Knowledge and games in modal semirings

Bernhard Möller

Angaben zur Veröffentlichung / Publication details:

Möller, Bernhard. 2008. "Knowledge and games in modal semirings." Lecture Notes in Computer Science 4988: 320–36.
https://doi.org/10.1007/978-3-540-78913-0_24.

Knowledge and Games in Modal Semirings

Bernhard Möller

Institut für Informatik, Universität Augsburg, D-86135 Augsburg, Germany
moeller@informatik.uni-augsburg.de

Abstract. Algebraic logic compacts many small steps of general logical derivation into large steps of equational reasoning. We illustrate this by representing epistemic logic and game logic in modal semirings and modal Kleene algebras. For epistemics we treat the classical wise men puzzle and show how to handle knowledge update and revision algebraically. For games, we generalise the well-known connection between game logic and dynamic logic to modal semirings and link it to predicate transformer semantics, in particular to demonic refinement algebra. The study provides evidence that modal semirings will be able to handle a wide variety of (multi-)modal logics in a uniform algebraic fashion well suited to machine assistance.

1 Introduction

Algebraic logic strives to compact many small steps of general logical derivation into large steps of equational reasoning. On the semantic side, it attempts to replace tedious model-theoretic argumentation by more abstract reasoning.

A very useful algebraic structure for this are *semirings* (e.g. [18]) that abstract (state) transition systems by axiomatising their fundamental operations choice and sequential composition. Semirings with idempotent choice have a natural approximation order that corresponds to implication, so that implicational inference is replaced by inequational reasoning. Adding finite and infinite iteration leads to Kleene algebras [16] and omega algebras [7].

Modal semirings [9] are based on the concept of *tests* [17] that represent state predicates algebraically. They add diamond and box operators and are more general than Kripke structures, since the access between possible worlds need not be described by relations, but, e.g., by sets of computation paths or even by computation trees. Adding finite and infinite iteration yields modal Kleene and omega algebras which admit algebraic semantics of PDL, LTL and CTL; the subclass of left Boolean quantales can even handle full CTL^* and the propositional μ-calculus [22]. Many further applications have been developed.

Here we show that modal semirings also lead to uniform and useful algebraisations of epistemic and game logics (e.g. [14, 26]). For the former we treat the classical wise men puzzle and show how knowledge update and revision operators can be defined algebraically. For the latter we extend the well-known connection with PDL to the more general case of modal semirings and link it to predicate transformer semantics, in particular to demonic refinement algebra [28].

The framework is intended to be used for defining the semantics of new, special-purpose modal logics as they arise, e.g., with multi-agent systems. The

advantage of using it is that many standard modal properties such as axioms M and K as well as certain induction rules hold automatically and don't need to be proved separately for each new logic.

The paper is organised as follows. Part I deals with an algebraisation of epistemic logic. This logic is recapitulated in Section 2 and illustrated with a variant of the Wise Men Puzzle. Section 3 defines 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 epistemic operators of 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 shows further use of the algebra in modelling certain aspects like preference relations between possible worlds and knowledge revision.

Part II treats games and predicate transformers. Section 7 provides a brief recapitulation of games and their algebra, in particular, of their representation as predicate transformers. These are analysed in a general fashion in Section 8, and a connection to Parikh's iteration operators for games is set up. Section 9 extends the left semiring of predicate transformers to a modal one and relates the box and diamond operators there to the enabledness and termination operators of demonic refinement algebra. Section 10 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 [19].

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, 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 that everyone knows that ... that everyone knows φ, 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 we have the following assertions about common knowledge, since everyone hears what is being said:

– Every man can only see 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 $\mathsf{C}(\neg K_i \neg r_i)$.

Can we infer anything about $\mathsf{K}_3 r_3$ from that?

The 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. [14]). 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.

