition of KH, we also have that $k^{-1}h^{-1} \in KH$. So $HK \subset KH$, and we conclude that $HK = KH$. $\square$

Remark: Note that $HK = KH$ does not imply that the elements of HK commute. Rather, for every $hk \in HK$, there exists a $k'h' \in KH$ such that $hk = k'h'$. For example, let $H = \langle r \rangle$ and $K = \langle s \rangle$. Then $D_{2n} = HK = KH$, but $sr = rs^{-1}$.

We have a nice corollary to Proposition 3.21.

Proposition 3.22. *If H and K are subgroups of G and $H \leq N_G(K)$, then $HK \leq G$. In particular, if $K \trianglelefteq G$, then $HK \leq G$ for all $H \leq G$.*

Proof. It suffices to show $HK = KH$. Let $h \in H, k \in K$. So $hkh^{-1} \in K$ as $H \leq N_G(K)$. It follows that $hk = (hkh^{-1})h \in KH$. So $HK \subset KH$. By similar argument, $kh = h(h^{-1}kh) \in HK$, which implies $KH \subset HK$. So $HK = KH$. $\square$

3.3.4 The Group Isomorphism Theorems

The group isomorphism theorems are elegant results relating a group G to a quotient group G/N. We have already proven the first isomorphism theorem, which states that for a group homomorphism $\phi : G \to H$, $\ker(\phi)$ partitions G into a quotient group isomrophic to $\phi(G)$. The second and fourth isomorphism theorems leverage the poset of subgroups to ascertain the structure of quotients. Finally, the third isomorphism theorem provides us with the "cancellation" of quotients like we would expect with fractions in $\mathbb{Q}$ or $\mathbb{R}$. We have already proven the First Isomorphism Theorem (Theorem 3.18), so we begin with the Second Isomorphism Theorem. The bulk of the machinery to prove the Second Isomorphism Theorem was developed in the last section, so it is a matter of putting the pieces together.

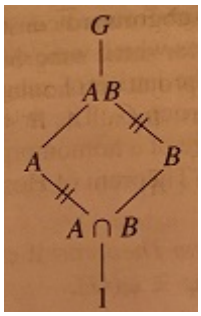
Theorem 3.22 (Second (Diamond) Isomorphism Theorem)**.** *Let G be a group, and let $A, B \leq G$. Suppose $A \leq N_G(B)$. Then $AB \leq G$, $B \trianglelefteq AB$, $A \cap B \trianglelefteq A$, and $AB/B \cong A/(A \cap B)$.*

Proof. By Proposition 3.22, we have $AB \leq G$. As $A \leq N_G(B)$ by assumption and $B \leq N_G(B)$, it follows that $AB \leq N_G(B)$. So $B \trianglelefteq AB$. Thus, AB/B is a well-defined quotient group. We define the map $\phi : A \to AB/B$ by sending $\phi(a) = aB$. This map is clearly surjective. We have $\phi(uv) = uvB = uB \cdot vB$ with the last equality by the group operation of AB/B. So $uB \cdot vB = \phi(u)\phi(v)$, and ϕ is a homomorphism. The kernel of this homomorphism is the set:

$$\ker(\phi) = \{a \in A : \phi(a) = B\} = \{a \in A : a \in B\} = A \cap B$$

So by the First Isomorphism Theorem, we have $A \cap B \trianglelefteq A$, and $A/(A \cap B) \cong \phi(A) = AB/B$. □

The Second Isomorphism Theorem is referred to the as the Diamond Isomorphism Theorem because of the portion of the lattice involved. The marked edges on the lattice indicate the isomorphic quotients.



We now prove the Third Isomorphism Theorem, which considers quotients of quotient groups. Informally, the cancellation property is shown to hold with groups. We also obtain that a quotient preserves normality.

Theorem 3.23 (Third Isomorphism Theorem)**.** *Let G be a group, and let H and K be normal subgroups of G with $H \leq K$. Then $K/H \trianglelefteq G/H$ and $(G/H)/(K/H) \cong G/K$.*

Proof. As H and K are normal in G, we have that G/H and G/K are well-defined quotient groups. We construct a homomorphism $\phi : G/H \to G/K$ sending $\phi(gH) = gK$. We first show ϕ is well-defined. Suppose $g_1H = g_2H$. Then there exists an $h \in H$ such that $g_1 = g_2h$. As $H \leq K$, $h \in K$. So $\phi(g_1H) = \phi(g_2H) = g_1K = g_2K$. As g may be chosen arbitrarily, ϕ is surjective. As ϕ is a projection, it is clearly a homomorphism. We now deduce $\ker(\phi)$.

We have $\ker(\phi) = \{gH \in G/H : \phi(gH) = K\} = \{gH \in G/H : g \in K\} = K/H$. So by the First Isomorphism Theorem, $K/H \trianglelefteq G/H$, and $(G/H)/(K/H) \cong G/K$. □

Remark: The Second and Third Isomorphism Theorems provide nice examples of leveraging the First Isomorphism Theorem. In general, when proving a subgroup H is normal in a parent group G, a good strategy is to constructe a surjective homomorphism from G to some quotient group Q and deduce that H is the kernel of said homomorphism. Projections are often good choices for these types of problems.

We conclude with the Fourth or Lattice Isomorphism Theorem, which relates the lattice of subgroups for the quotient group G/N to the lattice of subgroups of G. The lattice of subgroups of G/N can be constructed from the lattice of subgroups of G, by collapsing the group N to the trivial subgroup and G/N appears at the top of its lattice. In particular, there exists a bijection between the subgroups of G containing N and the subgroups of G/N. We will prove the Fourth Isomorphism Theorem. The general strategy in proving each of these parts is to apply a "lifting" technique, in which we study the quotient structure by taking (under the natural projection homomorphism) the preimages or orbits in G, operating on them, then projecting back down to the quotient. Alternatively, we also study the quotient then lift back to the parent group to study the structure of the original group.

Theorem 3.24 (The Fourth (Lattice) Isomorphism Theorem)**.** *Let G be a group, and let $N \trianglelefteq G$. Then there is a bijection from the set of subgroups A of G containing N onto the set of subgroups $\overline{A} = A/N$ of G/N. In particular, every subgroup of $\overline{G} = G/N$ is of the form A/N for some subgroup A of G containing N (i.e., its preimage in G under the natural projection homomorphism from G to G/N). This bijection has the following properties for all $A, B \leq G$ with $N \leq A$ and $N \leq B$:*

1. *$A \leq B$ if and only if $\overline{A} \leq \overline{B}$*
2. *If $A \leq B$, then $[B : A] = [\overline{B} : \overline{A}]$*
3. *$\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$*
4. *$\overline{A \cap B} = \overline{A} \cap \overline{B}$*
5. *$A \trianglelefteq B$ if and only $\overline{A} \trianglelefteq \overline{B}$*

Proof. Let $\mathcal{A} = \{A \leq G : N \leq A\}$ and $\mathcal{A}/N = \{A/N \leq G/N\}$. Let $\phi : \mathcal{A} \to \mathcal{A}/N$ be defined sending $A \mapsto A/N$. This map is clearly surjective. We now show that ϕ is injective. Suppose $A_1/N = A_2/N$. As the preimage of a subgroup in a homomorphism is a subgroup of the domain, we have that A_1 and A_2 are subgroups of G containing N, and so $A_1 = A_2$ must hold. So ϕ is injective. We now prove each of the conditions (1)-(5).

1. Suppose first $A \leq B$. For each $a \in A$, we have $\phi(a) = aN$. As $a \in B$, $aN \in BN$. Since ϕ is a homomorphism, we have $\phi(A) \leq \overline{B}$. Conversely, suppose $\overline{A} \leq \overline{B}$. We apply the subgroup criterion to show $A \leq B$. We clearly have $1N = N \in \overline{A}$, so $1 \in A \cap B$. Now let $\overline{g}, \overline{h} \in \overline{A}$. Then $\overline{h^{-1}} \in \overline{A}$. So $\overline{gh^{-1}} \in \overline{A}$ and $gh^{-1} \in A$. As $\overline{g}, \overline{h} \in \overline{B}$, it follows that $gh^{-1} \in B$ as well. So $A \leq B$.

2. Recall that $[B : A]$ counts the number of left cosets in $\overline{B}$. We map $\psi : B/A \to \overline{B}/\overline{A}$ by projection, sending $bA \mapsto \overline{bA}$. We show ψ is well-defined. Suppose $b_1A = b_2A$. Then $b_2^{-1}b_1A = A$, so $\psi(b_1A) = \psi(b_2A) = \overline{b_1A}$. So ψ is well-defined. Clearly, ψ is surjective. So it suffices to show that ψ is injective. Suppose $\psi(b_1A) = \psi(b_2A)$. Then $\overline{b_1A} = \overline{b_2A}$, which occurs if and only if $\overline{b_2^{-1}b_1}\overline{A} = \overline{A}$. The preimage is necessarily $b_2^{-1}b_1A = A$ (that is, $b_2A = b_1A$), so ψ is injective.

3. Let $g = \prod_{i=1}^{k} x_i \in \langle A, B\rangle$. Then:

$$\overline{g} = (\prod_{i=1}^{k} x_i)N = \prod_{i=1}^{k} x_iN$$

   Thus, $\overline{g} \in \langle \overline{A}, \overline{B}\rangle$. Conversely, let $\overline{h} = \prod_{i=1}^{j} \overline{x_i} \in \langle \overline{A}, \overline{B}\rangle$. By construction of G/N, each $x_i = y_in_i$ for some $y_i \in \langle A, B\rangle$ and $n_i \in N$. So:

$$h = \prod_{i=1}^{j} y_i \in \langle A, B\rangle$$

   Thus, $\overline{h} \in \overline{\langle A, B\rangle}$ and $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$.

4. Let $\overline{h} \in \overline{A \cap B}$. Then $h \in A$ and $h \in B$. So $\overline{h} \in \overline{A}$ and $\overline{h} \in \overline{B}$. Conversely, let $\overline{g} \in \overline{A} \cap \overline{B}$. So $g = kn$ for some $k \in A \cap B$ and $n \in N$. So $\overline{g} = \overline{k} \in \overline{A \cap B}$. Thus, $\overline{A \cap B} = \overline{A} \cap \overline{B}$.

5. Suppose that $A \trianglelefteq B$. Let $a \in A$ and $b \in B$. We have $\overline{b}\overline{A}\overline{b^{-1}} = \overline{bAb^{-1}} = \overline{A}$. So $\overline{A} \trianglelefteq \overline{B}$. Conversely, suppose $\overline{A} \trianglelefteq \overline{B}$. Let $\tau : B \to \overline{B}/\overline{A}$ be given by $\tau(g) = \overline{g}\overline{A}$. We have $\ker(\tau) = \{b \in B : \tau(b) = \overline{A}\}$, which is equivalent to $bN = aN$ for some $a \in A$. As $N \leq A$, so $bN = aN$ if and only if $b \in A$. So $\ker(\tau) = A$, and $A \trianglelefteq B$.

□

Remark: While the quotient group preserves many properties of its parent, it does not preserve isomorphism. Consider $\mathbb{Q}_8/\langle -1\rangle \cong D_8/\langle r^2\rangle \cong \mathbb{V}_4$. However, $Q_8 \ncong Q_8$. We see in the lattices of Q_8 and D_8 below where the sublattice of $\mathbb{V}_4$ is contained.

INCLUDE LATTICES

3.3.5 Alternating Group

In this section, we introduce the altenrating group of degree n, dentoed A_n. Intuitively, the altenrating group consists of the even permutations of S_n. With the integers, there is a clear notion of even and odd. It is necessary to define an analogous notion for permutations. Recall that every permutation can be written as the product of transpositions or 2-cycles. There are two approaches to formulate the parity of a permutation. The first approach is to consider the action of S_n on the following polynomial:

$$\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j) \tag{39}$$

The alternative formulation is to count the number of transpositions in the permutation's decomposition. In order to utilize this latter approach, it must first be shown that a permutation can be written uniquely as the product of disjoint cycles. The permutatoin's parity is then the product of the parity of each cycle in its decomposition. We begin by studying the action of S_n on Δ, which permutes the indices of the variables. That is, for $\sigma \in S_n$, we have:

$$\sigma(\Delta) = \prod_{1 \leq i < j \leq} (x_{\sigma(i)} - x_{\sigma(j)}) \tag{40}$$

Example 113. Suppose $n = 4$. Then:

$$\Delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4) \tag{41}$$

If $\sigma = (1, 2, 3, 4)$, then:

$$\sigma(\Delta) = (x_2 - x_3)(x_2 - x_4)(x_2 - x_1)(x_3 - x_4)(x_3 - x_1)(x_3 - x_4) \tag{42}$$

Here, we wrote the factors of $\sigma(\Delta)$ in the same order as σ. Observe that Δ has the factor $(x_i - x_j)$ for every $1 \leq i < j \leq n$. As σ is a bijection, $\sigma(\Delta)$ has either the factor $(x_i - x_j)$ or $(x_j - x_i)$. Observe that $(x_i - x_j) = -(x_j - x_i)$. It follows that $\sigma(\Delta) = \pm\Delta$ for every $\sigma \in S_n$. We define the parity homomorphism $\epsilon : S_n \to \{\pm 1\}$ as follows:

$$\epsilon(\sigma) = \begin{cases} 1 & : \sigma(\Delta) = \Delta \\ -1 & : \sigma(\Delta) = -\Delta \end{cases} \tag{43}$$

We use ϵ to define the sign or parity of a permutation.

Definition 105 (Sign of a Permutation)**.** The *sign* of the permutation σ is $\epsilon(\sigma)$. If $\epsilon(\sigma) = 1$, then σ is said to be *even*. Otherwise, σ is said to be *odd*.

In particular, ϵ is a homomorphism, which we easily verify below:

Proposition 3.23. *The function ϵ defined above is a homomorphism, where $\{\pm 1\} \cong \mathbb{Z}_2$ using the operation of multiplication for $\{\pm 1\}$.*

Proof. Let $\sigma, \tau \in S_n$. By definition:

$$(\tau\sigma)(\Delta) = \prod_{1 \leq i < j \leq n} (x_{\tau\sigma(i)} - x_{\tau\sigma(j)}) = \epsilon(\tau\sigma)\Delta$$

We now see that $(\tau\sigma)(\Delta) = \tau(\epsilon(\sigma)\Delta)$ by associativity of the group action. We then interchange $\tau(\epsilon(\sigma)\Delta) = \epsilon(\sigma)(\tau(\Delta)) = \epsilon(\sigma)\epsilon(\tau) = \epsilon(\tau)\epsilon(\sigma)$. So ϵ is a homomorphism. □

In particular, it follows that transpositions are odd permutations and ϵ is a surjective homomorphism. We now define the Alternating group of degree n:

Definition 106 (Alternating Group)**.** The *Alternating group of degree n*, denoted A_n, is $\ker(\epsilon)$.

By Lagrange's Theorem, $|A_n|$ divides $|S_n|$. Furthermore, as ϵ is a homomorphism onto $\{\pm 1\}$, we see that $[S_n : A_n] = 2$. So $|A_n| = \frac{1}{2}|S_n|$. That is, there are as many even permutations as odd permutations. We also see the map $\psi : S_n \to S_n$ sending $\sigma \mapsto \sigma \cdot (12)$ is a bijection. As $\epsilon(12) = -1$, ψ maps even permutations to odd permutations, and odd permutations to even permutations. This provides a bijective argument that there are just as many even permutations as odd permutations.

It is also easy to see why the Alternating group is the kernel of the parity homomorphism. Recall from homework that every permutation can be written as the product of transpositions. We first recognize that $\epsilon(\sigma) = \epsilon(\sigma^{-1})$. Let $\sigma = \prod_{i=1}^{k} s_i$, where each s_i is a transposition. Then $\sigma^{-1} = \prod_{i=1}^{k} s_{k-i+1}$. Intuitively, each transposition in the decomposition of σ needs to be cancelled to obtain the identity. Let S_n act on itself by conjugation. We consider $\epsilon(\sigma\tau\sigma^{-1}) = \epsilon(\sigma)\epsilon(\tau)\epsilon(\sigma^{-1})$. As $\epsilon(\sigma) = \epsilon(\sigma^{-1})$, we have $\epsilon(\sigma)\epsilon(\tau)\epsilon(\sigma^{-1}) = \epsilon(\tau) = 1$ if and only if τ is even and for all $\sigma \in S_n$.

We now seek to define the Alternating group in terms of the cycle decomposition. Recall that every permutation has a cycle decomposition. In Section 3.1.3, an algorithm was presented to compute the cycle decomposition of a permutation. This algorithm is formally justified using a group action. That is, we prove the cycle decomposition from this algorithm is unique. In order to prove this result, we need a result known as the Orbit-Stablizer Lemma which is also known as Burnside's Lemma. The Orbit-Stabilizer Lemma is a powerful tool in algebraic combinatorics, which is the foundation for Polyá Enumeration Theory.

Theorem 3.25 (Orbit-Stabilizer Lemma)**.** *Let G be a group acting on the set A. Then $|G_a| \cdot |\mathcal{O}(a)| = |G|$, where G_a is the stablizer of a and $\mathcal{O}(a)$ is the orbit of a.*

Proof. Recall that the orbits of a group action partition A (formally the equivalence relation on A is defined as $b \equiv a$ if and only if $b = g \cdot a$ for some $g \in G$). Recall that $\mathcal{O}(a) = \{g \cdot a : g \in G\}$. So we map $\mathcal{O}(a) \to g \cdot G_a$ by sending $g \cdot a \mapsto g \cdot G_a$. This map is clearly surjective. Now suppose $g \cdot G_a = h \cdot G_a$. Recall that $g \cdot a = h \cdot a$ if and only if $h^{-1}g \cdot a = a$, which is equivalent to $h^{-1}g \in G_a$. So $gG_a = hG_a$ if and only if $h^{-1}gG_a = G_a$. So this map is injective. It follows that $\mathcal{O}(a)$ partitions G into cosets of order $|G_a|$. □

We now prove the existence and uniqueness of the cycle decomposition of a permutation.

Theorem 3.26. *Every permutation $\sigma \in S_n$ can be written uniquely as the product of disjoint cycles.*

Proof. Let $\sigma \in S_n$, and let $G = \langle \sigma \rangle$ act on $[n]$. Let $x \in [n]$ and consider $\mathcal{O}(x)$. By the Orbit-Stabilizer Lemma, the map $\sigma^i x \mapsto \sigma^i G_x$ is a bijection. As G is cyclic, $G_x \trianglelefteq G$, so G/G_x is a well-defined quotient group. In particular, G/G_x is cyclic, and $d := |G/G_x|$ is the least positive integer such that $\sigma^d \in G_x$. By the Orbit-Stabilizer Lemma $[G : G_x] = |\mathcal{O}(x)| = d$. It follows that the distinct left-cosets of G_x are $G_x, \sigma G_x, \ldots, \sigma^{d-1} G_x$, and $\mathcal{O}(x) = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{d-1}(x)\}$. We iterate on this argument for each orbit to obtain a cycle decomposition for σ. The uniqueness of the cycle decomposition for σ follows from our selection of σ and the fact that a permutation is a bijection. □

Remark: Theorem 3.26 provides an algorithm for computing the cycle decomposition of a given permutation. We can further decompose each disjoint cycle of σ into a product of transpositions, giving us a factorization of σ in terms of transpositions. So by the Well-Ordering Principle, there exists a minimum number of transpositions whose product forms σ. We then say a permutation σ is even (odd) if its minimum factorization in terms of transpositions consists of an even (odd) number of 2-cycles. The Alternating group of degree n, A_n, can then be defined as the group of even permutations.

3.3.6 Algebraic Graph Theory- Graph Homomorphisms

In this section, we explore some basic results on graph homomorphisms. Recall that a graph homomorphism for the graphs G and H is a function $\phi : V(G) \to V(H)$ such that $ij \in E(G) \implies \phi(i)\phi(j) \in E(H)$. That is, a graph homomorphism preserves the adjacency relation from G into H. A well-known class of graph homomorphism is the graph coloring. A graph G is r-colorable if there exists a homomorphism $\phi : V(G) \to V(K_r)$. That is, the vertices of K_r are the r-colors of G. It is an $\mathcal{NP}$-Complete problem to decide if a graph G is r-colorable, which is equivalent to deciding if there exists a homomorphism $\phi : V(G) \to K_r$. So it is also $\mathcal{NP}$-Complete to decide if there even exists a homomorphism between graphs G and H.

