Modal knowledge and game semirings

Bernhard Möller

Angaben zur Veröffentlichung / Publication details:

Möller, Bernhard. 2013. "Modal knowledge and game semirings." *The Computer Journal* 56 (1): 53–69. https://doi.org/10.1093/comjnl/bxs140.

Modal Knowledge and Game Semirings

Bernhard Möller

Institut für Informatik, Universität Augsburg, Germany
Email: moeller@informatik.uni-augsburg.de

The aim of algebraic logic is to compact series of small steps of general logical inference into larger (in)equational steps. Algebraic structures that have proved very useful in this context are modal semirings and modal Kleene algebras. We show that they can also model knowledge and belief logics as well as games without additional effort; many of the standard logical properties are theorems rather than axioms in this setting. As examples of the first area we treat the classical puzzles of the Wise Men and the Muddy Children. Moreover, we show possibilities for handling knowledge update and revision algebraically. For the area of games, we generalise the well-known connection between game logic and dynamic logic to the setting of modal semirings and link it to predicate transformer semantics, in particular to demonic refinement algebra. We think that our study provides evidence that modal semirings are able to handle a wide variety of (multi-)modal logics in a uniform algebraic fashion.

Keywords: algebraic logic; modal logic; epistemic logic; game algebra; semantics; semiring

1. INTRODUCTION

The aim of algebraic logic is to compact series of small steps of general logical inference into larger (in)equational steps. Moreover, it attempts to replace tedious model-theoretic argumentation, in particular, elementwise argumentation, by more abstract and compact reasoning.

During the recent years it has turned out that variants of *semirings* (e.g. [2]) are very useful algebraic structures for this. They may be seen as abstract representations of (state) transition systems and axiomatise the fundamental operations of choice and sequential composition in such systems. Semirings with an idempotent choice operator have a natural approximation order that corresponds to implication (or inclusion); hence implicational inference can be replaced by inequational reasoning. Adding finite and infinite iteration leads to Kleene algebras [3] and omega algebras [4].

An essential extension of these basic structures is provided by *modal semirings*, as studied extensively in [5, 6]. They are based on the concept of *tests* [7] that algebraically represent state predicates. Modal semirings add diamond and box operators and are more general than Kripke structures: the access between possible worlds can be described not only by relations, but, e.g., by sets of computation paths or even by computation trees. Kleene and omega algebras with modal operators can be used to give algebraic semantics of PDL, LTL and CTL; as shown in [8], the subclass of left Boolean quantales can even handle full CTL* and the propositional μ-calculus. Many further applications have been developed.

In the present paper we show that modal semirings can also model knowledge and belief logics (e.g. [9]) as well as games (e.g. [10]) without additional effort; many of the standard logical properties there are theorems rather than axioms in this setting. As examples of the first area we treat the classical puzzles of the Wise Men and the Muddy Children and show possibilities for handling knowledge update and revision algebraically. The algebraic treatment offers a more concise way of reasoning than classical natural deduction proofs. Moreover, since the algebraic treatment is completely first-order, it offers the possibility of using off-the shelf fully automatic theorem provers without a need for specially tailoring them towards modal/epistemic logic. For the area of games, we generalise the well-known connection between game logic and dynamic logic to the setting of modal semirings and link it to predicate transformer semantics, in particular to demonic refinement algebra [11].

The character of this paper is that of a feasibility study, not that of a re-development of existing particular modal logics in a new setting. Nevertheless, a surprising result seems to be that the relatively simple axiomatisation of modal semirings and modal Kleene algebras achieves many of the standard properties of such logics in an easy and uniform way.

This paper is a significantly extended and revised version of [1].

Our framework is intended for defining the semantics of new, special-purpose modal logics as they arise, e.g., with multi-agent systems. Using it will provide the advantage that many standard modal properties such as axioms M and K as well as certain induction rules hold automatically and do not need to be reproved or added as axioms separately for each new logic.

The paper is organised as follows. Part I deals with an algebraisation of knowledge/belief logics. These are briefly recapitulated in Section 2 and illustrated with a variant of the Wise Men Puzzle. Section 3 defines several variants of modal (left) semirings and Kleene algebras and lists the most essential properties of the box and diamond operators. They are applied in Section 4 to represent the usual knowledge/belief operators for multiagent systems algebraically. The laws these inherit from the general algebraic framework are used in Section 5 for a concise solution of the Wise Men Puzzle. Section 6 reuses parts of the solution to treat the Muddy Children Puzzle. In Section 7 we show further use of the algebra in modelling certain aspects like knowledge/belief revision (e.g. [12]) and preference relations between possible worlds and their upgrade (e.g. [13]).

Part II treats games and predicate transformers. Section 8 gives a brief recapitulation of games and their algebra, in particular, of their representation by predicate transformers. These are analysed in a general fashion in Section 9, and a connection to Parikh's iteration operators for games is set up. Section 10 considers predicate transformers as elements of a left i-semiring which is extended to a modal one. It relates the box and diamond operators there to the enabledness and termination operators of demonic refinement algebra [14]. Section 11 provides a brief conclusion and outlook.

PART I: KNOWLEDGE

We first model epistemic logic in modal semirings. As our running example we use a particular version of the Wise Men Puzzle [15]. Although, of course, epistemic logic was not invented for the solution of such puzzles, they provide a nice illstration of the basic concepts of the logic.

2. THE WISE MEN PUZZLE AND EPISTEMIC MODAL LOGIC

A king wants to test the wisdom of his three wise men. They have to sit on three chairs behind each other, all facing the same direction. The king puts a hat on each head, either red or black, in such a way that no one can see his own hat or the hats behind him, only the hats of the men before him. Then the king announces that at least one hat is red. He asks the wise man in the back if he knows his hat colour, but that one denies. Then he asks the middle one who denies, too. Finally he says to the front one: "If you are really wise, you should now know the colour of your hat."

To treat the puzzle in epistemic logic, one uses formulae $\mathsf{K}_j\varphi$ (man j knows φ, *individual knowledge*), $\mathsf{E}\varphi$ (*everyone knows* φ) or $\mathsf{C}\varphi$ (everyone knows φ and everyone knows that everyone knows φ and everyone knows that everyone knows that everyone knows φ and $\ldots$, i.e., φ is *common knowledge*).

Let the men be numbered in the order of questioning, i.e., from back to front, and let r_i mean that i's hat is red. Then the following assumptions are usually made: the configuration of the chairs and the visibility are common knowledge, as is everything that is being said. None of that can be withdrawn or invalidated. This is formalised in epistemic logic as follows.

- Every man sees exactly the hats before him, i.e., for $j < i$, $\mathsf{C}(r_i \to \mathsf{K}_j r_i)$ and $\mathsf{C}(\neg r_i \to \mathsf{K}_j \neg r_i)$.
- At least one hat is red, i.e., $\mathsf{C}(r_1 \vee r_2 \vee r_3)$.
- After the king's questions, for $i = 1, 2$ we have $\mathsf{C}(\neg K_i r_i)$ and $\mathsf{C}(\neg K_i \neg r_i)$.

Now the question is whether we can infer anything about $\mathsf{K}_3 r_3$ from that.

One aim of Part I is to give an algebraic semantics for the knowledge operators and to solve the puzzle by (in)equational reasoning.

To prepare the algebraisation we recall the main elements of Kripke semantics for modal logic (e.g. [16]). We will use a multiagent setting (each wise man is an agent) in which each agent has his own box and diamond operators.

A *(multimodal) Kripke frame* is a pair $K = (W, R)$, where W is a set of *possible worlds* and $R = (R_i)_{i \in I}$, for some index set I, is a family of binary *access relations* $R_i \subseteq W \times W$ between worlds. Relation R_i expresses the uncertainty of agent i about the current state of affairs: if he actually is in a world w then he considers all worlds v with $w\, R_i\, v$, called the *epistemic R_i-neighbours* of w, as possible and has insufficient information to discern which of the worlds is the "real" one. The epistemic neighbours of w may or may not include w itself.

Note that, following the literature on modal logic, we view the "inputs" to a relation on the left, its "outputs" on the right.

The knowledge/belief of agent i in a world w consists of the formulae that are true in all epistemic R_i-neighbours of w. Knowledge and belief variants of the logic are distinguished by special assumptions about the relations R_i.

The semantics of modal formulae is modelled by the *satisfaction relation* $K, w \models \varphi$ which tells whether a formula φ holds in world w in frame K. Equivalently, a formula φ characterises the subset $[\![\varphi]\!] =_{df} \{w \mid K, w \models \varphi\}$ of possible worlds in which it holds.

The semantics of the modal operators $\langle R_i \rangle$ and $[R_i]$

are given by

$$w \in [\![\langle R_i\rangle\varphi]\!] \quad \Leftrightarrow_{df} \quad \exists\, v : R_i(w,v) \ \wedge\ v \in [\![\varphi]\!] \ ,$$
$$w \in [\![[R_i]\varphi]\!] \quad \Leftrightarrow_{df} \quad \forall\, v : R_i(w,v) \Rightarrow v \in [\![\varphi]\!] \ .$$

They are De Morgan duals:

$$[\![[R_i]\varphi]\!] \ = \ [\![\neg\langle R_i\rangle\neg\varphi]\!] \ .$$

By these definitions $[R_i]$ coincides with the knowledge/belief operator K_i, whereas $\langle R_i\rangle$ coincides with the possibility operator P_i.

Usually, special axioms for the knowledge operators are required:

$\mathsf{K}_i\varphi \to \varphi$	if i knows φ then φ is indeed true (truth, Axiom T)
$\mathsf{K}_i\varphi \to \mathsf{K}_i\mathsf{K}_i\varphi$	if i knows φ, he knows that (positive introspection PI)
$\neg\mathsf{K}_i\varphi \to \mathsf{K}_i\neg\mathsf{K}_i\varphi$	analogous (negative introspection NI)

If K_i is intended to model belief rather than true knowledge, only the introspection axioms are used. We will see in the solution of the puzzle which of these are actually needed.

3. ALGEBRAIC SEMANTICS: MODAL SEMIRINGS

We will now present our algebraic formalisation of the knowledge operators.

3.1. Semirings

There are already various algebraisations of modal operators, e.g., Boolean algebras with operators [17] and propositional dynamic logic PDL [18]. Moreover, a concrete algebraic treatment of Kripke frames can be given using relation algebra; the knowledge requirements above correspond to the following relational ones:

$\mathsf{K}_i\varphi \to \varphi$	$I \subseteq R_i$	(reflexive)
$\mathsf{K}_i\varphi \to \mathsf{K}_i\mathsf{K}_i\varphi$	$R_i \,;\, R_i \subseteq R_i$	(transitive)
$\neg\mathsf{K}_i\varphi \to \mathsf{K}_i\neg\mathsf{K}_i\varphi$	$R_i^{\smile}; R_i \subseteq R_i$	(euclidean)

Here, I is the identity relation, ; is relational composition and $^{\smile}$ is relational converse.

Modal semirings and Kleene algebras, as studied extensively in [5, 6], provide a very effective combination of PDL and algebraic operations on the access elements. Additionally, they abstract from the special case of access *relations* and allow more general *access elements* to connect states, such as sets of computation paths. The subclass of omega algebras [4] allows the incorporation of infinite iteration. A further subclass, the Boolean quantales, admit μ-calculus-like recursive definitions and can even realise full CTL*, as shown in [8].

One main aim of the present paper is to show that this well established structure of modal semirings also can, without effort, be re-used to model essential aspects of knowledge and game logics and perform corresponding algebraic proofs about them. To make the paper largely self-contained, we repeat the essential definitions (e.g. [2]).

Definition 3.1.

1. A *left idempotent semiring*, briefly a *left i-semiring*, is a structure $(S, +, 0, \cdot, 1)$ satisfying the following axioms.
   - The reduct $(S, +, 0)$ is a commutative and idempotent monoid. This induces the *natural order* $a \leq b \Leftrightarrow_{df} a + b = b$.
   - The reduct $(S, \cdot, 1)$ is a monoid.
   - Composition $\cdot$ is distributive and strict in its left argument, i.e., $(a + b) \cdot c = a \cdot c + b \cdot c$ and $0 \cdot a = 0$.
   - Composition is $\leq$-isotone or, equivalently, superdistributive in its right argument, i.e., $a \cdot b + a \cdot c \geq a \cdot (b + c)$.
2. A *weak i-semiring* is a left i-semiring in which composition is also distributive in its right argument, i.e., $a \cdot (b + c) = a \cdot b + a \cdot c$.
3. A weak i-semiring with right-strictness, i.e., $a \cdot 0 = 0$, is called an *i-semiring*.