The *satisfaction relation* $K, w \models \varphi$ tells whether a formula φ holds in world w in frame K. A formula 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 $[R_i]$ is given by

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

In epistemic logic the worlds accessible from a current world w through R_i are called the *epistemic R_i-neighbours* of w. The knowledge of agent i in a world w consists of the formulae that are true in all epistemic neighbours of w (which in presence of axiom (T) below include w itself). Therefore, the knowledge operator K_i coincides with $[R_i]$, whereas its de Morgan dual $\langle R_i \rangle$ 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 actually true (truth)	(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)

We will see in the solution of the puzzle which of these are actually needed.

3 Algebraic Semantics: Modal Semirings

There are already various algebraisations of modal operators, e.g., Boolean algebras with operators [15] and propositional dynamic logic PDL [12]. Moreover, a partly algebraic treatment of Kripke frames can be given using relation algebra; the knowledge requirements above correspond to the following relational ones:

$\mathsf{K}_i\varphi \to \varphi$	$\Delta \subseteq R_i$	reflexivity
$\mathsf{K}_i\varphi \to \mathsf{K}_i\mathsf{K}_i\varphi$	$R_i \,;\, R_i \subseteq R_i$	transitivity
$\neg\mathsf{K}_i\varphi \to \mathsf{K}_i\neg\mathsf{K}_i\varphi$	$R_i^{\smile}; R_i \subseteq R_i$	euclidean property

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

Modal semirings and Kleene algebras provide a very effective combination of PDL and algebraic operations on the access relations. Additionally, they abstract from the special case of access *relations* and allow more general access elements such as sets of computation paths. The particular subclass of Boolean quantales allows the incorporation of infinite iteration and μ-calculus-like recursive definitions, rendering it suitable for handling even full CTL* [22].

A *left semiring* is a structure $(S, +, 0, \cdot, 1)$ with axioms to be detailed below. In most applications these operators are interpreted as follows:

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

The axioms of a left semiring are now as follows.

- The reduct $(S, +, 0)$ is a commutative and idempotent monoid. This induces the *natural order* $a \leq b \Leftrightarrow_{df} a + b = b$ w.r.t. which 0 is the least element and $a + b$ is the join of a and b.
- The reduct $(S, \cdot, 1)$ is a monoid.
- Composition $\cdot$ is left-distributive and left-strict, i.e., $(a + b) \cdot c = a \cdot c + b \cdot c$ and $0 \cdot a = 0$.
- Composition is $\leq$-isotone in its right argument, i.e., $b \leq c \Rightarrow a \cdot b \leq a \cdot c$.

A *weak semiring* is a left semiring in which composition is also right-distributive. A weak semiring with right-strictness is called a *full semiring* or simply *semiring*. All these requirements can be axiomatised purely equationally.

A prominent full semiring is the set of all binary relations over a set W with union as $+$ and relational composition as $\cdot$.

A proper left semiring structure is at the core of process algebra frameworks (e.g. [6]); for further discussion of the connections see [21].

While general 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 by tests. A *test* is a subidentity $p \leq 1$ that has a complement $\neg p$ relative to 1, i.e., $p \cdot \neg p = 0 = \neg p \cdot p$ and $p + \neg p = 1$. If p characterises a set S of states then $\neg p$ characterises its complement. Note that $\neg$ is required only for tests, not for general semiring elements, which allows a much wider class of models. The set of all tests of S is denoted by $\mathsf{test}(S)$.

In the relation semiring, the tests are the subidentities of the form $\Delta_V =_{df} \{(x, x) \,|\, x \in V\}$ for subsets $V \subseteq W$. So Δ_V can represent V as a relation and hence model the predicate characterising V.

The above definition of tests deviates slightly from that in [17] in that 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 box to be presented below forces this maximality anyway (see [8]).

