Freie Universität Berlin

Bachelor's Thesis

Computer-supported Exploration of a Categorical Axiomatization of Miroslav Benda's Modeloids

Author:
Lucca Tiemens

Supervisor:
Prof. Dr. Christoph Benzmüller

A thesis submittted in partial fulfillment of the requirements for the degree of Bachelor of Science

at the

Department of Mathematics and Computer Science

First assessor:	Prof.	Dr. Christoph Benzmüller
Second assessor:	Prof.	Klaus Altmann
External advisor and reviewer:	Prof.	Dana S. Scott
External advisor and reviewer:	Dr.	Miroslav Benda

August 11, 2019

Abstract

A modeloid, a certain equivalence relation with an operation inspired by Ehrenfeucht-Fraïssé games, formulated by Miroslav Benda, is generalized first to an inverse semigroup and then to an inverse category. It is shown that a categorical modeloid on the category of a finite vocabulary can be used to play Ehrenfeucht-Fraïssé games. On the way the Wagner-Preston representation theorem and the Ehrenfeucht-Fraïssé theorem are proven. The whole development was supported by computer-based theorem proving.

Contents

Introduction

The starting point for this thesis came by coincidence. Miroslav Benda had contacted Dana Scott because he noticed that Scott was using the idea of an Ehrenfeucht-Fraïssé game implicitly in his paper "Invariant Borel sets".[1] Since Benda had studied and included these games into his own work "Modeloids. I"[2] he asked Scott if he knew of any further connections. Scott suggested to generalize the setting of a modeloid to category theory and shared this idea with Christoph Benzmüller, whom this author is a student of. This thesis is the result of this author connecting and detailing the fruitful ideas of Scott, Benda and Benzmüller.

Benda had long established that a modeloid, an equivalence relation enriched with additional axioms, can be seen as a set of partial one-one functions satisfying certain conditions. In private work he had also translated what is called the derivative of a modeloid into this setting. The derivative is the connection to Ehrenfeucht-Fraïssé games. This transition is presented in chapter 1.

It was due to Scott's memory that led to the discovery of inverse semigroups. The fact that these can be faithfully embedded into a set of partial one-one functions by the Wagner-Preston representation theorem enabled us to formulate a modeloid as an inverse semigroup. This is the subject of chapter 2.

Scott then proposed a category which when having just one object would be an inverse semigroup. It was Mark Lawson who remarked in an e-mail that this category is known as an inverse category in the literature. In chapter 3 we show the equivalence between the two formulations. Furthermore, the notion of a categorical modeloid is developed and shown to be a generalization of the initial modeloid.

Chapter 4 then makes the connection of categorical modeloids to Ehrenfeucht-Fraïssé games explicit.

Throughout this thesis computer-based theorem proving has been employed in order to demonstrate the capability of proof automation. The software used is Isabelle/HOL[3] in the 2018 Edition. As a result, unless stated otherwise, all computer-based proofs have been conducted using only the *sledgehammer*[4] command. This command uses the developed theory and the statement about to be proven as an input and requires no further interaction with the user. In addition,

[1] D. Scott, "Invariant Borel sets".
[2] Benda, "Modeloids. I".
[3] Isabelle/HOL is a higher-order logic theorem proving environment. More information can be found at `https://isabelle.in.tum.de/index.html`
[4] Meng and Paulson, "Lightweight relevance filtering for machine-generated resolution problems".

the command *nitpick*[5] was very enlightening for the author at times for learning the theory because it constructs counterexamples for incorrect statements hence deepening the understanding of a mathematical situation.

Having had relatively little knowledge in both, inverse semigroup theory and model theory, the development of this project taught the author a lot in the four-month period that has passed since the idea was proposed.

Acknowledgments

I want to express my gratitude to Christoph Benzmüller for being a carrying supervisor who provided everything I could ask for as his student and for the close communication he offered whenever needed. I am grateful to Dana Scott for the guidance and communication during the project and without whom this thesis would not exist. And I am grateful to Miroslav Benda for initiating this work, his ideas and his inspiring attitude in all the communication we had. I also want to thank Klaus Altmann for agreeing to become the second assessor of this thesis. Furthermore, I want to thank my family and friends for their unlimited support. Special thanks to Tobias Sanberger and Joaquim Ribeiro for proofreading parts of this work.

[5] Blanchette and Nipkow, "Nitpick: A counterexample generator for higher-order logic based on a relational model finder".

1 Modeloid

This chapter will serve as an introduction to modeloids. It is based on Miroslav Benda's original paper[1] in which he introduced the concept of a modeloid. In what follows some of the notation of the original version was changed. We will start by examining the basic terminology underlying the theory of modeloids. We then define the important concept of the derivative operation. The goal of this chapter is to develop a representation of a modeloid as a set of partial bijections in contrast to an equivalence relation enriched with additional axioms. This representation enables the transfer of a modeloid first into the language of semigroup theory and then into category theory.

1.1 Modeloidal equivalence relation

Let Σ be a finite non-empty set. The elements of Σ are called *letters*. Now take n different letters out of Σ and place them in an ordered sequence. What we get is a word in everyday language if Σ is the English alphabet or, of course, any other alphabet. Hence we call any such sequence a *word* and the set Σ an *alphabet* as is typically done in theoretical computer science. Formally we have the following definition:

Definition 1.1.1 (Word)**.** Let Σ be an alphabet, i.e. a non-empty finite set. Then the n-tuple $x = (x_1, ..., x_n) \in \Sigma^n$ for mutually distinct $x_1, .., x_n$ is called a word for $n \in \mathbb{N}$.

Each of the elements that compose the word appears only once. As a result a word cannot have more components than the size of its underlying alphabet Σ. It is the *set of all words* on Σ given by

$$\cup_{n=0}^{|\Sigma|}\Sigma^n \text{ and denoted by } \Sigma^*$$

that we want to define a modeloid on. Note that Σ^0 is the empty word denoted by ϵ. The *length* of a word is the function $l : \Sigma^* \to \mathbb{N}$. Since $w \in \Sigma^* \Rightarrow w \in \Sigma^n$ for some $n \in \mathbb{N}$, we define l by $w \mapsto n$. So the length of a word is the length of its sequence.

It will be necessary to talk about sub-words of a given word $w \in \Sigma^n$. Formally a sub-word v of w is a word $v \in \Sigma^m$ such that $m < n$ and $v_i = w_i$ for $i \in \{1, .., m\}$. We write $v \leq w$. Observe that this implies that $\epsilon \leq w$ for all $w \in \Sigma^*$. At last note that S_n is the symmetric group of $\{1, .., n\}$ and that for $w \in \Sigma^n$ and $\pi \in S_n$, writing $\pi(w)$ is an abuse of notation for $(x_{\pi(1)}, x_{\pi(2)}, .., x_{\pi(n)})$.

[1] Benda, "Modeloids. I".

Definition 1.1.2 (Modeloid[2])**.** Let Σ be an alphabet. A modeloid on Σ^* is a binary relation $E \subset \Sigma^* \times \Sigma^*$ such that E is an equivalence relation which satisfies the following three axioms:[3]

1. $(xEy) \Rightarrow l(x) = l(y)$
2. $((xEy) \wedge (u \leq x) \wedge (v \leq y) \wedge l(u) = l(v)) \Rightarrow (uEv)$
3. For $n := l(x)$ let $\pi \in S_n$. Then $(xEy) \Rightarrow (\pi(x)E\pi(y))$

As such a modeloid is an equivalence relation in which only words of the same length are in the same equivalence class. Furthermore, the second axiom, called the hereditary property, says that if two words are equivalent, so are their subwords of same length. It can be seen as a downward closer in regards of $\leq$. The third axiom states that given two equivalent words the permuted words stay in relation as long as they were permuted in the same way.

Example 1 (Finite linearly ordered set[4])**.** Let $(\Sigma, <)$ be a finite linearly ordered set. Take $x, y \in \Sigma^*$ and define the partial map[5] $h_{x,y} : \Sigma \to \Sigma$ by

$$h_{x,y}(x_i) = \begin{cases} y_i & \text{if } i \leq l(y) \\ y_{l(y)} & \text{if } i > l(y) \end{cases}, \qquad 1 \leq i \leq l(x)$$

Setting the equivalence relation E on Σ by $(xEy) :\Leftrightarrow (h_{x,y}$ is order-preserving and bijective) yields a modeloid as can be easily checked.

Example 2 (Subgroup of S_n[6])**.** Let $\Sigma = \{1, .., n\}$ and $H \subseteq S_n$ be a subgroup. For $x, y \in \Sigma^*$ define

$$xEy :\Leftrightarrow l(x) = l(y) \wedge \exists \sigma, \pi \in S_n : \sigma\pi^{-1} \in H \wedge \sigma(i) = x_i \wedge \pi(i) = y_i$$

for $1 \leq i \leq min\{l(x), l(y)\}$. The resulting equivalence relation is a modeloid.

As shown by the examples the axioms of a modeloid are satisfiable. In general we want to study an operation that is called a derivative on a modeloid. To define it we state what it means to append letters to a given word. The process is called *concatenation*. Let $x \in \Sigma^*$ and $v \in \Sigma$. We then define

$$x\hat{}v := \begin{cases} (x_1, .., x_n, v) & \text{if } \forall i \in \{1, .., n\} : v \neq x_i \\ (x_1, .., x_n) & \text{if } \exists i \in \{1, .., n\} : v = x_i \end{cases}$$

That way we ensure $x\hat{}v \in \Sigma^*$. From now on writing $x\hat{}v$ is replaced by simply typing xv as long as it is clear from the context that concatenation is being done.

[2] Benda, "Modeloids. I", p. 50.
[3] As is common we write (xEy) and mean $(x, y) \in E$
[4] Benda, "Modeloids. I", p. 50.
[5] A definition can be found on page 7
[6] Benda, "Modeloids. I", p. 50.

Definition 1.1.3 (Derivative[7])**.** The derivative on a modeloid E on Σ is the binary relation $D(E) \subset \Sigma^* \times \Sigma^*$ defined as

$$x\, D(E)\, y :\Leftrightarrow \forall a \in \Sigma\, \exists b \in \Sigma : xaEyb \wedge \\ \forall a \in \Sigma\, \exists b \in \Sigma : xbEya$$

The derivative is about the possibility of extending words. Given $x\, D(E)\, y$ we know that for every letter which we concatenate to x it is possible to find another letter that can be concatenated to y such that the equivalence for the resulting words holds and the other way around. It is worth noting that the derivative can also be defined on usual equivalence relations. The key property that makes the derivative so interesting is the fact that it yields a modeloid again.

Proposition 1.1.4. [8] *If E is a modeloid on Σ then so is $D(E)$. Furthermore we have that $D(E) \subset E$.*

The difference of defining the derivative on a modeloid instead of an equivalence relation is the inclusion statement. That is if we just require E to be an equivalence relation $D(E) \subset E$ cannot be ensured.

Proof. Let E be a modeloid on Σ. We have to check that the relation $D(E)$ satisfies all modeloidal axioms. Let's start with the property of $D(E)$ being an equivalence relation:

- Reflexivity: Let $x \in \Sigma^*$. Then $\forall a \in \Sigma : xaExa$ is true because E is reflexive. Hence also $x\, D(E)\, x$ by applying the definition.
- Symmetry: Suppose $x\, D(E)\, y$ holds. By definition and symmetry of E we get $\forall a \in \Sigma\, \exists b \in \Sigma : ybExa \wedge \forall a \in \Sigma\, \exists b \in \Sigma : yaExb$. Now symmetry of $\wedge$ yields exactly $y\, D(E)\, x$.
- Transitivity: Suppose $x\, D(E)\, y$ and $y\, D(E)\, z$. Given $a \in \Sigma$ we want to show that $\exists b \in \Sigma : xaEzb$. But because of the assumption we already know $\exists b' \in \Sigma : xaEyb'$ and $\exists \hat{b} \in \Sigma : yb'Ez\hat{b}$. Transitivity of E implies the desired formula. $\exists b \in \Sigma : xbEza$ for given $a \in \Sigma$ follows analogously. As a result using the definition of the derivative we have $x\, D(E)\, z$.

This leaves three axioms to go. But first we want to prove $D(E) \subset E$. So suppose that $x\, D(E)\, y$. Then we can fix some $a, b \in \Sigma$ such that $xaEyb$ holds. Since E is a modeloid we get $l(xa) = l(yb)$. Now $l(a) = l(b)$ implies $l(x) = l(y)$ has to hold. Hence we can use the hereditary property and get xEy as desired. On the way we also proved $x\, D(E)\, y \Rightarrow l(x) = l(y)$ and as a result $D(E)$ respects length.

Let's turn to the hereditary property of $D(E)$. So suppose $x\, D(E)\, y$ and fix $u \leq x$, $v \leq y$ such that $l(u) = l(v) =: k$. Fix again some $a \in \Sigma$ and choose b accordingly such that $xaEyb$ holds. Note that $xa = (x_1, .., x_n, a) = (u_1, .., u_k, x_{k+1}, .., x_n, a)$ and $yb = (y_1, .., y_n, b) = (v_1, .., v_k, y_{k+1}, .., y_n, b)$ which reveals that we can find a permutation $\pi \in S_{n+1}$ such that $\pi(xa) = (u_1, .., u_k, a, x_{k+1}, .., x_n)$ and $\pi(yb) =$

[7] Benda, "Modeloids. I", p. 52.
[8] Benda, "Modeloids. I", p. 52.

$(v_1, .., v_k, b, y_{k+1}, .., y_n)$. Since E is a modeloid we have $xaEyb \Rightarrow \pi(xa)\, E\, \pi(yb)$ and by the hereditary property $uaEvb$. But a was chosen arbitrarily in the beginning. As a result we get $\forall a \in \Sigma\, \exists b \in \Sigma : uaEvb$. In analogy we obtain $\forall a \in \Sigma\, \exists b \in \Sigma : ubEva$ and have $u\, D(E)\, v$ in total.

The last thing we have to show is $x\, D(E)\, y \Rightarrow \sigma(x)\, D(E)\, \sigma(y)$ for $\sigma \in S_{l(x)}$. So suppose $x\, D(E)\, y$ and fix $\sigma \in S_{l(x)}$. As before we obtain $\forall a \in \Sigma\, \exists b \in \Sigma : xaEyb$. Defining $\sigma' : \{1, .., l(x)+1\} \to \{1, .., l(x)+1\}$ by

$$\sigma'(m) := \begin{cases} \sigma(m) & , m \leq l(x)+1 \\ m & , m = l(x)+1 \end{cases}$$

one can see that $\sigma' \in S_{l(x)+1}$. This implies $\forall a \in \Sigma\, \exists b \in \Sigma : \sigma'(xa) E \sigma'(yb)$. Since $\sigma'(xa) = \sigma(x)a$ and $\sigma'(yb) = \sigma(y)b$ it follows that $\forall a \in \Sigma\, \exists b \in \Sigma : \sigma(x)aE\sigma(y)b$. By getting $\forall a \in \Sigma\, \exists b \in \Sigma : \sigma(x)bE\sigma(y)a$ in analogy, we have proven $x\, D(E)\, y \Rightarrow \sigma(x)\, D(E)\, \sigma(y)$. □

Now that we have seen that the derivative on a modeloid is a modeloid again, the natural question arises how the modeloid changes if one takes the derivative n times. This can be thought of as being able to expand a word by an arbitrary letter n times, each choice being independent from the last one. The next two definitions provide the terminology for this process. First we make precise what taking the derivative n-times means.

Definition 1.1.5. Let E be a modeloid on the alphabet Σ. Define

$$D^0(E) := E \text{ and } D^{n+1}(E) := D(D^n(E))$$

for $n \in \mathbb{N}$. Then taking the derivative n-times stands for $D^n(E)$.

Definition 1.1.6 (Complexity[9])**.** The complexity of a modeloid E is the first $n \in \mathbb{N}$ such that $D^{n+1}(E) = D^n(E)$. This modeloid $D^n(E)$ is called basic.

This can be seen as a stabilization. That is that the derivative on a basic modeloid E_{basic} does not change the modeloid anymore. Note that this unchanging modeloid will at least consist of all pairs $x\, E_{basic}\, x$ where x is a letter from the alphabet that the modeloid is defined on. For any basic modeloid one can extend a word x, if $x\, E_{basic}\, y$, arbitrarily with letters from the alphabet and be sure that the extended word will also be in relation with some other word and belong to E_{basic}.

1.2 Partial bijections

We will show now that modeloids can not only be represented by a relation E but also as a set M of partial bijections on an alphabet. Therefore, we will introduce the notion of a partial function. The definitions are taken from Lawson, *Inverse Semigroups*.

[9] Benda, "Modeloids. I", p. 53.

Definition 1.2.1 (Partial function[10])**.** Let X, Y be any two sets. A partial function $f : X \to Y$ is a function from a subset A of X to a subset B of Y. The set A consists of all those $a \in X$ for which $f(a)$ is defined. A is called the domain of f, denoted $dom f$. B is called the image or codomain of f and denoted by $cod\, f$. We have that $cod\, f = f(dom f)$.

Just as we can have the empty relation, the empty partial function 0 is also possible. It is unique for two given sets and characterized by $dom\, 0 = \varnothing$. Another important type of a partial function is a so called *partial identity*. Let A be a subset of a set X. Then the partial function $1_A : X \to X$ is called a partial identity if it is the identity on A and not defined outside of A.

