RWTH Aachen

Mathematische Grundlagen der Informatik

# The Model Theory of Semiring Semantics

Masterarbeit

Lovro Mrkonjić

*Erstgutachter:* Prof. Dr. Erich Grädel
*Zweitgutachter:* Prof. Dr. Martin Grohe

21. Oktober 2020

# Abstract

There are only two truth values in classical semantics for first-order logic, hence a first-order sentence is either true or false in a given structure. Semiring semantics extend the domain of truth values to an arbitrary commutative semiring $K$. Since a structure can be seen as a mapping from atomic facts to truth values, it is straightforward to replace structures with $K$-interpretations, which map atomic facts to values in $K$. Interpreting a logical formula under a $K$-interpretation yields a value in $K$ as well, which provides more information than "true" or "false".

A natural question that arises with the introduction of semiring semantics is to what extent model-theoretic results from classical semantics can be lifted to semiring semantics. This thesis is mainly concerned with the relationship between elementary equivalence and isomorphism under the new semiring semantics. Elementary equivalence is one of the core concepts of model theory and the Ehrenfeucht-Fraïssé theorem establishes its relationship with isomorphism under classical semantics, while also providing a game-theoretic characterization. In particular, elementary equivalence coincides with isomorphism on finite structures.

We will show that this is not the case for semiring interpretations over all semirings $K$ by providing a counterexample in a semiring $K$ with three elements. However, we will also see that there are infinite semirings where elementary equivalence and isomorphism do coincide on finite interpretations. Hence, the relationship of elementary equivalence and isomorphism heavily depends on the algebraic properties of the semiring in question. In an attempt to obtain more general results and tools, we examine the relationship on polynomial semirings, which allows us to draw conclusions for wider classes of semirings due to the "generality" of polynomial semirings. For example, elementary equivalence and isomorphism do not coincide on finite $K$-interpretations in any distributive lattice $K$ with at least three elements, but they do coincide on finite interpretations in the "most general" semiring $\mathbb{N}[X]$ of polynomials with natural coefficients and exponents.

Finally, we observe that most of the ideas used in the Ehrenfeucht-Fraïssé theorem can be generalized to semiring semantics if we extend first-order logic to a two-sorted logic where semiring elements can be accessed and compared directly. The full theorem holds in a semiring $K$ if we assume idempotence of addition and multiplication.

# Contents

# Chapter 1

# Introduction

The defining property of real-world logical statements is their unambiguity, that is, each statement is either true or false. In mathematical logic, statements are encoded as formulas $\varphi$ from a formal language $L$ and the real world is abstracted away by interpretations $\mathfrak{I}$, which provide truth values from the Boolean domain $\mathbb{B} = \{\bot, \top\}$ for atomic statements. Therefore, a formula $\varphi$ can be evaluated under an interpretation $\mathfrak{I}$, which yields a truth value $\llbracket \varphi \rrbracket^{\mathfrak{I}} \in \mathbb{B}$ for the formula under $\mathfrak{I}$. Typically, a formula is composed of atomic statements and logical connectives such as disjunction, conjunction and negation, denoted by $\vee$ ("or"), $\wedge$ ("and") and $\neg$ ("not") respectively. Informally, the result $\llbracket \varphi \rrbracket^{\mathfrak{I}} \in \mathbb{B}$ is obtained by combining the truth values for the atomic statements given by the interpretation $\mathfrak{I}$ using the logical connectives from the formula.

For example, consider the simple first-order sentence

$$\psi := Rc \vee Rd,$$

where $c$ and $d$ are constant symbols and $R$ is a unary relation symbol. In a suitable interpretation $\mathfrak{A}$, the constants $c$ and $d$ could represent two distinct real-world objects and the relation $R^{\mathfrak{A}}$ might contain all the objects satisfying some real-world property called $R$ for convenience. Informally, the sentence $\psi$ states that at least one of the objects denoted by $c$ and $d$ satisfies the property $R$. Assume in this example that $c, d \in R^{\mathfrak{A}}$ both satisfy the property, hence both atomic facts $Rc$ and $Rd$ are true in $\mathfrak{A}$. Since $\vee$ denotes "or", $\psi$ is clearly true under $\mathfrak{A}$. Algebraically, we could say that $\psi$ under $\mathfrak{A}$ is interpreted as

$$\llbracket \psi \rrbracket^{\mathfrak{A}} = \top \vee \top = \top.$$

The above view of semantics as an algebraic combination of truth values raises the natural question of why we should restrict it to the two-element Boolean algebra over $\mathbb{B} = \{\bot, \top\}$ and whether there is anything to be gained from generalizing the approach to other domains. Indeed, Grädel and Tannen introduced semiring semantics to first-order logic in 2017, where the domain of truth values may be any commutative semiring $(K, +, \cdot, 0, 1)$ [GT17]. As a motivating example, consider the same sentence $\psi$ and the same structure $\mathfrak{A}$ as before, but instead of truth values, assign the natural number 1 from the semiring $(\mathbb{N}, +, \cdot, 0, 1)$ to the atomic facts

$Rc$ and $Rd$, which usually represents "true" numerically in computer science. As for the disjunction $\vee$, an intuitive interpretation on the domain $\mathbb{N}$ would be the usual addition $+$, which yields the value $1 + 1 = 2$ for the sentence $\psi$. This value is meaningful, because it informally represents the number of ways to prove that $\psi$ is true in $\mathfrak{A}$, which can be done via $Rc$ or $Rd$.

On general commutative semirings $(K, +, \cdot, 0, 1)$, Grädel and Tannen replaced the classical interpretations by $K$-interpretations, which map atomic facts to values in $K$ instead of truth values. In order to interpret a formula, disjunctions and conjunctions are interpreted by the algebraic semiring operations of addition $(+)$ and multiplication $(\cdot)$ respectively. This leaves the problem of negation, since negation is easily defined on $\mathbb{B} = \{\bot, \top\}$, but it is not possible to sensibly define negation in semirings such as $(\mathbb{N}, +, \cdot, 0, 1)$ or the polynomial semiring $(\mathbb{N}[X], +, \cdot, 0, 1)$. Grädel and Tannen solved this by defining semiring semantics for formulas in negation normal form only, hence negations only appear at the atomic statements. This eliminates the need to interpret negations in the semirings directly, but $K$-interpretations have to assign values from $K$ to both positive atomic statements, such as $Rc$, and the corresponding negative statements, such as $\neg Rc$, in order to be able to interpret the negated atoms if they appear in a formula. The transformation from classical semantics to semiring semantics is illustrated below.

| **classical semantics** | **semiring semantics** |
|---|---|
| interpret over *structures* | interpret over $K$-*interpretations* |
| | |
| map atoms to truth values | map literals to semiring values |
| $Rc \mapsto \top$ | $Rc \mapsto 1 \qquad \neg Rc \mapsto 0$ |
| $Rd \mapsto \top$ | $Rd \mapsto 1 \qquad \neg Rd \mapsto 0$ |
| | |
| interpret with $\{\neg, \vee, \wedge\}$ | interpret with $\{+, \cdot\}$ |
| $\top \vee \top = \top$ | $1 + 1 = 2$ |

The practical use of semiring interpretations for first-order logic was also demonstrated by Grädel and Tannen in 2017. As hinted above, they proved that using a suitable $\mathbb{N}$-interpretation to interpret a first-order formula $\psi$ enables us to count all the possible proofs for $\psi$. Switching to other semirings, such as the polynomial semiring $(\mathbb{N}[X], +, \cdot, 0, 1)$, provides even more information. As a slightly more complex example, consider the first-order sentence

$$\vartheta \coloneqq (Rc \wedge Rd) \vee Re.$$

We use a $\mathbb{N}[X]$-interpretation and assign a unique variable to each atomic fact, in this case, let $\{x, y, z\} \subseteq X$ and assign $Rc \to x$, $Rd \to y$ and $Re \to z$. If we use this to interpret the formula over $\mathbb{N}[X]$, we obtain the result $xy + z$, where each monomial represents one possible "proof" for $\vartheta$ and the variables in the monomials correspond to the facts used in that proof. Grädel and Tannen called this *provenance analysis*, since we can exactly determine the atomic facts that contribute to the truth value of a formula and the manner of their contribution.

Moreover, Grädel and Tannen made the important observation that semiring semantics are compatible with semiring homomorphisms, hence we can even use the resulting polynomial to interpret $\vartheta$ under a $K$-interpretation for a different semiring

$K$. For example, consider the usual "counting" $\mathbb{N}$-interpretation that assigns 1 to $Rc$, $Rd$ and $Re$. Instead of interpreting $\vartheta$ from scratch under the counting interpretation, we can simply assign 1 to $x$, $y$ and $z$ in the polynomial $xy+z$ and obtain the desired result $1 \cdot 1 + 1 = 2$, which is the number of different proofs for $\vartheta$, without using $\vartheta$ again. This observation highlights the importance of polynomials for semiring semantics and will be used to obtain general model-theoretic results. Clearly, $K$-interpretations for various semirings $K$ would provide different kinds of information about $\vartheta$. Indeed, Grädel and Tannen demonstrated even more uses of $K$-interpretations on various semirings $K$.

In this thesis, we are interested in the model-theoretic properties of semiring semantics for first-order logic. First, the fundamental terms such as isomorphism or equivalence must be generalized to semiring semantics. The goal is to determine which results from classical two-valued model theory carry over to semiring semantics. As an orientation, we use the Ehrenfeucht-Fraïssé theorem, which provides useful insights into the relation between isomorphism and elementary equivalence of structures in classical logic. In particular, it is known that if two finite structures $\mathfrak{A}$ and $\mathfrak{B}$ satisfy the same first-order sentences, they must be isomorphic, that is, we can transform one into the other by renaming elements. This raises the question of whether a similar result holds for two finite $K$-interpretations. However, the answer does not only depend on the definition of the corresponding terms for $K$-interpretations, but also on the algebraic properties of the semiring $K$ in question.

To illustrate this, notice how the meaning of equivalence between first-order formulas changes depending on the semiring $K$. Consider two formulas

$$(\varphi \wedge \psi) \wedge \vartheta \quad \text{and} \quad \varphi \wedge (\vartheta \wedge \psi),$$

which are obviously equivalent in standard semantics. In a commutative semiring $(K, +, \cdot, 0, 1)$, since $\wedge$ is interpreted by $\cdot$, which is associative and commutative, those formulas are always equivalent as expected. However, this does not hold for all classical equivalences, such as $\varphi \vee \varphi \equiv \varphi$. On a semiring $K$, the formulas $\varphi \vee \varphi$ and $\varphi$ do not always yield the same value unless $K$ is idempotent, that is $a + a = a$ for all $a \in K$. An $\mathbb{N}$-interpretation that interprets $\varphi$ with 2 would interpret $\varphi \vee \varphi$ with $2 + 2 = 4 \neq 2$. Therefore, we need to categorize semirings based on their algebraic properties in order to study the model-theoretic properties of semiring semantics and results may vary between different semirings.

Finally, it is also possible to approach the problem from a different perspective. Instead of checking whether classical results from model theory can be lifted to semiring semantics for plain first-order logic, we may extend the logic's syntax so that classical theorems, such as the Ehrenfeucht-Fraïssé theorem, remain as intact as possible under semiring semantics. This will be achieved by introducing new constants and operators to first-order logic that access the elements of $K$ directly.

# Chapter 2

# Foundations

Before diving into model theory, it is necessary to state the syntax and Grädel and Tannen's semiring semantics for first-order logic formally. First, we will provide their definition of semirings and recapitulate some basic algebraic properties they observed in 2017 [GT17].

**(2.1) Definition** (Semiring)**.** A semiring is a structure $(K, +, \cdot, 0, 1)$ such that $(K, +, 0)$ is a commutative monoid, $(K, \cdot, 1)$ is a monoid, $0 \neq 1$, multiplication by 0 annihilates $K$ and multiplication distributes over addition, that is

$$\begin{aligned} &(1) \quad 0 \cdot a = a \cdot 0 = 0 && \text{for all } a \in K, \\ &(2) \quad a \cdot (b + c) = (a \cdot b) + (a \cdot c) && \text{for all } a, b, c \in K \quad \text{and} \\ &(3) \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a) && \text{for all } a, b, c \in K. \end{aligned}$$

$(K, +, \cdot, 0, 1)$ is commutative if the multiplication is commutative. If the operations and constants $(+, \cdot, 0, 1)$ can be inferred from the context, we may simply write $K$ instead of $(K, +, \cdot, 0, 1)$ to denote a semiring.

Since we only consider commutative semirings in this thesis, we will implicitly assume that semirings are commutative unless stated otherwise. Some semirings and their possible uses were already mentioned in the introduction, such as $(\mathbb{N}, +, \cdot, 0, 1)$ for proof counting or $(\mathbb{N}[X], +, \cdot, 0, 1)$ for provenance analysis. Of course, classical semantics may also be seen as a special case of semiring semantics over the Boolean semiring $\mathbb{B} = (\{\bot, \top\}, \vee, \wedge, \bot, \top)$ itself, but note that negation is not used. More examples include the Viterbi semiring $\mathbb{V} = ([0, 1]_{\mathbb{R}}, \max, \cdot, 0, 1)$ and the access control semiring $\mathbb{A} = (\{P, C, S, T, 0\}, \min, \max, 0, P)$. Values from the Viterbi semiring may be interpreted as confidence scores for practical purposes and values from the access control semiring are interpreted as access tokens with $P < C < S < T < 0$, where $P$ is public, $C$ is confidential, $S$ is secret, $T$ is top secret and 0 is inaccessible. Both these semirings will be further examined later on. Finally, $\mathbb{T} = (\mathbb{R}^{\infty}_{\geq 0}, \min, +, \infty, 0)$ and $\mathbb{F} = ([0, 1]_{\mathbb{R}}, \max, \min, 0, 1)$ are semirings as well, where $\mathbb{T}$ is the *tropical* semiring, usable for the calculation of shortest paths, and $\mathbb{F}$ is the *fuzzy* semiring, which can be used in fuzzy logic.

Although we will not refer to each of those examples specifically, their diversity provides the justification for the use of commutative semirings to generalize the semantics of first-order logic. Commutative semirings provide the two operations +

and $\cdot$ that are necessary to interpret $\vee$ and $\wedge$ in logics, but they impose very few restrictions on those operations compared to the more commonly studied structures in algebra, such as rings or fields. More specifically, they do not require the existence of inverse elements for any of the two operations $+$ and $\cdot$. In fact, we will later see that additive inverses may be undesirable for the sanity of semiring semantics, hence we mostly study semirings that do not satisfy the ring axioms.

However, while inverse elements are not required or not desired, we still rely on associativity and commutativity for both semiring operations $+$ and $\cdot$ due to the fact that they are intended to interpret disjunctions and conjunctions in logics that are commonly expected to be order-invariant. Therefore, given a finite index set $I$ and logical formulas $(\varphi_i)_{i\in I}$, we are still allowed to write disjunctions and conjunctions as

$$\bigvee_{i\in I} \varphi_i \quad \text{or} \quad \bigwedge_{i\in I} \varphi_i$$

respectively, without specifying the order. The informal conclusion is that commutative semirings impose the least possible restrictions on an algebraic structure with two operations $(K, +, \cdot, 0, 1)$ to be usable as a domain of truth values for logic.

## 2.1 Semiring Semantics for First-Order Logic

Before providing the semiring semantics for first-order logic $\mathsf{FO}(\tau)$ by Grädel and Tannen, we have to formally define the required interpretations and revise the syntax. First, assume that $\tau$ is a *relational* signature. In most contexts, we will require $\tau$ to be finite or at least countable as well. Instead of using $\tau$-structures $\mathfrak{A} = (A, \tau)$ as interpretations, we use $K$-interpretations. For a set $A$, define

$$\begin{aligned}
&\mathrm{Lit}_A^+(\tau) \coloneqq \{R\overline{a} \mid R \in \tau \text{ is a } k\text{-ary relation symbol and } \overline{a} \in A^k\},\\
&\mathrm{Lit}_A^-(\tau) \coloneqq \{\neg R\overline{a} \mid R \in \tau \text{ is a } k\text{-ary relation symbol and } \overline{a} \in A^k\} \quad \text{and}\\
&\mathrm{Lit}_A(\tau) = \mathrm{Lit}_A^+(\tau) \cup \mathrm{Lit}_A^-(\tau).
\end{aligned}$$

$\mathrm{Lit}_A^+(\tau)$ denotes the $\tau$-*atoms* over $A$, $\mathrm{Lit}_A^-(\tau)$ denotes the negated atoms and together, they make up $\mathrm{Lit}_A(\tau)$, the $\tau$-*literals* over $A$. Depending on the context, we may omit $A$ or $\tau$ if the notation is unambiguous. Note that if both $A$ and $\tau$ are finite, then $\mathrm{Lit}_A(\tau)$ is finite as well and if at least one of them is infinite, the cardinality of $\mathrm{Lit}_A(\tau)$ is $\max\{|A|, |\tau|\}$ since multiplication of infinite cardinals is idempotent by Hessenberg's theorem.

**(2.2) Definition** ($K$-interpretation)**.** Let $K$ be a semiring. A $K$-*interpretation* over a structure $\mathfrak{A} = (A, \tau)$ is a function $\pi : \mathrm{Lit}_A(\tau) \to K$.

Clearly, a structure $\mathfrak{A}$ that defines the relations in $\tau$ can be viewed as a $\mathbb{B}$-interpretation $\pi_{\mathfrak{A}} : \mathrm{Lit}_A(\tau) \to \mathbb{B}$ by simply setting

$$\pi_{\mathfrak{A}}(R\overline{a}) \coloneqq \begin{cases} \top & \text{if } \overline{a} \in R^{\mathfrak{A}},\\ \bot & \text{otherwise}\end{cases} \quad \text{and} \quad \pi_{\mathfrak{A}}(\neg R\overline{a}) \coloneqq \begin{cases} \top & \text{if } \overline{a} \notin R^{\mathfrak{A}},\\ \bot & \text{otherwise}\end{cases}$$

for all $R \in \tau$ and $\overline{a} \in A^k$ when $R$ is $k$-ary. Hence, the generalization of interpretations to $K$-interpretations for a relational signature $\tau$ is straightforward. However, if $\tau$

contains a $k$-ary function symbol $f$, it is usually interpreted by a function $f^{\mathfrak{A}} : A^k \to A$ in $\mathfrak{A}$. It is not immediately clear how to generalize this to $K$-interpretations. One approach would be to interpret the function symbols as usual in classical semantics by functions $f^{\mathfrak{A}} : A^k \to A$ and the relational part $\tau_R \subseteq \tau$ with a $K$-interpretation $\pi : \mathrm{Lit}_A(\tau_R) \to K$. Another possibility is removing the function symbols from $\tau$ and considering their graphs $G_f \subseteq A^{k+1}$ instead, which would create a relational signature. For simplicity, we omit functions altogether in this thesis. Therefore, we will provide the definition of the usual syntax of first-order logic, but there is no need to define first-order terms, since any term that is built without a function symbol is simply a variable.

**(2.3) Definition** (Syntax of First-Order Logic)**.** Let $\tau$ be a relational signature. The set of *variables* $V$ is a fixed, countably infinite set. The set $\mathsf{FO}(\tau)$ of first-order formulas over $\tau$ is inductively defined as the least set such that

(1) for all $x_1, x_1 \in V, x_1 = x_2 \in \mathsf{FO}(\tau)$,
(2) for all $k$-ary relation symbols $R \in \tau$ and $x_1, \ldots, x_k \in V, Rx_1 \ldots x_k \in \mathsf{FO}(\tau)$,
(3) if $\varphi \in \mathsf{FO}(\tau)$, then $\neg\varphi \in \mathsf{FO}(\tau)$,
(4) if $\varphi, \psi \in \mathsf{FO}(\tau)$, then $(\varphi \circ \psi) \in \mathsf{FO}(\tau)$ for $\circ \in \{\vee, \wedge, \to\}$ and
(5) if $\varphi \in \mathsf{FO}(\tau)$ and $x \in V$, then $Qx\varphi \in \mathsf{FO}(\tau)$ for $Q \in \{\exists, \forall\}$.

A formula is in *negation normal form* if it does not contain implications ($\to$) and negation ($\neg\varphi$) only occurs for atomic formulas $\varphi$ constructed by (1) or (2).

When dealing with semiring interpretations, the usual terms and definitions that apply to $\mathsf{FO}$-formulas as syntactic objects, such as "free" or "bound" variables, "depth" or "quantifier rank" can still be used. However, special emphasis must be put on the negation normal form. Since semirings do not provide a way to interpret negation, strictly speaking, we can only define semiring semantics on the fragment of $\mathsf{FO}$-formulas in negation normal form. However, since any $\mathsf{FO}$-formula can be syntactically transformed into negation normal form, for example by using de Morgan laws and the equivalence $\varphi \to \psi \equiv \neg\varphi \vee \psi$, this implicitly defines semiring semantics for all $\mathsf{FO}$-formulas.

**(2.4) Definition** (Semiring Semantics of First-Order Logic)**.** Let $K$ be a semiring, $\pi : \mathrm{Lit}_A(\tau) \to K$ a semiring interpretation, $\vartheta(\overline{x})$ a $\mathsf{FO}(\tau)$-formula in negation normal form with free variables $\overline{x} = (x_1, \ldots, x_k)$ and $\beta : X \to A$ an assignment of variables with $\{x_1, \ldots, x_k\} \subseteq X$. The semantics $\pi [\![\vartheta(\overline{x})]\!]^\beta \in K$ are inductively defined as follows.

(1) For $\vartheta(\overline{x}) \in \{x_1 = x_2, \neg x_1 = x_2\}$ with $x_1, x_2 \in V$,

$$\pi [\![x_1 = x_2]\!]^\beta := \begin{cases} 1 & \text{if } \beta(x_1) = \beta(x_2), \\ 0 & \text{otherwise} \end{cases} \quad \text{and}$$

$$\pi [\![\neg x_1 = x_2]\!]^\beta := \begin{cases} 1 & \text{if } \beta(x_1) \neq \beta(x_2), \\ 0 & \text{otherwise.} \end{cases}$$

(2) For $\vartheta(\overline{x}) \in \{Rx_{i_1} \dots x_{i_\ell}, \neg Rx_{i_1} \dots x_{i_\ell}\}$ with $R \in \tau$ $\ell$-ary and $\{x_{i_1}, \dots, x_{i_\ell}\} \subseteq X$,

$$\pi [\![Rx_{i_1} \dots x_{i_\ell}]\!]^\beta \coloneqq \pi(R\beta(x_{i_1}) \dots \beta(x_{i_\ell})) \quad \text{and}$$
$$\pi [\![\neg Rx_{i_1} \dots x_{i_\ell}]\!]^\beta \coloneqq \pi(\neg R\beta(x_{i_1}) \dots \beta(x_{i_\ell}))$$

(3) The case $\vartheta(\overline{x}) = \neg\varphi(\overline{x})$ can be omitted due to negation normal form.

(4) For $\vartheta(\overline{x}) = \varphi(\overline{x}) \circ \psi(\overline{x})$ with $\circ \in \{\vee, \wedge, \rightarrow\}$,

$$\pi [\![\varphi(\overline{x}) \vee \psi(\overline{x})]\!]^\beta \coloneqq \pi [\![\varphi(\overline{x})]\!]^\beta + \pi [\![\psi(\overline{x})]\!]^\beta \quad \text{and}$$
$$\pi [\![\varphi(\overline{x}) \wedge \psi(\overline{x})]\!]^\beta \coloneqq \pi [\![\varphi(\overline{x})]\!]^\beta \cdot \pi [\![\psi(\overline{x})]\!]^\beta .$$

We can omit $\circ \in \{\rightarrow\}$ due to negation normal form.

(5) For $\vartheta(\overline{x}) = Qx\varphi(\overline{x}, x)$ with $Q \in \{\exists, \forall\}$,

$$\pi [\![\exists x\varphi(\overline{x}, x)]\!]^\beta \coloneqq \sum_{a\in A} \pi [\![\varphi(\overline{x}, x)]\!]^{\beta[x\mapsto a]} \quad \text{and}$$
$$\pi [\![\forall x\varphi(\overline{x}, x)]\!]^\beta \coloneqq \prod_{a\in A} \pi [\![\varphi(\overline{x}, x)]\!]^{\beta[x\mapsto a]} ,$$

where $\beta[x \mapsto a]$ denotes the same assignment as $\beta$ except that the variable $x$ is remapped to $a$ if $\beta(x)$ was already defined or otherwise, the domain is extended and $x$ is mapped to $a$.

If $\vartheta(\overline{x})$ is not in negation normal form, let $\vartheta'$ be the negation normal form of $\vartheta$ and set $\pi [\![\vartheta(\overline{x})]\!]^\beta \coloneqq \pi [\![\vartheta'(\overline{x})]\!]^\beta$. Instead of explicitly defining variable assignments, we may write $\pi [\![\vartheta(\overline{a})]\!]$ instead of $\pi [\![\vartheta(\overline{x})]\!]^\beta$ with $\beta(x_i) = a_i$ for $i \in \{1, \dots, k\}$.

Apart from (5), all definitions straightforwardly follow from the main idea to interpret disjunctions and conjunctions with the semiring operations $+$ and $\cdot$. The values under definition (1) and (2) are directly supplied by the $K$-interpretation. The quantifiers are implicitly transformed into disjunctions (for $\exists$) and conjunctions (for $\forall$) over all elements of the structure. Although the elements of $A$ do not need to be ordered, since both $+$ and $\cdot$ are associative and commutative, the definition is reasonable for finite $A$.

Note that the transformation into negation normal form does not change the meaning of formulas under standard semantics over $\mathbb{B}$, but it may cause problems under semiring semantics for "guarded" formulas. As an example, consider the formula $\forall x(\varphi(x) \rightarrow \psi(x))$, which is interpreted by

$$\pi [\![\forall x(\varphi(x) \rightarrow \psi(x))]\!] = \pi [\![\forall x(\neg\varphi(x) \vee \psi(x))]\!] = \prod_{a\in A} (\pi [\![\neg\varphi(a)]\!] + \pi [\![\psi(a)]\!]).$$

Normally, we would expect the "guard" $\varphi(x)$ to filter out all the elements $a \in A$ where $\varphi(a)$ is not satisfied so that they do not contribute to the interpretation of the formula. Unfortunately, this is clearly not the case in semiring semantics, where, even if $\pi [\![\neg\varphi(a)]\!] = 1$, the element $a$ contributes with a factor of $(1+\pi [\![\psi(a)]\!])$ to the product. Hence, the elimination of implications via syntactical transformations may cause problems. Dannert and Grädel provide more detailed examples and workarounds for this problem in their paper on semiring provenance for guarded logics [DG20], but we will avoid guarded formulas and implications here. Another problem is introduced by infinite universes $A$ that require us to define infinitary sums and products on semirings $K$ in order to be able to interpret formulas with quantifiers.

**(2.5) Definition** (Infinitary Operations)**.** Let $K$ be a semiring. We say that $K$ *admits infinitary summation* if there is a summation operator $\Sigma$ such that for all sets $I$ and $(a_i)_{i\in I} \subseteq K$, the conditions

$$\begin{aligned}
&(1) && \sum_{i\in I} a_i = \sum_{i\in I}^{\text{fin}} a_i && \text{if } I \text{ is finite,}\\
&(2) && \sum_{i\in I} a_i = \sum_{i\in I} a_{\sigma(i)} && \text{for all bijections } \sigma : I \to I,\\
&(3) && \sum_{i\in I} a_i = \sum_{S\in P}\sum_{i\in S} a_i && \text{for all partitions } P \text{ of } I \quad \text{and}\\
&(4) && c\cdot\sum_{i\in I} a_i = \sum_{i\in I} c\cdot a_i && \text{for all } c\in K
\end{aligned}$$

are satisfied. Similarly, $K$ *admits infinitary multiplication* if there is a multiplication operator $\Pi$ such that for all $I$ and $(a_i)_{i\in I} \subseteq K$,

$$\begin{aligned}
&(5) && \prod_{i\in I} a_i = \prod_{i\in I}^{\text{fin}} a_i && \text{if } I \text{ is finite,}\\
&(6) && \prod_{i\in I} a_i = \prod_{i\in I} a_{\sigma(i)} && \text{for all bijections } \sigma : I \to I \quad \text{and}\\
&(7) && \prod_{i\in I} a_i = \prod_{S\in P}\prod_{i\in S} a_i && \text{for all partitions } P \text{ of } I
\end{aligned}$$

hold. $\Sigma^{\text{fin}}$ and $\Pi^{\text{fin}}$ denote the normal sums and products obtained by inductively adding or multiplying the $a_i$, which is possible for finite $I$. Finally, $K$ *admits infinitary operations* if it admits both infinitary summation and multiplication.

Inifinitary operations on semirings have already been studied in other contexts, for example in [GT19], [Mrk18], [Naa19] and [DGNT19] for the purpose of defining semiring semantics for temporal logics, fixed-point logics and games. While these papers provide the definitions of infinitary operations in more detail, such as [DGNT19], where a general definition via order theory is provided, the above definition summarizes the important properties for those operations to behave reasonably as sums and products without focusing on the concrete realization. For example, the bijection invariance conditions are important for semiring interpretations, since the universes $A$ of $K$-interpretations are not provided in any particular order, so the definitions

$$\pi [\![\exists x\varphi(x)]\!] = \sum_{a\in A} \pi [\![\varphi(a)]\!] \quad \text{and} \quad \pi [\![\forall x\varphi(x)]\!] = \prod_{a\in A} \pi [\![\varphi(a)]\!]$$

would not be sensible without (2) and (6) on infinite $A$.

It is sometimes useful or even necessary to restrict the cardinality of $I$. While semiring semantics are well-defined on all commutative semirings $K$ for $K$-interpretations over finite universes, we may only use $K$-interpretations over infinite universes if infinitary operations are defined on $K$ and support sufficient cardinalities. For example, $\mathbb{N}$ does not admit infinitary summation, since $\sum_{i\in\mathbb{N}} i$ cannot be defined adequately. If we set $\sum_{i\in\mathbb{N}} i := n$ for any $n \in \mathbb{N}$, then we have $n = (n+1) + \sum_{i\in\mathbb{N}\setminus\{n+1\}} i > n$ by condition (3), a contradiction. Hence, some semirings $K$ are not suited for $K$-interpretations over infinite universes.

## 2.2 The Fundamental Property

The fundamental property informally states that semiring interpretations are compatible with semiring homomorphisms. This property was observed by Grädel and Tannen in [GT17] and constitutes a very powerful model-theoretic tool because it enables us to analyze properties of $K$-interpretations via homomorphisms $h : K \to L$ into more "simple" semirings $L$, as we will see later on. First, we have to provide the necessary definitions.

**(2.6) Definition** (Semiring Homomorphism)**.** For two semirings $(K, +^K, \cdot^K, 0^K, 1^K)$ and $(L, +^L, \cdot^L, 0^L, 1^L)$, a function $h : K \to L$ is a *semiring homomorphism* if it satisfies

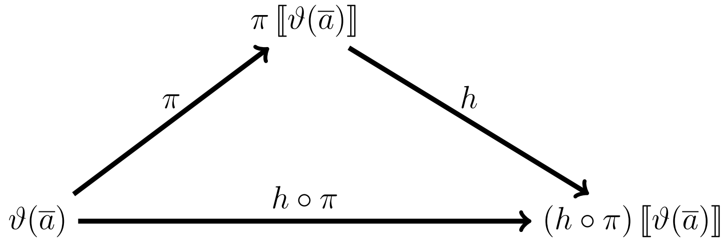
(1) $h(0^K) = 0^L$ and $h(1^K) = 1^L$ as well as

(2) $h(a +^K b) = h(a) +^L h(b)$ and $h(a \cdot^K b) = h(a) \cdot^L h(b)$ for all $a, b \in K$.

Since we will only refer to semiring homomorphisms here, we will simply call them homomorphisms for brevity.

Due to the fact that inverse elements need not exist in semirings, condition (2) does not imply (1). Recall that a $K$-interpretation is simply a function $\pi : \mathrm{Lit}_A(\tau) \to K$, hence $h \circ \pi : \mathrm{Lit}_A(\tau) \to L$ is an $L$-interpretation.

**(2.7) Lemma** (Fundamental Property)**.** For two semirings $K, L$, a $K$-interpretation $\pi : \mathrm{Lit}_A(\tau) \to K$ over a finite universe $A$ and a homomorphism $h : K \to L$, we have $h(\pi [\![\vartheta(\overline{x})]\!]^\beta) = (h \circ \pi) [\![\vartheta(\overline{x})]\!]^\beta$ for all $\vartheta(\overline{x}) \in \mathsf{FO}(\tau)$ and suitable assignments $\beta : X \to A$. In other words, the following diagram commutes.




*Proof.* Since definition (2.4) of semiring semantics only applies to formulas in negation normal form, we may assume that $\vartheta(\overline{x})$ is in negation normal form and proceed by induction as in the definition.

(1) If $\vartheta(\overline{x}) \in \{x_1 = x_2, \neg x_1 = x_2\}$ with $x_1, x_2 \in V$, then

$$h(\pi [\![x_1 = x_2]\!]^\beta) = \left.\begin{cases} h(1^K) \overset{*}{=} 1^L & \text{if } \beta(x_1) = \beta(x_2), \\ h(0^K) \overset{*}{=} 0^L & \text{otherwise} \end{cases}\right\} = (h \circ \pi) [\![x_1 = x_2]\!]^\beta$$

$$h(\pi [\![\neg x_1 = x_2]\!]^\beta) = \left.\begin{cases} h(1^K) \overset{*}{=} 1^L & \text{if } \beta(x_1) \neq \beta(x_2), \\ h(0^K) \overset{*}{=} 0^L & \text{otherwise} \end{cases}\right\} = (h \circ \pi) [\![\neg x_1 = x_2]\!]^\beta .$$

(2) For $\vartheta(\overline{x}) \in \{Rx_{i_1} \dots x_{i_\ell}, \neg Rx_{i_1} \dots x_{i_\ell}\}$ with $R \in \tau$ $\ell$-ary and $\{x_{i_1}, \dots, x_{i_\ell}\} \subseteq X$, the corresponding literal is $L := R\beta(x_{i_1}) \dots \beta(x_{i_\ell})$ or $L := \neg R\beta(x_{i_1}) \dots \beta(x_{i_\ell})$ respectively, with that, we have

$$h(\pi [\![\vartheta(\overline{x})]\!]^\beta) = h(\pi(L)) = (h \circ \pi)(L) = (h \circ \pi) [\![\vartheta(\overline{x})]\!]^\beta .$$

(4) If $\vartheta(\overline{x}) = \varphi(\overline{x}) \circ \psi(\overline{x})$ with $\circ \in \{\vee, \wedge\}$, then

$$\begin{aligned}
h(\pi \llbracket \varphi(\overline{x}) \vee \psi(\overline{x}) \rrbracket^{\beta}) &= h(\pi \llbracket \varphi(\overline{x}) \rrbracket^{\beta} + \pi \llbracket \psi(\overline{x}) \rrbracket^{\beta}) \\
&\stackrel{*}{=} h(\pi \llbracket \varphi(\overline{x}) \rrbracket^{\beta}) + h(\pi \llbracket \psi(\overline{x}) \rrbracket^{\beta}) \\
&\stackrel{\star}{=} (h \circ \pi) \llbracket \varphi(\overline{x}) \rrbracket^{\beta} + (h \circ \pi) \llbracket \psi(\overline{x}) \rrbracket^{\beta} \\
&= (h \circ \pi) \llbracket \varphi(\overline{x}) \vee \psi(\overline{x}) \rrbracket^{\beta} \quad \text{and} \\
h(\pi \llbracket \varphi(\overline{x}) \wedge \psi(\overline{x}) \rrbracket^{\beta}) &= h(\pi \llbracket \varphi(\overline{x}) \rrbracket^{\beta} \cdot \pi \llbracket \psi(\overline{x}) \rrbracket^{\beta}) \\
&\stackrel{*}{=} h(\pi \llbracket \varphi(\overline{x}) \rrbracket^{\beta}) \cdot h(\pi \llbracket \psi(\overline{x}) \rrbracket^{\beta}) \\
&\stackrel{\star}{=} (h \circ \pi) \llbracket \varphi(\overline{x}) \rrbracket^{\beta} \cdot (h \circ \pi) \llbracket \psi(\overline{x}) \rrbracket^{\beta} \\
&= (h \circ \pi) \llbracket \varphi(\overline{x}) \wedge \psi(\overline{x}) \rrbracket^{\beta} .
\end{aligned}$$

(5) If $\vartheta(\overline{x}) = Qx\varphi(\overline{x}, x)$ with $Q \in \{\exists, \forall\}$, then

$$\begin{aligned}
h(\pi \llbracket \exists x \varphi(\overline{x}, x) \rrbracket^{\beta}) &= h\left(\sum_{a \in A} \pi \llbracket \varphi(\overline{x}, x) \rrbracket^{\beta[x \mapsto a]}\right) \\
&\stackrel{*}{=} \sum_{a \in A} h(\pi \llbracket \varphi(\overline{x}, x) \rrbracket^{\beta[x \mapsto a]}) \\
&\stackrel{\star}{=} \sum_{a \in A} (h \circ \pi) \llbracket \varphi(\overline{x}, x) \rrbracket^{\beta[x \mapsto a]} \\
&= (h \circ \pi) \llbracket \exists x \varphi(\overline{x}, x) \rrbracket^{\beta} \quad \text{and} \\
h(\pi \llbracket \forall x \varphi(\overline{x}, x) \rrbracket^{\beta}) &= h\left(\prod_{a \in A} \pi \llbracket \varphi(\overline{x}, x) \rrbracket^{\beta[x \mapsto a]}\right) \\
&\stackrel{*}{=} \prod_{a \in A} h(\pi \llbracket \varphi(\overline{x}, x) \rrbracket^{\beta[x \mapsto a]}) \\
&\stackrel{\star}{=} \prod_{a \in A} (h \circ \pi) \llbracket \varphi(\overline{x}, x) \rrbracket^{\beta[x \mapsto a]} \\
&= (h \circ \pi) \llbracket \forall x \varphi(\overline{x}, x) \rrbracket^{\beta} .
\end{aligned}$$

Steps where the induction hypothesis is required are marked with ($\star$), whereas ($*$) indicates that properties of homomorphisms from definition (2.6) were used. This ends the induction and concludes the proof. □

In order to eliminate the condition that the universe $A$ must be finite, it would be sufficient to require that $K$ and $L$ admit infinitary operations and the homomorphism $h$ is compatible with those operations as well, that is,

$$h\left(\sum_{i \in I} a_i\right) = \sum_{i \in I} h(a_i) \quad \text{and} \quad h\left(\prod_{i \in I} a_i\right) = \prod_{i \in I} h(a_i)$$

for all index sets $I$ and $(a_i)_{i \in I} \subseteq K$. This would enable the proof of step (5) for infinite universes $A$. Although we will not use homomorphisms that preserve infinitary operations here, they may be required for stronger logics, such as fixed-point logics, thus they are used, for example, in [Naa19] and [DGNT19].