Straightforward calculations show that $\mathsf{test}(S)$ forms a Boolean algebra with $+$ as join, $\cdot$ as meet and 0 and 1 as its least and greatest elements. We will consistently write $a, b, c \ldots$ for arbitrary semiring elements and $p, q, r, \ldots$ for tests. When tests are viewed as predicates over a set W of possible worlds, the semiring operators play the following roles:

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

To ease reading, we will write $\wedge$ and $\vee$ instead of $\cdot$ and $+$ when both of their

arguments are tests (metalogical conjunction and disjunction will be denoted with the larger $\wedge$ and $\vee$ to avoid confusion). Also, we will freely use the standard Boolean operations on $\mathsf{test}(S)$, for instance implication $p \to q \ =_{df}\ \neg p \vee q$ and relative complementation $p - q \ =_{df}\ p \wedge \neg q$, with their usual laws, notably the Galois connection (*shunting rule*) $p \wedge q \leq r \ \Leftrightarrow\ p \leq q \to r$ with the special case $q \leq r \ \Leftrightarrow\ 1 \leq q \to r$.

We now axiomatise a box operator $[\_] : S \to (\mathsf{test}(S) \to \mathsf{test}(S))$. For semiring element a and test q the test $[a]q$ characterises those states for which all successor states under a satisfy q; this coincides with the classical semantics of $[\_]$ in multimodal logics (see e.g. [14]). The axioms are [23]

$$p \leq [a]q \ \Leftrightarrow\ p \cdot a \cdot \neg q = 0 \ , \quad \text{(b1)} \qquad\qquad [a \cdot b]p \ =\ [a][b]p \ . \quad \text{(b2)}$$

According to $(*)$ above, axiom (b1) 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; box is the abstract counterpart of the weakest liberal precondition predicate transformer wlp [11], with $p \leq [a]q$ representing the partial correctness semantics of the Hoare triple $\{p\}\, a\, \{q\}$. Axiom (b2) makes box well-behaved w.r.t. composition. Diamond is the de Morgan dual of box and by (b2) is again well-behaved w.r.t. composition:

$$\langle a \cdot b\rangle p = \langle a\rangle\langle b\rangle p \ , \qquad \langle a\rangle p \ =_{df}\ \neg[a]\neg p \tag{1}$$

A (left/weak) semiring with box (and hence diamond) is called *modal*. Both operators are unique if they exist. They coincide with the corresponding ones in PDL (e.g. [14]); the difference is that in PDL the first arguments a of the box are of a purely syntactic nature without any algebraic lawgs.

An equivalent purely equational axiomatisation via a domain operator has been presented in [8] for the case of a full semiring. In [21] it has been shown that it carries over to left semirings.

We list some useful properties. De Morgan duality gives the swapping rule

$$\langle a\rangle[b]p \leq [c]p \ \Leftrightarrow\ \langle c\rangle p \leq [a]\langle b\rangle p \ . \tag{2}$$

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

$$[a + b]p \ =\ [a]p \wedge [b]p \ , \qquad \langle a + b\rangle p \ =\ \langle a\rangle p \vee \langle b\rangle p \ . \tag{3}$$

Hence box is antitone and diamond is isotone in the first argument: if $a \leq b$ then

$$[a]p \geq [b]p \ , \qquad \langle a\rangle p \leq \langle b\rangle p \ .$$

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 $[b]p \leq [a]p$. Finally, for tests box and diamond can be given explicitly:

$$[p]q = p \to q \ , \qquad \langle p\rangle q = p \wedge q \ . \tag{4}$$

This agrees with the behaviour of the test operation $p?$ in PDL.

Next, we describe finite iteration. A *(left/weak) Kleene algebra* [16] is a structure $(S, +, 0, \cdot, 1, ^*)$ such that the reduct $(S, +, 0, \cdot, 1)$ is a (left/weak) 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 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 semiring is. In this case the axioms entail box and diamond star and plus induction [8]:

$$q \leq p \wedge [a]q \Rightarrow q \leq [a^*]p \ , \qquad p \vee \langle a\rangle q \leq q \Rightarrow \langle a^*\rangle p \leq q \tag{5}$$

$$q \leq [a]p \wedge [a]q \Rightarrow q \leq [a^+]p \ , \qquad \langle a\rangle p \vee \langle a\rangle q \leq q \Rightarrow \langle a^+\rangle p \leq q \ . \tag{6}$$