Up next is the question on how to compose partial functions. Given $f : X \to Y$ and $g : Y \to Z$ the crucial part is to define the new domain of $g \circ f$. It is straightforward to say

$$dom(g \circ f) = f^{-1}(dom\, g \cap cod\, f)$$

This way we ensure that if $x \in dom(g \circ f)$ then $(g \circ f)(x) = g(f(x))$ is defined. This shows why the empty partial function is especially important because the intersection between $dom\, g$ and $cod\, f$ can be empty and $g \circ f$ will become the empty partial function. Instead of $g \circ f$ we also simply write gf.

We are particularly interested in partial bijections. A *partial bijection* is a partial function $f : X \to Y$ that induces a bijection between its domain and its codomain. As a result it is possible to define the *inverse* $f^{-1} : Y \to X$ as the inverse of the underlying total function $f : dom f \to cod\, f$. With this in mind it follows that the composition of partial bijections is again a partial bijection.

The following proposition summarizes the most important immediate consequences. We omit the proof which can be found in Lawson, *Inverse Semigroups*, p. 5.

Proposition 1.2.2. *Let X, Y and Z be sets, and let $f : X \to Y$ be a partial bijection.*

1. *$f^{-1}f = 1_{dom f}$, a partial identity on X, and $ff^{-1} = 1_{cod\, f}$, a partial identity on Y*
2. *For a partial bijection $g : Y \to X$, the equations $f = fgf$ and $g = gfg$ hold if, and only if, $g = f^{-1}$*
3. *$(f^{-1})^{-1} = f$*
4. *$1_A 1_B = 1_{A \cap B} = 1_B 1_A$ for all partial identities 1_A and 1_B where $A, B \subseteq X$*
5. *$(gf)^{-1} = f^{-1}g^{-1}$ for any partial bijection $g : Y \to Z$*

[10] Lawson, *Inverse Semigroups*, p. 4.

1.3 Replacing the modeloidal relation

Now that the fundamentals of partial functions have been introduced we return to the question of how to replace the modeloidal relation. For this we define

$$F(\Sigma) := \{f : \Sigma \to \Sigma |\, f \text{ is a partial bijection}\} \tag{1.1}$$

for an alphabet Σ. Then let $E \subseteq \Sigma^* \times \Sigma^*$ and $M \subseteq F(\Sigma)$. The names E and M have been chosen suggestively but do not imply any property at this point. We then demand that

$$(x, y) \in E \Rightarrow \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \in M \tag{1.2}$$

and for $0 < k \leq |\Sigma|$.

$$\{(x_1, y_1), .., (x_k, y_k)\} \in M \Rightarrow \{(\pi(x), \pi(y)) |\, \pi \in S_k\} \subset E \tag{1.3}$$

As a result a relationship between E and M is established. In the two propositions that follow E and M are assumed to satisfy this relationship. It should be noted that $\{(x_1, y_1), .., (x_k, y_k)\}$ represents a function from Σ to Σ that sends x_i to y_i for $i \in \{1, .., k\}$. Concerning the resulting function in 1.2, since $\{x_1, .., x_k\} \subset \Sigma$, it is a partial function and in particular it is a partial bijection since it is injective as $y_1, .., y_k$ are mutually distinct because y was assumed to be a word. The next two propositions will reveal why we created this setting.

Proposition 1.3.1. *If E is a modeloid then M fulfills the following axioms:*

1. *Closure of composition: $f, g \in M \Rightarrow f \circ g \in M$*
2. *Closure of taking inverses: $f \in M \Rightarrow f^{-1} \in M$*
3. *Inclusion property: $f \in M$ and $A \subset domf$ implies $f|_A \in M$*
4. *Identity: $id_\Sigma \in M$*

In addition, E can be recovered from M. That is no information gets lost when going from the set E to M.

Proof. Let E be a modeloid on Σ and let M be a set such that 1.2 and 1.3 hold.

1. Closure of composition: Take $f, g \in M$ and denote the elements in $dom(fg) = g^{-1}(dom\, f \cap cod\, g)$ by $\{w_i |\, 0 \leq i \leq k\}$ where $k := |dom(fg)|$. Furthermore, set $q_i := g(w_i)$ and define $u_i := fg(w_i)$ for $i \in \{1, .., k\}$. What we want to prove now is that $(w_1, .., w_k)E(u_1, .., u_k)$. Because then we immediately get $fg \in M$ by 1.2.

   First observe that $dom(fg) \subseteq dom\, g$. Setting $m := |dom\, g|$ we can write

   $$g = \{(w_1, q_1), .., (w_k, q_k), (w_{k+1}, q_{k+1}), .., (w_m, q_m)\}.$$

   Because of 1.3 it holds that $(w_1, .., w_k)E(q_1, .., q_k)$. Defining $j := |domf|$ and writing

   $$f = \{(q_1, u_1), .., (q_k, u_k), (q_{k+1}, u_{k+1}), .., (q_j, u_j)\}$$

it follows that 1.3 implies $(q_1, .., q_k)E(u_1, .., u_k)$. Transitivity of E then implies $(w_1, .., w_k)E(u_1, .., u_k)$ as desired.

2. Closure of taking inverses: Let $f \in M$. Setting $k := |domf|$ we can write

$$f = \{(x_1, y_1), .., (x_k, y_k)\}.$$

1.3 implies that $(x_1, ..x_k)E(y_1, .., y_k)$. Using the symmetry of E and 1.2 again we then get

$$\{(y_1, x_1), .., (y_k, x_k)\} \in M.$$

But this is precisely f^{-1} as can be easily checked.

3. Inclusion property: For $f = \{(x_1, y_1), .., (x_k, y_k)\} \in M$ for some positive $k \leq |\Sigma|$ let A be any subset of $domf$. Define $m := |A|$. W.l.o.g we can say $A = \{x_1, .., x_m\}$ since we can always rename the elements of $domf$. Using 1.3 we can obtain $(x_1, .., x_m, .., x_k)E(y_1, .., y_k)$ and from there $(x_1, .., x_m)E(y_1, .., y_m)$ by the hereditary property of E. But using 1.2 we get

$$\{(x_1, y_1), .., (x_m, y_m)\} \in M.$$

4. Identity: Let x be a word in which every letter of Σ appears once, i.e. $x = (x_1, .., x_{|\Sigma|})$. Then by reflexivity of E we have xEx and hence by 1.2

$$id_\Sigma = \{(x_1, x_1), .., (x_{|\Sigma|}, x_{|\Sigma|})\} \in M.$$

It remains to show that we do not loose information when changing from E to M. For this reason suppose there is a new set E' such that M and E' are also sharing the relationships 1.2 and 1.3. It suffices to show that $E' = E$. To do this we will show both directions of the inclusion.
Show $E' \subseteq E$: So suppose $(x, y) \in E'$. Then by 1.2

$$\{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \in M.$$

But this now means that because of 1.3

$$\{(\pi(x), \pi(y))|\, \pi \in S_{l(x)}\} \subset E$$

and, therefore, also $(x, y) \in E$.
Showing $E \subseteq E'$ works in analogy. This completes the proof. □

Next we will show that the converse also works.

Proposition 1.3.2. *If $M \subseteq F(\Sigma)$ satisfies the four axioms from above then E is a modeloid. Furthermore, M can be recovered from E.*

Proof. So let $M \subseteq F(\Sigma)$ fulfill the axioms stated in 1.3.1. We will first show that E is an equivalence relation if it is in a relationship with M as required by 1.2 and 1.3.

1. Reflexivity: Let $x \in \Sigma^*$ be $x = (x_1, .., x_{l(x)})$ and define $A := \{x_1, .., x_{l(x)}\}$. We know that $id_\Sigma \in M$. As a result $id_\Sigma|_A \in M$. Then 1.3 implies that
$$\{(\pi(x), \pi(x))|\, \pi \in S_{l(x)}\} \subset E$$
and because of this we have xEx.

2. Symmetry: Suppose xEy. By the relationship to M we get
$$f = \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \in M$$
and because $f^{-1} \in M$ it yields that
$$\{(y_1, x_1), .., (y_{l(x)}, x_{l(y)})\} \in M.$$
Again by 1.3 it is sure that yEx holds.

3. Transitivity: Now let xEy and yEz. This implies that we have the following functions in M:
$$\{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \text{ and } \{(y_1, z_1), .., (y_{l(y)}, z_{l(z)})\}$$
The composition of these two functions then results in
$$\{(x_1, z_1), .., (x_{l(x)}, z_{l(z)})\} \in M.$$
This in turn yields xEz by using 1.3.

In the next step we show the remaining three axioms.

1. Suppose we have xEy. Then 1.2 implies $\{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \in M$. Since this is a partial bijection we get $l(x) = l(y)$.

2. Up next is the hereditary property. Let xEy, $u \leq x$, $v \leq y$ with $l(u) = l(v)$. We want to show that uEv holds.
First note that $x = (u_1, .., u_{l(u)}, .., x_{l(x)})$ and $y = (v_1, .., v_{l(v)}, .., y_{(l(y)})$ because u and v are initial sub-words. That implies by 1.2 and $l(u) = l(v)$
$$f := \{(u_1, v_1), .., (u_{l(u)}, v_{l(v)}), .., (x_{l(x)}, y_{l(y)})\} \in M.$$
Setting $A := \{u_i|0 < i \leq l(u)\}$ leads to the fact that $f|_A \in M$. This results by 1.3 in
$$\{(\pi(u), \pi(v))|\, \pi \in S_{l(u)}\} \subset E$$
which means that uEv holds.

3. At last we show that $(xEy) \Rightarrow (\pi(x)E\pi(y))$ for $n := l(x)$ and $\pi \in S_n$. But this is immediate because
$$xEy \Rightarrow \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \in M \Rightarrow \{(\pi(x), \pi(y))|\, \pi \in S_k\} \subset E.$$

In order to see that M can be recovered from E, let M' be a new set that shares the relationships 1.2 and 1.3 with E. We now show that this implies $M = M'$. As in the last proof we show the inclusion in one direction and deduce the other by analogy.
Show: $M' \subseteq M$ Let $\{(x_1, y_1), .., (x_k, y_k)\} \in M'$. By 1.3 for sure xEy and by 1.2 this yields $\{(x_1, y_1), .., (x_k, y_k)\} \in M$. □

As a result we have found a way to switch between a modeloid E and the set of partial bijections M without loosing information. Therefore, we call M a functional modeloid.

Definition 1.3.3 (Functional modeloid)**.** Let Σ be an alphabet and $M \subseteq F(\Sigma)$. M is called a functional modeloid if it satisfies the following axioms:

1. Closure of composition: $f, g \in M \Rightarrow f \circ g \in M$
2. Closure of taking inverses: $f \in M \Rightarrow f^{-1} \in M$
3. Inclusion property: $f \in M$ and $A \subset dom f$ implies $f|_A \in M$
4. Identity: $id_\Sigma \in M$

We can rework the definitions which we introduced for the modeloidal relation also in terms of a functional modeloid. This is a very important step because it shows that what we have done so far works for both kinds of modeloids. We start with the derivative operation for a functional modeloid M and want it to resemble the derivative for a modeloidal relation E. We can do that by considering the following diagram:

$$\begin{array}{ccc} M & \longrightarrow & E \\ & & \downarrow \\ D(M) & \longleftarrow & D(E) \end{array}$$

Looking at the chain of equivalences that emerge when following the diagram backwards we can define the derivative. That is:

$$\begin{aligned} & \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \in D(M) \\ \iff \quad & \{(\pi(x), \pi(y)) |\, \pi \in S_{l(x)}\} \subset D(E) \\ \iff \quad & \forall a \in \Sigma\, \exists b \in \Sigma : \{(\pi(x)a, \pi(y)b) |\, \pi \in S_{l(x)}\} \subset E \wedge \\ & \forall a \in \Sigma\, \exists b \in \Sigma : \{(\pi(x)b, \pi(y)a) |\, \pi \in S_{l(x)}\} \subset E \\ \iff \quad & \forall a \in \Sigma\, \exists b \in \Sigma : \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)}), (a, b)\} \in M \wedge \\ & \forall a \in \Sigma\, \exists b \in \Sigma : \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)}), (b, a)\} \in M \end{aligned} \tag{1.4}$$

Summarizing this last passage yields the following definition.

Definition 1.3.4 (Derivative on functional modeloid)**.** Let M be a functional modeloid on Σ. Then $D(M) \subseteq F(\Sigma)$ is defined as

$$\begin{aligned} \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)})\} \in D(M) :\Leftrightarrow & \\ \forall a \in \Sigma\, \exists b \in \Sigma : \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)}), (a, b)\} \in M \wedge & \\ \forall a \in \Sigma\, \exists b \in \Sigma : \{(x_1, y_1), .., (x_{l(x)}, y_{l(y)}), (b, a)\} \in M & \end{aligned}$$

We automatically get that $D(M) \subseteq M$ by 1.4 and that $D(M)$ is a functional modeloid again because of the diagram above and proposition 1.3.1. Definitions 1.1.5 and 1.1.6 just carry over and it is easy to check that the complexity stays the same regardless of which modeloid representation we use.

We are rewarded with the fact that a functional modeloid M can be seen as an inverse semigroup which will be the topic of the next chapter. This perspective allows for generalizing a modeloid in a natural way that could not be seen before when just having the modeloidal relation. This opens up the door for formulating a modeloid in category theory.

2 Inverse Semigroups and Modeloids

This chapter is about the transition form a functional modeloid to an inverse semigroup. We start by defining an inverse semigroup and showing that a functional modeloid *is* an inverse semigroup. The main result of this chapter is the Wagner-Preston representation theorem. With its help we can generalize a functional modeloid to the language of semigroup theory. While doing this automated theorem proving in Isabelle/HOL[1] will show to be very useful in this section because we will delegate a number of proofs to the system. The goal is to provide evidence for the possiblity to integrate computer-based theorem proving into mathematical work done by hand.

This approach enables one to quickly explore new ideas once the environment is set up. Of cause one has to bear in mind the limitations at this stage. That is the more structure was built by definitions the more unlikely it is that an automated theorem proving environment will find a proof without interaction. But an inverse semigroup is quite a simple object and therefore a perfect candidate.

2.1 An inverse semigroup

The plan for this section is to implement the mathematics shown and to have Isabelle/HOL carry out the proofs as far as this is easier then doing it by hand. We start with the definition of an inverse semigroup.

Definition 2.1.1 (Inverse semigroup[2])**.** Let S be a set equipped with the binary operation $* : S \times S \to S$ and the unary operation $a \mapsto a^{-1}$. $(S, *, ^{-1})$ is called an inverse semigroup if it satisfies the axioms

1. $(x * y) * z = x * (y * z)$ for all $x, y, z \in S$,
2. $x * x^{-1} * x = x$ for all $x \in S$,
3. $(x^{-1})^{-1} = x$ for all $x \in S$ and
4. $x * x^{-1} * y * y^{-1} = y * y^{-1} * x * x^{-1}$ for all $x, y \in S$

Note that this definition is purely equational. For our purposes we will represent an inverse semigroup the following way in Isabelle/HOL:

locale *inverseSemigroup* =

fixes — The two function symbols appearing in the vocabulary of an inverse semigroup

[1] Isabelle/HOL is a higher-order logic theorem proving environment. More information can be found at https://isabelle.in.tum.de/index.html.

[2] Howie, *Fundamentals of semigroup theory*, p. 145.

```
    inv::"'a⇒'a" ("inv _" 109) and
    mult::"'a⇒'a⇒'a" (infixl "⊗" 110)
```

assumes — Here we set the axioms that all individuals of type `a` have to obey

```
    Associativity: "(x ⊗ y) ⊗ z = x ⊗ (y ⊗ z)" and
    Regularity:    "x ⊗ (inv x) ⊗ x = x" and
    InvInv:        "((inv (inv x)) = x)" and
    IdemComm:      "x ⊗ (inv x) ⊗ y ⊗ (inv y) = y ⊗ (inv y) ⊗ x ⊗ (inv x)"
```

The domain for individuals is chosen to be `'a`. This means we have implemented a polymorphic version of an inverse semigroup making instantiation with other types possible.

Remark 2.1.2. *Every group G is an inverse semigroup. A comparison between the two structures will be done after the next definition.*
Furthermore, an inverse semigroup is a special case of a semigroup (S,) which only requires associativity to hold for $*$.*

Regarding the composition of two elements e and f in an inverse semigroup, we sometimes just write ef instead of $e * f$ if the context allows it. Naturally we are interested in knowing what an inverse for an element in an inverse semigroup is.

Definition 2.1.3 (Inverse)**.** Let S be an inverse semigroup and take $x \in S$. Then $t \in S$ is called an inverse of x if

$$x * t * x = x \text{ and } t * x * t = t$$

In analogy we implement the definition in Isabelle/HOL:

```
abbreviation (in inverseSemigroup) inverse:: "'a ⇒ 'a ⇒ bool" ("_ InverseOf
_")
  where "(y InverseOf x) ≡ (x ⊗ y ⊗ x = x) ∧ (y ⊗ x ⊗ y = y)"
```

This definition generalises the known inverses from group theory. Indeed let $(G, *, ^{-1}, e)$ be a group, $g \in G$ and $g^{-1} \in G$ its inverse in the group theoretical sense. Then

$$g * g^{-1} * g = e * g = g \text{ and } g^{-1} * g * g^{-1} = e * g^{-1} = g^{-1}.$$

So g^{-1} is also an inverse in the sense of definition 2.1.3.

