2020-01-01

Free Semigroups and Identites for a Class of Monoids

Enrique Salcido
University of Texas at El Paso

FREE SEMIGROUPS AND IDENTITIES FOR A CLASS OF MONOIDS

ENRIQUE SALCIDO

Master's Program in Mathematics

APPROVED:

Emil Daniel Schwab, Ph.D, Chair

Art Duval, Ph.D.

Vladik Kreinovich, Ph.D.

Stephen Crites, Ph.D.
Dean of the Graduate School

to my

FAMILY and FRIENDS

with love

FREE SEMIGROUPS AND IDENTITIES FOR A CLASS OF MONOIDS

by

ENRIQUE SALCIDO

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

Department of Mathematical Sciences

THE UNIVERSITY OF TEXAS AT EL PASO

May 2020

Abstract

The study of words as a mathematical object is a deep and rich field of study. Algebra, Combinatorics, Theoretical Computer Science etc., are major disciplines, which are fully using this study. Combinatorial properties (via Codes, Free Hulls, Infinite Words), and algebraic properties of words are presented in this thesis. The free semigroup on a set (alphabet) X and finite presentation of semigroups have a central place in the algebraic study of words. The last part of the thesis is devoted to the study of identities in the alphabet $X = \{x, y\}$ for a class of monoids. The characterization of such identities are given gradually; some elementary identities are established at the beginning. Using the canonical form of a word, mainly triples of positive integers are those that determine all these identities.

Table of Contents

Chapter 1

Words

In this chapter, we will focus on what others have called words and review some properties that they have. In the following chapter, we will talk about known properties of congruences and the already defined Bicyclic Semigroup. In the last chapter, we will present the new results of this thesis.

1.1 Definitions and Properties

In this section we will lay the foundation for alphabets and the words that can be created for them. Note that throughout this thesis we will use semigroup and monoid almost as synonyms but if a distinction has to be made, for example a theorem is only true if the algebraic structure is a monoid, then we will make this distinction.

1.1.1 Historical Background

Words have began to be studied in the early 1900's in the hopes to help deepen the understanding of language. As the century went on the study of words became a useful tool for Computer Scientists and an interesting free monoid to study for mathematicians. Most of the work done on words have been culminated into three books written by a group of mathematicians that refer to themselves as M. Lothaire, see [4].

1.1.2 Preliminaries

In our study of words we will first go over some preliminaries. We are going to start with the definition of some basic algebraic structures.

Definition 1 *Let S be a non-empty set and let $\cdot : S \times S \to S$ be a binary operation on S. S is called a* ***semigroup*** *if*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

for all $a, b, c \in S$.

Definition 2 *A semigroup M is called a* ***monoid*** *if there exists $1 \in M$ with the property that*

$$1 \cdot a = a \cdot 1 = a$$

for all $a \in M$

It will also be helpful to define structure preserving maps between two algebraic structures.

Definition 3 *Let M and N be monoids (semigroups) and let $\phi : M \to N$. We will say that ϕ is a* ***homomorphism*** *if*

$$\phi(xy) = \phi(x)\phi(y)$$

for all $x, y \in M$.

Definition 4 *We call a homomorphism an* ***isomorphism*** *if it is bijective. If there exists a isomorphism between two algebraic structures we will say that they are* ***isomorphic*** *to one another. We will use the symbol $\cong$ to say they are isomorphic.*

Here it is important to note that if there is an homomorphism then the domain and codomain have similar structure but if there is an isomorphism then both algebraic structures have the same structure, i.e. we are just changing the name of the elements.

The following definition of alphabet and subsequent definitions and notations are from Lothaire, see [4].

Definition 5 *Let X be a non-empty set which we will call the* ***alphabet*** *and let the set* $\boldsymbol{X^+}$ *be the set of all non-empty finite sequences of elements of X, which we will refer to as the* ***words over an alphabet X***.

Note that the alphabet does not have to be finite but in most of its applications it is considered to be finite. Some examples of alphabets are the English alphabet {a,b,c, ..., z} and {0,1} used for binary. We will be considering words much like vectors such that the letters in $u \in X^+$ will be referred by $u = u_0u_1 \dots u_n$. It can be observed that X^+ is a semigroup with concatenation as the operation i.e. $u, v \in X^+$ $u \cdot v = u_0u_1 \dots u_nv_1v_2 \dots v_m$. We will maintain the convention of writing $u \cdot v$ as simply uv.

Definition 6 *Let X^+ be the words over an alphabet X, then the* ***length of a word u****, $u \in X^+$, is denoted by $n_X(u) = n$ where $u = u_0u_1 \dots u_n$ and $u_i \in X$.*

Definition 7 *Let 1 denote a word where $n_X(1) = 0$. We will call 1 the* ***empty word****. Now define* $\boldsymbol{X^*} = X^+ \cup \{1\}$.

The notation for using 1 for the empty word reflects the fact that it is the identity of X^*. However, if the alphabet contains the character 1, such as the binary alphabet does, a different character should be used, such as e, to avoid confusion. Now it is clear that X^* is a monoid since for all $u \in X^*$ we have $u1 = 1u = u$. The following definition will impose an order on the set X^*.

Definition 8 *For $u, v \in X^*$ we say $u \leq v$ if there exist $w \in X^*$ such that $uw = v$. We say that w is a* ***left factor of v****.*

Definition 9 *A monoid (semigroup) M is said to be a* ***free monoid (semigroup)*** *if there exist an alphabet X for which M is isomorphic to X^* (X^+).*

So clearly X^+ and X^* are free. Note that all the definitions we have made for X we can also do with any subset of X, most notably when we consider a single element $u \in X$ so u^* (we will not use the braces here) is the free monoid generated by u. Free monoids will be covered extensively in a later chapter.

1.1.3 Codes and Free Hulls

Now that we have created a foundation of what we will dive into questions regarding subsets of monoids that are monoids themselves, which we will call submonoids.

Definition 10 *Let M be a monoid and let Z be a non empty subset of M. We will say that **Z generates M** if for every $x \in M$ we can express $x = z_1 z_2 \dots z_n$ for $z_i \in Z$ and $n \in \mathbb{N}$. Moreover, the identity of M is not an element of Z.*

The definition above can also be applied to semigroups by disregarding the condition of the identity since the identity does not exists.

Note that if we have a generating set Z for some submonoid Y of X^*, over some alphabet X, then every word in Y can be written as a product of words in Z. Thus, we can think about Z as being an alphabet generating Y, and vice versa. For example, consider the old Spanish alphabet that includes the letter *ch*. Notice how this letter is a combination of two symbols, yet it is a part of the alphabet and used as a single letter. This alphabet generates the set of all Spanish words.

Having this in mind, we will show that there exists a unique minimal generating set for every submonoid of X^* as shown in Lothaire, see [4]. By minimal in the previous statement we mean that there is no smaller set that can be a generator.

Theorem 1 *Let Y be a submonoid of X^*, then the smallest alphabet that can generate Y is $Z = (Y - 1) - (Y - 1)^2$.*

Proof. Let $w \in Y$. Note that w can be written as a product of non-empty words $w = y_1 y_1 \dots y_n$ where $y_i \in Y$ and each y_i cannot be written as a product of two non-empty words. Note that $Z = (Y - 1) - (Y - 1)^2$ is exactly the set of words in Y that cannot be written as a product of two non-empty words, thus $y_i \in Z$ for all i. Therefore, Z generates Y.

Now let Z' be another set that generates Y. Suppose that $Z' \subset Z$, then there exists $z \in Z$ such that $z = z_1 z_2$ where z_1 and z_2 are non-empty and $z_1, z_2 \in Z'$. Since Z' generates

Y then $z_1, z_2 \in Y$. We found $z \in Z$ such that it can be written as a non-empty product of two elements in Y which contradicts the definition of Z, so Z is minimal. $\square$

Definition 11 *The set Z from the theorem above is called* ***the minimal generating set of Y****. Z is called a* ***code*** *if Y is free.*

Now that we have defined the minimal generating set of a submonoid of X^*, we can use it to characterize free monoids.

Theorem 2 *Let Y be a submonoid of X^* and let Z be its minimal generating set. Y is free if and only if whenever*

$$x_1 x_2 \dots x_n = y_1 y_2 \dots y_m \text{ where } x_i, y_j \in Z$$

then $n = m$ and $x_i = y_i$

This theorem will be proved in the next chapter where we will have a more abstract definition of free monoids to show that indeed the two facts are equivalent. For now, note that this theorem states that Y is a free monoid with generating set Z if and only if

$$Y = Z^*$$

Therefore, if we have a free submonoid we can use its minimal generating set as an alphabet.

Remark 1 *We will say that Y is freely generated by Z if every element of Y can be uniquely written as a product of generators from Z.*

The following example comes from Lothaire, see [4]. We can see that if we have an alphabet $X = \{a, b\}$, then note that a submonoid Y of X^* is generated by $Z = \{a, ab, ba\} \subset X^*$, but it is not generated freely since $aba \in Y$ can be written in two ways: $aba = a(ba) = (ab)a$. On the other hand, set $Z' = \{aa, ba, baa, bb, bba\}$ freely generates a submonoid Y' of X^*: every element of Y' can be uniquely represented by a product of elements of Z'.

Another example of a code is $\{u, v\}$ where $u, v \in X^*$ and there does not exists $w \in X^*$ such that $u, v \in w^*$. Here a person can ask what happens if there does exists such a w. This is actually interesting question with very promising results. We will cover this more in detail in the next section.

Theorem 3 *A submonoid Y of X^* is free if and only if $pw, wq \in Y$ where $p, q \in Y$ and $w \in X^*$ implies $w \in Y$*

Proof. Let Y be a submonoid of X^* and let Z be its minimal generating set. Now suppose that if $w \in X^*$ and there exist $p, q \in Y$ such that $pw, wq \in Y$ implies $w \in Y$. Then if

$$x_1 x_2 \dots x_n = y_1 y_2 \dots y_m \quad x_i, y_j \in Z$$

we may suppose that $x_1 \leq y_1$, thus, $y_1 = x_1 w$ for some $w \in X^*$. Moreover we have $x_2 \dots x_n = w y_2 \dots y_n$. Now we have $x_1 w, w y_2 y_3 \dots y_n \in Y$ so $w \in Y$. Since Y is minimally generated by Z we get that $w = 1$ so $x_1 = y_1$. Performing induction we get that $n = m$ and that $x_i = y_i$, making Y free.

Suppose that Y is a free submonoid of X^*. Since Y is free there exists an isomorphism $\phi : B^* \to Y$ where $\phi(B) = Z$, Z being the minimally generating set. Now suppose that $w \in X^*$ and there exist $p, q \in Y$ where $pw, wq \in Y$. Let

$$\phi(x) = p, \quad \phi(y) = q, \quad \phi(s) = pw, \text{ and } \phi(t) = wq.$$

Now since ϕ is a isomorphism and that Y is a submonoid we get $\phi(xt) = \phi(sy)$ implying that $xt = sy$ and $pwq = pwq$ so $w \in Y$. □

Theorem 4 *Any intersection of free submonoids of X^* is free.*

Proof. Let $\{Y_i\}_{i \in I}$ be a family of free submonoids of X^*. Suppose that there exist

$$pw, wq \in \bigcap_{i \in I} Y_i \text{ such that } p, q \in Y_i \text{ for all } i \text{ and } w \in X^*.$$

By Theorem 3 we know that $w \in Y$ for all i since every Y_i is free. Thus, $w \in \bigcap_{i \in I} Y_i$. □

Since the property of being free is preserved by intersections, we can now talk about the smallest, in terms of set inclusion, free monoid containing a subset of X^*, since for any $A \subset X^*$ the set $\{Y \text{ — } A \subset Y \text{ and } Y \text{ is free}\}$ is not empty so there is always a free hull for any subset of X^*.

Definition 12 *Let $A \subset X^*$ and let Y be the smallest, in terms of set inclusion, free submonoid containing A. We will call the code generating Y the* ***free hull of A****.*

Now that we have made a connection between any subset of X^* and the smallest free submonoid containing it we can prove something intuitively obvious and very powerful.

Theorem 5 (Deflect Theorem) *Let A be the free hull of $Y \subset X^*$ such that Y is not a code, then the following inequality holds*

$$|A| \leq |Y| - 1$$

Proof. Let $\alpha : Y \to A,\ \alpha(y) = a$ such that $y \in aA^*$. To check if α is well-defined let $y \in Y$ then since A is a code there exists $a \in A$ such that $y \in aA^*$, so every element of Y is mapped onto A. Now suppose that $\alpha(y) = a_1$ and $\alpha(y) = a_2$. Then $y \in a_1A^*$ and $y \in a_2A^*$ so there exist $a \in a_1A^*$ and $a' \in a_2A^*$ such that $a = a'$. From Theorem 2 we can see that a and a' are of equal length and that each of their letters are equal thus $a = a'$ so $a_1A^* = a_2A^*$.

Now that we know that α is well defined we will show that α is not injective but it is surjective.

Since Y is not a code there exist an equality $x_1x_2 \dots x_n \neq y_1y_2 \dots y_m$ such that $x_i, y_i \in Y$ for all i and $x_1 \neq y_1$. Thus, $\alpha(x_1) = \alpha(y_1)$ but $x_1 \neq y_1$ so α is not injective.

Suppose that α is not surjective, then their would exists a $z \in A$ such that $z \notin \alpha(Y)$. Let $Z = (A - z)z^*$ which is the subset of A that would not be mapped to at all. Suppose that the following equality holds

$$z_1z_2 \dots z_n = z_1^{'}z_2^{'} \dots z_m^{'}, \quad z_i, z_i^{'} \in Z.$$

Then since $z_i, z_j^{'} \in Z$ we can write them as follows $z_i = y_i z^{k_i}$ and $z_j^{'} = y_j^{'} z^{k_i^{'}}$ where $y_i, y_j^{'} \in (A - z)$ and $k_i, k_j^{'} \geq 0$. Recall that A is a code $y_i = y_i^{'}$, $z^{k_i} = z^{k_i^{'}}$, and $n = m$. Therefore Z is a code. Note that $Y \subset Z^* \subset A^*$ which contradicts the minimality of A, therefore α is surjective.