Using Hoare triples the box part of (5) reads $(q \Rightarrow p \wedge \{q\}\, a\, \{q\}) \Rightarrow \{q\}\, a^*\, \{p\}$, which is related to the familiar Hoare rule for the while loop. Moreover, we have the PDL induction rules (see [23])

$$[a^*](p \rightarrow [a]p) \leq p \rightarrow [a^*]p \ , \qquad \langle a^*\rangle - 1 \leq \langle a^*\rangle(\langle a\rangle - 1) \ . \tag{7}$$

4 Knowledge Algebra

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

Using antidisjunctivity (3) of box we calculate, for $G = \{k_1, \ldots, k_m\}$,

$$\begin{aligned} \mathsf{E}_G p &= \mathsf{K}_{k_1} p \wedge \cdots \wedge \mathsf{K}_{k_m} p = [a_{k_1}]p \wedge \cdots \wedge [a_{k_m}]p \\ &= [a_{k_1} + \cdots + a_{k_m}]p = [a_G]p \ , \end{aligned}$$

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

Likewise, using the composition axiom (b2) and again antidisjunctivity (3) of box, we obtain, semiformally,[1]

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

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

In this way we have obtained an algebraic counterpart of the multiagent logic KT45^n (e.g. [14]) and dynamic epistemic logic [3].

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

$$\mathsf{C}_G p \leq \mathsf{E}_G p \leq \mathsf{K}_{k_j} p \qquad\qquad \mathsf{C}_G p \leq \mathsf{C}_G \mathsf{K}_{k_j} p \ . \tag{8}$$

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

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

If all K_i are reflexive (i.e., satisfy axiom (T)) then so is E_G and hence $\mathsf{C}_G = [a_G^*]$. Therefore the general induction rule (7) specialises to the knowledge induction rule

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

It means that if all agents in G know invariance of p under E_G and p is true then all agents know they all know p. Moreover, (b2) and a star property yield

$$\mathsf{C}_G\mathsf{C}_G p = [a_G^*][a_G^*]p = [a_G^* \cdot a_G^*]p = [a_G^*]p = \mathsf{C}_G p$$

and hence, by conjunctivity of C_G,

$$\mathsf{C}_G p \wedge \mathsf{C}_G q = \mathsf{C}_G\mathsf{C}_G p \wedge \mathsf{C}_G\mathsf{C}_G q = \mathsf{C}_G(\mathsf{C}_G p \wedge \mathsf{C}_G q) \ . \tag{9}$$

As another application of the algebra we show that negative introspection is preserved under transitive closure (for positive introspection this is trivial, since that property is equivalent to transitivity, so that transitive closure does not add anything). To this end we use the equivalent formulations

$$\mathrm{NI}(a) \ \Leftrightarrow_{df} \ \forall\, p \,.\, \langle a\rangle[a]p \leq [a]p \ \Leftrightarrow \ \forall\, p \,.\, \langle a\rangle p \leq [a]\langle a\rangle p$$

of that property to ease use of the above-mentioned (co-)induction rules.

Lemma 4.1 $\mathrm{NI}(a) \ \Rightarrow \ \mathrm{NI}(a^+)$.

Proof. The claim $\langle a^+\rangle[a^+]p \leq \langle a^+\rangle p$ reduces by the star induction axiom to $\langle a\rangle[a^+]p \vee \langle a\rangle\langle a^+\rangle p \leq \langle a^+\rangle p$, which splits into $\langle a\rangle[a^+]p \leq \langle a^+\rangle p \ \wedge \ \langle a\rangle\langle a^+\rangle p \leq \langle a^+\rangle p$. The second conjunct follows by $\langle a\rangle\langle a^+\rangle p = \langle a \cdot a^+\rangle p$ and $a \cdot a^+ \leq a^+$ by isotony of $\langle\ \rangle$. For the first conjunct we calculate

$$\begin{array}{lll} & \langle a\rangle[a^+]p \leq \langle a^+\rangle p & \\ \Leftrightarrow & \langle a^+\rangle p \leq [a]\langle a^+\rangle p & \text{swapping rule (2)} \\ \Leftarrow & \langle a\rangle p \vee \langle a\rangle[a]\langle a^+\rangle p \leq [a]\langle a^+\rangle p & \text{induction (6)} \\ \Leftrightarrow & \langle a\rangle p \leq [a]\langle a^+\rangle p \ \wedge \ \langle a\rangle[a]\langle a^+\rangle p \leq [a]\langle a^+\rangle p & \end{array}$$

