Journal of Logical and Algebraic Methods in Programming 83 (2014) 135–153

Contents lists available at ScienceDirect

Journal of Logical and Algebraic Methods in Programming

www.elsevier.com/locate/jlamp

Exploring modal worlds

Han-Hing Dang, Roland Glück, Bernhard Möller *, Patrick Roocks, Andreas Zelend

Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany

ARTICLE INFO

Article history:
Available online 15 February 2014

Keywords:
Bisimulation
Formal concept analysis
Pareto front
Rectangles
Separation logic
Software product lines

ABSTRACT

Modal idempotent semirings cover a large set of different applications. The paper presents a small collection of these, ranging from algebraic logics for program correctness over bisimulation refinement, formal concept analysis, database preferences to feature oriented software development. We provide new results and/or views on these domains; the modal semiring setting allows a concise and unified treatment, while being more general than, e.g., standard relation algebra.

1. Introduction

Algebraic structures, such as *modal* idempotent semirings or Kleene algebras, offer a large variety of applications, while requiring only a small set of operators and axioms. Such algebras abstractly capture so-called Kripke structures, i.e., access relations over a set of worlds or states. In addition they provide the associated multi-modal operators box and diamond that allow reasoning, e.g., about possible actions of agents in a system or about state transitions in general. Particular instances of modal semirings are provided by the algebra of homogeneous binary relations and by abstract relation algebras.

This setting allows many general considerations and results, ranging from epistemic logics with knowledge and belief [1] to propositional dynamic Hoare logic and resource-based settings such as separation logic [2]. Moreover, many further applications are covered, like abstract reasoning about bisimulations for model refinement [3], formal concept analysis, simple and concise correctness proofs for the optimisation of database preference queries [4] or generally applicable models of module hierarchies in a feature oriented software development process [5].

In this paper, we take the readers on a short tour through several of these modal worlds and hope that they will enjoy the ride, maybe even feel some kind of explorer's excitement. We provide new results and/or views on the mentioned applications; the modal semiring setting allows a concise and unified treatment, while being more general than, e.g., standard relation algebra. Nevertheless the excellent relational papers and books by Gunther Schmidt [6,7] are gratefully and respectfully acknowledged as a constant source of inspiration (although at times the relational encoding requires some "decryption" to obtain smooth modal formulations). It is our pleasure to dedicate this paper to Gunther on the occasion of his 75th birthday!

The paper is organised as follows. In Section 2 we recapitulate the main definitions of modal idempotent semirings and provide some generally applicable laws. Section 3 extends an existing algebraic framework from autobisimulations to bisimulations between different relations. An algebraic treatment of formal concepts and rectangles is given in Section 4, while in Section 5 we set up a connection between rectangles and Pareto fronts in databases with preference queries. Section 6

* Corresponding author.
E-mail addresses: h.dang@informatik.uni-augsburg.de (H.-H. Dang), glueck@informatik.uni-augsburg.de (R. Glück), moeller@informatik.uni-augsburg.de (B. Möller), roocks@informatik.uni-augsburg.de (P. Roocks), zelend@informatik.uni-augsburg.de (A. Zelend).

http://dx.doi.org/10.1016/j.jlap.2014.02.004

considers an abstract partial correctness approach to separation logic, and Section 7 provides an algebra of modules for structured documents in software product lines.

2. Basics of modal semirings

Idempotent semirings are a well-known concept for modelling choice and sequential composition by the algebraic operations $+$ and $\cdot$.

Definition 2.1. A *semiring* is a structure $(S, +, 0, \cdot, 1)$ with $0 \neq 1$ such that $+$ and $\cdot$ are associative binary operations on S with neutral elements 0 and 1 resp., $+$ is commutative, and $\cdot$ distributes both from left and right over $+$. Moreover, 0 is an annihilator of $\cdot$, i.e., $x \cdot 0 = 0 = 0 \cdot x$ holds for all $x \in S$.

The operations $+$ and $\cdot$ are also called *addition* and *multiplication*, resp. As usual, multiplication binds stronger than addition, so $x + y \cdot z$ stands for $x + (y \cdot z)$. Due to associativity we are free to omit superfluous parentheses.