The theory of graph homomorphisms has a similar flavor to the study of group homomorphisms. In a group homomorphism, the operation is preserved in the image. So a product in the domain translates to a product in the codomain. Graph homomorphisms similarly map walks in the domain to walks in the image. Much of what we know about group homomorphisms holds true for graph homomorphisms. One example of this deals with the composition of graph homomorphisms. Let $g : V(H) \to V(K)$ with $h : V(G) \to V(H)$ be graph homomorphisms. Then $g \circ h : V(G) \to V(K)$ is itself a graph homomorphism.

We now define the binary relation $\to$ on the set of finite graphs, where $X \to Y$ if there exists a homomorphism $\phi : V(X) \to V(Y)$. Clearly, $\to$ is reflexive, as $X \to X$ by the identity map. As the composition of two graph homomorphisms is a graph homomorphism, we have that $\to$ is transitive. However, $\to$ fails to be a partial order. Let G be a bipartite graph, and $Y := K_2$. Then there exists a homomorphism from X to Y, mapping one part of X to $v_1 \in Y$ and the other part of X to $v_2 \in Y$. Similarly, if there is an edge in X, there exists a homomorphism from Y to X mapping Y as some edge in X. However, any case when $|X| > |2|$ results in $X \ncong Y$. We need surjectivity of the homomorphisms from $X \to Y$ and $Y \to X$ to deduce that $X \cong Y$. If $X \to Y$ and $Y \to X$, we say that X and Y are *homomorphically equivalent*.

Much in the same way that we study quotient groups, we study quotient graphs. Let $f : V(X) \to V(Y)$ be a graph homomorphism. The preimages $f^{-1}(y)$ for each $y \in Y$ are the *fibers*, which partition the graph X. We refer to the partition as the *kernel*. In group theory, we refer to the kernel as the preimage of the identity in the codomain. The kernel then acts on the domain, partitioning it into a quotient group isomorphic to the image. In the graph theoretic setting, there is no identity element as there is no operation. So in a more general setting, we view the kernel as an equivalence relation π on the vertices of X. We construct a *quotient graph* X/π as follows. The fibers of π are the vertices of X/π. Then vertices $f^{-1}(u), f^{-1}(v)$ in X/π are adjacent if there exist representatives $a \in f^{-1}(u), b \in f^{-1}(v)$ such that $ab \in E(X)$. Note that if X has loops, it may be the case that $u = v$. There exists a natural homomorphism $\phi : V(X) \to V(X/\pi)$ sending $v \mapsto f^{-1}(f(v))$.

While deciding if there exists a homomorphism $\phi : V(X) \to V(Y)$ is $\mathcal{NP}$-Complete, we can leverage a couple invariants to make our life easier. First, if the graph Y is r-colorable and there exists a homomorphism from X to Y, then $\chi(X) \leq \chi(y) = r$. This follows from the fact that for graph homomoprhisms $g : V(Y) \to K_r$ and $f : V(X) \to V(Y)$, $g \circ f : V(X) \to K_r$ is a graph homomorphism.

We prove a second invariant based on the *odd girth*, or length of the shortest odd cycle in a graph.

Proposition 3.24. *Let X and Y be graphs, and let $\ell(X)$ be the odd girth in X. If there exists a graph homomorphism $f : V(X) \to V(Y)$, then $\ell(Y) \leq \ell(X)$.*

Proof. Let $v_0, v_1, \ldots, v_{\ell-1}, v_0$ be the sequence of vertices in X that form a cycle of length ℓ, with $v_0 = v_\ell$. Applying f, we obtain $f(v_i)f(v_{i+1}) \in E(Y)$ for each $i \in \{0, \ldots, \ell - 1\}$ with the indices taken modulo ℓ. So $f(v_0)f(v_1)\ldots f(v_{\ell-1})f(v_0)$ is a closed walk of odd length. By Lemma 1.1, $f(v_0)f(v_1)\ldots f(v_{\ell-1})f(v_0)$ contains an odd cycle, which implies $\ell(Y) \leq \ell(X)$. □

We now introduce the notion of a *core*. Formally:

Definition 107 (Core)**.** A graph X is a *core* if every homomorphism $\phi : V(X) \to V(X)$ is a bijection. That is, every homomorphism from a core to itself is an automorphism.

Example 114. The simplest class of cores is the set of complete graphs. Odd cycles are also cores. We verify that odd cycles are cores below.

Proposition 3.25. *Let $n \in \mathbb{N}$ and let $X := C_{2n+1}$ be an odd cycle. Let $f : V(X) \to V(X)$ be a homomorphism. Then f is a bijection.*

Proof. Suppose to the contrary that f is not a bijection. Then $f(v_i) = f(v_j) = v_k$ for $i, j, k \in [2n+1]$ and $i \neq j$. Let $P := v_i v_{i+1} \dots v_{j-1} v_j$ be a path of even length h. We have two cases. Suppose first $f(v_{i+1}) \neq f(v_{j-1})$. As f is a homomorphism, the two center vertices of P are not adjacent under f. However, as they are adjacent in P, they must be adjacent in f as f is a homomorphism, a contradiction. If instead $f(v_{i+1}) = f(v_{j-1})$, the two center vertices will map to the same vertex under f, contradicting the fact that f is a homomorphism. Therefore, it is necessary that f is a bijection. □

Cores provide a useful invariant to decide if there exists a homomorphism from $X \to Y$. We first show that X and Y being isomorphic cores is equivalent to X and Y being homomorphically equivalent. Next, we show that every graph has a core, and a graph's core is unique up to isomorphism. This implies that the relation $\to$ is a partial order on the class of cores.

Definition 108 (Core of a Graph)**.** Let X be a graph. The subgraph Y of X is said to be a *core of* X if Y is a core and there exists a homomorphism from X to Y. We denote the core of X as $X^\bullet$.

We introduce another example of a core, which relates to coloring.

Definition 109 (χ-Critical Graph)**.** A graph X is χ-critical if any proper subgraph of X has chromatic number less than $\chi(X)$.

Remark: In particular, a χ-critical graph cannot have a homomorphism to any of its proper subgraphs. So a χ-critical graph is a core (and therefore, its own core).

Lemma 3.6. *Let X and Y be cores. Then X and Y are homomorphically equivalent if and only if they are isomorphic.*

Proof. If $X \cong Y$, then the isomorphisms from X to Y and Y to X are homomorphisms and we are done. Conversely, let $f : V(X) \to V(Y)$ and $g : V(Y) \to V(X)$ be homomorphisms. Then $g \circ f$ and $f \circ g$ are homomorphisms, and they are bijections as X and Y are cores. □

We introduce the definition of a retract and induced subgraph before proving the next lemma.

Definition 110 (Retract)**.** Let X be a graph. The subgraph Y of X is said to be a *retract* if there exists a homomorphism $f : X \to Y$ such that the restriction of f to Y is the identity map. We refer to f as a *retraction.*

Definition 111 (Induced Subgraph)**.** Let X be a graph, and let Y be a subgraph of X. The graph Y is said to be an *induced subgraph* of X if $E(Y) = \{ij \in E(X) : i, j \in V(Y)\}$.

Lemma 3.7. *Every graph X has a core, which is an induced subgraph and is unique up to isomorphism.*

Proof. As X is finite and the identity map is a homomorphism, there is a finite and non-empty set of subgraphs Y of X such that $X \to Y$. So there exists a minimal element H with respect to inclusion. Let $f : X \to H$ be a homomorphism. As H is minimal, f restricted to H is an automorphism ϕ of H. Composing f with ϕ^{-1} yields the identity map on H. So H is a retract, and therefore a core. It also follows that H is an induced subgraph of X. Now suppose H_1, H_2 are cores of X. Let $f_i : V(X) \to V(H_i)$ be a homomorphism. Then for each $i \in [2]$, f_i restricted to H_{-i} is a homomorphism from H_i to H_{-i} (where $-i \in [2] - \{i\}$). So by Lemma 3.6, $H_1 \cong H_2$. □

We are now able to characterize homomorphic equivalence in terms of cores.

Theorem 3.27. *Two graphs X and Y are homomorphically equivalent if and only if their cores are isomorphic.*

Proof. Suppose first X and Y are homomorphically equivalent. Then we have a sequence of homomorphisms:

$$X^\bullet \to X \to Y \to Y^\bullet \tag{44}$$

These homomorphisms compose to form a homomorphism from $X^\bullet$ to $Y^\bullet$. By similar argument, there exists a homomorphism from $Y^\bullet$ to $X^\bullet$. Lemma 3.6 implies that $X^\bullet \cong Y^\bullet$.

Conversely, suppose $X^\bullet \cong Y^\bullet$. Then we have a sequence of homomorphisms:

$$X \to X^\bullet \to Y^\bullet \to Y \text{ and} \tag{45}$$
$$Y \to Y^\bullet \to X^\bullet \to X \tag{46}$$

Each of these sequences composes to form a homomorphism from X to Y and from Y to X respectively, so X and Y are homomorphically equivalent. □

We now discuss basic results related to cores of vertex-transitive graphs. These results are quite elegant, powerful, and simple. Furthermore, they provide nice analogs to group theoretic results such as Lagrange's Theorem and group actions. We begin by showing that the core of a vertex transitive graph is also vertex transitive.

Theorem 3.28. *Let X be a vertex transitive graph. Then the core of X, $X^\bullet$, is also vertex transitive.*

Proof. Let $x, y \in V(X^\bullet)$ be distinct. Then there exists $\phi \in \mathrm{Aut}(X)$ such that $\phi(x) = y$. Let $f : X \to X^\bullet$ be a retraction. The composition $f \circ \phi : X \to X^\bullet$ forms a homomorphism whose restriction to $X^\bullet$ is an automorphism of $X^\bullet$ mapping $x \mapsto y$. So $X^\bullet$ is vertex transitive. □

Our next theorem provides an analog of Lagrange's Theorem in the case of cores of vertex transitive graphs. Recall the proof of Lagrange's Theorem used group actions. In this next result, we use the core and the homomorphism to partition the parent graph into parts of equal cardinality, which is analogous to a group action.

Theorem 3.29. *Let X be a vertex transitive graph with the core $X^\bullet$. Then $|X^\bullet|$ divides $|X|$.*

Proof. Let $\phi : X \to X^\bullet$ be a surjective homomorphism, and let $\gamma : X^\bullet \to X$ be a homomorphism. It suffices to show each fiber of ϕ has the same order. Let $u \in X^\bullet$. Define the set S as follows:

$$S = \{(v, \psi) : v \in V(X^\bullet), \psi \in \mathrm{Aut}(X), \text{ and } \phi \circ \psi \circ \gamma(v) = u\} \tag{47}$$

We count S in two ways. As ϕ, ψ, and γ are all homomorphisms and $X^\bullet$ is a core, $\phi \circ \psi \circ \gamma \in \mathrm{Aut}(X^\bullet)$. As ϕ and γ are fixed, there exists a unique v dependent only on ψ such that $\phi \circ \psi \circ \gamma(v) = u$. So $|S| = |\mathrm{Aut}(X)|$.

We now count S in a second way. Note that $\phi \circ \psi \circ \gamma(v) = u$ implies that $\psi \circ \gamma(v) \in \phi^{-1}(u)$. We select $v \in V(X^\bullet)$, $x \in \phi^{-1}(u)$, and an automorphism ψ mapping $\gamma(v) \mapsto x$. There are $|X^\bullet|$ ways to select v and $|\phi^{-1}(u)|$ ways to select x. These selections are independent; so by rule of product, we multiply $|X^\bullet| \cdot |\phi^{-1}(u)|$. Now the set of automorphisms mapping $\gamma(v) \to x$ is a left-coset of $\mathrm{Stab}(\gamma(v))$, which has cardinality $|\mathrm{Stab}(\gamma(v))|$. As X is vertex transitive, the orbit of v under the action of $\mathrm{Aut}(X)$ is $V(X)$. So by the Orbit-Stabilizer Lemma, $|\mathrm{Stab}(\gamma(v))| = |\mathrm{Aut}(X)|/|X|$. By rule of product, $|S| = |X^\bullet| \cdot |\phi^{-1}(u)| \cdot |\mathrm{Aut}(X)|/|X|$. As $|\mathrm{Aut}(X)| = |S|$, we deduce that $|\phi^{-1}(u)| = |X|/|X^\bullet|$. So $|X^\bullet|$ divides $|X|$ and we are done. □

Theorem 3.29 provides a couple nice corollaries. The first is an analog of group theory, which states that a group of prime order p is isomorphic to $\mathbb{Z}_p$. The second corollary provides conditions to deduce when a graph is triangle free.

Corollary 3.25.1. *If X is a connected vertex transitive graph of prime order p, then X is a core.*

Corollary 3.25.2. *Let X be a vertex transitive graph of order n, with $\chi(X) = 3$. If n is not a multiple of 3, then X is triangle-free.*

Proof. As $\chi(X) = 3$, there exists a homomorphism from X to K_3. If K_3 was the core of X, then K_3 would be contained in X. By Theorem 3.29, 3 would divide n, a contradiction. □

We next introduce the notion of graph product, which is analogous to the direct product of groups. In group theory, the direct product of $G \times H$ is the set of ordered pairs $\{(g, h) : g \in G, h \in H\}$ with the operation preserved componentwise. That is, $(a, b)(c, d) = (ac, bd)$ where ac is evaluated in G and bd is evaluated in H. The graph product is based on this idea, preserving the adjacency relation component wise.

Definition 112 (Graph Product)**.** Let X and Y be graphs. Then the product $X \times Y$ is the grah with the vertex set $\{(x, y) : x \in V(X), y \in V(Y)\}$ and two vertices $(a, b), (c, d)$ in $X \times Y$ are adjacent if and only if $ac \in E(X)$ and $bd \in E(Y)$.

Remark: Note that the graph product is **not** a Cartesian product. In algebraic graph theory, the Cartesian product of two graphs is denoted as $X \square Y$ and is defined differently than the graph product above.

In a graph product, we have $X \times Y \cong Y \times X$, with the isomorphism sending $(x, y) \mapsto (y, x)$. So factors in a product graph may be reordered in the product. However, a graph may have multiple factorizations. We see that:

$$K_2 \times 2K_3 \cong 2C_6 \cong K_2 \times C_6$$

So $X \times Y \cong X \times Z$ does not imply that $Y \cong Z$. We also note that for a fixed $x \in V(X)$, the vertices of $X \times Y$ of the form $\{(x, y) : y \in Y\}$ form an independent set. So $X \times K_1$ is the empty graph of order $|X|$, rather than X.

We have already seen in the study of quotient groups that the natural projection homomorphism is quite useful. The natural projection homomorphism is also a common tool in studying direct products of groups, and it comes up frequently in the study of graph homomorphisms. Formally, if we have the product graph $X \times Y$, the projection map:

$$p_X : (x, y) \mapsto x$$

Is a homomorphism from $X \times Y \to X$. There is similarly a projection $p_Y : X \times Y \to Y$. We use the projection map to count homomorphisms from a graph Z to a product graph $X \times Y$. We denote the set of homomorphisms from a graph G to a graph H as $\mathrm{Hom}(G, H)$. Our next theorem provides a bijection from:

$$\mathrm{Hom}(Z, X \times Y) \to \mathrm{Hom}(Z, X) \times \mathrm{Hom}(Z, Y)$$

Theorem 3.30. *Let X, Y and Z be graphs. Let $f : Z \to X$ and $g : Z \to Y$ be homomorphisms. Then there exists a unique homomorphism $\phi : Z \to X \times Y$ such that $f = p_X \circ \phi$ and $g = p_Y \circ \phi$.*

Proof. The map $\phi : z \mapsto (f(z), g(z))$ is clearly a homomorphism from Z to $X \times Y$. Furthermore, we have $f = p_X \circ \phi$ and $g = p_Y \circ \phi$. The homomorphism ϕ is uniquely determined by our selections of f and g. So the map $\phi \mapsto (f, g)$ is a bijection. □

Corollary 3.25.3. *For any graphs X, Y, and Z, we have:*

$$|Hom(Z, X \times Y)| = |Hom(Z, X)| \cdot |Hom(Z, Y)|$$

3.3.7 Algebraic Combinatorics- The Determinant

TODO

3.4 Group Actions

3.4.1 Conjugacy

In this section, we explore results related to the action of conjugation. Recall that G acts on the set A by conjugation, with $g \in G$ sending $g : a \mapsto gag^{-1}$. We focus on the case when G acts on itself by conjugation.

Definition 113 (Conjugacy Classes)**.** We say that two elements $a, b \in G$ are *conjugate* if there exists a $g \in G$ such that $b = gag^{-1}$. That is, a and b are conjugate if they belong to the same orbit when G acts on itself by conjugation. Similarly, we say that two subsets of G, S and T, are conjugate if $T = gSg^{-1}$ for some $g \in G$. We refer to these orbits as *conjugacy classes.*

Example 115. If G is Abelian, the action of G on itself by conjugation is the trivial action because $gag^{-1} = gg^{-1}a = a$.

Example 116. When S_3 acts on itself by conjugation, the conjugacy classes are $\{1\}$, $\{(1,2),(1,3),(2,3)\}$, $\{(1,2,3),(1,3,2)\}$.

Remark: In particular, if $|G| > 1$; then under the action of conjugation, G does not act transitively on itself. We see that $\{1\}$ is always a conjugacy class, so there are at least two orbits under this action.

We now use the Orbit-Stabilizer Lemma to compute the order of each conjugacy class.

Proposition 3.26. *Let G be a group, and let $S \subset G$. The number of conjugates of S is the index of the normalizer in G, $[G : N_G(S)]$.*

Proof. We note that $\text{Stab}(S) = \{g \in G : gSg^{-1} = S\} = N_G(S)$. The conjugates of S lie in the orbit $\mathcal{O}(S) = \{gSg^{-1} : g \in G\}$. The result follows from the Orbit-Stabilizer Lemma. □

As the orbits partition the group, orders of the conjugacy classes add up to $|G|$. This observation provides us with the Class Equation, which is a powerful tool in studying the orbits in the action of conjugation.

Theorem 3.31 (The Class Equation)**.** *Let G be a finite group, and let $g_1, \ldots, g_r$ be represnetatives of the distinct conjugacy classes in G that are not contained in $Z(G)$. Then:*

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)] \tag{48}$$

Proof. We note that for a single $g_i \in G$, $N_G(g_i) = C_G(g_i)$. We note that for an element $x \in Z(G)$, $gxg^{-1} = x$ for all $g \in G$. So the conjugacy class of x contains only x. Thus, the conjugacy classes of G are:

$$\{1\}, \{z_2\}, \ldots, \{z_m\}, \mathcal{K}_1, \ldots, \mathcal{K}_r \tag{49}$$

Where $z_2, \ldots, z_m \in Z(G)$ and $g_i \in \mathcal{K}_i$ for each $i \in [r]$. As the conjugacy classes partition G and $|\mathcal{K}_i| = [G : C_G(g_i)]$ by the previous proposition, we obtain:

$$|G| = \sum_{i=1}^{m} 1 + \sum_{i=1}^{r} |\mathcal{K}_i| \tag{50}$$

$$= |Z(G)| + \sum_{i=1}^{r} [G : C_G(g_i)] \tag{51}$$

□

We consider some examples to demonstrate the power of the Class Equation.

Example 117. Let $G = D_8$. We use the class equation to deduce the conjugacy classes of D_8. We first note $Z(D_8) = \{1, r^2\}$, which yields the conjugacy classes $\{1\}$ and $\{r^2\}$. It will next be shown that for each $x \notin Z(D_8)$, $|C_G(x)| = 4$. As $C_G(x) = \text{Stab}(x)$ under the action of conjugation, the Orbit-Stabilizer Lemma gives us that the remaining conjugacy classes have order 2.

Recall that the three subgroups of order 4 in D_8 are $\langle r \rangle, \langle s, r^2 \rangle$, and $\langle sr, r^2 \rangle$. Each of these subgroups is Abelian. For any $x \notin Z(D_8)$, $\langle x \rangle \leq C_{D_8}(x)$ and $Z(D_8) \leq C_{D_8}(x)$. So by Lagrange's Theorem, $|C_{D_8}(x)| \geq 4$. As $x \notin Z(D_8)$, some element of G does not commute with x. So $|C_{D_8}(x)| \leq 7$. So by Lagrange's Theorem, $|C_{D_8}(x)| = 4$. So D_8 has three conjugacy classes of order 2, and two conjugacy classes of order 1, which are listed below:

$$\{1\}, \{r^2\}, \{r, r^3\}, \{s, sr^2\}, \{sr, sr^3\} \tag{52}$$

We next use the class equation to prove that every group of prime power order has a non-trivial center.

