BACHELORARBEIT

Varieties of rational languages and finite monoids

ausgeführt am

Institut für
Diskrete Mathematik und Geometrie
TU Wien

unter der Anleitung von

Associate Prof. Dipl.-Ing. Dr.techn. Stefan Hetzl

durch

Johannes Weiser, BSc
Matrikelnummer: 11906087
Danhausergasse 7/10
1040 Wien

Wien, am 27. Juni 2023

Contents

Introduction

Varieties of algebraic structures are interesting for a number of reasons. In universal algebra, a variety is a class of algebraic structures that all have the same signature and fulfill a certain set of identities. Probably the best example of their interesting properties is the variety theorem of Birkhoff that states that the varieties of a given algebraic signature are exactly the classes of structures with this signature that are closed under subalgebras, homomorphic images and arbitrary products. Since these varieties are closed under arbitrary products, they always contain an infinite algebra if they are not trivial. Therefore, there are no varieties of finite algebraic structures according to this definition. In this thesis, I will give an alternative definition of varieties[1] of finite monoids. We will see that there is a similar result to the theorem of Birkhoff, the theorem of Reiterman, and that these varieties of finite monoids are exactly the classes of finite monoids that fulfill given sets of so called *profinite* identities. Furthermore, we will discover the close relationship between finite monoids and rational languages. Therefore, it makes sense to define varieties of rational languages and look at the connection between the varieties of finite monoids and the varieties of rational languages. Indeed, we will see that there is a 1:1 correspondence between the varieties of finite monoids and the varieties of rational languages. This is known as the variety theorem of Eilenberg.

[1] This kind of variety is often refered to as a pseudovariety

1 Necessary lemmas and definitions

The goal of this chapter is to simply recall some basic definitions and lemmas regarding monoids and rational languages that should be known to the reader.

1.1 Metric spaces and topology

The results and definitions from this section are taken from the books [2] and [4]. The reader interested in the proofs, is refered to these books.

Definition 1.1.1. Let X be a set and $d : X \times X \to \mathbb{R}$ a funcion. (X, d) is a *metric space* and d a *metric* if the following criteria are met:

(i) $d(x, y) = 0 \Leftrightarrow x = y$

(ii) $d(x, y) \geq 0$ for all $x, y \in X$

(iii) $d(x, y) = d(y, x)$

(iv) $d(x, z) \leq d(x, y) + d(y, z)$ for all $x, y, z \in X$

A metric d is an *ultrametric* if the following holds:

(v) $d(x, y) \leq \max\{d(x, z), d(z, y)\}$ for all $x, y, z \in X$

Definition 1.1.2. Let (X, d) be a metric space. A set $O \subseteq X$ is open if for every $x \in O$ there is a $\rho > 0$ such that the open ball $U(x, \rho) = \{x \in X \mid d(x, y) < \rho\}$ is a subset of O.

Definition 1.1.3. Let (X, d) be a metric space. A set $A \subseteq X$ is *closed* if its complement is open. The *closure* $\overline{A}$ of A is the smallest closed set that contains A.

Definition 1.1.4. A sequence $(x_n)_{n\in\mathbb{N}}$ in a metric space (M, d) is convergent if there is an $x \in X$ and for every $\rho > 0$ there is an $N \in \mathbb{N}$ such that $d(x_n, x) < \rho$ for all $n \geq N$. In this case, the limit x is unique and we write $x = \lim x_n$.

Lemma 1.1.5. *Let* $(x_n)_{n\in\mathbb{N}}$ *and* $(y_n)_{n\in\mathbb{N}}$ *be two convergent sequences in the metric space* (X, d)*. It holds that* $\lim x_n = \lim y_n$ *iff* $\lim d(x_n, y_n) = 0$*.*

Definition 1.1.6. A sequence $(x_n)_{n\in\mathbb{N}}$ is a *Cauchy-sequence* if for every $\rho > 0$ there is an $N \in \mathbb{N}$ such that $d(x_n, x_m) < \rho$ for all $m, n \geq N$.

Lemma 1.1.7. *In a metric space* (X, d) *every convergent sequence is a Cauchy-sequence.*

Definition 1.1.8. A metric space (X, d), in which every Cauchy sequence converges is called *complete*.

Definition 1.1.9. A function $f : (X, d_1) \to (Y, d_2)$ is *continuous* if for all $x \in X$ and $\rho > 0$ there exists a $\delta > 0$ such that $d_1(x, y) < \delta \Rightarrow d_2(f(x), f(y)) < \rho$. A function is *uniformly continuous* if for every $\rho > 0$ there is a $\delta > 0$ such that $d_1(x, y) < \delta \Rightarrow d_2(f(x), f(y)) < \rho$.

Lemma 1.1.10. *A function is continuous iff one of the following criteria is met:*

(i) The inverse image of every open set is open

(ii) The inverse image of every closed set is closed

(iii) For every convergent sequence $(x_n)_{n\in\mathbb{N}}$ it holds that $\lim f(x_n) = f(\lim x_n)$

Definition 1.1.11. Let (X, d) be a metric space. Then $((\widehat{X}, \widehat{d}), \iota)$ with $(\widehat{X}, \widehat{d})$ being a metric space and $\iota : X \to \widehat{X}$ being a function, is a *completion* of (X, d) if the following criteria are met:

(i) $(\widehat{X}, \widehat{d})$ is complete

(ii) ι is isometric (i.e. $\forall x, y \in X : \widehat{d}(\iota(x), \iota(y)) = d(x, y)$)

(iii) $\overline{\iota(X)} = \widehat{X}$ with $\overline{X}$ being the closure of X with regard to $\widehat{d}$

Lemma 1.1.12. *For every metric space (X, d) there is a completion $(\widehat{X}, \widehat{d})$. Several completions of (X, d) are pairwise isomorphic.*

Definition 1.1.13. Let X be a set and $\mathcal{T} \subseteq 2^X$. Then $\mathcal{T}$ is a *topology* on X and $(X, \mathcal{T})$ is a topological space if the following criteria are met. In this case the sets of $\mathcal{T}$ are called the *open sets* of $(X, \mathcal{T})$.

(i) $X \in \mathcal{T}$ and $\emptyset \in \mathcal{T}$

(ii) If $(O_i)_{i\in I}$ is a family of sets with $O_i \in \mathcal{T}$ for all i, then $\bigcup_{i\in I} O_i \in \mathcal{T}$

(iii) If $O_1, O_2 \in \mathcal{T}$, then $O_1 \cap O_2 \in \mathcal{T}$

We can use Lemma 1.1.10 to motivate the following definition of continuity in topological spaces:

Definition 1.1.14. Let $(X, \mathcal{T}_1)$ and $(Y, \mathcal{T}_2)$ be topological spaces and $f : X \to Y$ a function. Then f is *continuous* if for every set $O \in \mathcal{T}_2$ it holds that $f^{-1}(O) \in \mathcal{T}_1$

Lemma 1.1.15. *et $(X, \mathcal{T}_1)$ and $(Y, \mathcal{T}_2)$ be topological spaces and $f : X \to Y$ a function. Then f is continuous iff for every closed set $A \subseteq Y$ it holds that $f^{-1}(A) \subseteq X$ is also closed.*

Definition 1.1.16. Let $(X, \mathcal{T})$ be a topological space. A set $A \subseteq X$ is *closed* if its complement is open. The closure $\overline{A}$ of a set $A \subseteq X$ is the smallest closed set containing A.

Lemma 1.1.17. *Every metric space (X, d) is a topological space if we equip X with the set of open sets in (X, d) as the topology.*

Definition 1.1.18. Let $(X, \mathcal{T})$ be a topological space and D a subset of X. D is dense in X if $\overline{D} = X$.

Lemma 1.1.19. *If D is dense in X, then for every $x \in X$ there is a sequence $(a_n)_{n\in\mathbb{N}} \in D^{\mathbb{N}}$ with $\lim a_n = x$.*

Definition 1.1.20. Let $(X, \mathcal{T})$ be a topological space. A set $K \subseteq X$ is *compact* if for every covering $(V_i)_{i\in I}$ there exists a finite subset $\mathcal{F} \subseteq I$ such that $(V_i)_{i\in\mathcal{F}}$ still covers K.

Definition 1.1.21. Let (X, d) be a metric space. A set $K \subseteq X$ is *totally bounded* if for every $\rho > 0$ there is a finite set of open balls with radius $\leq \rho$ that covers K.

Lemma 1.1.22. *Let (X, d) be a metric space. A set $K \subseteq X$ is compact iff K is totally bounded and $(K, d_{|K\times K})$ is complete. Let $(\widehat{X}, \widehat{d})$ be a completion of (X, d). $\widehat{X}$ is compact iff X is totally bounded.*

Theorem 1.1.23 (Tychonoff)**.** *Let $((X_i), \mathcal{T}_i)_{i\in I}$ be a family of topological spaces. Then $\prod_{i\in I} X_i$ is compact iff all of the X_i are compact.*

Lemma 1.1.24. *Let $K \subseteq X$ be a compact set and $C \subseteq K$ a closed subset. Then C is closed.*

Lemma 1.1.25. *Let $K \subseteq X$ be a compact set and $\varphi : X \to Y$ a uniformly continuous function. Then $\varphi(K)$ is also compact.*

Lemma 1.1.26. *Let $K \subseteq X$ be a compact set. Then K is also closed.*

Theorem 1.1.27. *Let (X, d_1) and (Y, d_2) be metric spaces and (Y, d_2) complete. Furthermore, let D be dense in X and $f : D \to Y$ be uniformly continuous function. Then the following holds:*

1. *There is a unique continuous extension $F : X \to Y$ of f. Furthermore, F is uniformly continuous.*
2. *If f is isometric, then F is isometric as well.*
3. *If (X, d_1) is complete, $f(D) \subseteq Y$ is dense in Y, f is injective and $f^{-1} : f(D) \to X$ is uniformly continuous, then F is bijective.*

Corollary 1.1.28. *Let X and Y be metric spaces with the completions $\widehat{X}$ and $\widehat{Y}$ and $\varphi : X \to Y$ a uniformly continuous function. Then there is a unique extension $\widehat{\varphi} : \widehat{X} \to \widehat{Y}$ that is also uniformly continuous. If φ is surjective and $\widehat{X}$ is compact, then $\widehat{\varphi}$ is surjective as well.*

1.2 Monoids, automata and languages

Now only the important definitions and results for monoids, automata and languages. These are taken from [1] and [3].
Generally notationwise, we remark the following: There will be a lot of monoids in this thesis and strictly speaking there is a difference between the monoid $(M, \cdot, e)$ and the set M. However, we will often make no difference between them because it is usually clear, what is meant. Also, we will often omit the $\cdot$ and simply write ab instead of $a \cdot b$.

Definition 1.2.1. A monoid $(M, \cdot, e)$ with a topology on M that fulfills that $\cdot : M \times M \to M$ is continuous is called a *topological monoid*.

Definition 1.2.2. A language $L \subseteq \Sigma^*$ is *rational* if it can be obtained using a rational expression over Σ.

Lemma 1.2.3. *A language $L \subseteq \Sigma^*$ is rational iff it is recognized by a DFA.*

Definition 1.2.4. Let $D = \langle Q, \Sigma, \cdot, q_0, F\rangle$ be a DFA. Then $L(D)$ is the language recognized by D.

Lemma 1.2.5. *Let $D = \langle Q, \Sigma, \cdot, q_0, F\rangle$ be a DFA with $\cdot : Q \times \Sigma \to Q$. We can equivalently characterise D with $\langle Q, \Sigma, \odot, q_0, F\rangle$ with $\odot$ being a function from $Q \times \Sigma^*$ to Q defined by $q \odot \varepsilon = q, q \odot a = q \cdot a$ for every $a \in \Sigma$ and $q \odot xy = (q \odot x) \odot y$.*

Proof. Obviously, every function $\odot : Q \times \Sigma^* \to Q$ defines a unique function $\cdot : Q \times \Sigma \to Q$. Conversely, $\cdot : Q \times \Sigma \to Q$ defines a unique $\odot : Q \times \Sigma^* \to Q$. ■

Note, that I used $\odot$ above to emphasize the difference between $\cdot$ and $\odot$. However, since they are basically the same and induce each other, I will write $\cdot$ for both from here on.

2 Semigroups, monoids and languages

This chapter's goal is to prove some properties of finite monoids and show some connections between finite monoids and rational languages. This will lay the foundation for the next chapter and Theorem 3.2.10. The results regarding monoids, congruences and languages are taken from [1, Chapter 2], while the results regarding semigroups can be found in [3, Chapter II].

2.1 Semigroups

Later on, we will need some minor results about finite semigroups, which we will prove here:

Lemma 2.1.1. *Let S be a finite semigroup and $s \in S$. Then s has a idempotent power $x = s^r$ with $r \leq n = |S|$ (i.e. $s^r s^r = s^r$). This element x is unique for every $s \in S$.*

Proof. Consider the set $S = \{s^n \mid n \in \mathbb{N}\} \subseteq S$. Since S is clearly finite, there have to be two powers $l \neq m$ such that $s^l = s^m$. Without loss of generality $l > m$. Then $s^l = s^m s^{l-m}$. By induction, we get that $s^{m+j(l-m)} = s^m$. If we take any $k \geq m$, we have that $k = m + i$ and therefore $s^{k+j(l-m)} = s^{m+j(l-m)} s^i = s^m s^i = s^k$. Now, consider $k = j(l - m)$ such that $k \geq m$. Then

$$x^k x^k = x^{2k} = x^{k+k} = x^{k+j(l-m)} = x^k$$

and therefore x^k is idempotent. Since S has at most n elements, it follows that there is an $r \leq n$ such that $s^r = s^k$, which proves the claim.
Now, assume that there are two idempotent elements $s^r = x, s^t = y$. Then we have that

$$x = s^r = (s^r)^t = s^{rt} = (s^t)^r = s^t = y.$$

Thus, the idempotent element is unique for every s. ■

Lemma 2.1.2. *Let S be a non-empty finite semigroup. Then S has at least one idempotent element.*

Proof. This follows directly from 2.1.1. ■

Lemma 2.1.3. *Let S be a finite semigroup. Then there exists an ω such that s^ω is idempotent for every $s \in S$.*

Proof. By Lemma 2.1.1 for every $s \in S$ there exists an r_s such that s^{r_s} is idempotent. Then s^ω is certainly idempotent if we define ω as the least common multiple of all the r_s. ■

Definition 2.1.4. Let S be a semigroup. Then ω from Lemma 2.1.3 is called the *exponent* of S.

Definition 2.1.5. Let S be a semigroup. Then, $\emptyset \neq I \subseteq S$ is an *ideal* of S if $IS \subseteq I$ and $SI \subseteq I$. An ideal I is *minimal* if for every ideal I' it holds that $I \subseteq I'$

Lemma 2.1.6. *Let S be a semigroup. Then, the following statements hold:*

(i) There is an ideal of S.

(ii) The intersection of ideals is also an ideal.

(iii) There exists a unique minimal ideal.

Proof.

(i) S is clearly an ideal of S.

(ii) Let $(R_i)_{i\in I}$ be a family of ideals an $R = \bigcap_{i\in I} R$. For $x \in R$, it holds that $sx, xs \in R_i$ for every $i \in I$ and for every $s \in S$ and therefore $sx, xs \in R$. Overall, that means $SR \subseteq R$ and $RS \subseteq R$. Therefore, R is an ideal.

(iii) This follows directly from (i) and (ii).