The second of these conjuncts holds by $\mathrm{NI}(a)$. For the first one we continue, using the definition of a^+ and the composition rule (1),

$$\langle a\rangle p \leq [a]\langle a^+\rangle p \ \Leftrightarrow \ \langle a\rangle p \leq [a]\langle a\rangle\langle a^*\rangle p \ \Leftarrow \ \mathrm{NI}(a) \ \wedge \ p \leq \langle a^*\rangle p \ ,$$

and are done[2], since the second conjunct follows from $1 \leq a^*$ and $\langle 1\rangle p = p$. □

5 Solving the Wise Men Puzzle

For the results of the present section we assume the underlying left semiring S to be weak. Then we have the following additional properties:

[2] The proof could be compacted even more by using a point-free style; e.g., $\mathrm{NI}(a)$ is equivalent to $\langle a\rangle \circ [a] \leq \langle a\rangle$ where $\leq$ is now the pointwise lifting of the semiring order to predicate transformers.

– Box is conjunctive and diamond is disjunctive:

$$[a](p \wedge q) = [a]p \wedge [a]q \ , \quad \langle a\rangle(p \vee q) = \langle a\rangle p \vee \langle a\rangle q \ .$$

– Hence both operators are isotone in the second argument: if $p \leq q$ then

$$[a]p \leq [a]q \ , \qquad \langle a\rangle p \leq \langle a\rangle q \ .$$

– Moreover, Box satisfies axiom K of modal logic and diamond its dual:

$$[a](p \to q) \leq [a]p \to [a]q \ , \qquad \langle a\rangle p - \langle a\rangle q \leq \langle a\rangle(p - q) \ . \tag{K}$$

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

$$[a](p \to q) \wedge \neg[a]q \leq \neg[a]p \ , \qquad [a](p \vee q) \wedge \neg[a]q \leq \neg[a]\neg p \ . \tag{K$'$}$$

– If S is full then box satisfies axiom M of modal logic and diamond its dual:

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

Let us now use the algebra to solve the Wise Men Puzzle over a full semiring. First we define validity of a test p by $\models p \Leftrightarrow_{df} 1 \leq p$. By shunting, $\models q \to r \ \Leftrightarrow \ q \leq r$. Moreover, $\models p \wedge p \leq q \ \Rightarrow \ \models q$.

With this notation we can repeat the assumptions about the puzzle from Section 2 in a more precise form (the indices of C and E are suppressed, since always the full group of all three agents is referred to):

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

Our main reasoning principle is isotony: If f is an isotone function from tests to tests then $p \leq q \ \wedge \ \models f(p) \ \Rightarrow \ \models f(q)$. Since we have defined E and C as boxes, this principle applies to them without the need for a separate proof.

Now we assume that all K_i and hence E and C are reflexive. Starting from a conjunction of formulae of type (c) and (d),we reason as follows,

$$\begin{array}{ll}
\mathsf{C}(r_1 \vee r_2 \vee r_3) \wedge \mathsf{C}(\neg \mathsf{K}_1 r_1) & \\
= \mathsf{C}(\mathsf{C}(r_1 \vee r_2 \vee r_3) \wedge \mathsf{C}(\neg \mathsf{K}_1 r_1)) & \text{by (9)} \\
\leq \mathsf{C}(\mathsf{K}_1(r_1 \vee r_2 \vee r_3) \wedge \neg \mathsf{K}_1 r_1) & \text{common knowledge (8) and reflexivity of } \mathsf{C} \\
\leq \mathsf{C}(\neg \mathsf{K}_1 \neg (r_2 \vee r_3)) & \text{by (K}') \\
= \mathsf{C}(\neg \mathsf{K}_1 (\neg r_2 \wedge \neg r_3)) & \text{de Morgan} \\
= \mathsf{C}(\neg (\mathsf{K}_1 \neg r_2 \wedge \mathsf{K}_1 \neg r_3)) & \text{conjunctivity of } \mathsf{K}_1 \\
= \mathsf{C}(\neg \mathsf{K}_1 \neg r_2 \vee \neg \mathsf{K}_1 \neg r_3) & \text{de Morgan} \\
\leq \mathsf{C}(r_2 \vee r_3) & \text{contrapositives of formulae (b)} \\
 & \text{and reflexivity of } \mathsf{C}
\end{array}$$