Now the key difference between an inverse semigroup and a group is that of the result of the composition of an element with its inverse. While in a group we require that $g * g^{-1} = e$ where e is the designated neutral element, in a semigroup in general there is no such unique element. This is the main point of inverse semigroups: allowing generalized neutral elements. They act only on subsets as neutral elements. And it is this partiality that is captured by the definition of an inverse in an inverse semigroup.
To justify the name inverse semigroup we still have to show that every element does have an inverse.

Lemma 2.1.4. *Let S be an inverse semigroup. Then $\forall x \in S$ we have that x^{-1} is the inverse of x.*

At this point we utilize Isabelle/HOL and let it take care of the prove of the lemma above.

```
lemma (in inverseSemigroup) "(inv x) InverseOf x"
  by (metis InvInv Regularity)
```

The framework finds the proof immediately - it takes 6ms for completion. Next we want to turn to the question what these partial neutral elements we just talked about exactly are. They will be called idempotents.

Definition 2.1.5 (Idempotent)**.** An idempotent element $x \in S$ in an inverse semigroup S is such that $x * x = x$.

In our proving environment we define:

```
abbreviation (in inverseSemigroup) idempotent:: "'a ⇒ bool" ("Idem _")
  where "(Idem a) ≡ (a ⊗ a = a)"
```

We can confirm that an element composed with its inverse really is an idempotent.

Lemma 2.1.6. *For each element x in an inverse semigroup S we have that $x * x^{-1}$ is an idempotent.*

```
lemma (in inverseSemigroup) IdemComp: "Idem (x ⊗ (inv x))"
  by (metis Associativity Regularity)
```

Idempotent elements share an important property which is that they commute.

Lemma 2.1.7. *Any two idempotents in an inverse semigroup commute.*

```
lemma (in inverseSemigroup) IdempotentsCommute:
  "(Idem x) ∧ (Idem y) ⟶ x ⊗ y = y ⊗ x"
    by (metis Associativity IdemComm InvInv Regularity)
```

With this result we conclude the uniqueness of inverses.

Lemma 2.1.8. *Each element in an inverse semigroup has a unique inverse.*

```
lemma (in inverseSemigroup) InverseIsUnique:
  "∀x. ((y InverseOf x) ∧ (z InverseOf x) ⟶ y = z)"
    by (metis Associativity IdempotentsCommute)

lemma (in inverseSemigroup) InverseIsUnique2: "∀x. ∃! y. (y InverseOf x)"
  by (metis InvInv InverseIsUnique Regularity)
```

This allows a more intuitive view on inverse semigroups because they can also be characterised by 2.1.8.

Proposition 2.1.9. *Let S be a semigroup (see 2.1.2). Then the statement that every element has a unique inverse is equivalent to the axioms 2), 3) and 4) of an inverse semigroup.*

We have just seen one direction. In order to show the other we want to set up a semigroup in Isabelle/HOL that axiomatizes unique inverses for all its elements.

```
locale inverseSemigroup2 =

  fixes      — The function symbol appearing in the vocabulary of a semigroup
    mult::"'a⇒'a⇒'a" (infixl "⊗" 110)

assumes    — Here we set the axioms that all individuals of type a have to obey
    Associativity: "(x ⊗ y) ⊗ z = x ⊗ (y ⊗ z)" and
    uniqueInverse: "∀x. ∃! y. ((x ⊗ y ⊗ x = x) ∧ (y ⊗ x ⊗ y = y))"


abbreviation (in inverseSemigroup2) inverse::"'a ⇒ 'a ⇒ bool" ("_ InverseOf
_") where
    "(y InverseOf x) ≡ (x ⊗ y ⊗ x = x) ∧ (y ⊗ x ⊗ y = y)"
```

To make the new setting more intuitive we define the inverse again in this context. Then we can create the same lemma as before.

```
lemma (in inverseSemigroup2) "∀x. ∃! y. (y InverseOf x)"
  by (simp add: uniqueInverse)
```

Skolemization is difficult for Isabelle/HOL. But in order to prove the inverse semigroup axioms we will need it because the inverse function $^{-1}$, that appears in the inverse semigroup definition, arises that way from lemma 2.1.8. As a result we will define the inverse function by hand and therefore, have shown its existence. In Isabelle/HOL we will then use the $\forall$-quantifier to quantify over all functions that would define an inverse knowing that there is exactly one.

Lemma 2.1.10. *Let S be a semigroup (see: 2.1.2) satisfying that every element has a unique inverse. Then we can define a unique function $i : S \to S$ such that $\forall x \in S$ we have that $i(x)$ is the inverse of x.*

Proof. Let $x \in S$. Then define $i(x) = y$, where y is the unique inverse of x. □

From a theorem provers perspective this almost trivial statement is much harder to cope with than one would expect because one is actually changing the vocabulary of the current theory.

But now we are in the position to almost show proposition 2.1.9.

```
context inverseSemigroup2 begin

lemma regularity:
  "∀i::('a⇒'a).( ∀x. ((i x) InverseOf x)) ⟶ x ⊗ (i x) ⊗ x = x"
    by blast
```

```
lemma invInv: "∀ i::('a⇒'a). (∀ x. ((i x) InverseOf x)) ⟶ (i (i x)) = x"
  using uniqueInverse by auto

end
```

As it turns out proving $x * x^{-1} * y * y^{-1} = y * y^{-1} * x * x^{-1}$ for all $x, y \in S$ (axiom 4 of 2.1.1) does not work with automation at this point. The attempt to insert intermediate steps led to the belief that the proof[3] of this statement will be easiest by hand.

Proof. First of all define $e := x * x^{-1}$ and $f := y * y^{-1}$. The strategy will be to show that $e * f$ and $f * e$ are both inverses of $e * f$. Because of the uniqueness of inverses this impies that $e * f = f * e$.

Let z be the inverse of $e * f$. Since e and f are trivially idempotent and keeping in mind that we have already proven axioms 2) and 3) of an inverse semigroup we have that

$$(ef)(fze)(ef) = ef^2ze^2f = efzef = ef$$

and

$$(fze)(ef)(fze) = fze^2f^2ze = f(zefz)e = fze.$$

As a result fze is also an inverse of ef and hence by uniqueness $fze = z$. As just seen $(fze)(fze) = fze$ and hence z is idempotent. But now z and ef are inverses of z which implies $z = ef$. In analogy we obtain that fe is also idempotent. Then

$$(ef)(fe)(ef) = efef = ef$$

and

$$(fe)(ef)(fe) = fefe = fe.$$

Because of this fe is the inverse of ef but so is ef by idempotence. We conclude $ef = fe$. □

In summary we have shown proposition 2.1.9. There is yet another way to define an inverse semigroup.

Proposition 2.1.11. *Let S be a semigroup. If*

$$\forall x \in S\, \exists y \in S : x * y * x = x$$

holds and idempotents in S commute then each element has a unique inverse in S. The converse is also true.

In order to show the converse it suffices to show that idempotents commute. We once again utilize our framework. We assume

$$x * x^{-1} * y * y^{-1} = y * y^{-1} * x * x^{-1}$$

for all $x, y \in S$ since we have only shown it on paper.

[3] Howie, *Fundamentals of semigroup theory*, p. 146.

```
— We need to define idempotent again in this context
abbreviation (in inverseSemigroup2) idempotent::"'a ⇒ bool" ("Idem _")
  where "(Idem x) ≡ x ⊗ x = x"

lemma (in inverseSemigroup2) assumes
  "∀i::('a⇒'a). (∀x. ((i x) InverseOf x))
    ⟶ (x ⊗ (i x) ⊗ y ⊗ (i y) = y ⊗ (i y) ⊗ x ⊗ (i x))"
      shows "∀i::('a⇒'a). (∀x. ((i x) InverseOf x))
          ⟶ (((Idem x) ∧ (Idem y)) ⟶ x⊗y = y⊗x)"
  by (metis Associativity assms uniqueInverse)
```

Next we will show the other direction. We define a semigroup with the assumed properties and show that each element has a unique inverse. This time there is no skolemization involved and everything works smoothly.

```
locale inverseSemigroup3 =

  fixes      — The function symbol appearing in the vocabulary of a semigroup
    mult::"'a⇒'a⇒'a" (infixl "⊗" 110)

assumes    — Here we set the axioms that all individuals of type a have to obey
    Associativity: "(x ⊗ y) ⊗ z = x ⊗ (y ⊗ z)" and
    Regularity:    "∀x. ∃y. x ⊗ y ⊗ x = x" and
    IdemComm:      "(x⊗x=x ∧ y⊗y=y) ⟶ (x⊗y = y⊗x)"
begin

abbreviation inverse::"'a ⇒ 'a ⇒ bool" ("_ InverseOf _")
  where "(x InverseOf y) ≡ (x ⊗ y ⊗ x = x) ∧ (y ⊗ x ⊗ y = y)"

lemma exInverse: "∀x. ∃y. (y InverseOf x)"
  by (metis Associativity Regularity)

lemma InverseIsUnique:
  "∀x. ((y InverseOf x) ∧ (z InverseOf x) ⟶ y = z)"
    by (metis Associativity IdemComm)

proposition uniqueInverse: "∀x. ∃!y. (y InverseOf x)"
  using InverseIsUnique exInverse by blast

end
```

In summary we have achieved to prove the following theorem:[4]

Theorem 2.1.12. *Let S be a semigroup. Then the following are equivalent:*

1. *S is an inverse semigroup.*
2. *Every element of S has a unique inverse.*
3. *$\forall x \in S \exists y \in S : x * y * x = x$ and its idempotents commute.*

[4] Howie, *Fundamentals of semigroup theory*, p. 145.

2.2 Functional modeloid is inverse semigroup

Next we want to show that a functional modeloid M is an inverse semigroup. For this task regard $(M, \circ)$ as a semigroup. This is clear since composition of partial functions is associative. Once we establish that the partial identities of M are exactly the idempotent elements in $(M, \circ)$ we can conclude by referring to proposition 1.2.2 that $(M, \circ, ^{-1})$ is an inverse semigroup because of the closure of taking inverses required by the functional modeloid.

Lemma 2.2.1. *Let M be a functional modeloid on Σ. Then the idempotent elements in M are exactly the partial identities.*

Proof. If $x \in M$ is idempotent then $x = x*x*x$ and by Proposition 1.2.2, $x = x^{-1}$. So we get $x = x * x = x * x^{-1}$ which implies that x is a partial identity.

Conversely if $x \in M$ is a partial identity then $x = 1_A$ for some $A \subseteq \Sigma$ and again by Proposition 1.2.2 x is idempotent. □

From this we can conclude that every functional modeloid is an inverse semigroup. This is of fundamental importance because of the Wagner-Preston representation theorem. It states that every inverse semigroup $(\Sigma, ^{-1}, *)$ can be faithfully embedded into what we defined as $F(\Sigma)$. Now if we were able to formulate the axioms for a functional modeloid in inverse semigroup theory, this would yield that such a structure could faithfully be embedded into a functional modeloid. As a result the modeloid would be generalised but at the same time its basic principles would be kept. Our hope is that we can redefine the derivative operation in this context. In order to achieve this task we shall translate the axioms of a modeloid. We examine them one by one.

1. Closure of Composition: Because of the faithfulness of the embedding the composition of partial functions will simply be the $*$-operation in an inverse semigroup.
2. Closure of taking inverses: By theorem 2.1.12 an inverse semigroup is such that the inverse exists for every element and is unique, hence resembling the inverses of partial function and in particular the closure property.
3. The inclusion property: Here it is not apparent from first sight how this can be expressed within an inverse semigroup. We shall see soon how it works.
4. The identity on Σ: The identity sure will be an idempotent element in an inverse semigroup. But which one we actually choose will be discussed after the representation theorem.

It is the third axiom that we want to focus our attention on in the next section.

2.3 The natural partial order

The inclusion property inherent to a functional modeloid can be seen as a statement about a partial order $\subseteq$. That is for two partial functions f, g, we have $f \subseteq g$ if the restriction of g to a smaller subset of $dom\, g$ yields f. We will save this thought[5] even though the proof that this actually defines a partial order is left to the reader.

Definition 2.3.1. Let $f, g : X \to Y$ be two partial functions such that

$$dom f \subseteq dom\, g \text{ and } f(x) = g(x)$$

for all $x \in dom f$. Then we write $f \subseteq g$ and call f the restriction of g.

It is this partial orders meaning that can also be found in an inverse semigroup. In order to see this we will first define a relation of which we will show to be a partial order. Then with the Wagner-Preston representation theorem it will be shown that this relation represents the partial order stated above. As a result it opens up a way to translate the third axiom from 1.3.3.

In this section we shall only introduce those facts about the natural partial order which are needed in order to prove the Wagner-Preston representation theorem. A full investigation can be found in Lawson, *Inverse Semigroups*, Chapter 3.

As before we will prove the facts with Isabelle/HOL. This time this will go far in the sense that we only have to prove the representation theorem by hand. And even in its proof we will use Isabelle. It should be noted that this is done in order to present the capability of the `sledgehammer` command. We start by the definition of the natural partial order[6] and will then pave the way for the theorem.

Definition 2.3.2 (Natural partial order)**.** Let Σ be an inverse semigroup. Let $\leq \subseteq \Sigma \times \Sigma$. We define

$$s \leq t :\Leftrightarrow s = t * e$$

for some idempotent $e \in \Sigma$.

```
context inverseSemigroup begin

abbreviation natOrder:: "'a ⇒ 'a ⇒ bool" (infixl "≤" 111) where
  "(x ≤ y) ≡ (∃e. (Idem e) ∧  (x = y⊗e))"
```

First we show that this relation really defines a partial order to justify the name. We do this by using the definition of a partial order from the Isabelle/HOL library which can be found in the theory `Orders`. In order to prove it by automation it was necessary to unfold the subgoals.

```
interpretation inverseSemigroup: partial_order "natOrder"
```

[5] Lawson, *Inverse Semigroups*, p. 8.
[6] Lawson, *Inverse Semigroups*, p. 21.

```
proof unfold_locales
  show "⋀x. x ≤ x"
    by (metis Associativity InverseIsUnique2)
  show "⋀x y z. x ≤ y ⟹ y ≤ z ⟹ x ≤ z"
    by (metis Associativity IdempotentsCommute)
  show "⋀x y. x ≤ y ⟹ y ≤ x ⟹ x = y"
    by (metis Associativity IdempotentsCommute)
qed
```

Lemma 2.3.3. [7] *Let $\leq$ be the natural partial order on the inverse semigroup S and $s, t \in S$. Then the following are equivalent:*

1. $s \leq t$
2. $s = f * t$ *for some idempotent* $f \in S$
3. $s^{-1} \leq t^{-1}$

We show the equivalence between (1) and (2).

```
lemma eqDefNatOrder1a: "(( s ≤ t) ⟶ (∃f. ((Idem f) ∧ s = f⊗t)))"
  by (smt Associativity InverseIsUnique2)

lemma eqDefNatOrder1b: "((∃f. ((Idem f) ∧ s = f⊗t)) ⟶ ( s ≤ t))"
  by (metis (full_types) Associativity IdemComm InverseIsUnique Regularity)
```

And then between (1) and (3).

```
lemma eqDefNatOrder2a:"( s ≤ t) ⟶ ((inv s) ≤ (inv t))"
  by (smt Associativity InvInv InverseIsUnique2 Regularity)

lemma eqDefNatOrder2b:"((inv s) ≤ (inv t)) ⟶ ( s ≤ t) "
  by (smt Associativity InvInv InverseIsUnique2 Regularity)
```

Lemma 2.3.4. [8] *Given that S is an inverse semigroup we have for $s, t \in S$ that*

$$s \leq t \Rightarrow s^{-1} * s \leq t^{-1} * t.$$

```
lemma natOrderProp: "( s ≤ t) ⟶ (((inv s) ⊗ s) ≤ ((inv t) ⊗ t))"
  by (smt Associativity IdempotentsCommute Regularity)
```

Up next we will define principal left and right ideals for inverse semigroups.[9] This notion will be needed in order to construct the prove of the representation theorem. It is in analogy to the definition used for rings.

Definition 2.3.5. Let S be an inverse semigroup. A principal left ideal of S generated by $a \in S$ is the set

$$aS := \{a * s \,|\, s \in S\}.$$

Similarly one defines a principal right ideal of S generated by $a \in S$ as

$$Sa := \{s * a \,|\, s \in S\}.$$

[7] Lawson, *Inverse Semigroups*, p. 21.
[8] Lawson, *Inverse Semigroups*, p. 22.
[9] Lawson, *Inverse Semigroups*, p. 20.

```
abbreviation leftIdeal:: "'a ⇒ 'a set" ("_ S") where
  "(a S) ≡ {x. (∃s. x = a ⊗ s)}"

abbreviation rightIdeal:: "'a ⇒ 'a set" ("S _") where
  "(S a) ≡ {x. (∃s. x = s ⊗ a)}"
```

Lemma 2.3.6. [10] *Suppose S is an inverse semigroup. Then*

1. $aS = (aa^{-1})S$ *for all* $a \in S$
2. $Sa = S(a^{-1}a)$ *for all* $a \in S$
3. $eS \cap fS = (ef)S$ *where* e, f *are idempotents*
4. $Se \cap Sf = S(ef)$ *where* e, f *are idempotents*

We prove all the statements in the above order. For each statement we first show the inclusion from left to right and then the other way around.

```
lemma IdealLemma1a: "(a S) ⊆ ((a ⊗ (inv a)) S)"
  by (smt Associativity Collect_mono inverseSemigroup.Regularity inverseSemigroup_axioms)

lemma IdealLemma1b: "((a ⊗ (inv a)) S) ⊆ (a S)"
  using Associativity by blast

lemma IdealLemma2a: "(S a) ⊆ ((S ((inv a) ⊗ a)))"
  by (smt Associativity Collect_mono Regularity)

lemma IdealLemma2b: "((S ((inv a) ⊗ a))) ⊆ (S a)"
  by (smt Associativity Collect_mono)

lemma IdealLemma3a: "((Idem e) ∧ (Idem f)) ⟶(((e S) ∩ (f S)) ⊆ ((e ⊗ f)
S))"
  by (smt Associativity CollectD CollectI Int_Collect subsetI)

lemma IdealLemma3b: "((Idem e) ∧ (Idem f)) ⟶((e ⊗ f) S) ⊆ ((e S) ∩ (f
S))"
  by (smt Associativity CollectD CollectI Collect_conj_eq IdempotentsCommute
subsetI)

lemma IdealLemma4a: "((Idem e) ∧ (Idem f)) ⟶(((S e) ∩ (S f)) ⊆ (S (e ⊗
f) ))"
  by (smt Associativity CollectD CollectI Int_Collect subsetI)

lemma IdealLemma4b: "((Idem e) ∧ (Idem f)) ⟶ (S (e ⊗ f)) ⊆ ((S e) ∩ (S
f))"
  by (smt Associativity CollectD CollectI Collect_conj_eq IdempotentsCommute
subsetI)
```

This concludes the preliminaries for the next section.

end

[10] Lawson, *Inverse Semigroups*, p. 21.