■

Lemma 2.1.7. *Let S be a semigroup and $s \in S$. Then the minimal ideal of the subsemigroup generated by s is a group G with neutral element s^ω with ω being the exponent of S.*

Proof. Let $n = |S|$. Obviously, the subsemigroup generated by s is the set $T = \{s^n \mid n \in \mathbb{N}\}$. Consider the set $I = \{s^l s^\omega \mid l \in \mathbb{N}\}$ with s^ω being the idempotent of s. Then since T is commutative, we have that $s^l s^\omega s^k = s^k s^l s^\omega = s^{l+k} s^\omega \in I$ for every $s^k \in T$. Therefore, I is an ideal. Furthermore, because of the commutativity, we have $s^\omega s^l s^\omega = s^l s^\omega s^\omega = s^l s^\omega$. Thus, s^ω is a neutral element in I. Moreover, take a multiple of ω, $k\omega$ such that $k\omega > l$. Then $s^l s^\omega s^{k\omega - l} = s^{k\omega - l} s^l s^\omega = s^{(k+1)\omega} = s^\omega$. Thus, we can invert in the ideal I. It remains to show that I is the minimal ideal of T. Let K be an ideal of S and $s^l \in K$. Then choose a multiple of ω, $k\omega$ such that $k\omega \geq l$. It follows that $s^{k\omega - l} s^l = s^{k\omega} = s^\omega$. Therefore, s^ω has to be in K. Therefore, $I \subseteq K$, which concludes the proof. ■

2.2 Monoids and congruences

Since monoids are the main topic of this thesis, it is clear, that we have to prove some properties of them. We will start with congruences and quotient-monoids. After that, we formulate a relevant lemma about the free monoid Σ^* and surjective monoid homomorphisms.

Definition 2.2.1. Let M be a monoid. An equivalence relation $\approx$ on M is called a *congruence* if for every a, b, x, y in M such that $a \approx x, b \approx y$, it holds that $ab \approx xy$.

Definition 2.2.2. Let $\approx_1$ and $\approx_2$ be equivalence relations on the set M. We say $\approx_2$ is a *refinement* of $\approx_1$ if $x \approx_2 y \Rightarrow x \approx_1 y$.

Definition 2.2.3. Let $\approx$ be an equivalence relation on the set M. Then the *index* of $\approx$ is the number of its equivalence classes of $\approx$.

Lemma 2.2.4. *Let $(\approx_i)_{i\in I}$ be a family of congruences on the monoid M. Define the relation $\approx$ on M by $x \approx y \Leftrightarrow \forall i \in I : x \approx_i y$. Then $\approx$ is also a congruence. Furthermore, $\approx$ is a refinement of every $\approx_i$.*

Proof. Obviously, $\approx$ is reflexive, symmetric and transitive because all of the $\approx_i$ are. Furthermore, if we take $a, b, x, y \in M$ such that $a \approx x$ and $b \approx y$, then $ab \approx_i xy$ for all $i \in I$ and therefore $ab \approx xy$. Trivially, $x \approx y$ implies that $x \approx_i y$ for every $i \in I$. ■

Lemma 2.2.5. *Let M be a monoid, $\approx$ a congruence on M and e the neutral element of M. Then $M_{/\approx}$ is a monoid if equipped with the operation $[x][y] = [xy]$ and the neutral element $[e]$.*

Proof.

- Let a, b, x, y be elements of M such that $[a] = [x], [b] = [y]$. Since $\approx$ is a congruence, we have that $ab \approx xy$ and therefore that $[a][b] = [ab] = [xy] = [x][y]$. Thus, the operation is well defined.
- Let a be in M. Then obviously $[a][e] = [ae] = [a] = [ea] = [e][a]$ and therefore $[e]$ is the neutral element.

■

Lemma 2.2.6. *Let $\varphi : M \to N$ be a homomorphism from the monoid M to the monoid N. Define the relation $\approx_\varphi$ by $x \approx_\varphi y \Leftrightarrow \varphi(x) = \varphi(y)$. Then $\approx_\varphi$ is a congruence. Furthermore, it holds that $\varphi(M) \cong M_{/\approx_\varphi}$.*

Proof. Let us prove the lemma in two steps:

- Obviously, $\approx_\varphi$ is reflexive, symmetric and transitive and thus an equivalence relation. Now let a, b, x, y be elements of M such that $a \approx_\varphi x$ and $b \approx_\varphi y$. Then $\varphi(ab) = \varphi(a)\varphi(b) = \varphi(x)\varphi(y) = \varphi(xy)$ and therefore $ab \approx_\varphi xy$ and $\approx_\varphi$ is a congruence.
- In order to show the isomorphy, consider the natural homomorphism $\psi : M_{/\approx_\varphi} \to \varphi(M) : [x] \mapsto \varphi(x)$. By the definition of $\approx_\varphi$, we get that ψ is well defined and injective. Clearly, it is also a homomorphism because φ is one. Furthermore, for any $\varphi(x) \in \varphi(M)$, we have that $\psi([x]) = \varphi(x)$, which shows that ψ is also surjecive, which concludes the proof.

■

Definition 2.2.7. Let M and N be two monoids. N is a *quotient* of M if there is a surjective homomorphism $\varphi : M \to N$.

Lemma 2.2.8. *Let M and N be two monoids. Then the following are equivalent:*

(i) N is a quotient of M

(ii) There is a congruence $\approx$ on M such that $N \cong M_{/\approx}$

Proof.

$\Rightarrow$ Let N be a quotient of M. Then, there is a surjective homomorphism $varphi : M \to N$. Now consider the congruence $\approx_\varphi$ and the function $\psi : M_{/\approx_\varphi} \to N : [x] \mapsto \varphi(x)$. By the defintion of $\approx_\varphi$ we have that ψ is well defined. Clearly, $\psi([xy]) = \varphi(xy) = \varphi(x)\varphi(y) = \psi(x)\psi(y)$ and therefore, ψ is a homomorphism. Moreover, ψ is obviously surjective and injective. Thus, $N \cong M_{/\approx_\varphi}$.

$\Leftarrow$ Let $N \cong M_{/\approx}$ with the isomorphism $\psi : M_{/\approx} \to N$. Then define the function $\varphi : M \to N : x \mapsto \psi([x])$. We see that $\varphi(xy) = \psi([xy]) = \psi([x][y]) = \psi([x])\psi([y]) = \varphi(x)\varphi(y)$ and therefore, φ is a homomorphism. Since ψ is surjective, so is φ and we get that N is a quotient of M.

■

Definition 2.2.9. Let M and N be two monoids. N is a *divisor* of M if N is a quotient of a submonoid of M. We then write $N \preccurlyeq M$.

Something that is unrelated to the definitions and lemmas above, but will be highly relevant later on is the following:

Lemma 2.2.10. *Let Σ^* be the free monoid over Σ, T, S monoids and $\eta : \Sigma^* \to S$ and $\beta : T \to S$ homomorphisms with β being surjective. Then there exists a homomorphism $\varphi : \Sigma^* \to T$ such that $\eta = \beta \circ \varphi$.*

Proof. For each letter $a \in \Sigma$ consider the set $\beta^{-1}(\eta(a))$ (this set is not empty because of the surjectivity of β), pick one representative $x_a \in T$ and define φ as the homomorphic extension of $a \mapsto x_a$. By the fact that both $\beta \circ \varphi$ and η are homomorphisms, we have that $\beta(\varphi(\varepsilon)) = \eta(\varepsilon)$. By the definition of φ, it holds for every $a \in \Sigma$ that $\beta(\varphi(a)) = \beta(x_a) = \beta(\beta^{-1}(\eta(a)) = \eta(a)$. Since every word w with length $n+1$ can be written as the concatenation of two words a, b with length ≤ 1, it follows that $\beta(\varphi(w)) = \beta(\varphi(a))\beta(\varphi(b)) = \eta(a)\eta(b) = \eta(ab)$. Therefore, $\eta = \beta \circ \varphi$. ■

2.3 Languages

Languages are closely related to monoids. In this chapter, we will formulate some of the most central connections between them. The overall goal is to find ways to characterize rational languages through monoids.

Definition 2.3.1. Let $L \subseteq \Sigma^*$ be a language. Then we define the relation $\approx_L$ by

$$x \approx_L y :\Leftrightarrow \forall v, w \in \Sigma^* : vxw \in L \Leftrightarrow vyw \in L.$$

It is called the *syntactic congruence*.

Lemma 2.3.2. *The relation $\approx_L$ is in fact a concruence.*

Proof. Clearly, $\approx_L$ is reflexive, symmetric and transitive and therefore an equivalence relation. Furthermore, let a, b, x, y be words in Σ^* such that $a \approx_L x$ and $b \approx_L y$. Now take two arbitrary words $v, w \in \Sigma^*$. We have that

$$vabw \in L \Leftrightarrow vxbw \in L \Leftrightarrow vxyw \in L$$

and therefore $ab \approx_L xy$. ■

Definition 2.3.3. Let $L \subseteq \Sigma^*$ be a language and $\approx_L$ the syntactic congruence. The monoid $(\Sigma^*/_{\approx_L}, [\varepsilon], \cdot)$ is called the *syntactic monoid* of L and is denoted with $M(L)$. The homomorphism $\eta : \Sigma^* \to M(L) : w \mapsto [x]$ is called the *syntactic homomorphism*.

Definition 2.3.4. Let $L \subseteq \Sigma^*$ be a language and $x \in \Sigma^*$. We define the *left-quotient* $x^{-1}L = \{v \in \Sigma^* \mid xv \in L\}$ and the *right-quotient* $Lx^{-1} = \{v \in \Sigma^* \mid vx \in L\}$. Since the concatenation is associative, we can also define $x^{-1}Ly^{-1}$ accordingly as $x^{-1}(Ly^{-1}) = (x^{-1}L)y^{-1}$.

Definition 2.3.5. Let $L \subseteq \Sigma^*$ be a language, M a monoid and $\varphi : \Sigma^* \to M$ a homomorphism. We say φ *recognizes* L if there is a subset P of M such that $L = \varphi^{-1}(P)$. If such a φ exists for a given monoid M, we say that M *recognizes* L.

Lemma 2.3.6. *Let $L \subseteq \Sigma^*$ be a language, M a monoid and $\varphi : \Sigma^* \to M$ a homomorphism. Then the following are equivalent:*

(i) *L is recognized by φ*

(ii) *$L = \varphi^{-1}(\varphi(L))$*

Proof.

⇒ If L is recognized by φ, then there is a subset $P \subseteq M$ such that $L = \varphi^{-1}(P)$. Clearly, $\varphi(L) \subseteq P$ and therefore $\varphi^{-1}(\varphi(L)) \subseteq \varphi^{-1}(P) = L$. On the other hand, we have that $L \subseteq \varphi^{-1}(\varphi(L))$. In total, we have that $L = \varphi^{-1}(\varphi(L))$.

⇐ If $L = \varphi^{-1}(\varphi(L))$, then we have a subset $P = \varphi(L)$ of M such that $L = \varphi^{-1}(P)$ and therefore, φ recognizes L.

■

Lemma 2.3.7. *Let $L \subseteq \Sigma^*$ be a language. Then the syntactic monoid $M(L)$ recognizes L with the syntactic homomorphism η.*

Proof. Consider $P = \{[x] \mid x \in L\} \subseteq M(L)$. Obviousyly, $L \subseteq \eta^{-1}(P)$. Now, let x be in L and $y \in \Sigma^*$ such that $y \in [x]$. That means that $y \approx_L y \Leftrightarrow (\forall a, b \in \Sigma^* : axb \in L \Leftrightarrow ayb \in L)$. Now, set $a = b = \varepsilon$. Then $x \in L \Leftrightarrow y \in L$ and since $x \in L$, we have that $y \in L$. Thus, $\eta^{-1}([x]) \subseteq L$ for all $x \in L$. Moreover, it holds that $\eta^{-1}(P) = \bigcup_{x \in L} \eta^{-1}([x])$ and therefore $\eta^{-1}(P) \subseteq L$. Overall, we have that $L = \eta^{-1}(P)$. ■

Theorem 2.3.8. *Let $L \subseteq \Sigma^*$ be a language and M a monoid. Then M recognizes L iff $M(L) \preccurlyeq M$.*

Proof.

$\Rightarrow$ Let M be a monoid that recognizes L with the homomorphism φ. Obviously, $\varphi(\Sigma^*)$ is a submonoid of M and also recognizes L with the homomorphism $\varphi' : \Sigma^* \to \varphi(\Sigma^*)$ and the subset P of $\varphi(\Sigma^*)$ such that $\varphi^{-1}(P) = L$. Morevoer, by Lemma 2.2.6 $\varphi(\Sigma^*) \cong \Sigma^*_{/\approx_\varphi}$ with the isomorphism $\psi : \varphi(\Sigma^*) \to \Sigma^*_{/\approx_\varphi}$. We now want to show that $\approx_\varphi$ is a refinement of the syntacic congruence $\approx_L$. For that purpose take two words $x, y \in \Sigma^*$ such that $x \approx_\varphi y$ and two more words $u, v \in \Sigma^*$. We now have that

$$uxv \in L \Leftrightarrow P \ni \varphi(uxv) = \varphi(u)\varphi(x)\varphi(v) = \varphi(u)\varphi(y)\varphi(v) = \varphi(uyv) \Leftrightarrow uyv \in L.$$

Therefore, $x \approx_L y$ and $\approx_\varphi$ is a refinement of $\approx_L$. Now, define $\pi : \Sigma^*_{/\approx_\varphi} \to \Sigma^*_{/\approx_L} : [x]_{\approx_\varphi} \mapsto [x]_{\approx_L}$. Since $\approx_\varphi$ is a refinement of $\approx_L$, we have that π is well defined. Furthermore, it clearly is a homomorphism and surjective. Therefore, the function $\pi \circ \psi : \varphi(\Sigma^*) \to M(L)$ is a surjective homomorphism and thus $M(L) \preccurlyeq M$.

$\Leftarrow$ Now, let us assume that $M(L) \preccurlyeq M$, which means that there is a surjective homomorphism φ from a submonoid of M to $M(L)$. Without loss of generality, we assume that the submonoid is M itself. By Lemma 2.3.7 we have that there is a subset P of $M(L)$ such that $\eta^{-1}(P) = L$. Since φ is surjective, we have by Lemma 2.2.10, that there is a homomorphism $\psi : \Sigma^{\to} M$ with $\eta = \varphi \circ \psi$. Therefore, $L = \eta^{-1}(P) = \psi^{-1}(\varphi^{-1}(P)$. Thus, M recognizes L with the homomorphism ψ.

■

Definition 2.3.9. Let $D = \langle Q, \Sigma, \cdot, q_0, F\rangle$ be a DFA. Every word $w \in \Sigma^*$ induces a function $\tau_{D,w} : Q \to Q : q \mapsto q \cdot w$, where $q \cdot w$ is defined inductively by $q \cdot \varepsilon = q$ and $q \cdot (w_1 w_2) = (q \cdot w_1) \cdot w_2$. The transitions for the letters are given by the transition function of the DFA. We define the *transition monoid* $M(D)$ of D by

$$M(D) = \{\tau_{D,w} \in Q^Q \mid w \in \Sigma^*\}$$

with the neutral element $\tau_{D,\varepsilon} : q \mapsto q$ and the reversed composition $\tau_{D,x}\tau_{D,y} : q \mapsto qxy$

Lemma 2.3.10. *$M(D)$ is in fact a monoid. Furthermore, $M(D)$ is finite and the function $\tau_D : \Sigma^* \to M(D) : x \mapsto \tau_{D,x}$ is a surjective monoid homomorphism.*

Proof. We have a neutral element and a binary operation which is clearly associative. $M(D)$ is clearly closed under this operation because $\tau_{D,x}\tau_{D,y} = \tau_{D,xy}$. Therefore, $M(D)$ is a monoid. As a subset of the finite set Q^Q, it is trivially finite. Obviously, the function τ_D is a homomorphism and surjective. ■

Definition 2.3.11. Let $D = \langle Q, \Sigma, \cdot, q_0, F\rangle$ be a DFA and τ_D as in Lemma 2.3.10. Then the congruence $\approx_D = \approx_{\tau_D}$ is the *congruence of D.*

Lemma 2.3.12. *Let $D = \langle Q, \Sigma, \cdot, q_0, F\rangle$ be a DFA. Then, it holds that $M(D) \cong \Sigma^*_{/\approx_D}$.*

Proof. This follows directly from Lemma 2.2.6. ■

Lemma 2.3.13. *Let $D = \langle Q, \Sigma, \cdot, q_0, F\rangle$ be a DFA that recognizes $L \subseteq \Sigma^*$. Then, $M(D)$ recognizes L with the homomorphism τ_D.*

Proof. Define $P = \{\tau \in M(D) \mid q_0\tau \in F\}$. Now, we have that

$$w \in L \Leftrightarrow q_0 \cdot \tau_{D,w} \in F \Leftrightarrow \tau_D(w) \in P \Leftrightarrow w \in \tau_D^{-1}(P).$$

Thus, $L = \tau_D^{-1}(P)$. ■

Lemma 2.3.14. *Let $L \subseteq \Sigma^*$ be a language. Then L is rational iff it is recognized by a finite monoid.*

Proof.