In most applications these operators are interpreted as follows:

$+ \ \leftrightarrow$ choice,
$\cdot \ \leftrightarrow$ sequential composition,
$0 \ \leftrightarrow$ empty choice,
$1 \ \leftrightarrow$ null action,
$\leq \ \leftrightarrow$ increase in information or in choices.

The axioms entail that 0 is the least element and $a + b$ is the least upper bound or *join* of a and b.

A prominent i-semiring is provided by the set of all binary relations over a set, with $+$ and $\cdot$ interpreted as union and relational composition.

A left i-semiring structure is also at the core of process algebra frameworks (e.g. [19]); for further discussion of the connection see [20].

3.2. Tests and Validity

While general i-semiring elements can be thought of as sets of transitions or transition paths between states, we now describe how to model state predicates or, isomorphically, sets of states algebraically.

Let us illustrate this in the i-semiring of binary relations over a set Q of elements (say, states). The subsets $P \subseteq Q$ are in one-to-one correspondence with subsets of the identity relation of the form $I_P =_{df} \{(x, x) \,|\, x \in P\}$. Therefore these I_P can represent the Ps as relations and hence model predicates characterising them. In PDL, the role of tests is played by statements

of the form $\varphi?$ that test whether φ holds in the current state.

The algebraic counterpart to this idea dates back at least to [21]; terminologically we follow [7].

DEFINITION 3.2. A *test* of a left i-semiring S is a *subidentity*, i.e., an element p with $p \leq 1$, that has a complement $\neg p$ relative to 1, i.e., $p \cdot \neg p = 0 = \neg p \cdot p$ and $p + \neg p = 1$. The set of all tests of S is denoted by $\mathsf{test}(S)$.

As described above, in the relation i-semiring the tests are the subsets of the identity relation.

We will consistently write $a, b, c \ldots$ for arbitrary i-semiring elements and $p, q, r, \ldots$ for tests. This way, tests may look like propositional variables, but they are not: as described above they abstract predicates with free variables and stand for the sets of states that fulfil the predicates.

It is not hard to show that Definition 3.2 entails uniqueness of the complement $\neg p$ of a test p. Note that $\neg$ is required only for tests, not for general elements, which allows a much wider class of models. In fact, the negation operator on tests is a *derived* concept: in any given i-semiring the set of tests is precisely the set of subidentities for which $\neg$ exists. This set may be very small, but it always contains at least 0 and 1.

DEFINITION 3.3. A *left test semiring* is a left i-semiring S in which all tests commute under $\cdot$, i.e., $p \cdot q = q \cdot p$ for all $p, q \in \mathsf{test}(S)$. This is equivalent to stipulating the distributivity law $p \cdot (q + r) = p \cdot q + p \cdot r$ for all $p, q, r \in \mathsf{test}(S)$.

Hence every weak i-semiring is a left test semiring.

The above notion of tests deviates slightly from that in [7]: it does not allow an arbitrary Boolean algebra of subidentities as $\mathsf{test}(S)$ but only the maximal complemented one. The reason is that the axiomatisation of the modal box operator to be presented below forces this maximality anyway (see [6]). Further ways of axiomatising tests and the associated modal operators will be discussed in the following section.

Straightforward calculations show that in a left test semiring S the set $\mathsf{test}(S)$ is closed under $+$ and $\cdot$ and forms a Boolean algebra with $+$ as join, $\cdot$ as greatest lower bound or *meet* and 0 and 1 as its least and greatest elements.

When tests are viewed as predicates over a set Q of states, the semiring operators play the following roles:

$$
\begin{array}{rcl}
0/1 & \leftrightarrow & \mathsf{FALSE}\ (\text{empty set})/\mathsf{TRUE}\ (\text{full set } Q), \\
+/\cdot & \leftrightarrow & \text{disjunction (union)/conjunction (intersection)}, \\
\leq & \leftrightarrow & \text{implication (subsethood)}, \\
p \cdot a / a \cdot p & \leftrightarrow & \text{input/output restriction of } a \text{ by } p, \\
p \cdot a \cdot q & \leftrightarrow & \text{the part of } a \text{ that takes } p\text{-elements to } q\text{-elements}. \qquad (*)
\end{array}
$$

In a left test semiring S we will freely use the standard Boolean operations on tests, like implication $p \to q =_{df} \neg p + q$ and relative complement $p - q =_{df} p \cdot \neg q$, with their usual laws, notably the Galois connection

$$p \cdot q \leq r \Leftrightarrow p \leq q \to r\ , \qquad \text{(shunting)}$$

which has contraposition as a special case. We assume that $\cdot$ binds tighter than $\to$.

In logic, a predicate is called valid if it holds for all states, which means that it coincides with the predicate TRUE, represented by the largest test 1. Therefore, we can define validity algebraically as follows.

DEFINITION 3.4. A test p is *valid*, in symbols $\models p$, if $1 \leq p$ (or, equivalently, $p = 1$).

By shunting,

$$\models q \to r \Leftrightarrow q \leq r\ .$$

Moreover,

$$\models p \ \wedge\ p \leq q \ \Rightarrow\ \models q\ . \qquad (1)$$

3.3. Modal Operators: Box and Diamond

We now axiomatise forward box operators; a backward version could be axiomatised symmetrically, but will not be needed in the present paper. The box operators we define are not (yet) epistemic operators. They are completely independent of any particular interpretation what the elements a of the underlying i-semiring may mean. Most generally, one may think of such an a as being some kind of transition system, for instance a Kripke structure. Then the box operator $[a]$ describes the connection between states via a: given a set of (post-)states, represented by a test q, the result of $[a]q$ (operator $[a]$ applied to q) is a test representing all (pre-)states for which all a-successors lie in q. This coincides with the classical semantics of $[a]$ in multimodal logics (see e.g. [16]), which admit several transition elements a. In monomodal logics, such as linear temporal logic, there is only one transition element which can therefore be omitted, leading to the familiar $\Box$ notation.

The general concept of box covers many familiar notions, for instance, the weakest liberal precondition and Hoare triples in program correctness. To explain this, assume that test q represents all states that satisfy a certain postcondition φ, and let a be the transition relation of a program. Then the test $[a]q$ represents all states for which all a-successors satisfy the postcondition φ. Hence $[a]$ corresponds to the weakest precondition under which a guarantees postcondition φ, i.e. to the weakest liberal precondition $\mathsf{wlp}(a, q)$ [22]. Therefore, algebraically one can consider a Hoare triple $\{p\}\, a\, \{q\}$ as standing for "p implies $[a]q$", in semiring notation, $p \leq [a]q$.

When the states are viewed as possible worlds and a represents the access relation of a Kripke structure, $[a]$

turns into the epistemic knowledge or belief operator: if q represents all worlds that satisfy a certain formula φ then $[a]q$ represents all worlds for which all a-neighbours satisfy φ.

DEFINITION 3.5. A *(left/weak) modal* semiring is a structure $(S, +, 0, \cdot, 1, [\_])$ such that the reduct $(S, +, 0, \cdot, 1)$ is a (left/weak) i-semiring and the *box operator* $[\_] : S \to (\mathsf{test}(S) \to \mathsf{test}(S))$ satisfies the axioms [23]

$$p \leq [a]q \;\Leftrightarrow\; p \cdot a \cdot \neg q = 0 \;, \qquad \text{(box1)}$$
$$[a \cdot b]p \;=\; [a][b]p \;. \qquad \text{(box2)}$$

The associated *diamond operator* $\langle\_\rangle : S \to (\mathsf{test}(S) \to \mathsf{test}(S))$ is defined as the de Morgan dual of box, viz.

$$\langle a\rangle p \;=_{df}\; \neg[a]\neg p \;.$$

We are well aware that there are different ways of axiomatising tests and box; however, the treatment we are choosing is the most adequate one for our purposes. We will discuss some of the alternatives below.

According to $(*)$ above, Axiom (box1) means that all p-worlds satisfy $[a]q$ iff there is no a-connection from p-worlds to $\neg q$-worlds. This specifies $[a]q$ as the weakest of all such predicates, which justifies the above discussion of the weakest liberal precondition predicate transformer wlp.

Axiom (box2) makes box well-behaved w.r.t. composition. An easy calculation shows that also diamond is well-behaved w.r.t. composition:

$$\langle a \cdot b\rangle p = \langle a\rangle\langle b\rangle p \;. \qquad (2)$$

Both operators are unique if they exist. They coincide with the corresponding ones in PDL (e.g. [18]); the difference is that in PDL the first argument a of the box is of a purely syntactic nature without any algebraic laws.

An equivalent purely equational axiomatisation via a domain operator has been presented in [6] for the case of an i-semiring. In [20] it has been shown that it carries over to left i-semirings. It works as follows. Given a domain operator $\ulcorner : S \to \mathsf{test}(S)$ such that $\ulcorner a$ is the test characterising the starting states of transition element a, diamond and box can be defined as

$$\langle a\rangle p \;=\; \ulcorner(a \cdot p) \;, \qquad [a]p \;=\; \neg\ulcorner(a \cdot \neg p) \;.$$

Conversely, domain can be defined by

$$\ulcorner a \;=\; \langle a\rangle 1 \;=\; \neg[a]0 \;.$$

Both from a mathematical and an automated theorem proving point of view, the two-sortedness of the box/diamond and the domain views is unsatisfactory. A number of authors have come up with one-sorted approaches where the sort of tests is implicitly defined as the image set of a certain endofunction on the i-semiring under consideration. One important, relationally based, approach in this vein is that of dynamic negation [24], another the antidomain approach of [25] in general i-semirings. We forego details of these approaches, since the present paper is not about axiomatisation, but about application of algebraic structures. A recent survey is given in [26].

We list some useful properties of the above box axioms. De Morgan duality gives the swapping rule

$$\langle a\rangle[b]p \leq [c]p \;\Leftrightarrow\; \langle c\rangle\neg p \leq [a]\langle b\rangle\neg p \;. \qquad (3)$$

Box is anti-disjunctive and diamond is disjunctive in the first argument:

$$[a+b]p \;=\; [a]p \cdot [b]p \;, \qquad \langle a+b\rangle p \;=\; \langle a\rangle p + \langle b\rangle p \;. \quad (4)$$

Hence box is antitone and diamond is isotone in the first argument:

$$a \leq b \;\Rightarrow\; [a]p \geq [b]p \;\wedge\; \langle a\rangle p \leq \langle b\rangle p \;. \qquad (5)$$

To understand the antitony, recall that the implication order $a \leq b$ expresses that b offers at least as many transition possibilities as a. Now, if more choices are offered, one can guarantee less, which is expressed by $[b]p \leq [a]p$.

Moreover, both box and diamond are isotone in their second arguments:

$$p \leq q \;\Rightarrow\; [a]p \leq [a]q \;\wedge\; \langle a\rangle p \leq \langle a\rangle q \;. \qquad (6)$$

This entails

$$\models [a]p \;\wedge\; p \leq q \;\Rightarrow\; \models [a]q \;. \qquad (7)$$

Finally, for tests box and diamond can be given explicitly:

$$[p]q = p \to q \;, \qquad \langle p\rangle q = p \cdot q \;. \qquad (8)$$

This agrees with the behaviour of the test operation $p?$ in PDL. Moreover, we have

$$[1]q = q = \langle 1\rangle q \;.$$

3.4. Modal operators in Weak Semirings

In a weak i-semiring S we have the following additional properties:

– Box is conjunctive and diamond is disjunctive:

$$[a](p \cdot q) = [a]p \cdot [a]q \;,$$
$$\langle a\rangle(p + q) = \langle a\rangle p + \langle a\rangle q \;.$$

– Moreover, Box satisfies Axiom K (*modal modus ponens*) and diamond its dual:

$$[a](p \to q) \leq [a]p \to [a]q \;, \qquad (9)$$
$$\langle a\rangle p - \langle a\rangle q \leq \langle a\rangle(p - q) \;.$$

By contraposition and shunting, this is equivalent to the following forms (*modal modus tollens*, given only for box):

$$[a](p \to q) \cdot \neg[a]q \leq \neg[a]p \ , \quad [a](p + q) \cdot \neg[a]p \leq \neg[a]\neg q \ . \tag{10}$$

– Box satisfies the following propagation law:

$$([a]q) \cdot a \ = \ ([a]q) \cdot a \cdot q \ , \tag{11}$$

which means that starting in a world for which all a-successors guarantee q allows indeed asserting q as a postcondition. This law entails

$$\models [a]q \ \Rightarrow \ a \ = \ a \cdot q \ . \tag{12}$$

In an i-semiring also the reverse implication holds which further entails $\models [a \cdot q]q$, since $a \cdot q \ = \ a \cdot q \cdot q$.