2.4 Wagner-Preston representation theorem

We have established enough theory to prove the theorem which enables us to speak of a modeloid in inverse semigroup theory. After the theorem is proven we reflect on the third axiom of a functional modeloid again and translate it to the new environment. The concluding question will be about the forth axiom.

Theorem 2.4.1 (Wagner-Preston representation theorem[11])**.**

Let $\Sigma = (\Sigma, ^{-1}, *)$ *be an inverse semigroup and recall the definition of* $F(\Sigma)$ *(1.1). Then there is an injective homomorphism* $\Omega : \Sigma \to F(\Sigma)$ *such that for* $a, b \in \Sigma$

$$a \leq b \Longleftrightarrow \Omega(a) \subseteq \Omega(b).$$

Proof. The proof will be constructive. We will define a function $\Omega : \Sigma \to F(\Sigma)$ and show that it fulfills the desired properties.

The natural question is how to create a function from an element. The key idea here is to set the domain of the function to the left principle ideal generated by $a^{-1}a$ and the codomain to the left principle ideal generated by aa^{-1}. So we create a function θ_a depending on $a \in \Sigma$. We define

$$\theta_a : (a^{-1}a)\Sigma \to (aa^{-1})\Sigma \quad \text{by} \quad x \mapsto a * x.$$

Now, because by lemma 2.3.6 we have that $aa^{-1}\Sigma = a\Sigma$, the above function is welldefined since $\forall x \in \Sigma : a * x \in a\Sigma$.

Next we need to show that $\forall a \in \Sigma : \theta_a$ is a bijection. Note that then θ_a will be a partial bijection on Σ and therefore, belong to $F(\Sigma)$. We use Isabelle/HOL for illustration to show

$$\theta_a(x) = \theta_a(y) \Rightarrow x = y$$

and

$$\forall y \in a\Sigma\, \exists x \in (a^{-1}a)\Sigma : \theta_a(x) = y \text{ for } a \in \Sigma \text{ and } x, y \in dom(\theta_a).$$

context *inverseSemigroup* **begin**

— The index `a` in the function definition above really is a parameter of the function.
fun Θ*::"a ⇒ a ⇒ a"* **where**
"Θ a x = a ⊗ x"

lemma *wellDef: "(Θ a x) ∈ (a S) "* — This shows that Θ is welldefined again.
using *inverseSemigroup.Θ.simps inverseSemigroup_axioms* **by** *blast*

— The proof for injectivity
lemma Θ*injective:*
"(x ∈ (((inv a)⊗a) S) ∧ y ∈ (((inv a)⊗a) S) ∧ (Θ a x) = (Θ a y)) ⟶ (x=y)"
by *(smt Associativity Regularity mem_Collect_eq Θ.simps)*

[11] Lawson, *Inverse Semigroups*, p. 36.

— Proof for surjectivity. A little help is needed here
lemma *helpFactΘsur: "y∈(((inv a)⊗a) S) ⟶ (∃m. y = (inv a) ⊗ a ⊗ m)"*

by *blast*

lemma *Θsurjective: "∀x∈(a S). ∃y∈(((inv a)⊗a) S). ((Θ a y) = x)"*
by *(metis (mono_tags) Associativity IdealLemma1a IdealLemma1b InvInv Θ.simps wellDef helpFactΘsur subset_antisym)*

Now we are in the position to construct $\Omega : \Sigma \to F(\Sigma)$ by $a \mapsto \theta_a$ for $a \in \Sigma$. This function is welldefined since we just proved $\theta_a \in F(\Sigma)$ for all $a \in \Sigma$. Next we will show that Ω is injective. Isabelle can do the proof.

lemma *Ωinjective: "((Θ a) = (Θ b)) ⟶ (a = b)"*
by *(metis Associativity InverseIsUnique2 Θ.simps)*

To prove that Ω is a homomorphism we have to show that $\theta_{a*b} = \theta_a * \theta_b$. First we have to establish that $dom(\theta_{a*b}) = dom(\theta_a * \theta_b)$. For that we show

$$(ab)^{-1}(ab)\Sigma = \theta_b^{-1}(a^{-1}a\Sigma \cap bb^{-1}\Sigma).$$

Note that for fixed $a \in \Sigma$ we have $a^{-1} * \theta_a(x) = x$ if $x \in a^{-1}a\Sigma$ and $\theta_a(a^{-1} * y) = y$ for $y \in aa^{-1}\Sigma$ together implying that $\theta_a^{-1} = \theta_{a^{-1}}$. Because of this and lemma 2.3.6 we know that

$$\theta_b^{-1}(a^{-1}a\Sigma \cap bb^{-1}\Sigma) = \theta_{b^{-1}}(a^{-1}abb^{-1}\Sigma) = b^{-1}a^{-1}ab\Sigma$$

If we can prove that $b^{-1}a^{-1}ab\Sigma = (ab)^{-1}(ab)\Sigma$ then Ω is a homomorphism since then

$$\forall x \in dom(\theta_{a*b}) : \theta_{a*b}(x) = (a * b) * x = a * (b * x) = \theta_a(\theta_b(x))$$

So we show $(ab)^{-1} = b^{-1}a^{-1}$ for $a, b \in \Sigma$ in Isabelle/HOL.

— Again a little bit of providing direction is needed.
lemma *helpInvSwitch: "(a ⊗ b) ⊗ ((inv b) ⊗ (inv a)) ⊗ (a ⊗ b) = (a ⊗ b)"*
by *(metis Associativity IdemComm InvInv Regularity)*

lemma *InvSwitch: "(inv (a ⊗ b)) = (inv b) ⊗ (inv a)"*
by *(smt Associativity InvInv Regularity helpInvSwitch InverseIsUnique)*

end

It remains to show $a \leq b \iff \Omega(a) \subseteq \Omega(b)$. We start with the direction from left to right.

So suppose $a \leq b$. First we want to prove $dom(\theta_a) \subseteq dom(\theta_b)$ For that fix $x \in a^{-1}a\Sigma$. So $x = a^{-1}am$ for some $m \in \Sigma$. Because of the assumption we get by lemma 2.3.4 that $a^{-1}a = b^{-1}be$ for some idempotent $e \in \Sigma$. As a result $x = b^{-1}bem$ and therefore, $x \in b^{-1}b\Sigma$.

Now that we have established the subset relationship we fix $y = a^{-1}am \in a^{-1}a\Sigma$. Then $\theta_a(y) = (aa^{-1}a) * y$. By the assumption we have $a = bf$ for some idempotent $f \in \Sigma$ which implies $a = af$. These two facts yield that

$$(aa^{-1}a) * y = bfa^{-1}a * y = b(af)^{-1}a * y = ba^{-1}a * y = b(a^{-1}aa^{-1}am) = b * y = \theta_b(y).$$

In total we have shown $\theta_a \subseteq \theta_b$.

For the other direction suppose $\theta_a \subseteq \theta_b$. Then by assumption $a^{-1}a\Sigma \subseteq b^{-1}b\Sigma$. Since $a^{-1} \in a^{-1}a\Sigma$ we get the following implications:

$$\begin{aligned} & \theta_a(a^{-1}) = \theta_b(a^{-1}) \\ \Rightarrow \quad & aa^{-1} = ba^{-1} \\ \Rightarrow \quad & a = ba^{-1}a \\ \Rightarrow \quad & a \leq b. \end{aligned}$$

This concludes the proof. □

Recall that the inclusion property of a functional modeloid M on Σ was given as

$$f \in M \text{ and } A \subset dom f \text{ implies } f|_A \in M.$$

We have introduced notation for partial bijections such that we can rewrite this formally as

$$(f \in M \ \wedge \ g \subseteq f) \Longrightarrow g \in M.$$

At this point the above axiom is in a form that can be quite naturally seen in inverse semigroup language. Though there is some information required in the above that is not available in an inverse semigroup. That is if we consider $g \subseteq f$. The problem is that the domain is not given explicitly anymore in semigroup language. Therefore, it is necessary to ask what g is an element of. And indeed implicitly also the above statement can actually be written as

$$\forall f \in M \, \forall g \in F(\Sigma) : g \subseteq f \Longrightarrow g \in M. \tag{2.1}$$

In this form the dependency of a functional modeloid on $F(\Sigma)$ can be seen explicitly. In translating 2.1 this has to be part of the statement. These considerations lead to the fact that a modeloid in semigroup theory is the subset of an inverse semigroup. So let $M \subset S$ where S is an inverse semigroup. Then 2.1 can be stated as

$$\forall f \in M \, \forall g \in S : g \leq f \Longrightarrow g \in M. \tag{2.2}$$

It is immediate that a functional modeloid, seen as an inverse semigroup, fulfills 2.2 by the following proposition.

Proposition 2.4.2. *Let M be a functional modeloid on $F(\Sigma)$ for some alphabet Σ. Then for $f, g \in M$*

$$g \leq f \Longleftrightarrow g \subseteq f$$

Proof. Let Σ be an alphabet and M a functional modeloid on $F(\Sigma)$. We have already established that $(M, {}^{-1}, \circ)$ is an inverse semigroup. Fix $f, g \in M$. Supposing that $g \leq f$ holds we know $g = f \circ e$ where e is an idempotent. As such e is a partial identity in M by lemma 2.2.1. As a result

$$dom(g) = e^{-1}(dom(f) \cap cod(e)) = dom(f) \cap cod(e)$$

and hence $dom(g) \subseteq dom(f)$. Furthermore, $g(x) = (f \circ e)(x) = f(x)$ for $x \in dom(g)$. This yields $g \subseteq f$.

Conversely suppose that $g \subseteq f$. Since $id_{dom(g)} \subseteq id_\Sigma$ we know that $id_{dom(g)} \in M$. In addition, the partial identity is idempotent by lemma 2.2.1. Now $f \circ id_{dom(g)} \in M$ and $g = f \circ id_{dom(g)}$ because $dom(g) = dom(f) \cap cod(id_{dom(g)})$ since $dom(g) \subseteq dom(f)$ and $g(x) = f(x) = f(id_{dom(g)}(x))$ for $x \in dom(g)$. As a result $g \leq f$ holds. □

One more fact to take care of is that in a functional modeloid M the axiom 2.1 implies that the empty partial bijection we denoted by 0 is also included in M. As a result we want to establish a similar behavior in an inverse semigroup. The deeper reason for this is the definition of the derivative operation in Section 2.5. Seeing M as an inverse semigroup 0 is an idempotent element for which the following property holds: $\forall x \in M : 0 * x = 0$. Hence in an inverse semigroup we will call the idempotent with this property the zero element. When defining a modeloid in semigroup language we will require the zero element to be part of it.

Turning to axiom 4 which is $id_\Sigma \in M$ we want to examine which element of an inverse semigroup S is most suitable for this task. To evaluate we again look at the functional modeloid M regarded as an inverse semigroup. In this semigroup id_Σ will be an idempotent e satisfying $\forall x \in M : e * x = x$. We know this element from group theory. It is the neutral element in that context. As a result we will require for the inverse semigroup which we want to call a modeloid that e is part of it. What we get is known as an inverse monoid in the literature.

Remark 2.4.3. *Given an inverse monoid called S^1 and the element e with $e * x = x$, $\forall x \in S^1$ consider the representation theorem again. This theorem does not give uniqueness of the embedding and in fact there can be several. As a result we can not suppose that e will be mapped to the identity id_Σ. However, for all idempotent $f \in S^1$ we have that $f \leq e$. That way e is an element that will always resemble the upper bound of all idempotents in S^1.*

We have prepared everything needed for defining a modeloid again. We shall call it a semimodeloid. Note, as mentioned before, that a functional modeloid is a subset of $F(\Sigma)$ for some alphabet Σ and, as discussed, we keep this subset property to state the inclusion axiom.

Definition 2.4.4 (Semimodeloid)**.** Let $S^1 = (\Sigma, {}^{-1}, *, e, 0)$ be an inverse monoid. Then a semimodeloid $M \subseteq \Sigma$ has to satisfy

1. $\forall x, y \in M : (x * y) \in M$
2. $\forall x \in M : x^{-1} \in M$
3. $\forall x \in M \, \forall y \in S^1 : y \leq x \Rightarrow y \in M$
4. $e \in M$

Remark 2.4.5. *A semimodeloid is again an inverse monoid with the zero element. Furthermore, by the considerations above, every functional modeloid is a semimodeloid.*

What we have built is a structure that resembles the main properties of a functional modeloid. This can be seen by the Wagner-Preston representation theorem which is the reason for its importance. The next section will deal with the derivative on functional modeloids and how this operation can be stated in the context of a semimodeloid.

2.5 The derivative on semimodeloids

Recall the definition of the derivative on a functional modeloid M on Σ (1.4). $D(M)$ was the set defined by

$$\begin{aligned}\{(x_1,y_1),..,(x_{l(x)},y_{l(y)})\} \in D(M) :\Leftrightarrow \\ \forall a \in \Sigma\, \exists b \in \Sigma : \{(x_1,y_1),..,(x_{l(x)},y_{l(y)}),(a,b)\} \in M \wedge \\ \forall a \in \Sigma\, \exists b \in \Sigma : \{(x_1,y_1),..,(x_{l(x)},y_{l(y)}),(b,a)\} \in M\end{aligned}$$

The main thing we can see is that the elements of Σ are of crucial importance. Furthermore, we are required to be able to extend the domain of a function by one element at a time. This poses a challenge because in an inverse monoid this information is not directly accessible. But as we shall see it is possible to obtain.

First we want to characterize the elements of Σ. Therefore, consider $F(\Sigma)$ and realize that all the singleton-identities $id_{\{a\}}$ for $a \in \Sigma$ are in natural bijection to the elements of Σ. Now what is the special property of such a singleton-identity? The answer is that

$$\forall f \in F(\Sigma) : f \subseteq id_{\{a\}} \Rightarrow (f = id_{\{a\}} \vee f = 0)$$

since $dom(id_{\{a\}}) = \{a\}$. Seeing $F(\Sigma)$ as an inverse monoid with zero element we can formulate it the following way.

Definition 2.5.1 (atomic[12])**.** Let S^1 be an inverse monoid with zero element 0. Then a non-zero element $x \in S^1$ is called atomic if and only if

$$\forall f \in S^1 : f \leq x \Rightarrow (f = x \vee f = 0)$$

Our plan is to use the notion of atomic to define the derivative. The next lemma will justify this usage.

Lemma 2.5.2. *The idempotent atomic elements in $F(\Sigma)$ are exactly the singleton-identities.*

Proof. By lemma 2.2.1 idempotent elements in $F(\Sigma)$ are the partial identities. So it suffices to show that $|dom(f)| = 1$ if and only if the idempotent $f \in F(\Sigma)$ is atomic. Assume $f \in F(\Sigma)$ is atomic and idempotent. Suppose now that $|dom(f)| > 1$.

[12] Cori and Lascar, *Mathematical Logic: Part 1: Propositional Calculus, Boolean Algebras, Predicate Calculus, Completeness Theorems*, p.79.

Then we can find $a, b \in dom(f)$ with $a \neq b$. But then we have that $id_{\{a\}} \subsetneq f$ and $id_{\{a\}} \neq 0$. This is a contradiction to f atomic. The case $|dom(f) = 0|$ implies that $f = 0$ but an atomic element is unequal to the zero element. As such that case is also taken care of.
Conversely assume $|dom(f)| = 1$ for some non-zero partial identity $f \in F(\Sigma)$. Then $g \subseteq f$ implies that $dom(g) = \varnothing \vee dom(g) = dom(f)$. If it is the first option we have $g = 0$. And if it is the second we get $g = f$. □

The plan now is to define the derivative for semimodeloids and then show that the definition matches the definition 1.4 if the semimodeloid is on $F(\Sigma)$.