A semiring is called *idempotent* if $x + x = x$ holds for all $x \in S$. In this case, the relation $\leqslant \subseteq S \times S$, defined by $x \leqslant y \Leftrightarrow_{df} x + y = y$, is a partial order on S, called the *natural order*. In particular, the supremum of two elements x and y with respect to the natural order is given by $x + y$, the least element is 0, and both addition and multiplication are isotone. The infimum of two elements x and y need not exist; if it does it is denoted by $x \sqcap y$. The element 0 is irreducible with respect to $+$, i.e., $x + y = 0 \Leftrightarrow x = 0 = y$ holds for all $x, y \in S$.

For an arbitrary set M, the structure $(\mathsf{Rel}(M), \cup, \emptyset, ;, \mathsf{id}(M))$ forms an idempotent semiring where $\mathsf{Rel}(M)$ denotes the set of all binary relations over M, ; denotes relational composition and $\mathsf{id}(M)$ the identity relation on M.

Definition 2.2. A semiring $(S, +, 0, \cdot, 1)$ is called *Boolean* if it is a distributive lattice with join $+$ and meet $\sqcap$ equipped with a *complement operation* $\bar{\cdot} : S \to S$ with the following properties for all $x, y \in S$:

$$x + \bar{x} = y + \bar{y} \quad \text{and} \quad x \sqcap \bar{x} = y \sqcap \bar{y}, \tag{1}$$

$$\overline{x + y} = \bar{x} \sqcap \bar{y} \quad \text{and} \quad \overline{x \sqcap y} = \bar{x} + \bar{y}. \tag{2}$$

In an idempotent Boolean semiring, the element $\top =_{df} \bar{0}$ is the greatest element with respect to the natural order. Moreover, $x + \bar{x} = \top$, $x \sqcap \bar{x} = 0$ and $\bar{\bar{x}} = x$ for all $x \in S$. The structure $(\mathsf{Rel}(M), \cup, \emptyset, ;, \mathsf{id}(M))$ becomes a Boolean semiring if we define the complement operation by $\bar{R} =_{df} (M \times M) \backslash R$ (where $\backslash$ denotes set theoretic difference). The greatest element is the universal relation $M \times M$.

In $\mathsf{Rel}(M)$ a subset $N \subseteq M$ can be characterised by the associated partial identity $\mathsf{id}(N)$. This is abstracted to general idempotent semirings by the notion of tests as axiomatised in [8].

Definition 2.3. An element p of an idempotent semiring is called a *test* if it has a *relative complement* $\neg p$ with the properties $p + \neg p = 1$ and $p \cdot \neg p = 0 = \neg p \cdot p$.

In an idempotent semiring $(S, +, 0, \cdot, 1)$ the set of tests is denoted by $\mathsf{test}(S)$. As a writing convention, elements of $\mathsf{test}(S)$ are denoted by p, q, r and variants thereof. On tests, multiplication coincides with the infimum, i.e., we have $p \sqcap q = p \cdot q$ for all $p, q \in \mathsf{test}(S)$. As a consequence of this fact, multiplication on tests is both idempotent and commutative. Moreover, on tests also addition distributes over multiplication, i.e., $p + q \cdot r = (p + q) \cdot (p + r)$ holds for all tests p, q and r. The structure $(\mathsf{test}(S), +, 0, \cdot, 1)$ is a Boolean semiring with $\neg$ as complement operation and greatest element 1. We set $p - q =_{df} p \cdot \neg q$.

Since all tests are $\leqslant 1$, multiplication with a test corresponds to restriction. If a stands for an abstract transition element, such as a relation, $p \cdot a$ restricts a to starting states that lie in the set p and $a \cdot q$ to ending states in q. In $(\mathsf{Rel}(M), \cup, \emptyset, ;, \mathsf{id}(M))$ the tests are exactly the subrelations of $\mathsf{id}(M)$. We will use that in Section 7.

A few further useful properties are collected in the following lemma.

Lemma 2.4.

1. *In a Boolean semiring $(S, +, 0, \cdot, 1)$ all elements $p \leqslant 1$ are tests with relative complement $\neg p = 1 \sqcap \bar{p}$.*
2. *In every idempotent semiring we have the following properties for all $a, b \in S$ such that $a \sqcap b$ exists, and all $p, q \in \mathsf{test}(S)$:*

$$p \cdot (a \sqcap b) = p \cdot a \sqcap b = p \cdot a \sqcap p \cdot b,$$

$$(a \sqcap b) \cdot p = a \cdot p \sqcap b = a \cdot p \sqcap b \cdot p.$$

The next concepts we introduce are the *domain* and *codomain* operations.