Finally we note that a weak i-semiring S is an i-semiring iff box satisfies Axiom M of modal logic and diamond its dual; algebraically they read

$$[a]1 = 1 \ , \qquad \langle a\rangle 0 = 0 \ . \tag{13}$$

Hence, if (13) holds then $\models p \ \Rightarrow \ \models [a]p$. A consequence of (13) and (9) is

$$\models p \to q \ \Rightarrow \ \models [a]p \to [a]q \ . \tag{14}$$

3.5. Modal Kleene Algebras

Next, we describe finite iteration. A *(left/weak) Kleene algebra* [3] is a structure $(S, +, 0, \cdot, 1, ^*)$ such that the reduct $(S, +, 0, \cdot, 1)$ is a (left/weak) i-semiring and the finite iteration operator * satisfies the left unfold and induction axioms

$$1 + a \cdot a^* \leq a^* \ , \qquad b + a \cdot c \leq c \Rightarrow a^* \cdot b \leq c \ .$$

In the relation i-semiring, a^* and $a^+ =_{df} a^* \cdot a$ are the reflexive-transitive and transitive closure of a, respectively.

A (left/weak) Kleene algebra is *modal* when the underlying left/weak i-semiring is. As shown in [6], in this case the axioms entail the laws of box and diamond star and plus induction (note that they need not be added as separate axioms):

$$q \leq p \cdot [a]q \ \Rightarrow \ q \leq [a^*]p \ , \quad p + \langle a\rangle q \leq q \ \Rightarrow \ \langle a^*\rangle p \leq q \tag{15}$$

$$q \leq [a]p \cdot [a]q \ \Rightarrow \ q \leq [a^+]p \ , \quad \langle a\rangle p + \langle a\rangle q \leq q \ \Rightarrow \ \langle a^+\rangle p \leq q \ . \tag{16}$$

Using Hoare triples, the box part of (15) reads $(q \leq p \wedge \{q\}\, a\, \{q\}) \ \Rightarrow \ \{q\}\, a^*\, \{p\}$, which is related to the familiar Hoare rule for the while loop. For the case $p = q$ (16) yields the laws

$$q \leq [a]q \ \Rightarrow \ q \leq [a^+]q \ , \quad \langle a\rangle q \leq q \ \Rightarrow \ \langle a^+\rangle q \leq q \ . \tag{17}$$

The first of these reads in terms of Hoare triples $\{q\}\, a\, \{q\} \ \Rightarrow \ \{q\}\, a^+\, \{q\}$, i.e., an invariant of a is also one of a^+. Finally, we have the PDL induction rules (see [23])

$$[a^*](p \to [a]p) \leq p \to [a^*]p \ , \quad \langle a^*\rangle p - p \leq \langle a^*\rangle(\langle a\rangle p - p) \ . \tag{18}$$

3.6. Reflexivity, Transitivity, Symmetry and Introspection

We now want to give general algebraic variants of the relational characterisations of reflexivity, transitivity, symmetry and introspection. The fundamental tool for this is the Geach formula (e.g. [16]) from standard modal correspondence theory: for relations R, S, T, U one has

$$R^\smile; S \subseteq T \, ; U^\smile \ \Leftrightarrow \ \forall\, P : \langle S\rangle[U]P \subseteq [R]\langle T\rangle P \ ,$$

where $^\smile$ is the relational converse operator and P ranges over the relational tests, i.e., the subidentity relations. If in addition to the forward modal operators $[\_]$ and $\langle\_\rangle$ also the backward ones $[\_]^-$ and $\langle\_\rangle^-$ are present, the relational form can be mimicked more directly by

$$R^\smile; S \subseteq T \, ; U^\smile \ \Leftrightarrow \ \forall\, P : \langle R\rangle^-\langle S\rangle P \subseteq \langle U\rangle\langle T\rangle^- P \ .$$

To obtain more compact formulas we lift the inclusion order between test relations pointwise to the box and diamond operators and denote composition of such operators by juxtaposition. With this convention and by shunting, the Geach equivalence simply becomes

$$R^\smile; S \subseteq T \, ; U^\smile \ \Leftrightarrow \ \langle S\rangle[U] \subseteq [R]\langle T\rangle \ \Leftrightarrow \ \langle R\rangle[T] \subseteq [S]\langle U\rangle \ .$$

The following properties of relations and their Geach equivalents are particularly useful here: A relation R is

– reflexive $\Leftrightarrow_{df} I \subseteq R \ \Leftrightarrow \ \langle I\rangle \subseteq \langle R\rangle \ \Leftrightarrow \ [R] \subseteq [I]$,
– euclidean $\Leftrightarrow_{df} R^\smile; R \subseteq R \ \Leftrightarrow \ \langle R\rangle[R] \subseteq [R] \ \Leftrightarrow \ \langle R\rangle \subseteq [R]\langle R\rangle$,
– symmetric $\Leftrightarrow_{df} R^\smile \subseteq R \ \Leftrightarrow \ [I] \subseteq [R]\langle R\rangle$,
– serial or total $\Leftrightarrow_{df} I \subseteq R \, ; R^\smile \Leftrightarrow \ [R] \subseteq \langle R\rangle$,
– deterministic $\Leftrightarrow_{df} R^\smile; R \subseteq I \ \Leftrightarrow \ \langle R\rangle \subseteq [R]$,
– transitive $\Leftrightarrow_{df} R \, ; R \subseteq R \ \Leftrightarrow \ \langle R\rangle\langle R\rangle \subseteq \langle R\rangle \ \Leftrightarrow \ [R] \subseteq [R][R]$.

Since general semirings do not furnish a converse operation, we use the modal Geach equivalents to transfer these notions to the abstract setting. Again we use the pointwise lifting of the order $\leq$ on tests to test transformers and denote test transformer composition by juxtaposition.

Definition 3.6. An element a of a left modal semiring is

– *m-reflexive* $\Leftrightarrow_{df} \langle 1\rangle \leq \langle a\rangle \ \Leftrightarrow \ [a] \leq [1]$,
– *m-euclidean* $\Leftrightarrow_{df} \langle a\rangle[a] \leq [a] \ \Leftrightarrow \ \langle a\rangle \leq [a]\langle a\rangle$,
– *m-symmetric* $\Leftrightarrow_{df} [1] \leq [a]\langle a\rangle \ \Leftrightarrow \ \langle a\rangle[a] \leq \langle 1\rangle$,
– *m-serial* or *m-total* $\Leftrightarrow_{df} [a] \leq \langle a\rangle$,
– *m-deterministic* $\Leftrightarrow_{df} \langle a\rangle \leq [a]$,
– *m-transitive* $\Leftrightarrow_{df} \langle a\rangle\langle a\rangle \leq \langle a\rangle \ \Leftrightarrow \ [a] \leq [a][a]$.

Finally, a is called an *m-equivalence* if a is m-reflexive, m-transitive and m-symmetric.

One may wonder about the qualifier "m-" (for "modally") in the above notions. The reason is that reflexivity and transitivity are usually defined as $1 \leq a$ and $a \cdot a \leq a$, resp. These notions are much stronger and coincide with the above ones only if the underlying modal semiring is *extensional*, i.e., satisfies $\langle a \rangle \leq \langle b \rangle \Rightarrow a \leq b$ for all a, b. An example of an extensional modal semiring is the relational one, whereas i-semirings of trace sets (see e.g. [8]) are not.

The m-euclidean elements correspond to knowledge operators that satisfy negative introspection. The following facts are well known (and can straightforwardly be shown from the above definitions):

- An m-reflexive and m-euclidean element is also m-symmetric and m-transitive.
- An m-symmetric and m-transitive element is also m-euclidean.

The case of m-symmetric elements is particularly important, since often one uses m-equivalences as access elements. We have the following useful properties.

LEMMA 3.7. *Let S be a left test semiring, $a \in S$ be m-symmetric and $p \in \mathsf{test}(S)$.*

1. *$p \cdot a \cdot p$ is again m-symmetric.*
2. *$\langle a \rangle 1 \leq p \Leftrightarrow \ \models [a]p$.*

Let now S be an i-semiring.

3. *$a = a \cdot p \Leftrightarrow a = p \cdot a$.*
4. *$a = a \cdot p \Leftrightarrow a = p \cdot a \cdot p \Leftrightarrow a = p \cdot a$.*

Proof.

1. We calculate

$$\begin{array}{ll} & [p \cdot a \cdot p]\langle p \cdot a \cdot p \rangle q \\ = & \quad \{\![\text{ by Axiom (box2) and modal operators of tests (8) }]\!\} \\ & [p \cdot a](p \to (p \cdot \langle a \cdot p \rangle q)) \\ = & \quad \{\![\text{ Boolean algebra }]\!\} \\ & [p \cdot a](p \to \langle a \cdot p \rangle q) \\ = & \quad \{\![\text{ by Axiom (box2) and modal operators of tests (8) }]\!\} \\ & [p \cdot a \cdot p]\langle a \cdot p \rangle q) \\ \geq & \quad \{\![\text{ antitony of box }]\!\} \\ & [p \cdot a]\langle a \cdot p \rangle q \\ = & \quad \{\![\text{ by Axiom (box2) and modal operators of tests (8) }]\!\} \\ & p \to [a]\langle a \rangle (p \cdot q) \\ \geq & \quad \{\![\text{ a m-symmetric and isotony }]\!\} \\ & p \to (p \cdot q) \\ = & \quad \{\![\text{ Boolean algebra }]\!\} \\ & p \to q \\ \geq & \quad \{\![\text{ Boolean algebra }]\!\} \\ & q \ . \end{array}$$

2. We have, by isotony (6) and m-symmetry,

$$\begin{array}{l} \langle a \rangle 1 \leq p \ \Rightarrow \ [a]\langle a \rangle 1 \leq [a]p \ \Rightarrow \\ 1 \leq [a]p \ \Rightarrow \ \langle a \rangle 1 \leq \langle a \rangle [a]p \ \Rightarrow \ \langle a \rangle 1 \leq p \ . \end{array}$$

3. We calculate

$$\begin{array}{ll} & a = a \cdot p \\ \Leftrightarrow & \quad \{\![\text{ by (12) and } S \text{ being an i-semiring }]\!\} \\ & \ \models [a]p \\ \Leftrightarrow & \quad \{\![\text{ Part (2) }]\!\} \\ & \langle a \rangle 1 \leq p \\ \Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\ & \neg p \leq [a]0 \\ \Leftrightarrow & \quad \{\![\text{ by Axiom (box1) }]\!\} \\ & \neg p \cdot a \leq 0 \\ \Leftrightarrow & \quad \{\![\text{ splitting } a = p \cdot a + \neg p \cdot a \ ]\!\} \\ & a = p \cdot a \ . \end{array}$$

4. Immediate from Part (3) and multiplicative idempotence of tests.

□

As another application of the algebra we show that, without any other assumption, negative introspection is preserved by transitive closure (for positive introspection this is trivial, since that property is equivalent to transitivity, so that transitive closure does not add anything).