Since we showed that α is surjective but not injective it follows that $|A| \leq |Y| - 1$ holds. $\square$

This proof comes from Lothaire, see [4]. The Deflect Theorem proves that codes of free monoids, free hulls, are the smallest way of representing any subset of X^*.

1.1.4 When Do Words Commute?

In the Preliminaries we noted that the monoid X^* is not commutative so let's investigate if it is possible to find a submonoid of X^* that is commutative. Let's start off by the simplest case, if we consider $\{a\}$, $a \in X$ as our submonoid then obviously any word in a^* commutes since we only have one letter. We will try to generalize this idea with the following definition, which was obtained from Lothaire and Mikhalev, see [4, 5].

Definition 13 *Let $u \in X^+$ then we call u **primitive** if $u \in w^*$ implies $u = w$.*

With a name like primitive we can see that we will show that we can use these words as building blocks to create other words.

Theorem 6 *If there exist $u, v \in X^*$ and $n, m \geq 0$ such that $u^n = v^m$ then there exists w such that $u, v \in w^*$.*

Proof. Suppose that there exist $n, m \geq 0$ such that $u^n = v^m$ for some $u, v \in X^*$. If $u = v$ then the result is trivial so suppose that $u \neq v$. The set $\{u, v\}$ is not a code since $u^n = v^m$ and by the Deflect Theorem we get that their must exist $w \in X^*$ such that $u, v \in w^*$. $\square$

Now we can see that for all $u \in X^+$ we have $u^1 = u^1$ so there exists a unique primitive word such that $u \in w^*$.

Theorem 7 *The set of words that commute with a word $u \in X^+$ is a monoid generated by a single primitive word.*

Proof. Let z be a primitive word such that $a \in z^*$. If $ab = ba$ then the set $\{a, b\}$ is not a code. So there exists a word $c \in A^+$ such that $a, b \in c^*$. Moreover, $c \in z^*$ since z is primitive, thus the set of all words that commute with a is z^*. □

From **Theorem 7** we can see that there are commutative submonoids of X^*. Moreover, this is also free and has a code of $\{w\}$. These are all nice properties to have but it is disappointing that to get all of this we have to limit ourselves to only using one word, so let's leave the question of submonoids behind and see what we can say if we can only commute by breaking down a word into two fixed words.

Definition 14 *Two words $x, y \in X^*$ are said to be **conjugates** if there exist $u, v \in X^*$ such that $x = uv$ and $y = vu$.*

Let $aaba, abaa \in \{a, b\}^*$, then $aaba$ and $abaa$ are conjugates since $a, aba \in \{a, b\}^*$, $aaba = a(aba)$, and $abaa = (aba)a$.

Similarly to before, we will follow the steps of Lothaire, see [4], and find an easy way to check if two words are conjugates or each other.

Theorem 8 *Two words x and y are conjugates if and only if there exists a word z such that $xz = zy$. More precisely we can show that there exist words u and v such that $x = uv$, $y = vu$, and $z = u(vu)^*$.*

Proof. Suppose that $x, y \in X^*$ are conjugates, thus $x = uv$ and $y = vu$ for some $u, v \in X^*$, and let $z \in u(vu)^*$. We know that $z = u(vu)^n$ for some non-negative integer n. Thus, $xz = (uv)(u(vu)^n) = (u(vu)^n)(vu) = zy$.

Conversely, suppose that $xz = zy$ for some $z \in X^*$. Then for all $n \in \mathbb{N}$ $x^n z = zy^n$ also holds. Note that there exist an $n_0 \in \mathbb{N}$ such that

$$(n_0 - 1)n_X(x) \leq n_X(z) \leq n_0 n_X(x).$$

With this n_0 we get that

$$z = x^{n_0-1}u, \quad x = uv, \text{ and } vz = y^{n_0}.$$

Thus, $y = vz = vx^{n_0-1}u = (vu)^{n_0}$ so $y = vu$ showing that x and y are conjugates of each other. □

1.1.5 Formal Series

Now that we have a foundation of words, how to represent them, and some basic properties they can have, we can move on to problems involving words. Enumeration problems come up frequently when working with words, and to tackle these type of problems we will create a mapping from X^* to a ring, usually the integers.

Definition 15 *Let X be an alphabet and K be a ring with unity. A **formal series with coefficients in $\boldsymbol{K}$ and variables in $\boldsymbol{X}$** is a mapping from X^* to K. The set of all of these functions will be denoted by $\boldsymbol{K\langle\langle X\rangle\rangle}$.*

The notation we will be using comes from Lothaire, see [4], and is different from traditional functional notation. Let $\sigma \in K\langle\langle X\rangle\rangle$ and let $w \in X^*$, then we will denote the value of σ at w by $\langle\sigma, w\rangle$; we will call this value the coefficient of w in σ.

One of the most useful formal series is the characteristic series of $A \subset X$ defined as $\boldsymbol{A} : X^* \to \mathbb{Z}$,

$$\begin{cases} \langle \boldsymbol{A}, w\rangle = 1 & \text{if } w \in A \\ \langle \boldsymbol{A}, w\rangle = 0 & \text{if } w \notin A \end{cases}$$

Another useful formal series is n_X which gives the length of a word.

Definition 16 *Let $\sigma \in K\langle\langle X\rangle\rangle$; if all but finitely many of the coefficients of σ are 0, then we will call σ a **polynomial**. We will denote the set of all polynomials by $\boldsymbol{K\langle X\rangle}$.*

Note that the set $K\langle X\rangle$ is a subring of $K\langle\langle X\rangle\rangle$ since adding two polynomials will create a formal series which has at most a finite number of non-zero entries. A polynomial we will be using later on in this section is the characteristic series of a single word.

Now that we have defined formal series we are able to define operations on them, see Lothaire [4].

Definition 17 *Let $\sigma, \tau \in K\langle\langle X\rangle\rangle$, then for all $w \in X^*$*

$$\langle \sigma + \tau, w\rangle = \langle \sigma, w\rangle + \langle \tau, w\rangle$$

$$\langle \sigma\tau, w\rangle = \sum_{uv=w} \langle \sigma, u\rangle\langle \tau, v\rangle$$

With this definition the following theorem tells us how these operations interact with characteristic functions.

Theorem 9 *Let X be an alphabet and consider $A, B \subset X^*$ then the following are true*

i *Let $C = A \cup B$, then $\boldsymbol{C} = \boldsymbol{A} + \boldsymbol{B}$ if and only if $A \cap B = \emptyset$*

ii *Let $C = AB$, then $\boldsymbol{C} = \boldsymbol{AB}$ if and only if $xy = x'y'$ implies $x = x'$ and $y = y'$ for $x, x' \in A$ and $y, y' \in B$.*

iii *Let $A \subset X^+$ and $P = A^*$ then $\boldsymbol{P} = \boldsymbol{A^*}$ if and only if A is a code.*

Proof.

i Let $C = A \cup B$ and $w \in X^*$.

Assume that $\boldsymbol{C} = \boldsymbol{A} + \boldsymbol{B}$ and suppose that $A \cap B \neq \emptyset$. Thus, let $w \in A \cap B$ so $w \in C$ and $\langle \boldsymbol{A}, w\rangle = 1$, $\langle \boldsymbol{B}, w\rangle = 1$, and $\langle \boldsymbol{C}, w\rangle = 1$. This contradicts to the fact that $\boldsymbol{C} = \boldsymbol{A} + \boldsymbol{B}$ so $A \cap B = \emptyset$.

Conversely assume that $A \cap B = \emptyset$. If $w \in C$, then $\langle \boldsymbol{C}, w\rangle = 1$. Note if $w \in C$ then $w \in A$ or $w \in B$ and since $A \cap B = \emptyset$ then only one of the following equals 1, $\langle \boldsymbol{A}, w\rangle = 1$

or $\langle \boldsymbol{B}, w\rangle = 1$, so $\langle \boldsymbol{A}, w\rangle + \langle \boldsymbol{B}, w\rangle = 1$. If $w \notin C$ then, $\langle \boldsymbol{C}, w\rangle = 0$. Since $w \notin C$ then $w \notin A$ and $w \notin B$ so $\langle \boldsymbol{A}, w\rangle + \langle \boldsymbol{B}, w\rangle = 0$ Thus $\langle \boldsymbol{A}, w\rangle + \langle \boldsymbol{B}, w\rangle = \langle \boldsymbol{C}, w\rangle$ for all $w \in A$ so $\boldsymbol{C} = \boldsymbol{A} + \boldsymbol{B}$.

ii Let $C = AB$ and $w \in X^*$.

Suppose that $\boldsymbol{C} = \boldsymbol{AB}$ and suppose that there exists a word $w \in C$ that can be written in the following ways $w = xy$ and $w = x'y'$. Then

$$\langle \boldsymbol{C}, w\rangle = \langle \boldsymbol{AB}, w\rangle = \sum_{uv=w} \langle \boldsymbol{A}, u\rangle\langle \boldsymbol{B}, v\rangle \geq \langle \boldsymbol{A}, x\rangle\langle \boldsymbol{B}, y\rangle + \langle \boldsymbol{A}, x'\rangle\langle \boldsymbol{B}, y'\rangle = 2$$

But this contradicts to the fact that $\boldsymbol{C}$ is a characteristic function thus w can be written uniquely as an element of XY.

Conversely suppose $w \in C$, then $w = xy$ where $x \in A$ and $y \in B$ and this representation is unique. Thus, $\langle \boldsymbol{C}, w\rangle = \langle \boldsymbol{C}, xy\rangle = 1$ and $\langle \boldsymbol{A}, x\rangle\langle \boldsymbol{B}, y\rangle = 1 \cdot 1 = 1$. Now, if $w \notin C$ then clearly $\langle \boldsymbol{C}, w\rangle = 0 = \langle \boldsymbol{A}, x\rangle\langle \boldsymbol{B}, y\rangle$ where $w = xy$. Thus $\boldsymbol{C} = \boldsymbol{AB}$.

iii Let $A \subset X^+$ and $P = A^*$.

Suppose that $\boldsymbol{P} = \boldsymbol{A^*}$ and suppose that A is not a code. Since A is not a code we are able to write some $w \in P$ in two different ways $w = b_1 \dots b_n$ and $w = c_1 \dots c_m$. Note that from (i) and (ii) we get that

$$\boldsymbol{A^*} = \prod_{a \in A} \boldsymbol{a}$$

therefore

$$\langle \boldsymbol{P}, w\rangle = \langle \boldsymbol{A^*}, w\rangle = \prod_{i=1}^{n} \langle \boldsymbol{b_i}, b_i\rangle + \prod_{j=1}^{m} \langle \boldsymbol{c_j}, c_j\rangle = 2.$$

But this contradicts to the fact that $\boldsymbol{P}$ is a characteristic function so A^* is a code.

Conversely suppose that A is a code then, if $w \in P$ then $w = a_1 \dots a_n$ where $a_n \in A$ and this representation is unique. Similarly to before we get that

$$\boldsymbol{A^*} = \prod_{a \in A} \boldsymbol{a}$$

and since the representation is unique we get

$$\langle \boldsymbol{P}, w\rangle = \prod_{i=1}^{n} \langle \boldsymbol{a_i}, a_i\rangle = 1.$$

Clearly if $w \notin P$ then the coefficients of both series are 0. Thus, we have $\boldsymbol{P} = \boldsymbol{A^*}$.

□

Definition 18 *Let $\sigma \in K\langle\langle X\rangle\rangle$ and let $\lambda \in K\langle X\rangle$ then we can define the product of them as follows*

$$\langle \sigma, \lambda\rangle = \sum_{w\in X^*} \langle \sigma, w\rangle\langle \lambda, w\rangle$$

Note that since λ is a polynomial we will not have an infinite product when multiplying by a formal series, such as σ. Since polynomials are so useful we will try to carry on the property of having infinitely many zero coefficients to a family of formal series to generalize the definition of sums.

Now we can break down any formal series into a sum of this form and work with a sum of a locally finite family which are easier to work with.

Definition 19 *Let $\sigma_i \in K\langle\langle X\rangle\rangle$ for $i \in I$. We will call $(\boldsymbol{\sigma_i})_{\boldsymbol{i\in I}}$ **locally finite** if for all $w \in X^*$ all but finitely many of the coefficients $\langle \sigma_i, w\rangle$ are zero.*

With this new definition we will be able to generalize addition for a certain family of series.

Definition 20 *Let $(\sigma_i)_{i\in I}$ be a locally finite family. The **sum of $(\boldsymbol{\sigma_i})_{\boldsymbol{i\in I}}$**, denoted by σ, is a formal series defined by,*

$$\langle \sigma, w\rangle = \sum_{i\in I} \langle \sigma_i, w\rangle.$$

For a simple example of a locally finite family in an alphabet X let $a \in X$ then consider the formal series of families $(\boldsymbol{a}^n)_{n\in\mathbb{N}}$. Moreover any infinite family of characteristic functions is a locally finite family since for all $w \in X^*$ there will be at most one function whose coefficient is 1 while the rest will be 0. The importance of these locally finite families is given by the following theorem.