## 2.3 Categorization of Semirings

Many of the semirings mentioned above have significantly different properties from $(\mathbb{B}, \vee, \wedge, \bot, \top)$, the standard semiring in logic. Due to the diversity of semirings, it is difficult to make general statements in semiring model theory. Therefore, we will often impose additional requirements on semirings. One example is idempotence of $+$ and $\cdot$.

**(2.8) Definition** (Idempotence)**.** A semiring $(K, +, \cdot, 0, 1)$ is *idempotent* if $a + a = a$ for all $a \in A$, that is, if $+$ is idempotent. It is *multiplicatively idempotent* if $a \cdot a = a$ for all $a \in A$.

Informally speaking, idempotence makes a semiring more similar to $\mathbb{B}$, since $\vee$ and $\wedge$ in $\mathbb{B}$ are idempotent. The consequence for semiring semantics is that the well-known equivalence $\varphi \vee \varphi \equiv \varphi$ in standard semantics still holds in a semiring $K$ if and only if $K$ is idempotent, while $\varphi \wedge \varphi \equiv \varphi$ holds if and only if $K$ is multiplicatively idempotent.

Another striking difference between standard and semiring semantics is that the potential presence of more than two elements in general semirings $K$ requires semiring semantics to be restricted to negation normal form and $K$-interpretations to assign values to both positive and negative literals. So far, we have not imposed any restrictions on this, hence, a $K$-interpretation $\pi : \mathrm{Lit}_A(\tau) \to K$ may assign seemingly contradictory values to literals. If $L \in \mathrm{Lit}_A^+(\tau)$ is a positive literals and $\neg L$ is the corresponding negative literal, we may have $\pi(L) = \pi(\neg L) = 0$ or $\pi(L) = \pi(\neg L) = 1$. This is even permitted when $\pi$ is a $\mathbb{B}$-interpretation. However, these counter-intuitive $K$-interpretations may be removed by imposing restrictions as suggested by Grädel and Tannen.

**(2.9) Definition** (Model-Defining)**.** A $K$-interpretation $\pi : \mathrm{Lit}_A(\tau) \to K$ is called *model-defining* if for each pair of complementary literals $L, \neg L$ with $L \in \mathrm{Lit}_A^+(\tau)$, exactly one of the values $\pi(L)$ and $\pi(\neg L)$ is 0.

In that case, the model defined by $\pi$ is the structure $\mathfrak{A} = (A, \tau)$ with $\mathfrak{A} \models L$ for precisely the literals $L$ with $\pi(L) \neq 0$, hence, we interpret 0 as "false" and nonzero values as "true". More formally, let $\dagger_K : K \to \mathbb{B}$ be defined as

$$\dagger_K(a) = \begin{cases} \top & \text{if } a \neq 0 \\ \bot & \text{otherwise} \end{cases} \qquad \text{for all } a \in K.$$

If $\pi$ is model-defining, then $\dagger_K \circ \pi$ is a $\mathbb{B}$-interpretation with $(\dagger_K \circ \pi)(L) \neq (\dagger_K \circ \pi)(\neg L)$ for all $L \in \mathrm{Lit}_A^+(\tau)$, therefore it induces a model $\mathfrak{A}$ in the classical sense.

Unfortunately, the property that $(\dagger_K \circ \pi)(L) \neq (\dagger_K \circ \pi)(\neg L)$ does not extend to all $\mathsf{FO}$-formulas. As an example, consider any ring $K$ with a nonzero element $a \neq 0$. Then, the additive inverse $(-a) \in K$ exists and is nonzero as well. Now, we pick $A := \{e, f\}$ with two elements and $\tau = \{R\}$ with one unary relation symbol and set

$$\begin{aligned} \pi(Re) &:= a, & \pi(\neg Re) &:= 0, \\ \pi(Rf) &:= (-a) \quad \text{and} & \pi(\neg Rf) &:= 0. \end{aligned}$$

Finally, choose $\vartheta(x, y) \coloneqq Rx \vee Ry$ and interpret the variables with $\beta : x \mapsto e, y \mapsto f$. We obtain

$$\pi [\![\vartheta(x, y)]\!]^\beta = \pi(Re) + \pi(Rf) = a + (-a) = 0,$$

but the negation normal form of $\neg\vartheta(x, y)$ is $\neg Rx \wedge \neg Ry$, so it is immediately clear that $\pi [\![\neg\vartheta(x, y)]\!]^\beta = 0$ as well. Although $\pi$ is model-defining and does not contain any unreasonable assignments, the interpretation yields a possibly undesirable result of $\pi [\![\vartheta(x, y)]\!]^\beta = 0 = \pi [\![\neg\vartheta(x, y)]\!]^\beta$.

This suggests that rings are unsuitable if we expect that a formula does not have the same interpretation as its negation. Grädel and Tannen have suggested the following definition to classify the semirings where we can expect exactly one of $\pi [\![\vartheta]\!]^\beta$ and $\pi [\![\neg\vartheta]\!]^\beta$ to be zero whenever $\pi$ is model-defining.

**(2.10) Definition** (Positive Semiring)**.** A semiring $K$ is *positive* if $\dagger_K : K \to \mathbb{B}$ defined as above is a homomorphism.

In order to verify the claim preceding the definition, it is sufficient to show that $\dagger_K(\pi [\![\vartheta]\!]^\beta) \neq \dagger_K(\pi [\![\neg\vartheta]\!]^\beta)$. By the fundamental property and with the fact that $\dagger_K$ is a homomorphism, this is equivalent to $(\dagger_K \circ \pi) [\![\vartheta]\!]^\beta \neq (\dagger_K \circ \pi) [\![\neg\vartheta]\!]^\beta$. Since $\pi$ was model-defining by assumption, $(\dagger_K \circ \pi)$ defines a model $\mathfrak{A}$ in the classical sense, hence the two interpretations must be distinct, since $\mathfrak{A}$ surely satisfies exactly one of the formulas $\vartheta$ and $\neg\vartheta$.

In conclusion, positive semirings enforce the convention that 0 corresponds to "false" and the remaining semiring elements represent different "levels" of truth. However, we would like to introduce even more structure to semirings by defining an order on the elements.

## 2.4 Natural Order

Order theory plays a crucial role in fixed-point logics due to the fact that least and greatest fixed points are defined with respect to an order. Moreover, as hinted above, infinitary operations are often defined via suprema and infima with respect to some order, hence order theory was brought to semiring semantics by Grädel and Tannen in order to perform provenance analysis on infinite games [GT19]. Their results are used and extended in [Naa19] and [DGNT19] for fixed-point logics. However, an order is also useful for model theory of first-order logic, since it may provide a meaning for semantic implication on semiring semantics that is parallel to the definition for classical semantics, where we say that $\varphi \models \psi$ if $[\![\varphi]\!]^\mathfrak{A} \leq [\![\psi]\!]^\mathfrak{A}$ for all suitable structures $\mathfrak{A}$. Hence, this section summarizes some of the order-theoretic results from [GT19], [Naa19] and [DGNT19] that are particularly useful for model theory.

Intuitively, an order on a semiring may be interpreted as "$b$ is more true than $a$ if $a < b$". This suggests that the order should be compatible with the semiring operations. Surely, we would expect that $\varphi \vee \psi$ is "at least as true as" $\varphi$ under any $K$-interpretation, which motivates the following definition, considering that the disjunction is interpreted by addition in $K$.

**(2.11) Definition** (Natural Order)**.** A semiring $K$ is *naturally ordered* if the order on $K$ defined by

$$a \leq b \quad \Leftrightarrow \quad \text{there is a } c \in K \text{ with } a + c = b$$

is a partial order. In that case, the aforementioned order is called the *natural order* on $K$ and the symbols $<$ and $\leq$ refer to this order.

By defining the natural order via semiring addition, it is guaranteed that the above intuition is upheld and the order is compatible with addition. Moreover, multiplication is also monotone thanks to distributivity, as stated in the following lemma.

**(2.12) Lemma.** On each naturally ordered semiring $K$, both addition and multiplication are monotone in each argument.

*Proof.* Thanks to commutativity, it suffices to prove the claim for the second argument of addition and multiplication respectively, that is

$$a \leq b \quad \text{implies} \qquad c + a \leq c + b \quad \text{and} \quad c \cdot a \leq c \cdot b \quad \text{for all } a, b, c \in K.$$

Since $a \leq b$, there is a $d \in K$ with $a + d = b$, hence $(c + a) + d = c + (a + d) = c + b$, which proves the first part. For multiplication, we have $c \cdot a + c \cdot d = c \cdot (a + d) = c \cdot b$, which ends the proof. □

Notice that once again, rings do not play along well with the definition of natural orders, since any ring $K$ with a nonzero element $a \neq 0$ has $0 + a = a$, but also $a + (-a) = 0$, which would imply $0 \leq a$ and $a \leq 0$ if $K$ was naturally ordered, a contradiction.

With addition increasing elements, we may also require that multiplication decreases elements, which corresponds to the intuition that $\varphi \wedge \psi$ is "at most as true as" $\varphi$ under any $K$-interpretation. In fact, we will see that on naturally ordered semirings, this is equivalent to the idea that every $a \in K$ "absorbs" the product $ab$ for all $b \in K$.

**(2.13) Definition** (Absorption)**.** A semiring $K$ is *absorptive* if $a + ab = a$ for all $a, b \in K$.

Clearly, multiplication decreases elements with respect to the natural order in any absorptive semiring, since $ab + a = a$ and $ab + b = b$, so $ab \leq a, b$. For the converse, notice that in a naturally ordered semiring, $a + ab \geq a$ by definition. If we assume that multiplication decreases elements, then $a + ab = a \cdot (1 + b) \leq a$ as well, hence $K$ is absorptive. Absorptive semirings have many useful properties summarized in the following lemma.

**(2.14) Lemma** (Properties of Absorptive Semirings)**.** Any absorptive semiring $K$ satisfies the following properties.

(1) $K$ is idempotent.

(2) $K$ is naturally ordered.

(3) $a \cdot b \leq a, b$ for all $a, b \in K$.

(4) 1 is the greatest element.

(5) $a + b = \sup\{a, b\}$ for all $a, b \in K$.

*Proof.* (1) immediately follows from absorption $(*)$ with $a + a = a + a \cdot 1 \stackrel{*}{=} a$.

(2) is important since (3), (4) and (5) rely on the natural order on $K$. Observe that the natural order is trivially reflexive and transitive, so it only remains to show that it is antisymmetric, that is, for $a, b \in K$, if $c, d \in K$ exist with $a+c = b$ and $b+d = a$, then $a = b$. We see that

$$a + b = a + (a + c) = (a + a) + c \stackrel{(1)}{=} a + c = b \quad \text{and}$$
$$a + b = (b + d) + b = (b + b) + d \stackrel{(1)}{=} b + d = a,$$

hence $a = b$ and $K$ is indeed naturally ordered.

(3) was already shown above as the motivation for considering absorptive semirings.

(4) is implied by (3) with $a = a \cdot 1 \stackrel{(3)}{\leq} 1$.

(5) follows by two observations. First, $a + b \geq a, b$ by definition of the natural order, hence $a + b$ is an upper bound on $\{a, b\}$. Then, for any upper bound $c \geq a, b$ in $K$, there are $d, e \in K$ such that $a + d = b + e = c$ by definition. Using (1), we obtain $(a + b) + (d + e) = (a + d) + (b + e) = c + c \stackrel{(1)}{=} c$, which shows that $a + b \leq c$ and $a + b$ is the least upper bound on $\{a, b\}$. ☐

Property (5) from the previous lemma relates absorptive semirings with distributive lattices. Indeed, each bounded distributive lattice $(K, \leq)$ can be viewed algebraically as a semiring $(K, \sup, \inf, \bot, \top)$, where addition is defined as the supremum of two elements, multiplication is defined as the infimum of two elements and the neutral elements $0, 1$ are the bottom and top elements of the lattice respectively. Clearly, $K$ is absorptive due to $\sup\{a, \inf\{a, b\}\} = a$ for all $a \in K$ and the natural order on $K$ is defined by the supremum of the lattice order, so it coincides with the lattice order.

Hence, a bounded distributive lattice satisfies all the properties (1) to (5) from lemma (2.14). This raises the question how absorptive semirings relate to lattices, which is answered by the following proposition.

**(2.15) Proposition.** The natural order of an absorptive semiring $(K, +, \cdot, 0, 1)$ is a bounded, distributive lattice and the operations $+$ and $\cdot$ on $K$ coincide with the lattice operations sup and inf if and only if multiplication is idempotent.

*Proof.* Suppose for "$\Leftarrow$" that multiplication is idempotent. Thanks to (5) from lemma (2.14), we already know that the natural order on $K$ admits suprema and $+$ coincides with the supremum of two elements. Additionally, thanks to (3), $a \cdot b$ is a lower bound on $\{a, b\}$. It remains to show $a \cdot b = \inf\{a, b\}$ by proving that it is the greatest lower bound. Suppose $c \leq a, b$ is a lower bound on $\{a, b\}$. With idempotence of multiplication $(*)$ and lemma (2.12), which states that multiplication is monotone $(\star)$, we have

$$c \stackrel{*}{=} c \cdot c \stackrel{\star}{\leq} a \cdot b,$$

hence $a \cdot b = \inf\{a, b\}$ is the greatest lower bound of $\{a, b\}$. Thus, the natural order is a lattice and the semiring operations coincide with suprema and infima, so the lattice is distributive as well. Moreover, 0 is clearly the least element and 1 is the greatest element thanks to (4) from lemma (2.14).

The direction "$\Rightarrow$" is easy, since $a \cdot a = \inf\{a, a\} = a$ for all $a \in A$ follows immediately from the assumption that $\cdot$ coincides with $\inf$. $\square$

With these definitions and observations, it is possible to define reasonable orders on semirings that are compatible with addition and multiplication to some degree, with the drawback that additional conditions must be satisfied by the semiring in question. For example, $(\mathbb{N}, +, \cdot, 0, 1)$ is naturally ordered, but not absorptive, hence multiplication does not decrease elements. Unfortunately, this is the case for the polynomial semiring $\mathbb{N}[X]$ as well. In the next chapter, we will focus on polynomials and show how absorption can be brought to them, as was done by Grädel and Tannen for provenance analysis on infinite games [GT19].

# Chapter 3

# Polynomials

In order to demonstrate the usefulness of polynomials in semiring semantics, we can pick up on the motivating idea from the introduction, where polynomials were used for provenance analysis in first-order logic, as suggested by Grädel and Tannen [GT17]. Let $A \coloneqq \{c, d, e\}$ be a universe with three elements, $\tau \coloneqq \{R\}$ consist of one unary relation and $\vartheta(\overline{a}) \coloneqq (Rc \wedge Rd) \vee \neg Re \vee \neg Rc$. We assume that the facts $Rc$ and $Rd$ are true while $Re$ is false. From that, we construct the $\mathbb{N}[X]$-interpretation $\pi$ with $X \coloneqq \{x, y, z\}$ as

$$\begin{aligned} \pi(Rc) &\coloneqq x, & \pi(\neg Rc) &\coloneqq 0, \\ \pi(Rd) &\coloneqq y, & \pi(\neg Rd) &\coloneqq 0, \\ \pi(Re) &\coloneqq 0 \quad \text{and} & \pi(\neg Re) &\coloneqq z. \end{aligned}$$

Each true literal is mapped to its own variable from $X$. Now, we obtain the polynomial $\pi\,[\![\vartheta(\overline{a})]\!] = xy + z$. We might want to interpret the same formula under different $K$-interpretations, such as the usual Boolean interpretation $\pi_{\mathbb{B}}$ or the counting interpretation $\pi_{\mathbb{N}}$ given by

$$\begin{aligned} \pi_{\mathbb{B}}(Rc) &\coloneqq \top, & \pi_{\mathbb{B}}(\neg Rc) &\coloneqq \bot, & \pi_{\mathbb{N}}(Rc) &\coloneqq 1, & \pi_{\mathbb{N}}(\neg Rc) &\coloneqq 0, \\ \pi_{\mathbb{B}}(Rd) &\coloneqq \top, & \pi_{\mathbb{B}}(\neg Rd) &\coloneqq \bot, & \pi_{\mathbb{N}}(Rd) &\coloneqq 1, & \pi_{\mathbb{N}}(\neg Rd) &\coloneqq 0, \\ \pi_{\mathbb{B}}(Re) &\coloneqq \bot, & \pi_{\mathbb{B}}(\neg Re) &\coloneqq \top, & \pi_{\mathbb{N}}(Re) &\coloneqq 0, & \pi_{\mathbb{N}}(\neg Re) &\coloneqq 1. \end{aligned}$$

Thanks to the fundamental property, there is no need to interpret the formula again, instead, we can simply plug the values into the polynomial $xy + z$ to obtain the desired results $\pi_{\mathbb{B}}\,[\![\vartheta(\overline{a})]\!] = (\top \wedge \top) \vee \top = \top$ and $\pi_{\mathbb{N}}\,[\![\vartheta(\overline{a})]\!] = 1 \cdot 1 + 1 = 2$.

This indicates that polynomials, or more specifically, $\mathbb{N}[X]$ constitutes the "most general" semiring, which was already observed by Green, Karvounarakis and Tannen in 2007, where they used polynomials to track provenance in databases [GKT07]. In order to capture the universality of $\mathbb{N}[X]$ formally, some algebraic observations are required.

## 3.1 Algebraic Basics

Intuitively, it is immediately clear that $\mathbb{N}[X]$ is "generated" by $X$. This means that we start from the variables in $X$ and each polynomial $p \in \mathbb{N}[X]$ can be constructed from the elements in $X$ by applying the semiring operations $+$ and $\cdot$ finitely many times. The goal of this section is to define this notion formally. In fact, any set of elements $G \subseteq K$ from a semiring $K$ generates some subset of $S \subseteq K$ in this manner and "generated" subsets have closure properties as shown below.

**(3.1) Definition** (Subsemiring)**.** A subset $S \subseteq K$ of a semiring $(K, +, \cdot, 0, 1)$ is a subsemiring of $K$ if $(S, +|_S, \cdot|_S, 0, 1)$ is a semiring, that is, $S$ equipped with the operations of $K$ restricted to $S$ is a semiring that shares the same neutral elements as $K$.

A simple way to check if $S$ is a subsemiring of $K$ is given by the following lemma.

**(3.2) Lemma** (Subsemiring Criteria)**.** $S \subseteq K$ for a semiring $(K, +, \cdot, 0, 1)$ is a subsemiring of $K$ if and only if $0, 1 \in S$ and $S$ is closed under addition and multiplication of $K$.

*Proof.* For "$\Rightarrow$", $(S, +|_S, \cdot|_S, 0, 1)$ being a semiring clearly implies $0, 1 \in S$ and $S$ being closed under $+$ and $\cdot$. The direction "$\Leftarrow$" can be verified by applying associativity and commutativity of $+$ and $\cdot$, distributivity of $\cdot$ over $+$ and the properties of the elements 0 and 1 from $K$. □

We can use the lemma immediately to prove that subsemirings are closed under intersection.

**(3.3) Lemma** (Closure of Subsemirings under Intersection)**.** If $(S_i)_{i\in I}$ with $S_i \subseteq K$ for all $i \in I$ are subsemirings of a semiring $(K, +, \cdot, 0, 1)$, then $S := \bigcap_{i\in I} S_i \subseteq K$ is a subsemiring of $K$ as well.

*Proof.* Since $0, 1 \in S_i$ for all $i \in I$ implies that $0, 1 \in S$ and for all $a, b \in S$, we have $a, b \in S_i$ for all $i \in I$ and therefore $a + b, a \cdot b \in S_i$ for all $i \in I$, which implies $a + b, a \cdot b \in S$, we can apply the subsemiring criteria above to conclude the proof. □

This allows us to precisely define the span of a set of generators $G \subseteq K$, which is, intuitively speaking, the set of elements from $K$ that can be expressed using elements from $G$ and finitely many semiring operations $+$ and $\cdot$.

**(3.4) Definition** (Span)**.** Let $K$ be a semiring and $G \subseteq K$. The *span* of $G$ on $K$, denoted by $\langle G\rangle_K$, is defined as

$$\langle G\rangle_K := \bigcap\{S \subseteq K \mid S \text{ is a subsemiring of } K \text{ with } S \supseteq G\} \subseteq K.$$

It is the smallest subsemiring of $K$ that contains $G$. The set $G$ is called a *generator* of $S$. We may omit $K$ if it is clear from the context.

Notice that semiring homomorphisms are also related to subsemirings. The following lemma shows that, unsurprisingly, semiring homomorphisms fulfill many properties that are parallel to the properties of homomorphisms between other algebraic structures such as rings.

**(3.5) Lemma** (Properties of Semiring Homomorphisms)**.** For two semirings $K$ and $L$, any semiring homomorphism $h : K \to L$ satisfies the following properties.

(1) If $h' : L \to L'$ is a semiring homomorphism into another semiring $L'$, then $h' \circ h : K \to L'$ is a semiring homomorphism as well.

(2) If $h$ is bijective, the inverse $h^{-1} : L \to K$ is also a semiring homomorphism.

(3) The image $h(K) \subseteq L$ of $h$ is a subsemiring of $L$.

*Proof.* (1) follows immediately from the properties of $h$ and $h'$, that is,

$$(h' \circ h)(e^K) = h'(h(e^K)) = h'(e^L) = e^{L'}$$

for the neutral elements $e \in \{0, 1\}$, and for $a, b \in K$ and $\star \in \{+, \cdot\}$, we have

$$(h' \circ h)(a \star b) = h'(h(a \star b)) = h'(h(a) \star h(b)) = h'(h(a)) \star h'(h(b)) = (h' \circ h)(a) \star (h' \circ h)(b).$$

(2) Clearly, $h^{-1}(e^L) = e^K$ for the neutral elements $e \in \{0, 1\}$. The compatibility with the operations $\circ \in \{+, \cdot\}$ is shown by observing that for all $a, b \in L$,

$$h^{-1}(a \circ b) = h^{-1}(h(h^{-1}(a)) \circ h(h^{-1}(b))) = h^{-1}(h(h^{-1}(a) \circ h^{-1}(b))) = h^{-1}(a) \circ h^{-1}(b).$$

(3) Since $h(e^K) = e^L$ for the neutral elements $e \in \{0, 1\}$, $e^L \in h(K)$ holds for both. In order to invoke the subsemiring criteria, it only remains to show that $h(K)$ is closed under $\circ \in \{+, \cdot\}$. For $a, b \in h(K)$, there are $a', b' \in K$ with $a = h(a')$ and $b = h(b')$, hence $a \circ b = h(a') \circ h(b') = h(a' \circ b')$ is in $h(K)$ as well, which proves the required closure properties. □

Clearly, a polynomial semiring such as $\mathbb{N}[X]$ is generated by $X$ according to the above definitions. However, we are still missing a formal proof for the universality of $\mathbb{N}[X]$.

## 3.2 Universal Property

First, we will formally define $\mathbb{N}[X]$ along with various kinds of polynomials.

**(3.6) Definition** (Monomial)**.** Let $X$ be a finite set of *variables* and $(E, +, 0)$ a commutative monoid of *exponents*. A *monomial* $m : X \to E$ is a function that assigns an exponent to each variable. If $X = \{x_1, \ldots, x_n\}$, we may informally write $m$ as $x_1^{e_1} \ldots x_n^{e_n}$. The set of all monomials with variables $X$ and exponents $E$ is denoted by $\mathrm{Mon}[E, X]$. The product of two monomials $m_1, m_2 \in \mathrm{Mon}[E, X]$ is defined by addition of exponents, that is $(m_1 \cdot m_2)(x) \coloneqq m_1(x) + m_2(x)$ for all $x \in X$.

For the set of exponents, the most common choice is $E \coloneqq \mathbb{N}$. However, we keep this general definition because in some contexts, we may allow infinite exponents or collapse the exponents to $\mathbb{B}$, in that case, a monomial is essentially a subset of $X$ and monomial multiplication corresponds to union.

Informally, a polynomial is simply a sum of monomials with coefficients.

**(3.7) Definition** (Polynomial)**.** For a finite set $X$ of variables, a commutative monoid $(E, +, 0)$ of exponents and a commutative semiring $(C, +, \cdot, 0, 1)$ of coefficients, a *polynomial* $p : \mathrm{Mon}[E, X] \to C$ is a function that assigns coefficients to each monomial such that $p(m) \neq 0$ for only finitely many monomials. The set of monomials with nonzero coefficient is called the *support* $\mathrm{supp}(p)$ of $p$. If $\mathrm{supp}(p) = \{m_1, \ldots, m_n\}$, we may informally write $p$ as a sum $c_1 m_1 + \ldots + c_n m_n$. The set of all polynomials with variables $X$, exponents $E$ and coefficients $C$ is denoted by $\mathrm{Poly}[C, E, X]$.

For two polynomials $p_1, p_2 \in \mathrm{Poly}[C, E, X]$, the sum is defined by addition of coefficients, that is $(p_1 + p_2)(m) \coloneqq p_1(m) + p_2(m)$ for all $m \in \mathrm{Mon}[E, X]$. The product is defined as

$$(p_1 \cdot p_2)(m) \coloneqq \sum_{m_1 \cdot m_2 = m, m_1 \in \mathrm{supp}(p_1), m_2 \in \mathrm{supp}(p_2)} p_1(m_1) \cdot p_2(m_2).$$

Note that the finiteness of polynomials is preserved by both operations.

*Formal power series* are defined the same way as polynomials, but we drop the finiteness condition. The set of formal power series with variables $X$, exponents $E$ and coefficients $C$ is denoted by $\mathrm{Poly}\,[\![C, E, X]\!]$.

Now, we have formally defined polynomials and set $\mathbb{N}[X] \coloneqq \mathrm{Poly}[\mathbb{N}, \mathbb{N}, X]$. We can finally provide the proof that $\mathbb{N}[X]$ is the "most general" semiring and can therefore be used for provenance tracking as in [GKT07] or [GT17].

**(3.8) Theorem** (Polynomial Evaluation)**.** Let $X$ be a set of variables and $K$ a semiring. Every function $e : X \to K$ that assigns values in $K$ to the variables induces a unique homomorphism $h_e : \mathbb{N}[X] \to K$ with $h(x) = e(x)$ for all $x \in X$. Moreover, the image of $h_e$ is precisely the span of the image of $e$ in $K$, that is $h_e(\mathbb{N}[X]) = \langle e(X) \rangle_K$.

*Proof.* We can explicitly provide the definition

$$h_e(p) \coloneqq \sum_{m \in \mathrm{supp}(p)} p(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \quad \text{for all } p \in \mathbb{N}[X].$$

Multiplication of elements of $K$ with natural numbers, denoted by $\cdot^{\mathbb{N}}$ above, is defined as usual by iterating the addition in $K$, a factor of 0 yields $0^K$. Similarly, exponentiation in $K$ with a natural number is defined as usual by iterating the multiplication in $K$, an exponent of 0 yields $1^K$. It is important to note that the intuitive multiplication and exponentiation laws still hold for those operations.

First, we prove that $h_e$ is indeed a homomorphism. Let $p_1, p_2 \in \mathbb{N}[X]$, then

$$\begin{aligned}
h_e(p_1 + p_2) &= \sum_{m \in \mathrm{supp}(p_1) \cup \mathrm{supp}(p_2)} (p_1(m) + p_2(m)) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \\
&= \sum_{m \in \mathrm{supp}(p_1) \cup \mathrm{supp}(p_2)} p_1(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} + p_2(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \\
&= \sum_{m \in \mathrm{supp}(p_1)} p_1(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} + \sum_{m \in \mathrm{supp}(p_2)} p_2(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \\
&= h_e(p_1) + h_e(p_2),
\end{aligned}$$

which proves compatibility with addition and $h_e(p_1 \cdot p_2)$

$$
\begin{aligned}
&= \sum_{m \in \operatorname{supp}(p_1 \cdot p_2)} \left( \sum_{m_1 \cdot m_2 = m} p_1(m_1) \cdot p_2(m_2) \right) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \\
&= \sum_{m \in \operatorname{supp}(p_1 \cdot p_2)} \sum_{m_1 \cdot m_2 = m} \left( (p_1(m_1) \cdot p_2(m_2)) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \right) \\
&= \sum_{m_1 \in \operatorname{supp}(p_1), m_2 \in \operatorname{supp}(p_2)} \left( (p_1(m_1) \cdot p_2(m_2)) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m_1(x)+m_2(x)} \right) \\
&= \sum_{m_1 \in \operatorname{supp}(p_1), m_2 \in \operatorname{supp}(p_2)} \left( (p_1(m_1) \cdot p_2(m_2)) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m_1(x)} \cdot e(x)^{m_2(x)} \right) \\
&= \sum_{m_1 \in \operatorname{supp}(p_1), m_2 \in \operatorname{supp}(p_2)} \left( p_1(m_1) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m_1(x)} \right) \cdot \left( p_2(m_2) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m_2(x)} \right) \\
&= \left( \sum_{m \in \operatorname{supp}(p_1)} p_1(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \right) \cdot \left( \sum_{m \in \operatorname{supp}(p_2)} p_2(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \right) \\
&= h_e(p_1) \cdot h_e(p_2)
\end{aligned}
$$

proves compatibility with multiplication. Finally, $0^{\mathbb{N}[X]}$ assigns the coefficient 0 to all monomials, hence $h_e(0^{\mathbb{N}[X]}) = 0^K$ is the empty sum and $1^{\mathbb{N}[X]}$ assigns the coefficient 1 to the monomial $m$ where all exponents are zero and 0 to all other monomials, hence

$$h_e(1^{\mathbb{N}[X]}) = 1 \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^0 = 1^K.$$

Now, the uniqueness of $h_e$ is easy to prove. Suppose that $h : \mathbb{N}[X] \to K$ is a homomorphism with $h(x) = e(x)$ for all $x \in X$. Clearly, we can rewrite each $p \in \mathbb{N}[X]$ as

$$p = \sum_{m \in \operatorname{supp}(p)} p(m) \cdot^{\mathbb{N}} \prod_{x \in X} x^{m(x)},$$

and since $h$ is compatible with addition and multiplication $(*)$, we obtain

$$
\begin{aligned}
h(p) &= h\left( \sum_{m \in \operatorname{supp}(p)} p(m) \cdot^{\mathbb{N}} \prod_{x \in X} x^{m(x)} \right) \\
&\overset{*}{=} \sum_{m \in \operatorname{supp}(p)} p(m) \cdot^{\mathbb{N}} \prod_{x \in X} h(x)^{m(x)} \\
&= \sum_{m \in \operatorname{supp}(p)} p(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \\
&= h_e(p).
\end{aligned}
$$

Recall that $\cdot^{\mathbb{N}}$ and exponentiation can be expressed by iterated addition and multiplication. This concludes the proof for the first part. Now, we move on to the second claim $h_e(\mathbb{N}[X]) = \langle e(X) \rangle_K$.

"$\subseteq$": The definition

$$h_e(p) = \sum_{m \in \operatorname{supp}(p)} p(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)}$$

makes it clear that $h_e(p)$ can be expressed by finitely many additions and multiplications involving only the elements from $e(X)$, hence each subsemiring of $K$ that contains $e(X)$, being closed under addition and multiplication by lemma (3.2), must contain $h_e(p)$, thus $h_e(\mathbb{N}[X]) \subseteq \langle e(X) \rangle_K$.

"$\supseteq$": According to definition (3.4), it suffices to show that $h_e(\mathbb{N}[X])$ is a subsemiring of $K$ and contains $e(X)$. Clearly, $h_e(\mathbb{N}[X])$ contains $h_e(X) = e(X)$. With observation (3) from lemma (3.5), $h_e(\mathbb{N}[X])$ is also a subsemiring of $K$, which ends the proof. $\square$

The property that each $e : X \to K$ induces a unique homomorphism $\mathbb{N}[X] \to K$ was crucial in the motivating example. This is called the *universal property* of $\mathbb{N}[X]$. In fact, $\mathbb{N}[X]$ has this property, because it is "freely generated" by $X$. Intuitively, this means that $\mathbb{N}[X]$ is generated by $X$, but two distinct representations only denote the same element if their equality follows from the commutative semiring axioms. As an example, consider the polynomial $x + y + x = 2x + y$, where the equality follows directly from associativity and commutativity of addition, whereas $2x \neq y^2$, because the semiring axioms do not imply the equality of $2x$ and $y^2$ directly. If we would map $x$ and $y$ to elements from a semiring such as $\mathbb{N}$, the induced values of $2x$ and $y^2$ may or may not be equal depending on the assignment, for example $x \mapsto 8$ and $y \mapsto 4$ would yield the value 16 for both polynomials, whereas $x \mapsto 3, y \mapsto 3$ would induce distinct values.

In fact, the universal property is the defining property for freely generated semirings. This means that we consider a semiring $K = \langle G \rangle_K$ to be freely generated if and only if it is possible to assign values from another semiring $L$ to the generators and lift this assignment to a homomorphism $h : K \to L$, which is similar to the evaluation of polynomials as functions shown above.

**(3.9) Definition** (Free Semiring)**.** Let $G$ be a set and $(K, +, \cdot, 0, 1)$ a semiring generated by $G$ with $K = \langle G \rangle_K$. We say that $K$ is *freely generated* by $G$ if for every semiring $L$ and every function $e : G \to L$, there is a unique homomorphism $h_e : K \to L$. In that case, the set $G$ is a set of *free generators* of $K$. We may refer to $K$ as a *free semiring* over $G$.

Clearly, $\mathbb{N}[X]$ is freely generated by $X$ according to theorem (3.8). Thanks to this insight, if we want to show that another semiring $K$ is freely generated by a finite set $G$, we do not need to go through the trouble of proving it directly, we can just use the following lemma, motivated by theorem (3.8).

**(3.10) Lemma** (Criteria for Free Semirings)**.** Let $G = \{g_1, \ldots, g_n\}$ be a finite set and $(K, +, \cdot, 0, 1)$ a semiring with $K = \langle G \rangle_K$. Define the variables $X = \{x_1, \ldots, x_n\}$ and the assignment $e : X \to G$ with $e(x_j) = g_j$ for $j \in \{1, \ldots, n\}$. Then, $K$ is freely generated by $G$ if and only if the unique homomorphism $h_e : \mathbb{N}[X] \to K$ induced by $e$ is injective. In that case, $h_e : \mathbb{N}[X] \xrightarrow{\sim} K$ is an isomorphism.

*Proof.* According to theorem (3.8), $h_e : \mathbb{N}[X] \to K$ is already a surjective homomorphism, since $K = \langle G \rangle_K$ and $e(X) = G$. Thus, $h_e$ is an isomorphism if and only if it is injective, which proves the second part of the lemma.