Definition 2.5.3 (Derivative on semimodeloid)**.** Let M be a semimodeloid on the inverse monoid S^1 with zero element 0. Then we define the derivative of M to be

$$\begin{aligned} &D(M) := \\ &\quad \{f \in M \mid \forall \text{ idempotent and atomic } a \in S^1 \, \exists x \in M : (f \leq x \wedge a \leq x^{-1}x) \wedge \\ &\qquad\qquad \forall \text{ idempotent and atomic } b \in S^1 \, \exists y \in M : (f \leq y \wedge b \leq yy^{-1}) \end{aligned}$$

Proposition 2.5.4. *The derivative on a functional modeloid M produces the same result as the semimodeloidal derivative on M.*

Proof. Let M be a functional modeloid on $F(\Sigma)$ for an alphabet Σ. We want to show that the two definitions of the derivative are equivalent in this case. It suffices to show that for fixed $f \in M$

$$\begin{gathered} \forall a \in \Sigma \, \exists b \in \Sigma : f \cup \{(a, b)\} \in M \\ \Longleftrightarrow \\ \forall \text{ idempotent and atomic } b \in F(\Sigma) \, \exists x \in M : (f \leq x \wedge b \leq x^{-1}x) \end{gathered}$$

because the second part of the definition of the derivative follows by analogy.

To start remember the natural bijection

$$\Psi : \Sigma \simeq \{p \in F(\Sigma) \mid p \text{ atomic and idempotent } \}.$$

Suppose the upper formula holds. Fix $a \in \Sigma$. Then setting $x := f \cup \{(a, b)\}$ yields that $f \leq x$ by proposition 2.4.2. Furthermore, $a \in dom(x) = dom(x^{-1}x)$. But then $\Psi(a) \leq x^{-1}x$. Hence we get that $\exists x \in M : (f \leq x \wedge \Psi(a) \leq x^{-1}x)$. But now we can quantify over $\{p \in F(\Sigma) \mid p \text{ atomic and idempotent } \}$ instead of Σ which yields the desired result.
Conversely suppose the bottom formula holds. Then fix an idempotent and atomic element $b \in F(\Sigma)$ and let x be the element with $f \leq x \wedge b \leq x^{-1}x$. It holds that $x|_{dom(f) \cup \Psi^{-1}(\{b\})} \in M$ because of the inclusion property. But this already yields that

$$f \cup \{(\Psi^{-1}(b), x(\Psi^{-1}(b)))\} \in M.$$

Quantifying over Σ instead of $\{p \in F(\Sigma) \mid p \text{ atomic and idempotent } \}$ concludes the proof.

□

As a result we consider the derivative on a semimodeloid as the correct generalization. It does what we expect on a functional modeloid. An interesting question to pursue is whether the derivative of a semimodeloid yields a semimodeloid again. This is believed to be true and the reader is encouraged to try to prove it but we shall only prove a similar fact in the next chapter for a modeloid then formulated in category theory. We end this chapter with a small discussion on how a semimodeloid can be seen in the context of partial symmetries.

2.6 Interlude: Symmetry and modeloids

In this section we want to informally talk about how the structure of a semimodeloid can be seen in the context of partial symmetries of a geometry and especially what the derivative operation does in this setting. A partial symmetry is a structure-preserving partial bijection in some geometry. The important fact is that the set of partial symmetries of a geometry forms an inverse semigroup S. Now we want to define a semimodeloid on S. That means we take a subset of the partial symmetries of the geometry chosen. This subset has to be closed under composition and inversion of partial symmetries. Furthermore, the inclusion property states that for a given symmetry all the resulting restricted symmetries should also be part of the semimodeloid. Keeping the neutral element in a semimodeloid comes down to having the self-symmetry included. That is using the identity function on the geometry. Now what is really of interest is what the derivative operation does. If a symmetry l is part of the derivative of a semimodeloid then this symmetry can be extended. This means that we can take any other point in the geometry and know that there is a symmetry L such that this point is in the domain of L and L and l coincide whenever l is defined. At the same time the chosen point is also in the codomain of some other symmetry K such that K and l also coincide wherever l is defined. As a result, taking the derivative multiple times can be thought of as extending the symmetry by a certain amount of *area* where the *area* can be arbitrarily placed within the geometry. As we shall see, this view can be taken in model theory where such a geometric perspective is perhaps not expected.

3 Categorical Axiomatization of a Modeloid

This chapter will show how to generalize a semimodeloid to category theory. We will make use of Isabelle/HOL again using the categorical framework developed by Benzmüller and Scott[1][2][3] and will extend it to represent an inverse category. An inverse category is the natural generalization of an inverse semigroup to category theory as will be shown. It is this environment that a categorical modeloid will be defined in. We then formulate the derivative again for this setting and show that this operation will yield a categorical modeloid again.

The reader is assumed to have a basic understanding of category theory. Definitions for terms that are not defined in this chapter have been taken from Riehl, *Category Theory in Context*.

3.1 Introduction to category theory in Isabelle/HOL

When looking at the definition[4] of a category $\mathbf{C}$, one can realize that the objects $A, B, C, ..$ are in natural bijection with the identity morphisms $\mathbf{1}_A, \mathbf{1}_B, \mathbf{1}_C, ...$ because these morphisms are unique. This gives rise to the fact that a category can be characterized just by its morphisms and their compositions. This fact can be used to establish a formal axiomatization of a category. A challenge one has to deal with when using this axiomatic approach however is that of partiality. That is because the composition between two morphisms $f, g \in \mathbf{C}$ is defined if and only if

$$\mathrm{dom}(g) = \mathrm{cod}(f). \tag{3.1}$$

As a result the composition is a partial operation.

One way to deal with this issue is to change the underlying logic to *free logic*.[5] That is that we want to introduce a notion of existence for the objects in the domain that we quantify over. In our case the domain will be the morphisms of a category. Now the idea is to define the composition total that is that any two morphisms can be composed but to have only those compositions exist that satisfy 3.1. Because we can distinguish between existing and non-existing morphisms we are able to formulate statements that take only existing morphisms

[1] Benzmüller and D. S. Scott, "Axiom Systems for Category Theory in Free Logic".
[2] Benzmüller and D. S. Scott, "Automating Free Logic in HOL, with an Experimental Application in Category Theory".
[3] Benzmüller and D. S. Scott, *Axiomatizing Category Theory in Free Logic*.
[4] taken from Riehl, *Category Theory in Context*, p. 3.
[5] D. Scott, "Existence and Description in Formal Logic".

into account. Due to the achievement of finding a shallow embedding of free logic in Isabelle/HOL by Benzmüller and Scott first order axiomatic category theory could also be implemented.[6]

Using this work a category in Isabelle/HOL can be defined as follows.

typedecl α — This type can be thought of to represent the morphisms of a category.

```
locale category =
        — We need three functions to define a category.
  fixes domain:: "α ⇒ α" ("dom _" [108] 109) and
        codomain:: "α ⇒ α" ("cod _" [110] 111) and
        composition:: "α ⇒ α ⇒ α" (infix "·" 110) and
        star::α ("*") — Symbol for non-existing elements

assumes
— Here we define the axioms that the morphisms in interaction with the functions have to obey.
        S1: "E(dom x) ⟶ E x" and
        S2: "E(cod y) ⟶ E y" and
        S3: "E(x·y) ⟷ dom x ≃ cod y" and — Here condition 3.1 can be seen.
        S4: "x·(y·z) ≅ (x·y)·z" and
        S5: "x·(dom x) ≅ x" and
        S6: "(cod y)·y ≅ y" and

— We add one more axiom that is not present in the original formulation. We want all non-existing morphisms to be equal.
        L1: "¬(E m) ⟶ (m = *)"
begin
— We show consistency.
lemma "True" nitpick[satisfy] oops

— As desired non-existing morphisms are equal.
lemma "(¬(E x) ∧ ¬(E y)) ⟶ (x = y ∧ x = *)"
  using L1 by blast

end
```

We want to give a brief explanation of the symbols used. Again this will be a short treatment and we refer to Benzmüller and D. S. Scott, "Automating Free Logic in HOL, with an Experimental Application in Category Theory" and Benzmüller and D. S. Scott, *Axiomatizing Category Theory in Free Logic* for a more complete account. It is worth noting that the following functions were defined polymorphic in order for the free logic implementation to be used type independent. This is why `'a` appears in the following as the type of the variables.

- The predicate `E` is defined as `E :: 'a ⇒ bool` and tells us whether or not the individual passed as a parameter exists.
- `(≃)` is called the *existing identity* and is defined as

$$(\simeq) \equiv \lambda x::'a\ y::'a.\ E\ x \wedge E\ y \wedge x = y.$$

[6] Benzmüller and D. S. Scott, "Automating Free Logic in HOL, with an Experimental Application in Category Theory".

Therefore, it is only true if both elements being compared exist and are equal.

- `(≅)` is called the *Kleene equality* and is defined as

$$\texttt{(≅)} \equiv \lambda\texttt{(x::'a) y::'a. (E x} \vee \texttt{E y)} \longrightarrow \texttt{x = y.}$$

  Therefore, this equality does not imply the existence of the elements being compared.

Moreover, we will encounter ∀ and ∃ which have been redefined to quantify only over the existing individuals. This is done by defining

$$\forall \equiv \lambda\Phi\texttt{::'a} \Rightarrow \texttt{bool. } \forall\texttt{x::'a. E x} \longrightarrow \Phi\ \texttt{x}$$

and

$$\exists \equiv \lambda\Phi\texttt{::'a} \Rightarrow \texttt{bool. } \neg\ \texttt{(}\forall\ \texttt{(}\lambda\texttt{y::'a. } \neg\ \texttt{(}\Phi\ \texttt{y)))}.$$

Note that writing $\forall\,$`x::'a. (Φ::'a ⇒ bool) x` really means $\forall\,\Phi$`::'a ⇒ bool` since we have the quantification in the definition of ∀. The situation is analogue for ∃.

3.2 Two axiomatizations of an inverse category

Given this framework our goal is to show that by adding to a category the axioms of an inverse semigroup that are responsible for shaping the inverse (definition 2.1.3, axioms 2), 3) and 4)) we arrive at a category that is equivalent to the definition of an inverse category.[7]

Definition 3.2.1 (Inverse category[8])**.** A small category **C** is called an inverse category if for any morphism $s : X \to Y \in \mathbf{C}$ there exists a unique morphisms $\hat{s} : Y \to X$ such that $s = s \cdot \hat{s} \cdot s$ and $\hat{s} = \hat{s} \cdot s \cdot \hat{s}$.

We will rewrite this in order to avoid to run into the problem with skolemization again as we did in 2.1. In Isabelle/HOL we define the inverse in the `locale category` and then go on to define an inverse category.

```
abbreviation (in category) inverseDef::"α ⇒ α ⇒ bool" ("_ inverseOf _")
  where "t inverseOf s ≡ s ≅ s·(t·s) ∧ t ≅ t·(s·t)"

locale inverseCategory = category +
  fixes inverse::"α ⇒ α" ("inv _")
  assumes  uniqueInv:
     "∀s. (((inv s) inverseOf s) ∧ (∀w. (w inverseOf s) → w ≅ (inv s)))"
```

— exNot: "$\exists x :: \alpha.\neg(Ex)$" was also tested as an axiom and nitpick confirmed satisfiability

```
begin
lemma "True" nitpick[satisfy] oops
```

— We prove that the existence of a morphism implies the existence of its inverse and the converse.

[7] This idea is due to Dana Scott.
[8] Kastl, "Inverse categories".

```
lemma exInv: "(E x) ⟶ (E (inv x))"
  by (metis S1 S2 S3 uniqueInv)

lemma "E (inv x) ⟶ (E x)"
  by (metis S1 S3 uniqueInv)

end
```

Next we want to prove that the set of axioms used in an inverse semigroup to characterize the inverse also hold in an inverse category.

```
context inverseCategory begin

proposition Regularity: "x·((inv x)·x) ≅ x"
  by (metis uniqueInv)

proposition InvInv: "((inv (inv x)) ≅ x)"
  by (metis uniqueInv)

proposition IdemComm:
  "((x·inv x)·(y·(inv y))) ≅ ((y·(inv y)) · (x·(inv x)))" oops
```

The last proposition cannot be proven at this moment by automation. The case is very similar to what we have already encountered in the proof of proposition 2.1.9. And in fact in this section we did the proof by hand. The same proof works here in analogy once we establish that given a morphism x in an inverse category it holds that $x \cdot \hat{x}$ is idempotent.

```
abbreviation (in category) Idem::"α ⇒ bool" ("Idem _")
  where "Idem x ≡ (x · x ≅ x)"

lemma compIdem: "(Idem (x·(inv x)))"
  by (metis S2 S3 S4 uniqueInv)
end
```

Hence we have shown that those three inverse semigroup axioms hold in an inverse category. Next we want to show that the converse also works and therefore we will have found a quantifier free axiomatization of an inverse category.

```
locale inverseCategoryQantFree = category +
  fixes inverse::"α ⇒ α" ("inv _")
  assumes C1: "x·((inv x)·x) ≅ x" and
          C2: "((inv (inv x)) ≅ x)" and
          C3: "((x·inv x) · (y·(inv y))) ≅ ((y·(inv y)) · (x·(inv x)))"
begin
lemma "True" nitpick[satisfy] oops

— We show the strictness of E for the inverse
lemma "(E x) ↔ (E (inv x))"
  by (metis C1 C2 S1 S2 S3)

— We need to build some theory in this context to show the result
lemma IdemComp: "Idem (x · (inv x))"
  by (smt S1 S3 S4 C1)
```

```
lemma (in inverseCategoryQantFree) IdempotentsCommute:
  "((E x) ∧ (E y) ∧ (Idem x) ∧ (Idem y)) → (x·y ≅ y·x)"
    by (smt C3 S1 S2 S3 S4 inverseCategoryQantFree.C1
        inverseCategoryQantFree.C2 inverseCategoryQantFree_axioms)


lemma inverseUnique: "((y inverseOf x) ∧ (z inverseOf x)) → (y ≅ z)"
  by (metis IdempotentsCommute S1 S2 S3 S4)
```

— The next proposition is the result we wanted to show.

```
proposition  inverseUnique2:
  "∀s. (((inv s) inverseOf s) ∧ (∀w. (w inverseOf s) → w ≅ (inv s)))"
  by (smt C1 C2 S1 S2 S3 inverseUnique)

end
```

3.3 Inverse category as a generalization of an inverse semigroup

A category can be seen as a generalization of a monoid in the sense that a one object category is a monoid. After what we have seen the inverse category seems to be a generalization of an inverse semigroup. We will prove now that this is indeed true.

Proposition 3.3.1. *Let* **C** *be an inverse category with exactly one object. Then* **C** *is an inverse semigroup.*

We will try to do the proof by inclusion of locales in Isabelle/HOL. Therefore we will define an inverse category for which we require to have exactly one object and then show that this is a sublocale of an inverse semigroup. Note that in this case we can assume all morphisms to exist because the composition is total if there is just one object. We make use of the element $*$ which represents the non-existing element if a non-existing element is present. Because we assume all morphisms to exist we can use $*$ to represent the single existing object. Also note that as a result the quantifiers for free logic collapse to the quantifiers of classical logic in a one-object inverse category.

```
locale inverseCategoryOneObject = inverseCategoryQantFree +
  assumes only_star: "(E *) ∧ (∀x. dom(x) = * ∧ cod(x) = *)"
begin
lemma "True"  nitpick[satisfy] oops

lemma "∀x::α. (E x)"
  using S1 only_star by auto

lemma associative: "((x·y)·z) = (x·(y·z))"
  using S2 S4 only_star by auto
```

— It is possible to have more than just one morphism. Exactly what we want.

```
lemma "∀x::α. x = star" nitpick oops

end
```

```
sublocale inverseCategoryOneObject ⊆ inverseSemigroup "inverse" "composition"
proof -
  have f1: "∀a. E (a::α)"
    by (metis S2 only_star)
  then have f2:
      "∀x. ∀y. ((y · ((inv y) · (x · (inv x))) = (x · ((inv x) · (y · (inv y))))))"
        using C3 associative by auto
  then show "inverseSemigroup inverse (·)"
    using f1 by (simp add: C1 C2 associative inverseSemigroup.intro)
qed
```

We have succeeded to prove that an inverse category with one element is a semigroup with the Isabelle/HOL command `sledgehammer`. It gave back a Isar proof in which we had to slightly correct parentheses but except for that it worked out of the box.

As a result we may now try to formulate the semimodeloidal axioms in the context of inverse categories. The outcome we want is that these axioms in a one object inverse category will form a semimodeloid.

3.4 Categorical modeloid

We will leave the focus on Isabelle/HOL for now but we want to keep the underlying logic and introduced symbols and functions. As a result a small category $\mathbf{C}$ will be a structure $(C, dom, cod, \cdot, \star)$ satisfying the axioms introduced in Isabelle/HOL and an inverse category $\mathbf{C}$ respectively $(C, dom, cod, \cdot, \star, {}^{-1})$. When convenient we will use the framework though.

To ease writing a morphism $f : X \to Y$ in a category $\mathbf{C}$ (so $f \in C$) will be from now on an *existing* morphism meaning that (Ef) is true. If there is a non-existing element $\star$ in the category $\mathbf{C}$ (recall that there can only be one) we also have the unique *non-morphism* $\star : \star \to \star$. Furthermore, writing for a morphism $f : X \to Y$ means that $(dom f) \simeq X$ and $(cod\, f) \simeq Y$ (Respectively for the non-morphism $\star$ we have that $dom \star = \star$ and $cod \star = \star$). As a result, it needs to be assumed that $X, Y \in C$. In addition, X and Y can be seen as fix points for the functions dom and cod. That is because

$$dom(f) \simeq X \Rightarrow dom(X) \simeq X (\Rightarrow cod(X) \simeq X)$$

and

$$cod(f) \simeq Y \Rightarrow cod(Y) \simeq Y (\Rightarrow dom(Y) \simeq Y).$$

Hence for X to be an object in $\mathbf{C}$ we require that $X \in C$ satisfies $X \simeq (dom\, X)$. This states that an object always exists in terms of free logic. To make the distinction more clear when quantifying we write $\forall_f$ and $\exists_f$ for the quantifiers in free logic.