⇒ If L is rational, then L is recognized by a DFA D and its monoid finite transition monoid $M(D)$ by Lemma 2.3.13.

⇐ Assume that L is recognized by a finite monoid M with the homomorphism φ and the set P. Then define the DFA $D = \langle M, \Sigma, \cdot, e, P\rangle$ with $m \cdot a = m\varphi(a)$ for $m \in M, a \in \Sigma$. Now, we have that for all words w of the length ≤ 1, it holds that $m \cdot w = m\varphi(m)$. Since every word w of lenght $n+1$ can be written as the product of two words x, y of length $\leq n$, we have that

$$m \cdot w = m \cdot xy = m\varphi(x)\varphi(y) = m\varphi(xy) = m\varphi(w)$$

and by induction, we get that for every word w and every element $m \in M$ it holds that $m \cdot w = m\varphi(w)$. Therefore, we have

$$w \in L(D) \Leftrightarrow e \cdot w \in P \Leftrightarrow e\varphi(w) \in P \Leftrightarrow \varphi(w) \in P \Leftrightarrow w \in \varphi^{-1}(P) = L.$$

Thus, L is recognized by a DFA and hence rational.

■

Corollary 2.3.15. *Let $L \subseteq \Sigma^*$ be a language. Then L is rational iff $M(L)$ is finite.*

3 The variety theorem of Eilenberg

In this chapter, we will show the connection between varieties of finite monoids and the varieties of rational languages building upon the foundations from the last chapter. The main result is Theorem 3.2.10. This chapter relatively closely follows [1, Section 2.4].

3.1 Varieties of finite monoids and rational languages

First, we need to define, what varieties of finite monoids and rational languages are.

Definition 3.1.1. Let $\mathcal{V}$ be a class of finite monoids. $\mathcal{V}$ is a *variety*[1] if the following criteria are met:

(i) If $M \in \mathcal{V}$ and N is a submonoid of M, then $N \in \mathcal{V}$

(ii) If $M \in \mathcal{V}$ and N is a quotient of M, then $N \in \mathcal{V}$

(iii) If $(M_i)_{i=1}^n \in \mathcal{V}^n$, then $\prod_{i=1}^n M_i \in \mathcal{V}$

By Definition 2.2.9 N is a divisor of M if it is a quotient of a submonoid of M. Since every monoid is a submonoid and a quotient of itself, we can replace (i) and (ii) with the criterion

(iv) If $M \in \mathcal{V}$ and $N \preccurlyeq M$, then $N \in \mathcal{V}$

Furthermore, we can allso replace (iii) with these two criteria:

(v) The trivial monoid $\{1\}$ is in $\mathcal{V}$

(vi) If $M, n \in \mathcal{V}$, then $M \times N \in \mathcal{V}$

While it is quite clear that we need (vi) to get (iii), it is a bit more subtle, why we need (v). It is necessary because (iii) also covers the empty product defined as $\{1\}$, which is essentially the neutral element of the product of monoids and allows to work with finite products without having to worry about the empty product.

Lemma 3.1.2. *Let $\mathcal{V}$ and $\mathcal{W}$ be two varieties of finite monoids, then $\mathcal{V} \cap \mathcal{W}$ is also a variety.*

Proof. Consider the three cases:

[1] Note, that this definition varies from the one in Birkhoff's theorem

(i) Let $M \in \mathcal{V} \cap \mathcal{W}$ and N is a submonoid of M. Since M is in both $\mathcal{V}$ and $\mathcal{W}$, N is in both as well and therefore in the intersection.

(ii) Let $M \in \mathcal{V} \cap \mathcal{M}$ and N is a quotient of M. For the same reason as above, N is in both $\mathcal{V}$ and $\mathcal{W}$ and therefore in the intersection.

(iii) Let $(M_i)_{i \in I}$ be a finite familiy of elements of $\mathcal{V} \cap \mathcal{W}$. Then the product of the M_i is in both $\mathcal{V}$ and $\mathcal{W}$ and therefore in the intersection.

■

Let us now look at varieties of rational languages.

Definition 3.1.3. A class of rational languages is a function $\mathcal{L}$ that maps each alphabet Σ to a set of rational languages $\mathcal{L}_\Sigma$

Note that our intuitive idea of a class of rational languages in the regular sense is very similar to this definition.

Definition 3.1.4. Let $\mathcal{L}$ be a class of rational languages. $\mathcal{L}$ is *variety* of rational languages if the following criteria are met for all alphabets Σ and Γ:

(i) $\mathcal{L}_\Sigma$ is closed under union, finite intersection and complement

(ii) For every $L \in \mathcal{L}_\Sigma$ and every $x \in \Sigma$ it holds that $x^{-1}L \in \mathcal{L}_\Sigma$ and $Lx^{-1} \in \mathcal{L}_\Sigma$

(iii) For every $L \in \mathcal{L}_\Sigma$ and every homomorphism $\varphi : \Gamma^* \to \Sigma^*$ it holds that $\varphi^{-1}(L) \in \mathcal{L}_\Gamma$

Because we only deal with varieties/classes of rational languages and finite monoids, we simply speak of varieties/classes of languages and varieties/classes of monoids instead.

3.2 The theorem of Eilenberg

Now, we want to look at the connection of varieties of monoids and varieties of languages.

Definition 3.2.1. Let $\mathcal{V}$ be a variety of monoids and Σ an alphabet. We define

$$\Phi(\mathcal{V})(\Sigma) = \Phi(\mathcal{V})_\Sigma = \{L \subseteq \Sigma^* \mid M(L) \in \mathcal{V}\}$$

We see that this definition maps a variety of finite monoids to a class of regular languages by Lemma 2.3.15. Our goal for the rest of the chapter now is to show that Φ is a bijection between the varieties of monoids and the varieties of languages. We start with the following:

Lemma 3.2.2. *Let $\mathcal{V}$ be a variety of monoids. It holds that*

$$\Phi(\mathcal{V})_\Sigma = \{L \subseteq \Sigma^* \mid \textit{There is a monoid } M \in \mathcal{V} \textit{ that recognizes } L\}$$

Proof. For this proof, let us define $B := \{L \subseteq \Sigma^* \mid \text{There is a monoid } M \in \mathcal{V} \text{ that recognizes } L\}$.

$\subseteq$ If $L \in \Phi(\mathcal{V})_\Sigma$, then $M(L) \in \mathcal{V}$. By Lemma 2.3.7 L is recognized by $M(L)$ and therefore $L \in B$.

$\supseteq$ If $L \in B$, then there is a monoid $M \in \mathcal{V}$ that recognizes L. By Lemma 2.3.8, we have that $M(L) \preccurlyeq M$ and therefore $M(L) \in \mathcal{V}$.

■

This leads to the following result:

Lemma 3.2.3. *Let $\mathcal{V}$ be a variety of monoids. Then $\Phi(\mathcal{V})$ is a variety of languages.*

Proof. (i) We fix an alphabet Σ and consider two languages $L_1, L_2 \in \Phi(\mathcal{V})_\Sigma$. Let $\eta_1 : \Sigma^* \to M(L_1)$ and $\eta_2 : \Sigma^* \to M(L_2)$ be the syntactic homomorphisms of L_1 and L_2 respectively. By Lemma 2.3.7 and Lemma 2.3.6 we have that $L_1 = \eta_1^{-1}(\eta_1(L_1))$ and $L_2 = \eta_2^{-1}(\eta_2(L_2))$. If we define the monoid $M = M(L_1) \times M(L_2)$, we see that M is a finite product of elements of $\mathcal{V}$ and therefore in $\mathcal{V}$. Now, define $\eta : \Sigma^* \to M : x \mapsto (\eta_1(x), \eta_2(x))$. Clearly η is a homomorphism. Furthermore, we notice that $x \in L_1 \Leftrightarrow x \in \eta^{-1}(\eta_1(L_1) \times M(L_2))$ and $x \in L_2 \Leftrightarrow x \in \eta^{-1}(M(L_1) \times \eta_2(L_2))$. Therefore, it holds that

$$\begin{aligned} L_1 \cap L_2 &= \eta^{-1}(\eta_1(L_1) \times \eta_2(L_2)), \\ L_1 \cup L_2 &= \eta^{-1}(\eta_1(L_1) \times M(L_2) \cup M(L_1) \times \eta_2(L_2)). \end{aligned}$$

Since $L_1 = \eta_1^{-1}(\eta_1(L_1))$, we have that $\Sigma^* \setminus L_1 = \eta_1^{-1}(M(L_1) \setminus \eta_1(L_1))$. In summary, we have that $L_1 \cap L_2, L_1 \cup L_2$ and L_1^c are all recognized by a monoid of $\mathcal{V}$.

(ii) Now let $L \subseteq \Sigma^*$ be a language in $\in \Phi(\mathcal{V})_\Sigma$, η the corresponding syntactic homomorphism and $x \in \Sigma$ a letter. We define $P := \{m \in M(L) \mid \eta(x)m \in \eta(L)\}$. From this definition it follows that:

$$\begin{aligned} \eta^{-1}(P) &= \{w \in \Sigma^* \mid \eta(w) \in P\} \\ &= \{w \in \Sigma^* \mid \eta(x)\eta(w) \in \eta(L)\} \\ &= \{w \in \Sigma^* \mid \eta(xw) \in \eta(L)\} \\ &= \{w \in \Sigma^* \mid xw \in L\} \\ &= x^{-1}L \end{aligned}$$

If we define $P' = \{m \in M(L) \mid m\eta(x) \in \eta(L)\}$, we get analogously that $\eta^{-1}(P') = Lx^{-1}$. Therefore, Lx^{-1} and $x^{-1}L$ are in $\Phi(\mathcal{V})_\Sigma$.

(iii) Now let Γ be another alphabet, $\varphi : \Gamma^* \to \Sigma^*$ a homomorphism and L a language in $\Phi(\mathcal{V})_\Sigma$. Again, η denotes the syntactic homomorphism of $\mathcal{L}$. If we define $\psi = \eta \circ \varphi : \Gamma^* \to M(L)$, we have that $\psi^{-1}(\eta(L)) = \varphi^{-1}(\eta^{-1}(\eta(L))) = \varphi^{-1}(L)$. Thus, $\varphi^{-1}(L)$ is recognized by ψ and therefore by $M(L)$.

■

The next step is to prove the injectivity of Φ. However, for this, we need some lemmas:

Lemma 3.2.4. *Let M be a monoid and $\approx_1$ and $\approx_2$ two congruences on M such that $\approx_1$ is a refinement of $\approx_2$ (i.e. $x \approx_1 y \Rightarrow x \approx_2 y$). Then $M_{/\approx_2}$ is a quotient of $M_{/\approx_1}$.*

Proof. If we recall Definition 2.2.7, we simply have to find a surjective homomorphism from $M_{/\approx_1}$ to $M_{/\approx_2}$. For this, simply consider $\varphi : M_{/\approx_1} \to M_{/\approx_2} : [x]_1 \mapsto [x]_2$. By the fact that $\approx_1$ is a refinement of $\approx_2$, we get that φ is well defined. Furthermore, by the definition of the binary operation on $M_{/\approx_1}$ and $M_{/\approx_2}$, we have that φ is clearly a homomorphism. Now, consider any $[x]_2 \in M_{/\approx_2}$. Clearly, $\varphi([x]_1) = [x]_2$ and therefore, φ is surjective. ■

Lemma 3.2.5. *Let M be a monooid and $(\approx_i)_{i\in I}$ a family of congruences on M. We define a new congruence $\approx$ by $x \approx y \Leftrightarrow \forall i \in I : x \approx_i y$. Then, $M_{/\approx}$ is isomorphic to a submonoid of $\prod_{i\in I} M_{/\approx_i}$.*

Proof. For all $i \in I$, define $\pi_i : M \to M_{/\approx_i} : x \mapsto [x]_i$. Then, define $\pi : M \to \prod_{i\in I} M_{/\approx_i} : x \mapsto (\pi_i(x))_{i\in I} = ([x]_i)_{i\in I}$. Clearly, all the π_i are homomorphisms and therefore also π is a homomorphism. Therefore, we can consider the congruence $\approx_\pi$. By construction of π, we have that

$$x \approx_\pi y \Leftrightarrow \pi(x) = \pi(y) \Leftrightarrow \forall i \in I : \pi_i(x) = \pi_i(y) \Leftrightarrow \forall i \in I : x \approx_i y \Leftrightarrow x \approx y.$$

Therefore, we get that $M_{/\approx} = M_{/\approx_\pi} \cong \pi(M)$, which is a submonoid of $\prod_{i\in I} M_{/\approx_i}$. The isomorphy between $M_{/\approx_\pi}$ and $\pi(M)$ follows from Lemma 2.2.6. ■

Lemma 3.2.6. *Let $\mathcal{V}$ be a variety of monoids and $M \in \mathcal{V}$. Then there is an alphabet Σ and languages $L_1, \dots L_n \in \Phi(\mathcal{V})_\Sigma$ such that $M \preccurlyeq \prod_{i=1}^n M(L_i)$.*

Proof. Consider the alphabet $\Sigma = M$ and the homomorphism $\varphi : \Sigma^* \to M$ that extends the identity function $\Sigma \to M : a \mapsto a$. Since M is finite, we can enumerate the elements of M such that $M = \{m_i \mid i = 1, \dots, n\}$. Now, consider the language $L_i = \varphi^{-1}(m_i)$. Obviously, every L_i is recognized by M and therefore every L_i lies in $\Phi(\mathcal{V})_\Sigma$. We define the relation $\approx$ on Σ^* by $x \approx y \Leftrightarrow \forall i \in \{1, \dots, n\} : x \approx_{L_i} y$. Then, by Lemma 2.2.4, we have that $\approx$ is a congruence. Now, let us also consider the congruence $\approx_\varphi$. Take arbitrary $x, y \in \Sigma^*$ such that $x \approx y$. Since, φ is surely surjective, there is an i such that $m_i = \varphi(x)$. By choice of x and y, we have that $x \approx_{L_{\varphi(x)}} y$, which means that $\varepsilon x \varepsilon \in L_{\varphi(x)}$ iff $\varepsilon y \varepsilon \in L_{\varphi(x)}$. However, $x \in L_{\varphi(x)} = \varphi^{-1}(\varphi(x))$ and therefore $y \in \varphi^{-1}(\varphi(x))$. In summary, that means that $x \approx y$ implies that $\varphi(x) = \varphi(y)$ and therefore that $\approx$ is a refinement of $\approx_\varphi$.
By Lemma 2.2.6, we have that $M = \varphi(\Sigma^*) \cong \Sigma^*_{/\approx_\varphi}$ and since $\approx$ is a refinement of $\approx_\varphi$, it follows that $\Sigma^*_{/\approx_\varphi}$ is a quotient of $\Sigma^*_{/\approx}$ by Lemma 3.2.4. Furthermore, we have by Lemma 3.2.5 that $\Sigma^*_{/\approx}$ is isomorphic to a submonoid of $\prod_{i=1}^n \Sigma^*_{/\approx_i} = \prod_{i=1}^n M(L_i)$. Therefore, by connecting the respective surjective homomorphisms and isomorphisms, we get a surjective homomorphism from a submonoid of $\prod_{i=1}^n M(L_i)$ to M and thus $M \preccurlyeq \prod_{i=1}^n M(L_i)$. ■

Lemma 3.2.7. *Let $\mathcal{V}$ and $\mathcal{W}$ be varieties of monoids. Then $\mathcal{V} \subseteq \mathcal{W}$ iff for every alphabet Σ, it holds that $\Phi(\mathcal{V})_\Sigma \subseteq \Phi(\mathcal{W})_\Sigma$. In particular it holds that $\mathcal{V} = \mathcal{W}$ iff for every alphabet Σ, we have that $\Phi(\mathcal{V})_\Sigma = \Phi(\mathcal{W})_\Sigma$ or in other words iff $\Phi(\mathcal{V}) = \Phi(\mathcal{W})$. Therefore, Φ is injective.*

Proof.