Analogous reasoning shows $\mathsf{C}(r_2 \vee r_3) \wedge C(\neg \mathsf{K}_2 r_2) \leq \mathsf{C}(r_3) \leq \mathsf{K}_3(r_3)$ and we are done, since this means that the third wise man knows his hat is red, which by reflexivity (T) is indeed true.

This latter step also shows that the solution easily generalises to n instead of three wise men. In fact, one can give a closed form of the generalised argument:

for 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,

$$\mathsf{C}(\bigvee_{j\in G} r_j) \wedge \mathsf{C}(\bigwedge_{i\in H} \neg \mathsf{K}_i r_i) \wedge \mathsf{C}(\bigwedge_{i\in H} \bigwedge_{j\in G-H} r_j \to \mathsf{K}_i r_j) \quad \leq \quad \mathsf{C}(\bigvee_{j\in G-H} r_j) \ .$$

Note that we have only used reflexivity of the knowledge modalities in Section 2, but neither positive nor negative introspection.

This argument can be re-used for puzzles with a similar structure, like the unexpected hanging paradox [29] or the muddy children [14], which adds several rounds of interrogation of the above shape. This works, because these puzzles have a "purely logical" structure. Contrarily, the puzzle about Mr. S and Mr. P [19] involves a lot of domain knowledge about arithmetic in addition to 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.

6 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. [5]).

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

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

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

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* [5]: the formula $\mathsf{K}_i \neg p \wedge \langle \preceq_i \rangle p$ expresses that although agent i knows that p is not true, he 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 [5] in our agent algebra.

In a *public announcement* of property p, denoted $!p$, one makes sure that all agents now know p. To this end, all links between p and $\neg p$ worlds are removed. In [5] this operator 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 accessibility 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

is that we now can just use the same algebraic laws as before and do not need to invent special inference rules for this operator.

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.

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 [27], where belief update is modelled using semiring concepts.

Part II: Games and Predicate Transformers

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

7 Games and Their Algebra

The algebraic description of two-player games dates back at least to [25]; for a more recent survey see [26]. The idea is to use a predicate transformer semantics that is 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:

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

Now again, sets of worlds are identified with predicates over worlds. As pointed out in [25], 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 (both ordered by 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 semirings; also the axioms (see [26]) are exactly those for left 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.

As 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.

8 Predicate Transformers

For our purposes, all that matters about $\mathcal{P}(W)$ is its structure as a Boolean algebra. Therefore, more abstractly, a *predicate transformer* is a function $f : B \to B$, where B is an arbitrary Boolean algebra. As in Section 3 we denote the infimum, supremum and complementation operators by $\wedge$, $\vee$ and $\neg$, the least element by 0 and the greatest one by 1. Using $\vee$ for $+$ and $\wedge$ for $\cdot$ makes B a full modal semiring with $\mathsf{test}(B) = B$ and $\langle p \rangle q = p \wedge q$ by (4).

If $p, q \in B$ and $f : B \to B$ satisfies $p \leq q \;\Rightarrow\; f(p) \leq f(q)$ then f is *isotone*. It is *disjunctive* if $f(p \vee q) = f(p) \vee f(q)$ and *conjunctive* if $f(p \wedge q) = f(p) \wedge f(q)$. It is *strict* if $f(0) = 0$ and *co-strict* if $f(1) = 1$. Finally, id is the identity transformer and $\circ$ denotes function composition.