LEMMA 3.8. *If a is m-euclidean then so is a^+.*

Proof. We calculate

$$\begin{array}{ll} & \langle a^+ \rangle [a^+]p \leq [a^+]p \\ \Leftarrow & \quad \{\![\text{ plus induction (17) }]\!\} \\ & \langle a \rangle [a^+]p \leq [a^+]p \\ \Leftrightarrow & \quad \{\![\text{ shunting }]\!\} \\ & \langle a^+ \rangle \neg p \leq [a]\langle a^+ \rangle \neg p \\ \Leftarrow & \quad \{\![\text{ plus induction (16) }]\!\} \\ & \langle a \rangle \neg p + \langle a \rangle [a]\langle a^+ \rangle \neg p \leq [a]\langle a^+ \rangle \neg p \\ \Leftarrow & \quad \{\![\text{ supremum }]\!\} \\ & \langle a \rangle \neg p \leq [a]\langle a^+ \rangle \neg p \ \wedge \\ & \langle a \rangle [a]\langle a^+ \rangle \neg p \leq [a]\langle a^+ \rangle \neg p \ . \end{array}$$

The first of these conjuncts follows from the second form of the m-euclidean property of a and $a \leq a^+$, together with isotony of diamond in its first argument (5) and of box in its second argument (6). The second conjunct is immediate from the first form of the m-euclidean property. □

4. KNOWLEDGE ALGEBRA

4.1. Common Knowledge

Using our modal operators we can now model common knowledge over a modal weak semiring S as follows. Assume a finite set of agents, represented by an index set $I = \{1, \ldots, n\}$, each with an access element $a_i \in S$.

As detailed in Section 2, for the case of Kripke structures with access relations R_i, the knowledge operators for the agents would be $[R_i]$. Therefore, in the abstract algebraic setting we define, analogously, $\mathsf{K}_i =_{df} [a_i]$.

An *agent group* is a subset $G \subseteq I$. We introduce two operators for expressing common knowledge:

- $\mathsf{E}_G p$: everyone in group G knows p;
- $\mathsf{C}_G p$: everyone in G knows that everyone in G knows that ... everyone in G knows p.

Using antidisjunctivity (4) of box we calculate, for $G = \{k_1, \ldots, k_m\}$,

$$\begin{array}{rcl} \mathsf{E}_G p & = & \mathsf{K}_{k_1} p \cdot \cdots \cdot \mathsf{K}_{k_m} p \;=\; [a_{k_1}]p \cdot \cdots \cdot [a_{k_m}]p \\ & = & [a_{k_1} + \cdots + a_{k_m}]p \;=\; [a_G]p \;, \end{array}$$

where $a_G =_{df} a_{k_1} + \cdots + a_{k_m}$.

Likewise, using the composition axiom (box2) and again antidisjunctivity (4) of box, we obtain, semi-formally,[1]

$$\begin{array}{rcl} \mathsf{C}_G p & = & \mathsf{E}_G p \cdot \mathsf{E}_G \mathsf{E}_G p \cdot \mathsf{E}_G \mathsf{E}_G \mathsf{E}_G p \cdot \cdots \\ & = & [a_G]p \cdot [a_G][a_G]p \cdot [a_G][a_G][a_G]p \cdot \cdots \\ & = & [a_G]p \cdot [a_G \cdot a_G]p \cdot [a_G \cdot a_G \cdot a_G]p \cdot \cdots \\ & = & [a_G + a_G^2 + a_G^3 \cdots]p \;. \end{array}$$

Therefore we define $\mathsf{C}_G p =_{df} [a_G^+]p$ if the underlying i-semiring is a Kleene algebra.

In this way we have obtained an algebraic counterpart of the multiagent logic KT45^n (e.g. [9]) and a fragment of Public Announcement Logic [27, 28].

4.2. Knowledge Laws

We shall now derive a number of laws for our knowledge operators that will come in handy in solving the Wise Men Puzzle and, later on, also the Muddy Children Puzzle.

First, from antitony of box in its first argument we get, since $a_{k_j} \leq a_G \leq a_G^+$,

$$\mathsf{C}_G p \leq \mathsf{E}_G p \leq \mathsf{K}_{k_j} p \qquad \mathsf{C}_G p \leq \mathsf{C}_G \mathsf{K}_{k_j} p \;. \tag{19}$$

For the remaining laws of this section we shall consider the agent group G and its access element fixed and just write $a, \mathsf{E}, \mathsf{C}$ instead of $a_G, \mathsf{E}_G, \mathsf{C}_G$.

By $a^+ \cdot a^+ \leq a^+$, again antitony of box in its first argument and Axiom (box2) we have

$$\mathsf{C}p = [a^+]p \leq [a^+ \cdot a^+]p = [a^+][a^+]p = \mathsf{CC}p \;,$$

i.e., C is transitive in the sense of knowledge operators:

$$\mathsf{C}p \leq \mathsf{CC}p \;. \tag{20}$$

From this we obtain two further properties that will be useful in the solution of the wise men puzzle:

$$\mathsf{C}p \cdot \mathsf{C}q \leq \mathsf{C}(\mathsf{C}p \cdot \mathsf{C}q) \;, \qquad \mathsf{C}p \cdot \mathsf{C}q \leq \mathsf{C}(\mathsf{C}p \cdot q) \tag{21}$$

They are shown, using conjunctivity, transitivity and conjunctivity of C again, by

$$\mathsf{C}p \cdot \mathsf{C}q = \mathsf{C}(p \cdot q) \leq \mathsf{CC}(p \cdot q) = \mathsf{C}(\mathsf{C}p \cdot \mathsf{C}q)$$

and, using transitivity and conjunctivity of C, by

$$\mathsf{C}p \cdot \mathsf{C}q \leq \mathsf{CC}p \cdot \mathsf{C}q = \mathsf{C}(\mathsf{C}p \cdot q) \;.$$

All our properties up to here hold irrespective of the knowledge axioms. Let us see what can be derived when some of these axioms are assumed.

If all K_i are reflexive (i.e., satisfy Axiom (T)) then so is E and hence $\mathsf{C} = [a^+] = [a^*]$. Therefore the general induction rule (18) specialises to the knowledge induction rule

$$\mathsf{C}(p \to \mathsf{E}p) \leq p \to \mathsf{C}p \;.$$

It means that if all agents in G know that p is invariant under E_G and p is true then all agents know they all know p. Moreover, (box2) and a star property yield

$$\mathsf{CC}p = [a^*][a^*]p = [a^* \cdot a^*]p = [a^*]p = \mathsf{C}p$$

and hence, by conjunctivity of C,

$$\mathsf{C}p \cdot \mathsf{C}q = \mathsf{CC}p \cdot \mathsf{CC}q = \mathsf{C}(\mathsf{C}p \cdot \mathsf{C}q) \;. \tag{22}$$

5. SOLVING THE WISE MEN PUZZLE

Let us now solve the Wise Men Puzzle using our encoding in the terminology of modal weak semirings.

With our algebraic definitions we can rephrase the assumptions from Section 2 in abstract algebraic form (the indices of C and E are suppressed, since always the full group of all three agents is referred to):

(a)	$\models \mathsf{C}(r_i \to \mathsf{K}_j r_i)$	$(j < i)$,
(b)	$\models \mathsf{C}(\neg r_i \to \mathsf{K}_j \neg r_i)$	$(j < i)$,
(c)	$\models \mathsf{C}(r_1 + r_2 + r_3)$,	
(d)	$\models \mathsf{C}(\neg \mathsf{K}_i r_i)$	$(i = 1, 2)$,
(e)	$\models \mathsf{C}(\neg \mathsf{K}_i \neg r_i)$	$(i = 1, 2)$.

Now, first the formulas (c) and (d) invite an application of modal modus tollens (10) from Section 3.4; afterwards the contrapositive $\neg K_j \neg r_i \to r_i$ of the formula within (b) can be used. We just have to wrap the corresponding inferences into applications of the common knowledge operator C. More precisely, for arbitrary agent number i and arbitrary tests p and q we can reason as follows:

[1] This notation is semi-formal, since general infinite products and sums need not exist in every left i-semiring; even if this particular one exists, it need not coincide with a_G^+.

$$
\begin{array}{ll}
& \mathsf{C}(p+q)\cdot\mathsf{C}(\neg\mathsf{K}_i p)\cdot\mathsf{C}(\neg\mathsf{K}_i\neg q\to q)\\
\leq & \quad \{\!\!\{ \text{ by (21) twice } \}\!\!\}\\
& \mathsf{C}(\mathsf{C}(p+q)\cdot\neg\mathsf{K}_i p\cdot(\neg\mathsf{K}_i\neg q\to q))\\
\leq & \quad \{\!\!\{ \text{ common knowledge (19) and isotony of } \mathsf{C} \}\!\!\}\\
& \mathsf{C}(\mathsf{K}_i(p+q)\cdot\neg\mathsf{K}_i p\cdot(\neg\mathsf{K}_i\neg q\to q))\\
\leq & \quad \{\!\!\{ \text{ by (K}') \text{ and isotony of } \mathsf{C} \}\!\!\}\\
& \mathsf{C}(\neg K_i\neg q\cdot(\neg\mathsf{K}_i\neg q\to q))\\
\leq & \quad \{\!\!\{ \text{ Boolean algebra (modus ponens) } \}\!\!\}\\
& \mathsf{C}(q)\ .
\end{array}
$$

In sum, we have shown the following lemma:

LEMMA 5.1 (Knowledge Strengthening). *Assume a group of agents indexed by some family I and consider an $i\in I$ and arbitrary tests p,q. Then*

$$\mathsf{C}_I(p+q)\cdot\mathsf{C}_I(\neg\mathsf{K}_i p)\cdot\mathsf{C}_I(\neg q\to\mathsf{K}_i\neg q)\ \leq\ \mathsf{C}_I(q)\ .$$

To make progress in the puzzle, we want to apply this lemma first for $p=r_1$ and $q=r_2+r_3$ and assumption (d) with $i=1$. Therefore we have to obtain information about $\mathsf{C}_I(\neg q\to\mathsf{K}_1\neg q)$. We calculate

$$
\begin{array}{ll}
& \mathsf{C}(\neg(r_2+r_3)\to\mathsf{K}_1\neg(r_2+r_3))\\
= & \quad \{\!\!\{ \text{ de Morgan } \}\!\!\}\\
& \mathsf{C}((\neg r_2\cdot\neg r_3)\to\mathsf{K}_1(\neg r_2\cdot\neg r_3))\\
= & \quad \{\!\!\{ \text{ conjunctivity of } \mathsf{K}_j \}\!\!\}\\
& \mathsf{C}((\neg r_2\cdot\neg r_3)\to(\mathsf{K}_1\neg r_2\cdot\mathsf{K}_1\neg r_3))\\
\geq & \quad \{\!\!\{ \text{ Boolean algebra and isotony of } \mathsf{C} \}\!\!\}\\
& \mathsf{C}((\neg r_2\to\mathsf{K}_1\neg r_2)\cdot(\neg r_3\to\mathsf{K}_1\neg r_3))\\
= & \quad \{\!\!\{ \text{ conjunctivity of } \mathsf{C} \}\!\!\}\\
& \mathsf{C}(\neg r_2\to\mathsf{K}_1\neg r_2)\cdot\mathsf{C}(\neg r_3\to\mathsf{K}_1\neg r_3)\ .
\end{array}
$$

Hence our assumptions and property (7) indeed entail $\mathsf{C}_I(\neg q\to\mathsf{K}_1\neg q)$ and hence, by Lemma 5.1 also

$$\mathsf{C}(r_1+r_2+r_3)\ \leq\ \mathsf{C}(r_2+r_3)\ \wedge\ \mathsf{C}(r_2+r_3)\ \leq\ \mathsf{C}(r_3)\ .$$

Finally, by the common knowledge law (19) we infer $\mathsf{C}(r_3)\leq\mathsf{K}_3(r_3)$. Since $\models\mathsf{C}(r_1+r_2+r_3)$ by Formula (1), we also have, using assumption (b), that $\models\mathsf{K}_3(r_3)$, which means that the third wise man knows his hat is red. Hence the puzzle is solved, because the King's question can now be answered in the affirmative. Note that assumption (a) was not used in this derivation.

We think that this algebraic solution is much more concise than standard treatments in multimodal logic with a natural deduction system (e.g. [29]). Moreover, the algebraic axiomatisation is completely first-order. Hence it can be treated by off-the-shelf fully automatic provers without specialising them in any way for the modal case.