"$\Leftarrow$": If $h_e$ is injective, it is an isomorphism from $\mathbb{N}[X]$ into $K$, hence there is an inverse isomorphism $i : K \to \mathbb{N}[X]$. Consider a semiring $L$ and a function $f : G \to L$, which induces a variable assignment $(f \circ e) : X \to L$. Hence, there is a unique homomorphism $h_{(f\circ e)} : \mathbb{N}[X] \to L$ with $h_{(f\circ e)}(x) = (f \circ e)(x)$ for all $x \in X$ by theorem (3.8). Now, we construct $(h_{(f\circ e)} \circ i) : K \to L$, which is a homomorphism from $K$ to $L$ such that

$$(h_{(f\circ e)} \circ i)(g_j) = h_{(f\circ e)}(i(g_j)) \overset{*}{=} h_{(f\circ e)}(x_j) = (f \circ e)(x_j) = f(e(x_j)) = f(g_j)$$

holds for all $g_j \in G$. $(*)$ is due to $h_e(x_j) = e(x_j) = g_j$ and $i$ being the inverse of $h_e$. Now, we show that any homomorphism $h : K \to L$ with this property is equal to $h_{(f\circ e)} \circ i$. Construct the homomorphism $h \circ h_e : \mathbb{N}[X] \to L$. Since

$$(h \circ h_e)(x_j) = h(h_e(x_j)) = h(e(x_j)) = h(g_j) = f(g_j)$$

for all $j \in \{1, \dots, n\}$, we have $h \circ h_e = h_{(f\circ e)}$. Hence, $(h \circ h_e) \circ i = h_{(f\circ e)} \circ i$, which yields $h = h_{(f\circ e)} \circ i$ due to $(h \circ h_e) \circ i = h \circ (h_e \circ i) = h$ and $i$ being the inverse of $h_e$.

"$\Rightarrow$": If $K$ is freely generated by $G$, then $f : G \to X$ with $f(g_j) = x_j$ for $j \in \{1, \dots, n\}$ induces a unique homomorphism $h_f : K \to \mathbb{N}[X]$. Now, for each $i \in \{1, \dots, n\}$,

$$(h_f \circ h_e)(x_i) = h_f(h_e(x_i)) = h_f(e(x_i)) = h_f(g_i) = f(g_i) = x_i.$$

Hence, $h_f \circ h_e : \mathbb{N}[X] \to \mathbb{N}[X]$ is the unique homomorphism induced by $\mathrm{id}_X$. Clearly, $\mathrm{id}_{\mathbb{N}[X]}$ itself is the homomorphism induced by $\mathrm{id}_X$, hence we have $h_f \circ h_e = \mathrm{id}_{\mathbb{N}[X]}$, therefore $h_e$ is left-invertible and thus injective. □

In conclusion, any semiring $K$ which is freely generated by a finite set $G$ is isomorphic to $\mathbb{N}[X]$ for a set $X$ with $|X| = |G|$. Note that we could write $\mathbb{N}[G]$ directly, but we avoid this to prevent confusion between polynomials and terms in $K$. In semiring semantics, this property of polynomials allows us to make general statements about semirings by examining $\mathbb{N}[X]$.

## 3.3 Polynomials for Restricted Semirings

Unfortunately, we will see that $\mathbb{N}[X]$ does not always lend itself to provide model-theoretic results for semiring semantics. For example, as hinted before, it is not absorptive, which means that multiplication does not decrease elements, contrary to the expectation in semiring semantics. In order to introduce absorption while still keeping the generality results from the previous section, we will move to "absorptive polynomials" by adding absorption to $\mathbb{N}[X]$.

Absorptive polynomials were studied for provenance analysis in various settings in [GT19], [Naa19] and [DGNT19] and we will define them based on those papers. The idea is that while $\mathbb{N}[X]$ contains all polynomials generated by $X$, many of those polynomials would be equivalent in an absorptive setting. Since absorptive semirings are idempotent, the coefficients clearly collapse to $\{0, 1\}$, or $\mathbb{B}$ to be more precise. More importantly, "longer" monomials like $x^7y^9$ are absorbed by "shorter" monomials $x^4y$, since $x^4y + x^7y^9 = x^4y + x^4y \cdot x^3y^8 = x^4y$ by absorption law.

The easiest way to formally define this is by using homomorphisms. We start from polynomials $\mathbb{B}[X] := \mathrm{Poly}[\mathbb{B}, \mathbb{N}, X]$ with Boolean coefficients and then apply a pruning operator $s : \mathbb{B}[X] \to \mathbb{B}[X]$ that eliminates the monomials that are absorbed as described above. More formally, we introduce an order on monomials $\mathrm{Mon}[\mathbb{N}, X]$ where we set $m_1 \leq m_2$ if and only if $m_1(x) \geq m_2(x)$ for all $x \in X$. Then, we can view a polynomial $p \in \mathbb{B}[X]$ with Boolean coefficients as a subset $p \subseteq \mathrm{Mon}[\mathbb{N}, X]$ and simply define

$$s(p) \coloneqq \{m \in p \mid m \text{ is maximal in } p \text{ with respect to the monomial order}\},$$

which prunes all the monomials that are unnecessarily long and absorbed by others.

**(3.11) Definition** (Absorptive Polynomial)**.** For a set of variables $X$, the *absorptive polynomials* $\mathbb{S}[X]$ are defined as the image of $\mathbb{B}[X]$ under the pruning operation $s$, that is $(s(\mathbb{B}[X]), +, \cdot, 0, 1)$, where the pruning $s$ is applied after addition and multiplication, that is $p +^{\mathbb{S}[X]} q = s(p +^{\mathbb{B}[X]} q)$ and $p \cdot^{\mathbb{S}[X]} q = s(p \cdot^{\mathbb{B}[X]} q)$.

Notice that from this definition, it is immediately clear that $s$ is a surjective homomorphism $s : \mathbb{B}[X] \to \mathbb{S}[X]$. Since dropping the coefficients from $\mathbb{N}[X]$ constitutes a surjective homomorphism $h_c : \mathbb{N}[X] \to \mathbb{B}[X]$ with $h_c(p) \coloneqq \dagger_{\mathbb{N}} \circ p$ for all $p \in \mathbb{N}[X]$, the concatenation $s \circ h_c : \mathbb{N}[X] \to \mathbb{S}[X]$ is a surjective homomorphism as well according to lemma (3.5) and $\mathbb{S}[X]$ is indeed a semiring. Clearly, $\mathbb{S}[X]$ is absorptive. [GT19]

Originally, Grädel and Tannen defined absorptive polynomials to allow infinite exponents on monomials in order to find a general semiring for infinite games. This yields the semiring $\mathbb{S}^{\infty}[X]$, which has the advantage over $\mathbb{S}[X]$ that it admits infinitary operations [GT19]. However, since we focus on finite interpretations, we will mostly use $\mathbb{S}[X]$ instead.

Unsurprisingly, $\mathbb{S}[X]$ is constructed with the purpose to have the universal property with respect to absorptive semirings [GT19]. The notion of free semirings for smaller classes of semirings is defined below in order to formally capture the idea that $\mathbb{S}[X]$ is a "free, absorptive semiring".

**(3.12) Definition** (Free Semiring in Restricted Class)**.** Let $\mathcal{C}$ be a class of semirings, $G$ a set and $K = \langle G \rangle_K \in \mathcal{C}$. We say that $K$ is a freely generated $\mathcal{C}$-semiring with the free generators $G$ if for every semiring $L \in \mathcal{C}$, every function $e : G \to L$ induces a unique homomorphism $h_e : K \to L$. We may omit mentioning $\mathcal{C}$ if it is clear from the context.

Now, it remains to show that $\mathbb{S}[X]$ indeed has the universal property. We can prove this by starting from theorem (3.8) and following the definition of $\mathbb{S}[X]$ via $\mathbb{B}[X]$ and the homomorphisms $h_c : \mathbb{N}[X] \to \mathbb{B}[X]$ and $s : \mathbb{B}[X] \to \mathbb{S}[X]$ mentioned above.

**(3.13) Proposition.** $\mathbb{B}[X]$ is a free idempotent semiring generated by $X$.

*Proof.* Clearly, $\mathbb{B}[X]$ is idempotent. Let $K$ be an idempotent semiring. Recall from theorem (3.8) that each assignment $e : X \to K$ induces the unique homomorphism $h_e^{\mathbb{N}} : \mathbb{N}[X] \to K$ with

$$h_e^{\mathbb{N}}(p) \coloneqq \sum_{m \in \mathrm{supp}(p)} p(m) \cdot^{\mathbb{N}} \prod_{x \in X} e(x)^{m(x)} \quad \text{for all } p \in \mathbb{N}[X].$$

Idempotence of $K$ immediately yields

$$h_e^{\mathbb{N}}(p) \coloneqq \sum_{m \in \mathrm{supp}(p)} \prod_{x \in X} e(x)^{m(x)} \quad \text{for all } p \in \mathbb{N}[X].$$

We can now claim that the unique homomorphism $h_e^{\mathbb{B}} : \mathbb{B}[X] \to K$ that we are looking for is

$$h_e^{\mathbb{B}}(p) := \sum_{m \in \text{supp}(p)} \prod_{x \in X} e(x)^{m(x)} \quad \text{for all } p \in \mathbb{B}[X].$$

Recall that dropping coefficients $h_c : \mathbb{N}[X] \to \mathbb{B}[X]$ is a surjective homomorphism. Since $h_e^{\mathbb{N}}(p) = h_e^{\mathbb{B}}(h_c(p))$ for all $p \in \mathbb{N}[X]$ and $h_c$ is surjective, we can immediately conclude for $p, q \in \mathbb{B}[X]$ that $p', q' \in \mathbb{N}[X]$ exist with $h_c(p') = p$ and $h_c(q') = q$, hence

$$\begin{aligned} h_e^{\mathbb{B}}(p \circ q) &= h_e^{\mathbb{B}}(h_c(p') \circ h_c(q')) &&= h_e^{\mathbb{B}}(h_c(p' \circ q')) \\ &= h_e^{\mathbb{N}}(p' \circ q') &&= h_e^{\mathbb{N}}(p') \circ h_e^{\mathbb{N}}(q') \\ &= h_e^{\mathbb{B}}(h_c(p')) \circ h_e^{\mathbb{B}}(h_c(q)) &&= h_e^{\mathbb{B}}(p) \circ h_e^{\mathbb{B}}(q) \end{aligned}$$

for $\circ \in \{+, \cdot\}$. With $h_e^{\mathbb{B}}(r) = r$ for $r \in \{0, 1\}$, we conclude that $h_e^{\mathbb{B}}$ is a homomorphism.

For the uniqueness, suppose $h : \mathbb{B}[X] \to K$ is a homomorphism with $h(x) = e(x)$ for all $x \in X$. Clearly, each $p \in \mathbb{B}[X]$ can be expressed as

$$p = \sum_{m \in \text{supp}(p)} \prod_{x \in X} x^{m(x)},$$

hence we obtain the equality

$$\begin{aligned} h(p) &= h\left( \sum_{m \in \text{supp}(p)} \prod_{x \in X} x^{m(x)} \right) \\ &= \sum_{m \in \text{supp}(p)} \prod_{x \in X} h(x)^{m(x)} \\ &= \sum_{m \in \text{supp}(p)} \prod_{x \in X} e(x)^{m(x)} \\ &= h_e^{\mathbb{B}}(p). \end{aligned}$$

This concludes the proof. With a similar argument as in theorem (3.8), we can also show that $h_e^{\mathbb{B}}(\mathbb{B}[X]) = \langle e(X) \rangle_K$. □

**(3.14) Proposition.** $\mathbb{S}[X]$ is a free absorptive semiring generated by $X$.

*Proof sketch.* We can use a similar approach as above. Use the fact that the function $s : \mathbb{B}[X] \to \mathbb{S}[X]$ from above that eliminates unnecessary monomials is a surjective homomorphism. Then, observe that each absorptive semiring $K$ is idempotent, hence $e : X \to K$ induces the homomorphism $h_e^{\mathbb{B}} : \mathbb{B}[X] \to K$ defined as

$$h_e^{\mathbb{B}}(p) := \sum_{m \in \text{supp}(p)} \prod_{x \in X} e(x)^{m(x)} \quad \text{for all } p \in \mathbb{B}[X]$$

from above. Now, set

$$h_e^{\mathbb{S}}(p) := \sum_{m \in \text{supp}(p) \text{ maximal}} \prod_{x \in X} e(x)^{m(x)} \quad \text{for all } p \in \mathbb{B}[X]$$

and observe that $h_e^{\mathbb{S}}(p) = h_e^{\mathbb{B}}(s(p))$, since the products from non-maximal monomials are absorbed in $K$. Proceed as above to show that $h_e^{\mathbb{S}}$ is indeed a semiring homomorphism. Finally, for uniqueness, observe that any absorptive polynomial can be written as

$$p = \sum_{m \in \text{supp}(p) \text{ maximal}} \prod_{x \in X} x^{m(x)},$$

since all its monomials are maximal. Proceed as above to conclude the proof. □

To conclude the section, we would like to mention multiplicatively idempotent semirings as well, since they play a crucial role in the next chapter. The corresponding polynomial semirings are constructed by simply collapsing exponents to $\mathbb{B}$. The non-absorptive version of a multiplicatively idempotent semiring is the why-semiring $\mathbb{W}[X] := \text{Poly}[\mathbb{B}, \mathbb{B}, X]$, which can be obtained from $\mathbb{B}[X]$ by dropping exponents. For absorptive semirings, we use $\text{PosBool}[X]$, which is obtained from $\mathbb{S}[X]$ by dropping exponents. Note that in both cases, dropping exponents is a homomorphism. Thus, we can derive the following propositions.

**(3.15) Proposition.** $\mathbb{W}[X]$ is freely generated by $X$ in the class of all semirings that are both idempotent and multiplicatively idempotent.

**(3.16) Proposition.** $\text{PosBool}[X]$ is freely generated by $X$ in the class of all semirings that are absorptive and multiplicatively idempotent.

The proof for both statements is derived from theorem (3.8) similarly to the proof of proposition (3.13). Hence, both $\mathbb{W}[X]$ and $\text{PosBool}[X]$ are universal in their respective classes of semirings. Note that due to proposition (2.15), we may also say that $\text{PosBool}[X]$ represents semirings induced by bounded distributive lattices.

Note that all polynomial semirings from this section were studied before as candidates for provenance semirings by Naaf, who also provides an overview of the homomorphisms that relate them to each other [Naa19].

# Chapter 4

# Characterization of Elementary Equivalence

With the algebraic foundations for semirings being established, we would like to return to model theory. One of the core concepts of model theory is elementary equivalence between structures. In classical semantics, characterizing elementary equivalence for a logic provides an indicator of its expressive power. Intuitively, a logic is more expressive the "closer" elementary equivalence comes to isomorphism and the "most powerful" logic would be a logic that is able to express anything up to isomorphism, since it would be undesirable for a logic to differentiate between isomorphic structures, which are the same up to "renaming". If two structures $\mathfrak{A}, \mathfrak{B}$ are not isomorphic, but elementarily equivalent in some logic $L$, denoted as $\mathfrak{A} \equiv \mathfrak{B}$, then the logic can be thought of as "too weak" to separate them. Of course, logics are limited by the fact that we often impose algorithmic requirements on them, such as the decidability of model checking, that is, $\mathfrak{A} \models \varphi$ or $\mathfrak{A} \not\models \varphi$ for any sentence $\varphi$. Therefore, it would be unreasonable to define a logic with unlimited expressive power and we usually have a trade-off between expressive power and algorithmic properties.

Focusing on first-order logic, it is well-known that it lacks the capability of describing infinite structures up to isomorphism thanks to the Löwenheim-Skolem theorems. We can provide two concrete examples, for an empty signature, we have $\mathbb{N} \equiv \mathbb{R}$ and for the signature $\tau = \{<\}$, $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$, where $<$ denotes the usual orders on $\mathbb{Q}$ and $\mathbb{R}$ respectively. However, for finite structures $\mathfrak{A} := (A = \{a_1, \dots, a_n\}, \tau)$, it is possible to define the *characteristic sentence*

$$\varphi_{\mathfrak{A}} := \exists x_1 \dots \exists x_n \left( \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1 \leq i \leq n} y = x_i \right) \wedge \bigwedge_{L \in \mathrm{Lit}_A(\tau), \mathfrak{A} \models L} L[\overline{a}/\overline{x}] \right),$$

which describes $\mathfrak{A}$ up to isomorphism. The first part of the formula requires the existence of exactly $n$ elements and in the last part, we simply use a conjunction of all true literals in $\mathfrak{A}$ and replace $a_i$ with $x_i$ for all $i \in \{1, \dots, n\}$. Clearly, $\mathfrak{A} \models \varphi_{\mathfrak{A}}$ with the assignment $\beta : x_i \mapsto a_i$ for $i \in \{1, \dots, n\}$, and any structure $\mathfrak{B} = (B, \tau)$ with $\mathfrak{B} \models \varphi_{\mathfrak{A}}$ is isomorphic to $\mathfrak{A}$, since the assignment $\gamma : \{x_1, \dots, x_n\} \to B$ used to satisfy $\varphi_{\mathfrak{A}}$ induces an isomorphism $\gamma \circ \beta^{-1} : \mathfrak{A} \xrightarrow{\sim} \mathfrak{B}$.

As a consequence, any two finite structures with $\mathfrak{A} \equiv \mathfrak{B}$ are also isomorphic due to $\mathfrak{B} \models \varphi_{\mathfrak{A}}$. This raises the question whether the same statement holds for finite $K$-interpretations $\pi_A$ and $\pi_B$. Of course, we first need to update the definitions of isomorphism and elementary equivalence to accommodate $K$-interpretations.

**(4.1) Definition** (Isomorphism)**.** Two $K$-interpretations over the same signature $\pi_A : \mathrm{Lit}_A(\tau) \to K, \pi_B : \mathrm{Lit}_B(\tau) \to K$ are *isomorphic*, denotes as $\pi_A \cong \pi_B$, if there is a bijective function $\sigma : A \to B$ such that for all $k$-ary $R \in \tau$ and $\overline{a} = (a_1, \dots, a_k) \in A^k$,

$$\begin{aligned} \pi_A(Ra_1 \dots a_k) &= \pi_B(R\sigma(a_1) \dots \sigma(a_k)) \quad \text{and} \\ \pi_A(\neg Ra_1 \dots a_k) &= \pi_B(\neg R\sigma(a_1) \dots \sigma(a_k)). \end{aligned}$$

We may informally write the condition as $\pi_A = \pi_B \circ \sigma$. A function $\sigma$ with this property is called an *isomorphism* and we denote it by $\sigma : \pi_A \xrightarrow{\sim} \pi_B$.

Isomorphic $K$-interpretations are essentially the same up to "renaming" of elements, hence no logic should distinguish between them. The isomorphism lemma states this formally.

**(4.2) Lemma** (Isomorphism Lemma)**.** Let $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$ be two isomorphic $K$-interpretations and $\sigma : \pi_A \xrightarrow{\sim} \pi_B$ an isomorphism. For any $\mathsf{FO}(\tau)$-formula $\vartheta(\overline{x})$ with free variables $\overline{x} = (x_1, \dots, x_k)$, we have

$$\pi_A \llbracket \vartheta(\overline{x}) \rrbracket^{\beta} = \pi_B \llbracket \vartheta(\overline{x}) \rrbracket^{\sigma \circ \beta}$$

for all $\beta : \{x_1, \dots, x_k\} \to A$. Informally, $\beta$ corresponds to $\overline{a} = (a_1, \dots, a_k) \in A^k$ with $\beta(x_i) = a_i \in A$ and $(\sigma \circ \beta)(x_i) = \sigma(\beta(x_i)) = \sigma(a_i) \in B$ for $i \in \{1, \dots, k\}$.

*Proof.* We prove the statement by induction on $\vartheta(\overline{x})$, assuming that it is in negation normal form. It is sufficient to follow the semiring semantics from definition (2.4).

(1) If $\vartheta(\overline{x}) \in \{x_1 = x_2, \neg x_1 = x_2\}$ with $x_1, x_2 \in V$, then

$$\begin{aligned} \pi_B \llbracket x_1 = x_2 \rrbracket^{\sigma \circ \beta} &= \begin{cases} 1 & \text{if } \sigma(\beta(x_1)) = \sigma(\beta(x_2)), \\ 0 & \text{otherwise} \end{cases} \quad \text{and} \\ \pi_B \llbracket \neg x_1 = x_2 \rrbracket^{\sigma \circ \beta} &= \begin{cases} 1 & \text{if } \sigma(\beta(x_1)) \neq \sigma(\beta(x_2)), \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Since $\sigma$ is bijective, $\sigma(\beta(x_1)) = \sigma(\beta(x_2))$ is equivalent to $\beta(x_1) = \beta(x_2)$, hence

$$\begin{aligned} \pi_B \llbracket x_1 = x_2 \rrbracket^{\sigma \circ \beta} &= \left. \begin{cases} 1 & \text{if } \beta(x_1) = \beta(x_2), \\ 0 & \text{otherwise} \end{cases} \right\} = \pi_A \llbracket x_1 = x_2 \rrbracket^{\beta} \\ \pi_B \llbracket \neg x_1 = x_2 \rrbracket^{\sigma \circ \beta} &= \left. \begin{cases} 1 & \text{if } \beta(x_1) \neq \beta(x_2), \\ 0 & \text{otherwise} \end{cases} \right\} = \pi_A \llbracket \neg x_1 = x_2 \rrbracket^{\beta}. \end{aligned}$$

(2) For $\vartheta(\overline{x}) \in \{Rx_{i_1} \dots x_{i_\ell}, \neg Rx_{i_1} \dots x_{i_\ell}\}$ with $R \in \tau$ $\ell$-ary and $\{x_{i_1}, \dots, x_{i_\ell}\} \subseteq X$,

we have

$$\begin{aligned}
\pi_A \left[\!\left[ Rx_{i_1} \dots x_{i_\ell} \right]\!\right]^\beta &= \pi_A(R\beta(x_{i_1}), \dots, \beta(x_{i_\ell})) \\
&\overset{*}{=} \pi_B(R\sigma(\beta(x_{i_1})), \dots, \sigma(\beta(x_{i_\ell}))) \\
&= \pi_B \left[\!\left[ Rx_{i_1} \dots x_{i_\ell} \right]\!\right]^{\sigma\circ\beta} \qquad \text{and} \\
\pi_A \left[\!\left[ \neg Rx_{i_1} \dots x_{i_\ell} \right]\!\right]^\beta &= \pi_A(\neg R\beta(x_{i_1}), \dots, \beta(x_{i_\ell})) \\
&\overset{*}{=} \pi_B(\neg R\sigma(\beta(x_{i_1})), \dots, \sigma(\beta(x_{i_\ell}))) \\
&= \pi_B \left[\!\left[ \neg Rx_{i_1} \dots x_{i_\ell} \right]\!\right]^{\sigma\circ\beta}.
\end{aligned}$$

(4) If $\vartheta(\overline{x}) = \varphi(\overline{x}) \circ \psi(\overline{x})$ with $\circ \in \{\vee, \wedge\}$, then

$$\begin{aligned}
\pi_A \left[\!\left[ \varphi(\overline{x}) \vee \psi(\overline{x}) \right]\!\right]^\beta &= \pi_A \left[\!\left[ \varphi(\overline{x}) \right]\!\right]^\beta + \pi_A \left[\!\left[ \psi(\overline{x}) \right]\!\right]^\beta \\
&\overset{\star}{=} \pi_B \left[\!\left[ \varphi(\overline{x}) \right]\!\right]^{\sigma\circ\beta} + \pi_B \left[\!\left[ \psi(\overline{x}) \right]\!\right]^{\sigma\circ\beta} \\
&= \pi_B \left[\!\left[ \varphi(\overline{x}) \vee \psi(\overline{x}) \right]\!\right]^{\sigma\circ\beta} \quad \text{and} \\
\pi_A \left[\!\left[ \varphi(\overline{x}) \wedge \psi(\overline{x}) \right]\!\right]^\beta &= \pi_A \left[\!\left[ \varphi(\overline{x}) \right]\!\right]^\beta \cdot \pi_A \left[\!\left[ \psi(\overline{x}) \right]\!\right]^\beta \\
&\overset{\star}{=} \pi_B \left[\!\left[ \varphi(\overline{x}) \right]\!\right]^{\sigma\circ\beta} \cdot \pi_B \left[\!\left[ \psi(\overline{x}) \right]\!\right]^{\sigma\circ\beta} \\
&= \pi_B \left[\!\left[ \varphi(\overline{x}) \wedge \psi(\overline{x}) \right]\!\right]^{\sigma\circ\beta}.
\end{aligned}$$

(5) If $\vartheta(\overline{x}) = Qx\varphi(\overline{x}, x)$ with $Q \in \{\exists, \forall\}$, then

$$\begin{aligned}
\pi_A \left[\!\left[ \exists x\varphi(\overline{x}, x) \right]\!\right]^\beta &= \sum_{a\in A} \pi_A \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{\beta[x\mapsto a]} \\
&\overset{\star}{=} \sum_{a\in A} \pi_B \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{\sigma\circ(\beta[x\mapsto a])} \\
&= \sum_{a\in A} \pi_B \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{(\sigma\circ\beta)[x\mapsto\sigma(a)]} \\
&\overset{r}{=} \sum_{b\in B} \pi_B \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{(\sigma\circ\beta)[x\mapsto b]} \\
&= \pi_B \left[\!\left[ \exists x\varphi(\overline{x}, x) \right]\!\right]^{\sigma\circ\beta} \quad \text{and}
\end{aligned}$$

$$\begin{aligned}
\pi_A \left[\!\left[ \forall x\varphi(\overline{x}, x) \right]\!\right]^\beta &= \prod_{a\in A} \pi_A \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{\beta[x\mapsto a]} \\
&\overset{\star}{=} \prod_{a\in A} \pi_B \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{\sigma\circ(\beta[x\mapsto a])} \\
&= \prod_{a\in A} \pi_B \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{(\sigma\circ\beta)[x\mapsto\sigma(a)]} \\
&\overset{r}{=} \prod_{b\in B} \pi_B \left[\!\left[ \varphi(\overline{x}, x) \right]\!\right]^{(\sigma\circ\beta)[x\mapsto b]} \\
&= \pi_B \left[\!\left[ \forall x\varphi(\overline{x}, x) \right]\!\right]^{\sigma\circ\beta}.
\end{aligned}$$

Since $\sigma$ is bijective, we merely rearrange the sum or product in the steps marked with $(r)$, which does not change the value.

Steps with $(*)$ use the isomorphism property $\pi_A = \pi_B \circ \sigma$ of $\sigma$ from definition (4.1) and steps marked with $(\star)$ require the induction hypothesis. □

Note that the isomorphism lemma also works for infinite $K$-interpretations, since we assume that infinitary operations respect bijections. If two $K$-interpretations $\pi_1 \cong \pi_2$ are isomorphic, no $\mathsf{FO}(\tau)$-sentence can distinguish those $K$-interpretations. However, we will show later that the converse does not hold. For that, we formally define the notion of $K$-interpretations that are "indistinguishable" by $\mathsf{FO}(\tau)$.

**(4.3) Definition** (Elementary Equivalence)**.** For two $K$-interpretations over the same signature $\tau$ $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$ with $k \in \mathbb{N}$ fixed elements $\overline{a} = (a_1, \ldots, a_k) \in A^k$ and $\overline{b} = (b_1, \ldots, b_k) \in B^k$, we say that $\pi_A, \overline{a}$ and $\pi_B, \overline{b}$ are *elementarily equivalent*, denoted by $\pi_A, \overline{a} \equiv \pi_B, \overline{b}$, if

$$\pi_A \llbracket \vartheta(\overline{a}) \rrbracket = \pi_B \llbracket \vartheta(\overline{b}) \rrbracket$$

holds for all $\vartheta(\overline{x}) \in \mathsf{FO}(\tau)$ with $k$ free variables. Often, $k$ will be 0, then we omit $\overline{a}$ and $\overline{b}$. We may also simply say "equivalent" instead of "elementarily equivalent".

For $m \in \mathbb{N}$, we say that $\pi_A, \overline{a}$ and $\pi_B, \overline{b}$ are $m$-equivalent, denoted as $\pi_A, \overline{a} \equiv_m \pi_B, \overline{b}$, if

$$\pi_A \llbracket \vartheta(\overline{a}) \rrbracket = \pi_B \llbracket \vartheta(\overline{b}) \rrbracket$$

for all $\vartheta(\overline{x}) \in \mathsf{FO}(\tau)$ with $k$ free variables and quantifier rank $\mathrm{qr}(\vartheta(\overline{x}))$ at most $m$.

**(4.4) Corollary** (to the Isomorphism Lemma)**.** If $\pi_A \cong \pi_B$ for two $K$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$, then $\pi_A \equiv \pi_B$. Moreover, if $\sigma : \pi_A \xrightarrow{\sim} \pi_B$ is an isomorphism, then $\pi_A, \overline{a} \equiv \pi_B, \overline{b}$ for all pairs of $k$-tuples $\overline{a} = (a_1, \ldots, a_k) \in A^k$ and $\overline{b} = (b_1, \ldots, b_k) \in B^k$ with $\sigma(a_i) = b_i$ for all $i \in \{1, \ldots, k\}$.

Before we move on to the attempt to characterize elementary equivalence, we will justify these definitions of isomorphism and elementary equivalence. Unlike $\mathbb{B}$, general semirings $K$ usually contain more than two elements. Therefore, we may consider weaker definitions of isomorphism and equivalence.

## 4.1 Congruence Relations

As an example for a weaker definition of equivalence, consider two $\mathbb{N}$-interpretations $\pi_{\mathfrak{A}}, \pi_{\mathfrak{B}}$ and a sentence $\psi \in \mathsf{FO}(\tau)$ such that $\pi_{\mathfrak{A}} \llbracket \psi \rrbracket = 42$ and $\pi_{\mathfrak{B}} \llbracket \psi \rrbracket = 43$. The concrete definitions of $\pi_{\mathfrak{A}}, \pi_{\mathfrak{B}}$ and $\psi$ are not important, for example, we may use $\mathbb{N}$-interpretations for proof counting as in the introduction. The conclusion would be that $\psi$ has 42 proofs in $\mathfrak{A}$ and 43 proofs in $\mathfrak{B}$. Now, our strict definition of equivalence would require equality of $\pi_{\mathfrak{A}} \llbracket \psi \rrbracket$ and $\pi_{\mathfrak{B}} \llbracket \psi \rrbracket$, hence $\pi_{\mathfrak{A}}$ and $\pi_{\mathfrak{B}}$ are not equivalent. However, $\psi$ is still "true" in both $K$-interpretations if we disregard the exact number of proofs.

Generally speaking, we might define equivalence in a way that merges certain elements of $K$ into an equivalence class. In the above example, we may regard all nonzero elements of $\mathbb{N}$ as equivalent. More formally, we will introduce a congruence relation $\sim \subseteq K \times K$ on $K$ and consider congruent elements as equal for the purpose of elementary equivalence.

**(4.5) Definition** (Congruence Relation)**.** A *congruence relation* on a semiring $K$ is an equivalence relation $\sim \subseteq K \times K$ such that for all $a_1, b_1, a_2, b_2 \in K$ with $a_1 \sim a_2$ and $b_1 \sim b_2$, we have $(a_1 + b_1) \sim (a_2 + b_2)$ and $(a_1 \cdot b_1) \sim (a_2 \cdot b_2)$.

Since $\sim$ respects the semiring operations, if $0 \not\sim 1$ holds as well, the quotient structure $K/{\sim} = \{[a]_\sim \mid a \in K\}$ is a semiring with the operations on equivalence classes defined in the obvious manner. If we look back at the introductory example and choose $\sim \subseteq \mathbb{N} \times \mathbb{N}$ as $\sim := \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a = b = 0 \text{ or } a, b > 0\}$, we obtain the equivalence classes $[0]_\sim$ and $[1]_\sim$, hence $\mathbb{N}/{\sim} \cong \mathbb{B}$ and we only distinguish the natural numbers based on their "truth". This intuition allows us to provide an alternative definition of elementary equivalence.

**(4.6) Definition** ($\sim$-equivalence)**.** Consider two $K$-interpretations $\pi_A, \pi_B$ over $\tau$ and a congruence relation $\sim \subseteq K \times K$ on $K$. We say that $\pi_A, \pi_B$ are $\sim$-equivalent, denoted by $\pi_A \equiv_\sim \pi_B$ if for all sentences $\psi \in \mathsf{FO}(\tau)$, $\pi_A [\![\psi]\!] \sim \pi_B [\![\psi]\!]$.

This enables us to use a notion of equivalence that is as coarse or as fine-grained as needed. Choosing the trivial congruence relation $\sim := \{(a, a) \in K \times K \mid a \in K\}$ yields the usual notion of equivalence where $\sim$ is equality. For positive semirings, $\sim := \{(a, b) \in K \times K \mid \dagger_K(a) = \dagger_K(b)\}$ is also a congruence relation. This congruence relation is the "most coarse", since it only distinguishes between zero and nonzero elements. Interestingly, the use of the homomorphism $\dagger_K$ demonstrates that congruence relations are strongly related to homomorphisms.

**(4.7) Proposition.** For a semiring $K$, every congruence relation $\sim \subseteq K \times K$ with $0 \not\sim 1$ induces a homomorphism $h_\sim : K \to K/{\sim}$ with $h_\sim(a) = [a]_\sim$ for all $a \in K$ and every homomorphism $h : K \to L$ into another semiring induces a congruence relation $\sim_h \subseteq K \times K$ with $a \sim_h b :\Leftrightarrow h(a) = h(b)$ so that $0 \not\sim_h 1$ and $K/{\sim_h} \cong h(K)$.

*Proof.* The first statement follows from the definition of $K/{\sim}$, which already yields $h_\sim(a \circ b) = [a \circ b]_\sim = [a]_\sim \circ [b]_\sim = h_\sim(a) \circ h_\sim(b)$ for $\circ \in \{+, \cdot\}$.

For the second part, it is clear that $\sim_h$ is an equivalence relation, since it is based on an equality. Now, if $a_1, b_1, a_2, b_2 \in K$ such that $a_1 \sim a_2$ and $b_1 \sim b_2$, then $h(a_1) = h(a_2)$ and $h(b_1) = h(b_2)$, so $h(a_1 \circ b_1) = h(a_1) \circ h(b_1) = h(a_2) \circ h(b_2) = h(a_2 \circ b_2)$, which implies $(a_1 \circ b_1) \sim_h (a_2 \circ b_2)$ for $\circ \in \{+, \cdot\}$. Since $h(0) \neq h(1)$, we have $0 \not\sim_h 1$.

$K/{\sim_h} \cong h(K)$ holds, since $i : K/{\sim_h} \to h(K)$ with $i([a]_{\sim_h}) = h(a)$ for all $a \in K$ is an isomorphism. Due to the definition of $\sim_h$, $i$ is clearly well-defined and injective, surjectivity is trivial. Moreover, $i([0]_{\sim_h}) = h(0) = 0$ and $i([1]_{\sim_h}) = h(1) = 1$ and $i([a]_{\sim_h} \circ [b]_{\sim_h}) = i([a \circ b]_{\sim_h}) = h(a \circ b) = h(a) \circ h(b) = i([a]_{\sim_h}) \circ i([b]_{\sim_h})$ for $\circ \in \{+, \cdot\}$, which ends the proof. ☐

Using the fundamental property, this justifies our definition (4.3) of elementary equivalence and eliminates the need to consider $\sim$-equivalence separately. Instead of considering $\sim$-equivalence of $\pi_A, \pi_B$ on $K$, we can simply apply the induced homomorphism $h_\sim$ and consider the usual equivalence of $(h_\sim \circ \pi_A), (h_\sim \circ \pi_B)$ on $K/{\sim}$, which is formalized by the following lemma.

**(4.8) Lemma** (Characterization of $\sim$-equivalence)**.** Let $\pi_A, \pi_B$ be $K$-interpretations over the signature $\tau$ and $\sim$ a congruence relation on $K$ with the induced homomorphism $h_\sim : K \to K/{\sim}$. Then, $\pi_A \equiv_\sim \pi_B$ on $K$ if and only if $(h_\sim \circ \pi_A) \equiv (h_\sim \circ \pi_B)$ on $K/{\sim}$.