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 supremum $f \vee g$ and infimum $f \wedge g$ of f and g are the pointwise liftings of $\vee$ and $\wedge$, respectively:

$$(f \vee g)(p) \;=_{df}\; f(p) \vee g(p) \;, \qquad (f \wedge g)(p) \;=_{df}\; f(p) \wedge g(p) \;.$$

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 $(\mathrm{ISO}, \vee, \mathbf{0}, \circ, id)$ is a left semiring; the substructure $(\mathrm{DIS}(B), \vee, \mathbf{0}, \circ, id)$ is even a weak semiring. Likewise, the structure $(\mathrm{CON}(B), \wedge, \top, \circ, id)$ is a weak semiring isomorphic to $\mathrm{DIS}(B)$, but with the mirror ordering. The isomorphism is provided by the *duality operator* $^d : \mathrm{PT}(B) \to \mathrm{PT}(B)$, defined by $f^d(p) \;=_{df}\; \neg f(\neg p)$.

If $B = \mathsf{test}(S)$ for some weak semiring S then the modal operator $\langle \_ \rangle$ provides a weak 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:

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

where μ is the least-fixpoint operator. It has been shown in [21] 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 [28] (except for infinite iteration).

A useful consequence of the star induction rule is a corresponding one for the dual of a star, generalising (5):

$$h \;\leq\; g \wedge f^d \circ h \;\;\Rightarrow\;\; h \leq (f^*)^d \circ g \;. \tag{10}$$

Let us now connect this to game algebra. For a predicate transformer g we find in [25] the following two definitions concerning iterations (we use boldface stars and brackets here to distinguish Parikh's notation from ours):

$$\text{(a)}\; \mathbf{<}g^\star\mathbf{>}p \;=_{df}\; \mu(\lambda y \,.\, p \vee g(y)) \;, \qquad \text{(b)}\; \mathbf{[}g^\star\mathbf{]}p \;=_{df}\; \nu(\lambda y \,.\, p \wedge g(y)) \;, \tag{11}$$

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

$$
\begin{array}{ll}
& [g^\star](p) \\
= & \nu(\lambda y \,.\, p \wedge g(y)) & \text{definition (11(b))} \\
= & \neg\mu(\lambda y \,.\, p \wedge g(y))^d & \text{above fixpoint law} \\
= & \neg\mu(\lambda y \,.\, \neg(p \wedge g(\neg y))) & \text{definition dual} \\
= & \neg\mu(\lambda y \,.\, \neg p \vee \neg g(\neg y))) & \text{de Morgan} \\
= & \neg\mu(\lambda y \,.\, \neg p \vee g^d(y)) & \text{definition dual} \\
= & \neg(g^d)^*(\neg p) & \text{definition (11(a))} \\
= & ((g^d)^*)^d(p) \;. & \text{definition dual}
\end{array}
$$

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 $(f^*)^d \;\leq\; 1 \wedge f^d \circ (f^*)^d$ and (10) as the induction axiom.

Let us finally set up the connection with termination analysis. In [25] Parikh states that for concrete access relation R the predicate $\langle [R]^\star \rangle \mathsf{false}$ characterises the worlds from which no infinite access paths emanate. Plugging in the definitions for a general access element a we obtain

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

This coincides with the *halting predicate* of the propositional μ-calculus [12]; in the semiring setting it and its complement have been termed the *convergence* and *divergence* of a and used extensively in [10]. 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.

9 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 now 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 characterise the tests in the set $\mathrm{ISO}(B)$; the proof of the following lemma can be found in the Appendix.

Lemma 9.1

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

Part 2. means that the tests in the semiring of isotone predicate transformers are precisely the diamonds of the elements of B (see Section 8).