⇒ By the definition of $\Phi(\mathcal{V})_\Sigma$, it is clear that $\mathcal{V} \subseteq \mathcal{W}$ implies that $\Phi(\mathcal{V})_\Sigma = \Phi(\mathcal{W})_\Sigma$ for every alphabet Σ.

$\Leftarrow$ Now assume that $\Phi(\mathcal{V})_\Sigma = \Phi(\mathcal{W})_\Sigma$ for every alphabet Σ and take a monoid $M \in \mathcal{V}$. By 3.2.6 we have that there are languages $L_1, \ldots, L_n \in \Phi(\mathcal{V})_\Sigma \subseteq \Phi(\mathcal{W})_\Sigma$ such that $M \preccurlyeq \prod_{i=1}^n M(L_i)$. By the definition of $\Phi(\mathcal{W})_\Sigma$, we have that all the $M(L_i)$ are in $\mathcal{W}$. Therefore, their product is also in $\mathcal{W}$ and thus $M \in \mathcal{W}$ because it divides a monoid of $\mathcal{W}$.

■

The last step is to show the surjectivity of Φ. Again, we need a lemma:

Lemma 3.2.8. *Let $\mathcal{L}$ be a variety of languages, Σ an alphabet, L a language in $\mathcal{L}_\Sigma$ and η the syntactic homomorphism of L. Then, for every $m \in M(L)$, it holds that $\eta^{-1}(m) \in \mathcal{L}_\Sigma$.*

Proof. For every word $w \in \Sigma^*$, we define:

$$C(w) = \{(u, v) \in \Sigma^* \times \Sigma^* \mid uwv \in L\} = \{(u, v) \in \Sigma^* \times \Sigma^* \mid w \in u^{-1}Lv^{-1}\}.$$

For two words x, y, we now have that

$$x \approx_L y \Leftrightarrow (\forall u, v \in \Sigma^* : uxv \in L \Leftrightarrow uyv \in L) \Leftrightarrow C(x) = C(y).$$

We now claim that

$$[x]_{\approx_L} = \Big(\bigcap_{(u,v)\in C(x)} u^{-1}Lv^{-1}\Big) \setminus \Big(\bigcup_{(u,v)\notin C(x)} u^{-1}Lv^{-1}\Big) = A \setminus B.$$

To prove this claim, let us consider two cases:

$\subseteq$ Let w be in $[x]_{\approx_L}$. Then $w \in u^{-1}Lv^{-1}$ for all $(u, v) \in C(x)$ since $C(x) = C(w)$.

$\supseteq$ For this direction consider a w in the right side of the equation above. Since w is in $u^{-1}Lv^{-1}$ for all the $(u, v) \in C(x)$ but in none of the $u^{-1}Lv^{-1}$ for $(u, v) \in C(x)^c$, we have that $C(x) = C(w)$ and therefore $[w]_{\approx_L} = [x]_{\approx_L}$.

We now note the following: L is rational and therefore $\approx_L$ has finite index. Now assume that there are infinitely many sets of the form $u^{-1}Lv^{-1}$, take a countable subset of non-empty sets of this kind and enumerate them with $(A_n)_{n\in\mathbb{N}}$. We now want to show with induction that this results in a contradiction:

- Consider the sets A_1, A_2. Without loss of generality, we have that there is an $x \in A_2 \setminus A_1$. Since A_1 is not empty, we get that there are at least two equivalence classes of $\approx_L$
- Now assume, that there are finitely many sets $(A_i)_{i=1}^k$ such that they induce n different equivalence classes of $\approx_L$. Let us denote them with $([x_i])_{i=1}^n$
- Now we now that there are only 2^n subsets of $\{[x_i] \mid i = 1, \ldots, n\}$ and since we have infinitely many sets left, we can assume A_{k+1} not to be a union of some or all of the $[x_i]$ with $i \leq n$. Now, we can distinguish two cases: If there is an $x \in A_{k+1}$ such that $x \notin A_i$ for $i \leq k$, then x is clearly not in any of the equivalence classes of $\approx_L$, we

already have. If that is not the case, then A_{k+1} is a subset of the union of all the A_i and since A_{k+1} is not the union of a subset of the $[x_i]$, we have that there is some $[x_i]$ that is partially contained in A_{k+1}. That means that there are $x, y \in [x_i]$ such that $x \in A_{k+1}$ and $y \notin A_{k+1}$. In summary, we get that there have to be at least $n+1$ equivalence classes of $\approx_L$.

Therefore an infinite set of $u^{-1}Lv^{-1}$ would induce an infinite index of $\approx_L$ and that cannot be the case. Thus, there are only finitely many $u^{-1}Lv^{-1}$. Since $L \in \mathcal{L}_\Sigma$, we have that all the $v^{-1}Lu^{-1}$ are in $\mathcal{L}_\Sigma$. Furthermore, A is the finite intersection of elements of $\mathcal{L}_\Sigma$ and B is the finite union of elements of $\mathcal{L}_\Sigma$. Therefore $[x]_{\approx_L} = A \setminus B = A \cap B^c$ is also in $\mathcal{L}$. Now, we now that η is surjective and for every $m \in M(L)$, we find an $x \in L$ such that $m = \eta(x)$ and therefore $\eta^{-1}(m) = \eta^{-1}(\eta(x)) = [x]_{\approx_L} \in \mathcal{L}_\Sigma$. ■

Now, we can finally prove the surjectivity:

Lemma 3.2.9. *For every variety $\mathcal{L}$ of languages, there is a variety of monoids $\mathcal{V}$ such that $\Phi(\mathcal{V}) = \mathcal{L}$*

Proof. Let $\mathcal{L}$ be a variety of languages and define $\mathcal{V}$ as the variety of monoids generated by $\{M(L) \mid L \in \mathcal{L}_\Sigma, \Sigma \text{ is an alphabet}\}$. We now want to show that $\Phi(\mathcal{V}) = \mathcal{L}$, which is equivalent to showing that $\Phi(\mathcal{V})_\Sigma = \mathcal{L}_\Sigma$ for all alphabets Σ. For that purpose, fix an alphabet Σ.

- $\subseteq$ If L is in $\mathcal{L}_\Sigma$, then $M(L)$ is in $\mathcal{V}$ and therefore L is in $\Phi(\mathcal{V})_\Sigma$ per definition.
- $\supseteq$ Let $L \in \Phi(\mathcal{V})_\Sigma$. Then $M(L)$ is in $\mathcal{V}$ and by Lemma 3.2.6, we have that there is an alphabet Γ, an $n \geq 1$ and languages $L_1, \dots L_n$ such that $M(L) \preccurlyeq \prod_{i=1}^n M(L_i) = M$. By Theorem 2.3.8 we have that M recognizes L and therefore, there is a homomorphism $\varphi : \Sigma^* \to M$ and a $P \subseteq M$ such that $\varphi^{-1}(P) = L$. Now, define $\pi_i : M \to M(L_i) : (m_k)_{k=1}^n \mapsto m_i$ and $\varphi_i = \pi_i \circ \varphi$. Moreover, let η_i be the syntactic hommomorphism of L_i. Since η_i is surjective, we have by Lemma 2.2.10 that there is a homomorphism ψ_i such that $\varphi_i = \eta_i \circ \psi_i$. This works for every i. That means, the following diagram commutates:

$$\begin{array}{ccc} \Sigma^* & \xrightarrow{\psi_i} & \Gamma^* \\ \downarrow{\scriptstyle \phi} & \searrow^{\phi_i} & \downarrow{\scriptstyle \eta_i} \\ M & \xrightarrow{\pi_i} & D \end{array}$$

We still want to show that $L \in \mathcal{L}_\Sigma$. First, we see that $L = \bigcup_{m \in P} \varphi^{-1}(m)$. Since P is finite as a subset of M and $\mathcal{L}_\Sigma$ is closed under finite union, it is enough to show that $\varphi^{-1}(m) \in \mathcal{L}_\Sigma$ for every $m \in P$. We now consider an arbitrary $m = (m_i)_{i=1}^n \in M$. Then clearly,

$$w \in \varphi^{-1}(m) \Leftrightarrow w \in \varphi^{-1}((m_i)_{i=1}^n) \Leftrightarrow \forall i = 1, \dots n : w \in \varphi_i^{-1}(m_i) \Leftrightarrow w \in \bigcap_{i=1}^n \varphi_i^{-1}(m_i).$$

Therefore, $\varphi^{-1}(m) = \bigcap_{i=1}^{n} \varphi_i^{-1}(m_i)$. Again, $\mathcal{L}_\Sigma$ is closed under finite intersection and we have, that it is enough to show that $\varphi_i^{-1}(m_i)$ is in $\mathcal{L}_\Sigma$ for all $i = 1, \ldots, n$ and $m_i \in M(L_i)$. Since $\varphi_i = \eta_i \circ \psi_i$, we have that $\varphi_i^{-1}(m_i) = \psi_i^{-1}(\eta_i^{-1}(m_i))$. However, ψ_i is a homomorphism from Σ^* to Γ^* and $\mathcal{L}_\Sigma$ is closed under inverse homomorphisms. Therfore, it suffices to show that $\eta_i^{-1}(m_i) \in \mathcal{L}_\Sigma$ for all $m_i \in \mathcal{M}(L_i)$. That follows from 3.2.8, which concludes the proof.

■

These results together, now lead to the following theorem:

Theorem 3.2.10 (Eilenberg)**.** Φ *is a bijection between the varieties of finite monoids and the varieties of rational languages.*

Proof. Φ is well defined by Lemma 3.2.3, injective by Lemma 3.2.7 and surjective by Lemma 3.2.9 ■

4 The profinite world

The goal of this chapter is to define the set of *profinite words* over an alphabet Σ and to prove some properties of it. This will be foundation for the next chapter and Theorem 5.3.5. In order to do this, we define a metric on the set of words and look at the completion of said set with regard to this metric. This chapter closely follows [3, Chapter X]. For the rest of the chapter, let Σ be a finite alphabet.

4.1 The profinite metric

In this section, we introduce a metric on Σ^* and prove some properties that will come in handy later on.

Definition 4.1.1. Let u, v be two words in Σ^* and $(M, \cdot, e)$ a finite monoid. A homomorphism $\varphi : \Sigma^* \to M$ *separates* u and v if $\varphi(u) \neq \varphi(v)$. Furthermore, $(M, \cdot, e)$ separates u and v if there exists a homomorphism $\varphi : (\Sigma^*, \cdot, \varepsilon) \to (M, \cdot, e)$ that separates u and v.

Example 4.1.2. Let u, v be two words in $\{a, b\}^*$ such that $|u|_a \not\equiv |v|_a \mod 2$ with $|x|_y$ being the number of occurences of y in x. Then $\varphi : \{a, b\}^* \to \mathbb{Z}_2$ with $\varphi(x) = |x| \mod 2$ is a homomorphism if we equip $\mathbb{Z}_2$ with $+$ as an operation. Furthermore, φ separates u and v.

This can be generalised:

Lemma 4.1.3. *Let u, v be distinct words in Σ^*. Then u and v can be separated by a finite monoid.*

Proof. We recall Lemma 2.3.14 that states that a language is rational iff it is recognised by a finite monoid. $\{u\}$ is surely rational. Therefore, there exists a monoid $(M, \cdot, e)$, a homomorhism $\varphi : \Sigma^* \to M$ and subset P of M, such that $\varphi^{-1}(P) = \{u\}$. Since $v \notin \{u\}$, $\varphi(v) \notin P$. Thus, $\varphi(u) \neq \varphi(v)$. ■

We can now define our metric:

Definition 4.1.4. Let u, v be two words from Σ^*. We define $r(u, v) = \min\{|M| \mid M \text{ separates } u \text{ and } v\}$ and $d(u, v) := 2^{-r}$ with the convention that $\min \emptyset = +\infty$ and $2^{-\infty} = 0$.

The name d already tells us, that it might be a metric. We can even say the following:

Lemma 4.1.5. *The function d is an ultra-metric (and in particular a metric). That means:*

(i) $d(u, v) = 0 \Leftrightarrow u = v$

(ii) $d(u, v) = d(v, u)$

(iii) $d(u,w) \leq \max\{d(u,v), d(w,v)\}$ *for all* $w \in \Sigma^*$

Furthermore, it holds that

(iv) $d(uw,vw) \leq d(u,v)$ *and* $d(wu,wv) \leq d(u,v)$ *for all* $w \in \Sigma^*$

Proof. We look at the properties individually:

(i) Follows directly from the definition of d since $2^{-r} > 0$ for all natural numbers r.

(ii) Follows directly from the definition.

(iii) Without loss of generality, we assume that u, v, w are all distinct since otherwise, it would become trivial. We now assume that M seperates u and w with the homomorphism φ. Then φ also separates either u and v or v and w because otherwise $\varphi(u) = \varphi(v) = \varphi(w)$. That means that $\min\{r(u,v), r(v,w)\} \leq r(u,w)$. Therefore, $d(u,w) \leq \max\{d(u,v), d(v,w)\}$.

(iv) If M separates uw and vw with the homomorphism φ, then ceratinly $\varphi(u) \neq \varphi(v)$. Again, this translates to $r(u,v) \leq r(uw,vw)$ and therefore $d(u,v) \geq d(uw,vw)$. Analogously, we get that $d(u,v) \geq d(wu,wv)$.

■

That means that (Σ^*, d) is a metric space. Before we carry on with the completion of (Σ^*, d), we prove some properties.

Lemma 4.1.6. *The topology defined by* d *on* Σ^* *is discrete. That means that every subset of* Σ^* *is clopen (i.e. open and closed).*

Proof. Let u be a word in Σ^*, M the syntactic monoid of $\{u\}$, n its size and $\varphi : \Sigma^* \to M$ the homomorphism that recognizes M. Now take any word v in Σ^* with $d(u,v) < 2^{-n}$. It follows that $r(u,v) > n$, and that M does not separate u and v. Therefore, $\varphi(u) = \varphi(v)$, which means that $v \in \varphi^{-1}(\varphi(\{u\})) = \{u\}$ (the equality holds because u is clearly rational, cf. Lemma 2.3.6). Thus, $u = v$. That means, $U(u, 2^{-n}) = \{u\}$ and that $\{u\}$ is open for every word $u \in \Sigma^*$. Now let A be any subset of Σ^*. We see that $A = \bigcup_{x \in A} \{x\}$ is open. Also, $A^c = \bigcup_{x \in A^c} \{x\}$ is open as well, which means that A is closed and therefore clopen. ■

Before we look at the connection of rational languages and open balls, we need to consider the following relation:

Definition 4.1.7. For any $n \in \mathbb{N}$, we define $\sim_n$ by

$$x \sim_n y :\Leftrightarrow \text{for all homomorphisms } \varphi \text{ from } \Sigma^* \text{ to a monoid of size} \leq n \text{ it holds that } \varphi(x) = \varphi(y).$$

This relation has some useful properties:

Lemma 4.1.8. *$\sim_n$ is a congruence relation with finite index. Moreover, the equivalence classes of $\sim_n$ are open balls with radius 2^{-n}. In particular, it holds that $\pi_n^{-1}([x]_{\sim_n}) = U(x, 2^{-1})$ with π_n being the canonical homomorphism from Σ^* to $\Sigma^*_{/\sim_n}$.*

Proof. It is obvious that $\sim_n$ is reflexive and symmetric. Almost as clearly it is transitive. Therefore, $\sim_n$ is an equivalence relation. Now, we take $a, b, x, z \in \Sigma^*$ such that $a \sim_n x$ and $b \sim_n y$ and an arbitrary homomorphism $\varphi : \Sigma^* \to M$ with $(M, \cdot, e)$ being a finite monoid of size $\leq$ n. It follows from the definition that $\varphi(ab) = \varphi(a)\varphi(b) = \varphi(x)\varphi(y) = \varphi(xy)$. Since φ and $(M, \cdot, e)$ were arbitrary, we get that $ab \sim_n xy$. Therefore, $\sim_n$ is also a congruence.
We also note the following: Σ is finite. That means, there are at most $n^{|\Sigma|}$ homomorphisms for any given monoid $(M, \cdot, e)$ with $|M| \leq n$. Also we see that there are only finitely many possibilities to define a binary relation on a finite set, which means that there are also finitely many monoids with cardinality $\leq n$ (up to isomorphy). That means, there are also finitely many homomorphisms from Σ^* to a monoid with cardinality $\leq n$ if we only consider the monoids that are not isomorphic. Let $\mathcal{M}$ be the set of these homomorphisms and m its cardinality. Then, there are only nm possible values for the tuple $(\varphi(x))_{\varphi \in \mathcal{M}}$ for any $x \in \Sigma^*$ and therefore also at most nm equivalence classes. That means, $\sim_n$ has finite index.
Also quite obviously

$$U(x, 2^{-n}) = \{y \in \Sigma^* \mid r(x, y) > n\} = \{y \in \Sigma^* \mid x \sim_n y\} = \pi_n^{-1}([x]_{\sim_n}),$$

which concludes the proof. ■

Now, let us look the connection of rational languages and open balls of (Σ^*, d):

Lemma 4.1.9. *It holds that:*

(i) Every open ball $U(x, \rho)$ of (Σ^*, d) is a rational language.