*Proof.* By definition, $\pi_A \equiv_\sim \pi_B$ holds if and only if $\pi_A [\![\psi]\!] \sim \pi_B [\![\psi]\!]$ for all $\mathsf{FO}(\tau)$-sentences $\psi$. Clearly, this is equivalent to $h_\sim(\pi_A [\![\psi]\!]) = h_\sim(\pi_B [\![\psi]\!])$. Applying the fundamental property yields that this is equivalent to $(h_\sim \circ \pi_A)\,[\![\psi]\!] = (h_\sim \circ \pi_B)\,[\![\psi]\!]$ for all sentences $\psi \in \mathsf{FO}(\tau)$, which is the definition of $(h_\sim \circ \pi_A) \equiv (h_\sim \circ \pi_B)$. □

Obviously, we can apply the idea of using congruences to the variations of equivalence given in definition (4.3), such as $m$-equivalence or elementary equivalence with fixed elements from the universes $A$ and $B$. However, the previous lemma can easily be adapted to these variations and shows that $\sim$-equivalence collapses to the usual equivalence anyway, thus, we do not need to bother pursuing this approach. A similar observation can be made if we define isomorphism via a congruence relation. Hence, our definitions of isomorphism and elementary equivalence are reasonable and we can move on to the attempt to relate them.

## 4.2 Approach with a Single Unary Relation

With the adapted definitions from the previous section, we can return to the question of whether elementary equivalence in first-order logic implies isomorphism over finite universes under semiring semantics, as is the case in classical semantics. In other words, the remainder of this chapter is dedicated to the following problem. *For two $K$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$ over finite universes $A, B$ with the same, finite signature $\tau$, does $\pi_A \equiv \pi_B$ imply $\pi_A \cong \pi_B$?*

Surely, we would not expect that first-order logic "loses" expressive power in the setting of semiring semantics compared to classical semantics, however, our notion of isomorphism of $K$-interpretations is stronger than the classical notion due to $K$ usually having more than two elements. Hence, we would like to know whether elementary equivalence on $K$-interpretations is able to "keep up". Our intuition is that this is not the case and we will therefore attempt to construct a counterexample in a very simple class of semirings.

**(4.9) Definition** (Min-Max-Semiring)**.** A finite set $K$ equipped with a linear order $<$ and $|K| \geq 2$ induces a *min-max-semiring* $(K, +, \cdot, 0, 1)$ where the operations $+ := \max_<$ and $\cdot := \min_<$ are defined via maxima and minima with respect to $<$ and the constants are $0 := \min_< K$ and $1 := \max_< K$.

It is easy to see that $(K, +, \cdot, 0, 1)$ is indeed a semiring. Moreover, we observe that it is naturally ordered by $<$, absorptive and both $+$ and $\cdot$ are idempotent. Min-max-semirings are a very straightforward generalization of $\mathbb{B}$, in fact, for $|K| = 2$, the min-max-semiring $(K, +, \cdot, 0, 1)$ is isomorphic to $(\mathbb{B}, \vee, \wedge, \bot, \top)$. Additionally, for a min-max-semiring $(K, \max, \min, 0, 1)$, we can reverse the underlying order and obtain $(K, \max, \min, 0, 1) \cong (K, \min, \max, 1, 0)$. However, $(K, \min, \max, 1, 0)$ is not naturally ordered by its underlying order anymore. Hence, for example, the access control semiring $\mathbb{A} = (\{P, C, S, T, 0\}, \min, \max, 0, P)$ that was briefly mentioned in the second chapter is isomorphic to a min-max-semiring with 5 elements, but its natural order is the reverse of the access token order $P < C < S < T < 0$.

The first idea for a possible counterexample is to use the fact that existential and universal quantifiers in min-max-semirings are interpreted by maxima and minima respectively. Hence, if we use the min-max-semiring $K_3 := (\{0, 1, 2, 3\}, \max, \min, 0, 3)$ with a sufficient number of elements, we suspect that the element 2 might be inaccessible to FO-formulas, because it is “in between” 1 and 3. Formally, we construct two $K_3$-interpretations $\pi_1, \pi_2 : \mathrm{Lit}_A(\tau) \to K_3$ over a simple signature $\tau = \{R\}$ with one unary relation symbol and the same universe $A = \{a, b, c\}$ as follows.

$\pi_1$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 1 | 0 |
| c | 3 | 0 |

$\pi_2$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 2 | 0 |
| c | 3 | 0 |

We will often write $K$-interpretations $\pi$ as tables, the columns represent the relations $R$ with arity $k$ and their negated counterparts $\neg R$ while each row represents one tuple $\overline{a} \in A^k$. Clearly, the cells represent the values $\pi((\neg)R\overline{a})$. This provides a very intuitive representation of $\pi$. Note that we may group relations with the same arity $k$ in the same table, but if $\tau$ contains relations with varying arities, we must represent $\pi$ with multiple tables, one for each arity.

Returning to our example of $\pi_1, \pi_2$, it is immediately clear that $\pi_1 \not\cong \pi_2$, but the simple formulas $\exists x Rx$ and $\forall x Rx$ with one quantifier cannot separate them, since

$$\begin{aligned} \pi_1 [\![\exists x Rx]\!] &= \max\{1,1,3\} = 3 = \max\{1,2,3\} = \pi_2 [\![\exists x Rx]\!] \quad \text{and} \\ \pi_1 [\![\forall x Rx]\!] &= \min\{1,1,3\} \ = 1 = \min\{1,2,3\} \ = \pi_2 [\![\forall x Rx]\!] . \end{aligned}$$

However, once we use two quantifiers, we can find a sentence $\psi$ with $\pi_2 [\![\psi]\!] = 2$ that separates the two $K$-interpretations. Pick $\psi := \exists x \exists y (x \neq y \wedge Rx \wedge Ry)$. The maximum is achieved by picking $x$ and $y$ so that $\pi [\![Rx]\!]$ and $\pi [\![Ry]\!]$ are maximized, but we have to choose distinct elements, otherwise $\pi [\![x \neq y]\!] = 0$ for $\pi \in \{\pi_1, \pi_2\}$. Hence,

$$\pi_1 [\![\psi]\!] = \min\{1,3\} = 1 \neq 2 = \min\{2,3\} = \pi_2 [\![\psi]\!]$$

and we have $\pi_1 \not\equiv \pi_2$. More importantly, we have found a way to construct a formula that “picks out” the second largest value of $\pi [\![Rx]\!]$ for any $K_3$-interpretation $\pi$. We aim to generalize this idea in order to prove that a counterexample with one unary relation symbol is not possible.

**(4.10) Definition** ($\pi$-Distribution)**.** Let $\pi : \mathrm{Lit}_A(\tau) \to K$ be a $K$-interpretation over a finite universe $A$ with $|A| = n$ and $\varphi(\overline{x}) \in \mathsf{FO}(\tau)$ a formula with $|\overline{x}| = k$ free variables. The $\pi$-*distribution* of $\varphi$ is a function $d^\pi_\varphi : K \to \mathbb{N}$ defined as

$$d^\pi_\varphi(k) := |\{\overline{a} \in A^k \mid \pi [\![\varphi(\overline{a})]\!] = k\}| \quad \text{for all } k \in K.$$

We omit $\pi$ when it is clear from the context. The support of the $\pi$-distribution is defined as usual with $\mathrm{supp}(d_\varphi) := \{k \in K \mid d_\varphi(k) \neq 0\}$ and always finite, since $A$ is finite.

If $K$ is naturally ordered and the natural order is linear, we additionally define the $\pi$-*series* of $\varphi$ as $s^\pi_\varphi : \{1, \dots, n^k\} \to K$ with

$$s^\pi_\varphi(i) := \min \left\{ k \in \mathrm{supp}(d^\pi_\varphi) \mid \sum_{l \in \mathrm{supp}(d^\pi_\varphi), l > k} d^\pi_\varphi(l) < i \right\}$$

for all $1 \leq i \leq n^k$.

Informally, the $\pi$-series is simply the set of values $\{\pi [\![\varphi(\overline{a})]\!] \mid \overline{a} \in A^k\}$ sorted in descending order and taking multiplicity into account. Unsurprisingly, the $\pi$-series of a formula exactly characterizes its $\pi$-distribution.

**(4.11) Lemma.** For two $K$-interpretations $\pi_A, \pi_B$ over universes with $n$ elements and a formula $\varphi(\overline{x})$ with $k$ free variables, $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$ if and only if $s_\varphi^{\pi_A} = s_\varphi^{\pi_B}$.

*Proof.* The direction "$\Rightarrow$" is clear by definition. For "$\Leftarrow$", assume $d_\varphi^{\pi_A} \neq d_\varphi^{\pi_B}$. Then, since both distributions have finite support, there is a maximal $k \in K$ such that $d_\varphi^{\pi_A}(k) \neq d_\varphi^{\pi_B}(k)$. Assume without loss of generality that $d_\varphi^{\pi_A}(k) < d_\varphi^{\pi_B}(k)$ and thus $k \in \mathrm{supp}(d_\varphi^{\pi_B})$. Now, pick

$$i := \sum_{l \in \mathrm{supp}(d_\varphi^{\pi_B}), l \geq k} d_\varphi^{\pi_B}(l).$$

Clearly, since $d_\varphi^{\pi_B}(k) > 0$, we have

$$\sum_{l \in \mathrm{supp}(d_\varphi^{\pi_B}), l > k} d_\varphi^{\pi_B}(l) < i.$$

Therefore, $s_\varphi^{\pi_B}(i) = k$, since for any $k' < k$,

$$\sum_{l \in \mathrm{supp}(d_\varphi^{\pi_B}), l > k'} d_\varphi^{\pi_B}(l) \geq \sum_{l \in \mathrm{supp}(d_\varphi^{\pi_B}), l \geq k} d_\varphi^{\pi_B}(l) = i.$$

For $\pi_A$, the value of $s_\varphi^{\pi_A}(i)$ is at most $k_<$, which is defined as the largest $k' < k$ in $\mathrm{supp}(d_\varphi^{\pi_A})$. Note that such an element must exist, since $d_\varphi^{\pi_A}$ and $d_\varphi^{\pi_B}$ are equal for all elements greater than $k$ and $d_\varphi^{\pi_A}(k) < d_\varphi^{\pi_B}(k)$, but the sums of both distributions are equal to $n^k$, so $d_\varphi^{\pi_A}$ must have a smaller element in $\mathrm{supp}(d_\varphi^{\pi_A})$ than $k$. Now, we obtain

$$\sum_{l \in \mathrm{supp}(d_\varphi^{\pi_A}), l > k_<} d_\varphi^{\pi_A}(l) = \sum_{l \in \mathrm{supp}(d_\varphi^{\pi_A}), l \geq k} d_\varphi^{\pi_A}(l) < \sum_{l \in \mathrm{supp}(d_\varphi^{\pi_B}), l \geq k} d_\varphi^{\pi_B}(l) = i,$$

hence $s_\varphi^{\pi_A}(i) \leq k_< < k = s_\varphi^{\pi_B}(i)$, which ends the proof. □

Informally speaking, $s_\varphi^\pi(i)$ is the $i$-th largest value in the $\pi$-distribution of $\varphi(\overline{x})$. Now, similarly to the example above where we used $\psi := \exists x \exists y (x \neq y \wedge Rx \wedge Ry)$ to pick out the second largest value of $\pi [\![Rx]\!]$ in our $K$-interpretations $\pi \in \{\pi_1, \pi_2\}$, we can attempt to construct a formula that picks out $s_\varphi^\pi(i)$ generally.

Since we are dealing with $k$-tuples instead of a unary relation, it is useful to introduce some notation for more clarity. For $k$-tuples of $\mathsf{FO}$-variables $\overline{x} = (x_1, \ldots, x_k)$ and $\overline{y} = (y_1, \ldots, y_k)$, we define

$$\begin{aligned} \exists \overline{x} \varphi &:= \exists x_1 \ldots \exists x_k \varphi, \\ \overline{x} = \overline{y} &:= \bigwedge_{1 \leq i \leq k} x_i = y_i \quad \text{and} \\ \overline{x} \neq \overline{y} &:= \bigvee_{1 \leq i \leq k} x_i \neq y_i \end{aligned}$$

as shorthands for formulas. In any semiring with $1 + 1 = 1$, in particular in any idempotent semiring, the formulas for equality or inequality have the intended meaning, that is, $\pi [\![\overline{x} = \overline{y}]\!]^\beta \in \{0, 1\}$ and it is 1 if and only if the tuples assigned to $\overline{x}$

and $\overline{y}$ by $\beta$ are equal and $\pi \llbracket \overline{x} \neq \overline{y} \rrbracket^\beta \in \{0,1\}$ and it is 1 if and only if the tuples are distinct. The condition $1+1=1$ is required for the disjunction in $\overline{x} \neq \overline{y}$, the remaining claims are directly implied by the semiring axioms. Now, we are ready to construct the desired formula.

**(4.12) Lemma** (Sorting Lemma)**.** Let $k \in \mathbb{N}$ and $\varphi(\overline{x})$ be any $\mathsf{FO}(\tau)$-formula with $k$ free variables. Then, there is a series of sentences $(\psi_i)_{i \in \mathbb{N}_{>0}} \subseteq \mathsf{FO}(\tau)$ such that for all $K$-interpretations $\pi : \mathrm{Lit}_A(\tau) \to K$ over a finite universe with $|A| = n$,

$$\pi \llbracket \psi_i \rrbracket = \begin{cases} \prod_{j=1}^{i} s^\pi_\varphi(j) & \text{if } 1 \leq i \leq n^k, \\ 0 & \text{otherwise,} \end{cases}$$

provided that $K$ is absorptive and naturally ordered by a linear order. The sentences are given by

$$\psi_i := \exists \overline{x}_1 \ldots \exists \overline{x}_i \left( \bigwedge_{1 \leq j < l \leq i} \overline{x}_j \neq \overline{x}_\ell \wedge \bigwedge_{1 \leq j \leq i} \varphi(\overline{x}_j) \right) \quad \text{for all } i \in \mathbb{N},$$

where we implicitly assume all tuples $\overline{x}_1, \ldots \overline{x}_i$ to be $k$-tuples.

*Proof.* For $i > n^k$, $i$ pairwise distinct $k$-tuples over $A$ do not exist, hence any assignment of $\overline{x}_1, \ldots, \overline{x}_i$ yields 0, since at least one subformula in the conjunction yields 0. Thus, $\pi \llbracket \psi \rrbracket = 0$. Now, assume $1 \leq i \leq n^k$.

The existential quantifiers are interpreted by summation in $K$. Recall from lemma (2.14) that $a + b = \sup\{a, b\}$ in any naturally ordered, absorptive semiring. Since the natural order on $K$ is also linear, we even have $a + b = \max\{a, b\}$ for all $a, b \in K$. Thus, summation is simply a maximum and we obtain

$$\pi \llbracket \psi_i \rrbracket = \max \left\{ \pi \left\llbracket \bigwedge_{1 \leq j < l \leq i} \overline{a}_j \neq \overline{a}_l \wedge \bigwedge_{1 \leq j \leq i} \varphi(\overline{a}_j) \right\rrbracket \mid \overline{a}_1, \ldots, \overline{a}_i \in A^k \right\}.$$

Choose $\overline{a}^*_1, \ldots, \overline{a}^*_i \in A^k$ pairwise distinct such that for all $1 \leq j \leq i$, $\pi \llbracket \varphi(\overline{a}^*_j) \rrbracket$ is maximal among the remaining values $\{\pi \llbracket \varphi(\overline{a}) \rrbracket \mid \overline{a} \in A^k \setminus \{\overline{a}^*_1, \ldots, \overline{a}^*_{j-1}\}\}$. By definition of $s^\pi_\varphi$ as the "sorted distribution" $d^\pi_\varphi$, we have $\pi \llbracket \varphi(\overline{a}^*_j) \rrbracket = s^\pi_\varphi(j)$. With this choice, we obtain

$$\pi \left\llbracket \bigwedge_{1 \leq j < l \leq i} \overline{a}^*_j \neq \overline{a}^*_l \wedge \bigwedge_{1 \leq j \leq i} \varphi(\overline{a}^*_j) \right\rrbracket = \prod_{1 \leq j \leq i} \pi \llbracket \varphi(\overline{a}^*_j) \rrbracket.$$

We argue that this choice is maximal and therefore yields the value of $\pi \llbracket \psi_i \rrbracket$.

For any other choice $\overline{a}_1, \ldots, \overline{a}_i \in A^k$, if the tuples are not pairwise distinct, then we obtain 0, which is the minimal element in $K$. Thus, assume they are pairwise distinct. Since their order is not important, assume without loss of generality that they are sorted descendingly so that

$$\pi \llbracket \varphi(\overline{a}_1) \rrbracket \geq \ldots \geq \pi \llbracket \varphi(\overline{a}_i) \rrbracket.$$

This choice of tuples yields the value

$$\pi \left\llbracket \bigwedge_{1 \leq j < l \leq i} \overline{a}_j \neq \overline{a}_l \wedge \bigwedge_{1 \leq j \leq i} \varphi(\overline{a}_j) \right\rrbracket = \prod_{1 \leq j \leq i} \pi \llbracket \varphi(\overline{a}_j) \rrbracket.$$

Now, since each $\overline{a}_j^*$ was chosen to maximize $\pi\, [\![\varphi(\overline{a}_j^*)]\!]$, we have $\pi\, [\![\varphi(\overline{a}_j)]\!] \leq \pi\, [\![\varphi(\overline{a}_j^*)]\!]$ for all $1 \leq j \leq i$. We obtain

$$\prod_{1\leq j\leq i} \pi\, [\![\varphi(\overline{a}_j)]\!] \leq \prod_{1\leq j\leq i} \pi\, [\![\varphi(\overline{a}_j^*)]\!]$$

by inductively applying the fact that multiplication is monotone from lemma (2.12).

In conclusion, $\overline{a}_1^*, \ldots, \overline{a}_i^*$ is indeed the maximal choice and we have

$$\pi\, [\![\psi]\!] = \prod_{1\leq j\leq i} \pi\, [\![\varphi(\overline{a}_j^*)]\!] = \prod_{1\leq j\leq i} s_\varphi^\pi(j),$$

which ends the proof. □

Unfortunately, the sentences $\psi_i$ do not quite capture $s_\varphi^\pi(i)$ yet, but rather, the product of all $s_\varphi^\pi(j)$ for $1 \leq j \leq i$. In order to remedy this, we can impose even more conditions on the semiring $K$. For example, this is not a problem on min-max-semirings, where products correspond to minima, so

$$\prod_{1\leq j\leq i} s_\varphi^\pi(j) = s_\varphi^\pi(i)$$

holds anyway due to $s_\varphi^\pi$ being non-increasing. In fact, min-max-semirings are linearly ordered lattices and the above equation holds in all linearly ordered lattices, because products always coincide with minima in such lattices.

**(4.13) Corollary** (to the Sorting Lemma)**.** If $K$ is a linearly ordered lattice, then for all $K$-interpretations $\pi : \mathrm{Lit}_U(\tau) \to K$ with $|U| = n$ and $\varphi(\overline{x})$ with $k$ free variables and the corresponding $\psi_i$ defined above, $\pi\, [\![\psi_i]\!] = s_\varphi^\pi(i)$ for $1 \leq i \leq n^k$. In particular, for two $K$-interpretations $\pi_A$ and $\pi_B$ over finite universes $A, B$, $\pi_A \equiv \pi_B$ implies $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$.

*Proof.* The first part immediately follows from the above observations. For the second part, notice that $\pi_A \equiv \pi_B$ implies that their underlying universes $A, B$ have the same number of elements, otherwise, they would be easily separated by the formula

$$\exists x_1 \ldots \exists x_n \left( \bigwedge_{1\leq j<l\leq n} x_j \neq x_l \right)$$

with $n \coloneqq \max\{|A|, |B|\}$. Now, due to $s_\varphi^{\pi_A}(i) = \pi_A\, [\![\psi_i]\!] = \pi_B\, [\![\psi_i]\!] = s_\varphi^{\pi_B}(i)$ for all $1 \leq i \leq n^k$ and lemma (4.11), we obtain $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$. □

The statement that $\pi_A \equiv \pi_B$ implies $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$ for all $\varphi$ is very interesting to us, because it brings us closer to isomorphism. It already shows that our previous attempt on a counterexample of $K_3$-interpretations $\pi_1, \pi_2$ with one unary relation symbol is futile. The intuition behind this is indicated in the following graphics.

$\pi_1$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | **1** | 0 |
| b | **1** | 0 |
| c | **3** | 0 |

$\pi_2$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | **1** | 0 |
| b | **2** | 0 |
| c | **3** | 0 |

If we choose $\varphi(x) \coloneqq Rx$, then the columns that constitute the distributions $d_\varphi^{\pi_1}$ and $d_\varphi^{\pi_2}$ are highlighted bold. Since we want $\pi_1 \equiv \pi_2$, the distributions of values in those columns must be equal by the above corollary and $\pi_1 \cong \pi_2$ follows immediately. Hence, we cannot hope to construct a counterexample with $\pi_1 \equiv \pi_2$ and $\pi_1 \ncong \pi_2$ in this manner.

**(4.14) Proposition.** For two model-defining $K$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$ over finite universes $A, B$ with $|A| = |B| = n$ and a signature $\tau = \{R\}$ with one unary relation symbol, $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$ for all $\varphi(\overline{x})$ implies $\pi_A \cong \pi_B$.

*Proof.* Recall that for a model-defining $K$-interpretation, exactly one out of two complementary literals has a nonzero value. Let $A^+ := \{a \in A \mid \pi_A(Ra) \neq 0\}$, $A^- := \{a \in A \mid \pi_A(\neg Ra) \neq 0\}$ and $B^+, B^-$ be defined in a similar way for $\pi_B$. Clearly, those sets partition $A$ and $B$ respectively.

Pick $\varphi(x) := Rx$, then $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$. In particular, $|A^-| = d_\varphi^{\pi_A}(0) = d_\varphi^{\pi_B}(0) = |B^-|$ and therefore, $|A^+| = |B^+|$ as well.

Now, thanks to $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$, we can construct a bijection $\sigma^+ : A^+ \to B^+$ such that $\pi_A [\![\varphi(a)]\!] = \pi_B [\![\varphi(\sigma^+(a))]\!]$ holds for all $a \in A^+$ by mapping $a$ to an element of $B^+$ according to the value $\pi_A [\![\varphi(a)]\!] = \pi_A(Ra) > 0$. The equality of the distributions guarantees that there are sufficiently many appropriate elements in $B^+$ for each value $\pi_A(Ra)$. Note that since $\varphi(x) = Rx$, we have $\pi_A(Ra) = \pi_B(R\sigma^+(a))$ for all $a \in A^+$. By definition, we also have $\pi_A(\neg Ra) = 0 = \pi_B(\neg R\sigma^+(a))$ for $a \in A^+$.

The same approach can be used for the negation. Let $\psi(x) := \neg Rx$ and observe that $d_\psi^{\pi_A} = d_\psi^{\pi_B}$ as well. From that, we obtain a bijection $\sigma^- : A^- \to B^-$ with $\pi_A(\neg Ra) = \pi_B(\neg R\sigma^-(a))$ for all $a \in A^-$. By definition, $\pi_A(Ra) = 0 = \pi_B(R\sigma^-(a))$ for all $a \in A^-$. Putting $\sigma^+$ and $\sigma^-$ together yields an isomorphism $\sigma : \pi_A \xrightarrow{\sim} \pi_B$. ☐

Our suspicion that a counterexample in a min-max-semiring over a signature with one unary relation is not possible is confirmed by applying the sorting lemma (4.12), its corollary (4.13) for lattices and finally proposition (4.14). Since the preconditions on the semiring $K$ imposed by the sorting lemma (4.12) are very strict, we may wonder if any semirings other than min-max-semirings, that is, linearly ordered lattices, meet them as well.

Recall the Viterbi semiring $\mathbb{V} = ([0,1]_\mathbb{R}, \max, \cdot, 0, 1)$, which is naturally ordered by the usual order on $[0,1]_\mathbb{R}$. Clearly, this is a linear order. Moreover, $\mathbb{V}$ is absorptive, since $\max\{a, ab\} = a$ for all $a, b \in [0,1]_\mathbb{R}$. Therefore, the sorting lemma also applies to $\mathbb{V}$-interpretations. However, multiplication on $\mathbb{V}$ is not idempotent, hence it is not a lattice and we cannot use corollary (4.13). Nevertheless, we can still arrive at proposition (4.14) using the property of $\mathbb{V}$ that multiplication with nonzero elements allows cancellation.

**(4.15) Definition** (Cancellation)**.** For a semiring $K$, we say that $K$ *allows cancellation* if for all $a \in K \setminus \{0\}$, $ab = ac$ implies $b = c$ for all $b, c \in K$.

**(4.16) Lemma.** For a semiring $K$ that is naturally ordered by a linear order, absorptive and allows cancellation, if $\pi_A, \pi_B$ are two $K$-interpretations over finite universes $A, B$, then $\pi_A \equiv \pi_B$ implies $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$ for all $\varphi(\overline{x})$ with $k$ free variables.

*Proof.* We have already established that $\pi_A \equiv \pi_B$ implies $|A| = |B| =: n$ in the proof of corollary (4.13). Now, it only remains to show $s_\varphi^{\pi_A} = s_\varphi^{\pi_B}$ due to lemma (4.11). We will prove $s_\varphi^{\pi_A}(i) = s_\varphi^{\pi_B}(i)$ for $1 \leq i \leq n^k$ by induction on $i$.

The case $i = 1$ follows directly from the sorting lemma (4.12). We take the sentences $\psi_i$ as defined in the sorting lemma and use elementary equivalence of $\pi_A$ and $\pi_B$ to obtain

$$s_\varphi^{\pi_A}(1) = \pi_A [\![\psi_1]\!] = \pi_B [\![\psi_1]\!] = s_\varphi^{\pi_B}(1).$$

Now, for the induction step, assume $1 < i \leq n^k$. The sorting lemma yields

$$\prod_{j=1}^{i} s_\varphi^{\pi_A}(j) = \pi_A [\![\psi_i]\!] = \pi_B [\![\psi_i]\!] = \prod_{j=1}^{i} s_\varphi^{\pi_B}(j).$$

By induction, we know that the first $(i-1)$ factors are equal, hence

$$\prod_{j=1}^{i-1} s_\varphi^{\pi_A}(j) = \prod_{j=1}^{i-1} s_\varphi^{\pi_B}(j) =: a.$$

This already yields $a \cdot s_\varphi^{\pi_A}(i) = a \cdot s_\varphi^{\pi_B}(i)$. If $a \neq 0$, then $s_\varphi^{\pi_A}(i) = s_\varphi^{\pi_B}(i)$ follows by cancellation. For the other case that $a = 0$, observe that $K$ does not have divisors of zero, since $bc = 0$ for $b, c \in K \setminus \{0\}$ would imply $b \cdot c = b \cdot 0 = 0$, which would yield $c = 0$ with cancellation, a contradiction. Hence, $a = 0$ implies that one of the factors $s_\varphi^{\pi_A}(j) = s_\varphi^{\pi_B}(j)$ for some $1 \leq j < i$ is already 0. Now, with $s_\varphi^{\pi_A}$ and $s_\varphi^{\pi_B}$ being non-ascending chains and 0 the minimal element of $K$, this already implies $s_\varphi^{\pi_A}(i) = s_\varphi^{\pi_B}(i) = 0$, which ends the induction and the proof. ☐

This shows that the sorting lemma is also useful in semirings where $\prod_{j=1}^{i} s_\varphi^{\pi}(j) \neq s_\varphi^{\pi}(i)$, as long as cancellation of $\cdot$ is available, as is the case in the Viterbi semiring $\mathbb{V}$. The conclusion of this section is formally stated in the following theorem.

**(4.17) Theorem.** Consider an absorptive semiring $K$ that is naturally ordered by a linear order. If multiplication on $K$ is idempotent or allows cancellation, then $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$ for all model-defining $K$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to K$, $\pi_B : \mathrm{Lit}_B(\tau) \to K$ with finite universes $A, B$ over a signature $\tau = \{R\}$ with one unary relation symbol.

*Proof.* Recall that $\pi_A \equiv \pi_B$ implies $|A| = |B|$. Now, we claim $d_\varphi^{\pi_A} = d_\varphi^{\pi_B}$ for all $\varphi(\overline{x})$. If $\cdot$ on $K$ is idempotent, then $K$ is a lattice thanks to proposition (2.15) and the claim follows by corollary (4.13), if $K$ allows cancellation, then it is derived from lemma (4.16). Note that in both cases, the sorting lemma is the core of the proof. We simply apply proposition (4.14) to conclude $\pi_A \cong \pi_B$. ☐

The takeaway is that the desired counterexample must be more complex than a pair of $K$-interpretations with a unary relation, as long as $K$ is a “simple” min-max-semiring. As a side product, we have additionally established that such a counterexample is not possible on the “more complex” Viterbi semiring $\mathbb{V}$.

## 4.3 Counterexample for Min-Max-Semirings

The theorem (4.17) from the previous section cannot be extended to signatures with multiple relation symbols, or even to signatures with a binary relation. While proposition (4.14) informally states that if $\pi_A \equiv \pi_B$, all relations $R \in \tau$ follow the same distribution under $\pi_A$ and $\pi_B$, this only yields isomorphisms $\sigma_R : \pi_A|_R \xrightarrow{\sim} \pi_B|_R$

if we restrict $\pi_A, \pi_B$ to $R$ and $R$ is unary. If $R$ is binary, such an isomorphism may not exist because we are not allowed to permute the tuples freely, for example, a pair $(a, a)$ must always be mapped to a pair $(b, b)$ by an isomorphism. In case of multiple unary relation symbols, the individual isomorphisms $\sigma_R$ may not be compatible with each other, hence we cannot combine them to construct an isomorphism $\sigma : \pi_A \xrightarrow{\sim} \pi_B$ in general.

We will exploit this fact to create a counterexample with two unary relations over $K_3$. Consider two $K_3$-interpretations $\pi_{PQ}, \pi_{QP} : \mathrm{Lit}_A(\tau) \to K_3$ on the universe $A = \{a, b, c\}$ over the signature $\tau = \{P, Q\}$ where $P, Q$ are unary, as depicted in the following table.

$\pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 1 | 3 | 0 | 0 |
| b | 2 | 1 | 0 | 0 |
| c | 3 | 2 | 0 | 0 |

$\pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 3 | 1 | 0 | 0 |
| b | 1 | 2 | 0 | 0 |
| c | 2 | 3 | 0 | 0 |

We claim that $\pi_{PQ} \equiv \pi_{QP}$, but $\pi_{PQ} \not\cong \pi_{QP}$. It is easy to see that $\pi_{PQ} \not\cong \pi_{QP}$. If an isomorphism $\sigma : \pi_{PQ} \xrightarrow{\sim} \pi_{QP}$ existed, then we would have

$$\begin{aligned} \pi_{PQ}(Pa) = 1 = \pi_{QP}(P\sigma(a)) \quad \text{and} \\ \pi_{PQ}(Qa) = 3 = \pi_{QP}(Q\sigma(a)). \end{aligned}$$

However, there is no suitable $\sigma(a) \in A$ with $\pi_{QP}(P\sigma(a)) = 1$ and $\pi_{QP}(Q\sigma(a)) = 3$.

The difficult part is proving that $\pi_{PQ} \equiv \pi_{QP}$. Before we can state the formal proof, notice that the distributions of values in both $P$-columns and $Q$-columns are equal. Hence, we cannot use a formula that only involves one of the relations as in theorem (4.17) to separate the two $K$-interpretations. However, if we want to use both relations, we have to somehow combine $P$-values with $Q$-values. Over a min-max-semiring, only max and min are available for use via disjunctions and conjunctions. Note that

$$\begin{aligned} \{\pi_{PQ}(Pa), \pi_{PQ}(Qa)\} = \{1, 3\} = \{\pi_{QP}(Pa), \pi_{QP}(Qa)\}, \\ \{\pi_{PQ}(Pb), \pi_{PQ}(Qb)\} = \{1, 2\} = \{\pi_{QP}(Pb), \pi_{QP}(Qb)\} \quad \text{and} \\ \{\pi_{PQ}(Pc), \pi_{PQ}(Qc)\} = \{2, 3\} = \{\pi_{QP}(Pc), \pi_{QP}(Qc)\}, \end{aligned}$$

therefore, any formula $Px \circ Qx$ yields the same value $\pi_{PQ} [\![Pe \circ Qe]\!] = \pi_{QP} [\![Pe \circ Qe]\!]$ for $e \in A$ with $\circ \in \{\vee, \wedge\}$. More intuitively, $\pi_{QP}$ is obtained from $\pi_{PQ}$ by swapping the $P$-column and the $Q$-column, which also explains the naming of the two interpretations. Graphically, this corresponds to a "horizontal" permutation and since $P$ and $Q$ follow the same distribution, we can also obtain $\pi_{QP}$ from $\pi_{PQ}$ by two distinct "vertical permutations" in the $P$-column and the $Q$-column. It is crucial that those permutations are distinct, otherwise our interpretations would be isomorphic.

Unfortunately, this does not prove $\pi_{PQ} \equiv \pi_{QP}$ and our toolbox for proving elementary equivalence in general semirings $K$ is empty, except for the isomorphism lemma, which states that isomorphic $K$-interpretations are elementarily equivalent. Of course, we cannot use this directly for our counterexample, since we must insist on $\pi_{PQ} \not\cong \pi_{QP}$. However, we can "reduce" $\pi_{PQ}$ and $\pi_{QP}$ to smaller semirings via homomorphisms $h$ and then show that $h \circ \pi_{PQ} \equiv h \circ \pi_{QP}$. With a little more effort, we can then use the fundamental property to prove $\pi_{PQ} \equiv \pi_{QP}$.

Firstly, it is clear that $h \circ \pi_{PQ} \equiv h \circ \pi_{QP}$ under a single homomorphism is not enough to prove $\pi_{PQ} \equiv \pi_{QP}$, but multiple homomorphisms may do the trick. Luckily, it is easy to find homomorphisms $h : K_n \to \mathbb{B}$ for min-max-semirings $K_n$ as follows.

**(4.18) Lemma** (Homomorphisms for Min-Max-Semirings)**.** For a min-max-semiring $K_n = (\{0, \dots, n\}, \max, \min, 0, n)$ with $(n+1)$ elements and $0 < i \leq n$, the function $h_i : K_n \to \mathbb{B}$ defined as

$$h_i(j) := \begin{cases} \top & \text{if } i \leq j, \\ \bot & \text{otherwise} \end{cases}$$

is a homomorphism.

*Proof.* $h(n) = \top$ is clearly true and since $i > 0$, $h(0) = \bot$. Moreover, we have $h(\max\{j, l\}) = \top$ if and only if $i \leq \max\{j, l\}$, which holds if and only if $i \leq j$ or $i \leq l$, which is true if and only if $h(j) = \top$ or $h(l) = \top$, so $h(\max\{j, l\}) = h(j) \vee h(l)$. Similarly, $h(\min\{j, l\}) = \top$ if and only if both $i \leq j$ and $i \leq l$, hence we conclude that $h(\min\{j, l\}) = h(j) \wedge h(l)$. □

For $K_3$, this yields three homomorphisms $h_1, h_2$ and $h_3$, which we can apply on $\pi_{PQ}$ and $\pi_{QP}$, as depicted in the following tables.

$\pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 1 | 3 | 0 | 0 |
| b | 2 | 1 | 0 | 0 |
| c | 3 | 2 | 0 | 0 |

$\pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 3 | 1 | 0 | 0 |
| b | 1 | 2 | 0 | 0 |
| c | 2 | 3 | 0 | 0 |

$h_1 \circ \pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\top$ | $\top$ | $\bot$ | $\bot$ |
| b | $\top$ | $\top$ | $\bot$ | $\bot$ |
| c | $\top$ | $\top$ | $\bot$ | $\bot$ |

$h_1 \circ \pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\top$ | $\top$ | $\bot$ | $\bot$ |
| b | $\top$ | $\top$ | $\bot$ | $\bot$ |
| c | $\top$ | $\top$ | $\bot$ | $\bot$ |

$h_2 \circ \pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| b | $\top$ | $\bot$ | $\bot$ | $\bot$ |
| c | $\top$ | $\top$ | $\bot$ | $\bot$ |

$h_2 \circ \pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\top$ | $\bot$ | $\bot$ | $\bot$ |
| b | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| c | $\top$ | $\top$ | $\bot$ | $\bot$ |

$h_3 \circ \pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| b | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| c | $\top$ | $\bot$ | $\bot$ | $\bot$ |

$h_3 \circ \pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\top$ | $\bot$ | $\bot$ | $\bot$ |
| b | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| c | $\bot$ | $\top$ | $\bot$ | $\bot$ |

Clearly, we have $h_i \circ \pi_{PQ} \cong h_i \circ \pi_{QP}$ for $i \in \{1, 2, 3\}$ via the respective isomorphisms

$$\begin{aligned} \sigma_1 :&\quad a \mapsto a,\ b \mapsto b,\ c \mapsto c \quad (\sigma_1 = \mathrm{id}_A), \\ \sigma_2 :&\quad a \mapsto b,\ b \mapsto a,\ c \mapsto c \quad (\sigma_2 \text{ swaps } a, b) \quad \text{and} \\ \sigma_3 :&\quad a \mapsto c,\ b \mapsto b,\ c \mapsto a \quad (\sigma_3 \text{ swaps } a, c). \end{aligned}$$

Hence, the isomorphism lemma yields $h_i \circ \pi_{PQ} \equiv h_i \circ \pi_{QP}$ for $i \in \{1, 2, 3\}$ and it only remains to show that this is "enough" to prove $\pi_{PQ} \equiv \pi_{QP}$, which is captured by the following definition and theorem.