The above derivation can be generalised to a group $G\subseteq I$ of agents and an index $j\in I$, which yields

$$\prod_{i\in G}\mathsf{C}(\neg r_i\to\mathsf{K}_j\neg r_i)\ \leq\ \mathsf{C}(\neg(\sum_{i\in G}r_i)\to\mathsf{K}_j\neg(\sum_{i\in G}r_i))\ .$$

Similarly, the whole solution easily generalises to n instead of three wise men. In fact, one can give a closed form of the generalised argument. Assume an agent group G and a subgroup $H\subseteq G$ of agents who have already been interrogated and have denied knowledge of their hat colour. Then

$$\mathsf{C}(\sum_{j\in G}r_j)\cdot\mathsf{C}(\prod_{i\in H}\neg\mathsf{K}_i r_i)\cdot\mathsf{C}(\prod_{i\in H}\prod_{j\in G-H}r_j\to\mathsf{K}_i r_j)\leq \mathsf{C}(\sum_{j\in G-H}r_j)\ .$$

Note that we have assumed neither reflexivity nor positive/negative introspection for the knowledge modalities; only transitivity of C and axiom K were used. Moreover, axiom M was not used either, which is why the assumption of a modal weak semiring was sufficient.

One may well argue that all this could have been done in conventional modal logic. This is true; however, our derivations work not only in relational Kripke models but just the same in many other models of modal semirings, such as algebras of traces and trajectories, to name just the most important ones. This will be fruitful, e.g., for combinations of temporal and epistemic logic, such as [30, 31]. However, the details will be the subject of further research.

6. THE MUDDY CHILDREN

The arguments of the previous section can be reused for puzzles with a similar structure, like the Surprise Examination Paradox [28] or the Muddy Children Puzzle (e.g. [9]), which add several rounds of interrogation of the above shape. Let us treat the latter as a somewhat more complicated example.

There are n children together in a playground. They have been told that they must not get dirty. However, during their play k of them get mud on their foreheads. Each can see the mud on the foreheads of others but not on her own. After a while a passer-by says to them "At least one of you has mud on her forehead". He then repeatedly asks "Does any one of you know whether you are muddy?" What will eventually happen if it is assumed that all the children are perceptive, intelligent, truthful and answer simultaneously after each repetition of the question?

For the case of n children we use the index set $I=\{1,\ldots,n\}$. Then we see immediately that we have a quite similar set of initial assumptions as for the Wise Men, where m_i now means that child i is muddy:

(a) $\models\mathsf{C}(m_i\to\mathsf{K}_j m_i)\qquad(j\neq i)$,

(b) $\models\mathsf{C}(\neg m_i\to\mathsf{K}_j\neg m_i)\quad(j\neq i)$,

(c) $\models\mathsf{C}(\sum_{i\in I}m_i)$.

Contrary to the Wise Men, the situation here is fully symmetric.

Assume now that after the first question all children simultaneously answer "no". Then we have the additional information

(d) $\models \mathsf{C}(\neg \mathsf{K}_i m_i) \qquad (i \in I)$.

This is again similar to the Wise Men case.

Set now, for $l \in [1,n]$,

$$\begin{aligned} \mathsf{dontknow}_l &=_{df} \prod_{G \subseteq I \wedge |G|=l} \prod_{i \in G} \neg \mathsf{K}_i m_i \ , \\ \mathsf{seecleans} &=_{df} \prod_{i \neq j} (\neg m_j \to \mathsf{K}_i \neg m_j) \ . \end{aligned}$$

Hence $\mathsf{dontknow}_l$ expresses that in every group of l children none of them knows whether she is muddy, while $\mathsf{seecleans}$ means that each child knows whether the others are clean. Assumptions (a) and (b) together with conjunctivity of C imply $\models \mathsf{C}(\mathsf{seecleans})$. With this we can calculate as follows:

$$\begin{aligned} & \mathsf{C}(\sum_{i \in I} m_i) \cdot \mathsf{C}(\mathsf{dontknow}_1) \cdot \mathsf{C}(\mathsf{seecleans}) \\ = \quad & \{\!\!\{ \text{ definition of } \mathsf{dontknow}_1, \text{ index chasing } \}\!\!\} \\ & \mathsf{C}(\sum_{i \in I} m_i) \cdot \mathsf{C}(\prod_{i \in I} \neg \mathsf{K}_i m_i) \cdot \mathsf{C}(\mathsf{seecleans}) \\ \leq \quad & \{\!\!\{ \text{ using conjunctivity of } \mathsf{C} \text{ and Lemma 5.1} \\ & \quad \text{for every } i \in I \ \}\!\!\} \\ & \prod_{i \in I} \mathsf{C}(\sum_{j \neq i} m_j) \\ = \quad & \{\!\!\{ \text{ by conjunctivity of } \mathsf{C} \ \}\!\!\} \\ & \mathsf{C}(\prod_{i \in I} \sum_{j \neq i} m_j) \\ = \quad & \{\!\!\{ \text{ Boolean algebra } \}\!\!\} \\ & \mathsf{C}(\sum_{j \neq i} m_i \cdot m_j) \end{aligned}$$

The test $\sum_{j \neq i} m_i \cdot m_j$ is valid iff at least 2 of the m_i are valid. This means that after the first round of questioning with uniformly negative answers all children know that at least two of them are muddy.

Define now, for $G \subseteq I$,

$$\mathsf{muddy}_G =_{df} \prod_{i \in G} m_i \ , \qquad \mathsf{clean}_G =_{df} \prod_{i \in G} \neg m_i$$

Then the group of muddy children is uniquely characterised by

$$\mathsf{mset}_G =_{df} \mathsf{muddy}_G \cdot \mathsf{clean}_{I-G} \ .$$

The fact that at least n children are muddy is formalised, for $l \in [1,n]$, by

$$\mathsf{atleast}_l =_{df} \sum_{G \subseteq I \wedge |G|=l} \mathsf{muddy}_G = \sum_{G \subseteq I \wedge |G| \geq l} \mathsf{muddy}_G \ .$$

In sum, the above derivation shows

$$\mathsf{C}(\mathsf{atleast}_1) \cdot \mathsf{C}(\mathsf{dontknow}_1) \cdot \mathsf{C}(\mathsf{seecleans}) \leq \mathsf{C}(\mathsf{atleast}_2) \ .$$

An easy induction using again Lemma 5.1 shows, for $1 \leq j < n$, that

$$\mathsf{C}(\mathsf{atleast}_j) \cdot \mathsf{C}(\mathsf{dontknow}_l) \cdot \mathsf{C}(\mathsf{seecleans}) \leq \mathsf{C}(\mathsf{atleast}_{l+1}) \ .$$

The remaining part of the solution uses the following observation: if a child m_i knows that there are at least l muddy children but sees only $l-1$ she must conclude that she herself is muddy, too. This conclusion is expressed by the following formula for $i \in I$ and $l \in [2,n]$:

$$\mathsf{concl}_{i,l} =_{df} \mathsf{atleast}_l \cdot \mathsf{seesmuddy}_{i,l-1} \to m_i \ ,$$

where

$$\mathsf{seesmuddy}_{i,l} =_{df} \sum_{G \subseteq I \wedge |G|=l \wedge i \notin G} \mathsf{muddy}_G \cdot \mathsf{clean}_{I-(G \cup \{i\})}$$

expresses that child i sees at least one group of l muddy children other than herself. Validity of $\mathsf{concl}_{i,j}$ is immediate from the definitions by Boolean algebra, so that by property (7) of C we may infer

$$\models \mathsf{C}(\mathsf{concl}_{i,j}) \ . \tag{23}$$

Now we reason as follows, assuming that $G \subseteq I$ is the group of muddy children, uniquely characterised by mset_G, and $k = |G|$. Then we have, for every $i \in G$, that $\models \mathsf{seesmuddy}_{i,k-1}$ and hence, again by (7), $\models \mathsf{C}(\mathsf{seesmuddy}_{i,k-1})$. According to the above induction we infer $\models \mathsf{C}(\mathsf{atleast}_k)$. Now modal modus ponens (9) using (23) and knowledge algebra yield the implications

$$\mathsf{C}(\mathsf{atleast}_k) \cdot \mathsf{C}(\mathsf{seesmuddy}_{i,k-1}) \ \leq \ \mathsf{C}(m_i) \ \leq \ K_i m_i \ ,$$

so that indeed after $k-1$ rounds of questioning all muddy children know that they are muddy. In fact, this is even common knowledge.

Note that the knowledge axioms of reflexivity and introspection as well as axiom M again have not been used, so that the whole solution goes through assuming only transitivity of C and Property (9); these properties come for free from the algebraic definition of C.

The approach works, because this type of puzzle has a "purely logical" structure. Contrarily, any analytical solution of the puzzle about Mr. S and Mr. P [15, 27, 32] (i.e., any solution by logical deduction and not by exhaustive checking of all pairs of numbers within the given range) will involve a lot of domain logic about arithmetic in addition to the logic of mutual knowledge of the agents about each other; therefore the abstract algebraic reasoning will cover only the overall structure of the solution, whereas the arithmetic details will take place within the test set of a particular semiring.

7. KNOWLEDGE PROPAGATION AND KNOWLEDGE UPDATE

7.1. Knowledge Propagation

We will now turn to another view of puzzles of the above type. Rather than accumulating knowledge about one and the same fixed Kripke structure we will increase knowledge by shrinking the initial Kripke structure until only worlds remain that are in some sense "interesting" for the solution. We will see that the modal semiring setting immediately allows knowledge

update operators as in e.g. [33] without adding any further axioms.

To illustrate this we sketch a particular Kripke structure for the Muddy Children Puzzle. As worlds in this structure we use minterms as known from the Boolean normal form of logical assertions. Again, let $I = \{1, \ldots, n\}$ be the index set for the case of n children. For $G \subseteq I$ the *minterm*

$$m_G =_{df} (\prod_{i \in G} m_i) \cdot (\prod_{i \in I-G} \neg m_i)$$

expresses that exactly the children in group G are muddy. Moreover, we say that world w satisfies a test q of the form m_i or $\neg m_i$, in symbols $w \models q$, iff $\models w \to q$.

Since no child i can see herself, she cannot distinguish between worlds that are identical except for the value of m_i. This induces as access relation the equivalence

$$w \sim_i w' \Leftrightarrow_{df} w' = w \vee w' = \mathit{flip}_i(w) \ ,$$

where $\mathit{flip}_i(m_G) =_{df} m_{G\Delta\{i\}}$ and the operator Δ forms the symmetric difference of sets, i.e., $F\Delta G = (F - G) \cup (G - F)$. As an equivalence, $\sim$ is reflexive and satisfies positive and negative introspection.

To solve the puzzle in a different way, we want to end up with a reduced Kripke structure in which for the actually muddy children only a single accessible world remains so that for them knowledge is complete.

Since we now have to work with knowledge in different structures, we have to give up the convenient operators $\mathsf{K}, \mathsf{E}, \mathsf{C}$ and to revert to the general box notation.

Shrinking a Kripke structure can be expressed through restricting access elements by tests. If the original access element was a we would now, e.g. like to consider only $a \cdot p$ where p is a test. This preserves only those transitions in a that lead into worlds satisfying p.

By antitony of box in its first argument (5), restricting an access element implies knowledge preservation: Since $p \leq 1$ implies $a \cdot p \leq a$, we have

$$\forall\, q : [a]q \ \Rightarrow\ [a \cdot p]q \ ,$$

i.e., in a restricted structure the knowledge of the original structure is preserved and possibly extended.

Moreover, by Axiom (box2) and the explicit form of the box of a test (8) there is an interplay between restriction and implication

$$[a](p \to q) \ =\ [a \cdot p]q \ . \tag{24}$$

Let us now, conversely, see how knowledge about a certain property q can be preserved when the relevant accessible worlds are restricted by a test p. Assume the underlying modal semiring to be weak. Then

$$\begin{array}{ll} & [a]q \\ = & \quad \{\![\text{ neutrality }]\!\} \\ & [a \cdot 1]q \\ = & \quad \{\![\text{ complements }]\!\} \\ & [a \cdot (p + \neg p)]q \\ = & \quad \{\![\text{ distributivity }]\!\} \\ & [a \cdot p + a \cdot \neg p]q \\ = & \quad \{\![\text{ antidisjunctivity }]\!\} \\ & [a \cdot p]q \cdot [a \cdot \neg p]q \\ = & \quad \{\![\text{ by (24) }]\!\} \\ & [a \cdot p]q \cdot [a](\neg p \to q) \ . \end{array}$$

If we now can show that $[a](\neg p \to q) = 1$ then $[a]q = [a \cdot p]q$.