(ii) Every rational language over Σ is a finite union of open balls.

Proof.

(i) We first note that for all $u, v \in \Sigma^*$ it holds that $d(u, v) \leq \frac{1}{4}$. Therefore, $U(x, \rho) = \Sigma^*$ if $\rho > \frac{1}{4}$ which is trivially rational. That means, we can assume ρ not to be bigger than $\frac{1}{4}$. Thus, there exists a unique natural number n such that $2^{-(n+1)} < \rho \leq 2^{-n}$. Now we consider $\sim_n$.
Let y be a word in $U(x, 2^{-n})$. Since $d(x, y) = 2^{-l}$ and $d(x, y) < 2^{-n}$ it holds that $d(x, y) \leq 2^{-(n+1)} < \rho$. Therefore, $U(x, 2^{-n}) \subseteq U(x, \rho)$. The inclusion $U(x, \rho) \subseteq U(x, 2^{-n})$ is trivial. It follows that $U(x, \rho) = U(x, 2^{-n})$.
Since $\sim_n$ is a congruence, we can consider the quotient monoid $(\Sigma^*_{/\sim_n}, \cdot, [\varepsilon])$ and the canonical homomorphism $\pi_n : \Sigma^* \to \Sigma^*_{/\sim_n}$. With our observation and Lemma 4.1.8, it now holds that

$$U(x, \rho) = U(x, 2^{-n}) = \pi_n^{-1}(\pi_n(\{x\})).$$

That means that $U(x, \rho)$ is recognized by $(\Sigma^*_{/\sim_n}, \cdot, [\varepsilon])$ and is therefore a rational language.

(ii) Now let L be a rational language and $(M, \cdot, e)$ be its syntactic monoid with the cardinality n and the homomorphism φ. Let x, y be two words in Σ^* and $x \sim_n y$. Then $\varphi(x) = \varphi(y)$ because they have the same image under any homomorphism to a monoid with cardinality $\leq n$. That means that the function $\psi : \Sigma^*_{/\sim_n} \to M$ with $\psi([x]) = \varphi(x)$ is well defined and obviously a homomorphism because φ is. We see that $\varphi = \psi \circ \pi_n$. Let $P = \varphi(L)$. By Lemma 2.3.7 and Lemma 2.3.6 and because set union and inverse image can be switched it follows that

$$L = \varphi^{-1}(P) = (\psi \circ \pi_n)^{-1}(P) = \pi_n^{-1}(\psi^{-1}(P)) = \bigcup_{m \in \psi^{-1}(P)} \pi_n^{-1}(m).$$

Now if $\pi_n(u) = [u]$, then $\pi_n^{-1}([u]) = \pi_n^{-1}(\pi_n(u)) = U(u, 2^{-n})$ as reasoned above. Since $\Sigma^*_{/\sim_n}$ is finite, so is $\psi^{-1}(P) \subseteq \Sigma^*_{/\sim_n}$. Therefore L is a finite union of open balls.

■

A property, we will need later on for the completion is the following:

Lemma 4.1.10. *The concatenation $(u, v) \mapsto uv$ from $\Sigma^* \times \Sigma^*$ to Σ^* is uniformly continuous (with $\Sigma^* \times \Sigma^*$ being equipped with the maximum-metric).*

Proof. By Lemma 4.1.5 it holds for $a, b, x, y \in \Sigma^*$ that

$$d(ab, xy) \leq \max\{d(ab, ay), d(ay, xy)\} \leq \max\{d(b, y), d(a, x)\} = d((a, b), (x, y)).$$

Therefore, it generally holds that $d((a, b), (x, y)) < \rho \Rightarrow d(ab, xy) < \rho$ for any $\rho > 0$. ■

It follows, that (Σ^*, d) is a topological monoid.
Another feature of (Σ^*, d) is the following:

Lemma 4.1.11. *(Σ^*, d) is totally bounded.*

Proof. Lemma 4.1.8 states that the equivalence classes of $\sim_n$ are open balls with radius 2^{-n} and that there are only finitely many, which proves the lemma. ■

We can now use this lemma, to prove an important theorem:

Theorem 4.1.12. *A function $\varphi : \Sigma^* \to \Gamma^*$ is uniformly continuous (both Σ^* and Γ^* are equipped with d) iff for every rational language L of Γ^*, the language $\varphi^{-1}(L)$ is also rational.*

Proof.

⇒ We assume that $\varphi : \Sigma^* \to \Gamma^*$ is uniformly continuous and $L \subseteq \Gamma^*$ is rational. By Lemma 4.1.9 L is a finite union of open balls. Therefore, it is enough to look at the case where L is a single open ball because otherwise we could switch inverse image and set union. Let $L = U(x, \rho)$. Since φ is uniformly continuous there is a $\delta > 0$ such that $d(x, y) < \delta \Rightarrow d(\varphi(x), \varphi(y)) < \rho$. We can assume that δ is of the form 2^{-n} with $n \in \mathbb{N}$. Let us now take a $u \in \varphi^{-1}(L)$ and a v such that $v \in U(u, 2^{-n})$. We

have that $d(x, \varphi(u)) < \rho$ because $u \in \varphi^{-1}(L)$ and also that $d(\varphi(u), \varphi(v)) < \rho$ because $d(u, v) \leq 2^{-n}$. By d being an ultrametric it follows that

$$d(x, \varphi(v)) \leq \max\{d(x, \varphi(u)), d(\varphi(u), \varphi(v))\} < \rho$$

and therefore $\varphi(v) \in L$. That means that for any $u \in \varphi^{-1}(L)$ it holds that $U(u, 2^{-n}) \subseteq \varphi^{-1}(L)$. Obviously, it also holds that

$$\varphi^{-1}(L) \subseteq \bigcup_{u \in \varphi^{-1}(L)} U(u, 2^{-n})$$

and therefore

$$\varphi^{-1}(L) = \bigcup_{u \in \varphi^{-1}(L)} U(u, 2^{-n}).$$

By Lemma 4.1.8 it follows that

$$\varphi^{-1}(L) = \bigcup_{u \in \varphi^{-1}(L)} U(u, 2^{-n}) = \bigcup_{u \in \varphi^{-1}(L)} \pi_n^{-1}(\pi_n(u)) = \pi_n^{-1}(\pi_n(\varphi^{-1}(L))).$$

That means, that $\phi^{-1}(L)$ is recognized by a finite monoid and therefore rational.

$\Leftarrow$ Now, we assume that for every rational language L of Γ^* it holds that $\varphi^{-1}(L)$ is also rational.
Let $\mathcal{L}_n$ be the finite set of the equivalence classes of $\sim_n$ in Γ^* for every $n \in \mathbb{N}$. Clearly, if for any $L \subseteq \Gamma^*$ it holds that $L \in \mathcal{L}_n$ it follows that L is recognized by a finite monoid, therefore rational and thus also $\varphi^{-1}(L)$. Let now $k(L)$ be the size of the syntactic monoid of $\varphi^{-1}(L)$ for any $L \in \mathcal{L}_n$ and $k = \max\{k(L) \mid L \in \mathcal{L}_n\}$. We now take arbitrary $u, v \in \Sigma^*$ such that $d(u, v) < 2^{-k}$. Since $\mathcal{L}_n$ is a partition of Γ^*, we have that $\{\varphi^{-1}(L) \mid L \in \mathcal{L}_n\}$ is a partition of Σ^*. Therefore, there is an $L \in \mathcal{L}_n$ such that $u \in \varphi^{-1}(L)$. Since $d(u, v) < 2^{-k}$ there exists no monoid with cardinality $\leq k$ that separates u and v. If $v \notin \varphi^{-1}(L)$, then $\varepsilon u \varepsilon \in \varphi^{-1}(L)$ and $\varepsilon v \varepsilon \notin \varphi^{-1}(L)$, which means that u and v are in different equivalence classes with regard to the syntactic congruence, which again would mean that the syntactic monoid with cardinality $\leq k$ separates u and v, which is a contradiction. Therefore, $v \in \varphi^{-1}(L)$. It follows that both $\varphi(u)$ and $\varphi(v)$ are in L and therefore $\varphi(u) \sim_n \varphi(v)$. Since the equivalence classes of $\sim_n$ are open balls with radius 2^{-n}, it follows that $d(x, y) < 2^{-k} \Rightarrow d(\varphi(x), \varphi(y)) < 2^{-n}$. Therefore, φ is uniformly continuous.

■

4.2 The free profinite monoid

Now, we will consider the completion of (Σ^*, d) and look at the properties.

Definition 4.2.1. $(\widehat{\Sigma^*}, \widehat{d})$ denotes the completion of (Σ^*, d). It is called the *free profinite monoid*.

Note, that the existence of such a completion is secured by Lemma 1.1.12. Furthermore, it is unique up to isomorphy. For the sake of readability (and writability) we will identify $x \in \Sigma^*$ with $\iota(x) \in \widehat{\Sigma^*}$ with ι being the isometric embedding of Σ^* in $\widehat{\Sigma^*}$. We now come to a very central lemma:

Lemma 4.2.2. *$(\widehat{\Sigma^*}, \widehat{d})$ is a topological monoid and compact.*

Proof. Lemma 1.1.22 states that every completion of a totally bounded topological space is compact, which is the case here.
For it to be a topological monoid, we simply need a binary operation on $\widehat{\Sigma^*}$ that is associative and continuous and a neutral element. Since $\Sigma^* \times \Sigma^*$ is dense in $\widehat{\Sigma^*} \times \widehat{\Sigma^*}$ and because the concatenation is uniformly continuous (cf. Lemma 4.1.10), we get that the concatenation of Σ^* can be extended to a uniformly continuous function on $\widehat{\Sigma^*} \times \widehat{\Sigma^*}$ by Corollary 1.1.28. Since the original concatenation is surjective and $\widehat{\Sigma} \times \widehat{\Sigma}$ is compact as the product of compact spaces (cf. Theorem 1.1.23), we have that the extension is also surjective. In order to clarify, when we use the original concatenation and when the extension in the next argument, we denote the concatenation with f and the extension with $\widehat{f}$ in prefix-form (e.g. $f(x, y) = xy$). To prove that $\widehat{f}$ is also associative, we now take $x, y, z \in \widehat{\Sigma^*}$. Since Σ^* is dense, we can find sequences $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}}, (z_n)_{n\in\mathbb{N}}$ in Σ^* with $\lim_{n\in\mathbb{N}} a_n = a$ for $a \in \{x, y, z\}$. Since $\widehat{f}$ is continuous and f is associative, we can do the following:

$$\begin{aligned}
(xy)z &= \widehat{f}(\widehat{f}(x, y), z) \\
&= \widehat{f}(\widehat{f}(\lim x_n, \lim y_n), \lim z_n) \\
&= \lim \widehat{f}(\widehat{f}(x_n, y_n), z_n) \\
&= \lim f(f(x_n, y_n), z_n) \\
&= \lim x_n(y_n z_n) \\
&= \lim f(x_n, f(y_n, z_n)) \\
&= \lim \widehat{f}(x_n, \widehat{f}(y_n, z_n)) \\
&= \widehat{f}(\lim x_n, \widehat{f}(\lim y_n, \lim z_n)) \\
&= x(yz)
\end{aligned}$$

Therefore, the extended concatenation is associative. Analogously, we get that ε stays the neutral element, which concludes the proof. ■

Another consequence of the density of Σ^* is the following:

Lemma 4.2.3. *Let φ be a homomorphism from Σ^* to the discrete finite monoid M. Then φ is uniformly continuous and can be extended in a unique way to a uniformly continuous homomorphism $\widehat{\varphi}$ from $\widehat{\Sigma^*}$ to M.*

Proof. Consider $u, v \in \Sigma^*$ such that $d(u, v) < 2^{-|M|}$. Then $r(u, v) > |M|$ and M and therefore φ does not separate u and v. Therefore $\varphi(u) = \varphi(v)$ and φ is uniformly continuous. Since Σ^* is dense, φ has a unique uniformly continuous extension $\widehat{\varphi}$ from $\widehat{\Sigma^*}$ to M. We need to show that $\widehat{\varphi}$ is a homomorphism. Let $D = \{(x, y) \in \widehat{\Sigma^*} \times \widehat{\Sigma^*} \mid \widehat{\varphi}(xy) = \widehat{\varphi}(x)\widehat{\varphi}(y)\}$. Clearly, $\Sigma^* \times \Sigma^* \subseteq D$. We also know that $\Sigma^* \times \Sigma^*$ is dense in $\widehat{\Sigma^*} \times \widehat{\Sigma^*}$ and therefore, we

only need to show that D is closed, to get that $D = \widehat{\Sigma^*} \times \widehat{\Sigma^*}$. Let f be the unique uniformly continuous extension of the concatenation on $\widehat{\Sigma^*} \times \widehat{\Sigma^*}$ and g the monoid operation on M. Since M is discrete, also $M \times M$ is discrete and therefore g is continuous (as every other function from $M \times M$ to M). We see that

$$\widehat{\varphi}(xy) = (\widehat{\varphi} \circ f)(x, y),\ \widehat{\varphi}(x)\widehat{\varphi}(y) = (g \circ (\widehat{\varphi} \times \widehat{\varphi}))(x, y).$$

Note that all the functions are compositions of continuous functions and therefore continuous themselves. Furthermore, we note that $\widehat{\varphi}(xy) = \widehat{\varphi}(x)\widehat{\varphi}(y) = m \Leftrightarrow (x, y) \in (\widehat{\varphi} \circ f)^{-1}(\{m\}) \cap (g \circ (\widehat{\varphi} \times \widehat{\varphi}))^{-1}(\{m\})$. Therefore, it holds that

$$D = \bigcup_{m \in M} (\widehat{\varphi} \circ f)^{-1}(\{m\}) \cap (f \circ \widehat{\varphi} \times \widehat{\varphi})^{-1}(\{m\}).$$

Since M is equipped with the discrete topology $\{m\}$ is closed for all $m \in M$ and because the functions are continuous, we have a finite union of closed subsets on the right side. Therefore, D is closed and we get, that $D = \widehat{\Sigma^*} \times \widehat{\Sigma^*}$. Thus, $\widehat{\varphi}$ is a homomorphism. ■

Note that the discrete topology can always be induced by the discrete metric d with $d(x, x) = 0$ and $d(x, y) = 1$ if $x \neq y$. Therefore, it makes sense to talk about uniform continuity in the theorem above.