We have a result on when the non-morphism is part of a category.

Lemma 3.4.1. *Let* $\mathbf{C}$ *be a category. Then having at least two different objects in* $\mathbf{C}$ *implies that* $\neg(E\star)$.

Proof. Assume that we have two different objects X and Y. Then $Y \cdot X$ is non-existing because $cod(X) \not\cong dom(Y)$ and hence $Y \cdot X = \star$. As a result $\star$is non-existing. □

In order to formulate the semimodeloidal axioms we need a partial order on the morphisms of an inverse category. There is a natural translation of the natural partial order on inverse semigroups to inverse categories.[9]

Definition 3.4.2. Let $\mathbf{C}$ be an inverse category and let $s, t : X \to Y$ be elements in $\mathbf{C}$. Then we define

$$s \leq t :\Leftrightarrow \exists \text{ idempotent } e \in End_C(X) : s \cong t \cdot e$$

where $End_C(X) := \{m \in C \,|\, m : X \to X \text{ is morphism or non-morphism }\}$ is called an Endoset. This way $End_C(\star)$ is always defined. The proof that $\leq$ defines a partial order again is very similar to the one done for the natural partial order in Lawson, *Inverse Semigroups*, p. 22 and is left to the reader. It is to note that this definition was designed to always yield $\star \leq \star$.

We will now define a categorical modeloid M on an inverse category $\mathbf{C}$ and then show that for each object X in $\mathbf{C}$, $End_C(X)$ will be a semimodeloid. As in the case of a semimodeloid we will require the inverse category to be finite meaning that the underlying set $|C|$ is finite and to have a zero element in each of its Endosets. For this we simply write that $\mathbf{C}$ has all zero elements.

Definition 3.4.3 (categorical modeloid)**.** Let $\mathbf{C}$ be a finite inverse category $\mathbf{C}$ with all zero elements. Then a *categorical modeloid* M on $\mathbf{C}$ is such that $M \subseteq C$ satisfies the following axioms.

1. $a, b \in M \Rightarrow a \cdot b \in M$
2. $a \in M \Rightarrow a^{-1} \in M$
3. $\forall_f\, a \in C\, \forall_f b \in M : a \leq b \Rightarrow a \in M$
4. $\forall_f$ objects $X \in C : X \in M$

Proposition 3.4.4. *Let* $\mathbf{C}$ *be a finite inverse category with all zero elements and* M *be a categorical modeloid on* $\mathbf{C}$*. Then for each object* X *in* M *we get that* $End_M(X)$ *is a semimodeloid (on itself).*

Proof. Fix an object X in M. Once we have proven that $End_M(X)$ is an inverse monoid it will follow that $End_M(X)$ is a semimodeloid. That is because $End_M(X)$ then is closed under composition and taking inverses. Furthermore, the definition of the partial order defined on morphisms above will simply reduce to the natural partial order. As a result the inclusion axiom also holds. And at last we have

[9] Linckelmann, "On inverse categories and transfer in cohomology", Section 2.

that $X \in End_M(X)$ with the property that $y \cdot X \simeq y$ for all $y \in End_M(X)$ hence giving us the neutral element required by a semimodeloid.

Let's now prove that $End_M(X)$ is an inverse monoid. First we will show the closure of the composition. For that fix two elements $a, b \in End_M(X)$. We know that $dom(a) \simeq dom(b) \simeq cod(a) \simeq cod(b) \simeq X$. As a result $a \cdot cod(a \cdot b)$ exists and therefore $dom(a) \simeq cod(cod(a \cdot b))$. Because $cod(cod(x)) \simeq cod(x)$ for all morphisms x in a category, we get that $X \simeq cod(a \cdot b)$. In analogy one obtains $X \simeq dom(a \cdot b)$. Hence the composition is closed.

The closure of inverses is immediate because taken an element $s \in End_M(X)$, $s^{-1} \in M$ by assumption but $dom(s^{-1}) \simeq cod(s^{-1}) \simeq X$ and as a result $s^{-1} \in End_M(X)$. Now one can regard the inverse function on $End_M(X)$ as a restriction of $(^{-1})$ on $\mathbf{C}$. As a result the inverses are unique. Associativity follows by the fact that the composition in M really is the composition in $\mathbf{C}$ restricted to M. Above we have already taken care of the neutral element. □

Remark 3.4.5. *Every semimodeloid can easily be seen as a categorical modeloid by the fact that an inverse monoid with zero element is an one-object inverse category.*

Remark 3.4.6. *A categorical modeloid M can also be characterized in a different way by the fact that M forms an inverse subcategory. That M itself forms an inverse category with all zero elements is immediate by the closure of composition and taking inverses. Hence a categorical modeloid M on $\mathbf{C}$ is a subcategory of $\mathbf{C}$ satisfying that all the objects of $\mathbf{C}$ are also in M and the inclusion axiom (the third axiom of 3.4.3).*

We have achieved to formulate a generalization of a modeloid in category theory. What is left now is to define the derivative in this context. For this we need the notions of a Homset, an atomic element and idempotence.

Definition 3.4.7 (Homset)**.** Let $\mathbf{C}$ be a small category. Then the Homset between two elements $X, Y \in C$, satisfying $X \cong dom(X)$ and $Y \cong dom(Y)$, is defined as

$$Hom_C(X, Y) := \{m \in C \,|\, m : X \to Y \text{ is morphism or non-morphism }\}$$

As a result, an Endoset is a special case of a Homset. We only assumed zero elements to be present in Endosets and as a result an atomic element needs to part of an Endoset.

Definition 3.4.8 (Atomic)**.** Let $\mathbf{C}$ be an inverse category with all zero elements. Then an element $a \in End_C(X)$ for some $X \in C$ is called *atomic* if the existence of a implies that $a \ncong 0_{End_C(X)}$ and

$$\forall e \in End_C(X) : e \leq a \text{ implies that } e \cong a \vee e \cong 0_{End_C(X)}.$$

Definition 3.4.9 (Idempotence)**.** Let $\mathbf{C}$ be a small category. Then an element $e \in C$ is called idempotent if

$$e \cdot e \cong e.$$

In general we want to formulate definitions for a category in free logic in such a way that it is clear what happens to the non-existing element if it is there. We will see that it is useful to have the non-existing element also be idempotent and atomic. Note that this element is also a zero element in its Endoset. We are now equipped for the next definition.

Definition 3.4.10 (Derivative on Homset)**.** Let $\mathbf{C}$ be a finite inverse category with all zeros and let M be a categorical modeloid on $\mathbf{C}$. We define the derivative on $Hom_M(X,Y)$ for $X,Y \in M$ as

$$\begin{aligned} &D(Hom_M(X,Y)) := \\ &\qquad \{f \in Hom_M(X,Y) \mid \\ &\forall \text{ idempotent atomic } a \in End_M(X)\, \exists h \in Hom_M(X,Y) : (f \leq h \wedge a \leq h^{-1}h) \wedge \\ &\quad \forall \text{ idempotent atomic } b \in End_M(Y)\, \exists g \in Hom_M(X,Y) : (f \leq g \wedge b \leq gg^{-1})\} \end{aligned}$$

Remark 3.4.11. *Done on a finite inverse category* $\mathbf{C}$ *with just one object* X *and a zero element by proposition 3.4.4* $D(Hom_C(X,X))$ *reduces to the definition of the derivative on a semimodeloid.*

We have defined the derivative only on a Homset. This way the definition is more flexible. The key property of this operation is nevertheless that it gives a categorical modeloid again when we apply it to *all* Homsets simultaneously. We shall prove that next. But first we state a lemma taking care of technicalities that will appear.

Lemma 3.4.12. *Let* $\mathbf{C}$ *be an inverse category and* $\leq$ *the defined partial order on morphisms. Let* $a,b,s,t, \in C$*. Then the following statements hold*

1. *If* a *and* b *are idempotent then* $ab \cong ba$*.*
2. *The existence of* $t \cdot s$ *implies* $dom(ts) \simeq dom(s)$ *and* $cod(ts) \simeq cod(t)$
3. $(ts)^{-1} = s^{-1}t^{-1}$
4. $s : X \to Y$ *implies* $s^{-1} : Y \to X$
5. $s \leq t$ *implies* $s^{-1} \leq t^{-1}$
6. $s \leq t$ *implies* $s \cong ts^{-1}s$ *and* $s \cong ss^{-1}t$
7. $a \leq s$ *and* $b \leq t$ *implies* $ba \leq ts$

Proof. We will prove the statements in order by Isabelle/HOL.

```
context inverseCategoryQantFree
begin

— It is to note that we do not need to specify the domain and codomain of the idempotent.
abbreviation natOrder:: "α ⇒ α ⇒ bool" ("_ ≤ _" 111) where
  "(x ≤ y) ≡ (∃e. (Idem e) ∧  (x ≅ y·e))"


lemma Nr1: "((Idem a) ∧ (Idem b)) ⟶ (a·b = b·a)"
  by (metis IdempotentsCommute L1 S1 S2 S3)
```

```
lemma Nr2a: "(E (t·s)) ⟶  (dom(t·s) ≃ dom(s))"
  by (metis S2 S3 S4 S5)

lemma Nr2b: "(E (t·s)) ⟶ (cod(t·s) ≃ cod(t))"
  by (metis S1 S3 S4 S6)

lemma helpInvSwitch: "(s·t)·(((inv t) · (inv s))·(s·t)) ≅ (s·t)"
proof -
  have
 "(s·((t·(inv t)) · (((inv s)·s)·t))) ≅ ((s·(inv s))·s) · ((t · (inv t)) · t)"
    by (smt Nr1 S1 S3 S4 inverseUnique2)
  then show ?thesis
by (smt S1 S2 S3 S4 inverseUnique2)
qed

lemma Nr3: "(inv (t·s)) ≅ (inv s) · (inv t)"
  by (smt L1 helpInvSwitch inverseUnique2)

lemma Nr4a: "dom (inv (s)) ≅ cod(s)"
  by (metis S1 S2 S3 inverseUnique2)

lemma Nr4b: "(cod (inv s)) ≅ dom(s)"
  by (metis S1 S2 S3 inverseUnique2)

lemma Nr5: "(s ≤ t) ⟶ ((inv s) ≤ (inv t))"
  by (metis S2 S3 S4 inverseUnique2)

lemma Nr6a: "(s ≤ t) ⟶ (s ≅ (t·((inv s)·s)))"
  by (smt Nr1 L1 category.S4 category_axioms inverseUnique2)

lemma Nr6b: "(s ≤ t) ⟶ (s ≅ (s·((inv s)·t)))"
  by (smt C2 L1 Nr2b Nr3 Nr4b S1 S4 inverseUnique2)

lemma helpNr7:
assumes "(s ≤ t)" shows "(t · ((inv s) · s)) ≅ (s · ((inv s) · t))"
  by (smt Nr6a Nr6b assms)
```

— This proof is really hard for sledgehammer.

```
lemma Nr7: assumes f1: "((a ≤ s) ∧ (b ≤ t))" shows "((b·a)≤(t·s))"
proof-
  from f1 have f2: "a ≅ s · ((inv a) · a)"
    using Nr6a by auto
  from f1 have f3: "b ≅ (b · (inv b)) · t"
    by (smt Nr6b S4)
  have f4: "b·a ≅ ((b · (inv b))·t)·(s ·((inv a) · a))"
    by (metis L1 f2 f3)
  then have "(inv (b·a)) ≅ (inv (t·(s·((inv a)·a)))) · (b · (inv b))"
    by (smt L1 Nr3 category.S4 category_axioms inverseUnique2)
  then have "(inv (b·a)) ≤ (inv (t·(s·((inv a)·a))))"
    by (smt IdemComp)
  then have "(inv (inv (b·a))) ≤ (inv (inv(t·(s·((inv a)·a)))))"
    using Nr5 by auto
  then have f5: "(b·a)  ≤ (t·(s·((inv a)·a)))"
```

```
    by (metis C2 Nr2b S2)
  then have "∃e. (Idem e) ∧ b·a ≅ ((t·s)·e)"
    by (smt C1 C2 IdemComp L1 Nr1 Nr2b Nr3 Nr4a S3 S4  category.S1 category.S2
category_axioms f2 f4 inverseUnique2)
  then show ?thesis
    by blast
qed
end
```

□

Theorem 3.4.13. *Let* **C** *be a finite inverse category with all zero elements and let* M *be a categorical modeloid on* **C**. *Then*

$$\bigcup_{X,Y \in M} D(Hom_M(X,Y))$$

is a categorical modeloid on **C**.

Proof. Assume the assumptions formulated above. Then we define

$$H := \bigcup_{X,Y \in M} D(Hom_M(X,Y)).$$

We will prove (1) that all objects from **C** are in H, (2) the closure of taking inverses from H, (3) the closure of the composition on H and (4) the inclusion property hold which is

$$\forall_f s \in C \, \forall_f t \in H : s \leq t \Rightarrow s \in H.$$

1. Fix an object $X \in C$. Since M is a categorical modeloid, $X \in M$ and, furthermore $X \in End_M(X)$. We need to prove that $X \in D(End_M(X))$. So fix an idempotent and atomic $a \in End_M(X)$. We show that $X \leq X$ and $a \leq X^{-1}X$. Note that, since $X \simeq dom(X)$, X is idempotent by axiom $S5$ of a category. As a result $X = X \cdot X$ and hence $X \leq X$. On the other hand by definition of $End_M(X)$ we have that $y \simeq y \cdot X \simeq y \cdot X^{-1}X$. Because y is idempotent it commutes with $X^{-1}X$ by lemma 3.4.12 and hence by definition $y \leq X^{-1}X$. The second part of the condition posed by the derivative holds simply because $X^{-1}X = XX^{-1}$.

2. Next take an element $s \in H$. Then $s \in D(Hom_M(X,Y))$ for some $X, Y \in M$. As a result we can write s as $s : X \to Y$. We know that $s^{-1} : Y \to X \in Hom_M(Y,X)$ and want to show that $s^{-1} : Y \to X \in D(Hom_M(Y,X))$.

   Fix an idempotent and atomic element $a \in End_M(Y)$. Then, since $s \in H$, we find $h \in Hom_M(X,Y) : s \leq h \wedge a \leq hh^{-1}$. By lemma 3.4.12 $s^{-1} \leq h^{-1}$ and $h^{-1} \in Hom_M(Y,X)$. Because $a \leq hh^{-1}$ we know that $a \leq (h^{-1})^{-1}h^{-1}$. In total that yields

   $$\forall \text{ idempotent atomic } a \in End_M(Y) \quad \exists h' \in Hom_M(Y,X) : (s^{-1} \leq h' \wedge a \leq h'^{-1}h')$$

   The second condition required by the derivative follows by an analogous construction. Hence $s^{-1} \in H$.

3. Up now is the closure of the composition. Let $s, t \in H$. We want to show that $t \cdot s \in H$. We will do this by case analysis.

   Case 1: s or t does not exist. W.l.o.g. s is non-existent. Then $s = \star \in H$ and $t \cdot s = \star \in H$ because if $t \cdot s$ existed, so would t and s.

   Case 2: s and t exist but $dom(t) \not\simeq cod(s)$. This implies that there are two different objects in $\mathbf{C}$. By lemma 3.4.1 this means that $t \cdot s = \star \in C$, the unique non-existing element. Because by definition $s, t \in M$ and M is closed for composition this yields $\star \in M$.

   But then $\star \in Hom_M(\star, \star)$. Now we show that $\star \in D(Hom_M(\star, \star))$. Note that $End_M(\star) = \{\star\}$ and $\star$ is idempotent. As a result $\star$ is by default atomic. But because $\star \leq \star \wedge \star \leq \star\star^{-1}$ we get that $\star \in D(Hom_M(\star, \star))$ as desired since the second part of the derivative reduces to what we have just shown. As a result we have $t \cdot s \in H$.

   Case 3: s and t exist and $dom(t) \simeq cod(s)$. As a result the composition exists and we can write s as $s : X \to Y$ and t as $t : Y \to Z$ for $X \simeq dom(s), Y \simeq cod(s)$ and $Z \simeq cod(t)$. By lemma 3.4.12 $dom(ts) \simeq dom(s)$ and $cod(ts) \simeq cod(t)$. As a result we want to show that $t \cdot s \in D(Hom_M(X, Z))$. First we will prove

   $$\begin{aligned} &\forall \text{ idempotent atomic } a \in End_M(X) \\ &\qquad\qquad \exists h \in Hom_M(X, Z) : ((t \cdot s) \leq h \wedge a \leq h^{-1}h). \end{aligned} \tag{3.2}$$

   For that fix such an idempotent and atomic $a \in End_M(X)$. We use the assumptions about s now. That yields

   $$\exists f \in Hom_M(X, Y) : s \leq f \wedge a \leq f^{-1}f. \tag{3.3}$$

   The idea is now to construct something which can be thought of as applying f to a which will be idempotent and atomic in $End_M(Y, Y)$. This construction is $fa(fa)^{-1}$.

   First note that $fa(fa)^{-1} \simeq faa^{-1}f^{-1} \simeq faf^{-1}$. Using lemma 3.4.12 twice we get that $dom(faf^{-1}) \simeq dom(f^{-1}) \simeq Y$ and $cod(faf^{-1}) \simeq cod(f) \simeq Y$. As a result $faf^{-1} \in End_M(Y, Y)$.