Theorem 3.32. *Let P be a group of order p^α for a prime p and $\alpha \geq 1$. Then $Z(P) \neq 1$.*

Proof. If P is Abelian, then $Z(P) = P$. So suppose P is not Abelian. Then there exists at least one element $g \in P$ such that $g \notin Z(P)$. Suppose the distinct conjugacy classes of P are:

$$\{1\}, \{z_2\}, \ldots, \{z_m\}, \mathcal{K}_1, \ldots, \mathcal{K}_r \tag{53}$$

Let $g_1, \ldots, g_r$ be distinct representatives of $\mathcal{K}_1, \ldots, \mathcal{K}_r$ respectively. As no conjugacy class is equal to P, p divides each $|\mathcal{K}_i| = [P : C_P(g_i)]$. By the class equation, we have:

$$|P| = |Z(P)| + \sum_{i=1}^{r} |\mathcal{K}_i|$$

As p divides $|P|$ and p divides each $|\mathcal{K}_i|$, p must divide $|Z(P)|$. So $Z(P) \neq 1$. □

Theorem 3.32 provides a nice corollary, allowing us to easily classify groups of order p^2 where p is prime.

Corollary 3.26.1. *Let P be a group of order p^2. Then $P \cong \mathbb{Z}_{p^2}$ or $P \cong \mathbb{Z}_p \times \mathbb{Z}_p$.*

Proof. By Theorem 3.32, $Z(P) \neq 1$. If P has an element of order p^2, then $P \cong \mathbb{Z}_{p^2}$ and we are done. So suppose instead that all every non-identity element has order p. Let $x \in P$ have order p, and let $y \in P \setminus \langle x \rangle$ have order p. Observe that $\langle x \rangle \cap \langle y \rangle = 1$, so $p^2 = |\langle x, y \rangle| > |\langle x \rangle| = p$. Thus, $P = \langle x, y \rangle$. As x, y have order p, $\langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. We construct an isomorphism from $\phi : \langle x \rangle \times \langle y \rangle \to P$ sending $(x^i, y^j) \mapsto x^i y^j$. We leave it as an exercise for the reader to verify that ϕ is an isomorphism. □

Remark: This proof is a more elegant way to demonstrate that a group of order p^2 for a prime p is Abelian. An alternate proof exists using the quotient $P/Z(P)$. We take representatives of P, project them down to $P/Z(P)$, operate in the quotient group, then lift back to P.

We now consider the case when the symmetry group acts on itself by conjugation. We obtain several important results. The first result we present shows that the permutation cycle type is preserved under conjugation. This observation was the key to breaking the Enigma cipher during World War II. The preservation of cycle type under conjugation yields a nice bijection between integer partitions of n and the conjugacy classes of S_n. Note that an integer partition is a sequence of non-decreasing positive integers that add up to n.

Proposition 3.27. *Let $\sigma, \tau \in S_n$. The cycle decomposition of $\tau\sigma\tau^{-1}$ is obtained from σ by replacing each entry i in the cycle decomposition of σ with $\tau(i)$.*

Proof. Suppose $\sigma(i) = j$. As τ is a permutation, we consider the input $\tau(i)$ without loss of generality. So $\tau\sigma\tau^{-1}(\tau(i)) = \tau\sigma(i) = \tau(j)$. So while i, j appear consecutively in σ, $\tau(i)$ precedes $\tau(j)$ in $\tau\sigma\tau^{-1}$. □

We now formally define the cycle type of a permutation.

Definition 114 (Cycle Type)**.** Let $\sigma \in S_n$ be the product of disjoint cycles of lengths $n_1, \ldots, n_k$ with $n_1 \leq n_2 \leq \ldots \leq n_k$ (including the 1-cycles), then the integers $(n_1, \ldots, n_k)$ are the *cycle type* of σ. Note that $n_1 + n_2 + \ldots + n_k = n$.

Remark: It is easy to see the bijection between integer partitions and cycle types. So it remains to be shown that all permutations of a given cycle type belong to the same conjugacy class.

Proposition 3.28. *Two elements of S_n are conjugate in S_n if and only if they have the same cycle type. The number of conjugacy classes of S_n equals the number of partitions of n.*

Proof. If two permutations are conjugate in S_n, then they have the same cycle type by Proposition 3.27. Conversely, suppose two permutations σ and τ have the same cycle type in S_n. We construct a permutation γ such that $\tau = \gamma\sigma\gamma^{-1}$. We begin by ordering the cycles in the decompositions of σ and τ in non-decreasing order, including the 1-cycles. We take the sequences of integers in σ and τ under this ordering, ignoring the parentheses dividing the cycles. The permutation γ then maps the ith term in the list of σ to the ith term in the list of τ. As σ and τ have the same cycle type, $\tau = \gamma\sigma\gamma^{-1}$. □

We illustrate the bijection in the case of S_5.

Example 118.

Partition of 5	**Representative of Conjugacy Class**
$1, 1, 1, 1, 1$	(1)
$1, 1, 1, 2$	$(1, 2)$
$1, 1, 3$	$(1, 2, 3)$
$1, 4$	$(1, 2, 3, 4)$
5	$(1, 2, 3, 4, 5)$
$1, 2, 2$	$(1, 2)(3, 4)$
$2, 3$	$(1, 2)(3, 4, 5)$

Example 119. Using the previous proposition and the Orbit-Stabilizer Lemma, we are able to compute the number of conjugates and centralizers for various permutations. We consider the case of an m cycle $\sigma \in S_n$. Recall that all m cycles belong to the same conjugacy class as σ. We first compute the number of m-cycles in S_n. We select m elements from $[n]$ which can be done in $\binom{n}{m}$ ways. Each set of m selements is then permuted

in $m!$ ways. As cyclic rotations are equivalent, we divide out by m to obtain $\binom{n}{m} \cdot (m-1)!$ cycles of length m in S_n. This is the order of the orbit or conjugacy class containing σ.

By the Orbit-Stabilizer Lemma, we have $\binom{n}{m} \cdot (m-1)! = \dfrac{|S_n|}{|C_G(\sigma)|}$, where $|S_n| = n!$. We now compute $|C_G(\sigma)|$. Any permutation σ commutes with $\langle \sigma \rangle$. Additionally, σ commutes with of the permutations from which it is disjoint. There are $(n-m)!$ such permutations. By the Orbit-Stabilizer Lemma, $|C_G(\sigma)| = m \cdot (n-m)!$. Similar combinatorial analysis can be used to deduce the order of both the centralizers and conjugacy classes for other cycle types.

The integer partitions of $n \in \mathbb{N}$ can be enumerated using techniques from algebraic combinatorics, such as generating functions. Nick Loehr's *Bijective Combinatorics* text and Herbert Wilf's *Generatingfunctionology* text are good resources for further study on enumerating integer partitions.

3.4.2 Automorphisms of Groups

In this section, we study basic properties of automorphisms of groups. We have already seen examples of automorphisms, with the study of graphs. Analogously, for a group G, $\mathrm{Aut}(G)$ denotes the automorphism group of G. The study of automorphisms provides additional information about the structure of a group or its subgroups. We begin by showing the action of conjugation induces automorphisms.

Theorem 3.33. *Let G be a group, and let $H \trianglelefteq G$. Then G acts by conjugation on H as automorphisms of H. In particular, the permutation representation of this action is a homomorphism from G into $Aut(H)$ with kernel $C_G(H)$, with $G/C_G(H) \leq Aut(H)$.*

Proof. Let $g \in G$, and let $\sigma_g : h \mapsto ghg^{-1}$ be the permutation representation of g. As H is normal, each such σ_g is a bijection. It suffices to show that σ_g is a homomorphism. Let $h, k \in H$ and consider $\sigma_g(hk) = g(hk)g^{-1} = (ghg^{-1})(gkg^{-1}) = \sigma_g(h)\sigma_g(k)$. So $\sigma_g \in \mathrm{Aut}(H)$. The kernel of this action are precisely the elements in g which induce the trivial action, which is equivalent to the kernel being $C_G(H)$. We apply the First Isomorphism Theorem to deduce that $G/C_G(H) \leq \mathrm{Aut}(H)$. □

Theorem 3.33 has a couple nice corollaries to tedious homework problems from the introductory group theory material. In particular, it follows immediately that conjugate elements and conjugate subgroups have the same order.

Corollary 3.28.1. *Let K be a subgroup of the group G. Then $K \cong gKg^{-1}$ for any $g \in G$. Conjugate elements and conjugate subgroups have the same order.*

Proof. We apply Theorem 3.33, using $H = G$ as G is normal in itself. The result follows immediately. □

Corollary 3.28.2. *For any subgroup H of a group G, the quotient group $N_G(H)/C_G(H) \leq Aut(H)$. In particular, $G/Z(G) \leq Aut(G)$.*

Proof. We apply Theorem 3.33 to $N_G(H)$ acting on H by conjugation to deduce that $N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$. As $G = N_G(G)$ and $C_G(G) = Z(G)$, we have that $G/Z(G) \leq \mathrm{Aut}(G)$ by the previous case. □

Definition 115 (Inner Automorphisms)**.** Let G be a group, and let $g \in G$. The *inner automorphisms* of G are $\mathrm{Inn}(G) \cong G/Z(G)$. The *outer automorphisms* of G are $Out(G) \cong \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Remark: Note that $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$, so any inner automorphism σ of the group G satisfies $g \circ \sigma(a)g^{-1} = \sigma(g(a))$ for any $g \in \mathrm{Aut}(G)$. The group $\mathrm{Out}(G)$ measures how far away $\mathrm{Aut}(G)$ is from consisting only of inner automorphisms.

We conclude with a final fact about cyclic groups:

Proposition 3.29. *Let $G \cong \mathbb{Z}_n$. Then $Aut(G) \cong \mathbb{Z}_n^\times$.*

Proof. There are $\phi(n)$ generators of $\mathbb{Z}_n$. So for every a such that $\gcd(a, n) = 1$, the map $\sigma_a : x \mapsto x^a$ is an automorphism. The map sending $\sigma_a \mapsto \overline{a}$ is a surjective map from $\mathrm{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^\times$. Now observe that $\sigma_a \circ \sigma_b(x) = (x^b)^a = x^{ab} = \sigma_{ab}(x)$, so the map sending $\sigma_a \mapsto \overline{a}$ is a homomorphism. The kernel of this homomorphism is $\{(1)\}$; so by the First Isomorphism Theorem, $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$. □

3.4.3 Sylow's Theorems

The Sylow Theorems are a stronger partial converse to Lagrange's Theorem than Cauchy's Theorem. More importantly, they provide an important set of combinatorial tools to study the structure of finite groups and are the high point of a senior algebra course. Standard proofs of the Sylow's First Theorem usually proceed by induction, leveraging the Well-Ordering Principle in the background. We instead offer a combinatorial proof using group actions, which is far more enlightening and elegant. To do this, we need a result from combinatorial number theory known as Lucas' Congruence for Binomial Coefficients. We begin with a couple helpful lemmas, which we will need to prove Lucas' Congruence for Binomial Coefficients.

Lemma 3.8. *Let $j, m \in \mathbb{N}$ and p be prime. Then:*

$$\binom{m+p}{j} \equiv \binom{m}{j} + \binom{m}{j-p} \pmod{p} \tag{54}$$

Proof. Let $\mathbb{Z}_p$ act on $Y = \binom{[m+p]}{j}$ sending $S \mapsto gS = \{g(s) : s \in S\}$. The orbits under this action partition Y. Every orbit has order 1 or order p, as p is prime. So $|Y|$ is congruent modulo p to the number of orbits M of order 1. We show $M = \binom{m}{j} + \binom{m}{j-p}$. The orbits of order 1 are in the kernel of the action; that is, the sets $S \in Y$ such that $gS = S$ for all $g \in \mathbb{Z}_p$. It suffices to count the number of sets $S \in Y$ such that the generator $h = (1, 2, \ldots, p) \in \mathbb{Z}_p$ fixes S. If $S \cap [p] = \emptyset$, then $h(x) = x$ for all $x > p$. There are $\binom{m}{j}$ such sets S in this case. If instead $S \cap [p] \neq \emptyset$, it is necessary that $[p] \subset S$. This leaves $j - p$ remaining choices for S, which must be chosen from $\{p + 1, \ldots, m + p\}$. So there are $\binom{m}{j-p}$ selections. By rule of sum, these cases are disjoint, so $M = \binom{m}{j} + \binom{m}{j-p}$. This completes the proof. □

Lemma 3.9. *Let p be prime. Let $a, c \in \mathbb{N}$ and $0 \leq b, d < p$. Then $\binom{ac+b}{cp+d} \equiv \binom{a}{c}\binom{b}{d} \pmod{p}$.*

Proof. The proof is by induction on a. When $a = 0$ and $c > 0$, both sides of the congruence are 0. If $a = c = 0$, then both sides of the congruence are $\binom{b}{d}$. Now suppose this result holds up to a given a, and for all b, c, d. We prove true for the $a + 1$ case. Consider $\binom{(a+1)p+b}{cp+d} = \binom{(ap+b)+p}{p+d}$. By Lemma 3.8, we have:

$$\binom{(ap+b)+p}{p+d} \equiv \binom{ap+b}{cp+d} + \binom{ap+b}{(c-1)p+d} \pmod{p} \tag{55}$$

$$\equiv \binom{a}{c}\binom{b}{d} + \binom{a}{c-1}\binom{b}{d} \pmod{p} \tag{56}$$

With the last equality from the inductive hypothesis. We now apply the binomial identity that $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ and factor the $\binom{b}{d}$ term in (56) to obtain:

$$\left(\binom{a}{c} + \binom{a}{c-1}\right)\binom{b}{d} \equiv \binom{a+1}{c}\binom{b}{d} \pmod{p} \tag{57}$$

Completing the proof. □

With Lemmas 3.8 and 3.9 in tow, we prove Lucas' Congruence for Binomial Coefficients.

Theorem 3.34 (Lucas' Congruence for Binomial Coefficients)**.** *Let p be prime, and let $k, n \in \mathbb{N}$ with $k \leq n$. Let n and k have the base-p expansion $\sum_{i\geq 0} n_i p^i$ and $k = \sum_{i\geq 0} k_i p^i$, where $0 \leq n_i, k_i < p$. Then:*

$$\binom{n}{k} \equiv \prod_{i\geq 0} \binom{n_i}{k_i} \pmod{p} \tag{58}$$

Where $\binom{0}{0} = 1$ and $\binom{a}{b} = 0$ whenever $b > a$.

Proof. The proof is by induction on n. When $k > n$, then $k_i > n_i$ for some i. So both sides of the congruence are 0. We now consider the case when $k \leq n$. The result holds when $n \in \{0, \ldots, p-1\}$ as $n_0 = n, k_0 = k$ and for all $i > 0$ we have $n_i = k_i = 0$. Now suppose the result holds true up to some arbitrary $n - 1 \geq p - 1$. We prove true for the n case. By the division algorithm, we write $n = ap + n_0$ and $k = bp + k_0$ where $n_0, k_0 \in \{0, \ldots, p-1\}$. We write $a = \sum_{i\geq 0} n_{i+1} p^i$ and $c = \sum_{i\geq 0} k_{i+1} p^i$ in base p. We apply Lemma 3.9 to obtain that:

$$\binom{n}{k} \equiv \binom{ap}{bp}\binom{n_0}{k_0} \pmod{p} \tag{59}$$

Applying the inductive hypothesis to $\binom{ap}{bp}$, we obtain that:

$$\binom{ap}{bp}\binom{n_0}{k_0} \equiv \binom{n_0}{k_0}\prod_{i\geq 1}\binom{n_i}{k_i} \equiv \prod_{i\geq 0}\binom{n_i}{k_i} \pmod{p} \tag{60}$$

Completing the proof. □

Lucas' Congruence for Binomial Coefficients provides a nice corollary, which we will need to prove Sylow's First Theorem.

Corollary 3.29.1. *Let $a, b \in \mathbb{Z}^+$, and let p be a prime that does not divide b. Then p does not divide $\binom{p^a b}{p^a}$.*

Proof. We write $b = \sum_{i\geq 0} b_i p^i$ in base p. The base p expansion of $p^a b = \ldots b_3 b_2 b_1 b_0 000 \ldots 0$, and the base p expansion of $p^a = 1 \ldots 00000$. Without loss of generality, suppose $b_0 \neq 0$. By Lucas' Congruence for Binomial Coefficients, we have:

$$\binom{p^a b}{p^a} \equiv \binom{b_0}{1} \equiv b_0 \neq 0 \pmod{p} \tag{61}$$

□

We now introduce a couple definitions before examining the Sylow Theorems.

Definition 116. Let G be a finite group, and let p be a prime divisor of $|G|$.

(A) A group of order p^α, for $\alpha > 0$, is called a *p-group*. Subgroups of p-groups are called p-subgroups.

(B) If $|G| = p^\alpha m$, where p does not divide m, then a subgroup of order p^α is called a Sylow p-subgroup of G. The set of Sylow p-subgroups of G is denoted $\mathrm{Syl}_p(G)$, and $n_p(G) := |\mathrm{Syl}_p(G)|$. When there is no ambiguity, we may simply right n_p instead of $n_p(G)$.

The Sylow Theorems provide combinatorial tools to count the number of Sylow p-subgroups, as well as characterize structural results. In particular, the Sylow Theorems give us the result that $n_p = 1$ if and only if unique Sylow p-subgroup is normal in G. This result helps us determine if a finite group is simple; that is, a group whose only normal subgroups are 1 and G. We begin with Sylow's First Theorem, which provides for the existence of Sylow p-subgroups for every prime divisor p of a finite group $|G|$. So Sylow's First Theorem is a stronger partial coverse to Lagrange's Theorem than Cauchy's Theorem.

Theorem 3.35 (Sylow's First Theorem)**.** *Let G be a finite group, and let p be a prime divisor of $|G|$. We write $|G| = p^\alpha m$, where $\alpha \in \mathbb{N}$ and p does not divide m. Then there exists a $P \leq G$ of order p^α. That is, $Syl_p(G) \neq \emptyset$.*

Proof. Let $X = \binom{G}{p^\alpha}$, so $|X| = \binom{p^\alpha m}{p^\alpha}$. Now let G act on X by left multiplication. So for $S \in X$, $gS = \{gs : s \in S\}$. By Lucas' Congruence for Binomial Coefficients, we note p does not divide $|X|$. So there exists some orbit of X whose order is not divisible by p. Let $T \in X$ such that $|\mathcal{O}(T)|$ is not divisible by p. Consider $\text{Stab}(T) \leq G$. By the Orbit-Stabilizer Lemma, $|\mathcal{O}(T)| = |G|/|\text{Stab}(T)| = p^\alpha m/|\text{Stab}(T)|$. As p does not divide $|\mathcal{O}(T)|$, $|\text{Stab}(T)| = cp^\alpha$ for some c that divides m. It suffices to show $c = 1$. Let $t \in T$ and consider $\text{Stab}(T)t = \{ht : h \in \text{Stab}(T)\}$, which is a subset of T. So $|\text{Stab}(T)| = |\text{Stab}(T)t| \leq |T| = p^\alpha$. Thus, $\text{Stab}(T) \in \text{Syl}_p(G)$. □

Prior to introducing Sylow's Second Theorem, we prove a lemma known as the p-group Fixed Point Theorem. We leverage this the p-group Fixed Point Theorem in proving both Sylow's Second and Third Theorems.

Theorem 3.36 (p-group Fixed Point Theorem)**.** *Let p be a prime, and let G be a finite group of order p^α for $\alpha > 0$. Let G act on a set X, and let S be the set of fixed points under this action. Then $|G| \equiv |S| \pmod p$. In particular, if p does not divide $|X|$, then $|S| \neq \emptyset$.*

Proof. Let $x \in X \setminus S$. Then $\text{Stab}(x)$ is a proper subgroup of G. Thus, p divides $[G : \text{Stab}(x)]$. Recall that the orbits partition X. Let $x_1, \ldots, x_k \in X \setminus S$ be representatives of the non-fixed point orbits. As the orbits partition X and by the Orbit-Stabilizer Lemma, we have:

$$|X| = |S| + \sum_{i=1}^{k} [G : \text{Stab}(x_i)] \tag{62}$$

As $\sum_{i=1}^{k} [G : \text{Stab}(x_i)]$ is divisible by p, we have $|X| \equiv |S| \pmod p$. If p does not divide $|X|$, then $|S| \neq 0 \pmod p$. So $S \neq \emptyset$ in this case. □

Sylow's Second Theorem follows as a consequence of the p-group Fixed Point Theorem. We show first that every p-subgroup is contained in a Sylow p-subgroup of G. This is done using the action of conjugation. Intuitively, a p-subgroup of G cannot be contained in a subgroup $H \leq G$ where $|H|$ divides m. This is a consequence of Lagrange's Theorem. In particular, Lagrange's Theorem implies that every subgroup of a Sylow p-subgroup is a p-subgroup of G. Sylow's Second Theorem provides a full converse to this statement. We then show that every pair of Sylow p-subgroups are conjugate, which follows from the fact that every p-subgroup of G is contained in a Sylow p-subgroup of G.