4.3 ω-terms

Until now, it is unclear, whether $\widehat{\Sigma^*}$ is actually bigger than Σ^* or if Σ^* itself is complete. We now want to give an example of a word that is in $\widehat{\Sigma^*}$, but not in Σ^*. For this purpose, we formulate the following lemma:

Lemma 4.3.1. *The sequence $(x_n)_{n\in\mathbb{N}} := (x^{n!})_{n\in\mathbb{N}}$ is a Cauchy sequence in $\widehat{\Sigma^*}$ with regard to the metric $\widehat{d}$ for any $x \in \widehat{\Sigma^*}$. The limit $x^\omega := \lim_{n\in\mathbb{N}} x_n$ lies in $\widehat{\Sigma^*} \setminus \Sigma^*$ for any $x \in \Sigma^*$. x^ω is idempotent.*

Proof. To show that $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence, we take an arbitrary $\rho > 0$. Now we take $k \in \mathbb{N}$ such that $2^{-k} < \rho$. It suffices to show, that there exists an $N \in \mathbb{N}$ such that $d(x_i, x_j) \leq 2^{-k}$ for all $i, j \geq N$. We claim that $N = k$. Let us take $p, q \geq k$. Since, x is not necessarily in Σ^*, we have to approach the metric with a sequence. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence in Σ^* such that $\lim a_n = x$. Since the extension of the concatenation is continuous, we get that $x^{p!} = \lim a_n^{p!}$. Furthermore, the metric $\widehat{d}$ is also continuous, which means that $\widehat{d}(x_p, x_q) = \lim d(a_n^{p!}, a_n^{q!})$. Now we take $n \in \mathbb{N}$, an arbitrary monoid M of size $\leq k$ with a homomorphism $\varphi : \Sigma^* \to M$ and set $\varphi(a_n) = s$. By Lemma 2.1.1 s has an idempotent power $s^r = x$ with $r \leq k$. By choice of p and q, r divides $p!$ and $q!$, which means that $p! = rl, q! = rm$. Therefore,

$$\varphi(a_n^{p!}) = s^{p!} = (s^r)^l = x^l = x^m = (s^r)^m = s^{q!} = \varphi(a_n^{q!}).$$

Thus, $a_n^{p!}$ and $a_n^{q!}$ cannot be separated by a monoid of size $\leq k$, which translates to $d(a_n^{p!}, a_n^{q!}) < 2^{-k}$ for any $n \in \mathbb{N}$. With the limit, we get that $d(x_p, x_q) = \lim d(a_n^{p!}, a_n^{q!}) \leq 2^{-k}$,

which proves the claim.
With $(x_n)_{n\in\mathbb{N}}$ being a Cauchy sequence, it makes sense to define x^ω as its limit in $\widehat{\Sigma^*}$. It follows from the definition of the sequence that x^ω is not in Σ^* for any $x \in \Sigma^*$.
Two show the idempotence, we recall that $f(x, y) = xy$ is continuous on $\widehat{\Sigma^*} \times \widehat{\Sigma^*}$ and consider the following term:

$$x^\omega x^\omega = f(\lim x_n, \lim x_n) = \lim f(x_n, x_n) = \lim x^{n!}x^{n!} = \lim x^{2\cdot n!} =: \lim y_n.$$

Again, we take $\rho > 0$ and n such that $2^{-n} \leq \rho$. If we take any $p \geq n$, we see for the same reason as above that there is no finite monoid of size $\leq n$ that separates y_n and x_n. Therefore, $\lim d(x_n, y_n) = 0$, which means that $(y_n)_{n\in\mathbb{N}}$ is a Cauchy sequence and that $(x_n)_{n\in\mathbb{N}}$ and $(y_n)_{n\in\mathbb{N}}$ have the same limit. Therefore, $x^\omega = x^\omega x^\omega$. ■

We can now look at how to interpret x^ω.
Let M be a finite monoid with exponent ω as described in Definition 2.1.4, a homomorphism φ from Σ^* to M, $\widehat{\varphi}$ its extension on $\widehat{\Sigma^*}$, $x \in \Sigma^*$ and $s = \varphi(x)$. Then, it holds $s^{n!} = s^\omega$ for all $n \geq \omega$ with s^ω being the unique idempotent element in the set $\{s^l \mid l \in \mathbb{N}_{\geq 1}\}$ (cf. Lemma 2.1.1). Therefore, we get that

$$\widehat{\varphi}(x^\omega) = \widehat{\varphi}(\lim x^{n!}) = \lim \widehat{\varphi}(x^{n!}) = \lim \varphi(x^{n!}) = \lim s^{n!} = s^\omega = \varphi(x)^\omega.$$

Since x^ω is idempotent, we have that $(x^\omega)^{n!} = x^\omega$ for any $n \in \mathbb{N}$ and therefore $(x^\omega)^\omega = x^\omega$.
Two related concepts are the following profinite words:

$$x^{\omega-1} = \lim x^{n!-1} \text{ and } x^{\omega+1} = \lim x^{n!+1}$$

We can prove the existence of these limits in the same way we prove the existence of x^ω. If we recall that the concatenation on $\widehat{\Sigma^*}$ is continuous, we immediately see that

$$xx^\omega = x^\omega x = x^{\omega+1} \text{ and } xx^{\omega-1} = x^{\omega-1}x = x^\omega.$$

Furthermore, if we define M, ω, φ and $\widehat{\varphi}$ as above, it holds that $\widehat{\varphi}(x^{\omega+1}) = \varphi(x)^{\omega+1}$ because

$$\widehat{\varphi}(x^{\omega+1}) = \lim \varphi(x^{n!+1}) = \lim s^{n!}s = s^\omega s = s^{\omega+1} = \varphi(x)^{\omega+1}.$$

However, we cannot use this approch to interpret $x^{\omega-1}$ since s^{-1} is generally not defined in a monoid or semigroup. We can solve this, if we recall Lemma 2.1.7 and that the minimal ideal G of the subsemigroup generated by s is a group with the neutral element s^ω. Certainly, $s^{\omega+1} = ss^\omega$ is in G. Also, since $2\omega - 1 \geq 1$, we have that $s^{2\omega-1}$ is also in G and clearly the unique inverse of $s^{\omega+1}$. We also have that $s^{n!-1}$ is the inverse of $s^{\omega+1}$ and clearly in G as a product of s for all $n \geq 2$. Therefore, $s^{n!-1} = s^{2\omega-1}$ for all $n \geq 2$, which means that $\lim s^{n!-1} = s^{2\omega-1}$. Finally, we get that

$$\widehat{\varphi}(x^{\omega-1}) = \lim \varphi(x^{n!-1}) = \lim s^{n!-1} = s^{2\omega-1} = \varphi(x)^{2\omega-1}.$$

Now, we can make an important definition:

Definition 4.3.2. The *ω-terms* are the smallest submonoid of $\widehat{\Sigma^*}$ that contains Σ^* and is

closed under $x \mapsto x^{\omega}, x \mapsto x^{\omega-1}, x \mapsto x^{\omega+1}$.

One can show that the ω-terms are countable, while the whole free profinite monoid is uncountable.

5 Varieties of finite monoids and profinite identites

In this chapter, we will prove the main theorem of this thesis. Theorem 5.3.5 characterises the connection between profinite words and the varieties of finite monoids. With Theorem 3.2.10, we can also infer the connection between profinite words and varieties of rational languages. This chapter closely follows [3, Chapter XI].

5.1 Free pro-$\mathcal{V}$ monoids

The goal of this section is to introduce the free pro-$\mathcal{V}$ monoid, which is a similar notion to the free profinite monoid. For this purpose, let $\mathcal{V}$ be a variety of monoids as defined in 3.1.1 and Σ^* an alphabet for the rest of this section.

Definition 5.1.1. Let u, v be words in Σ^*. We define

$$r_{\mathcal{V}} = \min\{|M| \mid M \in \mathcal{V} \text{ and } M \text{ separates } u \text{ and } v\} \text{ and } d_{\mathcal{V}}(u,v) = 2^{-r_{\mathcal{V}}(u,v)},$$

with the convention that $\min \emptyset = +\infty$ and $2^{-\infty} = 0$.

From the definition, it is clear that $d_{\mathcal{V}}$ should have some properties similar to the ones of d:

Lemma 5.1.2. *For every $u, v, w \in \Sigma^*$ it holds that:*

(i) $d_{\mathcal{V}}(u,v) = d_{\mathcal{V}}(v,u)$

(ii) $d_{\mathcal{V}}(uw, vw) \leq d_{\mathcal{V}}(u,v)$ *and* $d_{\mathcal{V}}(wu, wv) \leq d_{\mathcal{V}}(u,v)$

(iii) $d_{\mathcal{V}}(u,w) \leq \max\{d_{\mathcal{V}}(u,v), d_{\mathcal{V}}(v,w)\}$

Proof.

(i) This property is trivial

(ii) If $M \in \mathcal{V}$ separates uw and vw, it clearly separates u and v. Therefore, $d_V(uw, vw) \leq d_V(u,v)$. Analogously, we get that $d_{\mathcal{V}}(wu, wv) \leq d(u,v)$.

(iii) If $M \in \mathcal{V}$ separates u and w it certainly separates either u and v or v and w. Thus, $\min\{r_{\mathcal{V}}(u,v), r_{\mathcal{V}}(v,w)\} \leq r_{\mathcal{V}}(u,w)$ and $\max\{d_{\mathcal{V}}(u,v), d_{\mathcal{V}}(v,w)\} \geq d_{\mathcal{V}}(u,w)$.

■

We see that $d_{\mathcal{V}}(u,v) = 0$ does not necessarily imply that $u = v$.

Example 5.1.3. Consider the class $\mathcal{C}$ of all commutative finite monoids. That is the class of all the monoids M that fulfill that for all a, b in M it holds that $ab = ba$. It is trivial that this class is also a variety. Now consider the alphabet $\{a, b\}$. By choice of the variety have that ab and ba cannot be separated by any monoid of $\mathcal{C}$ and therefore $d_{\mathcal{C}}(ab, ba) = 0$.

However, we can look at the following relation:

Definition 5.1.4. Let $\sim_{\mathcal{V}}$ be the relation on Σ^* defined by

$$x \sim_{\mathcal{V}} y \Leftrightarrow d_{\mathcal{V}}(x, y) = 0$$

Lemma 5.1.5. *The relation $\sim_{\mathcal{V}}$ is a congruence.*

Proof. Clearly, $\sim_{\mathcal{V}}$ is reflexive and symmetric. By Lemma 5.1.2 (*iii*) we also get the transitivity. Therefore, $\sim_{\mathcal{V}}$ is an equivalence relation. Take $a, b, x, y \in \Sigma^*$ such that $a \sim_{\mathcal{V}} x$ and $b \sim_{\mathcal{V}} c$. Now let us take any monoid M in $\mathcal{V}$ and a homomorphism $\varphi : \Sigma^* \to M$. By the choice of a, b, x and y, it holds that $\varphi(a) = \varphi(x)$ and $\varphi(b) = \varphi(y)$. Therefore, $\varphi(ab) = \varphi(xy)$. Since M and φ were arbitrary, we get that $d_{\mathcal{V}}(ab, xy) = 0$ and $ab \sim_{\mathcal{V}} xy$. Thus, $\sim_{\mathcal{V}}$ is a congruence. ■

We can now look at the monoid $\Sigma^*_{/\sim_{\mathcal{V}}}$. We can define $d_{\mathcal{V}}$ in a natural way on $\Sigma^*_{/\sim_{\mathcal{V}}}$ by setting $d_{\mathcal{V}}([x], [y]) = d_{\mathcal{V}}(x, y)$. Let us take a, b, x, y in Σ^* such that $a \sim_{\mathcal{V}} x$ and $b \sim_{\mathcal{V}} y$. Then

$$\begin{aligned} d_{\mathcal{V}}([a], [b]) = d_{\mathcal{V}}(a, b) &\leq \max\{d_{\mathcal{V}}(a, x), d_{\mathcal{V}}(x, b)\} = d_{\mathcal{V}}(x, b) \leq \max\{d_{\mathcal{V}}(x, y), d_{\mathcal{V}}(y, b)\} \\ &= d_{\mathcal{V}}(x, y) = d_{\mathcal{V}}([x], [y]). \end{aligned}$$

Analogously, we get that $d_{\mathcal{V}}([x], [y]) \leq d_{\mathcal{V}}([a], [b])$. Therefore, $d_{\mathcal{V}}([a], [b]) = d_{\mathcal{V}}([x], [y])$ and our function is well defined. Because of the natural definition it makes sense to call it the same as the original function. Although Σ^* is something different than $\Sigma^*_{/\sim_{\mathcal{V}}}$, I will identify the equivalence classes of $\Sigma^*_{/\sim_{\mathcal{V}}}$ with words from Σ^*, to make the text more readable.

Lemma 5.1.6.

(i) d_v is an ultra-metric on $\Sigma^*_{/\sim_{\mathcal{V}}}$

(ii) The concatenation is a uniformly contiuous function from $\Sigma^*_{/\sim_{\mathcal{V}}} \times \Sigma^*_{/\sim_{\mathcal{V}}}$ to $\Sigma^*_{/\sim_{\mathcal{V}}}$ if $\Sigma^*_{/\sim_{\mathcal{V}}}$ is equipped with $d_{\mathcal{V}}$ and $\Sigma^*_{/\sim_{\mathcal{V}}} \times \Sigma^*_{/\sim_{\mathcal{V}}}$ is equipped with the associated maximum-metric.

Proof. (i) We have that $d_{\mathcal{V}}(u, v) = 0 \Leftrightarrow u \sim_{\mathcal{V}} v$. The other required properties are inherited from $d_{\mathcal{V}}$ on $\Sigma^* \times \Sigma^*$.

(ii) Let a, b, x, y be in $\Sigma^*_{/\sim_{\mathcal{V}}}$. Then, it follows directly from Lemma 5.1.2 that

$$d_{\mathcal{V}}(ab, xy) \leq \max\{d_{\mathcal{V}}(ab, ay), d_{\mathcal{V}}(ay, xy)\} \leq \max\{d_{\mathcal{V}}(b, y), d_{\mathcal{V}}(a, x)\} = d_{\mathcal{V}}((a, x), (b, y))$$

■

We can now again look at the completion of $\Sigma^*_{/\sim_\mathcal{V}}$.

Definition 5.1.7. The monoid $(\widehat{F}_\mathcal{V}(\Sigma), \widehat{d}_\mathcal{V})$ denotes the completion of $(\Sigma^*_{/\sim_\mathcal{V}}, d_\mathcal{V})$ and is called the *free pro-$\mathcal{V}$ monoid*.

Lemma 5.1.8. *$\widehat{F}_\mathcal{V}(\Sigma)$ is in fact a topological monoid.*

Proof. The proof is exactly the same as the one from Lemma 4.2.2. ■

In the following, let $\pi_\mathcal{V}$ be the natural homomorphism from Σ^* to $\Sigma^*_{/\sim_\mathcal{V}}$. We will now show some central properties of $\widehat{F}_\mathcal{V}(\Sigma)$.

Lemma 5.1.9. *Let φ be a homomorphism from $\Sigma_{/\sim_\mathcal{V}}$ to a discrete monoid $M \in \mathcal{V}$. Then φ is uniformly continuous and can be extended in a unique way to a uniformly continuous homomorphism from $\widehat{F}_\mathcal{V}(\Sigma)$ to M.*

Proof. The proof is exactly the same as the proof of Lemma 4.2.3. ■

Lemma 5.1.10. *For each finite alphabet Σ, the following properties hold:*

(i) The monoid $\widehat{F}_\mathcal{V}(\Sigma)$ is compact.

(ii) There is a unique surjective uniformly continuous homomorphism from $(\widehat{\Sigma^*}, \widehat{d})$ to $(\widehat{F}_\mathcal{V}(\Sigma), \widehat{d}_\mathcal{V})$ that extends $\pi_\mathcal{V}$

Proof.