Theorem 10 *Let the locally finite family $(\boldsymbol{w})_{w\in X^*}$ and let $\sigma \in K\langle\langle X\rangle\rangle$ then we can write σ in terms of an infinite sum*

$$\sigma = \sum_{w\in X^*} \langle \sigma, w\rangle \boldsymbol{w}.$$

Proof. Consider the locally finite family $(\boldsymbol{w})_{w\in X^*}$ and let $\sigma \in K\langle\langle X\rangle\rangle$. Let $\lambda = \sum_{w\in X^*}$ and $v \in X^*$ then,

$$\langle \lambda, v\rangle = \sum_{w\in X^*} \langle \boldsymbol{w}, v\rangle = \langle \boldsymbol{v}, v\rangle = 1.$$

Form this it follows that $\sigma = \sum_{w\in X^*}\langle \sigma, w\rangle \boldsymbol{w}$. □

1.2 Infinite Words

1.2.1 Defining and Constructing Infinite Words

Let us move on to defining infinite words. Note that the definition of these types of words is basically a sequence but the way we are going to work with them will be a bit different. The definitions and theorems in this section come from Lothaire, see [4].

Definition 21 *Let X be an alphabet. An **infinite word on $\boldsymbol{X}$** is a function*

$$\boldsymbol{a} : \mathbb{N} \to A$$

and we will say that $\boldsymbol{a} = a_0a_1a_2\ldots a_n\ldots$, $a_i \in X$.

Definition 22 *Let $\boldsymbol{a}$ be an infinite word on an alphabet X and let μ be a homomorphism from X^* to another free monoid Y^*, then $\mu(\boldsymbol{a}) = \mu(a_0)\mu(a_1)\ldots$.*

Definition 23 *Let $\boldsymbol{a}$ be an infinite word on an alphabet X then the **left factor of length $\boldsymbol{k}$**, $k \in \mathbb{N}$, is $\boldsymbol{a}^{[k]} = a_0a_1\ldots a_{k-1}$.*

Note that we can create an infinite word out of an infinite word by considering everything after a left factor of length k, i.e. $\boldsymbol{a} = \boldsymbol{a}^{[k]}\boldsymbol{b}$ where $\boldsymbol{b} = a_ka_{k+1}\ldots$.

Definition 24 *Let* $\boldsymbol{a}$ *be an infinite word on an alphabet* X *then a* ***factor of*** $\boldsymbol{a}$ *is any word* $u \in X^*$ *such that there exists* $k \in \mathbb{N}$ *where* $\boldsymbol{a} = \boldsymbol{a}^{[k]}u\boldsymbol{b}$.

From these definitions we see that we can create an infinite word by just creating a sequence of letters in a given alphabet, but we can also create infinite words from a specific sequence of words.

Definition 25 *Let* $w_0, w_1, w_2, \ldots$ *be a sequence of words in* X^* *such that* $w_{n-1} \leq w_n$ *for all* $n \in \mathbb{N}$ *and the length of the words is increasing. Then define the infinite word* $\boldsymbol{a}$ *by* $\boldsymbol{a}^{[k]} = w_n$ *if* $|w_n| = k$. *The infinite word* $\boldsymbol{a}$ *is called* ***the limit of*** $(\boldsymbol{w_n})_{\boldsymbol{n}\in\mathbb{N}}$ *and written* $\boldsymbol{a} = \lim w_n$.

The last common way of creating an infinite word is using a special kind of homomorphism and iterate it on some letter of X.

Theorem 11 *Let* $\alpha : X^* \to X^*$ *be a homomorphism such that* $\alpha(a) \neq 1$ *for some* $a \in X$ *and there exists some letter* a_0 *such that* $\alpha(a_0) = au$ *for some* $u \in X^+$. *Then the* $\lim \alpha^n(a_0)$ *is an infinite word.*

Proof. Let $\alpha : X^* \to X^*$ be a homomorphism and a_0 be as described in the theorem. Then for any $n \in \mathbb{N}$ we have the following

$$\alpha^{n+1}(a_0) = \alpha^n(a_0u) = \alpha^n(a_0)\alpha^n(u).$$

From this we can see that $\alpha^n(a_0) \leq \alpha^{n+1}(a_0)$ for all $n \in \mathbb{N}$ so $\lim \alpha^n(a_0)$ is well defined and therefore is an infinite word. □

1.2.2 Proving Properties Using Infinite Words

Now that we know some common ways of creating and working with infinite words we will move on to proving that if an infinite word on an alphabet X has a property then there are infinitely many words in X^* with that property if that property is carried out to the factors of the word.

Definition 26 *Let P be a property that a word v can have, denoted $P(v)$. P is said to be* ***stable for factors*** *if $P(xuy)$ implies $P(u)$ for all words x, y, and u such that $v = xuy$.*

The set that denotes the words that satisfy P is $\boldsymbol{L_P} = \{w \in X^* \mid P(w)$ is satisfied$\}$.

Note that in the definition above the word with the property in question does not have to be finite. Note that if the word is infinite then when we break the word down at least on of its factors must be infinite.

Theorem 12 *Let X be a finite alphabet and let P be a property of elements that is stable for factors, then the set L_P is infinite if and only if there exists an infinite word on X with property P.*

Proof. Suppose that the set L_P is infinite. Since X is finite we know by the Pigeonhole Principle that there are infinitely many words in L_P that start with the same letter, call it $a_0 \in X$. Since P is stable for factors that means that a_0 has property P, this will be the base case for our induction. Now assume that there exists a word $a_0a_1 \dots a_n$ that has the property P, thus $a_0a_1 \dots a_n \in L_P$. Consider the set $(a_0a_1 \dots a_n)X^*$. This set is clearly infinite and therefore once more by the Pigeonhole Principle there exists a letter a_n such that $L_P \cap (a_0a_1 \dots a_na_{n+1})X^*$ is infinite, thus $a_0a_1 \dots a_na_{n+1} \in L_P$. In conclusion, we created an infinite word letter by letter at is in L_P.

Conversely, suppose that there is an infinite word $\boldsymbol{a}$ on X with a stable property for factors P. Since P is a stable property for factors then every left factor of the infinite word $\boldsymbol{a}$ has property P. Therefore, $a^{[k]} \in L_P$ for all $k \in \mathbb{N}$ making L_P infinite. □

1.2.3 Infinite Square-Free Word

To be able to show that there is an infinite square-free word we must first show that there is an infinite word with no overlap called the infinite word of Thue-Morse. We will then create a homomorphism to apply to the infinite word with no overlap to create the square-free word. This construction of an infinite square-free word can be found in Lothaire and Mikalev, see [4, 5].

Definition 27 *Let X be an alphabet and let $w \in X^*$ where $w = a_0a_1 \dots a_n$ and $a_i \in X$ for all i. Then we will define the* ***reversal of w*** *by $\widetilde{w} = a_n a_{n-1} \dots a_1 a_0$. We will call a word w a* ***palindrome*** *if $w = \widetilde{w}$.*

If we are considering the reversal of a word, w, that is we can describe as the product of two words, $w = uv$, we will use the following notation, $\widetilde{w} = \widetilde{(uv)}$.

Definition 28 *Let $X = \{a, b\}$ and let $w \in X^*$. We will define the* ***complement of w*** *as by $\overline{w}$ where the every a in w is replaced with b and similarly every b is replaced with a.*

For example let $w = abbaba$ then $\overline{w} = baabab$.

Remark 2 *It is clear from the definition that $\overline{\overline{w}}$ and $\overline{wv} = \overline{wv}$ for any $w, v \in \{a, b\}^*$.*

Let $X = \{a, b\}$, this will be the alphabet we will use for the rest of the section unless specified otherwise, consider the homomorphism

$$\mu : X^* \to X^* \text{ where } \mu(a) = ab \text{ and } \mu(b) = ba.$$

We will use this homomorphism for the rest of the section.

Theorem 13 *Let $u_0 = a$, $v_0 = b$, and for any $n \geq 0$ we have $u_{n+1} = u_n v_n$ and $v_{n+1} = v_n u_n$. The following properties of μ are true:*

i $u_n = \mu^n(a)$ *and* $v_n = \mu^n(b)$ *for* $n \geq 0$.

ii $v_n = \overline{u}_n$ *and* $u_n = \overline{v}_n$ *for* $n \geq 0$.

iii u_{2n} *and* v_{2n} *are palindromes for* $n \geq 1$.

iv $u_{2n+1} = v_{2n+1}$ *for* $n \geq 0$.

Proof.

i For $n = 0$, μ^0 is just the identity mapping therefore $u_0 = a = \mu^0(a)$ and $v_0 = b = \mu^0(b)$. Moreover, note that $\mu^0(a)\mu^0(b) = ab = \mu^1(a)$ and $\mu^0(b)\mu^0(a) = ba = \mu^1(b)$.

Now suppose that, $u_n = \mu^n(a)$, $v_n = \mu^n(b)$, and $\mu^n(a)\mu^n(b) = \mu^{n+1}(a)$ for some n. Now

$$u_{n+1} = u_n v_n = \mu^n(a)\mu^n(b) = \mu^{n+1}(a),$$

therefore doing an induction on product of homomorphisms, we get that $\mu^n(a)\mu^n(b) = \mu^{n+1}(a)$ so we conclude that $u_{n+1} = \mu^{n+1}(a)$. Similarly, $v_{n+1} = \mu^{n+1}(b)$ completing the induction.

ii As a base for the induction note that $\overline{u_0} = \overline{a} = b = v_0$ and $\overline{v_0} = \overline{b} = a = u_0$.

Now suppose that, $v_n = \overline{u}_n$ and $u_n = \overline{v}_n$ for some n. Then, $\overline{u_{n+1}} = \overline{u_n v_n} = \overline{u_n v_n} = v_n u_n = v_{n+1}$. Similarly, $\overline{v_{n+1}} = u_{n+1}$.

iii For the case of $n = 1$ we can see that $u_2 = abba = \widetilde{u_2}$ and $v_2 = baab = \widetilde{v_2}$.

Suppose that u_n and v_n are palindromes and consider $\widetilde{u_{n+2}} = (u_{n+1}v_{n+1})\tilde{} = (u_n v_n v_n u_n)\tilde{} = u_n v_n v_n u_n = u_{n+1}v_{n+1} = u_{n+2}$ so u_{n+2} is a palindrome and similarly for v_{n+2}.

iv For $n = 0$ we have that $u_1 = ab = v_1$.

Now suppose that, $u_{2n-1} = v_{2n-1}$ for some n, and from here we can see that

$$u_{2n+1} = u_{2n}v_{2n} = (u_{2n-1}v_{2n-1})(v_{2n-1}u_{2n-1}) = (v_{2n-1}u_{2n-1})(u_{2n-1}v_{2n-1}) = v_{2n}u_{2n} = v_{2n+1}.$$

□

Remark 3 *By iterating μ on a we create an infinite word $\boldsymbol{t} = abbabaabbaababba\ldots$ likewise iterating μ on b we also create an infinite word $\overline{\boldsymbol{t}} = baababbaabbabaab\ldots$. $\boldsymbol{t}$ and $\overline{\boldsymbol{t}}$ are known as the infinite words of Thue-Morse.*

We will use the following two lemmas to show that $\boldsymbol{t}$ has no overlapping factors.

Lemma 1 *Let $Y = \{ab, ba\}$. If $w \in Y^*$, then $awa, bwb \notin Y^*$.*

Proof. This proof will be done by induction on $n_Y(w)$. If $n_Y(w) = 0$ then $w = 1$ and we only have two cases to consider and indeed $aa, bb \notin X^*$.

Now suppose that u is the smallest word (in terms of length) in Y^* such that $u = awa$ or $u = bwb$ for some $w \in Y^*$. Without loss of generality assume that $u = awa \in Y^*$, where $u = u_1 \dots u_n$ and $u_i \in Y$ for all i. We know that $u_1 = ab$ and that $u_n = ba$, therefore $u = abvba$ for some $v \in Y^*$. This means that there exist a smaller word than u, which we will denote by v, for which $bvb \in Y^*$. This contradicts the minimality of u so $awa \notin Y^*$ and $bwb \notin Y^*$. □

Lemma 2 *Let $w \in X^*$. If w has no overlapping factors, then $\mu(w)$ has no overlapping factors.*

Proof. By contraposition suppose that there exists some $w \in X$ such that $\mu(w)$ has an overlapping factor. Since $\mu(w)$ has an overlapping factor we know that there exist $x, y, v \in X^*$ and $c \in X$ such that $\mu(w) = xcvcvcy$. Since $x, y, v \in X^*$ they have even length and since $c \in X$ we know that $n_X(cvcvc)$ and $n_X(xy)$ are odd. Now note that since μ is a homomorphism we can apply to each letter individually therefore $\mu(w) \in \{ab, ba\}^* = Y^*$. Thus we have two cases.

Case 1: $n_X(x)$ is even and $x, cvcv, cy \in Y^*$

Case 2: $n_X(x)$ is odd and $xc, vcvc, y \in Y^*$

In both case we can deduce from Lemma 1 that $n_X(v)$ is odd since if it was even then $cvcv \in Y^*$ or $vcvc \in Y^*$ would give us $v, cvc \in Y^*$.

Note if $n_X(x)$ is even we can see that $cv \in Y^*$ and we can break down $w = rsst$ with $r, s, t \in X^*$, $\mu(r) = x$, $\mu(s) = cv$, and $\mu(t) = cy$. Note that s and t must start with the same letter to give that their image under μ starts with c so w has an overlapping factor.

Now if $n_X(x)$ is odd we have a similar case. We can break down $w = rsst$ with $r, s, t \in X^*$, $\mu(r) = xc$, $\mu(s) = vc$, and $\mu(t) = y$. In this case we get that r and s give us the overlapping factor in w. □

Theorem 14 ***t*** *has no overlapping factors.*

Proof. Assume towards contradiction that $\boldsymbol{t}$ has an overlapping factor. If $\boldsymbol{t}$ has an overlapping factor that means there exists a natural number k such that the overlapping factor is in the left factor $\mu^k(a)$. Note that a has no overlapping factors so applying Lemma 2 k times we would deduce that $\mu^k(a)$ has no overlapping factors which is a contradiction, therefore $\boldsymbol{t}$ has no overlapping factors. □

Sadly *the infinite word of Thue-Morse* is not square-free but we will now create a homomorphism to create a square-free word using *the infinite word of Thue-Morse*.