Theorem 3.37 (Sylow's Second Theorem)**.** *Let G be a finite group, and let p be a prime divisor of $|G|$. We write $|G| = p^\alpha m$, where $\alpha \in \mathbb{N}$ and p does not divide m. If P is a Sylow p-subgroup of G and Q is a p-subgroup of G, then there exists a $g \in G$ such that $Q \leq gPg^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate .*

Proof. Let $P \in \text{Syl}_p(G)$. We consider the left cosets of G/P. Let Q act on G/P by left-multiplication. Observe that p does not divide $[G : P] = |G/P|$. By the previous theorem, there exists a fixed point of this action. Let gP be such a fixed point. So for every $q \in Q$, $qgP = gP$, so $g^{-1}qgP = P$. That is, $g^{-1}Qg \subset P$; or equivocally, $Q \subset gPg^{-1}$. To show that all Sylow p-subgroups are conjugate, we utilize the above argument setting Q to be a Sylow p-subgroup of G. □

Sylows's Third Theorem provides us a way to determine the number of Sylow p-subgroups in a finite group G. This is particularly useful in deciding if a finite group has a normal subgroup of given prime power order. In turn, we have a combinatorial tool to help us decide if a finite group is simple. Before proving Sylow's Third Theorem, we introduce a helpful lemma.

Lemma 3.10. *Let G be a finite group, and let H be a p-subgroup of G. Then $[N_G(H) : H] \equiv [G : H] \pmod p$.*

Proof. Let H act on the set of left cosets G/H by left multiplication. The set of fixed points are of the form gH where $hgH = gH$ for all $h \in H$. This is equivalent to $g^{-1}hg \in H$ for all $h \in H$. This is equivalent to $g^{-1}Hg = H$. So each fixed point gH is contained in $N_G(H)$. Let S be the set of fixed points. Then $|N_G(H)| = |H| \cdot |S|$. By the p-group fixed point theorem, $[G : H] = |G/H| \equiv |S| \pmod{p}$. It follows immediately that $[N_G(H) : H] \equiv |S| \pmod{p}$, so $[N_G(H) : H] \equiv [G : H] \pmod{p}$ as desired. □

Theorem 3.38 (Sylow's Third Theorem)**.** *Let G be a finite group, and let p be a prime divisor of $|G|$. We write $|G| = p^\alpha m$, where $\alpha \in \mathbb{N}$ and p does not divide m. The number of Sylow p-subgroups of G, $n_p \equiv 1 \pmod{p}$. Furthermore, $n_p = [G : N_G(P)]$ for any $P \in Syl_p(G)$. So n_p divides m.*

Proof. By Sylow's Second Theorem, we have that all Sylow p-subgroups are conjugate. So by Proposition 3.26, $n_p = [G : N_G(P)]$ for any $P \in \mathrm{Syl}_p(G)$. In particular, we have:

$$m = [G : P] = [G : N_G(P)] \cdot [N_G(P) : P] = n_p \cdot [N_G(P) : P] \tag{63}$$

By the previous lemma, $m = [G : P] \equiv [N_G(P) : P] \pmod{p}$. As $m = n_p \cdot [N_G(P) : P]$, we have that $m \cdot n_p \equiv m \pmod{p}$. As p is prime and $n_p > 0$, $n_p \equiv 1 \pmod{P}$. □

The Sylow Theorems have a nice corollary, which allows us to characterize normal Sylow p-subgroups.

Corollary 3.29.2. *A Sylow p-subgroup P in the finite group G is normal in G if and only if $n_p = 1$.*

Proof. Suppose first $P \trianglelefteq G$. Then $N_G(P) = G$. As all Sylow p-subgroups are conjugate, the conjugacy class of P contains only P. This is equivalent to $n_p = 1$. □

3.4.4 Applications of Sylow's Theorems

The Sylow Theorems can be leveraged to provide deep insights into the structure of finite groups, particularly as it pertains to the existence of normal subgroups. This in turn allows us to better understand the structures of individual groups, large classes of finite groups, and to classify groups of a given order. We consider some examples. Let G be a finite group of order $p^\alpha m$ where p is a prime that does not divide m. Informally, if p^α is sufficiently large, then we have a unique Sylow p-subgroup

Proposition 3.30. *Let p be prime, $r \in \mathbb{Z}^+$, and $m \in [p-1]$. Let G be a group of order mp^r. Then G is not simple (that is, G has a proper normal subgroup).*

Proof. By Sylow's Third Theorem, $n_p \equiv 1 \pmod{p}$ and n_p divides m. Since $m < p$, this forces $n_p = 1$. So $P \in \mathrm{Syl}_p(G)$ is a proper normal subgroup of G. □

We now examine groups of order pq, where p and q are primes and $p < q$.

Proposition 3.31. *Let G be a group of order pq, where p and q are primes with $p < q$. Let $P \in Syl_p(G)$ and $Q \in Syl_q(G)$. Then $Q \trianglelefteq G$. If $q \neq 1 \pmod{p}$, then $P \trianglelefteq G$ as well and G is cyclic.*

Proof. By Sylow's Third Theorem, $n_q \equiv 1 \pmod{q}$ and n_q divides p. So $n_q \in \{1, p\}$. As $p < q$, $n_q = 1$, so $Q \trianglelefteq G$. Now suppose $q \neq 1 \pmod{p}$. We have that $n_p \in \{1, q\}$ as q is prime. As $q \neq 1 \pmod{p}$ by assumption, we have that $n_p = 1$. So $P \trianglelefteq G$. As $|P| = p$, P is cyclic. By Theorem 3.33, $G/C_G(P) \leq \mathrm{Aut}(P)$. As p is prime and P is cyclic, $|\mathrm{Aut}(P)| = p - 1$. By Lagrange's Theorem, neither p nor q divide $p - 1$. So $C_G(P) = G$, which implies that $P \leq Z(G)$. Now G contains elements $g \in P$ of order p and $h \in Q$ of order q. As $P \leq Z(G)$, $gh = hg$. So $|gh| = pq$. We conclude that $G \cong \mathbb{Z}_{pq}$. □

We next show that every group of order 30 has a subgroup isomorphic to $\mathbb{Z}_{15}$. Observe that if G is a group of order 30, then $[G : \mathbb{Z}_{15}] = 2$, so $\mathbb{Z}_{15}$ is necessarily a normal subgroup of G.

Proposition 3.32. *Let G be a group of order 30. Then $\mathbb{Z}_{15} \trianglelefteq G$.*

Proof. Note that $|G| = 2 \cdot 3 \cdot 5$. By Sylow's Third Theorem, we have that $n_3 \equiv 1 \pmod 3$ and $n_3 \big| 10$. So $n_3 \in \{1, 10\}$. By similar argument, $n_5 \in \{1, 6\}$. Suppose to the contrary that no Sylow-3 or Sylow-5 subgroup is normal in G. Then $n_3 = 10$ and $n_5 = 6$. Each Sylow-5 subgroup contains four non-identity elements, and each Sylow-3 subgroup contains two non-identity elements. This provides 20 elements of order 3 and 24 elements of order 4. However $20 + 24 > 30$, a contradiction. So there exists a normal Sylow-3 subgroup or normal Sylow-5 subgroup in G. Let $P \in \mathrm{Syl}_3(G)$ and $Q \in \mathrm{Syl}_5(G)$. By proposition 3.31, $PQ \leq G$. As $[G : PQ] = 2$, $PQ \trianglelefteq G$. So by Proposition 3.31, $PQ \cong \mathbb{Z}_{15}$. □

We next show that there are no simple groups of order 12. We will use this result to study simple groups of order 60. In particular, this result will help us show that A_5 is simple.

Proposition 3.33. *There is no simple group of order 12.*

Proof. By Sylow's Third Theorem, $n_3 \equiv 1 \pmod 3$ and $n_3 \in \{1, 4\}$. Similarly, $n_2 \equiv 1 \pmod 2$ and $n_2 \in \{1, 3\}$. If $n_3 = 1$, then we are done. Suppose instead that $n_3 = 4$. As every Sylow-3 subgroup is normal, each Sylow-3 subgroup has trivial intersection. This provides for 8 elements of order 3 and the identity. So necessarily, there exists one Sylow-2 subgroup, which has order 4. This accounts for the remaining three elements of order 2 or order 4. So there exists a non-trivial normal subgroup in a group of order 12. □

Proposition 3.34. *If G is a group of order 60 and G has more than one Sylow-5 subgroup, then G is simple.*

Proof. Suppose to the contrary that G has more than one Sylow-5 subgroup and G is not simple. Let $H \trianglelefteq G$ be a proper subgroup of G, with $H \neq 1$. By Sylow's Third Theorem, $n_5 = 6$. Let $P \in \mathrm{Syl}_P(G)$. So $|N_G(P)| = 6$ as $n_5 = [G : P] = 10$. Now suppose $5 \big| |H|$. Then H contains a Sylow-5 subgroup Q of G. As H is normal, H necessarily contains all the conjugates of Q, which are the 6 Sylow-5 subgroups of G. So $|H| > 25$, which implies $|H| = 30$. However, by Proposition 3.32, H contains a unique Sylow-5 subgroup, which is in turn a Sylow-5 subgroup of G. This contradicts the assumption that $n_5 = 6$. So 5 does not divide H.

If $|H| = 6$, then there is a single Sylow-3 subgroup in H which is also a Sylow-3 subgroup of G, which is normal in G (as H contains all the conjugates of this Sylow-3 subgroup). By Proposition 3.33, if $|H| = 12$, then H contains a normal subgroup which is also a normal Sylow subgroup of G. So without loss of generality, we have a normal subgroup of K of G with order $|K| \in \{2, 3, 4\}$. So $|G/K| \in \{15, 20, 30\}$. By the preceeding paragraph, there exists $\overline{P} \trianglelefteq |G/K|$ with $|\overline{P}| = 5$. Let $\phi : G \to G/K$ be the natural projection homomorphism sending $g \mapsto gK$. By the Lattice Isomorphism Theorem, $P := \phi^{-1}(\overline{P}) \trianglelefteq G$. As $\overline{P}$ has order 5, $|P|$ is necessarily divisible by 5. This contradicts the previous paragraph. So G is necessarily simple. □

Corollary 3.34.1. *A_5 is simple.*

Proof. Observe that $\langle (1, 2, 3, 4, 5) \rangle$ and $\langle (1, 3, 2, 4, 5) \rangle$ are two distinct Sylow-5 subgroups of A_5. So by Proposition 3.34, A_5 is simple. □

We conclude with the following remark. In many of these counting arguments, we used the fact that two Sylow-p subgroups intersected trivially. This holds true for cyclic subgroups; however, when p^α for $\alpha \geq 2$, two Sylow-p subgroups may have non-trivial intersection. In these cases, the problems are not as susceptible to counting arguments.

3.4.5 Algebraic Combinatorics- Pólya Enumeration Theory

TODO

4 Turing Machines and Computability Theory

In this section, we explore the power and limits of computation without regards to resource usage. That is, we seek to study which problems computers can and cannot solve, given unlimited time and space. More succinctly, the goal is to provide a model of computation powerful enough to be representative of an algorithm. The primitive automata in previous sections motivate this problem. Finite state automata compute memoryless algorithms. While regular languages are quite interesting and useful, finite state automata fail to decide context free languages such as $L_1 = \{0^n 1^n : n \in \mathbb{N}\}$. To this end, we add an infinite stack to the finite state automaton, where only the head of the stack may be accessed. We refer to this modified finite state automaton as a *pushdown automaton*, which accepts precisely context-free languages. We again find a language beyond the limits of pushdown automata- $L_2 = \{0^n 1^n 2^n : n \in \mathbb{N}\}$, which does not satisfy the Pumping Lemma for Context-Free Languages.

However, it is quite simple to design an algorithm to verify if an input string is of the form prescribed by L_1 or L_2. In fact, this would be a reasonable question in an introductory programming class. So clearly, it is quite feasible to decide if a string is in L_1 or L_2. Thus, both of our models of computation, the finite state automata and pushdown automata, are unfit to represent an algorithm in the most general sense. To this end, we introduce a Turing Machine, the model of computation which serves as the litmus test for which problems are solvable by computational means.

It is also important to note that there are numerous models of computation that are vastly different from the Turing Machine; but with the exception of hypercomputation model, none are more powerful than the Turing Machine. The Church-Turing Thesis conjectures that no model of computation is more powerful than the Turing Machine. As hypercomputation is not thus far physically realizable, the Church-Turing Thesis remains essentially an open problem.

4.1 Standard Deterministic Turing Machine

The standard deterministic Turing machine shares many similarities with the finite state automaton. Just like the finite state automaton, the Turing Machine solves decision problems; that is, it attempts to decide if a string is in a given language. Furthermore, both have a finite set of states. The next state of each machine is determined by the given character being parsed and the current state. Unlike a finite state automaton though, a Turing Machine can both read and write to the tape head. Furthermore, the Turing Machine also has unlimited memory to the right with a fixed end at the left, and the tape head can move both left and right. This allows us to parse characters multiple times and develop the notion of iteration in our computations. Lastly, the Turing Machine has explicit accept and reject states, which take effect immediately upon being reached. Formally, we define the standard Turing Machine as follows.

Definition 117 (Deterministic Turing Machine)**.** A Turing Machine is a 7-tuple $(Q, \Sigma, \Gamma, \delta, q_0, q_{\text{accept}} q_{\text{reject}})$ where Q, Σ, Γ are all finite sets and:

- Q is the set of states.
- Σ is the input alphabet, not containing the blank symbol β.
- Γ is the tape alphabet, where $\beta \in \Gamma$ and $\Sigma \subset \Gamma$.
- $\delta : Q \times \Gamma \to Q \times \Gamma \times \{\text{L, R}\}$ is the transition function, which takes a state and tape character and returns the new state, the tape character to write to the current cell, then a direction for the tape head to move one cell to the left or right (denoted by L or R respectively).
- $q_0 \in Q$, the initial state.
- $q_{\text{accept}} \in Q$, the accept state.
- $q_{\text{reject}} \in Q$, the reject state where $q_{\text{reject}} \neq q_{\text{accept}}$.

Let's now unpack the Turing Machine some more. Conceptually, a standard Turing Machine starts with an input string, which is written to an initially blank tape starting at the far left cell. It then executes starting at the initial state q_0, transitioning to other states as defined by the function δ, based on the current state and input from the given tape cell. If evaluating this string in such a manner results in the Turing Machine reaching its accepting halting state q_{accept}, then the Turing Machine is said to accept the input string. If the Turing Machine does not visit q_{accept}, then it does not accept the given input string. However, if it does not explicitly visit q_{reject}, then the Turing Machine does not reject the input string; rather, it enters into an infinite loop. The language of a Turing Machine M, $L(M)$, is the set of strings the Turing Machine M accepts. We introduce two notions of language acceptance.

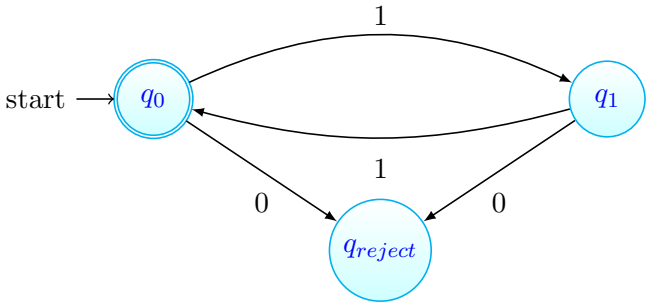
Definition 118 (Recursively Enumerable Language)**.** A language L is said to be *recursively enumerable* if there exists a deterministic Turing Machine M such that $LM) = L$. Note that if $\omega \notin L$, the machine M need not halt on ω.

Definition 119 (Decidable Language)**.** A language L is said to be *decidable* if L is there exists some Turing Machine M such that $L(M) = L$ and M halts on all inputs. We say that M *decides* L.

Remark: Every decidable language is clearly recursively enumerable. The converse is not true, and this will be shown later with the undecidabilitiy of the Halting problem.

We now consider an example of a Turing Machine.

Example 120. Let $\Sigma = \{0, 1\}$ and let $L = \{1^{2k} : k \in \mathbb{N}\} = (11)^*$, so L is regular. A finite state automaton can easily be constructed to accept L. Such a FSM diagram is provided below.



Now let's construct a Turing Machine to accept $(11)^*$. The construction of the Turing Machine, is in fact, almost identical to that of the finite state automaton. The Turing Machine will start with the input string on the far-left of the tape, with the tape head at the start of the string. The Turing Machine has $Q = \{q_0, q_1, q_{reject}, q_{accept}\}$, $\Sigma = \{0, 1\}$, and $\Gamma = \{0, 1, \beta\}$. Let the Turing Machine start at q_0 and read in the character under the tape head. If it is not a 1 or the empty string, enter q_{reject} and halt. Otherwise, if the string is empty, enter q_{accept} and halt. On the input of a 1, transition to q_1 and move the tape head one cell to the right. While in q_1, read in the character on the tape head. If it is a 1, transition to q_0 and move the tape head one cell to the right. Otherwise, enter q_{reject} and halt. The Turing Machine always halts, and accepts the string if and only if it halts in state q_{accept}.

Observe the similarities between the Turing Machine and finite state automaton. The intuition should follow that any language accepted by a finite state automaton (ie., any regular language) can also be accepted by a Turing Machine. Formally, the Turing Machine simulates the finite state automaton by omitting the ability to write to the tape or move the tape head to the left. We now consider a second example of a Turing Machine accepting a context-free language.

Example 121. Let $\Sigma = \{0, 1\}$ and let $L = \{0^n 1^n : n \in \mathbb{N}\}$. So L is context-free. We omit the construction of a pushdown automaton, but simply provide a Turing Machine to accept this language. The Turing Machine has a tape alphabet of $\Gamma = \{0, 1, \hat{0}, \hat{1}\}$ and set of states $Q = \{q_0, q_{\text{find-1}}, q_{\text{find-0}}, q_{\text{validate}}, q_{\text{accept}}, q_{\text{reject}}\}$. Conceptually, rather than using a stack as a pushdown automaton would, the Turing Machine will use its tape head.

Intuitively, the Turing Machine starts with a 0 and marks it, then moves the tape head to the right one cell at a time looking for a corresponding 1 to mark. Once it finds and marks the 1, the Turing Machine then moves the tape head to the left one cell at a time searching for the next unmarked 0 to mark. It then repeats this procedure, looking for another unmarked 1 to mark. If it finds an unpaired 0 or 1, it rejects the string. This procedure repeats until either the string is rejected, or we mark all pairs of 0's and 1's. In the latter case, the Turing Machine accepts the string.

So initially the Turing Machine starts at q_0 with the input string on the far-left of the tape, with the tape head above the first character. If the string is empty, the Turing Machine enters q_{accept} and halts. If the first character is a 1, the Turing Machine enters q_{reject} and halts. If the first character is 0, the Turing Machine replaces it with $\hat{0}$. It then moves the tape head to the right one cell and transitions to state $q_{\text{find-1}}$.

At state $q_{\text{find-1}}$, the Turing Machine moves the tape head to the right and stays at $q_{\text{find-1}}$ for each $0, \hat{0}$, or 1 character it reads in and writes back the character it parsed. If at $q_{\text{find-1}}$ and the Turing Machine reads 1, then it writes $\hat{1}$ to the tape, moves the tape head to the left, and transitions to $q_{\text{find-0}}$. If no 1 is found, the Turing Machine enters q_{reject} and halts.

At state $q_{\text{find-0}}$, the Turing Machine moves the tape head to the left and stays at $q_{\text{find-0}}$ until it reads in 0. If the Turing Machine reads in 0 at state $q_{\text{find-0}}$, it replaces the 0 with $\hat{0}$. It then moves the tape head to the right one cell and transitions to state $q_{\text{find-1}}$. If no 0 is found once we have reached the far-left cell, the Turing Machine transitions to state q_{validate}.

At state q_{validate}, the Turing Machine transitions to the right one cell at a time while staying at q_{validate}. If it encounters any 1, it enters q_{reject}. Otherwise, the Turing Machine enters q_{accept} once reading in β.