(i) By Lemma 1.1.22 and since $\widehat{F}_\mathcal{V}(\Sigma)$ is complete, we only need to show that $\Sigma^*_{/\sim_\mathcal{V}}$ is totally bounded. Consider the congruence $\sim_n$ on Σ^* defined by

$$x \sim_n y \Leftrightarrow x \text{ and } y \text{ are not separated by any monoid in } \mathcal{V} \text{ of size} \leq n.$$

First, we establish that $\sim_n$ is well defined. To realize that, take $x, y, a, b \in \Sigma^*$ such that $a \sim_\mathcal{V} x$ and $b \sim_\mathcal{V} y$. That means that $\varphi(a) = \varphi(x)$ and $\varphi(b) = \varphi(y)$ for any homomorphism φ onto any monoid of $\mathcal{V}$. That means, that a monoid M separates a and x iff it separates b and y. Therefore, the relation is well defined.
Furthermore, we see that $\sim_n$ is an equivalence relation as it is clearly reflexive, symmetri and transitive. Now, let $x, y, a, b \in \Sigma^*_{/\sim_\mathcal{V}}$ such that $a \sim_n x$ and $b \sim_n y$, $M \in \mathcal{V}$ with size $\leq n$ and φ a homomorphism from $\Sigma^*_{/\sim_\mathcal{V}}$ to M. By choice of a, b, x, y, it holds that $\varphi(a) = \varphi(x)$ and $\varphi(b) = \varphi(y)$ and therefore $\varphi(ab) = \varphi(xy)$. Since M and φ were arbitrary, we see that $ab \sim_n xy$. Therefore, $\sim_n$ is even a congruence.
We now claim that the index of $\sim_n$ is finite for the same reasons as in the proof of Lemma 4.1.8. First of all, we only have finitely many monoids of size $\leq n$ (up to isomorphy). Secondly, we only have finitely many homomorphisms from $\Sigma^*_{/\sim_\mathcal{V}}$ to a monoid of size $\leq n$ because Σ is finite. That means that the set $\mathcal{M}$ of homomorphisms from $\Sigma^*_{/\sim_\mathcal{V}}$ to monoids of size $\leq n$ is finite if we only consider monoids that are not isomorphic. Therefore, for each $x \in \Sigma^*_{/\sim_\mathcal{V}}$ there are only finitely many possible values for $(\varphi(x))_{\varphi \in \mathcal{M}}$ and thus only finitely many equivalence classes of $\sim_n$, which proves

the claim.
Now consider $x, y \in \Sigma^*/_{\sim_\mathcal{V}}$. Per definition $x \sim_n y$ iff x and y cannot be separated by a monoid of size $\leq n$ in $\mathcal{V}$. That is exactly the case if $r_\mathcal{V}(x, y) > n$ or equivalently $d_\mathcal{V}(x, y) < 2^{-n}$. It follows that the equivalence classes of $\sim_n$ are open balls of radius 2^{-n} and cover $\Sigma^*/_{\sim_\mathcal{V}}$ completely. Therefore, $\Sigma^*/_{\sim_\mathcal{V}}$ is totally bounded and $\widehat{F}(\Sigma)$ is compact.

(ii) It follows from the definition of $d_\mathcal{V}$ that $d_\mathcal{V}(x, y) \leq d(x, y)$. Therefore, $\pi_\mathcal{V}$ is uniformly continuous and since $\widehat{\Sigma^*}$ is compact, Corollary 1.1.28 states that $\pi_\mathcal{V}$ can be extended to a unique, uniformly continuous and surjective function from $\widehat{\Sigma^*}$ to $\widehat{F}_\mathcal{V}(\Sigma)$. By approaching elements of $\widehat{\Sigma^*}$ with sequences, we also get that this extension is a homomorphism.

■

Lemma 5.1.11. *For each function φ from Σ to a monoid $M \in \mathcal{V}$ (equipped with the discrete topology), there is a unique uniformly continuous homomorphism $\psi : \widehat{F}_\mathcal{V}(\Sigma) \to M$ such that for all $x \in \Sigma$ it holds that $\varphi(x) = \psi(\pi_\mathcal{V}(x))$.*

Proof. Let φ be function from Σ to $M \in \mathcal{V}$. This function can clearly be extended to a unique homomorphism φ' from Σ^* to M. By Lemma 4.2.3 φ' is uniformly continuous and there is a unique uniformly continuous extension φ'' from $\widehat{\Sigma^*}$ to M. Since $\mathcal{V}$ is a variety, $\varphi''(\widehat{\Sigma^*}) \preccurlyeq M$ is also in $\mathcal{V}$. Therefore, we can assume without loss of generality that φ'' is surjective. We know, that Σ^* is dense and $\varphi''(\Sigma^*)$ is closed because M is discrete. Let now m be in M such that $m = \varphi''(x)$ with $x \in \widehat{\Sigma^*}$ and $x = \lim x_n$ with $x_n \in \Sigma^*$ for all $n \in \mathbb{N}$. Since φ'' is continuous, we can write $m = \varphi''(x) = \varphi''(\lim x_n) = \lim \varphi''(x_n)$ as the limit of a sequence in $\varphi''(\Sigma^*)$. Therefore, $m \in \varphi''(\Sigma^*) = \varphi'(\Sigma^*)$ and we get that φ' is already surjective. Furthermore, we have that $x \sim_\mathcal{V} y$ implies that $\varphi'(x) = \varphi'(y)$ and we can define $\psi : \Sigma^*/_{\sim_\mathcal{V}} \to M$ with $\psi([u]) = \varphi'(u)$, which is obviously well defined and a homomorphism. We see that $\varphi' = \psi \circ \pi_\mathcal{V}$. We now claim that ψ uniformly continuous. To prove this claim, we set $n = |M|$ and consider $x, y \in \Sigma^*/_{\sim_\mathcal{V}}$ with $d_\mathcal{V}(x, y) < 2^{-n}$. We see that x and y cannot be separated by M and therefore $\psi(x) = \psi(y)$, which proves the claim. We can now extend ψ to a uniformly continuous homomorphism from $\widehat{F}_\mathcal{V}(\Sigma)$ to M because of Lemma 5.1.9. Clearly, it still holds for all $a \in \Sigma$ that $\psi(\pi_\mathcal{V}(a)) = \phi(x)$. ■

Lemma 5.1.12. *A finite Σ-generated monoid belongs to $\mathcal{V}$ iff it is a continuous quotient of $\widehat{F}_\mathcal{V}(\Sigma)$*

Proof.

⇒ Let $M \in \mathcal{V}$ be Σ-generated with size $\leq n$. Then we can extend the function $f : \Sigma \to M : a \mapsto a$ to a homomorphism φ from Σ^* to M. Note, that φ is surjective because M is Σ-generated. Now, define $\psi : \Sigma^*/_{\sim_n} \to M : [x] \mapsto \varphi(x)$. Again, this is function is clearly well defined because $u \sim_n v$ implies that M does not separate u and v and therefore $\varphi(u) = \varphi(v)$. Also, ψ inherits the necessary properties of φ to be a homomorphism. Furthermore, ψ is surjective as well. By Lemma 5.1.9 we get that there is a uniformly continuous extension of ψ from $\widehat{F}_\mathcal{V}(\Sigma)$ to M, which is clearly also surjective. Therefore, M is a continuous quotient of $\widehat{F}_\mathcal{V}(\Sigma)$.

$\Leftarrow$ Let M be a continuous quotient of $\widehat{F}_{\mathcal{V}}(\Sigma)$ and π the surjective homomorphism from $\widehat{F}_{\mathcal{V}}(\Sigma)$ to M. We define

$$D = \{(x, y) \in \widehat{F}_{\mathcal{V}}(\Sigma) \times \widehat{F}_{\mathcal{V}}(\Sigma) \mid \pi(x) = \pi(y)\},$$

which is inverse image of the diagonal of $M \times M$ under $\pi \times \pi$ (i.e. $(\pi \times \pi)^{-1}(\{(x, x) \mid x \in M\})$. We note that $\pi \times \pi$ is continuous because it is continuous in every component and since $M \times M$ is discrete because M is, we get that $\{(x, x) \mid x \in M\}$ is clopen. Therefore D is also clopen. Let $\mathcal{M}$ be the class of all homomorphisms from $\widehat{F}_{\mathcal{V}}(\Sigma)$ to a monoid of $\mathcal{V}$. For each $\phi \in \mathcal{M}$, we define

$$C_\varphi = \{(x, y) \in \widehat{F}_{\mathcal{V}}(\Sigma) \times \widehat{F}_{\mathcal{V}}(\Sigma) \mid \varphi(x) \neq \varphi(y)\}.$$

We note that C_φ is clopen because every φ is continuous and C_φ is inverse image of $M \times M \setminus \{(x, x) \mid x \in M\}$, which again is clopen because $M \times M$ is discrete. Furthermore, we see that if (x, y) is not in any C_φ, it certainly holds that $\pi(x) = \pi(y)$ and therefore $(x, y) \in D$. In total, this gives us that

$$\widehat{F}_{\mathcal{V}}(\Sigma) \times \widehat{F}_{\mathcal{V}}(\Sigma) = D \cup \bigcup_{\varphi \in \mathcal{M}} C_\varphi.$$

Since $\widehat{F}_{\mathcal{V}}(\Sigma) \times \widehat{F}_{\mathcal{V}}(\Sigma)$ is compact and all of the C_φ are open as is D, we get that there is a finite set $\mathcal{F} \subset \mathcal{M}$ such that

$$\widehat{F}_{\mathcal{V}}(\Sigma) \times \widehat{F}_{\mathcal{V}}(\Sigma) = D \cup \bigcup_{\varphi \in \mathcal{F}} C_\varphi.$$

Let us now consider the finite monoid $L = \prod_{\varphi \in \mathcal{F}} \varphi(\widehat{F}_{\mathcal{V}}(\Sigma))$. Every one of the $\varphi\widehat{F}_{\mathcal{V}}(\Sigma)$ is by definition of $\mathcal{M}$ a submonoid of some monoid $N \in \mathcal{V}$ and therefore in $\mathcal{V}$. Thus, L is in $\mathcal{V}$. Now look a the set $N := \{(\varphi(x))_{\varphi \in \mathcal{F}} \mid x \in \widehat{F}_{\mathcal{V}}(\Sigma)\}$. This set is clearly a submonoid of L and therefore in $\mathcal{V}$. We now see that for $x, y \in \widehat{F}_{\mathcal{V}}(\Sigma)$, it holds $\varphi(x) = \varphi(y)$ for all $\varphi \in \mathcal{F}$ implies $\pi(x) = \pi(y)$ since (x, y) is in none of the C_φ. That means that the function

$$\psi : L \to M : (\varphi(x))_{\varphi \in \mathcal{F}} \mapsto \pi(x)$$

is well defined and clearly a homomorphism. Also ψ is surjective because π is. It follows that M is a quotient of a monoid in $\mathcal{V}$ and therefore also in $\mathcal{V}$.

■

The next goal is to describe the structure of a variety $\widehat{F}\mathcal{V}$. In general, this is rather difficult, but let us assume that $\mathcal{V}$ is generated by a single monoid M. Let M^Σ be the set of all functions from Σ to M. All of these functions γ can be extended to a unique homomorphism $\widehat{\gamma}$ from Σ^* to M. Now let M^{M^Σ} be the set of all functions from M^Σ to M. Clearly, this set forms a monoid if equipped with the pointwise multiplication as the binary operation and the neutral element $f : \mathcal{M}^\Sigma \to M : \varphi \mapsto e$ with e being the neutral

element of M. Let us now define[1]

$$\varphi : \Sigma \to M^{M^\Sigma} : a \mapsto (\gamma \mapsto \gamma(a)).$$

We can now extend φ to a homomorphism ψ from Σ^* onto M^{M^Σ}. Now, consider any $x = a_1 a_2 \cdots a_n \in \Sigma^*$ with $a_i \in \Sigma$. For any $\gamma \in M^\Sigma$ it holds that $\psi(x)(\gamma) = \widehat{\gamma}(x)$ because

$$\psi(x)(\gamma) = \psi(a_1 \cdots a_n)(\gamma) = \psi(a_1)(\gamma) \cdots \psi(a_n)(\gamma) = \gamma(a_1) \cdots \gamma(a_n) = \widehat{\gamma}(a_1 \cdots a_n) = \widehat{\gamma}(x).$$

We define

$$F = \psi(\Sigma^*), \tag{5.1}$$

which is clearly a submonoid of M^{M^Σ}. We can even prove the following property:

Lemma 5.1.13. *If $\mathcal{V}$ is generated by a single monoid M, then $\widehat{F}_\mathcal{V}(\Sigma)$ is isomorphic to F as defined in (5.1) Therefore, $\widehat{F}_\mathcal{V}(\Sigma)$ is isomorphic to a submonoid of M^{M^Σ} and thus finite.*

Proof. Let again φ be the function from Σ to M with M^{M^Σ} with $\varphi(x) = (\gamma \mapsto \gamma(x))$ and ψ its homomorphic extension on Σ^*. Let us consider the function $\pi : \Sigma^*/_{\sim_n} \to F : [u] \mapsto \psi(u)$. First, let us show that this function is well defined. Let u, v be in $\Sigma^*/_{\sim_n}$ such that $u \sim_n v$. This means that for all monoids $N \in \mathcal{V}$ and homomorphisms $\gamma : \Sigma^* \to N$ it holds that $\gamma(u) = \gamma(v)$. Now let γ be any function from Σ to M. This function can be extended to a unique $\widehat{\gamma}$ homomorphism from Σ^* to M and since $M \in \mathcal{V}$ and $u \sim_\mathcal{V} v$, it holds that $\psi(u)(\gamma) = \widehat{\gamma}(u) = \widehat{\gamma}(v) = \psi(v)(\gamma)$. Since γ was arbitrary, we get that $\psi(u) = \psi(v)$. Therefore, π is well defined.
We also note, that π is a homomorphism because ψ is. Furthermore, π is clearly surjective. We claim, that π is injective. To prove this, we consider $u, v \in \Sigma^*$ such that $\psi(u) = \psi(v)$. Let us now take a monoid $N \in \mathcal{V}$ and a homomorphism $\zeta : \Sigma^* \to N$. Since $N \in \mathcal{V}$ and $\mathcal{V}$ is generated by M, we have that N is a quotient of a submonoid of a power of M. Therefore, there is an $n \in \mathbb{N}$, a submonoid T of M^n and a surjective homomorphism $\xi : T \to N$. By Lemma 2.2.10, there exists a homomorphism $\alpha : \Sigma^* \to T$ such that $\zeta = \xi \circ \alpha$. For all $i \leq n$, we define $\alpha_i = \pi_i \circ \alpha$ with $\pi_i : M^N \to M$ being the $i-th$ projection. Obviously, $\alpha(u) = (\alpha_i(x))_{i=1}^n$. Moreover, we see that α_i is a homomorphism from Σ^* to M for all i and that α_i implies a unique function β_i from Σ to M. Since $\psi(u) = \psi(v)$, we have that $\alpha_i(u) = \psi(u)(\beta_i) = \psi(v)(\beta_i) = \alpha_i(v)$ and therefore $\alpha(u) = \alpha(v)$. Thus, we get that $\zeta(u) = \zeta(v)$ because $\zeta = \xi \circ \alpha$. Since ζ and N were arbitrary, we get that u and v cannot be separated by any monoid in $\mathcal{V}$ and thus $u \sim_\mathcal{V} v$, which proves the claim.
We now have the situation that of Theorem 1.1.27 because π^{-1} is clearly uniformly continuous since F is equipped with the discrete metric. Therefore, there exists a unique bijective, uniformly continuous extension $\widehat{\pi}$ of π on $\widehat{F}_\mathcal{V}(\Sigma)$. By Lemma 5.1.9 this extension is also a homomorphism. Therefore, $\widehat{F}_\mathcal{V}(\Sigma)$ is isomorphic to F. ■

If $\widehat{F}_\mathcal{V}(\Sigma)$ is finite for every Σ, we call $\mathcal{V}$ *locally finite*. Clearly, every variety that is generated by a single monoid is locally finite, however the converse is generally not true.

[1] This concept is very similar to the evaluation functional known from functional analysis.