**(4.19) Definition** (Separating Homomorphisms)**.** Let $K, L$ be semirings. A set $S$ of homomorphisms $h : K \to L$ is called *separating* if for all $a, b \in K$ with $a \neq b$, there is a homomorphism $h \in S$ such that $h(a) \neq h(b)$ in $L$.

**(4.20) Theorem** (Reduction Theorem)**.** Let $K, L$ be semirings and $S$ a separating set of homomorphisms $K \to L$. For two $K$-interpretations $\pi_A, \pi_B$, $\pi_A \equiv \pi_B$ holds if and only if $h \circ \pi_A \equiv h \circ \pi_B$ for all $h \in S$.

*Proof.* The easy direction is "$\Rightarrow$". If $\pi_A \equiv \pi_B$, then for all $\psi \in \mathsf{FO}(\tau)$, $\pi_A [\![\psi]\!] = \pi_B [\![\psi]\!]$, which implies $h(\pi_A [\![\psi]\!]) = h(\pi_B [\![\psi]\!])$ for any $h \in S$. Using the fundamental property, we obtain $(h \circ \pi_A) [\![\psi]\!] = (h \circ \pi_B) [\![\psi]\!]$.

For the converse direction "$\Leftarrow$", we show the contraposition by exploiting that $S$ is separating. Suppose that $\pi_A \not\equiv \pi_B$, then there is a sentence $\psi \in \mathsf{FO}(\tau)$ with $\pi_A [\![\psi]\!] \neq \pi_B [\![\psi]\!]$. Hence, there must be a homomorphism $h \in S$ that keeps these two values separate, that is $h(\pi_A [\![\psi]\!]) \neq h(\pi_B [\![\psi]\!])$. The fundamental property yields $(h \circ \pi_A) [\![\psi]\!] \neq (h \circ \pi_B) [\![\psi]\!]$, which concludes the proof. $\square$

It is easy to see that $\{h_1, h_2, h_3\}$ is a separating set of homomorphisms for $K_3$. For $i \neq j$ in $K$, we can assume without loss of generality that $i < j$, but then $j \in \{1, 2, 3\}$ and $h_j(i) = \bot \neq \top = h_j(j)$, so $h_j$ separates the two values. With the reduction theorem and the observation that $h_i \circ \pi_{PQ} \equiv h_i \circ \pi_{QP}$ for $i \in \{1, 2, 3\}$, we can conclude that $\pi_{PQ} \equiv \pi_{QP}$ and our counterexample is indeed correct.

**(4.21) Theorem.** $\pi_A \equiv \pi_B$ does not imply $\pi_A \cong \pi_B$ for all semirings $K$ and all $K$-interpretations $\pi_A, \pi_B$ over finite universes $A, B$. In particular, there are two $K_3$-interpretations $\pi_{PQ}$ and $\pi_{QP}$ over a universe with three elements in the finite min-max-semiring $K_3$ with $\pi_{PQ} \equiv \pi_{QP}$ and $\pi_{PQ} \ncong \pi_{QP}$.

Unfortunately, this result cannot be lifted to all semirings $K$, in other words, we do not know if a counterexample can be found for any semiring $K$ or whether a semiring must have very specific properties, such as a min-max-semiring, to be able to produce a counterexample. Hence, the search for counterexamples in other semirings continues.

## 4.4 The Viterbi Semiring

The well-known fact that elementary equivalence implies isomorphism on finite structures in the "most simple" semiring $\mathbb{B}$ due to the possibility of constructing characteristic sentences together with the observation from the previous section that this does not hold in the "slightly more complex" min-max-semiring $K_3$ suggests that generally, elementary equivalence does not imply isomorphism in more "complex" semirings. This is not a formal statement, since our idea of "complexity" of semirings is purely intuitive and based on how much they "differ" from $\mathbb{B}$ in terms of their number of elements and operations. From this point of view, a min-max-semiring has more elements than $\mathbb{B}$, but the operations are essentially the same, since $\mathbb{B}$ is a special min-max-semiring. The Viterbi semiring $\mathbb{V}$ is "more complex" than finite min-max-semirings, because it contains more elements and its multiplication does not coincide with the minimum of two elements, as in $\mathbb{B}$ or min-max-semirings.

In this section, we will show that $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$ for finite $\mathbb{V}$-interpretations, which unfortunately means that our intuition of "more complex" semirings allowing counterexamples is wrong. Recall that in $\mathbb{B}$, we use the characteristic sentence

$$\varphi_{\mathfrak{A}} := \exists x_1 \dots \exists x_n \left( \bigwedge_{1 \le i < j \le n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1 \le i \le n} y = x_i \right) \wedge \bigwedge_{L \in \mathrm{Lit}_A(\tau), \mathfrak{A} \models L} L[\overline{a}/\overline{x}] \right)$$

to describe a structure $\mathfrak{A}$ up to isomorphism. The main reason why this does not work for general $K$-interpretations $\pi$ is the conjunction

$$\bigwedge_{L \in \mathrm{Lit}_A(\tau), \mathfrak{A} \models L} L[\overline{a}/\overline{x}],$$

which essentially just enumerates all literals that are true in $\mathfrak{A}$. In $\mathbb{B}$, if $\mathfrak{B}$ has the same number of elements as $\mathfrak{A}$ and satisfies these literals, then $\mathfrak{A} \cong \mathfrak{B}$. However, in a semiring $K$ with more than two elements, there is more than one nonzero element and the conjunction evaluates to the product of the values for the "true" literals. This is a problem, because we can permute the factors of a product without changing its value. $\mathbb{B}$ avoids this problem, because only one nonzero value exists, so permuting the factors does not have an effect if they are all $\top$. However, as our counterexample from the previous section, which is depicted below, suggests, semirings with more elements are vulnerable to this.

$\pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 1 | 3 | 0 | 0 |
| b | 2 | 1 | 0 | 0 |
| c | 3 | 2 | 0 | 0 |

$\pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 3 | 1 | 0 | 0 |
| b | 1 | 2 | 0 | 0 |
| c | 2 | 3 | 0 | 0 |

More intuitively, $K_3$ is vulnerable to "horizontal permutations" of the relations $P, Q$, since a formula $Px \circ Qx$ for $\circ \in \{\vee, \wedge\}$ cannot distinguish whether its value comes from $P$ or $Q$. However, this is where the "complexity" of $\mathbb{V}$ provides an advantage that gives more power to formulas. Since multiplication is not idempotent, if we repeat one of the literals, as in $Px \wedge Qx \wedge Qx$, we can no longer exchange $P$ and $Q$ and preserve the interpretation of the formula. In fact, this simple idea is enough to prove that $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$ on $\mathbb{V}$-interpretations.

**(4.22) Proposition** ($\varepsilon$-characteristic Sentence)**.** Consider two model-defining $\mathbb{V}$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to \mathbb{V}$ and $\pi_B : \mathrm{Lit}_B(\tau) \to \mathbb{V}$ over finite universes with $|A| = n$. Define the finite set of nonzero values

$$V := (\{\pi_A(L) \mid L \in \mathrm{Lit}_A(\tau)\} \cup \{\pi_B(L) \mid L \in \mathrm{Lit}_B(\tau)\}) \setminus \{0\} \subseteq (0,1]_{\mathbb{R}}.$$

Choose the minimum value $m := \min V > 0$ and the minimum ratio

$$r := \min \left\{ \frac{a}{b} \mid a, b \in V \text{ with } a > b \right\} > 1.$$

Finally, choose a rational number $\varepsilon \in \mathbb{Q}$ with $0 < \varepsilon < \min\{m, r-1\}$ so that $\varepsilon \le m$ and $(1+\varepsilon) < r$, which exists since $\mathbb{Q}$ is dense in $\mathbb{R}$.

Then, a $\mathsf{FO}(\tau)$-sentence $\psi_\varepsilon$ exists such that $\pi_A [\![\psi_\varepsilon]\!] = \pi_B [\![\psi_\varepsilon]\!]$ if and only if $\pi_A \cong \pi_B$ and $\psi_\varepsilon$ only depends on $\pi_A$ and $\varepsilon$. This sentence is called the *$\varepsilon$-characteristic sentence* of $\pi_A$.

*Proof.* We will construct $\psi_\varepsilon$ by adapting the "standard" sentence

$$\varphi_{\mathfrak{A}} := \exists x_1 \dots \exists x_n \left( \bigwedge_{1 \le i < j \le n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1 \le i \le n} y = x_i \right) \wedge \bigwedge_{L \in \mathrm{Lit}_A(\tau), \mathfrak{A} \models L} L[\overline{a}/\overline{x}] \right).$$

In order to ensure that the values of the literals cannot be permuted, we will repeat the literals "sufficiently often" so that permuting factors surely changes the value of the product. This is why we require the previous computation of $\varepsilon$.

Now, enumerate $A \coloneqq \{a_1, \dots, a_n\}$ arbitrarily and sort the set of "true" literals

$$\{L \in \mathrm{Lit}_A(\tau) \mid \pi_A(L) \neq 0\} \coloneqq \{L_1, \dots, L_k\}$$

non-decreasingly so that $0 < \pi_A(L_1) \leq \dots \leq \pi_A(L_k)$. Since $A$ and $\tau$ are finite, so is $\mathrm{Lit}_A(\tau)$. Moreover, $\pi_A$ is model-defining, so $k$ is finite and exactly one half of $|\mathrm{Lit}_A(\tau)|$, only depending on $|A|$ and $\tau$.

Now, we will repeat the literal $L_1$ with the smallest value only once, that is $f(1) = 1$. The remaining literals $L_i$ will be repeated $f(i) \in \mathbb{N}$ times, where the values $f(i)$ constitute an increasing sequence that depends on $\varepsilon$ and each $f(i)$ is "large enough" so that the value of $L_i$ is distinguishable. We will clarify the exact definition of $f(i)$ later, for now, we can state the formula $\psi_\varepsilon$ as

$$\psi_\varepsilon \coloneqq \exists x_1 \dots \exists x_n \left( \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1 \leq i \leq n} y = x_i \right) \wedge \bigwedge_{i=1}^{k} \bigwedge_{j=1}^{f(i)} L_i[\overline{a}/\overline{x}] \right).$$

Before thinking about $\pi_B$, we observe that existential quantifiers in $\mathbb{V}$ are interpreted by maxima. Hence, for $\pi_A$, the maximum $\pi_A [\![\psi_\varepsilon]\!]$ is achieved by the straightforward assignment $\beta : \overline{x} \to A$ with $\beta(x_i) = a_i$ for $i \in \{1, \dots, n\}$ due to the construction of $\psi_\varepsilon$, where literals are repeated more if their value under $\beta$ is larger. Since $A$ has $n$ elements and the first part of the formula clearly evaluates to 1 in $\mathbb{V}$, we obtain

$$\pi_A [\![\psi_\varepsilon]\!] = \prod_{i=1}^{k} \pi_A(L_i)^{f(i)} > 0.$$

Now, we can move on to $\pi_B$. Assume that $\pi_A [\![\psi_\varepsilon]\!] = \pi_B [\![\psi_\varepsilon]\!]$. The value $\pi_B [\![\psi_\varepsilon]\!]$ is achieved by an assignment $\overline{b} = (b_1, \dots, b_n)$, or more formally, $\gamma : \{x_1, \dots, x_n\} \to B$ with $\gamma(x_i) = b_i$ for $i \in \{1, \dots, n\}$. Since $\pi_A [\![\psi_\varepsilon]\!]$ is nonzero, $\gamma$ must be a bijection, otherwise $\pi_B [\![\psi_\varepsilon]\!]$ would be zero. Hence, $B = \{b_1, \dots, b_n\}$ and

$$\pi_B [\![\psi_\varepsilon]\!] = \prod_{i=1}^{k} \pi_B(L_i[\overline{a}/\overline{x}][\overline{x}/\overline{b}])^{f(i)} = \prod_{i=1}^{k} \pi_B(L_i[\overline{a}/\overline{b}])^{f(i)} > 0.$$

We claim that $\gamma \circ \beta^{-1} : \pi_A \xrightarrow{\sim} \pi_B$ is an isomorphism, written more simply as $\overline{a} \mapsto \overline{b}$. Since we have already argued that it is bijective, it only remains to show $\pi_A(L_i) = \pi_B(L_i[\overline{a}/\overline{b}])$ for the "true" literals in $\pi_A$. The reason why we do not need to consider "false" literals $L$ with $\pi_A(L) = 0$ is that $\pi_B [\![\psi_\varepsilon]\!] > 0$ already implies that all the literals involved in the product must have nonzero values in $\pi_B$, and since both $\pi_A$ and $\pi_B$ are model-defining, share the same signature and the size of their universes, they have an equal amount of "true" literals, which indicates that the other literals must be "false" in $\pi_B$, so $\pi_B(L[\overline{a}/\overline{b}]) = 0 = \pi_A(L) = 0$ automatically holds for false literals.

We conclude the proof by showing $\pi_A(L_j) = \pi_B(L_j[\overline{a}/\overline{b}])$ for $j \in \{1, \dots, k\}$ by induction on $j$ in reverse order from $k$ to 1. Assume the statement has been shown for all $k \geq l > j$ already, then, by cancellation

$$\prod_{i=1}^{k} \pi_A(L_i)^{f(i)} = \prod_{i=1}^{k} \pi_B(L_i[\overline{a}/\overline{b}])^{f(i)} \quad \text{implies} \quad \prod_{i=1}^{j} \pi_A(L_i)^{f(i)} = \prod_{i=1}^{j} \pi_B(L_i[\overline{a}/\overline{b}])^{f(i)}.$$

If $j = 1$, then we are done, since we have $f(1) = 1$ and $\pi_A(L_1) = \pi_B(L_1[\overline{a}/\overline{b}])$. Otherwise, assume for a contradiction that $\pi_A(L_j) \neq \pi_B(L_j[\overline{a}/\overline{b}])$. Without loss of generality, we can say $\pi_A(L_j) < \pi_B(L_j[\overline{a}/\overline{b}])$.

Recall that we have defined the set of all possible nonzero values $V$ under $\pi_A$ or $\pi_B$, its minimum $m$ and the "minimum ratio" $r$. Thus, we have

$$\frac{\pi_B(L_j[\overline{a}/\overline{b}])}{\pi_A(L_j)} \geq r > (1+\varepsilon).$$

Observe that the value of the product

$$\prod_{i=1}^{j} \pi_A(L_i)^{f(i)} \quad \text{is at most} \quad \pi_A(L_j)^{f(j)},$$

since the omitted factors can be at most $1 \in \mathbb{V}$. On the other side, the value of the product

$$\prod_{i=1}^{j} \pi_B(L_i[\overline{a}/\overline{b}])^{f(i)} \quad \text{is at least} \quad m^{\left(\sum_{i=1}^{j-1} f(i)\right)} \cdot \pi_B(L_j[\overline{a}/\overline{b}])^{f(j)},$$

due to $m$ being the minimal possible nonzero value in $V$. Now, we claim

$$\prod_{i=1}^{j} \pi_A(L_i)^{f(i)} \leq \pi_A(L_j)^{f(j)} \overset{*}{<} m^{\left(\sum_{i=1}^{j-1} f(i)\right)} \cdot \pi_B(L_j[\overline{a}/\overline{b}])^{f(j)} \leq \prod_{i=1}^{j} \pi_B(L_i[\overline{a}/\overline{b}])^{f(i)},$$

which is obviously a contradiction to the fact that the products on the left and right side must be equal. However, we first have to show $(*)$, which translates to

$$\begin{aligned} & \pi_A(L_j)^{f(j)} \overset{*}{<} m^{\left(\sum_{i=1}^{j-1} f(i)\right)} \cdot \pi_B(L_j[\overline{a}/\overline{b}])^{f(j)} \\ \Leftrightarrow \quad & 1 < m^{\left(\sum_{i=1}^{j-1} f(i)\right)} \cdot \underbrace{\frac{\pi_B(L_j[\overline{a}/\overline{b}])^{f(j)}}{\pi_A(L_j)^{f(j)}}}_{\geq r^{f(j)}}. \end{aligned}$$

Now, since $m \geq \varepsilon$ and $r \geq (1+\varepsilon)$, it is sufficient to prove

$$1 < \varepsilon^{\left(\sum_{i=1}^{j-1} f(i)\right)} \cdot (1+\varepsilon)^{f(j)}.$$

At this point, we can finally provide the definition of $f(j)$. It is recursively defined as $f(1) \coloneqq 1$ and

$$f(j) \coloneqq \min\left\{\ell \in \mathbb{N} \mid 1 < \varepsilon^{\left(\sum_{i=1}^{j-1} f(i)\right)} \cdot (1+\varepsilon)^{\ell}\right\}.$$

This is clearly well-defined, since the corresponding exponential function is unbounded, that is

$$\lim_{\ell \to \infty} \varepsilon^{\left(\sum_{i=1}^{j-1} f(i)\right)} \cdot (1+\varepsilon)^{\ell} = \infty.$$

Moreover, the definition only depends on $\varepsilon$ and, of course, the previous values of $f$, so the sentence $\psi_i$ indeed only depends on $\varepsilon$ and $\pi_A$. $\square$

If we consider the countable set $\Phi_A := \{\psi_\varepsilon \mid \varepsilon \in \mathbb{Q}\}$ of all $\varepsilon$-characteristic sentences for a $\mathbb{V}$-interpretation $\pi_A$ over a finite universe, then clearly, for all $\mathbb{V}$-interpretations $\pi_B$ over finite universes, $\pi_A [\![\varphi]\!] = \pi_B [\![\varphi]\!]$ for all $\varphi \in \Phi_A$ implies $\pi_A \cong \pi_B$, since $\pi_A [\![\psi_{\varepsilon^*}]\!] = \pi_B [\![\psi_{\varepsilon^*}]\!]$ holds in particular for the $\varepsilon^*$ from the above proposition.

Hence, we can say that $\Phi_A$ is a characteristic set of sentences for $\pi_A$. Of course, this trivially implies the fact that elementary equivalence and isomorphism coincide on $\mathbb{V}$ for finite universes.

**(4.23) Theorem.** For two $\mathbb{V}$-interpretations $\pi_A, \pi_B$ over finite universes, $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$.

Unfortunately, this means that we are still far from answering the question which semirings $K$ have coinciding notions of isomorphism and elementary equivalence for finite $K$-interpretations. Since it is impossible to go through all possible semirings, we would like to make more general statements in the next section about classes of semirings instead of single semirings.

## 4.5 Counterexample for Distributive Lattices

The most straightforward way to obtain general results is using polynomials and the fundamental property. For example, we could translate the counterexample of $\pi_{PQ}$ and $\pi_{QP}$ over $K_3$ to a polynomial semiring with variables $X' = \{x, y, z\}$ as follows.

$\pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 1 | 3 | 0 | 0 |
| b | 2 | 1 | 0 | 0 |
| c | 3 | 2 | 0 | 0 |

$\pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 3 | 1 | 0 | 0 |
| b | 1 | 2 | 0 | 0 |
| c | 2 | 3 | 0 | 0 |

translates to

$\pi'_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $x$ | $z$ | 0 | 0 |
| b | $y$ | $x$ | 0 | 0 |
| c | $z$ | $y$ | 0 | 0 |

$\pi'_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $z$ | $x$ | 0 | 0 |
| b | $x$ | $y$ | 0 | 0 |
| c | $y$ | $z$ | 0 | 0 |

Each nonzero element of $K_3$ is identified with its own variable. Of course, we cannot use $\mathbb{N}[X]$ as our polynomial semiring, because we relied heavily on the idempotence of both $+$ and $\cdot$ in $K_3$ for the proof that $\pi_{PQ} \equiv \pi_{QP}$, but $\mathbb{N}[X]$ is not idempotent. In fact, we will later see that absorption is also required. Hence, we translate the counterexample to $\text{PosBool}[X]$, which is the set of absorptive polynomials with exponents in $\mathbb{B}$, so it is absorptive and multiplication is idempotent.

Before moving on to prove that the counterexample is still valid, we will adapt it by reducing the number of variables and making use of the negative literals to make the result as general as possible. We will use the two $\text{PosBool}[X]$-interpretations $\pi_{xy} : \text{Lit}_A(\tau) \to \text{PosBool}[X]$ and $\pi_{yx} : \text{Lit}_A(\tau) \to \text{PosBool}[X]$ with two variables $X := \{x, y\}$, four elements $A := \{a, b, c, d\}$ and a signature $\tau = \{P, Q\}$ with two unary relation symbols depicted in the following tables.

$\pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $0$ | $y$ | $x$ | $0$ |
| b | $x$ | $0$ | $0$ | $y$ |
| c | $y$ | $x$ | $0$ | $0$ |
| d | $0$ | $0$ | $y$ | $x$ |

$\pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $y$ | $0$ | $0$ | $x$ |
| b | $0$ | $x$ | $y$ | $0$ |
| c | $x$ | $y$ | $0$ | $0$ |
| d | $0$ | $0$ | $x$ | $y$ |

The proof for $\pi_{xy} \not\cong \pi_{yx}$ is easy, since $\pi_{xy}(Pa) = 0$ and $\pi_{xy}(Qa) = y$, but there is no appropriate element $e \in A$ with $\pi_{yx}(Pe) = 0$ and $\pi_{yx}(Qe) = y$, hence an isomorphism $\sigma : \pi_{xy} \xrightarrow{\sim} \pi_{yx}$ cannot exist.

For the proof that $\pi_{xy} \equiv \pi_{yx}$, we intend to use the reduction theorem (4.20) again, which is why we require a separating set of homomorphisms $h : \mathrm{PosBool}[X] \to \mathbb{B}$. In order to construct those homomorphisms, it is useful to think of PosBool$[X]$ from the perspective of sets. Since the exponents of the monomials are in $\mathbb{B}$, we can think of the monomials in PosBool$[X]$ as subsets of $X$. Moreover, a polynomial $p \in \mathrm{PosBool}[X]$ can be thought of as a set of such monomials, since the coefficients are in $\mathbb{B}$ as well. In the following, we will use set notation on polynomials and monomials for more clarity.

**(4.24) Lemma** (Homomorphisms for PosBool$[X]$)**.** For each subset $S \subseteq X$, the function $h_S : \mathrm{PosBool}[X] \to \mathbb{B}$ defined as

$$h_S(p) := \begin{cases} \bot & \text{if } p = \sum_{x \in S} x \cdot p_x \text{ for } (p_x)_{x \in S} \subseteq \mathrm{PosBool}[X], \\ \top & \text{otherwise} \end{cases}$$

is a homomorphism. In other words, $h_S$ maps $p$ to $\bot$ if and only if each monomial $m$ in $p$ contains a variable $x$ from $S$.

*Proof.* Clearly, $h_S(0) = 0$, since 0 is the empty polynomial that does not contain any monomials, it can be expressed by choosing $p_x = 0$ for $x \in S$. Note that for $S = \emptyset$, the empty sum is 0 by definition. Also, $h(1) = 1$, because 1 contains only one empty monomial, which does not contain any variables.

For $p, q \in \mathrm{PosBool}[X]$, we must show that $h_S(p + q) = h_S(p) \vee h_S(q)$, that is, $h_S(p + q) = \top$ if and only if at least one of $h_S(p)$ or $h_S(q)$ is $\top$.

"$\Rightarrow$": If $h_S(p + q) = \top$, then $p + q$ contains monomials $m$ that contain no variable from $S$. Since $p + q$ is a subset of $p \cup q$, either $p$ or $q$ or both must already contain such a monomial, so $h_S(p) = \top$ or $h_S(q) = \top$.

"$\Leftarrow$": Suppose $p$ or $q$ contain monomials $m$ with no variables from $S$. Note that $p+q$ is obtained from $p \cup q$ with absorption. However, it is impossible that all monomials $m$ with no variables from $S$ are absorbed from $p \cup q$, because a monomial $m_x$ that does contain an $x \in S$ can never absorb a monomial $m$ that does not contain $x$ due to $m_x(x) = 1 > 0 = m(x)$. Thus, $p + q$ contains at least one monomial with no variables from $S$ and $h_S(p + q) = \top$.

Now, it remains to show $h_S(p \cdot q) = h_S(p) \wedge h_S(q)$, that is, $h_S(p \cdot q) = \bot$ if and only if at least one of $h_S(p)$ or $h_S(q)$ is $\bot$.

"$\Leftarrow$": Assume without loss of generality that $h_S(p) = \bot$. Then, $p = \sum_{x \in S} x \cdot p_x$ for some polynomials $(p_x)_{x\in S} \subseteq \text{PosBool}[X]$. Obviously,

$$p \cdot q = \left(\sum_{x\in S} x \cdot p_x\right) \cdot q = \sum_{x\in S} x \cdot (p_x \cdot q),$$

which yields $h_S(p \cdot q) = \bot$.

"$\Rightarrow$": We show the contraposition, assume $h_S(p), h_S(q)$ are both $\top$, hence they contain monomials $m_p, m_q$ without variables in $S$ respectively. Now, the product $p \cdot q$ prior to absorption contains $m_p \cdot m_q = m_p \cup m_q$, which does not contain a variable in $S$. As argued above, at least one such monomial is preserved in $p \cdot q$ after absorption, so $h_S(p \cdot q) = \top$, which ends the proof. □

It is not obvious that the homomorphisms defined in the lemma are in fact separating for PosBool$[X]$. In order to prove this, we require absorption. This explains why we use the absorptive version PosBool$[X]$ of polynomials that are idempotent in both operations, instead of the non-absorptive version $\mathbb{W}[X]$.

**(4.25) Lemma.** The set of homomorphisms $\{h_S \mid S \subseteq X\}$ defined in the previous lemma is separating for PosBool$[X]$.

*Proof.* According to definition (4.19), we must show that for all pairs $p, q \in \text{PosBool}[X]$ with $p \neq q$, there is an $S \subseteq X$ such that $h_S(p) \neq h_S(q)$. Instead, we show the contraposition, that is, we assume $h_S(p) = h_S(q)$ for all $S \subseteq X$ and prove that $p = q$ follows for all $p, q \in \text{PosBool}[X]$. Since we can view polynomials in PosBool$[X]$ as sets, we have to show that $m \in p$ if and only if $m \in q$ for all monomials $m \in \text{Mon}[\mathbb{B}, X]$. The monomials can be seen as sets of variables themselves, so we show this by induction on the size $|m| \in \mathbb{N}$ of the monomials.

Consider a monomial $m$ with $|m| \in \mathbb{N}$ and assume by induction that we have shown $m' \in p \Leftrightarrow m' \in q$ for all smaller monomials $m'$ with $|m'| < |m|$. For a contradiction, assume $m \in p$ and $m \notin q$ without loss of generality. Pick $S := X \setminus m$ as the set of all variables not contained in $m$. Clearly, $h_S(p) = \top$, since $p$ contains $m$, which contains no variables in $S$. By assumption, $h_S(q) = \top$ must hold as well, thus, $q$ contains a monomial $m_q$ that does not contain any variables from $X \setminus m$, which implies $m_q \subseteq m$. Since $m \notin q$, we have $m_q \subsetneq m$, but then, $m_q$ is smaller than $m$, so by induction, $m_q \in p$ as well. However, this is not possible, as $m_q$ would absorb $m$, which would imply $m \notin p$, a contradiction. We conclude that $m \in p$ if and only if $m \in q$. This ends the induction and the proof. □

Now that we have a separating set of homomorphisms, we can apply the reduction theorem (4.20) to show that $\pi_{xy} \equiv \pi_{yx}$. All that remains to show before applying the theorem is that $(h_S \circ \pi_{xy}) \equiv (h_S \circ \pi_{yx})$ for all $S \subseteq \{x, y\}$, which is easy to see from the following tables.

$\pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 0 | $y$ | $x$ | 0 |
| b | $x$ | 0 | 0 | $y$ |
| c | $y$ | $x$ | 0 | 0 |
| d | 0 | 0 | $y$ | $x$ |

$\pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $y$ | 0 | 0 | $x$ |
| b | 0 | $x$ | $y$ | 0 |
| c | $x$ | $y$ | 0 | 0 |
| d | 0 | 0 | $x$ | $y$ |

$h_\emptyset \circ \pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\top$ | $\top$ | $\bot$ |
| b | $\top$ | $\bot$ | $\bot$ | $\top$ |
| c | $\top$ | $\top$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\top$ | $\top$ |

$h_\emptyset \circ \pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\top$ | $\bot$ | $\bot$ | $\top$ |
| b | $\bot$ | $\top$ | $\top$ | $\bot$ |
| c | $\top$ | $\top$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\top$ | $\top$ |

$h_{\{x\}} \circ \pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| b | $\bot$ | $\bot$ | $\bot$ | $\top$ |
| c | $\top$ | $\bot$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\top$ | $\bot$ |

$h_{\{x\}} \circ \pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\top$ | $\bot$ | $\bot$ | $\bot$ |
| b | $\bot$ | $\bot$ | $\top$ | $\bot$ |
| c | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\bot$ | $\top$ |

$h_{\{y\}} \circ \pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\bot$ | $\top$ | $\bot$ |
| b | $\top$ | $\bot$ | $\bot$ | $\bot$ |
| c | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\bot$ | $\top$ |

$h_{\{y\}} \circ \pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\bot$ | $\bot$ | $\top$ |
| b | $\bot$ | $\top$ | $\bot$ | $\bot$ |
| c | $\top$ | $\bot$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\top$ | $\bot$ |

$h_X \circ \pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| b | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| c | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\bot$ | $\bot$ |

$h_X \circ \pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| b | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| c | $\bot$ | $\bot$ | $\bot$ | $\bot$ |
| d | $\bot$ | $\bot$ | $\bot$ | $\bot$ |

The pairs of corresponding $\mathbb{B}$-interpretations are isomorphic. As a formality, the isomorphisms are given by

$$\begin{aligned}
\sigma_\emptyset &: \; a \mapsto b,\; b \mapsto a,\; c \mapsto c,\; d \mapsto d \quad (\sigma_\emptyset \text{ swaps } a, b),\\
\sigma_{\{x\}} &: \; a \mapsto c,\; b \mapsto d,\; c \mapsto a,\; d \mapsto b \quad (\sigma_{\{x\}} \text{ swaps } a, c \text{ and } b, d),\\
\sigma_{\{y\}} &: \; a \mapsto d,\; b \mapsto c,\; c \mapsto b,\; d \mapsto a \quad (\sigma_{\{y\}} \text{ swaps } a, d \text{ and } b, c) \quad \text{and}\\
\sigma_X &: \; a \mapsto a,\; b \mapsto b,\; c \mapsto c,\; d \mapsto d \quad (\sigma_X = \mathrm{id}_A).
\end{aligned}$$

By the reduction theorem (4.20), $\pi_{xy} \equiv \pi_{yx}$. Unlike our counterexample on $K_3$, due to the universal property of PosBool$[X]$ stated in proposition (3.16), this counterexample is valid for a whole class of semirings, as stated in the following theorem.

**(4.26) Theorem.** For any absorptive, multiplicatively idempotent semiring $K$ with at least three elements, $\pi_A \equiv \pi_B$ does not imply $\pi_A \cong \pi_B$ for all pairs of model-defining $K$-interpretations $\pi_A, \pi_B$ over finite universes. In particular, there is a counterexample over a universe with four elements and a signature with two unary relations.

*Proof.* Pick $A := \{a, b, c, d\}$ and $\tau := \{P, Q\}$ as before. Now, choose two nonzero elements $r, s \in K$ with $r \neq s$, which exist by assumption. The counterexample is given as follows.

$\pi_{rs}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 0 | $s$ | $r$ | 0 |
| b | $r$ | 0 | 0 | $s$ |
| c | $s$ | $r$ | 0 | 0 |
| d | 0 | 0 | $s$ | $r$ |

$\pi_{sr}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $s$ | 0 | 0 | $r$ |
| b | 0 | $r$ | $s$ | 0 |
| c | $r$ | $s$ | 0 | 0 |
| d | 0 | 0 | $r$ | $s$ |

For $\pi_{rs} \not\cong \pi_{sr}$, observe that $\pi_{rs}$ has the element $a$ with $\pi_{rs}(Pa) = 0, \pi_{rs}(Qa) = s$, while $\pi_{sr}$ has no such element, since $\{0, r, s\}$ are pairwise distinct. Therefore, no isomorphism $\sigma : \pi_{rs} \xrightarrow{\sim} \pi_{sr}$ exists.

From proposition (3.16), we infer that for $X := \{x, y\}$, the assignment $e : X \to K$ with $x \mapsto r, y \mapsto s$ induces a unique homomorphism $h_e$ : PosBool$[X] \to K$ with $h_e(x) = r$ and $h_e(y) = s$. Clearly, this means $(h_e \circ \pi_{xy}) = \pi_{rs}$ and $(h_e \circ \pi_{yx}) = \pi_{sr}$. Now, consider any sentence $\psi \in \mathsf{FO}(\tau)$. By the fundamental property $(*)$ and the equivalence $\pi_{xy} \equiv \pi_{yx}$, marked with $(\star)$, we have

$$\pi_{rs}\,[\![\psi]\!] = (h_e \circ \pi_{xy})\,[\![\psi]\!] \overset{*}{=} h_e(\pi_{xy}\,[\![\psi]\!]) \overset{\star}{=} h_e(\pi_{yx}\,[\![\psi]\!]) \overset{*}{=} (h_e \circ \pi_{yx})\,[\![\psi]\!] = \pi_{sr}\,[\![\psi]\!]\,,$$

hence $\pi_{rs} \equiv \pi_{sr}$, which ends the proof. $\square$

**(4.27) Remark** (Binary Relations)**.** The above counterexample for PosBool$[X]$ can also be transformed into a counterexample with one binary relation $R$ instead of two unary relations $P$ and $Q$ as depicted below.

$\pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 0 | $y$ | $x$ | 0 |
| b | $x$ | 0 | 0 | $y$ |
| c | $y$ | $x$ | 0 | 0 |
| d | 0 | 0 | $y$ | $x$ |

$\pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $y$ | 0 | 0 | $x$ |
| b | 0 | $x$ | $y$ | 0 |
| c | $x$ | $y$ | 0 | 0 |
| d | 0 | 0 | $x$ | $y$ |

$\pi'_{xy}$ :

| $A \times A$ | $R$ | $\neg R$ | |
|---|---|---|---|
| (a, a) | 0 | $x$ | $P$ |
| (a, b) | $x$ | 0 | |
| (a, c) | $y$ | 0 | |
| (a, d) | 0 | $y$ | |
| (a, e) | $x$ | 0 | |
| (b, a) | 0 | $x$ | $P$ |
| (b, b) | $x$ | 0 | |
| (b, c) | $y$ | 0 | |
| (b, d) | 0 | $y$ | |
| (b, e) | $x$ | 0 | |
| (c, a) | 0 | $x$ | $P$ |
| (c, b) | $x$ | 0 | |
| (c, c) | $y$ | 0 | |
| (c, d) | 0 | $y$ | |
| (c, e) | $x$ | 0 | |
| (d, a) | 0 | $x$ | $P$ |
| (d, b) | $x$ | 0 | |
| (d, c) | $y$ | 0 | |
| (d, d) | 0 | $y$ | |
| (d, e) | $x$ | 0 | |
| (e, a) | $y$ | 0 | $Q$ |
| (e, b) | 0 | $y$ | |
| (e, c) | $x$ | 0 | |
| (e, d) | 0 | $x$ | |
| (e, e) | $y$ | 0 | |

$\pi'_{yx}$ :

| $A \times A$ | $R$ | $\neg R$ | |
|---|---|---|---|
| (a, a) | $y$ | 0 | $P$ |
| (a, b) | 0 | $y$ | |
| (a, c) | $x$ | 0 | |
| (a, d) | 0 | $x$ | |
| (a, e) | $x$ | 0 | |
| (b, a) | $y$ | 0 | $P$ |
| (b, b) | 0 | $y$ | |
| (b, c) | $x$ | 0 | |
| (b, d) | 0 | $x$ | |
| (b, e) | $x$ | 0 | |
| (c, a) | $y$ | 0 | $P$ |
| (c, b) | 0 | $y$ | |
| (c, c) | $x$ | 0 | |
| (c, d) | 0 | $x$ | |
| (c, e) | $x$ | 0 | |
| (d, a) | $y$ | 0 | $P$ |
| (d, b) | 0 | $y$ | |
| (d, c) | $x$ | 0 | |
| (d, d) | 0 | $x$ | |
| (d, e) | $x$ | 0 | |
| (e, a) | 0 | $x$ | $Q$ |
| (e, b) | $x$ | 0 | |
| (e, c) | $y$ | 0 | |
| (e, d) | 0 | $y$ | |
| (e, e) | $y$ | 0 | |

The idea behind this construction is that the elements $\{a, b, c, d\}$ may be swapped around by isomorphisms, while the element $e$ is a “special”, fixed element. This allows us to “split” the previous counterexample $\pi_{xy}, \pi_{yx}$ by $P$ and $Q$ and encode it into a single relation as indicated by the labels in the picture. The formal proof of $\pi'_{xy} \equiv \pi'_{yx}$ and $\pi'_{xy} \not\cong \pi'_{yx}$ will be omitted.