   Next we wish to show that faf^{-1} is idempotent and atomic. For idempotence see that $faf^{-1} \cdot faf^{-1} \simeq fa \cdot af^{-1} \simeq faf^{-1}$ by using that from 3.3 $a \simeq f^{-1}fa$ by lemma 3.4.12 and the fact that a is idempotent.

   In order to show that faf^{-1} is atomic in $End_M(Y, Y)$ we assume $c \leq faf^{-1}$ for $c \in End_M(Y, Y)$ and show that $c \simeq faf^{-1} \vee c \simeq 0$ where 0 is the zero element of $End_M(Y, Y)$. So let $c \leq faf^{-1}$. Then by lemma 3.4.12

   $$c \leq faf^{-1} \Rightarrow f^{-1}c \leq af^{-1} \Rightarrow f^{-1}cf \leq a.$$

   But because a is atomic by assumption it follows that $f^{-1}cf \simeq a \vee f^{-1}cf \simeq 0$. The later implies that $c \simeq 0$. We prove this by contraposition.

   Suppose $c \not\simeq 0$. $c \simeq faf^{-1}c^{-1}c$ by lemma 3.4.12 and hence $f^{-1}c \not\simeq 0$ since otherwise $c \simeq 0$. Since c is idempotent by the fact that faf^{-1} is

idempotent, $(f^{-1}c)^{-1} \simeq cf$ and by axiom $C1$ of an inverse category $cf \not\simeq 0$. But $cf \simeq faf^{-1}cf$ and as a result $f^{-1}cf \not\simeq 0$.

We may now assume that $f^{-1}cf \simeq a$. As a result $f^{-1}cf$ is idempotent and atomic. We wish to show now that c is an inverse of faf^{-1} because this will yield that $c \simeq faf^{-1}$ by the fact that faf^{-1} is its own inverse and as such unique.

It is immediate that

$$faf^{-1} \cdot c \cdot faf^{-1} \simeq faaaf^{-1} \simeq faf^{-1}.$$

Furthermore,

$$\begin{aligned} & c \cdot faf^{-1} \cdot c \\ \simeq\ & faf^{-1}c \cdot faf^{-1} \cdot faf^{-1}c \\ \simeq\ & faf^{-1}c \cdot faf^{-1}c \\ \simeq\ & faf^{-1}c \\ \simeq\ & c. \end{aligned}$$

We conclude that faf^{-1} is indeed atomic, idempotent and an element of $End_M(Y,Y)$. We now use the assumption about t which yields

$$\exists k \in Hom_M(Y,Z) : t \leq k \ \wedge\ faf^{-1} \leq k^{-1}k. \tag{3.4}$$

We are now in the position to say that we can find h such that 3.2 is satisfied. For this set $h = kf$. Because $s \leq f$ and $t \leq k$ by 3.3 and 3.4 respectively we have that $t \cdot s \leq kf$. Furthermore, by 3.4 it holds that

$$\begin{aligned} & faf^{-1} \simeq k^{-1}kfaf^{-1} \\ \Rightarrow\ & faf^{-1} \simeq faf^{-1}k^{-1}kfaf^{-1} && (3.5) \\ \Rightarrow\ & af^{-1} \simeq af^{-1}k^{-1}kfaf^{-1} && (3.6) \\ \Rightarrow\ & a \simeq af^{-1}k^{-1}kfa && (3.7) \\ \Rightarrow\ & a \leq f^{-1}k^{-1}kf && (3.8) \\ \Rightarrow\ & a \leq h^{-1}h. \end{aligned}$$

3.5 follows by the fact that faf^{-1} is idempotent. 3.6 and 3.7 follow because $a = f^{-1}fa$. Then 3.8 follows because a is idempotent and by lemma 3.4.12.

Hence we proved 3.2. The second part of the derivative is proven in a similar way and we leave it to the reader to write down the details.

4. What is left to show is that the inclusion property holds in H. For this task fix a morphism $s \in C$ with the property that $s \leq t$ for some $t \in H$. Since M is a categorical modeloid and also $t \in M$ we know that $s \in M$. As a result we need to show that

$$s \in D(Hom(dom(b), cod(b)))$$

by the fact that $s \leq t$ implies that the domain and codomain of s and t are equal.

Since $t \in H$ we know that

$$\forall \text{ idempotent atomic } a \in End_M(dom(b)) \\ \exists f \in Hom_M(dom(b), cod(b)) : (b \leq f \wedge a \leq f^{-1}f)$$

and

$$\forall \text{ idempotent atomic } b \in End_M(cod(b)) \\ \exists k \in Hom_M(dom(b), cod(b)) : (b \leq k \wedge b \leq kk^{-1}).$$

Because $s \leq t$ and the fact that $\leq$ is a partial order we get that $s \leq f$ and $s \leq k$. But this already implies that $s \in D(Hom(dom(b), cod(b)))$.

□

As a consequence we will also define the derivative on a categorical modeloid.

Definition 3.4.14 (Derivative on a categorical modeloid)**.** Let $\mathbf{C}$ be an inverse category with all zeros and let M be a categorical modeloid on $\mathbf{C}$. Then we set the derivative as

$$D(M) := \bigcup_{X,Y \in M} D(Hom_M(X, Y)).$$

Taking the derivative m-times for some natural number m is defined in the same way as in chapter 1. With this result in our hands we may now proceed to the next chapter where we will see the categorical modeloid in action in the environment of finite model theory.

4 Application (Origin) in Finite Model Theory

We will now present how the idea of a categorical modeloid can be used in finite model theory. The derivative operation in its design[1] is closely connected to the back-and-forth method developed by Fraïssé[2] as we will see and hence also to Ehrenfeucht's game theoretical approach[3] to play an Ehrenfeucht-Fraïssé game (EF game).

As a result EF games can be played in the language of categorical modeloids using the derivative. It is this chapters goal to show this. Given that this is possible one can view a categorical modeloid as a generalization of EF games to arbitrary inverse categories on which such a modeloid can be defined.

We will start by explaining the idea of an EF game and then move on to prove the Ehrenfeucht-Fraïssé theorem with the help of *m-Hintikka formulas*.[4] After this is done we connect the derivative operation of a categorical modeloid to the back and forth method.

As a note to the reader all undefined terms in this section corresponds to the definitions in Libkin, *Elements of finite model theory*. Furthermore it is assumed that the reader is familiar with basic terminology in finite model theory which can otherwise also be found in this book.

In this chapter ω will always represent a relational vocabulary and τ a *finite* relational vocabulary.

4.1 Ehrenfeucht-Fraïssé games

Ehrenfeucht-Fraïssé games are a powerful tool in finite model theory. For example they can be used to prove expressibility results especially over finite structures. In this section, however, we will not be concerned with the application but want to focus on showing the connection to the derivative of a modeloid.

To play an EF game two ω-structures $\mathcal{A}$ and $\mathcal{B}$ are needed. In order to give an intuitive view we imagine two players which we will call the spoiler and the duplicator playing the game. The rules are quite simple. In $n \in \mathbb{N}$ rounds the spoiler tries to show that the two structures are not equal while the duplicator tries to disprove the spoiler every time. A round consists of the following:

[1] Benda, "Modeloids. I".
[2] Fraïssé, "Sur quelques classifications des systèmes de relations".
[3] Ehrenfeucht, "An application of games to the completeness problem for formalized theories".
[4] Hintikka, *Distributive Normal Forms in the Calculus of Predicates*.

- The spoiler picks either $\mathcal{A}$ or $\mathcal{B}$ and then makes a move by choosing an element from that structure, so $a \in \mathcal{A}$ or $b \in \mathcal{B}$.
- After the spoiler is done the duplicator picks an element of the other structure and the round ends.

Next we will define what the winning condition for each round will be. For convenience we define that $Part(\mathcal{A}, \mathcal{B})$ is the set of all partial isomorphisms from $\mathcal{A}$ to $\mathcal{B}$.

Definition 4.1.1 (Winning position[5])**.** Suppose the EF game was played for n rounds. Then the spoiler has chosen $(a_1, ..a_n)$ and likewise the duplicator has $(b_1, .., b_n)$. For this to be a winning position we require that the map

$$\{(a_1, b_1), .., (a_n, b_n), (c_1^{\mathcal{A}}, c_1^{\mathcal{B}}), .., (c_r^{\mathcal{A}}, c_r^{\mathcal{B}})\} \in Part(\mathcal{A}, \mathcal{B})$$

where the $c_i^{\mathcal{A}}$ are all constant symbols of ω interpreted by the structure $\mathcal{A}$ and likewise $c_i^{\mathcal{B}}$ for the structure $\mathcal{B}$.

In order to win the duplicator needs to defeat the spoiler in every possible course of the game. We say the duplicator has an *n-round winning strategy in the Ehrenfeucht-Fraïssé game on $\mathcal{A}$ and $\mathcal{B}$*[6] if the duplicator ends the game in a winning position regardless of what the spoiler does. This is made precise by the back-and-forth method due to Fraïssé.

Definition 4.1.2 (back-and-forth relation[7])**.**

We define a binary relation $\equiv_m$, $m \in \mathbb{N}$ on all ω-structures by $\mathcal{A} \equiv_m \mathcal{B}$ iff there is a sequence (I_j) for $0 \leq j \leq m$ such that

- Every I_j is a non-empty set of partial isomorphisms from $\mathcal{A}$ to $\mathcal{B}$
- (Forth property) $\forall j < m$ we have $\forall a \in \mathcal{A} \forall f \in I_{j+1} \exists g \in I_j : f \subseteq g \wedge a \in dom(g)$
- (Back property) $\forall j < m$ we have $\forall b \in \mathcal{B} \forall f \in I_{j+1} \exists g \in I_j : f \subseteq g \wedge b \in cod(g)$

Hence $\mathcal{A} \equiv_n \mathcal{B}$ means that the duplicator has a n-round winning strategy.

4.2 Hintikka-formula and the Ehrenfreucht-Fraïssé theorem

In order to see what kind of similarity the duplicator establishes between two ω-structures we introduce the notion of a Hintikka formula. In what follows we will need the central notion of the set $FO[k, m]_\omega$ denoting all first order formulas in at most m free variables with quantifier rank of at most k over ω. We just write $FO[k, m]$ if the vocabulary is clear.

[5] Libkin, *Elements of finite model theory*, p.27.
[6] Libkin, *Elements of finite model theory*, p. 28.
[7] Ebbinghaus and Flum, *Finite Model Theory*, p. 20.

Definition 4.2.1 (m-Hintikka formula[8]). Let $\mathcal{A}$ be an ω-structure and $x = (x_1, .., x_m) \in \mathcal{A}^m$. We define for $k > 0$

$$\varphi^k_{\mathcal{A},x} := \bigwedge_{a\in\mathcal{A}} \exists b\, \varphi^{k-1}_{\mathcal{A},xa} \wedge \forall b \bigvee_{a\in\mathcal{A}} \varphi^{k-1}_{\mathcal{A},xa}$$

and for $k = 0$

$$\varphi^0_{\mathcal{A},x} := \bigwedge\{\varphi \mid \varphi \in FO[0, m] \text{ and } \mathcal{A} \models \varphi[x]\}$$

Note that this definition is welldefined for $m = 0$ where x will be the empty tuple. By $\mathcal{A} \models \varphi[x]$ we mean $\mathcal{A}, x_1, .., x_m \models \varphi$.

Next we bring the formulations together in what is known as the Ehrenfeucht-Fraïssé theorem.[9]

Theorem 4.2.2 (Ehrenfeucht-Fraïssé theorem[10][11]). *Let $\mathcal{A}$ and $\mathcal{B}$ be two ω-structures and $k \in \mathbb{N}$. Then the following are equivalent.*

1. *$\mathcal{A}$ and $\mathcal{B}$ satisfy the same formulas in $FO[k, k]$.*
2. *$\mathcal{A} \equiv_k \mathcal{B}$*
3. *$\mathcal{B} \models \varphi^k_{\mathcal{A}}$*

Proof. [12] (1.) $\Rightarrow$ (3.): It is easy to see that $\varphi^k_{\mathcal{A}} \in FO[k, k]$ since assuming it holds for $k - 1$ yields $qr(\varphi^k_{\mathcal{A}}) = 1 + qr(\varphi^{k-1}_{\mathcal{A},a}) = k$. Furthermore, $\mathcal{A} \models \varphi^k_{\mathcal{A}}$ because $\mathcal{A} \models \varphi^0_{\mathcal{A},a}$ is true for all $a \in \mathcal{A}^k$. As a result by using the assumption we get $\mathcal{B} \models \varphi^k_{\mathcal{A}}$.

(3.) $\Rightarrow$ (2.): We will prove the statement by induction on k.

Base case is $k = 0$. We want to show $\mathcal{B} \models \varphi^0_{\mathcal{A}} \Longrightarrow \exists p \in Part(\mathcal{A}, \mathcal{B})$. First we claim that $\mathcal{B} \models \varphi^0_{\mathcal{A}}$ implies $\mathcal{A}$ and $\mathcal{B}$ satisfy the same atomic sentences.

$\mathcal{A} \models \varphi \Rightarrow \mathcal{B} \models \varphi$ is clear by the assumption. For $\mathcal{B} \models \varphi \Rightarrow \mathcal{A} \models \varphi$ suppose that there is a closed $\varphi \in FO[0, 0]$ with $\mathcal{A} \not\models \varphi$. Then $\mathcal{A} \models \neg\varphi$ since φ does not depend on any variable assignment. But $\neg\varphi \in FO[0]$ and by the assumption $\mathcal{B} \models \neg\varphi$ which is a contradiction.

Let $c_1, c_2, ...$ denote the constant symbols of ω and let $I_{\mathcal{A}}$ be the interpretation of $\mathcal{A}$ and $I_{\mathcal{B}}$ of $\mathcal{B}$. Define a function h by

$$I_{\mathcal{A}}(c_i) \mapsto I_{\mathcal{B}}(c_i)$$

where $i \in \mathbb{N}$. Since $\mathcal{A}$ and $\mathcal{B}$ satisfy the same atomic sentences h is by definition a partial isomorphism.

Hence the induction hypothesis is that for any two structures $\mathcal{A}$ and $\mathcal{B}$ it holds that $\mathcal{B} \models \varphi^k_{\mathcal{A}} \Rightarrow \mathcal{A} \equiv_k \mathcal{B}$.

[8] inspired by Ebbinghaus and Flum, *Finite Model Theory*, p. 18.
[9] Libkin, *Elements of finite model theory*, p. 32.
[11] Fraïssé, "Sur quelques classifications des systèmes de relations".
[11] Ehrenfeucht, "An application of games to the completeness problem for formalized theories".
[12] inspired by Kolaitis et al., *Finite Model Theory and its applications*, p. 38, 40.

Induction step is $k \mapsto k+1$. Assume $\mathcal{B} \models \varphi^{k+1}_{\mathcal{A}}$. We need to construct a $k+1$-round winning strategy. For that first fix $a \in \mathcal{A}$. Then the assumption implies that $\mathcal{B} \models \exists b\, \varphi^{k}_{\mathcal{A},a}$. This is equivalent to $\mathcal{B}, b \models \varphi^{k}_{\mathcal{A},a}$. But now we can use the induction hypothesis which yields $(A,a) \equiv_k (B,b)$ because $\equiv_k$ is symmetric. Denote by $(W^a_j)_{0\leq j\leq k}$ the associated sequence to $(A,a) \equiv_k (B,b)$ satisfying the back-and-forth property.

Next release a and fix $b \in \mathcal{B}$. Then it holds that

$$\mathcal{B}, b \models \bigvee_{a\in\mathcal{A}} \varphi^{k}_{\mathcal{A},a} \text{ implies } \mathcal{A} \models \exists a\, \varphi^{k}_{\mathcal{B},b}.$$

We leave the proof of this fact to the reader. Now we can proceed as above and find a sequence $(W^b_j)_{0\leq j\leq k}$ that satisfies the back-and-forth property.

Hence we find such a sequence for every $a \in \mathcal{A}$ and for every $b \in \mathcal{B}$. In order to construct the $k+1$-round winning strategy between $\mathcal{A}$ and $\mathcal{B}$ we define

$$D_j := \bigcup_{x\in\mathcal{A}\cup\mathcal{B}} W^x_j, \qquad \text{for } 0 \leq j \leq k \text{ and } D_{k+1} := \{h\}$$

where h is the minimal partial isomorphism just defined on the interpreted constant symbols of $\mathcal{A}$ as above in the base case. That one can construct h is clear since $h \subseteq f$ for some $f \in D_1$ for example.

Now we need to prove that $(D_j)_{0\leq j\leq k+1}$ is indeed the desired sequence. First note, a fact which we also just used for h, that $p \in W^x_j \Rightarrow p \in Part(\mathcal{A},\mathcal{B})$ for all $x \in \mathcal{A}\cup\mathcal{B}$ and $0 \leq j \leq k$. As a result all D_j have at least one element and are subsets of partial isomorphisms from $\mathcal{A}$ to $\mathcal{B}$. Furthermore, the sequence satisfies the forth property.