Remark: Now that we provided formal specifications for a couple Turing Machines, we provide a more abstract representation from here on out. We are more interested in studying the power of Turing Machines rather than the individual state transitions, so high level procedures suffice for our purposes. This high level procedure from the above example provides sufficient detail to simulate the Turing Machine. So for our purposes, this level of detail is sufficient:

"*Intuitively, the Turing Machine starts with a* 0 *and marks it, then moves the tape head to the right one cell at a time looking for a corresponding* 1 *to mark. Once it finds and marks the* 1*, the Turing Machine then moves the tape head to the left one cell at a time searching for the next unmarked* 0 *to mark. It then repeats this procedure, looking for another unmarked* 1 *to mark. If it finds an unpaired* 0 *or* 1*, it rejects the string. This procedure repeats until either the string is rejected, or we mark all pairs of* 0*'s and* 1*'s. In the latter case, the Turing Machine accepts the string.*"

We now introduce the notion of a configuration and provides a concise representation of the Turing Machine's state, tape head position, and the string written to the tape. Aside from providing a concise representation of the Turing Machine, configurations are important in studying how Turing Machines work. In particular, certain results in space complexity are derived by enumerating the possible configurations of a Turing Machine on an arbitary input string. We formally define a Turing configuration below.

Definition 120 (Turing Machine Configuration)**.** Let M be a Turing Machine run on the string s. A *Turing Machine Configuration* is a string $\omega \in \Gamma^* Q \Gamma^*$, where Q is the current state of M, which we overlay on the character of s highlighted by the tape head. The remaining characters in ω are the characters of the input string s which M is parsing. The *start configuration* of M is $q_0 s_1 \dots s_n$ (where $n = |s|$). The *accept configuration* is a Turing Machine configuration where the state is q_{accept}, while in a *rejecting configuration* is a configuration where the state is q_{reject}. The accepting and rejecting configurations are both halting configurations.

Example 122. Recall the Turing Machine in Example 91. We consider the input string 1111. The initial configuration is $q_0 111$. The subsequent configuration is $1 q_1 11$.

This example motivates the *yields relation*, which enables us to textually represent a sequence of Turing com-

putations on a given input string.

Definition 121 (Yields Relation)**.** Let M be a Turing Machine parsing the input string ω. The *yields relation* is a binary relation on $\Gamma^* Q \Gamma^*$. We say that the configuration C_i *yields* the configuration C_{i+1} if C_{i+1} can be reached from a single step (or invocation of the transition function) from C_i. We denote this relation as $C_i \vdash C_{i+1}$.

Example 123. In running the Turing Machine from Example 91 on 1111, we have the sequence of configurations: $q_0 111 \vdash 1 q_1 11$. Similarly, $1 q_1 11 \vdash 11 q_0 1$. We then have $11 q_0 1 \vdash 111 q_1$, and in turn $111 q_1 \vdash 1111 q_{\text{accept}}$, where $1111 q_{\text{accept}}$ is an accepting configuration.

4.2 Variations on the Standard Turing Machine

In automata theory, one seeks to understand the robustness of a model of computation with respect to variation. That is, does the introduction of nuances such as non-determinism or multiple tapes allow for a more powerful machine? Recall that deterministic and non-deterministic finite state automata are equally powerful, as they each accept precisely regular languages. When considering context-free languages, we see that non-deterministic pushdown automata are strictly more powerful than deterministic pushdown automata. The Turing Machine is quite a robust model, in the sense that the standard deterministic model accepts and decides precisely the same languages as the multitape and non-deterministic variants. It should be noted that one model may actually be more efficient than another. In regards to language acceptance and computability, we ignore issues of efficiency and complexity. However, the same techniques we use to show that these models are equally powerful can be leveraged to show that two models of computation are equivalent both with regards to power and some measure of efficiency. That is, to show that the two models solve the same set of problems using a comparable amount of resources (e.g., polynomial time). This is particularly important in complexity theory, but we also leverage these techniques when showing Turing Machines equivalent to other models such as (but not limited to) the RAM model and the λ-calculus.

We begin by introducing the Multitape Turing Machine.

Definition 122 (Multitape Turing Machine)**.** A *k-tape Turing Machine* is an extension of the standard deterministic Turing Machine in which there are k tapes with infinite memory and a fixed beginning. The input initially appears on the first tape, starting at the far-left cell. The transition function is the addition difference, allowing the k-tape Turing Machine to simultaneously read from and write to each of the k-tapes, as well as move some or all of the tape cells. Formally, the transition function is given below:

$$\delta : Q \times \Gamma^k \to Q \times \Gamma^k \times \{\text{L, R, S}\}^k$$

The expression:

$$\delta(q_i, a_1, \ldots, a_k) = (q_j, b_1, \ldots, b_k, L, R, S, \ldots, R)$$

Indicates that the TM is on state q_i, reading a_m from tape m for each $m \in [k]$. Then for each $m \in [k]$, the TM writes b_m to the cell in tape m highlighted by its tape head. The mth component in $\{\text{L, R, S}\}^k$ indicates that the mth tape head should move left, right, or remain stationary respectively.

Our first goal is to show that the standard deterministic Turing Machine is equally as powerful as the k-tape Turing Machine, for any $k \in \mathbb{N}$. We need to show that the languages accepted (decided) by deterministic Turing Machines are exactly those languages accepted (decided) by the multitape variant. The initial approach of a set containment argument is correct. The details are not as intuitively obvious. Formally, we show that for any multitape Turing Machine, there exists an deterministic Turing Machine; and for any deterministic Turing Machine, there exists an equivalent multitape Turing Machine. In other words, we show how one model simulates the other and vice-versa. This implies that the languages accepted (decided) by one model are precisely the languages accepted (decided) by the other model.

Theorem 4.1. *A language is recursively enumerable (decidable) if and only if some multitape Turing Machine accepts (decides) it.*

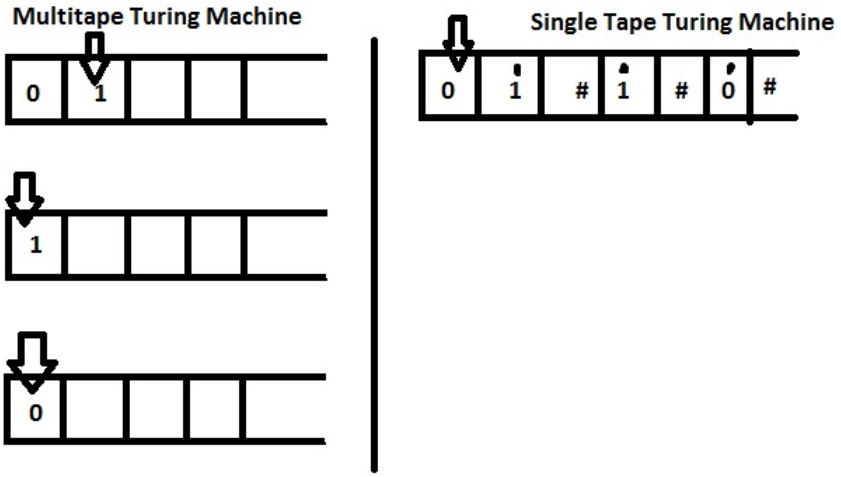
Proof. We begin by showing that the multitape Turing Machine model is at least as power as the standard deterministic Turing Machine model. Clearly, a standard deterministic Turing Machine is a 1-tape Turing Machine. So every language accepted (decided) by a standard deterministic Turing Machine is also accepted (decided) by some multitape Turing Machine.

Conversely, let M be a multitape Turing Machine with k tapes. We construct a standard determnistic Turing Machine M' to simulate M, which shows that $L(M') = L(M)$. As M has k-tapes, it is necessary to represent the strings on each of the k tapes on a single tape. It is also necessary to represent the placement of each of the k tape heads of M on the one tape of M'. This is done by using a special marker. For each symbol $c \in \Gamma(M)$, we include c and $\hat{c}$ in Γ', where $\hat{c}$ indicates a tape head on M is on the character c. We then have a special delimiter symbol $\#$, which separates the strings on each of the k tapes. So $|\Gamma(M')| = 2|\Gamma(M)| + 1$. M' simulates M in the following manner:

- M' scans the tape from the first delimiter to the last delimiter to determine which symbols are marked as under the tape heads on M.
- M' then evaluates the transition function of M, then makes a second pass along the tape to update the symbols on the tape.
- If at any point, the tape head of M' falls on a delimiter symbol $\#$, M would have reached the end of that specific tape. So M' shifts the string, cell by cell, starting at the current delimiter inclusive. A blank symbol is then overwritten on the delimiter.

Thus, M' simulates M. So any language accepted (decided) by a multitape Turing Machine is accepted (decided) by a single tape Turing Machine. □

Below is an illustration of a multitape Turing Machine an an equivalent single tape Turing Machine.



Remark: If the k-tape Turing Machine takes T steps, then each tape uses at most $T+1$ cells. So the equivalent one-tape deterministic Turing Machine constructed in the proof of Theorem 4.1 takes $(k \cdot (T+1))^2 = O(T^2)$ steps.

We now introduce the non-deterministic Turing Machine. The non-deterministic Turing Machine has a single, infinite tape with an end at the far-left. Its sole difference with the deterministic Turing Machine is the transition function.

Definition 123 (Non-Deterministic Turing Machine)**.** A non-deterministic Turing Machine is defined identically as a standard deterministic Turing Machine, but with the transition function of the form:

$$\delta : Q \times \Gamma \to 2^{Q \times \Gamma \times \{L,R\}}$$

We now show that the deterministic and non-deterministic variants are equally powerful. The proof for this is by simulation. Before introducing the proof, let's conceptualize this. Earlier in this section, a graph theory intuition was introduced for understanding the definition of what it means for a string to be accepted by a non-deterministic Turing Machine. That definition of string acceptance dealt with the existence of a choice string such that the non-deterministic Turing Machine would reach the accept state q_{accept} from the starting state q_0. The graph theory analog was that there existed a path for the input string from q_0 to q_{accept}.

So the way a deterministic Turing Machine simulates a non-deterministic Turing Machine is through, essentially, a breadth-first search. More formally, what actually happens is that a deterministic multitape Turing Machine is used to simulate a non-deterministic Turing Machine. It does this by generating choice strings in lexicographic order and simulating the non-deterministic Turing Machine on each choice string until the string is accepted or all the possibilities are exhausted.

Given the non-deterministic Turing Machine has a finite number of transitions, there are a finite number of choice input strings to generate. Thus, a multitape deterministic Turing Machine will always be able to determine if an input string is accepted by the non-deterministic Turing Machine. It was already proven that a multitape Turing Machine can be simulated by a standard deterministic Turing Machine, so it follows that any language accepted by a non-deterministic Turing Machine can also be accepted by a deterministic Turing Machine.

Theorem 4.2. *A language is recursively enumerable (decidable) if and only if it is accepted (decided) by some non-deterministic Turing Machine.*

Proof. A deterministic Turing Machine is clearly non-deterministic. So it suffices to show that every non-deterministic Turing Machine has an equivalent deterministic Turing Machine. From Theorem 4.1, it suffices to construct a multitape Turing Machine equivalent for every non-deterministic Turing Machine. The proof is by simulation. Let M be a non-deterministic Turing Machine.

We construct a three-tape Turing Machine M' to simulate all possibilities. The first tape contains the input string and is used as a read-only tape. The second tape is used to simulate M, and the third tape is the enumeration tape in which we enumerate the branches of the non-deterministic Turing Machine. Let:

$$b = \max_{q \in Q, a \in \Gamma} |\delta_M(q, a)|$$

The tape alphabet of M' is $\Gamma(M) \cup [b]$. On the third tape of M', we enumerate strings over $[b]^n$ in lexical order, where n is the length of the input string. At state i in the computation, we utilize the transition indexed by the number on the ith cell on the third tape.

Formally, M' works as follows:

1. M' is started with the input ω on the first tape.
2. We then copy the input string to the second tape and generate 0^ω.
3. Simulate M on ω using the choice string on ω. If at any point, the transition specified by the third tape is undefined (which may occur if too few choices are available), we terminate the simulation of M and generate the next string in lexical order on the third tape. We then repeat step (3).
4. M' accepts (rejects) ω if and only some simulation of M on ω accepts (rejects) ω.

By construction, $L(M') = L(M)$, yielding the desired result. □

4.3 Turing Machine Encodings

TODO

4.4 Chomsky Heirarchy and Some Decidable Problems

Thus far, we have introduced the Turing Machine as a model of computation and studied it from the perspective of automata theory. The goal of computability theory is to study the power and limits of computation. In this section, we explore problems that Turing Machines can effectively solve; that is, decidable languages.

Thus far, we have several classes of languages: regular, contex-free, decidable, and recursively enumerable languages. We have three relations that are easy to see:

1. Every regular language is context-free.
2. Every regular language is decidable.
3. Every decidable language is recursively enumerable.

These relationships are captured by the *Chomsky Heirarchy*, named for linguist Noam Chomsky. The Chomsky Heirarchy contains four classes of formal languages, with a strict increasing subset relation between them. Each class of formal language is characterized by the class of machines deciding them (or equivocally, the class of grammars generating them). The missing class of language is the set of context-sensitive languages. We mention them here for completeness, but will not explore them much further. Context-sensitive languages are accepted by linear bounded automata, which informally are Turing Machines with finite tape heads. It is thus easy to see that every context-sensitive language is recursively enumerable. In fact, every context-sensitive language is also decidable. We also note that every context-free language is also context-sensitive.

In order to see that every regular language is decidable, we simply use a Turing Machine to simulate a finite state automaton. Given a regular language L, we construct a deterministic Turing Machine to decide L quite easily. Let D be the DFA accepting L. Without loss of generality, suppose D has precisely one accept state. We let M be the corresponding Turing Machine, with $Q_M = Q_D, \Sigma_D = \Sigma_D$; and for each $((q_i, a), q_j) \in \delta_D$, we include $((q_i, a), (q_j, a, L)) \in \delta_M$. So M simulates D, and $L(M) = L$. We rephrase this notion with the following theorem, which will be of use later.

Theorem 4.3. *Let $A_{DFA} = \{\langle D, w\rangle : D \text{ is a DFA that accepts } w\}$. A_{DFA} is decidable.*

Proof. We construct a Turing Machine M to decide A_{DFA} as follows. On input $\langle D, w\rangle$, M simulates D on w. M accepts $\langle D, w\rangle$ if and only if D accepts w. As every FSM is a decider, it follows that M is also a decider. So M decides A_{DFA}. □

Remark: We similarly define $A_{\text{NFA}} = \{\langle N, w\rangle : N \text{ is an NFA that accepts } w\}$. A_{NFA} is decidable. We apply the NFA to DFA algorithm, then utilize the decider for A_{DFA}.

We use a similar argument to decide if a regular expression recognizes a given string. Using a programmer's intuition, we utilize existing algorithms and theory developed in the exposition on regular languages.

Theorem 4.4. *Let $A_{REX} = \{\langle R, w\rangle : R \text{ is a regular expression that matches the string } w\}$. A_{REX} is decidable.*

Proof. We construct a Turing Machine M to decide A_{REX} as follows. M begins by converting R to an ϵ-NFA N using Thompson's Reconstruction Algorithm. M then converts N to an NFA N' without ϵ transitions using the procedure outlined in our exposition on automata theory. From there, M simulates the decider S for A_{NFA} on $\langle N', w\rangle$ and accepts if and only if S accepts; and rejects if and only if S rejects. So M decides A_{REX}. □

We next consider two important problems: (1) Given a DFA D, is $L(D) = \emptyset$; and (2) Given two DFAs A and B, does $L(A) = L(B)$? Regular languages are decidable; so for every $w \in \Sigma^*$, some Turing Machine decides

if w is in the corresponding regular language L. However, for other classes of decidable languages (such as context-sensitive languages), it is undecidable whether the corresponding automaton accepts no string, which makes testing for language equality an undecidable problem for that class of language. With this in mind, we proceed with our next results:

Theorem 4.5. *Let $E_{DFA} = \{\langle D\rangle : D \text{ is a DFA and } L(D) = \emptyset\}$. E_{DFA} is decidable.*

Proof. We construct a Turing Machine M to decide E_{DFA} as follows. M begins by labeling the start state. Then while no new states have been marked, we mark any state with an incoming transition from an already marked state. D accepts some string if and only if some accept state was marked. So M accepts if no accept state has been reached, and rejects otherwise. □

We show next that testing for language equality is decidable, provided we have two regular languages. Recall that $L_1 = L_2$ if and only if $L_1 \triangle L_2 = \emptyset$. In order to prove this, we leverage closure properties of regular langauges (and the FSMs constructed in the proofs of these properties) to construct a DFA recognizing $L_1 \triangle L_2$, then defer to the decider for E_{DFA}.

Theorem 4.6. *Let $EQ_{DFA} = \{\langle A, B\rangle : A, B \text{ are DFAs and } L(A) = L(B)\}$. EQ_{DFA} is decidable.*

Proof. We construct a Turing Machine M to decide EQ_{DFA}. Recall that:

$$L(A) \triangle L(B) = (L(A) \cap \overline{L(B)}) \cup (\overline{L(A)} \cap L(B))$$

As regular languages are closed under union, intersection, and complementation, we construct a DFA for C using the constructions given in the proofs of these closure properties. So $L(C) = \emptyset$ if and only if $L(A) \triangle L(B) = \emptyset$. And $L(A) = L(B)$ if and only if E_{DFA} accepts $\langle C\rangle$. So M accepts $\langle A, B\rangle$ if and only if E_{DFA} accepts $\langle C\rangle$, and M rejects otherwise. So M decides EQ_{DFA}. □

We now provide analogous results for context-free languages as for regular languages. These results culminate with the following result: every context-free language is decidable. We will need a couple facts about context-free languages:

- Every context-free language has a context-free grammar which generates the language.
- Every context-free grammar can be written in Chomsky Normal Form. Any non-empty string ω of length n generated by the grammar is done so using a derivation of $2n - 1$ steps.

We use these facts to decide a language of ordered pairs, with each pair containing a context-free grammar and a string it generates.

Theorem 4.7. *Let $A_{CFG} = \{\langle G, w\rangle : G \text{ is a context-free grammar that generates } w\}$. A_{CFG} is decidable.*

Proof. We construct a Turing Machine M as follows. On input $\langle G, w\rangle$, where G is a context-free grammar and w is a string, M begins by converting G to an equivalent grammar in Chomsky Normal Form. If $n > 0$, then M enumerates all derivations with $2n - 1$ steps, where $n = |w|$. Otherwise, M enumerates all derivations with a single step. M accepts $\langle G, w\rangle$ if and only if one such derivation generates w. Otherwise, M rejects $\langle G, w\rangle$. So M decides A_{CFG}. □

We next show that it is quite easy to decide if $L(G) = \emptyset$ for an arbitrary context-free grammar G. The proof of this next theorem utilizes a dynamic programming algorithm which is modeled after the algorithm to construct a Huffman encoding tree.

Theorem 4.8. *Let $E_{CFG} = \{\langle G\rangle : G \text{ is a context-free grammar and } L(G) = \emptyset\}$. E_{CFG} is decidable.*

Proof. We construct a Turing Machine M, which utilizes a dynamic programming procedure. We begin by mark each terminal symbol in the grammar G. For the recursive step, we mark a non-terminal symbol A if there exists a rule $A \to x_1x_2x_3 \dots x_k$ where for each i, x_i was labeled at some previous iteration. The algorithm terminates if no additional symbol is marked at the last iteration. $L(G) \neq \emptyset$ if and only if S is marked (as tracing along the computation yields a derivation from S to some string of terminals). So M accepts G if and only if S is unmarked, and G rejects otherwise. □

We now show that every context-free language is decidable.

Theorem 4.9. *Let L be a context-free langauge. L is decidable.*

Proof. We construct a Turing Machine M to decide L as follows. Let S be the Turing Machine constructed in the proof of Theorem 4.3, and let G be a context-free grammar generating L. On input ω, M simulates S on $\langle G, \omega \rangle$ and accepts ω if and only if S accepts $\langle G, \omega \rangle$. M rejects ω otherwise. So M decides L, as S decides A_{CFG}. □

4.5 Undecidability

In the last section, we examined several problems which Turing Machines can decide, or solve. This section examines the limits of computation as a means to solve problems. This is important for several reasons. First, problems that cannot be solved need to be simplified to a formulation that is more amenable to computational approaches. Second, the techniques used in proving languages to be undecidable, including reductions and diagonalization, appear repeatedly in complexity theory. Lastly, undecidability is an interesting topic in its own right.

The canonical result in computability theory is the undecidability of the halting problem. Intuitively, no algorithm exists to decide if a Turing Machine halts on an arbitrary input string. While the result seems abstract and unimportant, the results are actually far reaching. Software engineers seek better ways to determine the correctness of their programs. The undecidability of the halting problem provides an impossibility result for software engineers; no such techniques exist to validate arbitrary computer programs.