Of course, this counterexample also lifts to all absorptive, multiplicatively idempotent semirings with at least three elements in the same manner as $\pi_{xy}, \pi_{yx}$.

For now, the question of isomorphism versus elementary equivalence has been sufficiently answered for absorptive, multiplicatively idempotent semirings. Note that according to proposition (2.15), those are precisely the semirings induced by bounded distributive lattices. Of course, this is a very restricted class of semirings, and we would like to lift some of the restrictions in the following.

## 4.6 General Polynomials

If we lift all the restrictions, we obtain $\mathbb{N}[X]$ as the most general semiring according to theorem (3.8). In the following, we are going to prove that elementary equivalence implies isomorphism on $\mathbb{N}[X]$. To simplify the approach, we can start with $\mathbb{N}$ and later lift the result to $\mathbb{N}[X]$.

Thanks to addition and multiplication not being idempotent in $\mathbb{N}$, we can imagine that a similar approach as proposition (4.22) for the Viterbi semiring might be viable. That is, we take the characteristic formula

$$\varphi_{\mathfrak{A}} := \exists x_1 \dots \exists x_n \left( \bigwedge_{1 \le i < j \le n} x_i \ne x_j \land \forall y \left( \bigvee_{1 \le i \le n} y = x_i \right) \land \bigwedge_{L \in \mathrm{Lit}_A(\tau), \mathfrak{A} \models L} L[\overline{a}/\overline{x}] \right)$$

for the structure $\mathfrak{A}$ in the standard $\mathbb{B}$-semiring and adapt it by repeating literals in order to make their values distinguishable and prevent “permutations of relations”. The first major problem with this approach over $\mathbb{N}$ is that the sum of two elements $a, b \in \mathbb{N}$ is not their maximum as in the Viterbi semiring. Hence, the existential quantifiers are not interpreted by maxima and the final interpretation of the characteristic formula takes multiple permutations of the same structure into account. Luckily, we can remedy this problem using the following lemma.

**(4.28) Lemma.** Let $\overline{a} = (a_1, \dots, a_k), \overline{b} = (b_1, \dots, b_k) \in \mathbb{N}^k$ be two $k$-tuples and $a_i, b_i < c \in \mathbb{N}$ for all $1 \le i \le k$. Then, an exponent $e \in \mathbb{N}$ exists such that

$$\sum_{i=1}^{k} a_i^e = \sum_{i=1}^{k} b_i^e$$

implies that there is a permutation $\sigma : \{1, \dots, k\} \to \{1, \dots, k\}$ with $a_i = b_{\sigma(i)}$ for all $1 \le i \le k$ and the exponent only depends on $k$ and the bound $c$.

*Proof.* Sort the tuples in non-decreasing order, or more formally, pick permutations $\sigma_a, \sigma_b : \{1, \dots, k\} \to \{1, \dots, k\}$ such that

$$a_{\sigma_a(1)} \le \dots \le a_{\sigma_a(k)} \quad \text{and}$$
$$b_{\sigma_b(1)} \le \dots \le b_{\sigma_b(k)}.$$

We will provide the value of $e$ later, for now, assume $e \in \mathbb{N}$ and

$$\sum_{i=1}^{k} a_i^e = \sum_{i=1}^{k} b_i^e.$$

Of course, since $\sigma_a, \sigma_b$ are permutations, we can rearrange the sums to

$$\sum_{i=1}^{k} a_{\sigma_a(i)}^e = \sum_{i=1}^{k} b_{\sigma_b(i)}^e.$$

We want to prove that $(*)$ $a_{\sigma_a(i)} = b_{\sigma_b(i)}$ for all $1 \leq i \leq k$. For a contradiction, assume this is not the case and pick the largest $1 \leq j \leq k$ such that $a_{\sigma_a(j)} \neq b_{\sigma_b(j)}$. Without loss of generality, we may say $a_{\sigma_a(j)} < b_{\sigma_b(j)}$. Now, we will show that

$$\sum_{i=1}^{k} a_{\sigma_a(i)}^e < \sum_{i=1}^{k} b_{\sigma_b(i)}^e.$$

Of course, we can leave the summands with $i > j$ out of the consideration, so it remains to show

$$\sum_{i=1}^{j} a_{\sigma_a(i)}^e < \sum_{i=1}^{j} b_{\sigma_b(i)}^e.$$

Since the sequences are sorted, $a_{\sigma_a(i)} \leq a_{\sigma_a(j)}$ for all $i \leq j$ and in the worst case, all $b_{\sigma_b(i)}$ with $j < i$ are zero, so it suffices to show

$$j \cdot a_{\sigma_a(j)}^e < b_{\sigma_b(j)}^e \quad \text{or just} \quad k \cdot a_{\sigma_a(j)}^e < b_{\sigma_b(j)}^e, \quad \text{due to } j \leq k.$$

If $a_{\sigma_a(j)} = 0$, we are done, otherwise, consider the ratio

$$\frac{b_{\sigma_b(j)}}{a_{\sigma_a(j)}} \geq \frac{b_{\sigma_b(j)}}{b_{\sigma_b(j)} - 1} > \frac{c}{c-1} > 1.$$

Notice that $c > 1$, otherwise all values would have to be zero. Obviously,

$$\lim_{n \to \infty} \left( \frac{c}{c-1} \right)^n = \infty,$$

so we can simply pick

$$e := \min \left\{ n \in \mathbb{N} \mid k < \left( \frac{c}{c-1} \right)^n \right\}.$$

Then, we have

$$k < \left( \frac{c}{c-1} \right)^e < \left( \frac{b_{\sigma_b(j)}}{b_{\sigma_b(j)} - 1} \right)^e,$$

which implies $k \cdot a_{\sigma_a(j)}^e < b_{\sigma_b(j)}^e$ and yields the desired contradiction. Note that $e$ only depends on $c$ and $k$.

Finally, we choose $\sigma := \sigma_b \circ \sigma_a^{-1}$, then $a_i = a_{\sigma_a(\sigma_a^{-1}(i))} \stackrel{*}{=} b_{\sigma_b(\sigma_a^{-1}(i))} = b_{\sigma(i)}$ with $(*)$ from above, which ends the proof. □

This lemma is very useful for "separating" the values of sums. We can use it in our characteristic formula as follows. Pick $e$ "large enough" and use the formula

$$\varphi_{\mathfrak{A}} := \exists x_1 \ldots \exists x_n \left( \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1 \leq i \leq n} y = x_i \right) \wedge \bigwedge_{L \in \mathrm{Lit}_A(\tau), \mathfrak{A} \models L} L[\overline{a}/\overline{x}] \right)^e,$$

where "exponentiation" simply means that we combine the same formula $e$ times with $\wedge$ into a conjunction. Now, the summands in the sum induced by the existential quantifiers $\exists x_1 \dots \exists x_n$ are exponentiated with $e$, so if two $\mathbb{N}$-interpretations with "small enough" values yield the same sum, then there must be a permutation between the summands. We can formalize the assertions that the values of an $\mathbb{N}$-interpretations are "small enough" as follows.

**(4.29) Definition** (Bounded $\mathbb{N}$-interpretation)**.** For $c \in \mathbb{N}$, an $\mathbb{N}$-interpretation $\pi : \mathrm{Lit}_A(\tau) \to \mathbb{N}$ is *bounded* by $c$ if $\pi(L) < c$ for all $L \in \mathrm{Lit}_A(\tau)$.

Before we are ready to define characteristic formulas for $\mathbb{N}$-interpretations, we have to clarify how the literals should be repeated. In $\mathbb{V}$, this was done by a conjunction, but for $\mathbb{N}$, it is easier to use a disjunction, as indicated by the following simple lemma.

**(4.30) Lemma** (Digit Lemma)**.** Let $\overline{a} = (a_1, \dots, a_k), \overline{b} = (b_1, \dots, b_k) \in \mathbb{N}^k$ be two $k$-tuples with $k \in \mathbb{N}_{>0}$ and $a_i, b_i < c \in \mathbb{N}$ for all $1 \leq i \leq k$. Then,

$$\sum_{i=1}^{k} a_i \cdot c^{i-1}, \sum_{i=1}^{k} b_i \cdot c^{i-1} < c^k$$

always holds and

$$\sum_{i=1}^{k} a_i \cdot c^{i-1} = \sum_{i=1}^{k} b_i \cdot c^{i-1}$$

implies $a_i = b_i$ for all $1 \leq i \leq k$.

*Proof.* We prove the lemma by induction on $k$. For $k = 1$, the first claim holds by assumption and the second claim is trivially true.

Now, consider $k > 1$, then

$$\begin{aligned}\sum_{i=1}^{k} a_i \cdot c^{i-1} &= a_k \cdot c^{k-1} + \sum_{i=1}^{k-1} a_i \cdot c^{i-1} \\ &\overset{*}{<} a_k \cdot c^{k-1} + c^{k-1} \\ &\leq (c-1) \cdot c^{k-1} + c^{k-1} \\ &= c^k,\end{aligned}$$

where $(*)$ holds by induction. The proof for $\overline{b}$ is similar.

For the second part, assume

$$\sum_{i=1}^{k} a_i \cdot c^{i-1} = \sum_{i=1}^{k} b_i \cdot c^{i-1}.$$

This implies

$$\sum_{i=1}^{k} a_i \cdot c^{i-1} \equiv \sum_{i=1}^{k} b_i \cdot c^{i-1} \mod c^{k-1},$$

and since

$$\sum_{i=1}^{k-1} a_i \cdot c^{i-1}, \sum_{i=1}^{k-1} b_i \cdot c^{i-1} < c^{k-1}$$

by induction, we have

$$\sum_{i=1}^{k-1} a_i \cdot c^{i-1} = \sum_{i=1}^{k-1} b_i \cdot c^{i-1}.$$

Then, $a_i = b_i$ for all $1 \leq i < k$ by induction, so $a_k \cdot c^{k-1} = b_k \cdot c^{k-1}$ remains after cancellation of equal summands, hence $a_k = b_k$ as well. □

This lemma is very straightforward and its name comes from the fact that the numbers $a_i, b_i$ can be seen as the $i$-th digit of the numbers $\overline{a}, \overline{b}$ in a numeral system with radix $c$. We will use it for the literals in our characteristic formula for $\mathbb{N}$-interpretations, which will be defined as follows.

**(4.31) Proposition** ($c$-characteristic Sentence)**.** Let $\pi_A : \mathrm{Lit}_A(\tau) \to \mathbb{N}$ be a model-defining $\mathbb{N}$-interpretation over a finite universe $A$ with $|A| = n$. Then, for each $c \in \mathbb{N}$ such that $\pi_A$ is bounded by $c$, there is a sentence $\psi_c \in \mathsf{FO}(\tau)$ such that for all model-defining $\mathbb{N}$-interpretations $\pi_B : \mathrm{Lit}_B(\tau) \to \mathbb{N}$ that are bounded by $c$, $\pi_A [\![\psi_c]\!] = \pi_B [\![\psi_c]\!]$ implies $\pi_A \cong \pi_B$.

*Proof.* Fix arbitrary orders $A := \{a_1, \ldots, a_n\}$ and $\mathrm{Lit}_A(\tau) := \{L_1, \ldots, L_k\}$, where $k = |\mathrm{Lit}_A(\tau)|$ is finite and only depends on $n$ and $\tau$. We construct the formula

$$\psi_c := \exists x_1 \ldots \exists x_n \left( \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1 \leq i \leq n} y = x_i \right) \wedge \left( \bigvee_{i=1}^{k} c^{i-1} \cdot L_i[\overline{a}/\overline{x}] \right) \right)^e,$$

where exponentiation with $e \in \mathbb{N}$ means that we repeat the formula $e$ times in a conjunction and multiplication with $c^{i-1} \in \mathbb{N}$ means that we repeat the formula $c^{i-1}$ times in a disjunction. We will clarify the value of $e$ later and subdivide the formula into

$$\varphi_n(\overline{x}) = \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1 \leq i \leq n} y = x_i \right),$$

the part that asserts that there are $n$ elements, and

$$\varphi_L(\overline{x}) = \bigvee_{i=1}^{k} c^{i-1} \cdot L_i[\overline{a}/\overline{x}],$$

the part with the literals, so that we can write

$$\psi_c = \exists x_1 \ldots \exists x_n (\varphi_n(\overline{x}) \wedge \varphi_L(\overline{x}))^e.$$

Also, let $\varphi(\overline{x}) := (\varphi_n(\overline{x}) \wedge \varphi_L(\overline{x}))^e$ so that $\psi_c = \exists x_1 \ldots \exists x_n \varphi(\overline{x})$.

Our first observation is that $\pi_A [\![\psi_c]\!] > 0$, because $\pi_A [\![\varphi(\overline{a})]\!] > 0$. This is explained by the fact that $\pi_A [\![\varphi_n(\overline{a})]\!] = 1$ clearly holds and $\pi_A [\![\varphi_L(\overline{a})]\!] > 0$ as well, since $\pi_A$ is model-defining, so it must assign a nonzero value to at least one of the literals.

Now, assume $\pi_B$ is defined as above with $\pi_B [\![\psi_c]\!] = \pi_A [\![\psi_c]\!] > 0$. This implies $|B| = n$, because $\pi [\![\varphi_n(\overline{t})]\!] \in \{0, 1\}$ evaluates to 1 for any $\mathbb{N}$-interpretation $\pi$ if and only if the $n$ elements $\overline{t}$ assigned to $\overline{x}$ are pairwise distinct and there are no more elements in the universe of $\pi$. We write $B = \{b_1, \ldots, b_n\}$ and $\overline{b} = (b_1, \ldots, b_n)$.

Since $\varphi_n(\overline{x})$ filters out assignments where the values of $\overline{x}$ are not pairwise distinct and otherwise evaluates to 1, we can conclude

$$\pi_A \llbracket \psi_c \rrbracket = \sum_{\sigma \in S_n} \pi_A \llbracket \varphi_L(\sigma(\overline{a})) \rrbracket^e \quad \text{and}$$
$$\pi_B \llbracket \psi_c \rrbracket = \sum_{\sigma \in S_n} \pi_B \left\llbracket \varphi_L(\sigma(\overline{b})) \right\rrbracket^e,$$

where $S_n$ denotes the group of permutations $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ and $\sigma(\overline{t})$ for an $n$-tuple $\overline{t} = (t_1, \ldots, t_n)$ simply denotes the permuted tuple by $\sigma$, that is, $\sigma(\overline{t}) \coloneqq (t_{\sigma(1)}, \ldots, t_{\sigma(n)})$.

Before we continue, we must choose an appropriate value of $e$. For that, we observe that $\pi_A \llbracket \varphi_L(\sigma(\overline{a})) \rrbracket$ and $\pi_B \left\llbracket \varphi_L(\sigma(\overline{b})) \right\rrbracket$ are bounded by $c^k$ due to lemma (4.30), since both $\pi_A$ and $\pi_B$ are bounded by $c$. Moreover, $|S_n| = n!$, so we can apply lemma (4.28) and choose $e \in \mathbb{N}$ so that

$$\sum_{\sigma \in S_n} \pi_A \llbracket \varphi_L(\sigma(\overline{a})) \rrbracket^e = \pi_A \llbracket \psi_c \rrbracket = \pi_B \llbracket \psi_c \rrbracket = \sum_{\sigma \in S_n} \pi_B \left\llbracket \varphi_L(\sigma(\overline{b})) \right\rrbracket^e$$

implies that there is a permutation $\rho$ between the summands. Note that $e$ only depends on $n!$ and $c^k$, so the formula is well-defined.

Now, the existence of a permutation $\rho$ between the above summands implies in particular that two of them are equal, hence there are $\sigma_A, \sigma_B \in S_n$ such that

$$\pi_A \llbracket \varphi_L(\sigma_A(\overline{a})) \rrbracket = \pi_B \left\llbracket \varphi_L(\sigma_B(\overline{b})) \right\rrbracket.$$

Looking at $\varphi_L(\overline{x})$ yields the observation that

$$\pi_A \llbracket \varphi_L(\sigma_A(\overline{a})) \rrbracket = \sum_{i=1}^{k} c^{i-1} \pi_A(L_i[\overline{a}/\sigma_A(\overline{a})]) \quad \text{and}$$
$$\pi_B \left\llbracket \varphi_L(\sigma_B(\overline{b})) \right\rrbracket = \sum_{i=1}^{k} c^{i-1} \pi_B(L_i[\overline{a}/\sigma_B(\overline{b})]).$$

Again, recall that the values of $\pi_A$ and $\pi_B$ are bounded by $c$. Applying lemma (4.30) yields that

$$\sum_{i=1}^{k} c^{i-1} \pi_A(L_i[\overline{a}/\sigma_A(\overline{a})]) = \sum_{i=1}^{k} c^{i-1} \pi_B(L_i[\overline{a}/\sigma_B(\overline{b})])$$

implies $\pi_A(L_i[\overline{a}/\sigma_A(\overline{a})]) = \pi_B(L_i[\overline{a}/\sigma_B(\overline{b})])$ for all $1 \leq i \leq k$.

We claim that $\sigma : \pi_A \xrightarrow{\sim} \pi_B$ defined as $\sigma(a_i) \coloneqq b_{\sigma_B(\sigma_A^{-1}(i))}$ for all $1 \leq i \leq n$ is an isomorphism. Due to $|A| = |B| = n$ and $\sigma_A, \sigma_B$ being permutations, $\sigma$ is clearly bijective. Now, for $L \in \mathrm{Lit}_A(\tau)$, let $j$ be the index of $L$ so that $L = L_j$. Then,

$$\pi_A(L_j) = \pi_A(L_j[\overline{a}/\sigma_A(\sigma_A^{-1}(\overline{a}))]) = \pi_B(L_j[\overline{a}/\sigma_B(\sigma_A^{-1}(\overline{b}))]) = \pi_B(L_j[\overline{a}/\sigma(\overline{a})]),$$

which concludes the proof, since it shows $\pi_A = \pi_B \circ \sigma$. □

**(4.32) Corollary.** For two model-defining $\mathbb{N}$-interpretations $\pi_A, \pi_B$ over finite universes with the same signature, $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$.

*Proof.* Since $\pi_A, \pi_B$ are finite, there is a $c \in \mathbb{N}$ so that both are bounded by $c$. Now, construct $\psi_c$ for $\pi_A$ or $\pi_B$ according to the above proposition. Then, $\pi_A \equiv \pi_B$ implies $\pi_A [\![\psi_c]\!] = \pi_B [\![\psi_c]\!]$, which yields $\pi_A \cong \pi_B$. □

Similarly to $\mathbb{V}$, an $\mathbb{N}$-interpretation is characterized up to isomorphism by a countably infinite set of formulas $\Phi_A := \{\psi_c \mid c \in \mathbb{N}, \pi_A \text{ is bounded by } c\}$. Unfortunately, the $\mathbb{N}$-semiring by itself is not particularly interesting, since it does not immediately provide any insights for other semirings. However, with a little more work and the beloved fundamental property, we can lift this result to $\mathbb{N}[X]$.

Suppose $X = \{x_1, \dots, x_k\}$. By theorem (3.8), each assignment $e : X \to \mathbb{N}$ induces a unique homomorphism $h_e : \mathbb{N}[X] \to \mathbb{N}$. Now, suppose we have two finite $\mathbb{N}[X]$-interpretations $\pi_A, \pi_B$ and the corresponding $\mathbb{N}$-interpretations induced by the assignment $\pi'_A := h_e \circ \pi_A, \pi'_B := h_e \circ \pi_B$. By the fundamental property, if $\pi_A \equiv \pi_B$, then $\pi'_A \equiv \pi'_B$ as well, and since they are $\mathbb{N}$-interpretations, this implies $\pi'_A \cong \pi'_B$. We would like to infer that $\pi_A \cong \pi_B$, however, we can only do this if $h_e$ is injective.

Of course, $h_e$, which corresponds to evaluating a polynomial, is never injective unless $X = \emptyset$. If we take the value $c \in \mathbb{N}$ assigned to $x_1$, that is $e(x_1) = c$, then, we can already provide two distinct polynomials that map to $c$, the constant polynomial $c$ and the polynomial $x_1$ that only contains one variable both clearly map to

$$h_e(c) = c = h_e(x_1).$$

Therefore, we cannot hope to find an injective $h_e$ that would allow us to lift our result from $\mathbb{N}$ to $\mathbb{N}[X]$ directly.

However, any polynomial in $\mathbb{N}[X]$ is finite, which implies that it is bounded in the sense that both coefficients and exponents cannot exceed a certain value, as formalized in the following definition.

**(4.33) Definition** (Bounded Polynomial)**.** A polynomial $p \in \mathbb{N}[X]$ is *bounded* by $(c, n) \in \mathbb{N} \times \mathbb{N}$ if all its coefficients are smaller than $c$ and all its exponents are smaller than $n$. More formally, recall the definition of polynomials in $\mathbb{N}[X]$ as functions $p : \text{Mon}[\mathbb{N}, X] \to \mathbb{N}$, now, $p$ is bounded by $(c, n)$ if

$$\begin{aligned} p(m) &< c \quad \text{for all } m \in \text{Mon}[\mathbb{N}, X] \quad \text{and} \\ m(x) &< n \quad \text{for all } m \in \text{supp}(p) \text{ and } x \in X. \end{aligned}$$

Any polynomial is bounded due to the finiteness of supp($p$). In the following, the set of $(c, n)$-bounded polynomials in $\mathbb{N}[X]$ is denoted as $\mathbb{N}[X](c, n)$.

A $\mathbb{N}[X]$-interpretation $\pi : \text{Lit}_A(\tau) \to \mathbb{N}[X]$ is *bounded* by $(c, n)$ if every polynomial $\pi(L)$ for $L \in \text{Lit}_A(\tau)$ is bounded by $(c, n)$, or more concisely, $\pi(\text{Lit}_A(\tau)) \subseteq \mathbb{N}[X](c, n)$. If $A$ is finite, then $\pi$ must be bounded.

With the insight that any finite $\mathbb{N}[X]$-interpretation is bounded, our next goal is to produce an assignment of variables $e : X \to \mathbb{N}$ such that the induced homomorphism $h_e : \mathbb{N}[X] \to \mathbb{N}$ is at least injective when restricted to bounded polynomials $\mathbb{N}[X](c, n)$. This can be done by a series $e(x_1), \dots, e(x_k)$ of increasingly "large" values, as shown in the following lemma.

**(4.34) Lemma.** Let $X = \{x_1, \dots, x_k\}$. Consider the assignment $e : X \to \mathbb{N}$ with

$$e(x_i) = c^{n^{i-1}} \quad \text{for all } i \in \{1, \dots, k\}.$$

Then, the induced homomorphism $h_e : \mathbb{N}[X] \to \mathbb{N}$ has the properties

$$\begin{aligned}&(1) \quad h_e|_{\mathbb{N}[X](c,n)} \text{ is injective and}\\ &(2) \quad h_e(\mathbb{N}[X](c,n)) = \{i \in \mathbb{N} \mid i < c^{n^k}\}.\end{aligned}$$

In other words, $h_e|_{\mathbb{N}[X](c,n)}$ is a bijection between $\mathbb{N}[X](c,n)$ and $[0,C)_{\mathbb{N}}$ with $C := c^{n^k}$.

*Proof.* We prove the claim via induction on the number of variables $k \in \mathbb{N}$. For $k = 0$, we have $\mathbb{N}[\emptyset] \cong \mathbb{N}$ and $e$ is the empty assignment. Of course, $\mathbb{N}[\emptyset](c,n) = \{0, \ldots, c-1\}$ and clearly, $h_e$ maps all of these constant polynomials to their respective constant, so $h_e$ is a bijection between $\mathbb{N}[X](c,n)$ and $[0,c)_{\mathbb{N}}$. Note that $c = c^1 = c^{n^0} = C$, so the base case is covered.

Now, assume $k > 0$. It is useful to observe that a polynomial $\mathbb{N}[X]$ can be seen as a polynomial in $\mathbb{N}[\{x_1, \ldots, x_{k-1}\}][\{x_k\}]$ with "coefficients" being other polynomials in $\mathbb{N}[\{x_1, \ldots, x_{k-1}\}] = \mathbb{N}[X \setminus \{x_k\}]$ and a single variable $x_k$. We can write any $p \in \mathbb{N}[X](c,n)$ uniquely as

$$p = \sum_{i=0}^{n-1} p_i \cdot x_k^i,$$

where the "coefficients" $(p_i)_{0 \le i < n}$ are in fact polynomials in $\mathbb{N}[X \setminus \{x_k\}](c,n)$. The converse also holds, that is, any $p$ with such a representation is in $\mathbb{N}[X](c,n)$.

Notice that on $\mathbb{N}[X \setminus \{x_k\}]$, $h_e$ coincides with the homomorphism $h' : \mathbb{N}[X \setminus \{x_k\}] \to \mathbb{N}$ induced by the restricted assignment $e|_{X \setminus \{x_k\}}$. Moreover, by induction, $h'$ is a bijection between $\mathbb{N}[X \setminus \{x_k\}](c,n)$ and $[0, c^{n^{k-1}})_{\mathbb{N}}$. Now, pick $p, q \in \mathbb{N}[X](c,n)$ with their representations

$$p = \sum_{i=0}^{n-1} p_i \cdot x_k^i \quad \text{and} \quad q = \sum_{i=0}^{n-1} q_i \cdot x_k^i,$$

where $(p_i)_{0 \le i < n}$ and $(q_i)_{0 \le i < n}$ are all in $\mathbb{N}[X \setminus \{x_k\}](c,n)$. We observe that

$$\begin{aligned} h_e(p) &= h_e\left(\sum_{i=0}^{n-1} p_i \cdot x_k^i\right) = \sum_{i=0}^{n-1} h_e(p_i) \cdot h_e(x_k)^i = \sum_{i=0}^{n-1} h'(p_i) \cdot \left(c^{n^{k-1}}\right)^i \quad \text{and} \\ h_e(q) &= h_e\left(\sum_{i=0}^{n-1} q_i \cdot x_k^i\right) = \sum_{i=0}^{n-1} h_e(q_i) \cdot h_e(x_k)^i = \sum_{i=0}^{n-1} h'(q_i) \cdot \left(c^{n^{k-1}}\right)^i. \end{aligned}$$

Since the values of $h'(p_i), h'(q_i)$ are bounded by $c^{n^{k-1}}$ by induction, we can apply the "digit" lemma (4.30) and obtain that

$$h_e(p), h_e(q) < \left(c^{n^{k-1}}\right)^n = c^{n^{k-1} \cdot n} = c^{n^k} = C,$$

in particular, $h_e(\mathbb{N}[X](c,n)) \subseteq [0,C)_{\mathbb{N}}$, since $p, q$ were arbitrary in $\mathbb{N}[X](c,n)$.

Moreover, if $h_e(p) = h_e(q)$, this implies $h'(p_i) = h'(q_i)$ for all $0 \le i < n$. By induction, $h'$ is injective on $\mathbb{N}[X \setminus \{x_k\}](c,n)$, hence this would yield $p_i = q_i$ for $0 \le i < n$ and therefore $p = q$. Thus, we have shown that $h_e|_{\mathbb{N}[X](c,n)} : \mathbb{N}[X](c,n) \to [0,C)_{\mathbb{N}}$ is injective.

Since both sets are finite, we can conclude the proof by counting $|\mathbb{N}[X](c,n)|$. Consider a polynomial $p \in \mathbb{N}[X]$ and a monomial $m \in \mathrm{supp}(p)$ that occurs in $p$. There are $k$

variables and each of them may only be assigned with any of the $n$ possible exponents by $m$ due to the bound $n$ on the exponents, so there are exactly $n^k$ distinct monomials that may occur in $p$. The polynomial $p$ may assign any of the $c$ possible coefficients to each of the monomials, so there are exactly $c^{n^k} = C$ polynomials in $\mathbb{N}[X](c,n)$, hence

$$|\mathbb{N}[X](c,n)| = C = |[0,C)_{\mathbb{N}}|.$$

An injective function between two finite universes is always surjective, thus, $h_e|_{\mathbb{N}[X](c,n)}$ is a bijection between $\mathbb{N}[X](c,n)$ and $[0,C)_{\mathbb{N}}$, which ends the proof. ☐

Now, as announced earlier, we can lift the result that elementary equivalence implies isomorphism for $\mathbb{N}$-interpretations to $\mathbb{N}[X]$ by invoking the fundamental property.

**(4.35) Proposition** ($(c,n)$-characteristic Sentence)**.** Let $\pi_A : \mathrm{Lit}_A(\tau) \to \mathbb{N}[X]$ be a model-defining $\mathbb{N}[X]$-interpretation over a finite universe $A$. For each $(c,n) \in \mathbb{N} \times \mathbb{N}$ such that $\pi_A$ is bounded by $(c,n)$, there is a sentence $\psi_{(c,n)} \in \mathsf{FO}(\tau)$ such that for all model-defining $\mathbb{N}[X]$-interpretations $\pi_B : \mathrm{Lit}_B(\tau) \to \mathbb{N}$ that are bounded by $(c,n)$, $\pi_A [\![\psi_{(c,n)}]\!] = \pi_B [\![\psi_{(c,n)}]\!]$ implies $\pi_A \cong \pi_B$.

*Proof.* Observe that this statement is very similar to proposition (4.31). First of all, choose $C := c^{n^{|X|}}$ and invoke the previous lemma (4.34), which provides a homomorphism $h : \mathbb{N}[X] \to \mathbb{N}$ so that $h|_{\mathbb{N}[X](c,n)}$ is injective and $h(p) < C$ for all $p \in \mathbb{N}[X](c,n)$.

Construct the $\mathbb{N}$-interpretations $\pi'_A := h \circ \pi_A$ and $\pi'_B := h \circ \pi_B$. Since both $\pi_A$ and $\pi_B$ are bounded by $(c,n)$, that is $\pi_U(\mathrm{Lit}_U(\tau)) \subseteq \mathbb{N}[X](c,n)$ for $U \in \{A,B\}$, we have

$$\pi'_U(\mathrm{Lit}_U(\tau)) \subseteq h(\pi_U(\mathrm{Lit}_U(\tau))) \subseteq h(\mathbb{N}[X](c,n)) \subseteq [0,C)_{\mathbb{N}} \quad \text{for } U \in \{A,B\}.$$

Thus, both $\pi'_A$ and $\pi'_B$ are bounded by $C$. Moreover, $\pi'_A$ has a finite universe and is clearly still model-defining, since $h(p) = 0$ if and only if $p = 0$. Thus, we can invoke proposition (4.31) and define $\psi_{(c,n)} := \psi_C$ for $\pi'_A$ from proposition (4.31).

To show that this sentence has the required property, assume $\pi_A [\![\psi_C]\!] = \pi_B [\![\psi_C]\!]$ $(\star)$. With the fundamental property $(*)$, we have

$$\pi'_A [\![\psi_C]\!] = (h \circ \pi_A) [\![\psi_C]\!] \overset{*}{=} h(\pi_A [\![\psi_C]\!]) \overset{\star}{=} h(\pi_B [\![\psi_C]\!]) \overset{*}{=} (h \circ \pi_B) [\![\psi_C]\!] = \pi'_B [\![\psi_C]\!],$$

hence, due to the properties of $\psi_C$ described in proposition (4.31), we can conclude that $\pi'_A \cong \pi'_B$ and a corresponding isomorphism $\sigma : A \to B$ exists.

Since $\sigma$ is an isomorphism, for all literals $L \in \mathrm{Lit}_A(\tau)$, $\pi'_A(L) = \pi'_B(\sigma(L))$ holds, where $\sigma(L) \in \mathrm{Lit}_B(\tau)$ is defined straightforwardly by replacing any $a \in A$ that occurs in $L$ with $\sigma(a) \in B$. We claim that $\sigma : \pi_A \xrightarrow{\sim} \pi_B$ is even an isomorphism between $\pi_A$ and $\pi_B$.

Clearly, $\sigma$ is bijective. Assume for a contradiction that $\pi_A(L) \neq \pi_B(\sigma(L))$ for some literal $L \in \mathrm{Lit}_A(\tau)$. Since $\pi_A(L), \pi_B(\sigma(L)) \in \mathbb{N}[X](c,n)$ and $h$ is injective on $\mathbb{N}[X](c,n)$, this implies $h(\pi_A(L)) \neq h(\pi_B(\sigma(L)))$. By definition, $\pi'_A(L) = h(\pi_A(L))$ and $\pi'_B(\sigma(L)) = h(\pi_B(\sigma(L)))$, so we would obtain $\pi'_A(L) \neq \pi'_B(\sigma(L))$, a contradiction. This ends the proof. ☐

Intuitively, we have lifted the result that $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$ to $\mathbb{N}[X]$ by simply evaluating the polynomials in $\mathbb{N}$ with a suitable assignment so that each polynomial that occurs in the image of $\pi_A$ or $\pi_B$ can be identified by its result. We conclude the section with the corresponding theorem.

**(4.36) Theorem.** Let $\pi_A, \pi_B$ be two model-defining $\mathbb{N}[X]$-interpretations over finite universes with the same signature. Then, $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$. In particular, there is a countable set of sentences

$$\Phi_A := \{\psi_{(c,n)} \mid (c,n) \in \mathbb{N} \times \mathbb{N}, \pi_A \text{ is bounded by } (c,n)\}$$

such that $\pi_A \cong \pi_B$ if $\pi_A [\![\varphi]\!] = \pi_B [\![\varphi]\!]$ for all $\varphi \in \Phi_A$.

*Proof.* Construct $\Phi_A$ according to the above proposition (4.35). Clearly, since $\pi_A$ and $\pi_B$ are both defined over finite universes, there is a $(c,n) \in \mathbb{N} \times \mathbb{N}$ so that they are both bounded by $(c,n)$. Then, by proposition (4.35), $\psi_{(c,n)} \in \Phi_A$ already has the property that $\pi_A [\![\psi_{(c,n)}]\!] = \pi_B [\![\psi_{(c,n)}]\!]$ implies $\pi_A \cong \pi_B$. □

**(4.37) Corollary** (Equivalence on Free Semirings)**.** Let $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$ be model-defining $K$-interpretations over finite universes $A, B$. If the subsemiring

$$L := \langle \pi_A(\mathrm{Lit}_A(\tau)) \cup \pi_B(\mathrm{Lit}_B(\tau)) \rangle_K$$

generated by all values in the images of $\pi_A$ and $\pi_B$ is freely generated by a finite set $G = \{g_1, \dots, g_k\} \subseteq K$, then $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$.

*Proof sketch.* The proof is a simple reduction to $\mathbb{N}[X]$ with $X := \{x_1, \dots, x_k\}$. By theorem (3.8), the assignment $e : X \to G$ with $e(x_i) = g_i$ for $i \in \{1, \dots, k\}$ induces the homomorphism $h_e : \mathbb{N}[X] \to K$ with $h_e(\mathbb{N}[X]) = \langle e(X) \rangle_K = \langle G \rangle_K = L$. We can see $h_e$ as a surjective function $h_e : \mathbb{N}[X] \to L$. Moreover, since $L$ is freely generated by $G$, $h_e$ is injective according to lemma (3.10), therefore, it is an isomorphism and there is an inverse isomorphism $h : L \to \mathbb{N}[X]$.

Now, by the fundamental property, $\pi_A \equiv \pi_B$ implies $(h \circ \pi_A) \equiv (h \circ \pi_B)$. Since $h$ is injective, $h(a) = 0$ if and only if $a = 0$, hence the two $\mathbb{N}[X]$-interpretations $(h \circ \pi_A)$ and $(h \circ \pi_B)$ are model-defining and finite, which implies $(h \circ \pi_A) \cong (h \circ \pi_B)$ by the above theorem (4.36). This yields $\pi_A \cong \pi_B$ due to injectivity of $h$. We omit the formal argument, since it is similar to the proof of proposition (4.35). □

Corollary (4.37) appears to be a very strong result for general semirings, however, we have to keep in mind that due to lemma (3.10), a semiring $K$ that is freely generated by a finite set of generators is already isomorphic to $\mathbb{N}[X]$. Hence, for "most" semirings $K$, we cannot expect the values of $K$-interpretations to be freely generated. Therefore, it is still worth asking whether elementary equivalence implies isomorphism on more restricted semirings.