Let $X = \{a, b\}$ and $Y = \{a, b, c\}$. Consider the homomorphism

$$\lambda : Y^* \to X^* \text{ where } \lambda(a) = abb, \quad \lambda(b) = ab, \text{ and } \lambda(c) = a.$$

With this homomorphism we can take any infinite word $\boldsymbol{b}$ on Y and create an infinite word on X that starts with the letter a.

Lemma 3 *Let $\boldsymbol{a}$ be an infinite word on $X = \{a, b\}$ that starts with the letter a and has no overlapping factors, then we can write $\boldsymbol{a} = y_0 y_1 \dots y_n \dots$ where $y_n \in \{a, ab, abb\}$. The factorization is unique.*

Proof. We can clearly see that any a in $\boldsymbol{a}$ must be followed by at most two b's since bbb is an overlapping factor. That justifies the inclusion of ab and abb. To justify the inclusion of a note that aa is not an overlapping factor.

For uniqueness suppose that $\boldsymbol{a} = y_0 y_1 \cdots = z_0 z_1 \dots$ where $y_n, z_n \in \{a, ab, abb\}$. Note that since words are left cancellative there must be some $k \in \mathbb{N}$ where $y_k \neq z_k$. But due to the set $\{a, ab, abb\}$ we can assume without lost of generality that $y_k < z_k$ meaning that y_{k+1} has to start with b but that is a contradiction. □

This lemma tells us that given any infinite word on X without overlapping factors we can find a unique infinite work on Y, $\boldsymbol{b}$, with the property that $\lambda(\boldsymbol{b}) = \boldsymbol{a}$

Theorem 15 *Let $\boldsymbol{a}$ be an infinite word on X that starts with the letter a and has no overlapping factors and and let $\boldsymbol{b}$ be an infinite word on Y such that $\lambda(\boldsymbol{b}) = \boldsymbol{a}$, then $\boldsymbol{b}$ is square-free.*

Proof. Assume towards contradiction that $\boldsymbol{b}$ is not square-free, then there exists some word $u \in Y^*$ such that uu is in $\boldsymbol{b}$. Let d be the letter after uu in $\boldsymbol{b}$. Since λ is a homomorphism we can study $\lambda(uud)$. We know that $\lambda(uud)$ is a factor of $\boldsymbol{a}$. Now recall that all the images of λ start with a so $\lambda(uud) = avavaw$ for some $v, w \in X^*$, so $\boldsymbol{a}$ has an overlapping factor which is a contradiction. Therefore, we can conclude that $\boldsymbol{b}$ is square-free. □

With this theorem and lemma we can say that $\boldsymbol{t}$ is produced by a infinite square-free word which is usually called $\boldsymbol{m}$. We can construct $\boldsymbol{m}$ by breaking down $\boldsymbol{t}$ into the $y_n \in \{a, ab, abb\}$ from Lemma 3 and creating $\boldsymbol{m}$ one letter at a time.

Another way of constructing $\boldsymbol{m}$, which does not depend on $\boldsymbol{t}$, is by iterating the homomorphism

$$\phi : X^* \to X^*, \phi(a) = abc, \quad \phi(b) = ac, \text{ and } \phi(c) = b$$

on a, thus

$$\lambda(\boldsymbol{t}) = \boldsymbol{m} = \lim \phi^n(a),$$

see [4].

Chapter 2

Algebraic Properties of Free Semigroups

2.1 Relations and Mappings

This goal of this section is to introduce relations that are able to work with the binary relations on a semigroup or monoid. We will look at specific sets that are created from these relations. Moreover, in this section we will be looking at mappings between the algebraic structures that we have been studying. The notations and theorems from this section were obtained from Howie, see [3].

Let us start by getting some basic definitions and conventions that we will be using out of the way.

Definition 29 *A relation ρ on sets X and Y is a subset of the Cartesian product $X \times Y$, if we have $X = Y$ then we call ρ a* ***relation on X****.*

There is some common terminology that we will be using such as if $(x, y) \in \rho$ then we will say that x is related to y and will often use the notation $x\rho y$. Note that relations do not have to be symmetric therefore stating that y is related to x is not given. We will also use the notation

$$x\rho = \{y \in X : x\rho y\}$$

to describe the set of all elements related to x.

The diagonal, $\{(x, x) : x \in X\}$, is relation that we will often refer to, so we will conveniently refer to it as 1_X.

Relations are usually described as the generalization of mappings since they do not have the restriction that every element has to be related to a element and that it can only related to one element. From this idea of generalizing mappings comes the next definitions.

Definition 30 *Let ρ be a relation on a set X then the following sets are known as the* ***domain and image of the relation*** *respectively,*

$$dom(\rho) = \{x \in X : \text{ there exists } y \in X \text{ such that } x\rho y\},$$

$$im(\rho) = \{y \in X : \text{ there exists } x \in X \text{ such that } x\rho y\}.$$

Definition 31 *Let ρ be a relation on a set X. Then we call ρ a* ***partial mapping*** *if $|x\rho| = 1$ for all $x \in dom(\rho)$. If $dom(\rho) = X$ then we will call ρ a* ***map****.*

Notice that in this generalization not every element in X has to related to an element but we keep the restriction that every element that is actually related to an element is related to exactly one element of X. Since it is suppose to be a generalization of mappings it can be seen that an equivalent definition of a partial mapping is: if $x\rho y$ and $x\rho z$ then $y = z$.

Similarly to mappings we can compose to relations by the following definition.

Definition 32 *Let ρ and σ be relations on X, then* ***the composition of ρ and σ*** *is denoted*

$$\rho \circ \sigma = \{(x, y) \in X \times X : \text{ there exists } z \in X \text{ such that } x\rho z \text{ and } z\rho y\}.$$

From this definition it is easy to see that composition of partial maps is a binary relation on the set of all partial maps denoted $\mathcal{P}_{\mathcal{X}}$. Recall that functions with the same domain and codomain form a monoid with their composition. Similarly we have that the composition of partial maps is associative and the relation 1_X is the identity element. With this intuition in mind we go consider the following remark.

Remark 4 *$\mathcal{P}_{\mathcal{X}}$ is a monoid with the operation $\circ$, where $\mathcal{P}_{\mathcal{X}}$ is the set of all partial maps on a non-empty set X.*

Definition 33 *Let ρ be a relation on a sets X and Y then we will call $\rho^{-1} = \{(y, x) \in Y \times X : x\rho y\}$ the* ***inverse of ρ****.*

Note that ρ^{-1} is always a relation but it is not always guaranteed that the inverse of a partial map is a partial map. For a quick example consider $\rho : a, b \to a, b$ where $a\rho = \{a\}$ and $b\rho = \{a\}$. Then ρ^{-1} is not a partial map since $|a\rho^{-1}| = 2$.

Since we will be sometimes dealing with a monoid it is always necessary to make the distinction between the inverse relation and the inverse relation in terms of the operation of composition.

Now we will turn our attention to one of the most useful types of relations.

Definition 34 *Let ε be a relation on X, then we call ε an* ***equivalence relation*** *if ε satisfies the following properties*

i $1_X \subset \varepsilon$ *(reflexive)*

ii $\varepsilon = \varepsilon^{-1}$ *(symmetric)*

iii $\varepsilon \circ \varepsilon \subset \varepsilon$ *(transitive)*

Remark 5 *Symmetry can can also be reformulated in these terms $x\varepsilon y$ then $y\varepsilon^{-1}x$.*

Likewise, transitivity can also be reformulated in the terms of $x\varepsilon z$ and $z\varepsilon y$ then $x\varepsilon y$.

Equivalence relations are an essential tool for studying many areas of mathematics due to the following theorem.

Theorem 16 *Let ε be an equivalence relation on a non-empty set X, then the sets*

$$x\varepsilon \text{ for } x \in X$$

create a partition on X.

Conversely, if we have a partition of X, $\{A_i\}_{i\in I}$ then the relation

$$x\rho y \text{ if } x, y \in A_i \text{ for some } i.$$

is an equivalence relation.

Proof. Let ε be an equivalence relation on X and we have to show that the sets of the form $x\varepsilon$ form a partition.

i From relexivity we get that $x \in x\varepsilon$ for all $x \in X$.

ii Now let $x, y \in X$ such that $x\varepsilon \cap y\varepsilon \neq \emptyset$. Then there exists $z \in x\varepsilon \cap y\varepsilon$. That is $x\varepsilon z$ and $z\varepsilon y$ and from transitivity we get that $x\varepsilon y$ implying that $x\varepsilon = y\varepsilon$.

iii Since $x\varepsilon \subset X$ for all $xinX$ we get that $\cup_{x\in X} x\varepsilon \subset X$. To show the other inclusion, let $a \in X$. Then $a \in a\varepsilon$ from (i) so $a \in \cup_{x\in X} x\varepsilon$ and thus $X \subset \cup_{x\in X} x\varepsilon$

From $(i), (ii)$, and (iii) we can see that the sets $x\varepsilon$ for $x \in X$ create a partition on X.

For the converse, let $\{A_i\}_{i\in I}$ be a partition on X and define ρ as stated by the theorem.

i Since $\{A_i\}_{i\in I}$ is a partition then for all $x \in X$ we have that $x \in A_i$ for some i, thus $x\rho x$ for all $x \in X$.

ii Suppose that $x\rho y$ then $x, y \in A_i$ for some i. Then $y, x \in A_i$ so $y\rho^{-1}x$.

iii Suppose that $x\rho y$ and $y\rho z$ then $x, y \in A_i$ and $y, z \in A_j$. Since $\{A_i\}_{i\in I}$ is a partition then $A_i = A_j$ so $x, z \in A_i$ implying that $x\rho z$.

From $(i), (ii)$, and (iii) we can see that ρ is an equivalence relation. □

The following theorem allows us to create an equivalence relation from any mapping.

Theorem 17 *Let $\rho : X \to Y$ be a mapping, then $\rho \circ \rho^{-1}$ is an equivalence relation.*

Proof. Let $\rho : X \to Y$ be a mapping, then $x\rho \neq \emptyset$ for all $x \in X$. Let $y \in x\rho$. We can see that $x \in y\rho^{-1}$, therefore $(x, x) \in \rho \circ \rho^{-1}$ for all x. Showing that $1_X \subset \rho \circ \rho^{-1}$.

Suppose that $x(\rho\circ\rho^{-1})z$. This implies that there exists $y \in Y$ such that $x\rho y$ and $y\rho^{-1}z$. From here we can see that $z(\rho \circ \rho^{-1})^{-1}x$.

Suppose that $x(\rho \circ \rho^{-1})y$ and $y(\rho \circ \rho^{-1})z$. Then there exists $a, b \in Y$ such that $x\rho a$, $a\rho^{-1}y$, $y\rho b$, and $b\rho^{-1}z$. Since ρ is a mapping we get that $a = b$. Therefore we get that $x(\rho \circ \rho^{-1})z$ making $\rho \circ \rho^{-1}$ transitive. □

Definition 35 *The equivalence relation from the previous theorem, $\rho \circ \rho^{-1}$, is known as the* ***kernel of ρ*** *and is denoted $ker(\rho)$.*

Similarly to the previous theorem, the next theorem will also lead to a new definition.

Theorem 18 *Let us denote $\{\varepsilon\}_{i\in I}$ to be a family of equivalence relations on a set X then*

$$\cap_{i\in I}\varepsilon_i$$

is also an equivalence relation on X.

Proof. Out of convenience let $\cap_{i\in I}\varepsilon_i = \mathcal{E}$. Note that $1_X \subset \varepsilon_i$ for all $i \in I$ so $1_X \subset \mathcal{E}$.

Suppose that $x\mathcal{E}y$, then $x\varepsilon_i y$ for all $i \in I$. Since each ε_i is an equivalence relation we get that $y\varepsilon_i^{-1}x$ for all $i \in I$ so $y\mathcal{E}^{-1}x$.

Now suppose that $x\mathcal{E}y$ and $y\mathcal{E}z$, then $x\varepsilon_i y$ and $y\varepsilon_i z$ for all i. Since these are equivalence relations we get that $x\varepsilon_i z$ for all i, thus $x\mathcal{E}z$. □

Definition 36 *Let ρ be a relation on a set X then we will denote $\boldsymbol{\rho^e}$ to be the smallest, in terms of set inclusion, equivalence relation containing ρ.*

Since equivalence relations are closed under intersections then the previous definition is well defined since we can just take the intersection of all the equivalence relations that contain ρ,

$$\rho^e = \cap_{i\in I}\varepsilon_i$$

where ε_i is an equivalence relation containing ρ. This is a not the nicest definition to work with. Therefore, following the ideas presented in Howie, see [3], we will create an equivalent condition that we can work with better.

Definition 37 *Let ρ be a reflexive relation on a set X then we will define*

$$\boldsymbol{\rho^{\infty}} = \cup_{n\in\mathbb{N}}\rho^n$$

where $\rho^n = \rho \circ \rho \circ \cdots \circ \rho$, n many times.

We force ρ to be reflexive so we insure that $\rho^n \subset \rho^{n+1}$ for all $n \in \mathbb{N}$. ρ^{∞} is usually transitive closure of ρ due to the following theorem.

Theorem 19 *If ρ is a reflexive relation on a set X, then ρ^{∞} is the smallest transitive relation that contains ρ.*

Proof. We will start off by showing that ρ^{∞} is transitive. Suppose that $x\rho^{\infty}y$ and $y\rho^{\infty}z$. This means that there exists $i, j \in \mathbb{N}$ such that $x\rho^i y$ and $y\rho^j z$. We can now see that $x(\rho^i \circ \rho^j)z$ which is the same as saying $x\rho^{i+j}z$. From the definition of ρ^{∞} we can see that $\rho^{i+j} \subset \rho^{\infty}$. We can now conclude that $x\rho^{\infty}z$ showing that ρ^{∞} is transitive.