5.2 Identites

Definition 5.2.1. Let Σ be an alphabet, u, v in $\widehat{\Sigma^*}$ and M a monoid. *M satisfies the profinite identity $u = v$* if for every homomorphism $\varphi : \Sigma^* \to M$ and its extension $\widehat{\varphi} : \widehat{\Sigma^*} \to M$ it holds that $\widehat{\varphi}(u) = \widehat{\varphi}(v)$. If u and v are words, we call $u = v$ an *explicit identity.*

Note, that we could speak of the homomorphisms from $\widehat{\Sigma^*}$ to M directly because they each induce a unique homomorphism from Σ^* to M. As stated in the definition above a profinite identity is actually a pair of profinite words. However, if we have an explicit identity, we can think of it in terms of elements of a monoid. Consider the following example:

Example 5.2.2. Given the explicit identity $ab = ba$ with $a, b \in \Sigma$, we can look at the monoids fulfilling it in two ways. One way is the definition, that M fulfills the identity if for every homomorphism φ it holds that $\varphi(ab) = \varphi(ba)$. Note, that we don't have to consider the extension of φ since ab and ba are words. Since we can choose $\varphi(a)$ and $\varphi(b)$ freely, we have that M fulfills that for every $x, y \in M$ it holds that $xy = yx$. Furthermore, if this property holds for all $x, y \in M$, it clearly follows that $\varphi(ab) = \varphi(ba)$ for every homomorphism φ. Therefore, we can simply consider a and b to be elements of the monoid M and do not have to rename them to x and y.

We can also use this approach to interpret identities containing ω-terms:

Example 5.2.3. Consider the profinite identity $x^\omega y^\omega = y^\omega x^\omega$ with letters x and y. We claim that this identity is equivalent to the demand that for all idempotent elements a, b of M it holds that $ab = ba$. We have shown that under every homomorphism ψ from $\widehat{\Sigma^*}$ to M it holds that $\psi(x^\omega) = \psi(x)^\omega$ (with ω being the exponent of M) is idempotent. Therefore, the implication that M satisfies the identity if all the idempotents of M commute is trivial. On the other hand, assume that M satisfies the identity and let a, b be two idempotent elements of M. Now consider the homomorphism ψ that fulfills $x \mapsto a$ and $y \mapsto b$. This is possible because x and y are letters. Now, a and b have to commute in M, which proves the claim.

One important property of identities is the following:

Lemma 5.2.4. *Let u and v be profinite words in $\widehat{\Sigma^*}$ and M a monoid that satisfies the identity $u = v$. Then for all $x, y \in \widehat{\Sigma^*}$ it holds that M satisfies the identity $xuy = xvy$. Furthermore, for every alphabet Γ and homomorphism $\varphi : \Sigma^* \to \Gamma^*$ with extension $\widehat{\varphi}$ it holds that M satisfies the identity $\widehat{\varphi}(u) = \widehat{\varphi}(v)$.*

Proof. Let φ be any homomorphism from Σ^* to M and $\widehat{\varphi}$ its extension from $\widehat{\Sigma}$ to M. Since M fulfills the identity $u = v$, it clearly holds that $\widehat{\varphi}(xuy) = \widehat{\varphi}(x)\widehat{\varphi}(u)\widehat{\varphi}(y) = \widehat{\varphi}(x)\widehat{\varphi}(v)\widehat{\varphi}(y) = \widehat{\varphi}(xvy)$. Therefore, M satisfies the identity $xuy = xvy$.
Let ζ be a homomorphism from Σ^* to Γ^* with extension $\widehat{\zeta}$ and φ a homomorphism from Γ^* to M with extension $\widehat{\varphi}$. Then, it holds that $\varphi \circ \zeta$ is a homomorphism from Σ^* to M with extension χ. Furthermore, we see that $\widehat{\varphi} \circ \widehat{\zeta}$ extends $\varphi \circ \zeta$ and because this extension is unique, we have that $\widehat{\varphi} \circ \widehat{\zeta} = \chi$. Because M satisfies the original identity, we have that $\widehat{\varphi}(\widehat{\zeta}(u)) = \chi(u) = \chi(v) = \widehat{\varphi}(\widehat{\zeta}(v))$ and therefore that M satisfies the identity $\widehat{\zeta}(u) = \widehat{\zeta}(v)$. ■

5.3 Reiterman's theorem

We now come to the most important result of this thesis: Theorem 5.3.5. It shows the connection between varieties of monoids and profinite identities. Before we get to the theorem, we should agree on important notation:

Definition 5.3.1. Let E be a set of profinite identities. Then $[E]$ denotes the class of finite monoids that satisfy E.

This leads directly to this important lemma:

Lemma 5.3.2. *Let E be a set of profinite identities. Then $[E]$ is a variety of monoids.*

Proof. We know from Lemma 3.1.2 that varieties of monoids are closed under intersection. Therefore, it suffices to consider the case, where $E = \{u = v\}$. Now let us show, that $[E]$ is a variety.

(i) Let M be a monoid that satisfies $u = v$. Then clearly, every submonoid N of M satifies the identity and $N \in [E]$

(ii) Let M be in $[E]$ and N a quotient of M. That means, there is a surjective homomorphism π from M to N. Now take any homomorphism φ from Σ^* to N with extension $\widehat{\varphi}$. By Lemma 2.2.10 there exists a homomorphism $\gamma : \Sigma^* \to M$ such that $\varphi = \pi \circ \gamma$. Since M satisfies the identity, we have that $\widehat{\gamma}(u) = \widehat{\gamma}(v)$ and therefore $\pi(\widehat{\gamma}(u)) = \pi(\widehat{\gamma}(v))$. Moreover, we have that $\pi \circ \widehat{\gamma}$ extends φ. But since this extension is unique, we have that $\widehat{\varphi} = \pi \circ \widehat{\gamma}$ and therefore N satisfies the identity.

(iii) Let $(M_i)_{i \in I}$ be a finite family of monoids that satisfy the identity and define $M = \prod_{i \in I} M_i$. Now take any homomorphism from Σ^* to M and consider the homomorphisms $\pi_i \circ \varphi$ from Σ^* to M_i with π_i being the projection from M onto M_i. Since $\pi_i \circ \varphi$ is a homomorphism from Σ^* to M_i and because $\pi_i \circ \widehat{\varphi}$ is the unique extension of $\pi_i \circ \varphi$, we have that $\pi_i(\widehat{\varphi}(u)) = \pi_i(\widehat{\varphi}(v))$ for every $i \in I$. Therefore, $\widehat{\varphi}(u) = \widehat{\varphi}(v)$ and M fulfills the identity.

■

Definition 5.3.3. We say a variety of monoids $\mathcal{V}$ satisfies an identity if all the monoids of $\mathcal{V}$ satisfy the identity. In this case, we say the identity is an identity of $\mathcal{V}$.

Lemma 5.3.4. *Let Σ be a finite alphabet and u, v two profinite words of $\widehat{\Sigma^*}$. Then a variety $\mathcal{V}$ satisfies the identity $u = v$ iff $\widehat{\pi}_{\mathcal{V}}(u) = \widehat{\pi}_{\mathcal{V}}(v)$ with $\widehat{\pi}_{\mathcal{V}}$ being the extension of π_V.*

Proof.

⇒ If $\mathcal{V}$ satisfies $u = v$, then u and v cannot be separated by any monoid of $\mathcal{V}$. Unfortunately, u and v are not words and we have to approach this problem via sequences. Let $(u_n)_{n \in \mathbb{N}}$ and $(v_n)_{n \in \mathbb{N}}$ be sequences in Σ^* such that $\lim u_n = u$ and $\lim v_n = v$. Since $\mathcal{V}$ satisfies the identity, we have that for every $M \in \mathcal{V}$ and every homomorphism $\varphi : \Sigma^* \to M$ it holds that $\widehat{\varphi}(u) = \widehat{\varphi}(v)$. Note that φ and $\widehat{\varphi}$ are continuous

and therefore $\lim \varphi(u_n) = \widehat{\varphi}(u) = \widehat{\varphi}(v) = \lim \varphi(v)$. Since M is discrete, this can only be the case if there is an $N_\varphi \in \mathbb{N}$ such that $\varphi(u_n) = \varphi(v_n)$ for all $n \geq N_\varphi$. If we now take any $n \in \mathbb{N}$ and consider $\mathcal{M}$ as the class of all homomorphisms from Σ^* to any $M \in \mathcal{V}$ with size $\leq n$. Note, that this class is a finite set, if we only consider the monoids that are not isomorphic. Now define $N = \max\{N_\varphi \mid \varphi \in \mathcal{M}\} < +\infty$. By choice of N it follows that $\varphi(u_k) = \varphi(v_k)$ for all $\varphi \in \mathcal{M}, k \geq N$ and therefore $d_\mathcal{V}(u_k, v_k) < 2^{-n}$ for all $k \geq N$. That means that $\lim d_\mathcal{V}(u_n, v_n) = 0$. Now consider the sequences $\pi_\mathcal{V}(u_n)$ and $\pi_\mathcal{V}(v_n)$. Per definition, it holds for all $n \in \mathbb{N}$ that $d_\mathcal{V}(\pi_\mathcal{V}(u_n), \pi_\mathcal{V}(v_n)) = d_\mathcal{V}(u_n, v_n)$. Therefore, $\lim d_\mathcal{V}(\pi_\mathcal{V}(u_n), \pi_\mathcal{V}(v_n)) = 0$ and thus, we get by Lemma 1.1.5 that $\widehat{\pi}_\mathcal{V}(u) = \lim \pi_\mathcal{V}(u_n) = \lim \pi_\mathcal{V}(v_n) = \widehat{\pi}(v)$.

$\Leftarrow$ Now let $\widehat{\pi}_\mathcal{V}(u) = \widehat{\pi}_\mathcal{V}(v)$. This means, that u and v can be approached with sequences $(u_n)_{n\in\mathbb{N}}$ and $(v_n)_{n\in\mathbb{N}}$ such that $\lim \pi_\mathcal{V}(u_n) = \lim \pi_\mathcal{V}(v_n)$ and therefore $\lim d_\mathcal{V}(u_n, v_n) = \lim d_\mathcal{V}(\pi_\mathcal{V}(u_n), \pi_\mathcal{V}(v_n)) = 0$. Thus, for every $k \in \mathbb{N}$ there exists an $N \in \mathbb{N}$ such that u_n and v_n cannot be separated by a monoid in $\mathcal{V}$ with size $\leq k$ for all $n \geq N$. Therefore, for any homomorphism $\varphi : \Sigma^* \to M$ with $M \in \mathcal{V}$ there is an N such that $\varphi(u_n) = \varphi(v_n)$ for all $n \geq N$ and thus $\widehat{\varphi}(u) = \widehat{\varphi}(v)$.

■

Theorem 5.3.5 (Reiterman)**.** *A class of finite monoids is a variety iff it can be defined by a set of profinite identities.*

Proof. We have already shown in Lemma 5.3.2 that the class of monoids defined by a set of profinite identities is a variety. Now, we only need to show that every variety can be described that way. Let $\mathcal{V}$ be a variety of finite monoids, E the class of profinite identities that are satisfied by all $M \in \mathcal{V}$ and $\mathcal{W} = [E]$. Obviously, $\mathcal{V} \subseteq \mathcal{W}$. Now take any monoid in $\mathcal{W}$. We claim that M is in $\mathcal{V}$. M is finite and therefore, there is an alphabet Σ and a surjective homomorphism $\varphi : \Sigma \to M$, which can be extended to a uniformly continuous homomorphism $\widehat{\varphi} : \widehat{\Sigma^*} \to M$, which is clearly surjective as well. Without loss of generality, we can assume that M is Σ-generated. If it were not, we could consider the Σ-generated monoid that is isomorphic to M, which is clearly in $\mathcal{V}$ if and only if M is in $\mathcal{V}$. Now let $\widehat{\pi}_\mathcal{V} : \widehat{\Sigma^*} \to \widehat{F}_\mathcal{V}(\Sigma)$ be the extension of the natural homomorphism $\pi_\mathcal{V}$ and $u, v \in \widehat{\Sigma^*}$. By Lemma 5.3.4 we have that $\widehat{\pi}_\mathcal{V}(u) = \widehat{\pi}_\mathcal{V}(v)$ iff $u = v$ is an identity of $\mathcal{V}$. In particular, it holds that $\pi_\mathcal{V}(u) = \pi_\mathcal{V}(v)$ implies that $\widehat{\varphi}(u) = \widehat{\varphi}(v)$. Therefore, the function $\gamma : \widehat{F}_\mathcal{V}(\Sigma) \to M : \widehat{\pi}_\mathcal{V}(u) \mapsto \widehat{\varphi}(u)$ is well defined because $\widehat{\pi}_\mathcal{V}$ is surjective. We also see that $\widehat{\varphi} = \gamma \circ \widehat{\pi}_\mathcal{V}$ and that γ is a surjective homomorphism. We now show that γ is continuous. M is discrete and finite. Therefore, every closed set can be written as finite union of sets of the kind $\{m\}$. Showing that $\gamma^{-1}(\{m\})$ is closed, proves that γ is continuous. We see that $\widehat{\varphi}^{-1}(\{m\}) = (\gamma \circ \widehat{\pi}_\mathcal{V})^{-1}(\{m\} = \widehat{\pi}_\mathcal{V}^{-1}(\gamma^{-1}(\{m\}))$ and therefore $\widehat{\pi}_\mathcal{V}(\widehat{\varphi}^{-1}(\{m\})) = \gamma^{-1}(\{m\})$. Since $\widehat{\varphi}$ is continuous, we have that $\widehat{\varphi}^{-1}(\{m\})$ is closed and as a closed subset of a compact set it is also compact by Lemma 1.1.24. Therefore $\widehat{\pi}_\mathcal{V}(\widehat{\varphi}^{-1}(\{m\}))$ is compact by Lemma 1.1.25 and thus closed, which shows that γ is continuous. That means, that M is in $\mathcal{V}$ by Lemma 5.1.12 as it is a continuous quotient of $\widehat{F}_\mathcal{V}(\Sigma)$ and Σ-generated. ■

Example 5.3.6. As we have seen in Example 5.1.3, the class $\mathcal{C}$ of the commutative finite monoids is a variety. Having defined identities, we also see with whith identity we can

describe $\mathcal{C}$. Clearly, all the monoids in satisfy the identity $ab = ba$ over the alphabet $\{a, b\}$. Furthermore, if a monoid satisfies this identity, it is clearly commutative and we get the equality.

Example 5.3.7. Consider the aperiodic monoid M. That means that for every element $x \in M$ there is an $n \in \mathbb{N}$ such that $x^{n+1} = x^n$. Let x be any element in M and $x^l = s$ its idempotent power. Now take a multiple ml of l such that $ml > n$. Then $sx = s^m x x^{ml} x = x^{ml} = x^l = s$. Therefore M fulfills the profinite identity $x^\omega x = x^\omega$.

Now consider any monoid M that fulfills the profinite identity $x^\omega x = x^\omega$. Then, clearly M is aperiodic. Simply choose the homomorphism $\varphi : \Sigma^* \to M$ that maps x to any element $m \in M$. Then x^ω is mapped to the idempotent m^l and we have that $m^l m = m^l$.

It follows that the class of aperiodic finite monoids can be described by the profinite identity $x^\omega x = x^\omega$ and is therefore a variety.

Bibliography

[1] Stefan Hetzl. *Automata and Formal Languages*. Available at: `https://www.dmg.tuwien.ac.at/hetzl/teaching/index.html` (visited on 27.06.2023). 2023.

[2] Michael Kaltenbäck. *Fundament Analysis*. Available at (chapterwise - german): `https://www.asc.tuwien.ac.at/~mbaeck/?id=fundam` (visited on 27.06.2023). Heldermann Verlag, 2015.

[3] Jean-Éric Pin. *Mathematical Foundations of Automata Theory*. Available at: `https://www.irif.fr/~jep/MPRI/MPRI.html` (visited on 27.06.2023). 2022.

[4] Harald Woracek, Michael Kaltenbäck, and Martin Blümlinger. *Funktionalanalysis*. Available at: `https://www.asc.tuwien.ac.at/functionalanalysis/?id=skripten` (visited on 27.06.2023). 2022.