This is summarised by

LEMMA 7.1 (Knowledge Propagation).

$$\models [a](\neg p \to q) \ \Rightarrow\ [a]q = [a \cdot p]q \ .$$

As an example, for three Muddy Children we have for all $i \in \{1, 2, 3\}$, by Boolean algebra,

$$\mathsf{C}(m_1 + m_2 + m_3) \ =\ \mathsf{C}(\neg(\neg m_1 \cdot \neg m_2) \to m_3) \leq \mathsf{K}_i(\neg(\neg m_1 \cdot \neg m_2) \to m_3) \ .$$

Hence $[a_i]m_3 \ =\ [a_i \cdot \neg m_1 \cdot \neg m_2]m_3$.

7.2. Public Announcement

In the *public announcement* (e.g. [27, 12, 34]) of a property p one makes sure that all agents henceforth know p. This can be realised in various ways.

For instance, the semantics of $\mathit{Pub}\, p$ in [12] corresponds to changing an access element a to $a \cdot p$. Therefore the knowledge propagation rule (24) applies; it is called "atomic permanence" in [12]. In fact, the operator $[\mathit{Pub}\, p]$ there largely behaves like $[p]$. With this, the Action-Knowledge and Partial Functionality axioms of [12] translate into[2]

$$\begin{array}{rl} [p][a]q & =\ p \to [a][p]q \ , \\ [p]\neg q & =\ p \to \neg[p]q \ . \end{array}$$

Using (8) and (box2), the first of these compacts into

$$[p \cdot a]q \ =\ [p \cdot a \cdot p]q \ .$$

For the second one we calculate, using again (8), the definition of $\to$ and Boolean algebra,

$$p \to \neg[p]q \ =\ p \to \neg(p \to q) \ =\ p \to \neg q \ =\ [p]\neg q \ ,$$

so that in the modal semiring setting this is a theorem rather than an axiom. A more detailed analysis is beyond the scope of this paper.

Another possibility would be to use the smaller restriction $p \cdot a \cdot p$ as the definition of the public announcement of p in access element a; this would eliminate the need for the Action-Knowledge axiom.

Restriction is particularly well-behaved if the access element a under consideration is m-symmetric, since we

[2] I am grateful to one of the referees for pointing that out.

know from Lemma 3.7(1) that then $p \cdot a \cdot p$ is symmetric again. Moreover, axiom (box2) and the explicit form (8) of box for tests imply

$$[p \cdot a \cdot p]q \;=\; p \to [a](p \to q) \;.$$

Hence, in a modal semiring we have

$$\models p \to q \;\Rightarrow\; \models [p \cdot a \cdot p]q$$

which implies

$$\models [p \cdot a \cdot p]p \;. \tag{25}$$

Note that p here is a semantic value and not a formula; otherwise this law would not be valid, as the discussion on (un)successful updates in [27, 34] shows. In fact, so far we have refrained from giving a syntax.

One can do this using a set Π of propositional atoms and again a finite index set $I = \{1, \ldots, n\}$. Then the set Φ of *propositions* is defined by the grammar

$$\Phi ::= \Pi \,|\, \neg\Phi \,|\, \Phi \wedge \Phi \,|\, \mathsf{K}_i\Phi \,|\, \mathsf{E}\Phi \,|\, \mathsf{C}\Phi \,|\, \Phi!\Phi \;,$$

where i ranges over I. (We use the notation $\varphi!\psi$ rather than $\varphi+\psi$ of [27] or $[\varphi]\psi$ of [34] to avoid confusion with the $+$ and box of modal semirings.)

To define a semantics for these formulas over a modal semiring S we choose an access element $a_i \in S$ for every $i \in I$ and a test $\hat{\pi} \in \mathsf{test}(S)$ for every $\pi \in \Pi$. Moreover, we again set $a_I =_{df} a_1 + \cdots + a_n$. The semantics $[\![\varphi]\!]_q \in \mathsf{test}(S)$ is parameterised by a test q that determines the subset of possible worlds w.r.t. which φ is evaluated. The semantic clauses corresponding to the approach of [34] read as follows.

$$\begin{array}{ll}
[\![\pi]\!]_q & =_{df}\; \hat{\pi} \cdot q \;, \\
[\![\neg\varphi]\!]_q & =_{df}\; q - [\![\varphi]\!]_q \;, \\
[\![\varphi \wedge \psi]\!]_q & =_{df}\; [\![\varphi]\!]_q \cdot [\![\psi]\!]_q \;, \\
[\![\mathsf{K}_i\varphi]\!]_q & =_{df}\; [q \cdot a_i \cdot q][\![\varphi]\!]_q \;, \\
[\![\mathsf{E}\varphi]\!]_q & =_{df}\; [q \cdot a_I \cdot q][\![\varphi]\!]_q \;, \\
[\![\mathsf{C}\varphi]\!]_q & =_{df}\; [(q \cdot a_I \cdot q)^+][\![\varphi]\!]_q \;, \\
[\![\varphi!\psi]\!]_q & =_{df}\; u \to [\![\psi]\!]_{q \cdot u} \text{ where } u =_{df} [\![\varphi]\!]_q \;.
\end{array}$$

Based on this relative semantics we can define the absolute semantics $[\![\varphi]\!]$ as

$$[\![\varphi]\!] =_{df} [\![\varphi]\!]_1 \;.$$

From this definition it is clear that in a formula $(\mathsf{K}\varphi)!(\mathsf{K}\varphi)$ the two occurrences of $\mathsf{K}\varphi$ may be evaluated in different substructures and hence yield different tests, in which case Law (25) does not apply. This is what is referred to as unsuccessful update in [27, 34]: a formula may become false after publicly announcing it. The classical example for this is the Moore sentence "π is true and you don't know this" [35].

A different approach to modelling public announcement of a test p is to remove all links between p-worlds and $\neg p$-worlds. In [13] the corresponding operator $!p$ is explained in two ways:

- Satisfaction of $[!p]q$ in a frame is defined as satisfaction of q in a modified frame.
- The semantics is again given in a PDL-like fashion, making the new access relation explicit in the first argument of box.

We can represent the latter approach directly in our setting by defining the modification of access element a_i as $a_i!p =_{df} p \cdot a_i \cdot p + \neg p \cdot a_i \cdot \neg p$.

The advantage of our approach is that in both cases we can just use the same algebraic laws as before and do not need to invent special inference rules for the announcement operators.

In the literature there are many more logics dealing with knowledge or belief revision. We are convinced that a large portion of these can be treated uniformly in the setting of modal semirings. For a related approach see [36], where belief update is modelled using semiring concepts. That paper enriches test semirings with a special operator for belief revision (where beliefs are represented as tests). It presents an axiomatisation of that operator which entails the standard AGM axioms [37]. Contrarily, our aim was to show that already the general concept of modal semirings is adequate.

7.3. Preferences and Their Upgrade

We now return to our general setting of modal semirings; in particular we assume neither of the axioms (T), (PI) or (NI). Let us briefly show how one can reason about other aspects of knowledge and belief. Some agent logics allow expressing preferences between possible worlds (e.g. [13]).

Since we are completely free in choosing our access elements, we can also include these. To this end we equip each agent i with her own preference relation $\preceq_i$. The intention is that $[\preceq_i]p$ holds in a world w iff p holds in all worlds w' that agent i prefers over w under $\preceq_i$, i.e., for which $w \preceq_i w'$.

Usually one requires that $\preceq_i$ be a preorder, modally,

$$[\preceq_i]p \leq p \;, \qquad [\preceq_i]p \leq [\preceq_i][\preceq_i]p \;.$$

Antisymmetry is not required: if $w_1 \preceq_i w_2 \wedge w_2 \preceq_i w_1$ then agent i is *indifferent* about w_1 and w_2 .

Using the preference concept, one can, e.g., model *regret* [13]: the formula $\mathsf{K}_i\neg p \wedge \langle\preceq_i\rangle p$ expresses that although agent i knows that p is not true, she would still prefer a world where it would be.

A preference agent system can be updated in various ways. In *belief revision* agents may discard or add links to epistemic neighbour worlds. We model the two possibilities presented in [13] in our agent algebra.

Another change operation is *preference upgrade* by *suggesting* that p be observed. This affects the preference relations, not the accessibilities:

$$p\#\preceq_i =_{df} p \cdot \preceq_i \cdot p + \neg p \cdot \preceq_i \;.$$

Now agent i no longer prefers $\neg p$ worlds over p ones.

PART II: GAMES AND PREDICATE TRANSFORMERS

In this part we return to the case of modal left semirings.

8. GAMES AND THEIR ALGEBRA

The algebraic description of two-player games dates back at least to [38]; for a more recent survey see [10]. The idea is to use a predicate transformer semantics that is a variant of (a μ-calculus-like enrichment of) PDL.

The starting point is, however, a slightly different relational model. It does not use relations of type $\mathcal{P}(W \times W)$, where the set of worlds W consists of the game positions and $\mathcal{P}$ is the power set operator, but rather of type $\mathcal{P}(W \times \mathcal{P}(W))$. A pair (s, X) in relation R models that the player whose turn it is has a strategy to move from starting position s into a position in set X. To make this well-defined, R has to be $\subseteq$-*isotone* in its second argument:

$$(s, X) \in R \wedge X \subseteq Y \Rightarrow (s, Y) \in R \ .$$

This type of structure is similar to the so-called minimal models used in the semantics of non-normal logics [39] and has been rediscovered under the name of "upclosed multirelations". Now again, sets of worlds are identified with predicates over worlds. As pointed out in [38], such a relation R induces an isotone predicate transformer $\rho(R) : \mathcal{P}(W) \to \mathcal{P}(W)$ via $\rho(R)(X) =_{df} \{s \mid (s, X) \in R\}$. It is easy to check that the set of $\subseteq$-isotone relations is isomorphic to that of isotone predicate transformers (the latter ordered by pointwise relational inclusion).

The basic operations to build up more complex games from atomic ones (such as single moves) are choice, sequential composition, finite iteration and tests, which are also basic operations found in left i-semirings; also the axioms (see [10]) are exactly those for left i-semirings. There are no constants 0 and 1; but they could easily be added by the standard extension of semigroups to monoids. The only operation particular to game construction is *dualisation* in which the two players exchange their roles.

Since games can be viewed as isotone predicate transformers, we study these from a bit more abstract viewpoint in the next section. Based on that we will show that they form a modal left semiring with dualisation, i.e., an abstract algebraic model of games. We will also show how to add finite iteration.

9. PREDICATE TRANSFORMER SEMIRINGS

For our purposes, all that matters about $\mathcal{P}(W)$ is its structure as a Boolean algebra. Therefore we generalise as follows.

Definition 9.1. Given an arbitrary Boolean algebra B, a *predicate transformer* (over B) is a function $f : B \to B$. By id we denote the identity transformer and $\circ$ denotes function composition.

As in Section 3 we denote the meet, join and complementation operators of B by $\cdot$, $+$ and $\neg$, the least and greatest elements by 0 and 1. This makes B a modal i-semiring with $\mathsf{test}(B) = B$ and $\langle p \rangle q = p \cdot q$ by (8).

Definition 9.2. Consider a predicate transformer $f : B \to B$ over a Boolean algebra B.

1. If for all $p, q \in B$ with $p \leq q$ we have $f(p) \leq f(q)$ then f is *isotone*.
2. f is *disjunctive* if $f(p + q) = f(p) + f(q)$ and *conjunctive* if $f(p \cdot q) = f(p) \cdot f(q)$.
3. f is *strict* if $f(0) = 0$ and *co-strict* if $f(1) = 1$.

Let $\mathrm{PT}(B)$, $\mathrm{ISO}(B)$, $\mathrm{CON}(B)$ and $\mathrm{DIS}(B)$ be the set of all, of isotone, of conjunctive and of disjunctive predicate transformers over B.