Recall that both A_{DFA} and A_{CFG} were both decidable. The corresponding language for Turing Machines is given below:

$$A_{\text{TM}} = \{\langle M, w \rangle : M \text{ is a Turing Machine that accepts } w\}$$

It turns out that A_{TM} is undecidable. We actually the following language undecidable:

$$L_{\text{diag}} = \{\omega_i : \omega_i \text{ is the ith string in } \Sigma^*, \text{ which is accepted by the ith Turing Machine } M_i\}$$

L_{diag} is designed to leverage a diagonalization argument. We note that Turing Machines are representable as finite strings (just like computer programs), and that the set of finite length strings over an alphabet is countable. So we can enumerate Turing Machines using $\mathbb{N}$. Similarly, we also enumerate input strings from Σ^* using $\mathbb{N}$. Before proving L_{diag} undecidable, we need the following result.

Theorem 4.10. *A language L is decidable if and only if L and $\overline{L}$ are recursively enumerable.*

Proof. Suppose first L is decidable, and let M be a decider for L. As M decides L, M also accepts L. So L is recursively enumerable. Now define $\overline{M}$ to be a Turing Machine that, on input ω, simulates M on ω. $\overline{M}$ accepts (rejects) ω if and only if M rejects (accepts) ω. As M is a decider, $\overline{M}$ decides $\overline{L}$. So $\overline{L}$ is also recursively enumerable.

Conversely, suppose L and $\overline{L}$ are recursively enumerable. Let B and $\overline{B}$ be Turing Machines that accept L and $\overline{L}$ respectively. We construct a Turing Machine K to decide L. K works as follows. On input ω, K simulates B and $\overline{B}$ in parallel on ω. As L and $\overline{L}$ are recursively enumerable, at least one of B or $\overline{B}$ will halt and accept ω. If B accepts ω, then so does K. Otherwise, $\overline{B}$ accepts ω and K rejects ω. So K decides L. □

In order to show that L_{diag} is undecidable, Theorem 4.10 provides that it suffices to show $\overline{L_{\text{diag}}}$ is not recursively enumerable. This is the meat of the proof for the undecidability of the halting problem. It turns out that L_{diag} is recursively enumerable, which is easy to see.

Theorem 4.11. *L_{diag} is recursively enumerable.*

Proof. We construct an acceptor D for A_{diag} which works as follows. On input ω_i, D simulates M_i on ω_i and accepts ω_i if and only if M_i accepts ω_i. So $L(D) = L_{\text{diag}}$, and L_{diag} is recursively enumerable. □

We now show that $\overline{L_{\text{diag}}}$ is not recursively enumerable.

Theorem 4.12. *$\overline{L_{diag}}$ is not recursively enumerable.*

Proof. Suppose to the contrary that $\overline{L_{\text{diag}}}$ is recursively enumerable. Let $k \in \mathbb{N}$ such that the Turing Machine M_k accepts $\overline{L_{\text{diag}}}$. Suppose $\omega_k \in \overline{L_{\text{diag}}}$. Then M_k accepts ω_k, as $L(M_k) = \overline{L_{\text{diag}}}$. However, $\omega_k \in \overline{L_{\text{diag}}}$ implies that M_k does not accept ω_k, a contradiction.

Suppose instead $\omega_k \notin \overline{L_{\text{diag}}}$. Then $\omega_k \notin L(M_k) = \overline{L_{\text{diag}}}$. Since M_k does not accept ω_k, it follows by definition of $\overline{L_{\text{diag}}}$ that $\omega_k \in \overline{L_{\text{diag}}}$, a contradiction. So $\omega_k \in \overline{L_{\text{diag}}}$ if and only if $\omega_k \notin \overline{L_{\text{diag}}}$. So $\overline{L_{\text{diag}}}$ is not recursively enumerable. □

Corollary 4.0.2. *L_{diag} is undecidable.*

Proof. This follows immediately from Theorem 4.10, as L_{diag} is recursively enumerable, while $\overline{L_{\text{diag}}}$ is not. □

4.6 Reducibility

The goal of a reduction is to transform one problem A into another problem B. If we know how to solve this second problem B, then this yields a solution for A. Essentially, we transform A into B, solve it in B, then apply this solution in A. Reductions thus allow us to order problems based on how hard they are. In particular, if we know that A is undecidable, a reduction immediately implies that B is undecidable. Otherwise, a Turing Machine to decide B could be used to decide A. Reductions are also a standard tool in complexity theory, where we transform problems with some bound on resources (such as time or space bounds). In computability theory, reductions need only be computable. We formalize the notion of a reduction with the following two definitions.

Definition 124 (Computable Function)**.** A function $f : \Sigma^* \to \Sigma^*$ is a *computable function* if there exists some Turing Machine M such that on input ω, M halts with just $f(\omega)$ written on the tape.

Definition 125 (Reduction)**.** Let A, B be languages. A *reduction* from A to B is a computable function $f : \Sigma^* \to \Sigma^*$ such that $\omega \in A$ if and only if $f(\omega) \in B$. We say that A is reducible to B, denoted $A \leq B$, if there exists a reduction from A to B.

We deal with reductions in a similar high-level manner as Turing Machines, providing sufficient detail to indicate how the original problem instances are transformed into instances of the target problem. In order for reductions to be useful in computability theory, we need an initial undecidable problem. This is the language L_{diag} from the previous section. With the idea of a reduction in mind, we proceed to show that A_{TM} is undecidable.

Theorem 4.13. *A_{TM} is undecidable.*

Proof. It suffices to show $L_{\text{diag}} \leq A_{\text{TM}}$. The function $f : \Sigma^* \to \Sigma^*$ maps $\omega_i \in L_{\text{diag}}$ to $\langle M_i, \omega_i \rangle \in A_{\text{TM}}$. Any string not in L_{diag} is mapped to ϵ under f. As Turing Machines are enumerable, a Turing Machine can clearly write $\langle M_i, \omega_i \rangle$ to the tape when started with ω_i. So f is computable. Furthermore, observe that $\omega_i \in L_{\text{diag}}$ if and only if $\langle M_i, \omega_i \rangle \in A_{\text{TM}}$. So f is a reduction from L_{diag} to A_{TM} and we conclude that A_{TM} is undecidable. □

With A_{TM} in tow, we prove the undecidability of the halting problem, which is given by:

$$H_{\text{TM}} = \{\langle M, w \rangle : M \text{ is a Turing Machine that halts on the string } w\}$$

Theorem 4.14. *H_{TM} is undecidable.*

Proof. It suffices to show that $A_{\text{TM}} \leq H_{\text{TM}}$. Each element of A_{TM} is clearly an element of H_{TM}. So we map each element of A_{TM} to itself in H_{TM}, and all other strings to ϵ. This map is clearly a reduction, so H_{TM} is undecidable. □

The reductions to show A_{TM} and H_{TM} undecidable have been rather trivial. We will examine some additional undecidable problems. In particular, the reduction will be from A_{TM}. The idea moving forward is to pick a desirable solution and return it if and only if a Turing Machine M halts on a string ω. A decider for the target problem would thus give us a decider for A_{TM}, which is undecidable. We illustrate the concept below.

Theorem 4.15. *Let $E_{TM} = \{\langle M \rangle : M$ is a Turing Machine s.t. $L(M) = \emptyset\}$. E_{TM} is undecidable.*

Proof. It suffices to show that $A_{\text{TM}} \leq E_{\text{TM}}$. For each instance of $\langle M, \omega \rangle \in A_{\text{TM}}$, we construct an instance of E_{TM} M' as follows. On input $x \neq \omega$, M' rejects x. Otherwise, M' simulates M on ω. If M accepts (rejects) ω, then M' rejects (accepts) ω. So $\langle M, \omega \rangle \in A_{\text{TM}}$ implies that $M' \in E_{\text{TM}}$. So E_{TM} is undecidable. □

We use the same idea to show that it is undecidable if a Turing Machine accepts the empty string. Observe above that our desirable solution for E_{TM} was $\emptyset$. Then M' accepted the desired solution if and only if the instance Turing Machine M accepted ω. We *conditioned* acceptance of the target instance based on the original problem. In this next problem, the target solution is ϵ, the empty string.

Theorem 4.16. *Let $L_{ES} = \{\langle M \rangle : M$ is a Turing Machine that accepts $\epsilon\}$. L_{ES} is undecidable.*

Proof. We show that $A_{\text{TM}} \leq E_{\text{TM}}$. Let $\langle M, \omega \rangle \in A_{\text{TM}}$. We construct an instance of L_{ES}, M', as follows. On input $x \neq \epsilon$, M' rejects x. Otherwise, M' simulates M on ω. M' accepts ϵ if and only if M accepts ω. So $\langle M, \omega \rangle \in A_{\text{TM}}$ if and only if $M' \in L_{\text{ES}}$. This function is clearly computable, so L_{ES} is undecidable. □

Recall that any regular language is decidable. We may similarly ask if a given language is regular. It turns out that this new problem is undecidable.

Theorem 4.17. *Let $L_{Reg} = \{L : L$ is regular $\}$. L_{Reg} is undecidable.*

Proof. We reduce A_{TM} to L_{Reg}. Let $\langle M, \omega \rangle \in A_{\text{TM}}$. We construct a Turing Machine M' such that $L(M')$ is regular if and only if M accepts ω. M' works as follows. On input x, M' accepts x if it is of the form $0^n 1^n$ for some $n \in \mathbb{N}$. Otherwise, M' simulates M on ω, and accepts x if and only if M accepts ω. So $L(M') = \Sigma^*$ if and only if M accepts ω, and $L(M') = \{0^n 1^n : n \in \mathbb{N}\}$ otherwise which is not regular. Thus, $L(M') \in L_{\text{Reg}}$ if and only if $\langle M, \omega \rangle \in A_{\text{TM}}$. So L_{Reg} is undecidable. □

The common theme in each of these undecidability results is that not every language satisfies the given property. This leads us to one of the major results in computability theory: Rice's Theorem. Intuitively, Rice's Theorem states that any non-trivial property is undecidable. A property is said to be trivial if it applies to either every language or no language. We formalize it as follows.

Theorem 4.18 (Rice)**.** *Let $\mathcal{R}$ be the set of recursively enumerable languages, and let C be a non-empty, proper subset of $\mathcal{R}$. Then C is undecidable.*

Proof. We reduce A_{TM} to C. Without loss of generality, suppose $\emptyset \in C$. As C is a proper subset of $\mathcal{R}$, $\overline{C}$ is non-empty. Let $L \in \overline{C}$. Let $\langle M, \omega \rangle \in A_{\text{TM}}$. We consturct a Turing Machine $M' \in C$ as follows. On input x, M' rejects x if $x \notin L$. Otherwise, M' simulates M on ω. M' rejects x if and only if M accepts ω. So $L(M') = \emptyset \in C$ if and only if $\langle M, \omega \rangle \in A_{\text{TM}}$. Thus, C is undecidable. □

Remark: Observe that the proof of Rice's Theorem is a template for the previous undecidability proofs in this section. Rice's Theorem generalizes all of our undecidability results and provides an easy test to determine if a language is undecidable. In short, to show a property undecidable, it suffices to exhibit a language satisfying said property and a language that does not satisfy said property.

5 Complexity Theory

The goal of Complexity Theory is to classify decidable problems according to the amount of resources required to solve them. Space and time are the two most common measures of complexity. Time complexity measures how many computations are required for a computer to solve decide an instance of the problem, with respect to the instance's size. Space complexity is analogously defined for the amount of extra space a computer needs to decide an instance of the problem, with respect to the instance's size.

In the previous sections, we have discussed various classes of computational machines- finite state automata, pushdown automata, and Turing Machines; as well as the classes of formal languages they accept. These automata answer decision problems: given a string $\omega \in \Sigma^*$, does ω belong to some language L? If L is regular, then a finite state automaton can answer this question. However, if L is only decidable, then the power of a Turing Machine (or Turing-equivalent model) is required. Formally, we define a decision problem as follows.

Definition 126 (Decision Problem)**.** Let Σ be an alphabet and let $L \subset \Sigma^*$. We say that the language L is a *decision problem.*

The complexity classes $\mathcal{P}$ and $\mathcal{NP}$ deal with decision problems. That is, they are sets of languages. In the context of an algorithms course, we abstract to the level of computational problems rather than formal languages. It is quite easy to formulate a computational decision problem as a language, though.

Example 124. Consider the problem of determining whether a graph G has a Hamiltonian cycle. The corresponding language would then be:

$$L_{HC} = \{\langle G \rangle : G \text{ is a graph that has a Hamiltonian Cycle}\} \tag{64}$$

We would then ask if the string $\langle H \rangle$ is in L_{HC}. In other words, does H have a Hamiltonian Cycle? Note that $\langle H \rangle$ denotes an encoding of the graph H. That means the language L_{HC} contains string-representations of graphs, such that the graphs contain Hamiltonian Cycles. From a computational standpoint, we represent graph as finite data structures programatically. Examples include the adjacency matrix, the adjacency list, or the incidence matrix representations. As computers deal with strings, it is important that our mathematical objects be encoded as strings.

5.1 Time Complexity- $\mathcal{P}$ and $\mathcal{NP}$

Time complexity is perhaps the most familiar computational resource measure. We see this as early as our introductory data structures class. Nesting loops results in $O(n^2)$ runtime, and mergesort takes $O(n \log(n))$ time to run. Junior and senior level data structures and algorithm analysis courses provide more rigorous frameworks to evaluate the runtime of an algorithm. This section does not focus on these tools. Rather, this section provides a framework to classify decision problems according to their time complexities. In order to classify such problems, it suffices to design a correct algorithm with the desired time complexity. This shows the problem is decidable in the given time complexity. With this in mind, we formalize the notion of time complexity.

Definition 127. Let $T : \mathbb{N} \to \mathbb{N}$ and let M be a Turing Machine that halts on all inputs. We say that M *has time complexity* $O(T(n))$ if for every $n \in \mathbb{N}$, M halts in at most $T(n)$ steps on any input string of length n. We refer to:

$$\mathbf{DTIME}(T(n)) = \{L \subset \Sigma^* : L \text{ is decided by some deterministic TM } M \text{ in time } O(T(n))\} \tag{65}$$

Remark: DTIME is the first complexity class we have defined. Observe that **DTIME** is defined based on a deterministic Turing Machine. Every complexity class must have some underlying model of computation. In order to measure complexity, it is essential that the computational machine is clearly defined. That is, we need to know what is running our computer program or algorithm to solve the problem. The formal language framework provides a notion of what the computer is reading. Intuitively, computers deal with binary strings. Programmers may work in an Assembly dialect, which varies amongst architectures, or some higher level language like Python or Java. In any case, the computer deals with some string representation of the algorithm as well as the problem.

With the definition of **DTIME** in tow, we have enough information to begin defining the class $\mathcal{P}$.

Definition 128 (Complexity Class $\mathcal{P}$)**.** The complexity class $\mathcal{P}$ is the set of languages that are decidable in polynomial time. Formally, we define:

$$\mathcal{P} = \bigcup_{k \in \mathbb{N}} \mathbf{DTIME}(n^k) \tag{66}$$

Example 125. The PATH problem is defined as follows: REL-PRIMES, LINEAR PROGRAMMING.

$$L_{PATH} = \{\langle G, u, v\rangle : G \text{ is a graph; } u, v \in V(G), \text{ and } G \text{ has a path from } u \text{ to } v\} \tag{67}$$

The PATH problem is decidable in polynomial time using an algorithm like breadth-first search or depth-first search, both of which run in $O(|V|^2)$ time. So $L_{PATH} \in \mathcal{P}$ since we have a polynomial time algorithm to decide L_{PATH}.

Example 126. Relative primality is another problem that is decidable in polynomial time. We wish to check if two positive integers have no common positive factors greater than 1. Formally:

$$L_{REL-PRIME} = \{(a, b) \in \mathbb{Z}^+ \times \mathbb{Z}^+ : \gcd(a, b) = 1\} \tag{68}$$

We have $L_{REL-PRIME} \in \mathcal{P}$, as the Euclidean algorithm computes the gcd of two positive integers in $O(\log(n))$ time, where $n = \max\{a, b\}$.

Remark: Note that the PATH and REL-PRIME problems are shown to be in $\mathcal{P}$ using conventional notions of an algorithm, which include random access. Turing Machines do not allow for random access, so it should raise an eyebrow about using more abstract notions of an algorithm to place problems into $\mathcal{P}$. The reason we can do this is because the RAM model of computation is polynomial-time equivalent to the Turing Machine. That is, if we have a RAM computation that takes $T_1(n)$ steps on an input of size n, then a Turing Machine can simulate this RAM computation in $p_1(T_1(n))$ steps where p is some fixed polynomial. Similarly, if a Turing Machine executes a computation in $T_2(n)$ steps where n is the size of the input, then a RAM machine can simulate the Turing computation in $p_2(T(n))$ steps for some fixed polynomial $p_2(T(n))$. In fact, $\mathcal{P}$ can be equivocally defined using any model of computation that can simulate a Turing Machine in polynomial time.

Note that problems in $\mathcal{P}$ are considered computationally easy problems. Intuitively, computationally easy problems are those that can be solved in polynomial time. This does not mean that a problem is easy for which to develop a solution. Many of the algorithms to place problems in $\mathcal{P}$ are quite complex and elegant. For a long time, the LINEAR PROGRAMMING problem was not known to be in $\mathcal{P}$. The common algorithm was the Simplex procedure, which was developed in 1947 and is still taught in undergraduate and graduate optimization classes. In most cases, the Simplex algorithm works quite efficiently, but it does have degenerate cases resulting in exponential time computations. The Ellipsoid algorithm was developed in 1979, which

placed the LINEAR PROGRAMMING problem in $\mathcal{P}$. In fact, LINEAR PROGRAMMING is $\mathcal{P}$-Complete, which means that it is one of the hardest problems in $\mathcal{P}$. We will discuss what constitutes a complete problem later.

We now develop some definitions, which will allow us to define $\mathcal{NP}$. Intuitively, the class $\mathcal{NP}$ contains problems for which correct solutions are easy to verify. The original definition of $\mathcal{NP}$ deal with non-deterministic Turing machines. Formally, the original definition is as follows:

Definition 129 (Complexity Class $\mathcal{NP}$ (Original Definition))**.** A language $L \in \mathcal{NP}$ if there exists a non-deterministic Turing machine M and polynomial p such that for any $\omega \in L$, M accepts ω in $p(|\omega|)$ time.

This definition of $\mathcal{NP}$ has since been generalized to utilize verifiers. This generalized definition of $\mathcal{NP}$ actually implies the original definition of $\mathcal{NP}$.

Definition 130 (Verifier)**.** A *verifier* for a language L is a Turing Machine M that halts on all inputs where:

$$L = \{\omega : M(\omega, c) = 1 \text{ for some string } c\}$$

We refer to the string c as the *witness* or *certificate*. M is a *polynomial time verifier* if it runs in $p(|\omega|)$ time for a fixed polynomial p and every string $\omega \in L$. This implies that $|c| \leq p(|\omega|)$.

Definition 131 (Complexity Class $\mathcal{NP}$ (Modern Definition))**.** The complexity class $\mathcal{NP}$ is the set of languages that have polynomial time verifiers.

Intuitively, the class $\mathcal{NP}$ contains problems for which correct solutions are easy to verify. Intuitively, we have a Turing machine M, a string input ω, and the certificate c which provides a proof that ω belongs to L. The Turing Machine uses c to then verify $\omega \in L$. We can show both definitions of $\mathcal{NP}$ are equivalent.

Proposition 5.1. *A language L is decided by some non-deterministic Turing Machine M which halts in $p(|\omega|)$ steps on all inputs ω, for some fixed polynomial p, if and only if there exists some polynomial time verifier for L.*

Proof. Let L be a language and let p be a polynomial. Suppose first that L is decided by a non-deterministic Turing Machine M that halts on all inputs ω in $p(|\omega|)$ time steps. We construct a polynomial time verifier from M. Let $\hat{\delta_M}(\omega)$ be a complete accepting computation. Let M' be a verifier accepting strings in $\Sigma^* \times (Q(M))^*$. The verifier M' simulates M on ω visiting the sequence of states specified by $(Q(M))^*$. M' accepts $\langle \omega, \hat{\delta_M}(\omega) \rangle$ if and only if M accepts ω using the computation $\hat{\delta_M}(\omega)$. As M decides L in polynomial time, M' halts in polynomial time and $\hat{\delta_M}(\omega)$ is a certificate for ω. Thus, M' is a polynomial time verifier for L.