To show that ρ^{∞} is the smallest relation on X that contains ρ, let σ be a transitive relation that contains ρ. Note that $\rho^2 \subset \rho \circ \rho \subset \sigma \circ \sigma$. Recall that σ is transitive so $\sigma \circ \sigma \subset \sigma$, thus $\rho^2 \subset \sigma$. By induction we can see that $\rho^n \subset \sigma$ for any $n \in \mathbb{N}$, therefore $\rho^{\infty} \subset \sigma$.

□

With this new definition we can now give a workable definition to ρ^e by this following theorem.

Theorem 20 *Let ρ be a relation on X, then*

$$\rho^e = (\rho \cup \rho^{-1} \cup 1_X)^{\infty}.$$

Proof. Out of convenience let $P = (\rho \cup \rho^{-1} \cup 1_X)^{\infty}$. Note that P is a transitive and reflexive relation. Moreover, since $\rho \cup \rho^{-1} \cup 1_X$, we get that P is symmetric. Thus, P is an equivalence relation.

Now we are going to show that P is the smallest equivalence relation containing ρ. Let ε be an equivalence relation containing ρ. Note that $1_X \subset \sigma$ and $\rho \subset \sigma$. Moreover, since σ is symmetric we get that $\rho^{-1} \subset \sigma^{-1} = \sigma$. These subset conditions imply that $\rho \cup \rho^{-1} \cup 1_X \subset \sigma$. Now we have,

$$(\rho \cup \rho^{-1} \cup 1_X)^2 = (\rho \cup \rho^{-1} \cup 1_X) \circ (\rho \cup \rho^{-1} \cup 1_X) \subset \sigma \circ \sigma = \sigma.$$

By induction we get that $(\rho \cup \rho^{-1} \cup 1_X)^n \subset \sigma$ for all $n \in \mathbb{N}$. Therefore, $P \subset \sigma$. This shows that P is the smallest equivalence relation that contains ρ, i.e. ρ^e. □

2.1.1 Congruences and $\rho^\sharp$

Now that we have laid a solid foundation for relations we are now able to see how these relations and operations from semigroups (and monoids) interact with the goal in mind that we will be using congruences to represent a specific semigroup.

Definition 38 *A relation ρ on a semigroup S is called **left (right) compatible** if for all $a, x, y \in S$ we have*

$$\textit{if } x\rho y \textit{ then } (ax)\rho(ay) \qquad (\textit{ if } x\rho y \textit{ then } (xa)\rho(ya) \ )$$

Definition 39 *We say a relation ρ on a semigroup S is **compatible** if*

$$\textit{if } a\rho b \textit{ and } x\rho y \textit{ then } (ax)\rho(by)$$

for all $a, b, x, y \in S$.

Remark 6 *A relation is compatible if and only if it is right and left compatible.*

Now we will prove some useful theorems that will assist us in working with compatible relations.

Theorem 21 *Let ρ be a compatible relation on a semigroup S, then ρ^n is compatible for all $n \in \mathbb{N}$.*

Proof. Let $x\rho^2 y$, then there exists $z \in S$ such that $x\rho z$ and $z\rho y$. Since ρ is right compatible we get that $ax\rho az$ and $az\rho ay$ for every $a \in S$, therefore $ax\rho^2 ay$. Similarly we can show that ρ^2 is left compatible showing that ρ^2 is compatible. Now by induction we get that ρ^n is compatible for all $n \in \mathbb{N}$. □

Theorem 22 *A right and left compatible equivalence relation ε on a semigroup S is compatible on S.*

Proof. Suppose that ε is a right and left compatible equivalence relation on a semigroup S and $a\varepsilon b$ and $x\varepsilon y$. From right compatibility we get that $(ax)\varepsilon(bx)$. Similarly, by left compatibility we get that $(bx)\varepsilon(by)$. Now by transitivity we get that $(ax)\varepsilon(by)$. □

Compatible equivalence relations are going to be used so often that it will be useful to give them a name.

Definition 40 *Let σ be a relation on a semigroup S then we say σ is a **congruence** if σ is an equivalence relation and compatible on S.*

Since we will be working with quotient sets in this section it will be useful to define the following mapping.

Definition 41 *Let ρ be a congruence on a semigroup X then we can define*

$$\boldsymbol{\rho^\natural} : X \to X/\rho \text{ where } a\rho^\natural = a\rho$$

for all $x \in X$.

This mapping is well defined since ρ is an equivalence relation so there is no possible way that an element of X can be mapped to distinct subsets of X.

Remark 7 *Let X be a semigroup and let ρ be a congruence relation then X/ρ is a semigroup under the following operation,*

$$(x\rho)(y\rho) = (xy)\rho$$

for all $x, y \in X$.

Theorem 23 *$\rho^\natural$ as defined above is a homomorphism.*

Proof. Let $a, b \in X$. Consider $(ab)\rho^\natural = (ab)\rho = (a\rho)(b\rho) = (a\rho^\natural)(b\rho^\natural)$ □

Now we can move on to prove a useful property of congruences.

Theorem 24 *Let $\{\sigma_i\}_{i\in I}$ be a family of congruences on a semigroup S, then*

$$\cap_{i_I}\sigma_i$$

is also a congruence.

Proof. Let Since we know that intersection of arbitrary equivalence relations is an equivalence relation so we only have to show that $\cap_{i_I}\sigma_i$ is compatible.

Suppose that $a(\cap_{i_I}\sigma_i)b$ and $x(\cap_{i_I}\sigma_i)y$, then $a\sigma_i b$ and $x\sigma_i y$ for all $i \in I$. Since each $sigma_i$ is compatible we get that $(ax)\sigma_i(by)$ for all $i \in I$, therefore, $(ax)(\cap_{i_I}\sigma_i)(by)$. □

Definition 42 *Let ρ be a relation on a semigroup S, then we denote the smallest, in terms of set inclusion, congruence containing ρ by $\boldsymbol{\rho^\sharp}$*

Since the intersection of congruences is closed by intersection, this definition makes sense because we can just consider the intersection of all congruences containing a relation, i.e.

$$\rho^\sharp = \cap_{i\in I}\sigma_i$$

where σ_i is a congruence containing ρ. This definition and reasoning is very similar to the one used for ρ^e.

Similar to how we found a nice way of finding ρ^e for any given relation, ρ, we will do the same for $\rho^\sharp$ following the ideas presented in Howie, see [3]. Similarly for this we will have to define some more concepts and prove a couple of theorems so let us start with some new definitions.

Definition 43 *Let ρ be a relation on a monoid X then*

$$\boldsymbol{\rho^c} = \{(xay, xby) \mid x, y \in X \text{ and } a\rho b\}.$$

By **Theorem 24** and the same logic we have used before for ρ^e and ρ^∞ we will show the following theorem.

Theorem 25 *For any relation ρ on a monoid X, ρ^c is the smallest compatible relation that contains ρ.*

Proof. Since X is a monoid we can see that $(1a1)\rho^c(1b1)$ showing that $\rho \subset \rho^c$. Now to show that ρ^c is compatible we will show that it is left and right compatible. Suppose that $u\rho^c v$, then $u = xay$ and $v = xby$ for some $x, y \in X$ and $a\rho b$. Now let $z \in X$, then $zu = (zx)ay$ and $zv = (zx)by$. Thus, $zu\rho^c zv$. It can be shown in a similar fashion that ρ^c is right compatible.

Now suppose that σ is a compatible relation that contains ρ. Since σ is compatible and contains ρ then $axy\sigma ayb$ for all $a, b \in X$ and $x\rho y$. Thus, $\rho^c \subset \sigma$. □

Now the following lemma show some useful properties of ρ^c that will be useful in the proof of some properties of $\rho^\sharp$.

Lemma 4 *Let ρ and σ be relations on a semigroup X then the following properties hold,*

i *if $\rho \subset \sigma$ then $\rho^c \subset \sigma^c$*

ii $(\rho^{-1})^c = (\rho^c)^{-1}$

iii $(\rho \cup \sigma)^c = \rho^c \cup \sigma^c$

Proof.

i Suppose that $\rho \subset \sigma$, then $a\sigma b$ whenever $a\rho b$. From here we can see that for all $x, y \in X$ $xay\rho xby$ implies that $xay\sigma xby$.

ii Let $u(\rho^{-1})^c v$ then $u = xay$ and $v = xby$ for some $x, y \in X$ and $a\rho^{-1}b$. We know that $b\rho a$ so $xby\rho^c xay$, which is $v\rho^c u$. Thus, we get $u(\rho^c)^{-1}v$.

iii Suppose that $u(\rho \cup \sigma)^c v$, then $u = xay$ and $v = xby$ where $a(\rho \cup \sigma)b$. From $a(\rho \cup \sigma)b$ we know that $a\rho b$ or $a\sigma b$. If we have $a\rho b$ then $u\rho^c v$. If we have $a\sigma b$ then $u\sigma v$. Therefore, $(\rho \cup \sigma)^c \subset \rho^c \cup \sigma^c$.

For the other inclusion, suppose that $u(\rho^c \cup \sigma^c)v$ where $u\rho^c v$ or $u\sigma^c v$. Giving us that for $x, y \in X$ we have $u = xay$ and $v = xby$, where $a\rho b$ or $a\sigma b$. Thus $a(\rho \cup \sigma)b$ giving us that $xay(\rho \cup \sigma)^c xby$. Therefore, $\rho^c \cup \sigma^c \subset (\rho \cup \sigma)^c$.

□

Remark 8 *The last property that we will need for ρ^c is that $1_X = 1_X^c$ for any non-empty set X, which is clear.*

With these properties in mind we are finally able to prove the following theorem.

Theorem 26 *For any relation ρ on a semigroup X we have that*

$$\rho^\sharp = (\rho^c)^e.$$

Proof. Note that ρ^c contains ρ and $(\rho^c)^e$ is the smallest equivalence relation containing ρ^c and thus it contains ρ. Thus, we only have to show that $(\rho^c)^e$ is compatible.

Recall that we know that

$$(\rho^c)^e = (\rho^c \cup (\rho^c)^{-1} \cup 1_X^c)^\infty$$

and by the previous lemma we get

$$(\rho^c \cup (\rho^c)^{-1} \cup 1_X^c) = (\rho \cup \rho^{-1} \cup 1_X)^c.$$

Note that $(\rho \cup \rho^{-1} \cup 1_X)^c$ is compatible and $((\rho \cup \rho^{-1} \cup 1_X)^c)^n$ is compatible for all $n \in \mathbb{N}$ by **Theorem 23**. Therefore, $((\rho \cup \rho^{-1} \cup 1_X)^c)^\infty$ is compatible.

The only thing left to show is that $(\rho^c)^e$ is the smallest congruence containing ρ. Let σ be a congruence containing ρ. Notice that $\sigma^c = \sigma$ by definition of σ^c, and since $\rho \subset\subset \sigma$ we have that $\rho^c \subset \sigma^c = \sigma$ by **Lemma 4**. Recall that $(\rho^c)^e$ is the smallest equivalence containing ρ^c and σ is an equivalence, thus $(\rho^c)^e \subset \sigma$. □

2.2 Free Semigroups

Throughout this section note that we will be focusing on semigroups but all the definitions make sense and theorems are true if the word semigroup is replaced with monoid.

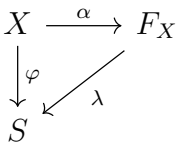
2.2.1 Categorical Definition

In this section we are going to be working with an alternative, more general, definition of Free Semigroups found in Howie, see [3]. Moreover, we are going to connect this new definition to the earlier definition in Chapter 1, so let us start with the new alternative definition.

Theorem 27 *A semigroup F_X is free on a set X if and only if*

i *There exists a function $\alpha : X \to F_X$*

ii *For any semigroup S and $\varphi : X \to S$ there exists a unique homomorphism $\lambda : F_X \to S$ such that*



commutes, i.e. $\lambda\alpha = \phi$.

Proof. Let X^+ be a free semigroup on an alphabet X. Define

$$\alpha : X \to X^+, \alpha(x) = x.$$

Note that this function just takes the letters in X to the words of length one in X^+. This function is usually called the natural embedding.

Now let S be a semigroup and let φ be a function from X onto S. We will define

$$\lambda : X^+ \to S, \lambda(x) = \varphi(x_1) \dots \varphi(x_n).$$

This function takes a word, applies φ to each of its letters and then multiplies them in S. To show that λ is a homomorphism, let $x, y \in X^+$ and consider,

$$\lambda(xy) = \varphi(x_1) \dots \varphi(x_n)\varphi(y_1) \dots \varphi(y_m) = \lambda(x)\lambda(y).$$

Now to show that the diagram commutes, let $a \in X$, then we have

$$\lambda\alpha(a) = \lambda(a) = \varphi(a).$$

Conversely, let conditions (i) and (ii) hold when X is an alphabet, $S = X^+$ and $\varphi = \beta$ which will be the standard embedding. We will show that λ is actually a isomorphism. Since the following diagram commutes,

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & F_X \\ \downarrow{\scriptstyle \beta} & \swarrow{\scriptstyle \lambda} & \\ X^+ & & \end{array}$$

we have that $\lambda\alpha = \beta$. Suppose that for $a, b \in X$ we have $\alpha(a) = \alpha(b)$. We can apply λ to both sides and get $\lambda(\alpha(a)) = \lambda(\alpha(b))$ which is the same thing as saying $\beta(a) = \beta(b)$ which implies that $a = b$. Thus since β is injective so is α.