To see this choose $0 \leq j \leq k$ and fix $a \in \mathcal{A}$ and take an arbitrary $g \in D_{j+1}$. Now if $j = k$ then $g = h$. So let $f \in W^a_k \subset D_k$. Because f is a partial isomorphism defined on $(\mathcal{A}, a)$ it follows that $a \in dom(f)$ and $h \subseteq f$. On the other hand if $j < k$ we have that

$$g \in \bigcup_{x\in\mathcal{A}\cup\mathcal{B}} W^x_{j+1} \Rightarrow g \in W^c_{j+1}$$

for some $c \in \mathcal{A}\cup\mathcal{B}$. But then the assumption that $(W^c_l)_{0\leq l\leq k}$ is a k-round winning strategy implies

$$\exists f \in W^c_j : g \subseteq f \wedge a \in dom(f).$$

At the same time $W^c_j \subset D_j$ and as a result we have proven the forth property for $(D_j)_{0\leq j\leq k+1}$. The back property follows in a similar way.

(2.) $\Rightarrow$ (1.): The last implication will also be proven by induction.

Base case is $k = 0$. $\mathcal{A} \equiv_0 \mathcal{B}$ simply means that we can find $p \in Part(\mathcal{A},\mathcal{B})$. Given this we want to prove $\mathcal{A} \models \varphi \Rightarrow \mathcal{B} \models \varphi$ for $\varphi \in FO[0,0]$. Assume $\mathcal{A} \models \varphi$. Then since φ has zero free variables it is closed. Hence, it is a boolean combination of atomic sentences. The partial isomorphism p preserves by definition all atomic sentences. This implies $\mathcal{B} \models \varphi$. Furthermore, also $\mathcal{B} \models \varphi \Rightarrow \mathcal{A} \models \varphi$.

The induction hypothesis hence is $\mathcal{A} \equiv_k \mathcal{B}$ implies that $\mathcal{A}$ and $\mathcal{B}$ satisfy the same formulas.

Induction step is $k \mapsto k+1$. Assume $\mathcal{A} \equiv_{k+1} \mathcal{B}$ and $\mathcal{A} \models \varphi$, $\varphi \in FO[k+1, k+1]$. We wish to show $\mathcal{B} \models \varphi$.

First we examine φ. If $qr(\varphi) < k+1$ then by the induction hypothesis $\mathcal{B} \models \varphi$ because $\mathcal{A} \equiv_{k+1} \mathcal{B} \Rightarrow \mathcal{A} \equiv_k \mathcal{B}$. Hence we assume $qr(\varphi) = k+1$. This implies that $\varphi = \exists x\psi(x) \vee \varphi = \forall x\psi(x)$ for some $\psi \in FO[k,k]$. Because $\forall x\psi(x)$ is equivalent to $\exists x\neg\psi(x)$ it suffices to show that $\mathcal{A} \models \exists x\psi(x) \Rightarrow \mathcal{B} \models \exists x\psi(x)$.

$\mathcal{A} \models \exists x\psi(x)$ implies that we can find $a \in \mathcal{A}$ such that $(\mathcal{A}, a) \models \psi$. Denote by $(I_j)_{0\leq j\leq k+1}$ the associated sequence to $\mathcal{A} \equiv_{k+1} \mathcal{B}$. Note that we can find $p \in I_k$ such that $a \in dom(p)$. Hence p is a partial isomorphism from $(\mathcal{A}, a)$ to $(\mathcal{B}, p(a))$. The goal now is to establish that $(\mathcal{A}, a) \equiv_k (\mathcal{B}, p(a))$. For that we construct a sequence in the following way:

$$D_j := \{q \in I_j \,|\, p \subseteq q\}, \text{ for } j < k \text{ and } D_k := \{p\}.$$

All D_j are non-empty and consist of partial isomorphisms from $(\mathcal{A}, a)$ to $(\mathcal{B}, p(a))$. To check the forth property fix $c \in \mathcal{A}$ and an arbitrary $g \in D_j$ for $0 \leq j \leq k$. We have that $g \in D_j \Rightarrow g \in I_j$ but I_j satisfies the forth property so we can find $f \in I_{j-1} : g \subseteq f \wedge c \in dom(f)$. But then also $p \subseteq f$ and as a result $f \in D_{j-1}$. Hence $(D_j)_{0\leq j\leq k}$ satisfies the forth property. The back property is done in analogy.

We obtained $(\mathcal{A}, a) \equiv_k (\mathcal{B}, p(a))$. This implies that $(\mathcal{A}, a) \models \psi \Rightarrow (\mathcal{B}, p(a)) \models \psi$ by the induction hypothesis. As a result $(\mathcal{B}, p(a)) \models \psi$ holds. Furthermore, we have that $\mathcal{B} \models \exists x\psi(x)$. □

As a concluding remark we can say that the duplicator of an EF game which was described at the beginning of this chapter is really trying to show that the two structures $\mathcal{A}$ and $\mathcal{B}$ satisfy the same formulas up to a certain quantifier rank and a certain amount of free variables.

4.3 The derivative and Fraïssé's method

We want to relate the categorical modeloid to the Ehrenfeucht-Fraisse theorem which we have just seen. In order to do this we define a categorical modeloid on the category of τ-structures, where τ is a finite relational vocabulary. For that let $\mathcal{A}$ and $\mathcal{B}$ be two τ-structures. Denote by $F(\mathcal{A}, \mathcal{B})$ the set

$$\bigcup_{(X,Y)\in\{\mathcal{A},\mathcal{B}\}^2} Part(X, Y)$$

and let $\star \notin F(\mathcal{A}, \mathcal{B})$ be an arbitrary element. Then define $C := F(\mathcal{A}, \mathcal{B}) \cup \{\star\}$.

We construct two functions $dom : C \to C$ and $cod : C \to C$ such that for a partial isomorphism $f : X \to Y \in C \setminus \{\star\}$ we set $dom(f) = id_X$ and $cod(f) = id_Y$ and for the element $\star$ we define $dom(\star) = \star$ and $cod(\star) = \star$.

Remark 4.3.1. *For $f : X \to Y$ we will also use $dom(f)$ and $cod(f)$ to refer to the* sets *X and Y respectively. The context will make clear if the notion of an identity function or a set is required.*

We define a binary operation $\cdot : C \to C$ by

$$f \cdot g = \begin{cases} f \circ g, & \text{if } dom(f) = cod(g) \text{ and } f, g \neq \star \\ \star, & \text{else} \end{cases}$$

where $\circ$ denotes the composition of partial functions as defined in section 1.2.[13]

Proposition 4.3.2. $\mathbf{C} := (C, dom, cod, \cdot, \star, ^{-1})$ *is an inverse category in the sense of section 3.4 where* f^{-1} *denotes the inverse of each partial isomorphism* f *and* $\star^{-1} = \star$*. The existing elements are exactly all elements in* $F(\mathcal{A}, \mathcal{B})$ *and the compositions* $f \circ g$ *in case* $dom(f) = cod(g)$ *for* $f, g \in F(\mathcal{A}, \mathcal{B})$*.*

Proof. It is easy to verify that the axioms for a category hold by the constructions of the functions. Using proposition 1.2.2 it also follows that the axioms additionally required by an inverse category hold. □

Corollary 4.3.3. $\mathbf{C} := (C, dom, cod, \cdot, \star, ^{-1})$ *is also a categorical modeloid on itself.*

Proof. Closure of composition and taking inverses follow by the totality of $\cdot$ and $^{-1}$. The inclusion property and the requirement that all objects of $\mathbf{C}$ be in $\mathbf{C}$ trivially hold since the modeloid is on itself.

What is to show is that $\mathbf{C}$ has a zero element for each Endoset $End_C(X)$ where X is an object of $\mathbf{C}$. $End_C(X)$ trivially includes the partial isomorphism that is only defined on the constant symbols of τ. We denote it by 0_X. To see that this is a zero element first note that $\forall p \in End_C(X) : 0_X \subseteq p$ by definition of a partial isomorphism. In addition, since the partial composition is defined

$$dom(p \circ 0_x) = 0_X^{-1}(cod(0_X) \cap dom(p)) = 0_X^{-1}(dom(0_X)) = dom(0_X).$$

As a result we have that $p \circ 0_X = 0_X \; \forall p \in End_C(X)$. □

Remark 4.3.4. *Hence we have shown that every inverse category having a zero element for each of its Endosets is also a categorical modeloid and thus admits a derivative.*

At this point we are able to use the derivative on $\mathbf{C}$. The next theorem will draw the concluding connection between modeloids and Ehrenfeucht-Fraïssé's theorem. We will show that in the established setting an m-round winning strategy between $\mathcal{A}$ and $\mathcal{B}$ is given by the sets which the derivative produces if applied m times.

Theorem 4.3.5. *Let* M *be the categorical modeloid* $\mathbf{C}$*. Then*

$$\exists_f \, x \in D^m(M) \iff dom(x) \equiv_m cod(x), \quad m \in \mathbb{N}$$

[13] Note that the composition of partial isomorphisms also results in a partial isomorphism.

Proof. '⇒': First we define the sets $X := dom(x)$ and $Y := cod(x)$. Then define $I_j := D^j(M) \cap Part(X,Y)$ for $0 \leq j \leq m$. We want to prove that $(I_j)_{0\leq j\leq m}$ is a m-round winning strategy between X and Y. Because $D^m(M) \subseteq D^{m-1}(M) \subseteq ... \subseteq D(M) \subseteq M$ holds all I_j are non-empty and it is clear that $I_j \subseteq Part(X,Y)$ for $0 \leq j \leq m$. To show the forth property fix $a \in X$ and some $g \in I_{j+1}$ for $j < m$. Then we know by the definition of I_{j+1} that $dom(g) = X$ and $cod(g) = Y$. Furthermore we have that

$$\forall \text{ idempotent and atomic } c \in End_M(X) \exists f \in Hom(X,Y) : g \leq f \wedge c \leq f^{-1}f.$$

Similar to proposition 2.4.2 we have that $s \leq t \Leftrightarrow s \subseteq t$ for $s,t \in Part(X,Y)$. Note that $End_M(X)$ is just $Part(X,X)$ and $Hom_M(X,Y) \subseteq Part(X,Y)$. Now let 0_X denote the zero element of $End_M(X)$. We have that $e := 0_X \cup \{(a,a)\} \in End_M(X)$ is idempotent and atomic. As a result there is $f \in Hom(X,Y)$ such that $e \subseteq f^{-1}f$. But then we also have that $a \in dom(f)$ and $g \subseteq f$. Hence the forth property holds. The back property follows in a similar way.

'⇐': Again denote $dom(x)$ by X and $cod(x)$ by Y. Assume that $(I_j)_{0\leq j\leq m}$ is a m-round winning strategy between X and Y. Note first that $\forall j \forall x : x \in Part(X,Y)$ implies that x exists in terms of free logic. We now want to prove $I_j \subseteq D^j(M)$ by induction on j. The base case is clear since $I_0 \subseteq M$. For the induction step take $j \mapsto j+1$. Fix $g \in I_{j+1}$. Then by assumption

$$\forall a \in X \, \exists f \in I_j : g \subseteq f \wedge a \in dom(f).$$

By the induction hypothesis it follows that $f \in D^j(M)$. It is easy to check that the set $E := \{0_X \cup \{(c,c)\} \mid c \in X\}$ resembles exactly all idempotent and atomic elements in $End_M(X)$. Hence fix $\hat{a} \in E$. By construction $\hat{a} = 0_X \cup \{(v,v)\}$ for some $v \in X$. Now we know that $\exists f \in I_j : g \subseteq f \wedge v \in dom(f)$. This yields $g \leq f$ and $\hat{a} \leq f^{-1}f$ again similar to proposition 2.4.2 and by the fact that f is a partial isomorphism and hence $0_X \subset f^{-1}f$. The second condition of the derivative is shown to be true in a similar way. As a result $g \in D^{j+1}(M)$. □

Seeing this result it is clear that the derivative operation is in its virtue equal to Fraïssé's idea. And hence also to the construction of Hintikka's m-formulas and Ehrenfeucht's game theoretical characterization of two structure satisfying the same formulas in $FO[m,m]$. The derivative however is not restricted to the setting that the other formulations require. It has been attached to a modeloid by Benda in his paper "Modeloids. I" and hence became an operation on a structure that allows to be generalized to category theory which was the primary goal of the presented work here.

5 Conclusion

In the course of this thesis we have touched on a lot of different topics in mathematics and computer science ranging from semigroup theory over category theory to model theory as well as to interactive/automated theorem proving. The goal was always to motivate the notion of a categorical modeloid and to present its origins. The development process, however, made it possible to see overlaps between different theories most notable between semigroup theory and category theory.

In a nutshell a modeloid defined as an equivalence relation was taken and shown to correspond to a set of partial functions. Knowing the Wagner-Preston representation theorem this set of partial functions was faithfully embedded into an inverse semigroup which in turn was generalized to an inverse category. This process led to the definition of a categorical modeloid. The resulting notion was then interpreted in model theory to see the close connection to Ehrenfeucht-Fraïssé games which originally inspired the derivative operation. Hence this closes the loop back to the modeloidal relation.

Now that a notion of a categorical modeloid is presented further investigations can be done on this bases. For example it is not clear how the derivative can be used in other settings. In a sense it is the question of the usability of generalized Ehrenfeucht-Fraïssé games. Furthermore, a categorical modeloid has not been implemented in Isabelle/HOL yet and it seems to be an interesting exercise to see if Ehrenfeucht-Fraïssé games can be played using automated theorem proving.

At the same time the formalization of category theory on the bases of free logic was also slightly advanced by formulating an inverse category in this setting. The whole of computer-based theorem proving alongside ordinary mathematics in this thesis was useful for a better understanding of the material because a wrong formulation usually results in Isabelle/HOL presenting a counterexample to the statement that one wants to prove. This results in acquiring a clear understanding of the mathematical content.

Bibliography

[Ben79] Miroslav Benda. "Modeloids. I". In: *Transactions of the American Mathematical Society* 250 (1979), pp. 47–90. DOI: 10.1090/s0002-9947-1979-0530044-4.

[BN10] Jasmin Christian Blanchette and Tobias Nipkow. "Nitpick: A counterexample generator for higher-order logic based on a relational model finder". In: *International conference on interactive theorem proving*. Springer. 2010, pp. 131–146.

[BS16] Christoph Benzmüller and Dana S. Scott. *Axiomatizing Category Theory in Free Logic*. Tech. rep. http://arxiv.org/abs/1609.01493. CoRR, 2016. URL: http://arxiv.org/abs/1609.01493.

[BS18] Christoph Benzmüller and Dana S. Scott. "Axiom Systems for Category Theory in Free Logic". In: *Archive of Formal Proofs* (2018). Note: formally verified data publication. URL: https://www.isa-afp.org/entries/AxiomaticCategoryTheory.html.

[BS19] Christoph Benzmüller and Dana S. Scott. "Automating Free Logic in HOL, with an Experimental Application in Category Theory". In: *Journal of Automated Reasoning* (2019). Url (preprint): http://doi.org/10.13140/RG.2.2.11432.83202. DOI: 10.1007/s10817-018-09507-7.

[CL00] René Cori and Daniel Lascar. *Mathematical Logic: Part 1: Propositional Calculus, Boolean Algebras, Predicate Calculus, Completeness Theorems*. OUP Oxford, 2000.

[EF95] Heinz-Dieter Ebbinghaus and Jörg Flum. *Finite Model Theory*. Springer Berlin Heidelberg, 1995. DOI: 10.1007/3-540-28788-4.

[Ehr61] Andrzej Ehrenfeucht. "An application of games to the completeness problem for formalized theories". In: *Fundamenta Mathematicae* 49.129-141 (1961), p. 13.

[Fra53] Roland Fraïssé. "Sur quelques classifications des systèmes de relations". PhD thesis. University of Paris, 1953.

[Hin53] Jaakko Hintikka. *Distributive Normal Forms in the Calculus of Predicates*. [Edidit Societas Philosophica;,] [Distribuit Akatesminen Kirjakauppa,] 1953.

[How95] John Mackintosh Howie. *Fundamentals of semigroup theory*. Oxford University Press, 1995.

[Kas79] J Kastl. "Inverse categories". In: *Algebraische Modelle, Kategorien und Gruppoide* 7 (1979), pp. 51–60.

[Kol+07] Phokion G Kolaitis et al. *Finite Model Theory and its applications*. Springer Science & Business Media, 2007.

[Law98] Mark V Lawson. *Inverse Semigroups*. WORLD SCIENTIFIC, Nov. 1998. DOI: 10.1142/3645.

[Lib13] Leonid Libkin. *Elements of finite model theory*. Springer Science & Business Media, 2013.

[Lin12] Markus Linckelmann. "On inverse categories and transfer in cohomology". In: *Proceedings of the Edinburgh Mathematical Society* 56.1 (Dec. 2012), pp. 187–210. DOI: 10.1017/s0013091512000211. URL: https://doi.org/10.1017/s0013091512000211.

[MP09] Jia Meng and Lawrence C Paulson. "Lightweight relevance filtering for machine-generated resolution problems". In: *Journal of Applied Logic* 7.1 (2009), pp. 41–57.

[Rie17] E. Riehl. *Category Theory in Context*. Aurora: Dover Modern Math Originals. Dover Publications, 2017. ISBN: 9780486820804. URL: https://books.google.de/books?id=6B9MDgAAQBAJ.

[Sco64] Dana Scott. "Invariant Borel sets". In: *Fundamenta Mathematicae* 56.1 (1964), pp. 117–128. DOI: 10.4064/fm-56-1-117-128. URL: https://doi.org/10.4064/fm-56-1-117-128.

[Sco67] Dana Scott. "Existence and Description in Formal Logic". In: *Journal of Symbolic Logic*. Ed. by Ralph Schoenman. 1967, pp. 181–200.