## 4.7 Absorptive Semirings

The first class of semirings that comes to mind is the class of absorptive semirings. As an introductory example, consider the absorptive polynomials with infinite exponents $\mathbb{S}^\infty[X]$. As mentioned before, this semiring is extensively used by in [GT19], [Naa19] and [DGNT19] thanks to the fact that it admits infinitary operations, which makes it suitable for semiring interpretations in logics that are stronger than FO, such as fixed-point logics, or semiring interpretations over infinite universes. For example, we have

$$\sum_{i=1}^{\infty} x^i = x \quad \text{and} \quad \prod_{i=1}^{\infty} x^i = x^\infty.$$

In fact, even infinite sums and products of polynomials in $\mathbb{S}^\infty[X]$ are finite, since only finitely many monomials can survive absorption, as observed by Grädel and Tannen, which means that the polynomials can be finitely represented without effort. [GT19]

However, we observe that $x^\infty \cdot x^\infty = x^\infty$ for all $x \in X$. Hence, if we use the set $X^\infty = \{x^\infty \mid x \in X\}$, the subsemiring of $\mathbb{S}^\infty[X]$ generated by $X^\infty$ is multiplicatively idempotent and the exponents are either 0 or $\infty$. In fact, $\langle X^\infty \rangle_{\mathbb{S}^\infty[X]}$ is isomorphic to PosBool$[X]$. Now, we can simply translate our PosBool$[X]$-interpretations $\pi_{xy}$ and $\pi_{yx}$ from before to $\langle X^\infty \rangle_{\mathbb{S}^\infty[X]}$ and obtain the two $\mathbb{S}^\infty[X]$-interpretations $\pi^\infty_{xy}, \pi^\infty_{yx}$ as follows.

$\pi_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 0 | $y$ | $x$ | 0 |
| b | $x$ | 0 | 0 | $y$ |
| c | $y$ | $x$ | 0 | 0 |
| d | 0 | 0 | $y$ | $x$ |

$\pi_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $y$ | 0 | 0 | $x$ |
| b | 0 | $x$ | $y$ | 0 |
| c | $x$ | $y$ | 0 | 0 |
| d | 0 | 0 | $x$ | $y$ |

translates to

$\pi^\infty_{xy}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 0 | $y^\infty$ | $x^\infty$ | 0 |
| b | $x^\infty$ | 0 | 0 | $y^\infty$ |
| c | $y^\infty$ | $x^\infty$ | 0 | 0 |
| d | 0 | 0 | $y^\infty$ | $x^\infty$ |

$\pi^\infty_{yx}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $y^\infty$ | 0 | 0 | $x^\infty$ |
| b | 0 | $x^\infty$ | $y^\infty$ | 0 |
| c | $x^\infty$ | $y^\infty$ | 0 | 0 |
| d | 0 | 0 | $x^\infty$ | $y^\infty$ |

Clearly, $\pi^\infty_{xy} \equiv \pi^\infty_{yx}$, but $\pi^\infty_{xy} \not\cong \pi^\infty_{yx}$, as stated in the following proposition.

**(4.38) Proposition.** For two $\mathbb{S}^\infty[X]$-interpretations $\pi_A, \pi_B$ over finite universes, $\pi_A \equiv \pi_B$ does not imply $\pi_A \cong \pi_B$. There is a counterexample over a universe with four elements and a signature with two unary relation symbols.

Unfortunately, this counterexample is not particularly useful for two reasons. First of all, since only elements of $\langle X^\infty \rangle_{\mathbb{S}^\infty[X]} \subsetneq \mathbb{S}^\infty[X]$ are used, most elements of $\mathbb{S}^\infty[X]$ do not "take part" in the counterexample, hence it does not provide much insight into $\mathbb{S}^\infty[X]$, but rather restates the result for PosBool$[X] \cong \langle X^\infty \rangle_{\mathbb{S}^\infty[X]}$.

Secondly, the use of elements in $X^\infty$ makes it difficult to translate this counterexample to other absorptive semirings. For example, one absorptive semiring that would allow infinitary operations is the Viterbi semiring $\mathbb{V}$. Since $\mathbb{S}^\infty[X]$ is, informally speaking, the "general" absorptive semiring with infinitary operations, we might expect at first glance that a counterexample in $\mathbb{S}^\infty[X]$ contradicts our previous result from theorem (4.23) that $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$ for finite $\mathbb{V}$-interpretations, because we could try to construct a counterexample in $\mathbb{V}$ from $\pi^\infty_{xy}$ and $\pi^\infty_{yx}$.

However, this is not the case. Surely, we could pick elements $r, s \in \mathbb{V}$ and the assignment $e : x \mapsto r, y \mapsto s$. For the sake of this argument, just assume that this would induce a "sensible" homomorphism $h_e^\infty : \mathbb{S}^\infty[X] \to \mathbb{V}$ that preserves infinitary operations. Now, construct two $\mathbb{V}$-interpretations as follows.

$h_e^\infty \circ \pi_{xy}^\infty$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 0 | $s^\infty$ | $r^\infty$ | 0 |
| b | $r^\infty$ | 0 | 0 | $s^\infty$ |
| c | $s^\infty$ | $r^\infty$ | 0 | 0 |
| d | 0 | 0 | $s^\infty$ | $r^\infty$ |

$h_e^\infty \circ \pi_{yx}^\infty$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | $s^\infty$ | 0 | 0 | $r^\infty$ |
| b | 0 | $r^\infty$ | $s^\infty$ | 0 |
| c | $r^\infty$ | $s^\infty$ | 0 | 0 |
| d | 0 | 0 | $r^\infty$ | $s^\infty$ |

Surely, $\pi_{xy}^\infty \equiv \pi_{yx}^\infty$ and an "infinitary" fundamental property would also imply that $(h_e^\infty \circ \pi_{xy}^\infty) \equiv (h_e^\infty \circ \pi_{yx}^\infty)$. Still, this is not a counterexample on $\mathbb{V}$, because in order for $(h_e^\infty \circ \pi_{xy}^\infty) \not\cong (h_e^\infty \circ \pi_{yx}^\infty)$ to hold, $\{0, r^\infty, s^\infty\}$ would have to be pairwise distinct, but on $\mathbb{V}$, the only "sensible" definition of infinitary exponentiation is

$$a^\infty = \begin{cases} 1 & \text{if } a = 1, \\ 0 & \text{otherwise} \end{cases} \qquad \text{for } a \in [0,1]_\mathbb{R}.$$

Hence, only one nonzero element $a^\infty$ exists and the argument fails, as it should.

This suggests that we should turn to $\mathbb{S}[X]$ for more insights on general absorptive semirings and leave out $X^\infty$, since these elements induce a multiplicatively idempotent subsemiring. Not knowing whether elementary equivalence implies isomorphism on $\mathbb{S}[X]$ or not, we could turn to the absorptive semiring $\mathbb{V}$ for inspiration and recall the $\varepsilon$-characteristic formulas from proposition (4.22). We managed to construct characteristic formulas for $\mathbb{V}$-interpretations by creating a conjunction of literals and repeating them for a varying number of times.

However, this approach relies heavily on the cancellation property of multiplication in $\mathbb{V}$. Intuitively speaking, cancellation makes sure that factors in a product do not "get lost". Unfortunately, $\mathbb{S}[X]$ does not admit cancellation, as shown by

$$\begin{aligned} (x^2+xy+y^2)\cdot(x+y) &= s(x^3+2x^2y+2xy^2+y^3) = x^3+x^2y+xy^2+y^3 \quad \text{and} \\ (x^2+y^2)\cdot(x+y) &= s(x^3+x^2y+xy^2+y^3) \quad = x^3+x^2y+xy^2+y^3, \end{aligned}$$

where $s$ denotes the "pruning" operator for absorption. We have

$$(x^2+xy+y^2)\cdot(x+y) = (x^2+y^2)\cdot(x+y), \quad \text{but} \quad (x^2+xy+y^2) \neq (x^2+y^2).$$

Informally, this is due to the fact that all contributions of $xy$ to the product are redundant.

In fact, we can immediately derive a counterexample for $\mathbb{S}[X]$ as follows. Define the $\mathbb{S}[X]$-interpretations $\pi_r : \mathrm{Lit}_A(\tau)$ and $\pi_m : \mathrm{Lit}_A(\tau)$ with $X := \{x, y\}$, $A := \{a, b\}$ and $\tau := \{R\}$ with one unary relation symbol as shown below.

$\pi_r$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | $x+y$ | 0 |
| b | $x^2+xy+y^2$ | 0 |

$\pi_m$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | $x+y$ | 0 |
| b | $x^2+y^2$ | 0 |

Clearly, $\pi_r \not\cong \pi_m$. The difficult part is to prove $\pi_r \equiv \pi_m$. To explain the idea of the proof, define

$$\begin{aligned} p_r &:= x^2+xy+y^2 && \text{with the redundant monomial } xy, \\ p_m &:= x^2+y^2 && \text{with no redundant monomials and} \\ q &:= x+y. \end{aligned}$$

As shown above, we have $p_r q = p_m q$, which inductively lifts to $p_r^i q^j = p_m^i q^j$, as long as $j > 0$. Now, if we interpret a sentence $\psi$, we informally obtain that $\pi_r [\![\psi]\!]$ is polynomial in $p_r$ and $q$ and $\pi_m [\![\psi]\!]$ is polynomial in $p_m$ and $q$. In fact, both should yield the same polynomial, except that $\pi_r$ uses $p_r$ and $\pi_m$ uses $p_m$. Since $p_r^i q^j = p_m^i q^j$ for $j > 0$, most monomials should have equal values.

In order to capture this idea formally, consider $\mathbb{N}[V]$ with the variables $V := \{v, w\}$ and the $\mathbb{N}[V]$-interpretation $\pi : \mathrm{Lit}_A(\tau) \to \mathbb{N}[V]$ given below.

$\pi$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | $v$ | 0 |
| b | $w$ | 0 |

The two assignments $e_r : v \mapsto q, w \mapsto p_r$ and $e_m : v \mapsto q, w \mapsto p_m$ induce homomorphisms $h_r, h_m : \mathbb{N}[V] \to \mathbb{S}[X]$ such that obviously,

$$h_r \circ \pi = \pi_r \quad \text{and} \quad h_m \circ \pi = \pi_m.$$

For any sentence $\psi \in \mathsf{FO}(\tau)$, we can use the fundamental property $(*)$ and obtain

$$\begin{aligned} \pi_r [\![\psi]\!] &= (h_r \circ \pi) [\![\psi]\!] \stackrel{*}{=} h_r(\pi [\![\psi]\!]) = h_r(p_\psi) \quad \text{and} \\ \pi_m [\![\psi]\!] &= (h_m \circ \pi) [\![\psi]\!] \stackrel{*}{=} h_m(\pi [\![\psi]\!]) = h_m(p_\psi), \end{aligned}$$

where $p_\psi := \pi [\![\psi]\!] \in \mathbb{N}[X]$ is a polynomial that is fixed for $\psi$. Intuitively, $\pi_r$ and $\pi_m$ are interpreted by evaluating the same polynomial with different variable assignments.

Since we wanted to show $\pi_r [\![\psi]\!] = \pi_m [\![\psi]\!]$, it only remains to show $h_r(p_\psi) = h_m(p_\psi)$. As hinted before, since multiplication absorbs the redundant monomial in $p_r$, we can throw away all monomials from $p_\psi$ where both variables $v$ and $w$ occur together. More formally let $n$ be a number so that all exponents in $p_\psi$ are less than $n$, then we can write $p_\psi$ as

$$p_\psi = \underbrace{\sum_{i=0}^{n-1} c_i^v \cdot v^i + \sum_{i=0}^{n-1} c_i^w \cdot w^i}_{=:q_\psi} + \sum_{(i,j)\in\{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot v^i w^j.$$

We will show that the important part is $q_\psi$, the remaining part of $p_\psi$ can be ignored, since we have

$$\begin{aligned} h_r(p_\psi) &= h_r(q_\psi) + \sum_{(i,j)\in\{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot^{\mathbb{N}} h_r(v)^i \cdot h_r(w)^j \\ &= h_r(q_\psi) + \sum_{(i,j)\in\{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot^{\mathbb{N}} q^i p_r^j \qquad \text{and} \\ h_m(p_\psi) &= h_m(q_\psi) + \sum_{(i,j)\in\{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot^{\mathbb{N}} h_m(v)^i \cdot h_m(w)^j \\ &= h_m(q_\psi) + \sum_{(i,j)\in\{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot^{\mathbb{N}} q^i p_m^j, \end{aligned}$$

But if $i, j > 0$, then $q^i p_r^j = q^i p_m^j$, as argued above, since a single factor $q$ can inductively annihilate the redundant monomial from $p_r^j$. Thus, it only remains to show that $h_r(q_\psi) = h_m(q_\psi)$ to complete the proof.

Unfortunately, this is the difficult part. The intuition is that, when looking at $\pi$, we see that $v$ and $w$ are interchangeable. Thus, they should be interchangeable in the polynomial $q_\psi$ as well, that is, $v^i$ and $w^i$ should have the same coefficient. Since $h_r$ and $h_m$ assign $q$ to $v$ and $q$ absorbs both $p_r$ and $q_r$, this would imply that the values of $w^i$ would be absorbed by the values of $v^i$. In order to prove this formally, we require the following lemma.

**(4.39) Lemma** (Variable Permutation Lemma)**.** Let $\sigma : X \to X$ be a permutation on a finite set, then, permuting the variables on polynomials in $\mathbb{N}[X]$ is an isomorphism.

*Proof.* By theorem (3.8), $\sigma$ induces a homomorphism $h_\sigma : \mathbb{N}[X] \to \mathbb{N}[X]$. Moreover, $h_\sigma(\mathbb{N}[X]) = \langle \sigma(X) \rangle_{\mathbb{N}[X]} = \langle X \rangle_{\mathbb{N}[X]} = \mathbb{N}[X]$, and since $\mathbb{N}[X]$ is freely generated by $X$, $h_\sigma$ is also injective by lemma (3.10).

Now, according to the definition of $h_\sigma$ from theorem (3.8),

$$h_\sigma(p) = \sum_{m \in \mathrm{supp}(p)} p(m) \cdot \prod_{x \in X} \sigma(x)^{m(x)}$$

for all $p \in \mathbb{N}[X]$, hence $h_\sigma$ indeed permutes the variables on all monomials with $\sigma$. □

Now, consider $h_{v\leftrightarrow w} : \mathbb{N}[V] \to \mathbb{N}[V]$, the isomorphism induced by swapping $v$ and $w$. If we apply it to the above $\mathbb{N}[V]$-interpretation $\pi$, we obtain

$\pi$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | $v$ | 0 |
| b | $w$ | 0 |

$h_{v\leftrightarrow w} \circ \pi$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | $w$ | 0 |
| b | $v$ | 0 |

Obviously, $\pi \cong (h_{v\leftrightarrow w} \circ \pi)$ with the isomorphism $\rho : a \mapsto b, b \mapsto a$. Hence, for all $\psi \in \mathsf{FO}(\tau)$, we have

$$\pi [\![\psi]\!] = (h_{v\leftrightarrow w} \circ \pi) [\![\psi]\!] \overset{*}{=} h_{v\leftrightarrow w}(\pi [\![\psi]\!])$$

with the fundamental property $(*)$. In particular, $p_\psi = h_{v\leftrightarrow w}(p_\psi)$ for the polynomial $p_\psi$ from above. Recall that

$$p_\psi = \underbrace{\sum_{i=0}^{n-1} c_i^v \cdot v^i + \sum_{i=0}^{n-1} c_i^w \cdot w^i}_{=: q_\psi} + \sum_{(i,j) \in \{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot v^i w^j,$$

so by applying the permutation $h_{v\leftrightarrow w}$, we obtain

$$\begin{aligned} h_{v\leftrightarrow w}(p_\psi) &= h_{v\leftrightarrow w} \left( \sum_{i=0}^{n-1} c_i^v \cdot v^i + \sum_{i=0}^{n-1} c_i^w \cdot w^i + \sum_{(i,j) \in \{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot v^i w^j \right) \\ &= \sum_{i=0}^{n-1} c_i^v \cdot h_{v\leftrightarrow w}(v)^i + \sum_{i=0}^{n-1} c_i^w \cdot h_{v\leftrightarrow w}(w)^i + \sum_{(i,j) \in \{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot h_{v\leftrightarrow w}(v^i w^j) \\ &= \sum_{i=0}^{n-1} c_i^v \cdot w^i + \sum_{i=0}^{n-1} c_i^w \cdot v^i + \sum_{(i,j) \in \{1,\dots,n-1\}^2} c_{ij}^{vw} \cdot w^i v^j. \end{aligned}$$

We are mainly interested in $q_\psi$, thus, by comparing coefficients of $p_\psi$ and $h_{v\leftrightarrow w}(p_\psi)$, we obtain $c_i^v = c_i^w =: c_i$ for all $0 \leq i < n$. Therefore,

$$q_\psi = \sum_{i=0}^{n-1} c_i(v^i + w^i).$$

With this insight, we are ready to prove $h_r(q_\psi) = h_m(q_\psi)$, which was the last missing step to show $\pi_r \equiv \pi_m$. This is done by calculating

$$\begin{aligned}
h_r(q_\psi) &= \sum_{i=0}^{n-1} c_i \cdot^{\mathbb{N}} (h_r(v)^i + h_r(w)^i) \\
&= \sum_{i=0}^{n-1} c_i \cdot^{\mathbb{N}} (q^i + p_r^i) \\
&\overset{\star}{=} \sum_{i=0}^{n-1} c_i \cdot^{\mathbb{N}} q^i \quad \text{and similarly} \\
h_m(q_\psi) &= \sum_{i=0}^{n-1} c_i \cdot^{\mathbb{N}} (h_m(v)^i + h_m(w)^i) \\
&= \sum_{i=0}^{n-1} c_i \cdot^{\mathbb{N}} (q^i + p_m^i) \\
&\overset{\star}{=} \sum_{i=0}^{n-1} c_i \cdot^{\mathbb{N}} q^i.
\end{aligned}$$

The steps ($\star$) use the fact that $q = (x + y)$ absorbs both $p_r = (x^2 + xy + y^2)$ and $p_m = (x^2 + y^2)$. Of course, this implies that $q^i \geq p_r^i, p_m^i$ as well due to monotonicity of multiplication.

This ends the proof for $\pi_r \equiv \pi_m$, and with $\pi_r \not\cong \pi_m$, we have constructed a counterexample in $\mathbb{S}[X]$. Notice that instead of $p_r$, $p_m$ and $q$, we could have used other polynomials as well, the only properties that we used in the proof are

$$\begin{aligned}
&(1) \quad q \geq p_r, p_m, \\
&(2) \quad qp_r = qp_m \quad \text{and} \\
&(3) \quad p_r \neq p_m.
\end{aligned}$$

This yields the following theorem.

**(4.40) Theorem.** In $\mathbb{S}[X]$, $\pi_A \equiv \pi_B$ does not imply $\pi_A \cong \pi_B$ for all finite $\mathbb{S}[X]$-interpretations $\pi_A, \pi_B$ over the same signature. There is a counterexample over a universe with two elements and a signature with one unary relation.

In particular, for any $p_1, p_2, q \in \mathbb{S}[X]$ with $q \geq p_1, p_2$ such that $q$ does not cancel over $p_1$ and $p_2$, that is

$$qp_1 = qp_2, \quad \text{but} \quad p_1 \neq p_2,$$

the following two $\mathbb{S}[X]$-interpretations $\pi_1 : \mathrm{Lit}_A(\tau) \to \mathbb{S}[X], \pi_2 : \mathrm{Lit}_B(\tau) \to \mathbb{S}[X]$ over $A = \{a, b\}$ and $\tau = \{R\}$ defined as

$\pi_1$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | $q$ | 0 |
| b | $p_1$ | 0 |

$\pi_2$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | $q$ | 0 |
| b | $p_2$ | 0 |

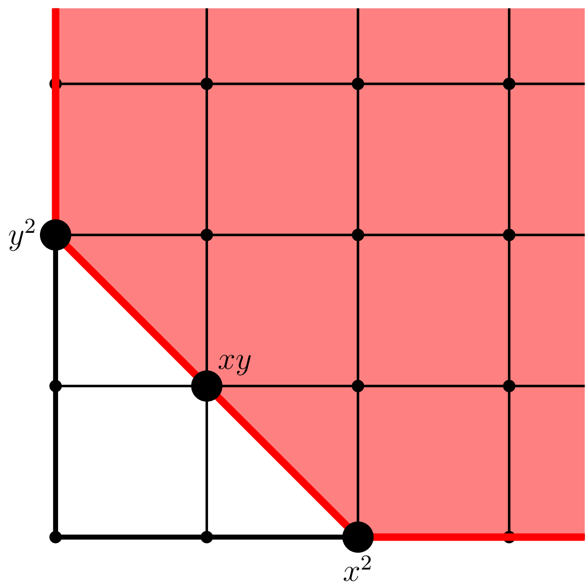
are elementarily equivalent, but not isomorphic.

**(4.41) Remark** (Choice of $p_1$, $p_2$ and $q$)**.** The above theorem yields an entire set of counterexamples for $\mathbb{S}[X]$. This raises the question of how to find $p_1$, $p_2$ and $q$ that satisfy the conditions from the theorem and yield a valid counterexample.

We believe that such a counterexample can be constructed from any absorptive polynomial $p_o \in \mathbb{S}[X]$ that contains an "obscured" monomial $m$. Recall that monomials in $\mathbb{S}[X]$ are functions $m : X \to \mathbb{N}$, which we can see as vectors of exponents $m \in \mathbb{N}^k$ for $k = |X|$. A monomial $m$ in a polynomial $p \in \mathbb{S}[X]$ is called *obscured* if there is no positive direction $c \in \mathbb{R}^k_{\geq 0} \setminus \{0\}$ such that the exponents of $m$ are uniquely minimal in that direction, that is,

$$c^T \cdot m < c^T \cdot m' \quad \text{for all } m' \in p \setminus \{m\},$$

where $\cdot$ denotes the dot product on $\mathbb{R}^k$. While this definition may be surprising, note that we used the polynomial $p_r = x^2 + xy + y^2$ in the proof above. The monomials of $p_r$ can be represented graphically as follows.



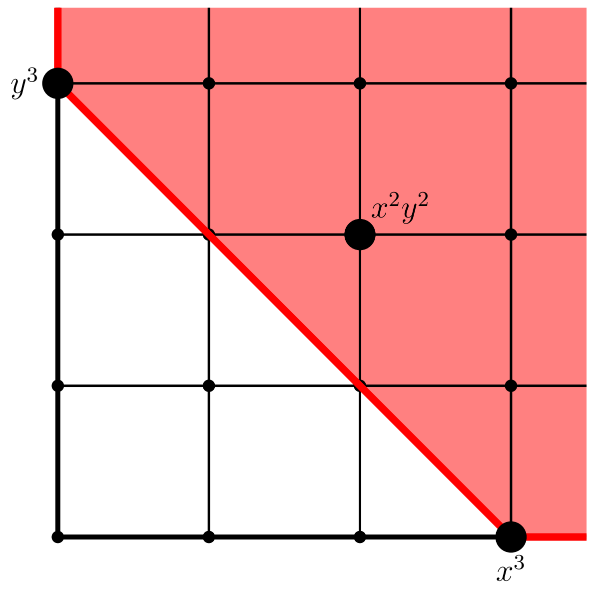

Obviously, the monomial $x^2$ is minimal in $y$-direction $c_y = (0, 1)$ and $y^2$ is minimal in $x$-direction $c_x = (1, 0)$, but crucially, $xy$ is not uniquely minimal in any direction, hence it is obscured. In fact, all monomials in the highlighted area, including the edges but excluding the nodes, are obscured, while $xy$ is the only one of them that is not absorbed by $x^2$ or $y^2$. Note that this graphical representation is similar to solution spaces of linear programs.

Recall that we used $p_m = x^2 + y^2$ in the proof before, which corresponds to $p_r$ without the obscured monomial $xy$. This means that our counterexample was constructed by taking a polynomial with an obscured monomial and removing it. More formally, we believe that for any $p_o \in \mathbb{S}[X]$ with at least one obscured monomial, we can simply prune the obscured monomials by setting

$$p_p \coloneqq \{m \in p_o \mid m \text{ is not obscured}\}$$

and then find a $q$ with $q \geq p_o, p_p$ and $qp_o = qp_p$, which delivers a counterexample, since $p_o \neq p_p$ surely holds due to the removal of the obscured monomials.

This assumption is reaffirmed by constructing many examples. We will present one more example here, that is $p_o \coloneqq x^3 + x^2y^2 + y^3$, where the monomial $x^2y^2$ is obscured as depicted in the following picture.




The corresponding pruned polynomial is $p_p = x^3 + y^3$. Sure enough, if we pick $q = x + y$ as before, we have

$$\begin{aligned} q \cdot p_o &= (x+y)(x^3 + x^2y^2 + y^3) \\ &= s(x^4 + x^3y^2 + xy^3 + x^3y + x^2y^3 + y^4) \\ &= x^4 + xy^3 + x^3y + y^4 \\ &= (x+y)(x^3 + y^3) \\ &= q \cdot p_p, \end{aligned}$$

thus, a counterexample can be constructed using $p_o, p_p$ and $q$, since $q \geq p_o, p_p$ holds as well.

We even believe that the condition of obscured monomials may be necessary for the construction of a counterexample and absorptive semirings $K$ that "do not admit obscured elements" allow the construction of characteristic sentences and therefore do not admit a counterexample. Formally, a semiring $K$ does not admit obscured elements if for any $p_o \in \mathbb{S}[X]$ and the corresponding pruned polynomial $p_p \in \mathbb{S}[X]$, the induced homomorphism $h_e : \mathbb{S}[X] \to K$ by any assignment $e : X \to K$ has the property that $h_e(p_o) = h_e(p_p)$, in other words, the obscured monomials from $p_o$ do not matter in $K$.

In fact, the Viterbi semiring is a good example of an absorptive semiring where obscured monomials do not matter. If we choose $r, s \in \mathbb{V}$ arbitrarily and assign $x \mapsto r$, $y \mapsto s$, the value of $p_r = x^2 + xy + y^2$ is $r^2$ if $r \geq s$ and $s^2$ if $r \leq s$, hence the obscured monomial $xy$ is not used in any case. A similar observation can be made for $p_o = x^3 + x^2y^2 + y^3$.

In conclusion, the question remains open for which absorptive semirings the counterexamples from theorem (4.40) can be lifted, however, it is clear that they are valid for the free absorptive semiring $\mathbb{S}[X]$ itself, but not applicable to some absorptive semirings, such as $\mathbb{V}$.

## 4.8 Summary

Unfortunately, the central question of this chapter still remains open, that is, we do not have an exact characterization of the semirings $K$ where $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$ for finite $K$-interpretations $\pi_A$ and $\pi_B$. However, we have encountered a useful proof technique for elementary equivalence on $K$, namely the reduction theorem, which allows us to reduce elementary equivalence on $K$ to elementary equivalence on a different semiring. This was used, for example, in our first counterexample on the four-element min-max-semiring $K_3$. Moreover, we have refined the characteristic sentences from classical model theory to show that elementary equivalence does imply isomorphism on finite $K$-interpretations for some semirings, such as $\mathbb{V}$ or $\mathbb{N}$.

More importantly, we observed that polynomial semirings may provide insight into an entire class of semirings, as was successfully demonstrated on $\mathrm{PosBool}[X]$, which allowed us to construct a counterexample on all lattice semirings except for the two-element semiring $\mathbb{B}$ itself. Also, a counterexample on $\mathbb{S}[X]$ exists, but it is not easily lifted to all absorptive semirings.

In the future, we may clarify the situation for absorptive semirings and look to other polynomial semirings such as $\mathbb{B}[X]$ and $\mathbb{W}[X]$ in an effort to find counterexamples for other interesting classes of semirings or prove that they do not exist. However, in the next chapter, we will approach model theory for semiring semantics from a different perspective.

# Chapter 5

# Two-Sorted Approach

Instead of accepting the limitations of first-order logic "as-is" and attempting to prove or disprove classical theorems under semiring semantics, we may also extend the syntax of first-order logic to provide more expressive power. As a motivating example, recall the following two $K_3$-interpretations from the previous chapter.

$\pi_1$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 1 | 0 |
| c | 3 | 0 |

$\pi_2$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 2 | 0 |
| c | 3 | 0 |

The most obvious issue is that first-order logic lacks the power to "pick out" the value 2 in $\pi_2$, in other words, there is no obvious way to distinguish the two interpretations with one quantifier as in the hypothetical formula "$\exists x(Rx = 2)$", which is obviously not syntactically correct.

However, we can remedy this by making it syntactically correct. All that is required are constants for semiring elements and a new equality operator that allows the comparison of those constants to formulas as shown above.

**(5.1) Definition** (Syntax and Semantics of Two-Sorted $\mathsf{FO}$)**.** The syntax and semantics of $\mathsf{FO}(K, \tau)$ are the same as the syntax and semantics of $\mathsf{FO}(\tau)$ provided in definition (2.3) and definition (2.4) with the following extension to the formula building rules.

For each $a \in K$ and each literal $\varphi \in \mathsf{FO}(K, \tau)$, there is a formula $(\varphi \overset{K}{=} a) \in \mathsf{FO}(K, \tau)$ with the semantics

$$\pi \left[\!\left[\varphi \overset{K}{=} a\right]\!\right]^{\beta} = \begin{cases} 1 & \text{if } \pi \left[\!\left[\varphi\right]\!\right]^{\beta} = a, \\ 0 & \text{otherwise} \end{cases}$$

for all $K$-interpretations $\pi$ and suitable variable assignments $\beta$.

The formula $(\varphi \overset{K}{=} a) \in \mathsf{FO}(K, \tau)$ is considered to be atomic, hence, in negation normal form, the corresponding negated formula is $\neg(\varphi \overset{K}{=} a) \in \mathsf{FO}(K, \tau)$, which is interpreted as

$$\pi \left[\!\left[\neg\varphi \overset{K}{=} a\right]\!\right]^{\beta} = \begin{cases} 1 & \text{if } \pi \left[\!\left[\varphi\right]\!\right]^{\beta} \neq a, \\ 0 & \text{otherwise} \end{cases}$$

We may write $\varphi = a$ and $\varphi \neq a$ for the new equality operator and its negation respectively if there is no risk of confusion with the usual equality operator in $\mathsf{FO}(\tau)$. Notice that the syntax of $\mathsf{FO}(K, \tau)$ now depends on the semiring $K$ where the formulas are interpreted.

The reason why we informally call this extended logic $\mathsf{FO}(K, \tau)$ "two-sorted $\mathsf{FO}$" is its similarity to Grädel and Gurevich's logics on metafinite structures. Metafinite structures essentially consist of a primary, finite structure $\mathfrak{A}$ in the usual sense and a secondary structure, for example $\mathbb{R}$, whose elements serve as weights for tuples in $\mathfrak{A}$. Indeed, looking at our definition of $\mathsf{FO}(K, \tau)$, we may view it as an extension of the $K$-interpretation $\pi$ with the secondary structure $K$ and constants for each $a \in K$ as well as the ability to compare the interpretations $\pi [\![\varphi]\!]^\beta$ of literals to those constants. Note that there are formal differences to metafinite structures, since $\pi$ need not be finite and formulas are still interpreted in $K$ rather than in $\mathbb{B}$, but the intuition of describing $\mathsf{FO}(K, \tau)$ as two-sorted $\mathsf{FO}$ is still justified. [GG98]

Now, the formula $\exists x(Rx = 2)$ becomes syntactically correct on $K_3$ and indeed separates the two $K_3$-interpretations $\pi_1$ and $\pi_2$ from the motivating example. However, $\mathsf{FO}(K, \tau)$ opens up even more possibilities.

## 5.1 Ehrenfeucht-Fraïssé Theorem

The Ehrenfeucht-Fraïssé theorem is a powerful tool from classical model theory that characterizes elementary equivalence. In fact, it even characterizes $m$-equivalence $\equiv_m$ for bounded quantifier ranks by relating it to other concepts, such as back-and-forth systems and Ehrenfeucht-Fraïssé games, which we will present in this chapter. An overview on the classical Ehrenfeucht-Fraïssé theorem was given by Thomas in 1993 [Tho93]. Our goal is to translate this to $K$-interpretations.

**(5.2) Theorem** (Classical Ehrenfeucht-Fraïssé Theorem)**.** For a finite, relational signature $\tau$ and two $\tau$-structures $\mathfrak{A} = (A, \tau)$ and $\mathfrak{B} = (B, \tau)$ with fixed $k$-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$, the following statements are equivalent.

(1) $\mathfrak{A}, \overline{a} \equiv_m \mathfrak{B}, \overline{b}$

(2) $\mathfrak{A}, \overline{a} \cong_m \mathfrak{B}, \overline{b}$

(3) $\mathfrak{B} \models \chi^m_{\mathfrak{A},\overline{a}}(\overline{b})$

(4) Duplicator wins $G_m(\mathfrak{A}, \overline{a}, \mathfrak{B}, \overline{b})$

The symbol $\equiv_m$ denotes *m-equivalence*, while $\cong_m$ stands for *m-isomorphism*, a concept related to *back-and-forth systems*, $\chi^m_{\mathfrak{A},\overline{a}}(\overline{x})$ is the *m-characteristic formula* for $\mathfrak{A}, \overline{a}$ and $G_m(\mathfrak{A}, \overline{a}, \mathfrak{B}, \overline{b})$ denotes the *Ehrenfeucht-Fraïssé game* between the *Spoiler* and the *Duplicator* on $\mathfrak{A}, \overline{a}$ and $\mathfrak{B}, \overline{b}$ for $m$ turns.

Apart from $m$-equivalence for formulas with bounded quantifiers, which was straightforwardly adapted to $K$-interpretations in definition (4.3), we have not introduced any of the concepts from the theorem yet. In the following, we will refer to [Tho93] to introduce the remaining concepts and simultaneously try to adapt them to $K$-interpretations.

We will start with the $m$-characteristic formulas $\chi^m_{\mathfrak{A},\overline{a}}(\overline{x})$, since we have already seen some adaptations of characteristic sentences to semiring semantics in the previous chapter. However, while the construction of characteristic sentences in the previous chapter was usually very difficult compared to the classical characteristic sentences, $\mathsf{FO}(K,\tau)$ makes it very easy.

As an example for this, observe that the question if $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$ for finite $K$-interpretations is trivial in $\mathsf{FO}(K,\tau)$ for positive semirings $K$. For any finite $\pi_A : \mathrm{Lit}_A(\tau) \to K$ with $A = \{a_1,\dots,a_n\}$, we can simply adapt the characteristic sentence

$$\chi \coloneqq \exists x_1 \dots \exists x_n \left( \bigwedge_{1\le i<j\le n} x_i \neq x_j \wedge \forall y \left( \bigvee_{1\le i\le n} y = x_i \right) \wedge \bigwedge_{L\in \mathrm{Lit}_A(\tau)} L[\overline{a}/\overline{x}] \overset{K}{=} \pi_A(L) \right),$$

which clearly describes $\pi_A$ up to isomorphism thanks to the new equality operator, hence $\pi_A \equiv \pi_B$ implies $\pi_A \cong \pi_B$. Note that this characteristic sentence behaves almost like a classical formula, since the interpretations of all its atomic subformulas are either 0 or 1, hence a non-classical value can only be obtained in $K$ if $1+1\neq 1$.

Contrary to characteristic sentences, which describe a structure or $K$-interpretation completely, $m$-characteristic formulas $\chi^m_{\mathfrak{A},\overline{a}}(\overline{x})$ are intended to describe the structure $\mathfrak{A} = (A,\tau)$ with the designated tuple $\overline{a}$ only "up to quantifier rank $m$". Thus, they are inductively defined in [Tho93] as follows.

$$\chi^0_{\mathfrak{A},\overline{a}}(\overline{x}) \coloneqq \bigwedge\{\varphi(\overline{x}) \mid \varphi(\overline{x}) \in \mathsf{FO}(\tau) \text{ is a literal and } \mathfrak{A} \models \varphi(\overline{a})\} \qquad \text{and}$$
$$\chi^{m+1}_{\mathfrak{A},\overline{a}}(\overline{x}) \coloneqq \bigwedge_{a\in A} \exists x \chi^m_{\mathfrak{A},\overline{a},a}(\overline{x},x) \wedge \forall x \bigvee_{a\in A} \chi^m_{\mathfrak{A},\overline{a},a}(\overline{x},x) \qquad \text{for } m\in\mathbb{N}.$$

For the case $m = 0$, it is immediately clear why this characteristic formula works as intended. If $\mathfrak{B} \models \chi^0_{\mathfrak{A},\overline{a}}(\overline{b})$, then $\mathfrak{B},\overline{b}$ coincides on $\mathfrak{A},\overline{a}$ on all literals, that is, atomic formulas or negated atoms using variables from $\overline{x}$. Thus, no formula without quantifiers can separate $\mathfrak{A},\overline{a}$ from $\mathfrak{B},\overline{b}$. Before we continue with the argument, observe that we can straightforwardly translate this to $\mathsf{FO}(K,\tau)$.