Suppose that $u, v \in X^+$ such that $u = v$, then $u_1 \dots u_n = v_1 \dots v_n$ where $u_i = v_i$. Now we have that,

$$u = \beta(u_1) \dots \beta(u_n) = \lambda(\alpha(u_1)) \dots \lambda(\alpha(u_n)) = \lambda(x_1) \dots \lambda(x_n) = \lambda(x_1 \dots x_n) = \lambda(x).$$

Similarly we get that $v = \lambda(y)$ where $x_i = y_i$ for all i since α is an injection. Therefore we conclude that $x = y$.

Now let $x \in X^*$, then

$$x = \beta(x_1) \dots \beta(x_n) = \lambda(\alpha(x_1)) \dots \lambda(\alpha(x_n)) = \lambda(y_1) \dots \lambda(y_n) = \lambda(y_1 \dots y_n) = \lambda(y).$$

Therefore, λ is surjective. $\square$

Note that this theorem shows that the definition of free semigroup we had before is equivalent to having a set F_X that satisfies conditions (i) and (ii). The diagram, condition (ii), is known as the Universal Property in category theory and is used to generalize the idea of free semigroups to free objects. We will not go into free objects but we will use the definition to show interesting properties that free semigroups have. Finally the homomorphism λ is usually called a substitution by elements of S.

Theorem 28 *Two free semigroups on the same set X are isomorphic.*

Proof. Let F_X and G_X be free semigroups on X then there exist homomorphisms λ and μ such that

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & F_X \\ \downarrow{\scriptstyle \varphi} & \swarrow{\scriptstyle \lambda} & \\ S & & \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{\beta} & G_X \\ \downarrow{\scriptstyle \rho} & \swarrow{\scriptstyle \mu} & \\ T & & \end{array}$$

commute for any semigroups S and T and functions φ, and ρ. Since the diagram commutes for any semigroups we can replace G_X for S and F_X for T. This will give us the following

$$\begin{array}{ccc} X & \xrightarrow{\alpha} & F_X \\ \downarrow{\scriptstyle \beta} & \swarrow{\scriptstyle f} & \\ G_X & & \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{\beta} & G_X \\ \downarrow{\scriptstyle \alpha} & \swarrow{\scriptstyle g} & \\ F_X & & \end{array}$$

We know both of these diagrams commute so we know that

$$\beta = f\alpha \text{ and } \alpha = g\beta,$$

giving us

$$\beta = f(g\beta) \text{ and } \alpha = g(f\alpha).$$

Now since f and g are unique and α and β are standard embeddings we get that f and g are inverse functions. Hence, f and g are isomorphisms and we have $F_X \cong G_X$. $\square$

The proof of this theorem is an adaptation of themes shown in Howie, see [3]. Moreover, this theorem tells us that if we ever have a free semigroup on a set X, call it F_X, then we can just work with X^*. Thus, we can apply all the theory we have shown with X^* instead of working with an abstract free semigroup F_X.

2.2.2 Characterizations and Theorems

Now we will use the definition from the previous section to create some characterizations of free semigroups and show some properties. We have already seen some characterizations of free submonoids when the superset is free in the first chapter. We will use these and intuition to see what equivalent conditions to being free.

Lets start by proving recalling and proving **Theorem 2** using the categorical definition of free semigroups as it is done in Lothaire, see [4].

Theorem 2 *Let Y be a submonoid of X^* and let Z be its minimal generating set. Y is free if and only if whenever*

$$x_1x_2\dots x_n = y_1y_2\dots y_m \text{ where } x_i, y_j \in Z$$

then $n = m$ and $x_i = y_i$

Proof. Suppose that Y is free with minimal generating set Z and we have

$$x_1x_2\dots x_n = y_1y_2\dots y_m \text{ where } x_i, y_j \in Z.$$

Without loss of generality we can say that $x_1 \leq y_1$. Therefore we have $y_1 = x_1u$ where $u \in Y$ but recall that $x_1, y_1 \in Z$ which are all the words in Y that cannot be written as the product of two different words, thus we get $u = 1$. Now we have $x_2\dots x_n = y_2\dots y_m$ but using the same argument as before we can see that $n = m$ and $x_i = y_i$ for all i.

Conversely suppose that every word in Y can be written uniquely as a product of elements of its minimal generating set Z. We will show that $Y = Z^*$. Let S be a semigroup

and let φ be a function from Z to S. Similarly to before, we will define

$$\alpha : Z \to Y, \alpha(z) = z \text{ (the standard embedding)}$$

$$\lambda : Y \to S, \lambda(y) = \varphi(y_1) \dots \varphi(y_n) \text{ where } y_i \in Z \text{ for all } i.$$

From the proof of **Theorem 27** we can see that λ is an homomorphism and the uniqueness comes from the ability to write any word in Y as a unique product of elements of Z. Thus, $Y = Z^*$ showing that Y is free. □

This proof is an excellent example to show why it is beneficial to have two different ways of defining a concept. Proving this theorem can be tedious and unintuitive with the definition in Chapter 1.

Now let us shift our focus to some definitions which are going to assist us in the characterization of free semigroups. Moreover, we will show some properties that free semigroups have. Both the characterization and properties can be found in Howie, see [3].

Definition 44 *Let M be a monoid. We will define the* ***units of M*** *as the set containing the invertible elements in M. We will denote it by* $\boldsymbol{\mathcal{U}(M)}$.

Note that we can write

$$\mathcal{U}(M) = \{x \in M \mid \text{there exists } x^{-1} \in M \text{ where } xx^{-1} = x^{-1}x = 1\}.$$

For an example, consider the monoid $\mathbb{Z}$ with the usual multiplication then $\mathcal{U}(\mathbb{Z}) = \{1, -1\}$. Note that for any monoid M we have $\mathcal{U}(M) \neq \emptyset$ since $1 \in \mathcal{U}(M)$.

Definition 45 *A monoid M is called* ***cancellative*** *if*

$$xy = xz \text{ implies } y = z \text{ and } yx = zx \text{ implies } y = z$$

for all $x, y, z \in M$.

Definition 46 *A monoid M is called* ***equidivisible*** *if $xy = zw$ implies*

$$x = za \text{ and } w = ay \text{ for some } a \in M \text{ or } z = xb \text{ and } y = bw \text{ for some } b \in M$$

Definition 47 *We say a monoid M has **proper length** if there exists a homomorphism $f : M \to \mathbb{N}$ and $f(x) = 0$ if and only if $x = 1$.*

Remark 9 *X^* has proper length since $n_X(xy) = n_X(x) + n_X(y)$ for all $x, y \in X^*$ and $f(x) = 0$ if and only if $x = 1$ by definition of the empty word.*

Moreover, note that n_X has the following property: if $x \neq 1$, $y \neq 1$, and $n_X(x)+n_X(y) = n_X(z)$ then $n_X(x) < n_X(z)$ and $n_X(y) < n_X(z)$.

We will not be able to exchange semigroup and monoid for the theorems involving proper length since X^+ does not have proper length.

Now that we have some definitions out of the way we can move on to the theorems. The first theorem is similar to **Theorem 2** but now we are not requiring the monoid of a subset of a free monoid, thus, we could see **Theorem 2** as a corollary of this theorem.

Theorem 29 *A monoid X is free if and only if for all $w \in X$ there exists a unique factorization of elements in $Z = (X - 1) \setminus (X - 1)^2$.*

The proof of this theorem is almost exactly the same as converse of the proof for **Theorem 2** therefore it will be omitted. For an alternative proof of this theorem see Clifford, see [2].

Theorem 30 *If a monoid X is equidivisible and has proper length then X is free.*

Proof. Let X be an equidivisible monoid with proper length. Let $Z = (X - \{1\}) - (X - \{1\})^2$. We will show that that every element of X can uniquely be factorized by elements of Z.

Let $a, b \in X - \{1\}$ such that $ab = 1$, thus giving us $n_X(ab) = 0$. Since the X has proper length we get that $n_X(a) + n_X(b) = 0$ giving us that $a = b = 1$. Consider $x \in (X - \{1\})^2$, then there exists two words $u, v \in X - \{1\}$ such that $x = uv$. From proper length we get that $n_X(u)+n_X(v) = n_X(x)$ and since n_X has a lower bound we can say write $x = x_1 \dots x_n$ where $x_i \in Z$ for all i.

Now suppose that

$$x_1x_2\dots x_n = y_1y_2\dots y_m \text{ where } x_i, y_j \in Z.$$

Then once more since we have that $x_i, y_i \in Z$ and Z is the set of words that cannot be written as a product of two words we get that $n = m$ and $x_i = y_i$ for all i, thus X free. □

Theorem 31 *X is free if and only if the following properties are satisfied:*

i $\mathcal{U}(X) = \{1\}$

ii *X is cancellative and equidivisible*

iii *every $w \in X$ has finitely many non-trivial left factors*

Proof. Suppose that X is free. Note that by **Theorem 28** we can think of X as the usual words with concatenation that we are familiar with. By the definition of concatenation it is easy to see $\mathcal{U}(X) = \{1\}$ and that every $w \in X$ has finitely many non-trivial left factors.

Suppose that $zx = zy$ and $x \neq y$ where $x, y, z \in X$. Since X has proper length we can see that $n_X(z) + n_X(x) = n_X(z) + n_X(y)$ which implies that $n_X(x) = n_X(y)$. Since $x \neq y$ we know that there exists a letter in x and y in the same position that do not coincide giving us that this same letter does not coincide in zx and zy, therefore $zx \neq zy$. This is a contradiction giving us that X is right cancellative. It can be shown that X is left cancellative in a similar way.

Suppose that we have $xy = zw$ for $w, x, y, z \in X$. Then we have that $xy = zw = a_1\dots a_n$. We know that there exists $l, k \in \mathbb{N}$ such that

$$x = a_1\dots a_k, y = a_{k+1}\dots a_n \text{ and } z = a_1\dots a_l, w = a_{l+1}\dots a_n.$$

If $k = l$ we can use 1 to show the property of equidivisibility is satisfied. Without loss of generality we can assume that $k < l$. Now we have

$$xy = a_1\dots a_n = (a_1\dots a_k)(a_{k+1}\dots a_l)(a_{l+1}\dots a_n) = xbw,$$

thus X is equidivisible.

Conversely, suppose that X has properties $(i), (ii)$, and (iii). Let $x, y \in X$ such that $xy = 1$. We will show that $x = y = 1$. Let $e = yx$ and consider $(yx)^2 = y(xy)x = yx = e$. This gives us that $e^2 = e$ and by cancellation we get that $eyx = 1$. We have shown that x and y are inverses but $\mathcal{U}(X) = \{1\}$ so $x = y = 1$.

Now suppose that $X - \{1\} = (X - \{1\})^2$. Supposing this allows us to take any $x \in X - \{1\}$ and give it a left factorization as long as we please. Since we showed that no elements of X have left or right inverses all these factorizations are distinct contradicting (iii). We can conclude that $(X - \{1\}) - (X - \{1\})^2 \neq \emptyset$.

With similar reasoning we can show that the sets of the form $(X - \{1\})^i$ are nested for $i \in \mathbb{N}$. Therefore every element $x \in X$ can be written $x = x_1 \dots x_n$ for a unique n, i.e. X has proper length. Since X is equidivisible and has proper length by **Theorem 30** we get that X is free. □

Note that these types of theorems help in two different ways. They give us a criteria to check besides a definition and if we satisfy a definition then we have properties that we can use.

The last theorem in this section is from Clifford, see [2]. In this theorem we are going to show that if two free semigroups are isomorphic then the alphabets are mapped to each other via the isomorphism.

Theorem 32 *Let F_X be a free semigroup on X and let G_Y be a free semigroup on Y. If there exists an isomorphism $\varphi : F_X \to G_Y$ then $\varphi(X) = Y$.*

Proof. We know that X and Y are the minimal generating sets for F_X and G_Y respectively. Note that

$$\varphi(F_X^2) = \varphi(F_X)\varphi(F_X) \subset G_Y^2$$

and

$$\varphi(X) = \varphi(F_X - F_X^2) = \varphi(F_X) - \varphi(F_X^2) \supset G_Y - G_Y^2 = Y.$$

Similarly, we get that $Y \subset \varphi(X)$. □

2.2.3 Ranks and Codes

Recall that in section 1.1.3 we studied that there is a unique set that generates a free semigroup. In this section we will explore this concept through a more algebraic perspective. The following definition comes from Mikhalev, see [5].

Definition 48 *Let Y be a submonoid of X^* on a finite alphabet X with generating set $Z = (Y-1) \setminus (Y-1)^2$ then the **rank of X^*** is the cardinality of Z.*

Note that the rank of any submonoid is well defined since X is finite and the generating set of a submonoid is unique.

Remark 10 *A free submonoid, Y^*, of a free monoid, X^*, not necessarily have to have a smaller rank than X^*.*

For this consider an the alphabet $X = \{a, b\}$. Then we know that X^* has rank 2. Now consider the free submonoid Y^* generated by $Y = \{aa, ba, baa, bb, bba\}$. Y^* has rank 5.

The fact that the generating set is unique is not usually true. Consider $\mathbb{Z}$ with the usual addition then $\mathbb{Z}$ can be generated by $\langle -1 \rangle$ and $\langle 1 \rangle$ so $\mathbb{Z}$ does not have a unique generating set. Consider a group with three elements $\{a, b, e\}$ with identity e. This group can be generated by $\langle a, b \rangle$ and $\langle a, ab \rangle$.

Remark 11 *From **Theorem 32** we can see that two free semigroups with finite alphabets are isomorphic if they have the same rank.*

2.3 Finite Presentation

In this section we will be continue working with the ideas of congruences and generating set to be able to create an equivilent way of describing a monoid. Moreover, we will be defining a important semigroup that we will be working with later.

2.3.1 Semigroups and Isomorphisms

We are going to start off this section by seeing an interesting consequence of the categorical definition of free semigroups presented in Clifford, see [2].