Conversely, let K be a polynomial time verifier for L. We construct a non-deterministic Turing Machine K' to accept L. On the input string ω, K' guesses a certificate C and simulates M on $\langle \omega, c \rangle$. K' accepts ω if and only if K accepts $\langle \omega, c \rangle$. Since K is a polynomial time verifier, K' will halt in polynomial time on all inputs and $\omega \in L(K')$ if and only if there exists some certificate c on which K accepts $\langle \omega, c \rangle$. So $L = L(K')$ and so K' is a non-deterministic Turing Machine accepting L. □

Let's develop some intuition about the class $\mathcal{NP}$. In order to show a problem is in $\mathcal{NP}$, we take an instance and provide a certificate, then construct a verifier. Just like with $\mathcal{P}$, it suffices to provide a high level algorithm to verify an input and certificate pair due to the fact that our RAM computations are polynomial time equivalent to computations on a Turing machine.

Example 127. The HAMILTONIAN PATH problem belongs to the class $\mathcal{NP}$. Formally, we have:

$$L_{HP} = \{\langle G \rangle : G \text{ is a graph that has a Hamiltonian Path } \} \tag{69}$$

Our instance is clearly $\langle G \rangle$, a string encoding of a graph. A viable certificate is a sequence of vertices that form a Hamiltonian path in G. We then check that the consecutive vertices in the sequence are adjacent, and that each vertex in the graph is included precisely once in the sequence. This algorithm takes $O(|V|)$ time to verify the certificate, so $L_{HP} \in \mathcal{NP}$.

Example 128. Deciding if a positive integer is composite is also in $\mathcal{NP}$. Recall that a composite integer $n > 1$ can be written as $n = ab$ where $a, b \in \mathbb{Z}^+$ and $1 < a, b < n$. That is, n is not prime. Formally:

$$L_{COMP} = \{n \in \mathbb{Z}^+ : \exists a, b \in [n-1] \text{ s.t. } n = ab\} \tag{70}$$

Our instance is $n \in \mathbb{Z}^+$ and a viable certificate is a sequence of positive integers $a_1, \ldots, a_k$ such that each $a_i \in [n-1]$ and $\prod_{i=1}^{k} a_i = n$. It takes $O(k)$ time to verify that the certificate is a valid factorization of n. As $k < n$, we have a clear polynomial time algorithm to verify an integer is composite given a certificate.

We now arrive at the $\mathcal{P} = \mathcal{NP}$ problem. Intuitively, the $\mathcal{P} = \mathcal{NP}$ problem asks if every decision problem that can be easily verified can also be easily solved. It is straight-forward to show that $\mathcal{P} \subset \mathcal{NP}$. It remains open as to whether $\mathcal{NP} \subset \mathcal{P}$.

Proposition 5.2. $\mathcal{P} \subset \mathcal{NP}$.

Proof. Let $L \in \mathcal{P}$ and let M be a deterministic, polynomial time Turing Machine that decides L. We construct a polynomial time verifier M' for L as follows. Let $\omega \in \Sigma^*$. On input $\langle \omega, 0 \rangle$, M' simulates M on ω ignoring the certificate. M' accepts $\langle \omega, 0 \rangle$ if and only if M accepts ω. Since M decides L in polynomial time, M' is thus a polynomial time verifier for L. So $L \in \mathcal{NP}$. □

5.2 $\mathcal{NP}$-Completeness

The $\mathcal{P} = \mathcal{NP}$ problem has been introduced at a superficial level- are problems whose solutions can be verified easily also easy to solve? In some cases, the answer is yes- for the problems in $\mathcal{P}$. In general, this is unknown. However, it is widely believed that $\mathcal{P} \neq \mathcal{NP}$. In this section, the notion of $\mathcal{NP}$-Completeness will be introduced. $\mathcal{NP}$-Complete problems are the hardest problems in $\mathcal{NP}$ and are widely believed to be intractible. We begin with the notion of a reduction.

Definition 132 (Polynomial Time Computable Function)**.** A function $f : \Sigma^* \to \Sigma^*$ is a *polynomial time computable function* if some polynomial time TM M exists that halts with just $f(w)$ on the tape when started on w.

Definition 133 (Polynomial Time Reducible)**.** Let $A, B \subset \Sigma^*$. We say that A is *polynomial time reducible* to B, which is denoted $A \leq_p B$ if there exists a polynomial time computable function $f : \Sigma^* \to \Sigma^*$ such that $\omega \in A$ if and only if $f(\omega) \in B$.

The notion of reducibility provides a partial order on computational problems with respect to hardness. That is, suppose A and B are problems such that $A \leq_p B$. Then an algorithm to solve B can be used to solve A. Suppose we have the corresponding polynomial time reduction $f : \Sigma^* \to \Sigma^*$ to reduce A to B. Formally, we take an input $\omega \in \Sigma^*$ and transform it into $f(\omega)$. We use a decider for B to decide if $f(\omega) \in B$. As $\omega \in A$ if and only if $f(\omega) \in B$, we have an algorithm to decide if $\omega \in A$. This brings us to the definition of $\mathcal{NP}$-Hard.

Definition 134 ($\mathcal{NP}$-Hard)**.** A problem A is $\mathcal{NP}$-Hard if for every $L \in \mathcal{NP}$, $L \leq_p A$.

Definition 135 ($\mathcal{NP}$-Complete)**.** A language L is $\mathcal{NP}$-Complete if $L \in \mathcal{NP}$ and L is $\mathcal{NP}$-Hard.

Remark: Obseve that every $\mathcal{NP}$-Complete problem is a decision problem. In general, $\mathcal{NP}$-Hard problems need not be decision problems. Optimization and enumeration problems are common examples of $\mathcal{NP}$-Hard problems. Note as well that any two $\mathcal{NP}$-Complete languages are polynomial time reducible to each other, and so are equally hard. That is, a solution to one $\mathcal{NP}$-Complete language is a solution to all $\mathcal{NP}$-Complete languages. This leads to the following result.

Theorem 5.1. *Let L be an $\mathcal{NP}$-Complete language. If $L \in \mathcal{P}$, then $\mathcal{P} = \mathcal{NP}$.*

Proof. Proposition 5.2 already provides that $\mathcal{P} \subset \mathcal{NP}$. So it suffices to show that $\mathcal{NP} \subset \mathcal{P}$. Let $L \in \mathcal{NP}$ and let K be an $\mathcal{NP}$-Complete language that is also in $\mathcal{P}$. Let $f : \Sigma^* \to \Sigma^*$ be a polynomial time reduction from L to K, and let M be a polynomial time decider for K. Let $\omega \in L$. We transform ω into $f(\omega)$ and run M on $f(\omega)$. From the reduction, we have $\omega \in L$ if and only if $f(w) \in K$ accepts $f(\omega)$. Since M is a decider, we have a polynomial time decider for L. Thus, $L \in \mathcal{P}$ and we have $\mathcal{P} = \mathcal{NP}$. □

In order to show that a language L is $\mathcal{NP}$-Complete, it must be shown that $L \in \mathcal{NP}$ and for every language $K \in \mathcal{NP}$, $K \leq L$. Constructing a polynomial-time reductions from each language in $\mathcal{NP}$ to the target language L is not easy. However, if we already have an $\mathcal{NP}$-Complete problem J, it suffices to show $J \leq_p L$, which shows L is $\mathcal{NP}$-Hard. Of course, in order to use this technique, it is necessary to have an $\mathcal{NP}$-Complete language with which to begin. The Cook-Levin Theorem provides a nice starting point with the Boolean Satisfiability problem, better known as SAT. There are several variations on the Cook-Levin Theorem. One variation restricts to CNF-SAT, in which the Boolean formulas are in *Conjunctive Normal Form*. Another version shows that the problem of deiding if a combinatorial circuit is satisfiable, better known as CIRCUIT-SAT, is $\mathcal{NP}$-Complete. I begin with a some definitions:

Definition 136 (Boolean Satisfiability Problem (SAT))**.**

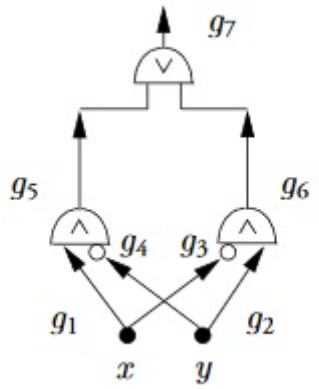
- **INSTANCE**: Let $\phi : \{0,1\}^n \to \{0,1\}$ be a Boolean function, restricted to the operations of AND, OR, and NOT.
- **DECISION:** Does there exist an input vector $x \in \{0,1\}^n$ such that $\phi(x) = 1$?

Example 129. The Boolean function $\phi(x_1, x_2, x_3) = x_1 \vee x_2 \wedge \overline{x_3}$ is an instance of SAT.

We next introduce the combinatorial circuit.

Definition 137 (Combinatorial Circuit)**.** A *Combinatorial Circuit* is a directed acyclic graph where the vertices are labeled with a Boolean operation or variable (input). Each operation computes a Boolean function $f : \{0,1\}^n \to \{0,1\}^m$, with the vertex having n incoming arcs, and m outgoing arcs.

Example 130. Consider the following combinatorial circuit. Here, x and y are the input vertices which feed into AND gates and NOT gates. The white vertices are the NOT gates, and the vertices labeled $\wedge$ are the AND gates. Each AND gate then feeds into an OR gate, which produces the final output of 0 or 1.



With this in mind, we define CIRCUIT-SAT, our first $\mathcal{NP}$-Complete language.

Definition 138 (CIRCUIT-SAT)**.**

- **INPUT:** Let C be a combinatorial circuit with a single output.

- **DECISION:** Does there exist an input vector $x \in \{0,1\}^n$ such that $C(x) = 1$?

Theorem 5.2 (Cook-Levin)**.** *CIRCUIT-SAT is $\mathcal{NP}$-Complete.*

The proof of the Cook-Levin Theorem is quite involved. We sketch the ideas here. In order to show CIRCUIT-SAT is in $\mathcal{NP}$, it is shown that a Turing Machine can simulate a combinatorial circuit taking T steps in $p(T)$ steps for a fixed polynomial p. This enables a verifier to be constructed for a given combinatorial circuit. In order to show that CIRCUIT-SAT is $\mathcal{NP}$-Hard, it is shown that any Turing Machine can be simulated by a combinatorial circuit with a polynomial time transformation. Since $\mathcal{NP}$ is the set of languages with polynomial time verifiers, this shows that each verifier can be transformed into a combinatorial circuit with a polynomial time computation. So CIRCUIT-SAT is $\mathcal{NP}$-Complete.

With CIRCUIT-SAT in tow, we can begin proving other languages are $\mathcal{NP}$-Complete, starting with CNF-SAT which we introduce below. Note that we could have started with any $\mathcal{NP}$-Complete problem. CIRCUIT-SAT happened to be proven $\mathcal{NP}$-Complete without an explicit reduction from another $\mathcal{NP}$-Complete problem; hence out choice of it.

Definition 139 (Clause)**.** A *Clause* is a Boolean function $\phi : \{0,1\}^n \to \{0,1\}$ where ϕ is written as consists of variables or their negations, all added together (where addition is the OR operation).

Definition 140 (Conjunctive Normal Form)**.** A Boolean function $\phi : \{0,1\}^n \to \{0,1\}$ is in *Conjunctive Normal Form* if $\phi = C_1 \wedge C_2 \wedge \ldots C_k$, where each C_i is a clause.

Definition 141 (CNF-SAT)**.**

- **INSTANCE:** A Boolean function $\phi : \{0,1\}^n \to \{0,1\}$ in Conjunctive Normal Form.
- **DECISION:** Does there exist an input vector $x \in \{0,1\}^n$ such that $\phi(x) = 1$?

Example 131. The Boolean function $\phi(x_1, x_2, x_3) = (x_1 \vee x_2) \wedge (x_2 \vee \overline{x_3})$ is in Conjunctive Normal Form.

Theorem 5.3. *CNF-SAT is $\mathcal{NP}$-Complete.*

Proof. In order to show CNF-SAT is $\mathcal{NP}$-Complete, we show that CNF-SAT is in $\mathcal{NP}$ and CNF-SAT is $\mathcal{NP}$-Hard.

- **Claim 1:** CNF-SAT is in $\mathcal{NP}$.

  Proof. In order to show CNF-SAT is in $\mathcal{NP}$, it suffices to exhibit a polynomial time verification algorithm. Let $\phi : \{0,1\}^n \to \{0,1\}$ be a Boolean function with k literals (either a variable or its negation). Let $x \in \{0,1\}^n$ such that $\phi(x) = 1$. We simply evaluate $\phi(x)$, which takes $O(k)$ time. So CNF-SAT is in $\mathcal{NP}$. □

- **Claim 2:** CNF-SAT is $\mathcal{NP}$-Hard.

  Proof. We show CIRCUIT-SAT $\leq_p$ CNF-SAT. Let C be a combinatorial circuit. We convert C to a Boolean function as follows. For each vertex v of C, we construct a Boolean function ϕ in Conjunctive Normal Form as follows:

  - If v is an input for C, then construct the literal x_v.
  - If v is the NOT operation with input x_k, we create the variable x_v and include the following clauses in ϕ: $(x_v \vee x_k)$ and $(\overline{x_v} \vee \overline{x_k})$. Thus, in order for ϕ to be satisfiable, it is necessary that $x_v = \overline{x_k}$.
  - If v is the OR operation with inputs x_i, x_j, we create the variable x_v and include the following clauses in ϕ: $(x_v \vee \overline{x_i}), (x_v \vee \overline{x_j}), (\overline{x_i} \vee x_i \vee x_j)$. Thus, in order for ϕ to be satisfiable, it is necessary that $x_v = 0$ if and only if $x_i = x_j = 0$, which realizes the OR operation from C.

– If v is the AND operation with inputs x_i, x_j, we create the variable x_v and include the following clauses in ϕ: $(\overline{x_v} \vee x_i), (\overline{x_v} \vee x_j), (x_v \vee \overline{x_i} \vee \overline{x_j})$. Thus, in order for ϕ to be satisfiable, it is necessary that $x_v = 1$ if and only if $x_i = x_j = 1$, which realizes the AND operation from C.
– If v is the output vertex, we construct the variable x_v and add it to ϕ.

There are at most $9|V|$ literals in ϕ, where $|V|$ is the number of vertices in C. So this construction occurs in polynomial time. It suffices to show that C is satisfiable if and only if ϕ is satisfiable. Suppose first C is satisfiable. Let $x \in \{0,1\}^n$ be a satisfying configuration for C. For each logic gate vertex v, set x_v to be the resultant of that operation on the inputs. By the analysis during the construction of ϕ, we have that ϕ is satisfiable. Conversely, suppose ϕ is satisfiable with input configuration $y \in \{0,1\}^k$ where k is the number of clauses. The first n elements of y, $(y_1, \ldots, y_n)$ corresponding to the input vertices of C form a satisfying configuration for C. So CNF-SAT is $\mathcal{NP}$-Hard. □

□

We now reduce CNF-SAT to the general SAT problem to show SAT is $\mathcal{NP}$-Complete.

Theorem 5.4. *SAT is $\mathcal{NP}$-Complete.*

Proof. The procedure to show CNF-SAT $\in \mathcal{NP}$ did not rely on the fact that the Boolean functions were in Conjunctive Normal Form. So this same procedure also suffices to show SAT is in $\mathcal{NP}$. As CNF-SAT is a subset of SAT, the identity map is a polynomial time reduction from CNF-SAT to SAT. So SAT is $\mathcal{NP}$-Hard. So SAT is $\mathcal{NP}$-Complete. □

From CNF-SAT, there is an easy reduction to the CLIQUE problem.

Definition 142 (CLIQUE)**.**

- **INSTANCE:** Let G be a graph and $k \in \mathbb{N}$.
- **DECISION:** Does G contain a complete subgraph with k vertices?

Theorem 5.5. *CLIQUE is $\mathcal{NP}$-Complete.*

Proof. We show that CLIQUE is in $\mathcal{NP}$ and that CLIQUE is $\mathcal{NP}$-Hard.

- **Claim 1:** CLIQUE is in $\mathcal{NP}$.

  Proof. Let (G, k) be an instance of CLIQUE. Let $S \subset V(G)$ be a set of vertices that induce a k-clique. We check that all $\binom{k}{2}$ edges are present in $G[S]$, the subgraph of G induced by S. This takes $O(n^2)$ time, which is polynomial. So CLIQUE is in $\mathcal{NP}$. □

- **Claim 2:** CLIQUE is $\mathcal{NP}$-Hard.

  Proof. It suffices to show CNF-SAT $\leq_p$ CLIQUE. Let ϕ be an instance of CNF-SAT with k-clauses. We construct an instance of CLIQUE as follows. Let G be the graph we construct. Each occurrence of a variable in ϕ corresponds to a vertex in G. We add all possible edges except if: (1) two vertices belong to the same clause; or (2) if two vertices are contradictory. If the length of ϕ is n, then this construction takes $O(n^2)$ time which is polynomial time. It suffices to show that ϕ is satisfiable if and only if there exists a k-clique in G.

  Suppose first ϕ is satisfiable. Let x be a satisfying configuration for ϕ. As ϕ is in Conjunctive Normal Form, there exists a literal in each clause that evaluates to 1. We select one such literal from each clause. As none of these literals are contradictory, the corresponding vertices in G induce a k-clique.

  Conversely, suppose G has a k-clique. Let $S \subset V(G)$ be a set of vertices that induce a k-clique in G. If $v \in S$ corresponds to a variable x_i, then we set $x_i = 1$. Otherwise, v corresponds to a variable's negation and we set $x_i = 0$. Any variable not corresponding to a vertex in the set is set to 0. Recall that each vertex in S corresponds to a literal from each clause and the literals are not contradictory. As ϕ is in Conjunctive Normal Form, we have a satisfying configuration for ϕ. We conclude that CLIQUE is $\mathcal{NP}$-Hard. □

□

The CLIQUE problem gives us two additional $\mathcal{NP}$-Complete problems. The first problem is the INDEPENDENT SET problem, and the second is the SUBGRAPH ISOMORPHISM problem. The SUBGRAPH ISOMORPHISM problem is formally:

Definition 143 (SUBGRAPH ISOMORPHISM)**.**

$$L_{SI} = \{\langle G, H\rangle : G, H \text{ are graphs, and } H \subset G\} \tag{71}$$

The identity map from CLIQUE to SUBGRAPH ISOMORPHISM provides that SUBGRAPH ISOMORPHISM is $\mathcal{NP}$-Hard. It is quite easy to verify that H is a subgraph of G given an isomorphism.

An independent set is the complement of a clique. Formally:

Definition 144 (Independent Set)**.** Let G be a graph. An independent set is a set $S \subset V(G)$ such that for any $i, j \in S$, $ij \notin E(G)$. That is, all vertices of S are pairwise non-adjacent in G.

This leads to the INDEPENDENT SET problem.

Definition 145 (INDEPENDENT SET (Problem))**.**

- **INSTANCE:** Let G be a graph and $k \in \mathbb{N}$.
- **DECISION**: Does G have an independent set with k vertices?

Theorem 5.6. *INDEPENDENT SET is $\mathcal{NP}$-Complete.*

Proof. We show that INDEPENDENT SET is in $\mathcal{NP}$, and that INDEPENDENT SET is $\mathcal{NP}$-Hard.

- **Claim 1:** INDEPENDENT SET is in $\mathcal{NP}$.

  Proof. Let $\langle G, k\rangle$ be an instance of INDEPENDENT SET and let $S \subset V(G)$ be an independent set of order k. S serves as our certificate. We check that for each distinct $i, j \in S$, $ij \notin E(G)$. This check takes $\binom{k}{2}$ steps, which is $O(|V|^2)$ time. So INDEPENDENT SET is in $\mathcal{NP}$. □

- **Claim 2:** INDEPENDENT SET is $\mathcal{NP}$-Hard.

  Proof. We show CLIQUE $\leq_p$ INDEPENDENT SET. Let $\langle G, k\rangle$ be an instance of CLIQUE. Let $\overline{G}$ be the complement of G, in which $V(\overline{G}) = V(G)$ and $E(\overline{G}) = \{ij : i, j \in V(G), ij \notin E(G)\}$. This construction takes $O(|V|^2)$ time. So this construction is in polynomial time. As an independent set is the complement of a clique, G has a k-clique if and only if $\overline{G}$ has an independent set with k-vertices. So INDEPENDENT SET is $\mathcal{NP}$-Hard. □

□

We provide one more $\mathcal{NP}$-Hardness proof to illustrate that not all $\mathcal{NP}$-Hard problems are in $\mathcal{NP}$. We introduce the HAMILTONIAN CYCLE and TSP_{OPT} problems.

Definition 146. HAMILTONIAN CYCLE

- **INSTANCE:** Let $G(V, E)$ be a graph.
- **DECISION:** Does G contain a cycle visiting every vertex in G?