**(5.3) Definition** ($m$-characteristic sentence)**.** Let $\pi_A : \mathrm{Lit}_A(\tau) \to K$ be a $K$-interpretation and $\overline{a} \in A^k$, then the $m$-characteristic sentence $\chi^m_{\pi_A,\overline{a}}(\overline{x}) \in \mathsf{FO}(K,\tau)$ is defined inductively by

$$\chi^0_{\pi_A,\overline{a}}(\overline{x}) \coloneqq \bigwedge\{\varphi(\overline{x}) \overset{K}{=} c \mid \varphi(\overline{x}) \in \mathsf{FO}(\tau) \text{ is a literal and } \pi_A[\![\varphi(\overline{a})]\!] = c\} \qquad \text{and}$$
$$\chi^{m+1}_{\pi_A,\overline{a}}(\overline{x}) \coloneqq \bigwedge_{a\in A} \exists x \chi^m_{\pi_A,\overline{a},a}(\overline{x},x) \wedge \forall x \bigvee_{a\in A} \chi^m_{\pi_A,\overline{a},a}(\overline{x},x) \qquad \text{for } m\in\mathbb{N},$$

provided that $\tau$ is relational and finite and either $A$ or $K$ is finite.

Clearly, $\chi^0_{\pi_A,\overline{a}}(\overline{x})$ works exactly like the corresponding classical formula $\chi^0_{\mathfrak{A},\overline{a}}(\overline{x})$. Also, it is well-defined thanks to the new operator of $\mathsf{FO}(K,\tau)$ and the fact that there are only finitely many distinct literals $\varphi(\overline{x})$ over $\overline{x}$. However, the conjunctions and disjunctions over all $a \in A$ in the recursive part $\chi^{m+1}_{\pi_A,\overline{a}}(\overline{x})$ may cause a problem with the finiteness of the formula, which is why we assume that $A$ or $K$ is finite. If $A$ is finite, then there is obviously no problem. If $K$ is finite, then, much like in the classical case, we can observe that for each $m \in \mathbb{N}$, there are only finitely many possible characteristic formulas $\chi^m_{\pi_A,\overline{a}}(\overline{x})$, only depending on $m$, $\tau$, the size of the tuple $\overline{a}$ and the size of the semiring $|K|$, hence the formula $\chi^{m+1}_{\pi_A,\overline{a}}(\overline{x})$ is well-defined even if $A$ is infinite, provided that we skip repetitions in conjunctions and disjunctions over $a \in A$. Unfortunately, this is clearly not the case if both $K$ and $A$ are infinite, so we implicitly assume that one of them is finite in the following.

Now, it only remains to prove that the inductively constructed formulas $\chi^{m+1}_{\pi_A,\overline{a}}(\overline{x})$ actually fulfill their purpose, which is characterizing $\pi_A, \overline{a}$ up to quantifier rank $m+1$. This is done by introducing more concepts from the Ehrenfeucht-Fraïssé theorem.

## 5.2 Back-and-Forth Systems

Recall that $\mathfrak{B} \models \chi^0_{\mathfrak{A},\overline{a}}(\overline{b})$ implies that $\overline{a}$ satisfies the same literals in $\mathfrak{A}$ as $\overline{b}$ does in $\mathfrak{B}$. We can formalize this by saying that $\sigma : \overline{a} \mapsto \overline{b}$ is a "local isomorphism" between $\mathfrak{A}$ and $\mathfrak{B}$, meaning that it is an isomorphism between $\mathfrak{A}$ and $\mathfrak{B}$ if we only consider the substructure induced by the domain $\overline{a}$ of $\sigma$ in $\mathfrak{A}$ and the substructure induced by the image $\overline{b}$ of $\sigma$ in $\mathfrak{B}$. Of course, this definition easily lifts to $K$-interpretations.

**(5.4) Definition** (Local Isomorphism)**.** For two $K$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$, a partial function $\sigma : A \to B$ is a *local isomorphism* if it is an isomorphism between $\pi_A|_{\mathrm{Lit}_{\mathrm{dom}(\sigma)}(\tau)}$ and $\pi_B|_{\mathrm{Lit}_{\mathrm{img}(\sigma)}(\tau)}$. In other words, $\sigma$ must be injective so that it is a bijection between $\mathrm{dom}(\sigma)$ and $\mathrm{img}(\sigma)$ and preserve the values of all the literals between $\pi_A$ and $\pi_B$, provided that it is actually defined for the elements occurring in those literals.

Clearly, if $\sigma : \overline{a} \mapsto \overline{b}$ is a local isomorphism, then $\pi_A [\![\varphi(\overline{a})]\!] = \pi_B [\![\varphi(\overline{b})]\!]$ on all formulas $\varphi(\overline{x})$ without quantifiers, since formulas without quantifiers are only constructed from literals over $\overline{x}$, but $\pi_A$ and $\pi_B$ coincide on those literals if we assign $\overline{a}$ to $\overline{x}$ for $\pi_A$ and $\overline{b}$ to $\overline{x}$ for $\pi_B$.

Before introducing quantifiers, we draw inspiration from the inductive parts of the $m$-characteristic formulas, that is,

$$\chi^{m+1}_{\mathfrak{A},\overline{a}}(\overline{x}) \coloneqq \bigwedge_{a\in A} \exists x \chi^{m}_{\mathfrak{A},\overline{a},a}(\overline{x},x) \wedge \forall x \bigvee_{a\in A} \chi^{m}_{\mathfrak{A},\overline{a},a}(\overline{x},x) \qquad \text{and}$$
$$\chi^{m+1}_{\pi_A,\overline{a}}(\overline{x}) \coloneqq \bigwedge_{a\in A} \exists x \chi^{m}_{\pi_A,\overline{a},a}(\overline{x},x) \wedge \forall x \bigvee_{a\in A} \chi^{m}_{\pi_A,\overline{a},a}(\overline{x},x)$$

for $m \in \mathbb{N}$. Notice that both are very similar and if we look at the classical formula $\chi^1_{\mathfrak{A},\overline{a}}(\overline{x})$, then $\mathfrak{B} \models \chi^1_{\mathfrak{A},\overline{a}}(\overline{b})$ basically states that for each $a \in A$ there is a $b \in B$ (the element assigned to $x$) so that $\mathfrak{B} \models \chi^0_{\mathfrak{A},\overline{a},a}(\overline{b}, b)$ and for each $b \in B$, there is an $a \in A$ with this property. In other words, $\overline{a} \mapsto \overline{b}$ can be extended to a local isomorphism $\overline{a}, a \mapsto \overline{b}, b$ in either "direction", that is, we may choose $a$ or $b$ first. This concept is formally captured by "back-and-forth systems" in [Tho93] for the classical case, and we will straightforwardly adapt it to semiring interpretations.

**(5.5) Definition** (Back-and-Forth System)**.** Consider any two $K$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$. Denote the set of local isomorphisms between $\pi_A$ and $\pi_B$ as $\mathrm{Loc}(\pi_A, \pi_B)$. We say that a local isomorphism $\sigma \in \mathrm{Loc}(\pi_A, \pi_B)$ satisfies the *back-and-forth property* (BFP) with respect to a set of local isomorphisms

$I \subseteq \mathrm{Loc}(\pi_A, \pi_B)$ if it satisfies the two conditions that

(forth) for all $a \in A$, there is an element $b \in B$ such that $\sigma \cup \{(a,b)\} \in I$ and
(back) for all $b \in B$, there is an element $a \in A$ such that $\sigma \cup \{(a,b)\} \in I$,

where $\sigma \cup \{(a,b)\}$ denotes the partial function $\sigma$ extended by the assignment $a \mapsto b$.

Consequently, the *back-and-forth system* $(I_m(\pi_A, \pi_B))_{m\in\mathbb{N}}$ between $\pi_A$ and $\pi_B$ is defined inductively by

$$\begin{aligned} I_0(\pi_A, \pi_B) &\coloneqq \mathrm{Loc}(\pi_A, \pi_B) \qquad \text{and} \\ I_{m+1}(\pi_A, \pi_B) &\coloneqq \{\sigma \in \mathrm{Loc}(\pi_A, \pi_B) \mid \sigma \text{ satisfies the BFP w.r.t. } I_m\} \quad \text{for } m \in \mathbb{N}. \end{aligned}$$

Given some $k$-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$, we say that $\pi_A, \overline{a}$ and $\pi_B, \overline{b}$ are *m-isomorphic*, denoted as $\pi_A, \overline{a} \cong_m \pi_B, \overline{b}$, if $\overline{a} \mapsto \overline{b} \in I_m(\pi_A, \pi_B)$. In other words, the mapping $\sigma : \overline{a} \mapsto \overline{b}$ must be a local isomorphism and it must be possible to extend it at least $m$ times via the back-and-forth property.

Note that the only difference between our definition of back-and-forth systems and the classical definition is the fact that we use local isomorphisms between $K$-interpretations, as defined in definition (5.4), instead of local isomorphisms between classical structures $\mathfrak{A}, \mathfrak{B}$. Now, we are finally able to explain the meaning of the inductive definition of $\chi^{m+1}_{\pi_A,\overline{a}}(\overline{x})$, which essentially captures the back-and-forth property, as formalized by the following lemma.

**(5.6) Lemma** (Back-and-Forth Lemma)**.** Let $K$ be a positive semiring. For two $K$-interpretations $\pi_A : \mathrm{Lit}_A(\tau) \to K$ and $\pi_B : \mathrm{Lit}_B(\tau) \to K$,

$$\pi_B \left[\!\left[\chi^m_{\pi_A,\overline{a}}(\overline{b})\right]\!\right] \neq 0 \quad \text{if and only if} \quad \pi_A, \overline{a} \cong_m \pi_B, \overline{b}$$

holds for all $k$-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$.

*Proof.* We will prove the claim by induction on $m$, and the base case $m = 0$ was already explained above. More formally, we observe that $\pi_B \left[\!\left[\chi^0_{\pi_A,\overline{a}}(\overline{b})\right]\!\right] \in \{0,1\}$ thanks to the construction of $\chi^0_{\pi_A,\overline{a}}(\overline{x})$ as a conjunction of equality formulas that only yield the values 0 or 1. It is also clear that $\pi_B \left[\!\left[\chi^0_{\pi_A,\overline{a}}(\overline{b})\right]\!\right] = 1$ if and only if the mapping $\overline{a} \mapsto \overline{b}$ respects all literals, that is $\overline{a} \mapsto \overline{b} \in \mathrm{Loc}(\pi_A, \pi_B) = I_0(\pi_A, \pi_B)$, which shows $\pi_A, \overline{a} \cong_0 \pi_B, \overline{b}$.

For the induction step, consider the formula $\chi^{m+1}_{\pi_A,\overline{a}}(\overline{x})$ and assume the claim was already shown for $i \leq m$. Thanks to the assumption that $K$ is positive, we know that the mapping $\dagger_K : K \to \mathbb{B}$ that maps zero to false and nonzero values to true is a semiring homomorphism. Also, $\pi_B \left[\!\left[\chi^{m+1}_{\pi_A,\overline{a}}(\overline{b})\right]\!\right] \neq 0$ is equivalent to $\dagger_K \left(\pi_B \left[\!\left[\chi^{m+1}_{\pi_A,\overline{a}}(\overline{b})\right]\!\right]\right) = \top$. We compute the value

$$\begin{aligned} \dagger_K \left(\pi_B \left[\!\left[\chi^{m+1}_{\pi_A,\overline{a}}(\overline{b})\right]\!\right]\right) &= \dagger_K \left(\pi_B \left[\!\left[\bigwedge_{a\in A} \exists x \chi^m_{\pi_A,\overline{a},a}(\overline{b}, x) \wedge \forall x \bigvee_{a\in A} \chi^m_{\pi_A,\overline{a},a}(\overline{b}, x)\right]\!\right]\right) \\ &= \dagger_K \left(\prod_{a\in A} \sum_{b\in B} \pi_B \left[\!\left[\chi^m_{\pi_A,\overline{a},a}(\overline{b}, b)\right]\!\right] \cdot \prod_{b\in B} \sum_{a\in A} \pi_B \left[\!\left[\chi^m_{\pi_A,\overline{a},a}(\overline{b}, b)\right]\!\right]\right) \\ &= \bigwedge_{a\in A} \bigvee_{b\in B} \dagger_K(\pi_B \left[\!\left[\chi^m_{\pi_A,\overline{a},a}(\overline{b}, b)\right]\!\right]) \wedge \bigwedge_{b\in B} \bigvee_{a\in A} \dagger_K(\pi_B \left[\!\left[\chi^m_{\pi_A,\overline{a},a}(\overline{b}, b)\right]\!\right]). \end{aligned}$$

By induction, $\dagger_K(\pi_B [\![\chi^m_{\pi_A,\overline{a},a}(\overline{b},b)]\!])$ is true if and only if $\overline{a}, a \mapsto \overline{b}, b \in I_m(\pi_A, \pi_B)$. With this observation, it is clear that $\dagger_K \left(\pi_B [\![\chi^{m+1}_{\pi_A,\overline{a}}(\overline{b})]\!]\right)$ is true if and only if for each $a \in A$, there is a $b \in B$ such that $\overline{a}, a \mapsto \overline{b}, b \in I_m(\pi_A, \pi_B)$ (forth) and for each $b \in B$, there is an $a \in A$ with $\overline{a}, a \mapsto \overline{b}, b \in I_m(\pi_A, \pi_B)$ (back), meaning that $\overline{a} \to \overline{b}$ satisfies the BFP with respect to $I_m(\pi_A, \pi_B)$, which is equivalent to $\overline{a} \mapsto \overline{b} \in I_{m+1}(\pi_A, \pi_B)$.

Hence, $\pi_B [\![\chi^{m+1}_{\pi_A,\overline{a}}(\overline{b})]\!] \neq 0$ if and only if $\pi_A, \overline{a} \cong_{m+1} \pi_B, \overline{b}$. □

This relates $m$-characteristic formulas to back-and-forth systems. Before moving on to $m$-equivalence, we will present a game-theoretic view on the back-and-forth property.

## 5.3 Ehrenfeucht-Fraïssé Games

Similarly to back-and-forth systems, classical Ehrenfeucht-Fraïssé games, as presented in [Tho93], can be adapted to semiring semantics without effort as follows.

**(5.7) Definition** (Ehrenfeucht-Fraïssé Game)**.** Let $\pi_A : \mathrm{Lit}_A(\tau) \to K$ as well as $\pi_B : \mathrm{Lit}_B(\tau) \to K$ be $K$-interpretations with $k$-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$. The *Ehrenfeucht-Fraïssé game* $G_m(\pi_A, \overline{a}, \pi_B, \overline{b})$ is played between two players for $m$ turns. We will call the players *Spoiler* and *Duplicator*. The starting position of the game is $\sigma : \overline{a} \mapsto \overline{b}$ and the Duplicator loses as soon as $\sigma$ is not a local isomorphism between the interpretations $\pi_A$ and $\pi_B$.

In each turn, the Spoiler first chooses an element $a \in A$ or $b \in B$, and the Duplicator must respond with $b \in B$ or $a \in A$ from the other interpretation respectively. Then, the position $\sigma$ is updated to $\sigma \coloneqq \sigma \cup \{(a, b)\}$, that is, the mapping is extended by $a \mapsto b$. If the Duplicator manages to uphold the local isomorphism property for all the $m$ turns, they win the game, otherwise, the Spoiler wins.

As an example, consider the two $K_3$-interpretations from the beginning of the chapter.

$\pi_1$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 1 | 0 |
| c | 3 | 0 |

$\pi_2$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 2 | 0 |
| c | 3 | 0 |

The Spoiler wins $G_1(\pi_1, \pi_2)$ in one turn by picking $b$ from $\pi_2$, since $\pi_2(Rb) = 2$ and the Duplicator cannot choose any corresponding element $e \in \{a, b, c\}$ for $\pi_1$ such that $\pi_1(Re) = 2$. It is easy to construct a slightly more complex example by adding an element as follows.

$\pi'_1$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 1 | 0 |
| c | 2 | 0 |
| d | 3 | 0 |

$\pi'_2$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 2 | 0 |
| c | 2 | 0 |
| d | 3 | 0 |

Here, the Duplicator wins the one-turn game $G_1(\pi'_1, \pi'_2)$, since for any $e \in \{a, b, c, d\}$, the value of $\pi'_i(Re)$ can be mirrored in the other $K_3$-interpretation. However, the Spoiler still wins $G_2(\pi'_1, \pi'_2)$ in two turns, for example by choosing $b$ and $c$ from $\pi'_2$. In order to uphold the local isomorphism property, the Duplicator would have to answer with two distinct elements $e, f \in \{a, b, c, d\}$ from $\pi'_1$ with $\pi'_1(Re) = \pi'_1(Rf) = 2$, which is not possible, as $c$ is the only element with $\pi'_1(Rc) = 2$.

There is an obvious similarity between back-and-forth systems and Ehrenfeucht-Fraïssé games. Intuitively, if $\overline{a} \mapsto \overline{b} \in I_m(\pi_A, \pi_B)$, then the Duplicator can play for at least $m$ turns by simply exploiting the BFP, as stated in the following lemma.

**(5.8) Lemma** (Winning Strategy for Duplicator)**.** For any two $K$-interpretations $\pi_A$ and $\pi_B$ with $k$-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$, $\pi_A, \overline{a} \cong_m \pi_B, \overline{b}$ implies that the Duplicator can win $G_m(\pi_A, \overline{a}, \pi_B, \overline{b})$.

*Proof.* We show the claim by induction on $m$. For $m = 0$, if $\pi_A, \overline{a} \cong_0 \pi_B, \overline{b}$, then $\overline{a} \mapsto \overline{b} \in \mathrm{Loc}(\pi_A, \pi_B)$, hence the Duplicator wins $G_0(\pi_A, \overline{a}, \pi_B, \overline{b})$ automatically by definition.

For $m + 1$, the Duplicator plays $G_{m+1}(\pi_A, \overline{a}, \pi_B, \overline{b})$ as follows. If the Spoiler chooses $a \in A$, respond with $b \in B$ such that $\overline{a}, a \mapsto \overline{b}, b \in I_m(\pi_A, \pi_B)$. This is possible thanks to the assumption that $\overline{a} \mapsto \overline{b} \in I_{m+1}(\pi_A, \pi_B)$ and the forth property. Similarly, if the Spoiler picks $b \in B$, respond with $a \in A$ such that $\overline{a}, a \mapsto \overline{b}, b \in I_m(\pi_A, \pi_B)$, which is possible with the back property. By induction, the Duplicator wins the “remaining” game $G_m(\pi_A, \overline{a}, a, \pi_B, \overline{b}, b)$ due to $\pi_A, \overline{a}, a \cong_m \pi_B, \overline{b}, b$. □

Now, we can attempt to put all those concepts together and arrive at an Ehrenfeucht-Fraïssé theorem for semiring semantics.

## 5.4 Resulting Theorem

Unfortunately, we will see that we cannot prove the full Ehrenfeucht-Fraïssé theorem for all positive semirings $K$. We start by stating the desired theorem without specifying the conditions on $K$.

**(5.9) Theorem** (Ehrenfeucht-Fraïssé Theorem for Semiring Semantics)**.** Let $K$ be a suitable semiring and $\pi_A : \mathrm{Lit}_A(\tau) \to K$, $\pi_B : \mathrm{Lit}_B(\tau) \to K$ two $K$-interpretations with $k$-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$. Then, the statements

(1) $\pi_A, \overline{a} \equiv_m \pi_B, \overline{b}$
(2) $\pi_A, \overline{a} \cong_m \pi_B, \overline{b}$
(3) $\pi_B \, [\![\chi^m_{\pi_A,\overline{a}}(\overline{b})]\!] \neq 0$
(4) Duplicator wins $G_m(\pi_A, \overline{a}, \pi_B, \overline{b})$

are equivalent for all $m \in \mathbb{N}$.

Most of the work has already been done in the previous sections. For example, “(2) ⇔ (3)” was shown for positive semirings $K$ in the back-and-forth lemma (5.6) and “(2) ⇒ (4)” holds by lemma (5.8).

“(1) ⇒ (3)” is very easy to show on positive semirings, since $\pi_A \, [\![\chi^m_{\pi_A,\overline{a}}(\overline{a})]\!] \neq 0$ holds by construction of characteristic formulas, which describe $\pi_A, \overline{a}$, hence $\pi_A, \overline{a} \equiv_m \pi_B, \overline{b}$ implies that $\pi_B \, [\![\chi^m_{\pi_A,\overline{a}}(\overline{b})]\!] \neq 0$ as well, since $\chi^m_{\pi_A,\overline{a}}(\overline{x})$ has quantifier rank $m$.

In order to complete the proof, it would suffice to show "(4) ⇒ (1)", or alternatively, the contraposition, that is

$$\pi_A, \overline{a} \not\equiv_m \pi_B, \overline{b} \quad \text{implies that} \quad \text{Spoiler wins } G_m(\pi_A, \overline{a}, \pi_B, \overline{b}).$$

We can attempt to prove this statement by deriving a winning strategy for the Spoiler in $G_m(\pi_A, \overline{a}, \pi_B, \overline{b})$ from a separating formula $\varphi(\overline{x})$ with quantifier rank at most $m$ and $\pi_A [\![\varphi(\overline{a})]\!] \neq \pi_B [\![\varphi(\overline{b})]\!]$, which exists by the assumption $\pi_A, \overline{a} \not\equiv_m \pi_B, \overline{b}$.

Assuming that $\varphi(\overline{x})$ is in negation normal form, the Spoiler proceeds by induction on the formula and "moves" to its subformulas whenever required, while upholding the invariant that $\varphi(\overline{x})$ is a separating formula for the currently selected tuples $\overline{a} \mapsto \overline{b}$. For the induction on $\varphi(\overline{x})$, recall the syntax of first-order logic from definition (2.3) and the corresponding semantics in definition (2.4) as well as the additional operator in $\mathsf{FO}(K, \tau)$ introduced in definition (5.1).

- If $\varphi(\overline{x})$ is a literal, then $\overline{a} \to \overline{b}$ is not a local isomorphism and the Spoiler wins. Note that this also applies to the new equality operator $\varphi(\overline{x}) = (\psi(\overline{x}) \overset{K}{=} c)$, since the new operator only accepts literals $\psi(\overline{x})$ and $\pi_A, \overline{a}$ may not differ from $\pi_B, \overline{b}$ on any literal if $\overline{a} \mapsto \overline{b}$ is a local isomorphism.
- If $\varphi(\overline{x}) = \psi(\overline{x}) \circ \vartheta(\overline{x})$ for $\circ \in \{\vee, \wedge\}$, then pick $\psi(\overline{x})$ or $\vartheta(\overline{x})$ as the next formula. Due to the invariant $\pi_A [\![\varphi(\overline{a})]\!] \neq \pi_B [\![\varphi(\overline{b})]\!]$, it is obvious that for at least one of the two formulas, $\pi_A [\![\psi(\overline{a})]\!] \neq \pi_B [\![\psi(\overline{b})]\!]$ or $\pi_A [\![\vartheta(\overline{a})]\!] \neq \pi_B [\![\vartheta(\overline{b})]\!]$ holds, so it is always possible to find a suitable choice $\varphi(\overline{x}) := \psi(\overline{x})$ or $\varphi(\overline{x}) := \vartheta(\overline{x})$ that upholds the desired invariant.
- If $\varphi(\overline{x}) = Qy\psi(\overline{x}, y)$ for $Q \in \{\exists, \forall\}$, then $(*)$ find an element $a \in A$ (or $b \in B$) such that $\pi_A [\![\psi(\overline{a}, a)]\!] \neq \pi_B [\![\psi(\overline{b}, b)]\!]$ for all $b \in B$ (or for all $a \in A$), pick this element in the Ehrenfeucht-Fraïssé game and move to the new formula $\psi(\overline{x}, y)$. Note that after this move, the Spoiler has "expended" one turn in the game, the new position is $\overline{a}, a \mapsto \overline{b}, b$ and the formula $\psi(\overline{x}, y)$ separates those tuples, hence the invariant is upheld.

Since the initial formula's quantifier rank was at most $m$, we can see that the Spoiler wins $G_m(\pi_A, \overline{a}, \pi_B, \overline{b})$ after at most $m$ turns, due to the fact that each turn "removes" one quantifier. However, an issue arises due to $(*)$, because we have not clarified how a suitable element can be found. As an example, consider the following two $\mathbb{N}$-interpretations.

$\pi_4$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 1 | 0 |
| c | 2 | 0 |

$\pi_5$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 2 | 0 |
| c | 2 | 0 |

Clearly, the sentence $\varphi := \exists x Rx$ with quantifier rank 1 separates them, since

$$\pi_4 [\![\varphi]\!] = 1 + 1 + 2 = 4 \quad \text{and} \quad \pi_5 [\![\varphi]\!] = 1 + 2 + 2 = 5.$$

Thus, the Spoiler should be able to win $G_1(\pi_4, \pi_5)$ in one turn, but it is obvious that the Duplicator can respond adequately to any move, hence the Spoiler loses.

This shows that our proof of the Ehrenfeucht-Fraïssé theorem does not work on all positive semirings, in particular, it does not work on $\mathbb{N}$, because the step $(*)$ is problematic. Note that quantifiers are interpreted as sums and products, so the step $(*)$ operates under the assumption that if two sums or products are distinct, then the set of the summands or factors is distinct as well, which would allow us to find $a$ or $b$ as suggested in $(*)$. More formally, the choice in $(*)$ is possible, if and only if the conditions

$$\begin{aligned} &(S) \quad \sum_{i\in I} a_i \neq \sum_{j\in J} b_j \quad \Rightarrow \quad \{a_i \mid i \in I\} \neq \{b_j \mid j \in J\} \quad \text{and} \\ &(P) \quad \prod_{i\in I} a_i \neq \prod_{j\in J} b_j \quad \Rightarrow \quad \{a_i \mid i \in I\} \neq \{b_j \mid j \in J\} \end{aligned}$$

are satisfied for all index sets $I$, $J$ and $(a_i)_{i\in I}, (b_j)_{j\in J} \subseteq K$. Of course, when dealing with finite $K$-interpretations, we can assume that $I$, $J$ are finite.

Interestingly, condition $(S)$ is equivalent to idempotence of $+$ on $K$. Note that the contraposition of $S$ is

$$(S) \quad \{a_i \mid i \in I\} = \{b_j \mid j \in J\} \quad \Rightarrow \quad \sum_{i\in I} a_i = \sum_{j\in J} b_j,$$

which clearly implies idempotence of $+$, since $\{a\} = \{a, a\}$ for all $a \in K$, hence $a = a + a$ by $(S)$. We can also prove $(S)$ from the idempotence of $+$ as follows.

Suppose that $I$, $J$ are index sets and we have families $(a_i)_{i\in I}, (b_j)_{j\in J} \subseteq K$ of summands such that the sets of their values are equal, that is,

$$\{a_i \mid i \in I\} = V = \{b_j \mid j \in J\}.$$

Since summation is invariant under partition $(\star)$ of the index set, we can group the summands by their values to obtain

$$\begin{aligned} \sum_{i\in I} a_i &\overset{\star}{=} \sum_{c\in V} \sum_{i\in I, a_i = c} a_i \\ &= \sum_{c\in V} \sum_{i\in I, a_i = c} c \\ &\overset{\text{i}}{=} \sum_{c\in V} c \qquad\qquad \text{and} \\ \sum_{j\in J} b_j &\overset{\star}{=} \sum_{c\in V} \sum_{j\in J, b_j = c} b_j \\ &= \sum_{c\in V} \sum_{j\in J, b_j = c} c \\ &\overset{\text{i}}{=} \sum_{c\in V} c, \end{aligned}$$

which implies that the sums are equal as well. The steps marked with (i) use the idempotence of addition. It is worth mentioning that this also works for infinitary sums, provided that the reasonable assumption of "infinitary idempotence", that is, $\sum_{i\in I} c = c$ for infinite $I$, holds as well. As seen in definition (2.5), we usually assume partition-invariance of infinitary operations in any case.

The same technique can be used to show that the property $(P)$ is equivalent to idempotence of $\cdot$ in $K$ with similar assumptions in case of infinitary products. Therefore, we conclude that the full proof of the Ehrenfeucht-Fraïssé theorem in semiring semantics works on positive semirings $K$ that are idempotent in both addition and multiplication, which can be summarized as follows.

**(5.10) Theorem** (Conditions for the Ehrenfeucht-Fraïssé Theorem)**.** Let $K$ be a semiring and $\pi_A : \mathrm{Lit}_A(\tau) \to K$, $\pi_B : \mathrm{Lit}_B(\tau) \to K$ two $K$-interpretations with $k$-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$. Consider the four statements

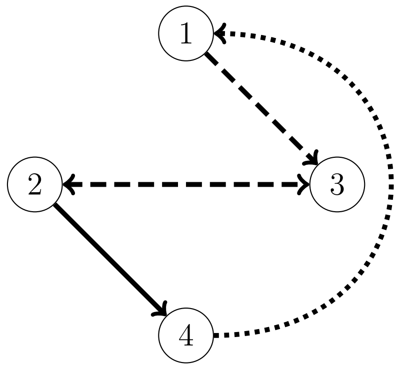
(1) $\pi_A, \overline{a} \equiv_m \pi_B, \overline{b}$

(2) $\pi_A, \overline{a} \cong_m \pi_B, \overline{b}$

(3) $\pi_B \, [\![\chi^m_{\pi_A,\overline{a}}(\overline{b})]\!] \neq 0$

(4) Duplicator wins $G_m(\pi_A, \overline{a}, \pi_B, \overline{b})$

from the Ehrenfeucht-Fraïssé theorem. The proofs for the implications between those statements that we presented in this chapter and the corresponding requirements on $K$ are illustrated in the following picture.




Solid arrows indicate that the implication holds for all semirings $K$. Dashed arrows indicate that $K$ must be positive, while dotted arrows require $K$ to be idempotent in both operations. In particular, all statements are equivalent in positive semirings that are idempotent in both operations.

Note that we do not claim the "minimality" of the conditions we imposed for our proofs and we only included arrows in the picture for implications that we mentioned directly. However, it is worth pointing out that, unfortunately, the "strict" condition of idempotence in both operations is necessary for the Ehrenfeucht-Fraïssé theorem. Suppose that a semiring $K$ is not idempotent in one of the operations, then we can pick an element $e \in K$ with $e + e \neq e$ or $e \cdot e \neq e$ to construct the following counterexample on $K$.

$\pi_e$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | e | 0 |

$\pi_{ee}$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | e | 0 |
| b | e | 0 |

By the choice of $e$, one of the sentences $\exists x Rx$ or $\forall x Rx$ of quantifier rank 1 separates $\pi_e$ and $\pi_{ee}$, however, the Spoiler clearly does not win $G_1(\pi_e, \pi_{ee})$ in one turn.

In spite of that, we can conclude that the two-sorted approach via $\mathsf{FO}(K, \tau)$ comes much closer to the classical Ehrenfeucht-Fraïssé theorem than "pure" first-order logic from the previous chapter. In fact, the Ehrenfeucht-Fraïssé theorem "almost" holds for all positive semirings $K$ under $\mathsf{FO}(K, \tau)$ and holds with the additional condition of idempotence in both operations, for example, in PosBool$[X]$. Hence, it may pay off to consider $\mathsf{FO}(K, \tau)$ for semiring model theory in the future in order to adapt more classical results to semiring semantics.

# Chapter 6

# Conclusion

In the previous chapters, we mainly gained insights about the meaning of elementary equivalence between $K$-interpretations. The first surprising result that we presented is the elementary equivalence of the two $K_3$-interpretations below.

$\pi_{PQ}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 1 | 3 | 0 | 0 |
| b | 2 | 1 | 0 | 0 |
| c | 3 | 2 | 0 | 0 |

$\pi_{QP}$ :

| $A$ | $P$ | $Q$ | $\neg P$ | $\neg Q$ |
|---|---|---|---|---|
| a | 3 | 1 | 0 | 0 |
| b | 1 | 2 | 0 | 0 |
| c | 2 | 3 | 0 | 0 |

The reason why this equivalence is surprising is that we can derive the fact that first-order logic, without any additions to its syntax, is not even able to distinguish two finite interpretations over a finite semiring $K_3$. Thus, it does not nearly have enough expressive power to adapt the Ehrenfeucht-Fraïssé theorem to semiring semantics, as illustrated by the fact that the Spoiler wins the Ehrenfeucht-Fraïssé game between $\pi_{PQ}$ and $\pi_{QP}$ in a single turn.

In fact, the expressive power of first-order logic, especially the power to separate non-isomorphic $K$-interpretations, depends heavily on the algebraic properties of $K$, which is why the relationship of elementary equivalence and isomorphism is difficult to capture generally. As a consequence, the question on which semirings $K$ elementary equivalence implies isomorphism for finite $K$-interpretations still remains open and our attempts to solve it have shown that polynomial semirings with varying restrictions are the best starting point to search for counterexamples.

In order for semiring semantics to behave more similarly to classical semantics, we proposed the two-sorted extension of first-order logic, which eases the construction of $m$-characteristic formulas and therefore enables the re-introduction of Ehrenfeucht-Fraïssé methods to semiring semantics. Interestingly, it appears that first-order logic may have too much expressive power for some aspects of the Ehrenfeucht-Fraïssé theorem, as was illustrated by the following $\mathbb{N}$-interpretations.

$\pi_4$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 1 | 0 |
| c | 2 | 0 |

$\pi_5$ :

| $A$ | $R$ | $\neg R$ |
|---|---|---|
| a | 1 | 0 |
| b | 2 | 0 |
| c | 2 | 0 |

First-order logic is able to separate $\pi_4$ and $\pi_5$ with only one quantifier, but we may say that it should not be able to do so, considering that the Duplicator wins the corresponding one-turn Ehrenfeucht-Fraïssé game.

These results suggest that we should work on defining new games to capture $m$-equivalence under semiring semantics in the future. While adapting model-theoretic results to semiring semantics, we may follow the philosophy of leaving first-order logic as-is and observing its properties, as we have done for the most part of this thesis, or we may try to modify it in order to gain stronger results, similarly to the approach from the previous chapter.

In conclusion, we have provided some model-theoretic tools and insights into elementary equivalence of finite $K$-interpretations under first-order logic, but, as suggested by the open problem mentioned before, there is still room for future research.

Another area left open for future research is infinite model theory for semiring semantics. Although many definitions in this thesis have touched on the possibility of considering infinite semiring interpretations, they were mostly left out. Also, we may look at algorithmic aspects of semiring semantics and attempt to adapt the classical compactness and completeness theorems in the future. As a final suggestion for future research, we would like to mention that semiring model theory can be extended to more logics with varying expressive power, for example, it may be interesting to characterize the meaning of elementary equivalence of semiring interpretations under fixed-point logics.

# Bibliography


[DG20] Katrin M. Dannert and Erich Grädel. Semiring Provenance for Guarded Logics. In *Hajnal Andréka and István Németi on Unity of Science: From Computing to Relativity Theory through Algebraic Logic (to appear)*, Outstanding Contribution to Logic. Springer, 2020.

[DGNT19] Katrin M. Dannert, Erich Grädel, Matthias Naaf, and Val Tannen. Generalized Absorptive Polynomials and Provenance Semantics for Fixed-Point Logic. *arXiv e-prints*, page arXiv:1910.07910, Oct 2019.

[GG98] Erich Grädel and Yuri Gurevich. Metafinite Model Theory. *Information and Computation*, 140:26–81, 1998.

[GKT07] Todd J. Green, Grigoris Karvounarakis, and Val Tannen. Provenance Semirings. In *Proceedings of the twenty-sixth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 31–40. ACM, 2007.

[GT17] Erich Grädel and Val Tannen. Semiring Provenance for First-Order Model Checking. arXiv:1712.01980 [cs.LO], 2017.

[GT19] Erich Grädel and Val Tannen. Provenance Analysis for Logic and Games. arXiv 1907.08470 [cs.LO], 2019.

[Mrk18] Lovro Mrkonjić. Provenance Analysis for Temporal and Dynamic Logics. Bachelor thesis, RWTH Aachen University, 2018.

[Naa19] Matthias Naaf. Semirings for Provenance Analysis of Fixed-point Logics and Games. Master thesis, RWTH Aachen University, 2019.

[Tho93] Wolfgang Thomas. On the Ehrenfeucht-Fraïssé Game in Theoretical Computer Science. In *Colloquium on Trees in Algebra and Programming*, pages 559–568. Springer, 1993.