Theorem 33 *Let X^+ be the free semigroup on the alphabet X and let S be a semigroup with a set of generators M such that $|M| \leq |X|$. Then S is isomorphic to a quotient semigroup of X^+*

Proof. Note that since $|M| \leq |X|$ we can see that there exists a surjective function $\varphi : X \to M$. We can now extend φ to be a function λ from X^+ to S. Note that since λ maps X^+ onto the generators of S then λ also maps X^+ onto S. Now by the Fundamental Theorem of Homomorphisms we have that $S \cong X^+/ker(\lambda)$. □

Note α, φ, λ, and S from the theorem above will be used for the rest of the section.

From the this theorem we can see that any semigroup S is isomorphic to a quotient semigroup, X^+/ρ, of some free semigroup X^+. Since we know what the generators of a free semigroup are we will try to do the same for an arbitrary semigroup with the following definition, see Howie, see [3].

Definition 49 *If there exists a finite relation σ on X^+ such that X is finite and $\rho = \sigma^\sharp$, then we say that $S \cong X^+/\rho$ has a **finite presentation**.*

Moreover, if $\sigma = \{(x_1, y_1), \ldots, (x_m, y_m)\}$ and $X = \{u_1, \ldots, u_n\}$ then we will express

$$S = \langle u_1, \ldots, u_n \mid x_1 = y_1, \ldots, x_m = y_m \rangle.$$

*We will call the elements of X **the generators of S** and the elements of σ are the **defining relations**.*

Note that the first theorem of this section allows us to represent any semigroup as a free semigroup modulo an equivalence relation. In the definition above we are doing something similar where we are considering a free semigroup modulo an unique congruence. Thus, we have found a way of describing a semigroup based on the letters of an alphabet and some congruences on words made from these letters.

2.3.2 Bicyclic Semigroup

In this section we will be looking at a semigroup known as the bicyclic semigroup. We will show some properties of this semigroup that are covered in Clifford, see [1]. Then we will give a generalization of this semigroup which we will use in the following section.

Definition 50 *The **bicyclic semigroup** has the following finite presentation*

$$B_0 = \langle a, b \mid ba = 1 \rangle = X^*/\rho$$

where $X = \{a, b\}$ *and* $\rho = \{(ba, 1)\}^\sharp$

Note that B_0 is actually a monoid but similar to the other sections we will use monoid and semigroup as almost synonyms.

For an example of the operation we have

$$aababba = a^2(ba)b(ba) = a^2 1b1 = a^2 b.$$

It is easy to see that every element of B_0 is of the form $a^n b^m$ where $n, m \in \mathbb{N} \cup \{0\}$. The formulation of the product in B_0 is as follows

$$a^k b^m \cdot a^r b^s = \begin{cases} a^k b^{m-r+s} & \text{if} \quad m \geq r \\ a^{k-m+r} b^s & \text{if} \quad m < r. \end{cases}$$

We can also see that a and b are not really adding anything to the computation therefore we can disregard them and see that $B_0 \cong \mathbb{N} \cup \{0\} \times \mathbb{N} \cup \{0\}$ where the product is just the result of applying the corresponding operations to the exponents.

Definition 51 *Let M be a monoid and $x \in M$. The cardinality of the set $\{x^n \mid n \in \mathbb{N} \cup \{0\}\}$ is called the **order of the x**.*

Remark 12 *One of the most important properties of B_0 is that both a and b have infinite order.*

The following theorems are some of the theorems that make the bicyclic semigroup so important to study.

Theorem 34 *Let S be a semigroup with e, a, b with the following properties*

$$ae = ea = a, \quad be = eb = b, \quad ba = e, \quad \textit{and} \quad ab \neq e$$

then the semigroup made from these three elements is isomorphic to B_0.

Proof. Since $ae = ea = a, \quad be = eb = b$, and $ba = e$ we can see that $e \in \langle a, b \rangle$ and e is the identity of this monoid. Note that since $ba = e$ we can write every element of $\langle a, b \rangle$ in the form $a^n b^m$. Now we just need to show the uniqueness of n and m and we are done. To show this we are going to need to show the following properties first.

i Suppose that b has a finite order, then there exists $k, l \in \mathbb{N}$ such that $b^{k+l} = b^k$. We get $b^l = e$ by multiplying from the left to both sides by a^k. Now we can see that

$$a = ea = b^l a = b^{l-1}$$

from which we get that $ab = b^{l-1}b = b^l = e$ which is a contradiction, thus b has infinite order. Similarly, we can show that a has an infinite order.

ii Suppose that $a^k = b^l$ for some $k, l \in \mathbb{N}$, then by multiplying to the right by b^k we get that $b^k a^k = b^{k+l} = e$. Now from (i) we get that $k + l = 0$ thus $k = l = 0$.

iii We will show that if $a^k b^l = e$, $k, l \in \mathbb{N}$ then $k = l = 0$. It is easy to see that it true if $k = l = 0$ so suppose towards contradiction that $k \neq 0$. Then we would have

$$b = be = ba^k b^l = a^{k-1} b^l$$

and thus $ab = a^k b^l = e$ which is a contradiction.

Now we are ready to prove that expressing the elements of $\langle a, b \rangle$ in the form $a^n b^m$ is unique. Suppose that $a^n b^m = a^i b^j$ where either $n \neq i$ or $m \neq j$. Without loss of generality

we can assume that $m < j$. Multiplying to the right by a^m we have $a^n = a^i b^{j-m}$. If $i \leq n$ then multiplying by b^i to the left would give us $a^{n-i} = b^{j-m}$ where $j - m > 0$ giving us $j > m$ which is a contradiction to (ii). Also, if $n < i$ we can multiply by b^n from the left to get $e = a^{i-n}b^{j-m}$ where $j - m > 0$ which contradicts (iii). □

Theorem 35 *Let S be a semigroup and $\varphi : B_0 \to S$ be a homomorphism then $\varphi(B_0)$ is cyclic or φ is an monomorphism.*

Proof. Let $\varphi(1) = e, \varphi(a) = x$, and $\varphi(b) = y$. We can see that all the conditions of **Theorem 34** are meet by e, x, and y except $yx \neq e$.

Suppose $xy = e$. Note that x and y are now inverses of each other, thus for $x^i y^j$ we can write this as x^{i-j}. If $i \geq j$ then this is a power of x, otherwise it is a power of y but recall that $y = x^{-1}$ so $\varphi(B_0)$ is cyclic group generated by x.

Suppose $xy \neq e$, then $\varphi(x^n y^m) = \varphi(x^i y^j)$ gives us $a^n b^m = a^i b^j$ then by **Theorem 34** we have that $n = i$ and $m = j$ making φ an injective homomorphism. □

Chapter 3

Identities for a Class of Monoids

3.1 Preliminaries

The results in this chapter were published in Notes on Number Theory and Discrete Mathematics, see [6]. In this chapter we will be working with the length of a word in a slightly different way than what we have been used to. Recall that if we have $v \in X^*$ then $n_X(v)$ is the length of this word. The following definition will try to only count the occurrences of one specific letter in X.

Definition 52 *Let X be an alphabet and let $x \in X$, then the function $\boldsymbol{n_x} : X^* \to \mathbb{N} \cup \{0\}$ gives the number of times the letter x occurs in v.*

For an example consider $X = \{a, b, c\}$, then $n_a(abacba) = 3$. Note that $n_a(abacba) = n_a(a^3)$ yet $n_X(abacba) \neq n_X(a^3)$.

Remark 13 *Note that the length of a word, $v \in X^*$ can be recovered in the following way,*

$$n_X(v) = \sum_{x \in X} n_x(v).$$

Definition 53 *We say $v, w \in X^+$ are **balanced** if $n_x(v) = n_x(w)$ for all $x \in X$.*

Note that if $v, w \in X^*$ are balanced then v is just a permutation of the letter of w, or vice versa. Therefore, it is easy to see that if $v, w \in X^*$ are balanced then $\lambda(v) = \lambda(w)$.

Now recall that X^+ is a free semigroup on an alphabet X, therefore it satisfies the universal property **Theorem 27** (ii). In **Theorem 27** (ii) recall that the homomorphism λ is known as a substitution be elements of S. With this in mind we can see that the following definition is well defined.

Definition 54 *We will call the pair $(v, w) \in S \times S$ an **identity satisfied in the semigroup S**, denoted $x \approx y$, if $\lambda(v) = \lambda(w)$ for all substitution by elements of S.*

Now that we have defined identities satisfied in a semigroup S we will define some more concepts that are closely related to identities.

Definition 55 *If v and w are balanced and $v \approx w$ is an identity satisfied on S, then we say that the **identity $v \approx w$ is balanced in S**. Moreover, since $n_X(v) = n_X(w)$ we will call $n_X(v)$ the **length of the identity**.*

Definition 56 *If $v \approx w$ is an identity in S and $a, b \in S$, then the identity **$avb \approx awb$** satisfied in S and is called a **simple consequence of $v \approx w$**.*

For this definition we can see that since λ is a homomorphism and an identity $v \approx w$ is satisfied in S we have $\lambda(v) = \lambda(w)$. Then if we take $a, b \in X^*$ then

$$\lambda(avb) = \lambda(a)\lambda(v)\lambda(b) = \lambda(a)\lambda(w)\lambda(b) = \lambda(awb).$$

Thus, $avb \approx awb$ is an identity satisfied in S.

Remark 14 *The relation $\approx$ is an equivalence relation on the set S. We will call the equivalence classes formed by this partition the identities partition for S, denoted $\mathcal{P}_S$.*

3.2 Identities on B_n

Recall that in section 2.3.2 we defined the bicyclic semigroup. In the next definition we will define a more general family of semigroups.

Definition 57 *Let n be a non-negative integer, then we can present the monoid B_n in the following way,*

$$\boldsymbol{B_n} = \langle a, b \mid ba = b^n \rangle.$$

In section 2.3.2 we gave a formulation of the multiplication for B_0 so we will do the same here for $n > 0$. If $n > 0$ then the formulation of the product in B_n is as follows

$$a^k b^m \cdot a^r b^s = \begin{cases} a^{k+r} b^s & \text{if} \quad m = 0; \\ a^k b^{m+(n-1)r+s} & \text{if} \quad m > 0. \end{cases}$$

In this section we will see some of the properties that identities in B_n must have and prove an identity exists in B_n for all n.

First note that B_n is right cancellative for all n. This implies that the identities for B_n are also right cancellative. Moreover, since B_n contains a copy of the infinite cyclic group, $\langle a \rangle$ or $\langle b \rangle$ as shown in **Theorem 34**, we have that any identity $v \approx w$ is balanced. Recall that every element of B_n is of the form $a^k b^j$. Therefore for every identity satisfied in B_n we must have that the first letter must coincide, we will suppose they start with the letter x. Lastly, we will say that if the letters in an identity are swapped this is not a new identity.

Now that we have laid out the foundation for some properties and what we are looking for the following theorem will show us that there is an identity in B_0.

Theorem 36 *Let $x, y \in B_0$ then*

$$(I) \qquad xyyxxyxyyx \approx xyyxyxxyyx, \qquad (xy^2x^2yxy^2x \approx xy^2xyx^2y^2x)$$

is an identity satisfied in B_0. This identity is known as Adjan identity. Moreover, Adjan identity and this following identity are the only identities in $\{x, y\}$ of length 10,

$$(II) \qquad xyyxxyyxxy \approx xyyxyxyxxy \qquad (xy^2x^2y^2x^2y \approx xy^2xyxyx^2y).$$

Note that this identity is only for B_0 so now we will show that there is an identity for B_n.

Theorem 37 *Let $j \leq i$ for $i, j \in \mathbb{N}$ and $n > 0$ we have that*

$$(A_{i,j}) \quad xy^{i+1}x \approx xy^j xy^{i-j+1} \qquad ((A'_{i,j}) \quad yx^{i+1}y \approx yx^j yx^{i-j+1})$$

is an identity satisfied in B_n.

Proof. Since $x, y \in B_n$ let $x = a^r b^s$ and $y = a^k b^m$. Recall that identities are right cancellative so to prove $(A_{i,j})$ we actually only have to show that $y^{i+1}x \cong y^j x j^{i-j+1}$. Let us start by considering $i = j = 1$. This gives us

$$(a) \qquad y^2 x = \begin{cases} a^{2k+r}b^s & \text{if} \quad m = 0 \\ a^k b^{2m+(n-1)k+(n-1)r+s} & \text{if} \quad m > 0, \end{cases}$$

and

$$(b) \qquad yxy = \begin{cases} a^{2k+r} & \text{if} \quad m = 0 \text{ and } s = 0 \\ a^{k+r}b^{s+(n-1)k} & \text{if} \quad m = 0 \text{ and } s > 0 \\ a^k b^{2m+(n-1)k+(n-1)r+s} & \text{if} \quad m > 0. \end{cases}$$

Note that $y^2x = yxy$ for every case except the case $m = 0$ and $s > 0$. Thus, we will only consider this case. We have

$$xy^{i+1}x = xy^{i-1}(y^2x) = a^r b^s a^{(i-1)k} a^{2k+r} b^s = a^r b^s a^{(i+1)k+r} b^s = a^r b^{2s+(n-1)[(i+1)k+r]},$$

and

$$\begin{aligned} xy^i xy = xy^{i-1}(yxy) = a^r b^s a^{(i-1)k} a^{k+r} b^{s+(n-1)k} = a^r b^s a^{ik+r} b^{s+(n-1)k} \\ = a^r b^{2s+(n-1)[(i+1)k+r]}. \end{aligned}$$

Thus, $(A_{i,j})$ is true when $i = j$ for B_n.