And the Traveling Salesman optimization problem is defined as follows:

Definition 147. *TSP_{OPT}*

- **INSTANCE:** Let $G(V, E, W)$ be a weighted graph where $W : E \to \mathbb{R}_+$ is the weight function.
- **SOLUTION:** Find the minimum cost Hamiltonian Cycle in G.

We first note that HAMILTONIAN CYCLE is $\mathcal{NP}$-Complete, though we won't prove this. In order to show TSP_{OPT} is $\mathcal{NP}$-Hard, we reduce from HAMILTONIAN CYCLE.

Theorem 5.7. *TSP_{OPT} is $\mathcal{NP}$-Hard.*

Proof. We show HAMILTONIAN CYCLE $\leq_p \text{TSP}_{OPT}$. Let G be a graph with n vertices and a Hamiltonian cycle C. We construct a weighted K_n as follows. Each edge in K_n corresponding to C is weighted 0. All other edges are weighted 1. So any minimum weight Hamiltonian cycle in K_n has weight at least 0. We show that G has a Hamiltonian cycle if and only if the minimum weight Hamiltonian cycle in the K_n has weight 0. Suppose first G has a Hamiltonian cycle C. We trace along C in K_n to obtain a Hamiltonian cycle of weight 0 in K_n. Conversely, suppose K_n has a Hamiltonian cycle of weight 0. By construction, this corresponds to the Hamiltonian cycle C in G. We conclude that HAMILTONIAN CYCLE $\leq_p \text{TSP}_{OPT}$, so TSP_{OPT} is $\mathcal{NP}$-Hard. □

5.3 More on $\mathcal{P}$ and $\mathcal{P}$-Completeness

In this section, we explore the complexity class $\mathcal{P}$ as well as $\mathcal{P}$-Completeness. Aside from containing languages that are decidable in polynomial time, $\mathcal{P}$ is important with respect to parallel computation. Just as $\mathcal{NP}$-Hard problems are difficult to solve using a sequential model of computation, $\mathcal{P}$-Hard problems are difficult to solve in parallel. We omit exposition on parallel computation. Rather, there are two big takeaways. The first is that many $\mathcal{NP}$-Complete languages have subsets which are easily decidable. The second important takeaway is a clear understanding of $\mathcal{P}$-Completeness.

We begin with the 2-SAT problem.

Definition 148 (k-CNF-SAT)**.**

- **INSTANCE:** A Boolean function $\phi : \{0,1\}^n \to \{0,1\}$ in Conjunctive Normal Form, where each clause has precisely k literals.
- **DECISION:** Does there exist an input vector $x \in \{0,1\}^n$ such that $\phi(x) = 1$?

It is a well known fact that k-CNF-SAT is $\mathcal{NP}$-Complete for every $k \geq 3$. However, 2-CNF-SAT is actually in $\mathcal{P}$. One proof of this is by a reduction to another problem in $\mathcal{P}$: the STRONGLY CONNECTED COMPONENT problem. We can decide the STRONGLY CONNECTED COMPONENT problem using Tarjan's Algorithm, an $O(|V| + |E|)$ time algorithm. We define the STRONGLY CONNECTED COMPONENT problem formally.

Definition 149 (STRONGLY CONNECTED COMPONENT (SCC))**.**

- **INSTANCE:** A directed graph $G(V, E)$.
- **DECISION:** Does there exist vertices i, j such that there are directed $i \to j$ and $j \to i$ paths in G?

Theorem 5.8. *2-CNF-SAT is in $\mathcal{P}$.*

Proof. We show 2-CNF-SAT $\leq_p$ SCC. We begin by constructing the implication graph G, which is a directed graph. The vertices of G are the components of x and their negations, yielding $2n$ vertices in total. For each clause in C $(x_i \vee x_j)$, add directed edges $(\neg x_i, x_j), (\neg x_j, x_i)$. (So for example, if a clause contained $(\neg x_2 \vee x_3)$, the edges added to G would be $(x_2, x_3), (\neg x_3, \neg x_2)$.) The reduction to SCC looks at the implication graph to determine if there is a component x_i such that there is a directed path x_i to $\neg x_i$, and a directed path $\neg x_i to x_i$.

Notice that there are at most $\binom{n}{2}$ clauses to examine and so at most $\binom{2n}{2}$ edges to add to G, so the reduction is polynomial in time.

So we need to prove a couple facts:

- If there exists an $a \to b$ directed path in G, then there exists a directed $\neg b \to \neg a$ path in G. We will use this fact to justify the existence of a strongly connected component if there is a directed $x_i \to \neg x_i$.
- C is satisfiable if and only if there is no strongly connected component in G containing both a variable and its negation. This will substantiate the validity of the reduction.

We proceed with proving these claims:

- **Claim 1**: If there exists a directed $a \to b$ path in G, then there exists a directed $\neg b \to \neg a$ path in G.

  Proof. Suppose there exists an $a \to b$ directed path in G. By construction, for each edge $(c, d) \in G$, there exists an edge (d, c). So given the $a \to b$ directed path: $a \to p_1 \to ... \to p_k \to b$, there exist directed edges in G: $(\neg b, \neg p_k), ..., (\neg p_1, \neg a)$, yielding a directed $\neg b \to \neg a$ path, as claimed. □

- **Claim 2**: C is satisfiable if and only if there is no strongly connected component in G.

  Proof. It will first be shown that if C is satisfiable, then there is no strongly connected component in G. This will be done by contradiction. Let x be a satisfying configuration of C, and let x_i such that there is a strongly connected component including x_i and $\neg x_i$. Let $x_i \to p_1 \to ... \to p_n \to \neg x_i$ be the directed $x_i \to \neg x_i$ path in G. Suppose first $x_i = 1$. By construction, the edges $(\neg x_i, p_1), (\neg p_i, p_{i+1})$ for each $i = 1, ..., n-1$; and $(\neg p_n, \neg x_n)$ are in G. And so for each $i = 1, ..., n$, p_i must be 1 to satisfy the corresponding clause in C. However, since $\neg x_i$ is 0, p_n must be 0 to satisfy $(\neg p_n, \neg x_n)$, a contradiction. By similar analysis, x_i cannot be 0 either. And so C is unsatisfiable. Thus, if C is satisfiable, there is no strongly connected component containing both x_i and $\neg x_i$.

  Now suppose there is no strongly connected component in G. It will be shown that C is satisfiable by contradiction. Suppose there are no $x_i \in x$ such that there exists a directed $x_i \to \neg x_i$ path. For each unmarked vertex $v \in V(G)$ such that no $v \to \neg v$ path exists, mark v as 1. Now mark each neighbor of v as 1, and the negations of each marked variable as 0. Repeat this process until all vertices have been marked. By finiteness of the graph, this process terminates. Since there are no strongly connected components in G, all vertices will be marked. As C is unsatisfiable, let $i, j \in \{1, ..., n\}$ such $i \neq j$ and that there exists directed $x_i \to x_j$ and $x_i \to \neg x_j$ paths. So x_i implies both x_j and $\neg x_j$, which is a fallacy. By construction of G, there must exist a $\neg x_j \to \neg x_i$ directed path in G, which implies that G has a strongly connected component. However, G has no strongly connected component by assumption, a contradiction.

  Thus, we conclude C is satisfiable if and only if there exists no strongly connected component in G, proving Claim 2. □

As 2-CNF-SAT $\leq_p$ SCC, it follows that 2-CNF-SAT is in $\mathcal{P}$. □

Another example of an $\mathcal{NP}$-Complete problem that has a subset in $\mathcal{P}$ is the HAMILTONIAN CYCLE problem. Consider the subset $\{\langle C_n \rangle : n \geq 3\}$. It is easy to check if a graph is a cycle; and hence, has a Hamiltonian cycle.

We now introduce the notion of a $\mathcal{P}$-Hard problem. A $\mathcal{P}$-Hard problem is defined similarly as an $\mathcal{NP}$-Hard problem, with the exception of the fact that the reductions are bounded in space rather than time. Formally, the reductions have to be computable with an additional logarithmic amount of space based on the input string. In fact, a log-space computation is necessarily polynomial time. We will prove this when we discuss the complexity class **PSPACE** and space complexity.

Definition 150 (Log-Space Computable Function)**.** A function $f : \Sigma^* \to \Sigma^*$ is a *log-space computable function* if some TM M exists that halts with just $f(w)$ on the tape when started on w, and uses at most $O(\log(|\omega|))$ additional space.

Definition 151 (Log-Space Reducible)**.** Let A, B be languages. We say that A is *log-space reducible* to B, denoted $A \leq_\ell B$, if there exists a log-space computable function $f : \Sigma^* \to \Sigma^*$ such that $\omega \in A$ if and only if $f(\omega) \in B$.

Definition 152 ($\mathcal{P}$-Hard)**.** A problem K is $\mathcal{P}$-Hard if for every $L \in \mathcal{P}$, $L \leq_\ell K$.

And so we now define $\mathcal{P}$-Complete analogously to $\mathcal{NP}$-Complete.

Definition 153 ($\mathcal{P}$-Complete)**.** A language L is $\mathcal{P}$-Complete if $L \in \mathcal{P}$ and L is $\mathcal{P}$-Hard.

The proof of the Cook-Levin Theorem provides us a first $\mathcal{P}$-Complete problem: CIRCUIT VALUE. The CIRCUIT-SAT problem takes a combinatorial circuit and asks if it is satisfiable. The CIRCUIT VALUE problem takes a combinatorial circuit and an input vector as the instance, and the decision problem is if the input vector satisfies the circuit.

Definition 154 (CIRCUIT VALUE (CV))**.**

- **INSTANCE:** Let C be a combinatorial circuit computing a function $\phi : \{0,1\}^n \to \{0,1\}$, and let $x \in \{0,1\}^n$.
- **DECISION:** Is $C(x) = 1$?

Theorem 5.9. *CIRCUIT VALUE is $\mathcal{P}$-Complete.*

With CIRCUIT VALUE in mind, we prove another $\mathcal{P}$-Complete problem: MONOTONE CIRCUIT VALUE. The difference between CIRCUIT VALUE and MONOTONE CIRCUIT VALUE is that we restrict to the operations of $\{\text{AND}, \text{OR}\}$ in MONOTONE CIRCUIT VALUE. So in order to prove MONOTONE CIRCUIT VALUE, we flush the negations down to the inputs using DeMorgan's Law. We define MONOTONE CIRCUIT VALUE formally below.

Definition 155 (MONOTONE CIRCUIT VALUE (MCV))**.**

- **INSTANCE:** Let C be a combinatorial circuit in which only AND and OR gates are used, and let $\phi : \{0,1\}^n \to \{0,1\}$ be the function C computes. Let $x \in \{0,1\}^n$.
- **DECISION:** Is $\phi(x) = 1$?

In order to prove MCV is $\mathcal{P}$-Complete, we need a few important facts:

- All Boolean functions $f : \{0,1\}^n \to \{0,1\}^m$ can be computed using the operations AND, OR, and NOT.
- All Boolean functions can be computed using operations equivalent to AND, OR, and NOT.
- All logical circuits can be written as straight-line programs. That is, we have only variable assignments and arithmetic being performed. There are no loops, conditionals, or control structures of any kind.

We begin by sketching the proof that MCV is $\mathcal{P}$-Complete, so the ideas are clear. Since MCV is a subset of CV (we take circuits without the NOT operation, which are also instances of CV), MCV is in $\mathcal{P}$. To show MCV is $\mathcal{P}$-Hard, we show CV $\leq_\ell$ MCV. That is, for each instance of CV, a corresponding instance of MCV will be constructed. This is difficult though, as it is necessary to get rid of the NOT operations from CV. We do this by flushing the NOT operations down each layer of the circuit using DeMorgan's Law.

We then construct Dual-Rail Logic (DRL) circuits, where each variable x_i from x in the CV instance is represented as $(x_i, \neg x_i)$ in the MCV instance. So any negations we may want are constructed up-front, so the NOT operation becomes unnecessary. The DRL operations are defined as follows:

- DRL-AND: $(x, \neg x) \wedge (y, \neg y) = (x \wedge y, \neg(x \wedge y)) = (x \wedge y, \neg x \vee \neg y)$

- DRL-OR: $(x, \neg x) \vee (y, \neg y) = (x \vee y, \neg(x \vee y)) = (x \vee y, \neg x \wedge \neg y)$
- DRL-NOT: $\neg(x, \neg x)$ is given just by twisting the wires, sending x and $\neg x$ in opposite directions.

Since the NOT operation is given upfront in the variable declarations, the DRL operations are all realizable over the monotone basis of {AND, OR}. DRL is also equally as powerful as the basis {AND, OR, NOT}. So any Boolean function can be computed with DRL Circuits.

We now formally prove MCV is $\mathcal{P}$-Complete.

Theorem 5.10. *MONOTONE CIRCUIT VALUE is $\mathcal{P}$-Complete.*

Proof. In order to show MCV is $\mathcal{P}$-Complete, we show that MCV is in $\mathcal{P}$ and every problem in $\mathcal{P}$ is log-space reducible to MCV (ie., MCV is $\mathcal{P}$-Hard). As MCV is a subset of CV and CV is in $\mathcal{P}$, it follows that MCV is in $\mathcal{P}$.

To show MCV is $\mathcal{P}$-Hard, we show CV $\leq_\ell$ MCV. Let (C, x) be an instance of CV where C is the circuit over the basis {AND, OR, NOT} and x is the input sequence. We construct C' over the monotone basis {AND, OR} from C, by rewriting C as a dual-rail circuit. Let $P(C)$ be the straight-line program representing C. Let P' be the straight-line program used to construct C'. For each line n in $P(C)$, let this instruction be line $2n$ in P'. Line $2n+1$ in P' corresponds to the negation of line n in $P(C)$.

The NOT operation in $P(C)$ is realized in P' by twisting the wires. That is, the step $(2k = \neg 2i)$ is realized by the steps $(2k = 2i + 1)$ and $(2k + 1 = 2i)$. The AND operation in $P(C)$ $(2k = 2i \wedge 2j)$ is replaced by the steps $(2k = 2i \wedge 2j)$ and $(2k + 1 = (2i + 1) \vee (2j + 1))$. Finally, the OR operation $(2k = 2i \vee 2j)$ is realized by $(2k = 2i \vee 2j)$ and $(2k + 1 = (2i + 1) \wedge (2j + 1))$. And so $P(C) = P'$ for all inputs. So $P(C) = 1$ if and only if $P' = 1$, and $P(C) = 0$ if and only if $P' = 0$. So the reduction is valid.

It now suffices to argue the reduction takes a logarithmic amount of space. Generating P' from $P(C)$ can be done using a counter variable. So for each step i in $P(C)$, we perform operations at lines $2i$ and $2i+1$ in P'. So if there are n steps in $P(C)$, we need $log_2(\lceil 2n+1 \rceil)$ bits, which grows asymptotically with $c(log_2(2) + log_2(n)) = c(1 + log_2(n))$ for some integer constant $c > 1$. So the amount of space required is $O(log(n))$. And so we conclude that MCV is $\mathcal{P}$-Complete. □

5.4 Closure Properties of $\mathcal{NP}$ and $\mathcal{P}$

TODO

5.5 Structural Proofs for $\mathcal{NP}$ and $\mathcal{P}$

TODO

5.6 Ladner's Theorem

Ladner's Theorem states that if $\texttt{P} \neq \texttt{NP}$, then there exists a problem $L \in \texttt{NP} \setminus \texttt{P}$ such that $L \notin \texttt{NP}$-Complete. We refer to the set $\texttt{NP} \setminus \texttt{P}$ as NP-Intermediate. The consequence of Ladner's Theorem is that finding an NP-Intermediate language would settle the $\texttt{P} = \texttt{NP}$ problem, providing a separation.

We prove Ladner's theorem as follows. Define the language:

$$L := \{x \in \texttt{SAT} : f(|x|) \text{ is even } \},$$

where f is a function we will construct later. Here, L is our target NP-Intermediate language. The goal is to "blow holes" in L, so that L is not NP-Complete, while also ensuring L is not "easy enough" to be in P. We accomplish this by diagonalizing against polynomial time reductions, as well as polynomial time deciders. The trick is to ensure that f is computable in polynomial time, which ensures that $L \in \texttt{NP}$.

In order to accomplish this, f tracks the given stage. At even-indexed stages (i.e., $f(n) = 2i$), we diagonalize against the ith polynomial time decider. While at odd-indexed stages (i.e., $f(n) = 2i + 1$), we diagonalize against polynomial time reductions from SAT to L. That is, we want that $\texttt{SAT} \not\leq_p L$. As SAT is NP-Complete, this ensures that L is *not* NP-Complete.

We now proceed with the formal proof.

Theorem 5.11 (Ladner, 1975)**.** *If $\texttt{P} \neq \texttt{NP}$, then there exists a language $L \in \texttt{NP} \setminus \texttt{P}$, such that $L \notin \texttt{NP}$-Complete.*

Proof. Define:

$$L := \{x \in \texttt{SAT} : f(|x|) \text{ is even } \}.$$

Let $(M_i)_{i \in \mathbb{Z}^+}$ be an enumeration of polynomial-time Turing machines (**Remark:** Observe that this provides an enumeration of the languages in P), and let $(F_i)_{i \in \mathbb{Z}^+}$ be an enumeration of polynomial time Turing Machines without restriction to their output length. (**Remark:** Observe that $(F_i)_{i \in \mathbb{N}}$ provides an enumeration of polynomial-time computable functions, which include potential reductions).

Now let $M_{\texttt{SAT}}$ be a decider for SAT. We now define f recursively as follows. First, define $f(0) = f(1) = 2$. We associate f with the Turing Machine M_f that computes it. On input 1^n (with $n > 1$), M_f proceeds in two stages, each lasting exactly n steps. During the first stage, M_f computes $f(0), f(1), \ldots$, until it runs out of time. Suppose the last value M_f computed at the first stage was $f(x) = k$. At the next stage, the output of M_f will either be k or $k + 1$, to be determined in the second stage.

In the second stage, we have one of two cases:

- **Case 1:** Suppose that $k = 2i$. Here, we diagonalize against language i in P as follows. The goal is to find a string $z \in \Sigma^*$ such that $z \in (L(M_i) \triangle L)$. We enumerate such strings z in lexicographic order, and then computing $M_i(z), M_{\texttt{SAT}}(z)$, and $f(|z|)$ for all such strings. Note that by definition of L, we must compute $f(|z|)$ to ensure that $f(|z|)$ is even. If such a string z is found in the allotted time (n steps), then M_f outputs $k+1$ (so M_f can proceed to diagonalize against polynomial time reductions on the next iteration). Otherwise, M_f outputs k (as we have not successfully diagonalized against M_i yet and need to do so on the next iteration).
- **Case 2:** Suppose that $k = 2i - 1$. Here, we diagonalize against polynomial-time computable functions. In this case, M_f searches for a string $z \in \Sigma^*$ such that F_i is an incorrect Karp reduction on z. That is, either:
  - $z \in \texttt{SAT}$ and $F_i(z) \notin A$; or
  - $z \notin \texttt{SAT}$ and $F_i(z) \in A$.

  We accomplish this by computing $F_i(z), M_{\texttt{SAT}}(z)$, $M_{\texttt{SAT}}(F_i(z))$, and $f(|F_i(z)|)$ (**Remark:** Here, we use clocking to ensure that $M_{\texttt{SAT}}$ is not taking too long). If such a string is found in the allotted time, then the output of M_f is $k + 1$. Otherwise, M_f outputs k.

Claim: $L \notin \texttt{P}$.

Proof. Suppose to the contrary that $L \in \texttt{P}$. Let M_i be a TM that decides L. By Case 1 in the second stage of the construction of M_f, no string z is found satisfying $z \in L$ and $z \notin L(M_i)$. Thus, $f(n)$ is even for all but finitely many n. Thus, L and SAT coincide for all but finitely many strings. It follows that SAT is decidable in polynomial time (decide if a string is in L; if not, we only have finitely many cases to check). So $\texttt{SAT} \in \texttt{P}$, contradicting the assumption that $\texttt{P} \neq \texttt{NP}$. □

Claim: $L \notin \texttt{NP}$-Complete.

Proof. Suppose to the contrary that L is NP-Complete. Then there is a polynomial time reduction F_i from SAT to L. So $f(n)$ will be even for only finitely many n, which implies that L is finite. So $L \in \texttt{P}$, which implies that $\texttt{SAT} \in \texttt{P}$, contradicting the assumption that $\texttt{P} \neq \texttt{NP}$. □

□

5.7 PSPACE

TODO

5.8 PSPACE-Complete

TODO