It is well known that conjunctivity and disjunctivity imply isotony. Under the pointwise ordering $f \leq g \Leftrightarrow_{df} \forall p \,.\, f(p) \leq g(p)$, PT forms a lattice where the join $f + g$ and meet $f \sqcap g$ of f and g are the pointwise liftings of $+$ and $\cdot$, respectively:

$$(f + g)(p) =_{df} f(p) + g(p) \ , \ (f \sqcap g)(p) =_{df} f(p) \cdot g(p) \ .$$

The least and greatest elements of $\mathrm{PT}(B)$ (and $\mathrm{ISO}(B)$ and $\mathrm{DIS}(B)$) are the constant functions $\mathbf{0}(p) =_{df} 0$ and $\top(p) =_{df} 1$. Note that $\mathbf{0}$ and $\top$ both are left zeros w.r.t. $\circ$. The substructure $(\mathrm{ISO}, +, \mathbf{0}, \circ, id)$ is a left i-semiring; the substructure $(\mathrm{DIS}(B), +, \mathbf{0}, \circ, id)$ is even a weak i-semiring. Likewise, the structure $(\mathrm{CON}(B), \sqcap, \top, \circ, id)$ is a weak i-semiring isomorphic to $\mathrm{DIS}(B)$, but with the mirror ordering [14]. The isomorphism is provided by the *duality operator* $^d : \mathrm{PT}(B) \to \mathrm{PT}(B)$, defined by $f^d(p) =_{df} \neg f(\neg p)$.

In the case where $B = \mathsf{test}(S)$ for some weak i-semiring S, the modal operator $\langle \_ \rangle$ provides a weak i-semiring homomorphism from S into $\mathrm{DIS}(B)$.

If B is a complete Boolean algebra then $\mathrm{PT}(B)$ is a complete lattice with $\mathrm{ISO}(B)$, $\mathrm{DIS}(B)$ and $\mathrm{CON}(B)$ as complete sublattices. Hence we can extend $\mathrm{ISO}(B)$ and $\mathrm{DIS}(B)$ by a star operator via a least fixpoint definition:

$$f^* =_{df} \mu(\lambda g \,.\, id + f \circ g) \ ,$$

where μ is the least-fixpoint operator. It has been shown in [20] that this satisfies the star laws. By passing to the mirror ordering, one sees that also the subalgebra of conjunctive predicate transformers can be made into a left Kleene algebra; this is essentially the approach taken in [14] (except for infinite iteration).

A useful consequence of the star induction rule is a corresponding one for the dual of a star, generalising (15):

$$h \leq g \sqcap f^d \circ h \ \Rightarrow \ h \leq (f^*)^d \circ g \ . \qquad (26)$$

Let us now connect this to game algebra. For a predicate transformer g we find in [38] the following two definitions concerning iterations (we use boldface stars and brackets here to distinguish Parikh's notation from ours):

$$\langle g^\star\rangle p \quad =_{df} \quad \mu(\lambda y\,.\,p + g(y))\ , \tag{27}$$

$$[g^\star]\,p \quad =_{df} \quad \nu(\lambda y\,.\,p \cdot g(y))\ , \tag{28}$$

where ν is the greatest-fixpoint operator. Hence $\langle g^\star\rangle$ in Parikh's notation coincides with g^* in ours. The defining functions of $\langle g^\star\rangle$ and $[g^\star]$ are de Morgan duals of each other; hence we can use the standard law $\nu f = \neg\,\mu f^d$ to calculate

$$\begin{array}{ll} & [g^\star]\,p \\ = & \quad \{\![\text{ definition (28) }]\!\} \\ & \nu(\lambda y\,.\,p \cdot g(y)) \\ = & \quad \{\![\text{ above fixpoint law }]\!\} \\ & \neg\mu(\lambda y\,.\,p \cdot g(y))^d \\ = & \quad \{\![\text{ definition of dual }]\!\} \\ & \neg\mu(\lambda y\,.\,\neg(p \cdot g(\neg y))) \\ = & \quad \{\![\text{ de Morgan }]\!\} \\ & \neg\mu(\lambda y\,.\,\neg p + \neg g(\neg y))) \\ = & \quad \{\![\text{ definition of dual }]\!\} \\ & \neg\mu(\lambda y\,.\,\neg p + g^d(y)) \\ = & \quad \{\![\text{ definition (27) }]\!\} \\ & \neg\,\langle (g^d)^\star\rangle\,\neg p \\ = & \quad \{\![\text{ above correspondence }]\!\} \\ & \neg\,(g^d)^*(\neg p) \\ = & \quad \{\![\text{ definition of dual }]\!\} \\ & ((g^d)^*)^d(p)\ . \end{array}$$

Thus, $[g^\star]$ coincides with $((g^d)^*)^d$. This shows that we can fully represent game algebra with finite iteration in modal left Kleene algebras; the standard star axioms for iteration suffice. If desired, one could also axiomatise the dual of the star using the dualised unfold axiom $(f^*)^d \;\leq\; 1 \sqcap f^d \circ (f^*)^d$ and (26) as the induction axiom.

Let us finally set up the connection with termination analysis. In [38] Parikh states that for concrete access relation R and the predicate transformer $g =_{df} [R]$ the predicate $\langle g^\star\rangle\,\mathsf{false}$ characterises the worlds from which no infinite access paths emanate. Plugging in the definitions for a general access element a and the predicate transformer $g =_{df} [a]$ we obtain

$$\langle g^\star\rangle 0 \;=\; \mu(\lambda y\,.\,[a]y)\ .$$

This coincides with the *halting predicate* of the propositional μ-calculus [18]; in the i-semiring setting it and its complement have been termed the *convergence* and *divergence* of a and used extensively in [40, 41]. They need not exist in arbitrary modal left semirings; rather they have to be axiomatised by the standard unfold and induction/co-induction laws for least and greatest fixpoints.

10. MODAL SEMIRINGS OF PREDICATE TRANSFORMERS AND DEMONIC REFINEMENT ALGEBRA

Although we have now seen a somewhat more abstract predicate transformer model of game algebra, we will take one step further and present a modal left Kleene algebra of isotone predicate transformers. This will link game semantics directly with refinement algebra.

First we want to characterise the tests in the set $\mathrm{ISO}(B)$. To this end we prove an auxiliary lemma about relative complements.

LEMMA 10.1. *Let p, q, r, s be elements of a Boolean algebra.*

1. *If $r \leq p \cdot q \wedge s \leq p \cdot \neg q \wedge r + s = p$ then $r = p \cdot q \wedge s = p \cdot \neg q$.*
2. *If $p \cdot q = p \cdot r$ then $p \cdot \neg q = p \cdot \neg r$.*

Proof.

1. Observe that $s \cdot q \leq p \cdot \neg q \cdot q = p \cdot 0 = 0$, i.e., $s \cdot q = 0$. Hence $p \cdot q = (r+s) \cdot q = r \cdot q + s \cdot q = r \cdot q \leq r$, which shows $r = p \cdot q$. Reasoning for s is symmetric.
2. $p = p \cdot q + p \cdot \neg q = p \cdot r + p \cdot \neg q$. Hence $p \cdot \neg r = p \cdot r \cdot \neg r + p \cdot \neg q \cdot \neg r = p \cdot \neg q \cdot \neg r \leq p \cdot \neg q$. Symmetrically one sees $p \cdot \neg q \leq p \cdot \neg r$.

□

Now we can show

LEMMA 10.2. *Let B be a Boolean algebra and $\mathrm{ISO}(B)$ its set of isotone predicate transformers as in Definition 9.1.*

1. *$f \in \mathsf{test}(\mathrm{ISO}(B)) \;\Leftrightarrow\; f(p) = p \cdot f(1)$.*
2. *If $B = \mathsf{test}(S)$ for some left i-semiring S then $\mathsf{test}(\mathrm{ISO}(B)) = \{\langle p\rangle \mid p \in B\}$.*

Proof.

1. ($\Leftarrow$) By definition, $f \leq id$. A straightforward calculation shows that $g(p) =_{df} p \cdot \neg f(1)$ is the complement of f relative to id.
   ($\Rightarrow$) Let $g \in \mathrm{ISO}(B)$ be the complement of $f \leq id$ relative to id, i.e., $f + g = id$ and $f \sqcap g = \mathbf{0}$. First, $f \leq id$ implies $f(p) \leq p$. Second, $f \in \mathrm{ISO}(B)$ means $f(p) \leq f(1)$. Hence $f(p) \leq p \cdot f(1)$. From $f + g = id$ we conclude $g(1) = \neg f(1)$ and hence, by symmetric reasoning, $g(p) \leq p \cdot \neg f(1)$. Since $f(p) + g(p) = p$, Lemma 10.1 shows the claim.
2. By Equation (8) and Part (1) we have for $f \in \mathsf{test}(\mathrm{ISO}(B))$ that $f = \langle f(1)\rangle$, which shows ($\subseteq$). The reverse inclusion is immediate from isotony of $\langle p\rangle$ as well as $p \leq 1$ and isotony of $\langle\_\rangle$.

□

Part (2) means that the tests in the i-semiring of isotone predicate transformers are precisely the diamonds of the elements of B (see Section 9).

Because of Part (1) and (8) we will, for convenience, denote mappings of the form $\lambda q \,.\, p \cdot q$ by $\langle p \rangle$ also in the general case of ISO(B). The proof also shows that $\neg\langle p\rangle = \langle \neg p\rangle$.

Now we are ready to enrich ISO(B) by box and diamond operators. To this end we work out what the right hand side of axiom (box1) means there:

$$\langle p\rangle \circ f \circ \neg\langle q\rangle \leq 0 \;\Leftrightarrow\; \forall\, r : p \cdot f(\neg q \cdot r) \leq 0 \;\Leftrightarrow\; p \cdot f(\neg q \cdot 1) \leq 0 \;\Leftrightarrow\; p \leq \neg f(\neg q) \;\Leftrightarrow\; p \leq f^d(q)\ ;$$

the second equivalence holds by isotony of f. So the only possible choice is

$$[f]\langle q\rangle \;=_{df}\; \langle f^d(q)\rangle\ , \qquad \langle f\rangle\langle q\rangle \;=_{df}\; \langle f(q)\rangle\ .$$

Let us check that this satisfies axiom (box2) as well:

$$[f \circ g]\langle q\rangle \;=\; \langle (f\circ g)^d(q)\rangle \;=\; \langle (f^d(g^d(q))\rangle \;=\; [f]\langle g^d(q)\rangle \;=\; [f][g]\langle q\rangle\ .$$

Hence box and diamond are well defined in ISO(B). In sum:

THEOREM 10.3. *For a Boolean algebra B the set* ISO(B) *with the above operations forms a modal left Kleene algebra with dualisation.*

This rounds off the picture in that now also the test operations of game algebra and PDL have become first-class citizens in predicate transformer algebra. Moreover, we can enrich that algebra by a domain operator which will provide the announced connection with refinement algebra.

As mentioned in Section 3.3, in a modal left semiring the *domain operator* [6] $\ulcorner : S \to \mathsf{test}(S)$ is given by $\ulcorner a =_{df} \langle a\rangle 1$. This characterises the set of starting worlds of access element a. For ISO(B) this works out to $\ulcorner f \;=\; \langle f(1)\rangle$. This expression coincides with that for the termination operator τf in the concrete model of *demonic refinement algebra (DRA)* given at the end of [14]. That algebra is an axiomatic algebraic system for dealing with predicate transformers under a demonic view of non-determinacy. However, τf is not a test (or *guard* [42]), but an *assumption* (unfortunately called "assertion" in [14]). These take the form $\neg p \cdot \top + 1$ where $\top$ is the greatest element (which always exists in DRA).

Besides τ (which is characterised by the domain axioms of [6]), DRA has an enabledness operator ϵ, defined by dual axioms in terms of guards.

Let us explain the relation between tests and assumptions. We first introduce a test-based conditional by

$$\mathsf{if}\, p \;\mathsf{then}\; a \;\mathsf{else}\; b \;\Leftrightarrow_{df}\; p \cdot a + \neg p \cdot b\ .$$

Using it, assertions and assumptions can be defined as

$$\begin{array}{lll} \mathsf{assert}\ p & =_{df} & \mathsf{if}\, p \;\mathsf{then}\; 1 \;\mathsf{else}\; 0 \\ \mathsf{assume}\ p & =_{df} & \mathsf{if}\, p \;\mathsf{then}\; 1 \;\mathsf{else}\; \top\ , \end{array}$$

the latter provided S has a greatest element $\top$. In an operational view, both constructs check whether p holds at the time of their execution. If so, they simply proceed (remember that 1 stands for the null action). If not, the assertion aborts while the assumption may do anything ($\top$ means the set of all possible choices, so we have the behaviour *ex falso quodlibet*).