Now we can see that for any $i > j$ we have that

$$xy^{i+1}x \approx xy^i xy \approx xy^{i-1}xy^2 \approx xy^{i-2}xy^3 \approx \cdots \approx xy^j xy^{i-j+1}.$$

□

It can be shown that identities of length 2 or 3 do not exist in B_0 leaving us with $(A_{1,1})$ begin the smallest identity in B_0. The follow remark states that this statement can generalized for an n.

Remark 15 $(A_{1,1})$ *is the shortest nontrivial identity satisfied in* B_n *for all* $n > 0$.

With this theorem we can show that Adjan identity and the identity (II) are satisfied in B_n.

Remark 16 *Adjan identity and (II) are both simple consequences of $(A'_{1,1})$, therefore they are both satisfied in B_n.*

$$(A'_{1,1}) \;\Rightarrow\; \underline{xy}\,\overbrace{yx^2y}\,\underline{\underline{xy^2x}} \approx \underline{xy}\,\overbrace{yxyx}\,\underline{\underline{xy^2x}} \quad \textit{that is (I)};$$

$$(A'_{1,1}) \;\Rightarrow\; \underline{xy}\,\overbrace{yx^2y}\,\underline{\underline{yx^2y}} \approx \underline{xy}\,\overbrace{yxyx}\,\underline{\underline{yx^2y}} \quad \textit{that is (II)}.$$

3.3 Canonical Form and Identities Partition $\mathcal{P}_{B_n}$

For this section we will consider words and identities that start with the letter $x \in B_n$ and that have $n_y(v) > 0$, i.e. we are looking at words of the form $v = x^k u$ where $k > 0$ and the first letter of $u \in B_n$ is y.

Definition 58 *Let v be a word, then* ***the canonical form of v*** *is*

$$(*) \qquad x^{\ell_1}(yx)^{\ell_2}z^{\ell_3} \qquad (\textit{where } z \in \{x,y\},\ \ell_1 > 0 \textit{ and } \ell_2, \ell_3 \geq 0)$$

Remark 17 *If we have a word v with canonical form $x^{\ell_1}(yx)^{\ell_2}z^{\ell_3}$, then*

$$v \approx x^{\ell_1}(yx)^{\ell_2}z^{\ell_3}$$

is an identity satisfied in B_n for all n.

The following lemma will give a nice way of getting the canonical form of any word $v = x^k u$ using $n_x(u)$ and $n_y(u)$.

Lemma 5 *Let v be a word then the canonical form of v is given by,*

$$v \approx \begin{cases} x^k(yx)^{n_x(u)}y^{n_y(u)-n_x(u)} & \textit{if} \quad n_y(u) \geq n_x(u) \\ x^k(yx)^{n_y(u)}x^{n_x(u)-n_y(u)} & \textit{if} \quad n_y(u) < n_x(u). \end{cases}$$

Proof. Note that the first letter of u is y so by using $(A_{i,1})$ and $(A'_{i,1})$ we get

$$v \approx x^k yxyx \cdots yxz^m \qquad (m \geq 0),$$

where $z = x$ or $z = y$.

If $n_y(u) \geq n_x(u)$ we get that $z = y$ meaning that all the $x's$ in u are in the yx terms of the identity give us $n_x(u)$ many yx terms. Moreover, since every identity is balanced in B_n we can see that that $m = n_y(u) - n_x(u)$. If $n_x(u) = n_y(u)$, then the number of yx terms is still $n_x(u)$. Similarly, to before due to the balance identities in B_n we get $z = y$ and $m = n_y(u) - n_x(u)$.

If $n_y(u) < n_x(u)$ then we have $z = x$ and the number of yx terms is $n_y(u)$ leaving us with $m = n_x(u) - n_y(u)$. □

Finally, we have the two big results.

Theorem 38 *Let v and w be words of the form $v = x^k u$ and $w = x^{k'} u'$, then the following are equivalent:*

i $v \approx w$ *is satisfied in B_n for all n*

ii v *and* w *have the same canonical form*

iii $n_x(u) = n_x(u'), n_y(u) = n_y(u')$, *and* $k = k'$

iv (v, w) *is balanced and* $k = k'$

Proof. We will first show that (ii) if and only if (i), so suppose that v and w have the same canonical form then by **Remark 14** and **Remark 17** we get that $v \approx w$.

Conversely, suppose that $v \cong w$ is satisfied in B_n for all n and $v \approx x^{\ell_1}(yx)^{\ell_2} z^{\ell_3}$ and $w \approx x^{\ell'_1}(yx)^{\ell'_2} z'^{\ell'_3}$. To show these two canonical forms are the same we need to show that $\ell_1 = \ell'_1$, $\ell_2 = \ell'_2$, $\ell_3 = \ell'_3$, and $z = z'$ if $\ell_3 = \ell'_3 \neq 0$.

Let $\sigma_{1,1}$ be a substitution by elements of B_n for $n \in \mathbb{N}$ such that $\sigma_{1,1}(x) = a$ and $\sigma_{1,1}(y) = b$. From here we get,

$$\sigma_{1,1}(x^{\ell_1}(yx)^{\ell_2} z^{\ell_3}) = a^{\ell_1} b^{n\ell_2} b^{\ell_3} = a^{\ell_1} b^{n\ell_2 + \ell_3} \qquad \text{if } z = y$$

and

$$\sigma_{1,1}(x^{\ell_1}(yx)^{\ell_2}z^{\ell_3}) = a^{\ell_1}b^{n\ell_2}a^{\ell_3} = a^{\ell_1}b^{n\ell_2+(n-1)\ell_3} \qquad \text{if } z = x.$$

Similarly,

$$\sigma_{1,1}(x^{\ell'_1}(yx)^{\ell'_2}z'^{\ell'_3}) = a^{\ell'_1}b^{n\ell'_2+\ell'_3} \quad \text{if } z' = y$$

and

$$\sigma_{1,1}(x^{\ell'_1}(yx)^{\ell'_2}z'^{\ell'_3}) = a^{\ell'_1}b^{n\ell'_2+(n-1)\ell'_3} \quad \text{if } z' = x.$$

From the equalities above we can see that $\ell_1 = \ell'_1$. Moreover, since identities satisfied in B_n are balanced we get that $2\ell_2 + \ell_3 = 2\ell'_2 + \ell'_3$.

We are now left with three cases:

1. $(z = z' = y)$: $n\ell_2 + \ell_3 = n\ell'_2 + \ell'_3$, that is $(n-2)(\ell'_2 - \ell_2) = 0$.

2. $(z = z' = x)$: $n\ell_2 + (n-1)\ell_3 = n\ell'_2 + (n-1)\ell'_3$, that is $(n-2)(\ell'_2 - \ell_2) = 0$.

3. $(z \neq z')$: without loss of generality, we can assume $z = y$ and $z' = x$ then $n\ell_2 + \ell_3 = n\ell'_2 + (n-1)\ell'_3$ which implies $2n(\ell'_2 - \ell_2) = 2\ell_3 - 2(n-1)\ell'_3$ and so, $(n-2)(\ell_3 + \ell'_3) = 0$

From the cases above we can see that the canonical forms on v and w match for all n except $n = 2$.

For the case of $n = 2$ we are going to be considering a substitution by elements of B_2, $\sigma_{1,2}$ where $\sigma_{1,2}(x) = a$ and $\sigma_{1,2}(y) = b^2$. From here we get,

$$\sigma_{1,2}(x^{\ell_1}(yx)^{\ell_2}z^{\ell_3}) = a^{\ell_1}b^{3\ell_2}a^{\ell_3} = a^{\ell_1}b^{3\ell_2+\ell_3} \quad \text{if } z = x$$

and

$$\sigma_{1,2}(x^{\ell_1}(yx)^{\ell_2}z^{\ell_3}) = a^{\ell_1}b^{3\ell_2}b^{2\ell_3} = a^{\ell_1}b^{3\ell_2+2\ell_3} \quad \text{if } z = y.$$

Similarly,

$$\sigma_{1,2}(x^{\ell'_1}(yx)^{\ell'_2}z'^{\ell'_3}) = a^{\ell'_1}b^{3\ell'_2+\ell'_3} \quad \text{if } z' = x$$

and

$$\sigma_{1,2}(x^{\ell'_1}(yx)^{\ell'_2}z'^{\ell'_3}) = a^{\ell'_1}b^{3\ell'_2+2\ell'_3} \quad \text{if } z' = y.$$

Similarly to $\sigma_{1,1}$ we can see that $\ell_1 = \ell'_1$ regardless of z. Recall that from $\sigma_{1,1}(u) = \sigma_{1,1}(v)$ we also got that $2\ell_2 + \ell_3 = 2\ell'_2 + \ell'_3$.

We now are left with the following three cases:

1. $(z = z' = y)$: $3\ell_2 + \ell_3 = 3\ell'_2 + \ell'_3$ which with $2\ell_2 + \ell_3 = 2\ell'_2 + \ell'_3$ we get $\ell_2 = \ell'_2$ and $\ell_3 = \ell'_3$.

2. $(z = z' = x)$: $3\ell_2 + 2\ell_3 = 3\ell'_2 + 2\ell'_3$ which with $2\ell_2 + \ell_3 = 2\ell'_2 + \ell'_3$ we get $\ell_2 = \ell'_2$ and $\ell_3 = \ell'_3$.

3. $(z \neq z')$: without loss of generality, we can assume $z = y$ and $z' = x$ then $3\ell_2 + \ell_3 = 3\ell'_2 + 2\ell'_3$ which implies $\ell_2 = \ell'_2 + \ell'_3$ and so $2\ell'_2 + \ell'_3 = 2(\ell'_2 + \ell'_3) + \ell_3$, that is $\ell'_3 + \ell_3 = 0$ and therefore $\ell'_3 = \ell_3 = 0$

We have shown that if $v \approx w$ is an identity satisfied in B_n then v and w have the same canonical form and thus showing (ii) if and only if (i).

We can see that (ii) if and only if (iii) follows from **Lemma 5**, since if v and w have the same canonical form then they can can be represented in the same way by $n_x(u) = n_x(u'), n_y(u), n_y(u')$ and $k = k' = n_x(u) - n_y(u)$ or $k = k' = n_y(u) - n_x(u)$ dependent on z.

(iii) and (iv) is true since balanced and $n_x(u) = n_x(u')$ and $n_y(u), n_y(u')$ are equivalent statements. □

Remark 18 *If we have two words v and w such that k is the largest positive integer such that $x^k \leq v$ and $x^k \leq w$, $n_y(v) = n_y(w) = l > 1$, and $n_x(v) - k = n_y(u) = m > 0$, then $v \approx w$ is a nontrivial identity for B_n for all n. Thus, the triples of three positive integers (k, l, m) give us a set of nontrivial identities.*

For example, the triple of positive integers $(3, 2, 3)$ determine the set of words

$$P_{3,2,3} = \{x^3y^2x^3,\ x^3yx^3y,\ x^3yxyx^2,\ x^3yx^2yx\}$$

and the set of nontrivial identities

$$I_{3,2,3} = \{x^3y^2x^3 \approx x^3yx^3y,\quad x^3y^2x^3 \approx x^3yxyx^2,\quad x^3y^2x^3 \approx x^3yx^2yx,$$

$$x^3yx^3y \approx x^3yxyx^2, \quad x^3yx^3y \approx x^3yx^2yx, \quad x^3yxyx^2 \approx x^3yx^2yx\}.$$

Note that every distinct triple produces a different set of nontrivial identities. The following theorem will show that we can represent every nontrivial identity with these triples.

Theorem 39 *Let* $P_{k,l,m} = \{x^k u \mid$ *the first letter of* u *is* y, $n_y(u) = l$ *and* $n_x(u) = m\}$, *then*

i)

$$\mathcal{P}_{B_n} = \{\{P_{k,l,m}\}_{k,l>0,m\geq 0}, \ \{x^k\}_{k>0}\}$$

is the identities partion (the set of equivalence classes) for B_n $(n > 0)$.

ii) The elements of this partition are finite sets and if $k, l > 0, m \geq 0$ *then*

$$|P_{k,l,m}| = \begin{pmatrix} l+m-1 \\ l-1 \end{pmatrix}.$$

iii) The cardinality of the finite set of all identities corresponding to the triples (k, ℓ, m), *where* $k, l > 0$ *amd* $m \geq 0$, *is the following one:*

$$|I_{k,l,m}| = \begin{pmatrix} |P_{k,l,m}| \\ 2 \end{pmatrix}.$$

References

[1] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups* (Vol. I). American Mathematical Society, 1961.

[2] A. H. Clifford and G. B. Preston. *The Algebraic Theory of Semigroups* (Vol. II). American Mathematical Society, 1967.

[3] J. M. Howie. *Fundamentals of Semigruop Theory*. Oxford University Press Inc., 1995.

[4] M. Lothaire. *Combinatorics on Words*. Cambridge University Press, 1997.

[5] A. V. Mikhalev and G. F. Pilz. *The Concise Handbook of Algebra*. Kluwer Academic Publishers, 2002.

[6] E. Salcido and E. D. Schwab. A note on identities in two variables for a class of monoids. *Notes on Number Theory and Discrete Mathematics*, Vol 26, No.1(2020), 86-92.

Curriculum Vitae

Enrique Salcido was born on March 24, 1998, the second son of Clarissa Salcido and Carlos Salcido. He graduated from Transmountain Early College High School, El Paso, Texas, in the spring of 2016. He worked as an Undergraduate Research Assistant for the University of Kansas in the summer of 2017. While working for his bachelor's degree he worked as an Undergraduate Research Assistant at the University of Texas at El Paso under the supervision of Dr. Art Duval. In spring 2018, he graduated with a Bachelor's in Mathematics form the University of Texas at El Paso. In the fall of 2018, he entered the Graduate School of The University of Texas at El Paso. While working towards his Master's degree in Mathematical Sciences he worked as a Teaching Assistant at the Department of Mathematics Sciences at the University of Texas at El Paso. He received his Master's degree in Mathematical Sciences in spring 2020.