Both expressions can be simplified. For assertions we obtain

$$\mathsf{assert}\ p \;=\; p \cdot 1 + \neg p \cdot 0 \;=\; p + 0 \;=\; p\ .$$

Hence the construct $\mathsf{assert}\ p$ could be omitted; we have introduced it just for symmetry. For assumptions we get, since $\neg p \cdot 1 \leq \neg p \cdot \top$,

$$\begin{array}{lll} \mathsf{assume}\ p & = & p \cdot 1 + \neg p \cdot \top \;=\; p \cdot 1 + \neg p \cdot 1 + \neg p \cdot \top \\ & = & (p + \neg p) \cdot 1 + \neg p \cdot \top \;=\; 1 + \neg p \cdot \top\ , \end{array}$$

which is the expression given above for assumptions.

Let us now see which elements of a set ISO(B) of isotone predicate transformers are assumptions in this sense:

$$(\langle \neg p\rangle \circ \top + id)(q) \;=\; \langle \neg p\rangle(\top(q)) + q \;=\; \langle \neg p\rangle 1 + q \;=\; \neg p + q \;=\; [p]q\ .$$

Written in point-free style, $\langle \neg p\rangle \circ \top + id = [p]$. So in ISO($B$) the assumptions are the de Morgan duals of the tests.

For the dual of the domain operator we obtain

$$(\ulcorner f)^d = \langle f(1)\rangle^d = [f(1)] = [f(\neg 0)] = [\neg f^d(0)]\ . \quad (29)$$

This latter expression coincides with that for $\epsilon(f^d)$ in the mentioned concrete model of [14], so that by $(g^d)^d = g$ we have the equation $\tau f = (\epsilon(f^d))^d$. Finally, it should be noted that the rightmost expression in (29) also corresponds to the *guard* $\neg\mathsf{wp}(a, \mathit{false})$ of [43], while that for τ coincides with the termination predicate $\mathsf{wp}(a, \mathit{true})$ there.

11. CONCLUSION AND OUTLOOK

We have shown that modal i-semirings and Kleene algebras form a comprehensive and flexible framework for handling various modal logics in a uniform algebraic fashion. We therefore think that the design of new modal systems geared toward special applications may benefit from using this algebraic approach.

An interesting approach, close in spirit, is [44], where modules over quantales are used to define an algebraic semantics of modal operators. However, having separate sorts for actions and (the equivalents of) tests makes that framework less flexible than ours, since those entities cannot be combined freely with the same operators. Moreover, the restriction to (full) quantales is less general than what the i-semiring framework offers.

One topic we have omitted from the present paper is that of infinite iteration. This has been treated

in [20]. However, there is a restriction. Although, over a complete Boolean algebra B, infinite iteration can be defined in $\mathrm{ISO}(B)$ as $f^\omega =_{df} \nu g \,.\, f \circ g$, this does not imply the usual omega coinduction law $c \leq a \cdot c + b \Rightarrow c \leq a^\omega + a^* \cdot b$ [4]. It only does so in the set $\mathrm{DIS}(B)$ of disjunctive predicate transformers over B. However, as stated in [10], disjunctivity is not a natural requirement for games. Future work will deal with a suitably revised axiomatisation of infinite iteration of games.

Further applications will concern the analysis of winning and losing positions (extending [45] and [5]).

Moreover, we will improve work on the automatic verification of properties in knowledge and game semirings using, e.g., the tools Prover9 and Mace4 [46] along the lines of [47]. While we have succeeded in an automatic verification of the Wise Men Puzzle in a simplified version, full automation of the solution in the present paper still faces performance problems which we hope to overcome by a modified axiomatisation.

Acknowledgments I am grateful to E. André for drawing my attention to the area of modal agent logics and to J. Desharnais, B. Dill, R. Glück, P. Höfner, H. Leiß, M.E. Müller, P. Roocks, K. Solin and the anonymous referees for many helpful comments and suggestions.

REFERENCES

[1] Möller, B. (2008) Knowledge and games in modal semirings. In Berghammer, R., Möller, B., and Struth, G. (eds.), *RelMiCS*, Lecture Notes in Computer Science, **4988**, pp. 320–336. Springer.

[2] Hebisch, U. and Weinert, H. (1998) *Semirings: Algebraic Theory and Applications in Computer Science* Series in Algebra. World Scientific.

[3] Kozen, D. (1994) A completeness theorem for Kleene algebras and the algebra of regular events. *Inf. Comput.*, **110**, 366–390.

[4] Cohen, E. (2000) Separation and reduction. In Backhouse, R. C. and Oliveira, J. N. (eds.), *MPC*, Lecture Notes in Computer Science, **1837**, pp. 45–59. Springer.

[5] Desharnais, J., Möller, B., and Struth, G. (2004) Modal Kleene Algebra and Applications — A Survey —. *JoRMiCS*, **1**, 93–131.

[6] Desharnais, J., Möller, B., and Struth, G. (2006) Kleene algebra with domain. *ACM Trans. Comput. Log.*, **7**, 798–833.

[7] Kozen, D. (1997) Kleene algebra with tests. *ACM Trans. Program. Lang. Syst.*, **19**, 427–443.

[8] Möller, B., Höfner, P., and Struth, G. (2006) Quantales and temporal logics. In Johnson, M. and Vene, V. (eds.), *AMAST*, Lecture Notes in Computer Science, **4019**, pp. 263–277. Springer.

[9] Fagin, R., Moses, Y., Halpern, J., and Vardi, M. (2003) *Reasoning About Knowledge*. Mit Press.

[10] Pauly, M. and Parikh, R. (2003) Game logic - an overview. *Studia Logica*, **75**, 165–182.

[11] von Wright, J. (2004) Towards a refinement algebra. *Sci. Comput. Program.*, **51**, 23–45.

[12] Baltag, A. and Moss, L. S. (2004) Logics for epistemic programs. *Synthese*, **139**, 165–224.

[13] van Benthem, J. and Liu, F. (2007) Dynamic logic of preference upgrade. *Journal of Applied Non-Classical Logics*, **17**, 157–182.

[14] Solin, K. and von Wright, J. (2006) Refinement algebra with operators for enabledness and termination. In Uustalu, T. (ed.), *MPC*, Lecture Notes in Computer Science, **4014**, pp. 397–415. Springer.

[15] McCarthy, J. (1990) Formalization of two puzzles involving knowledge. *Formalizing Common Sense - Papers by John McCarthy*, pp. 158–166. Ablex Publishing Corporation. `http://www-formal.stanford.edu/jmc/puzzles/puzzles.html`.

[16] Popkorn, S. (1994) *First Steps in Modal Logic*. Cambridge University Press.

[17] Jónsson, B. and Tarski, A. (1951) Boolean algebras with operators, part I. *American Journal of Mathematics*, **73**, 891–939.

[18] Harel, D., Kozen, D., and Tiuryn, J. (2000) *Dynamic Logic* Foundations of Computing. MIT Press.

[19] J.A. Bergstra, A. P., W. Fokkink (2001) Process algebra with recursive operations. In Bergstra, J., Ponse, A., and Smolka, S. A. (eds.), *Handbook of Process Algebra*, pp. 333–389. Elsevier.

[20] Möller, B. (2007) Kleene getting lazy. *Sci. Comput. Program.*, **65**, 195–214.

[21] Manes, E. and Benson, D. (1985) The inverse semigroup of a sum-ordered semiring. *Semigroup Forum*, **31**, 129–152.

[22] Dijkstra, E. W. (1976) *A Discipline of Programming*. Prentice-Hall.

[23] Möller, B. and Struth, G. (2006) Algebras of modal operators and partial correctness. *Theor. Comput. Sci.*, **351**, 221–239.

[24] Hollenberg, M. (1997) An equational axiomatization of dynamic negation and relational composition. *Journal of Logic, Language and Information*, **6**, 381–401.

[25] Desharnais, J. and Struth, G. (2008) Modal semirings revisited. In Audebaud, P. and Paulin-Mohring, C. (eds.), *MPC*, Lecture Notes in Computer Science, **5133**, pp. 360–387. Springer.

[26] Hirsch, R. and Mikulás, S. (2011) Axiomatizability of representable domain algebras. *J. Log. Algebr. Program.*, **80**, 75–91.

[27] Plaza, J. (2007) Logics of public communications. *Synthese*, **158**, 165–179.

[28] Gerbrandy, J. (2007) The surprise examination in dynamic epistemic logic. *Synthese*, **155**, 21–33.

[29] Huth, M. and Ryan, M. (2004) *Logic in Computer Science: modelling and reasoning about systems (second edition)*. Cambridge University Press.

[30] van der Hoek, W. and Wooldridge, M. (2003) Cooperation, knowledge, and time: Alternating-time temporal epistemic logic and its applications. *Studia Logica*, **75**, 125–157.

[31] Ågotnes, T. (2006) Action and knowledge in alternating-time temporal logic. *Synthese*, **149**, 375–407.

[32] van Ditmarsch, H. P., Ruan, J., and Verbrugge, R. (2008) Sum and product in dynamic epistemic logic. *J. Log. Comput.*, **18**, 563–588.

[33] Baltag, A., Moss, L. S., and Solecki, S. (1998) The logic of public announcements and common knowledge and private suspicions. In Gilboa, I. (ed.), *Proc. TARK '98 — 7th Conference on Theoretical Aspects of Rationality and Knowledge*, pp. 43–56. Morgan Kaufmann.

[34] van Ditmarsch, H. P. and Kooi, B. P. (2006) The secret of my success. *Synthese*, **151**, 201–232.

[35] Moore, G. (1942) A reply to my critics. In Schilpp, P. (ed.), *The Philosophy of G.E. Moore*, The Library of Living Philosophers, **4**, pp. 535–677. Northwestern University, Evanston IL.

[36] Solin, K. (2010) A sketch of a dynamic epistemic semiring. *Inf. Comput.*, **208**, 594–604.

[37] Alchourrón, C. E., Gärdenfors, P., and Makinson, D. (1985) On the logic of theory change: Partial meet contraction and revision functions. *J. Symb. Log.*, **50**, 510–530.

[38] Parikh, R. (1983) Propositional logics of programs: New directions. In Karpinski, M. (ed.), *Proc. FCT 83 — Fundamentals of Computation Theory*, Lecture Notes in Computer Science, **158**, pp. 347–359. Springer.

[39] Chellas, B. (1980) *Modal Logic: An Introduction.* Cambridge University Press.

[40] Desharnais, J., Möller, B., and Struth, G. (2004) Termination in modal Kleene algebra. In Lévy, J.-J., Mayr, E. W., and Mitchell, J. C. (eds.), *IFIP TCS*, pp. 647–660. Kluwer.

[41] Desharnais, J., Möller, B., and Struth, G. (2011) Algebraic notions of termination. *Logical Methods in Computer Science*, **7**, 1–29.

[42] Back, R. and Wright, J. (1998) *Refinement Calculus: A Systematic Introduction* Graduate Texts in Computer Science. Springer.

[43] Nelson, G. (1989) A generalization of Dijkstra's calculus. *ACM Trans. Program. Lang. Syst.*, **11**, 517–561.

[44] Baltag, A., Coecke, B., and Sadrzadeh, M. (2007) Epistemic actions as resources. *J. Log. Comput.*, **17**, 555–585.

[45] Backhouse, R. C. and Michaelis, D. (2003) Fixed-point characterisation of winning strategies in impartial games. In Berghammer, R., Möller, B., and Struth, G. (eds.), *RelMiCS*, Lecture Notes in Computer Science, **3051**, pp. 34–47. Springer.

[46] McCune, W. (2005–2010) Prover9 and Mace4. `http://www.cs.unm.edu/~mccune/prover9/`.

[47] Höfner, P. and Struth, G. (2007) Automated reasoning in Kleene algebra. In Pfenning, F. (ed.), *CADE*, Lecture Notes in Computer Science, **4603**, pp. 279–294. Springer.