Because of Part 1. and (4) we will, for convenience, denote mappings of the form $\lambda q \,.\, p \wedge q$ by $\langle p \rangle$ also in the general case of ISO(B). The proof shows also 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 box axiom (b1) means there:

$$\begin{aligned}\langle p\rangle \circ f \circ \neg\langle q\rangle \leq 0 \;&\Leftrightarrow\; \forall\, r : p \wedge f(\neg q \wedge r) \leq 0 \;\Leftrightarrow\; p \wedge f(\neg q \wedge 1) \leq 0\\ &\Leftrightarrow\; p \leq \neg f(\neg q) \;\Leftrightarrow\; p \leq f^d(q)\ ;\end{aligned}$$

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

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

Let us check that this satisfies the second box axiom (b2) as well:

$$\begin{aligned}[f \circ g]\langle q\rangle \;&=\; \langle (f\circ g)^d(q)\rangle \;=\; \langle (f^d \circ g)^d(q)\rangle\\ &=\; \langle (f^d(g^d(q))\rangle \;=\; [f]\langle g^d(q)\rangle \;=\; [f][g]\langle q\rangle\ .\end{aligned}$$

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

Theorem 9.2 ISO(B) *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 to refinement algebra.

Generally, in a modal left semiring the *domain operator* [8] $\ulcorner : S \to \mathsf{test}(S)$ 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 [28]. That algebra is an axiomatic algebraic system for dealing with predicate transformers under a demonic view of non-determinacy.

Besides τ (which is characterised by the domain axioms of [8]) DRA has an enabledness operator ϵ, defined not in terms of tests but by dual axioms in terms of *guards* or assumptions. These take the form $\neg p \cdot \top + 1$ where $\top$ is the greatest element (which always exists in DRA). The intuitive meaning of tests and assumptions is briefly elaborated in the Appendix.

Let us see what assumptions (also called *guards*) are in ISO(B):

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

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

For the dual of the domain we obtain

$$(\ulcorner f)^d = \langle f(1)\rangle^d = [f(1)] = [f(\neg 0)] = [\neg f^d(0)]\ . \tag{12}$$

This latter expression coincides with that for $\epsilon(f^d)$ in the mentioned concrete model of [28], 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 (12) also corresponds to the *guard* $\neg\mathsf{wp}(a, \mathit{false})$ of [24], while that for τ coincides with the termination predicate $\mathsf{wp}(a, \mathit{true})$ there.

10 Conclusion and Outlook

We have shown that modal 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 [4], where modules over quantales are used to define an algebraic semantics of modal operators. However, having separate sorts for actions and (the equivalent) test 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 semiring framework offers.

One topic we have omitted from the present paper is that of infinite iteration. This has been treated in [21]. However, there is a restriction. Although over a complete Boolean algebra B infinite iteration can be defined as $f^\omega =_{df} \nu g \,.\, f \circ g$ in $\mathrm{ISO}(B)$, this does not imply the usual omega coinduction law $c \leq a \cdot c + b \Rightarrow c \leq a^\omega + a^* \cdot b$ [7]. It only does so in $\mathrm{DIS}(B)$. However, as stated in [26], disjunctivity is not a natural requirement for games.

Other future work will concern the proper treatment of infinite iteration of games, further applications (e.g., extending the work on characterisation of winning strategies in [2] and of winning and losing positions in [9]), but also partial mechanisation of the (largely equational and fully first-order) axiomatic system. First steps into the latter direction using the tools Prover9 and Mace4 [20] have been taken by P. Höfner and G. Struth at Sheffield [13].

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

References

1. R.J. Back, J. von Wright: Refinement calculus — A systematic introduction. Springer 1998
2. R. Backhouse, D. Michaelis: Fixed-point characterisation of winning strategies in impartial games. In: R. Berghammer, B. Möller, G. Struth (eds.): Relational and Kleene-algebraic methods in computer science. LNCS 3051. Springer 2004, 34–47
3. A. Baltag, L. Moss, S. Solecki: The logic of public announcements, common knowledge, and private suspicions. Proc. 7th conference on Theoretical Aspects of Rationality and Knowledge, Evanston, Illinois 1998, 43–56
4. A. Baltag, B. Coecke, M. Sadrzadeh: Epistemic actions as resources. J. Log. Comput. 17, 555–585 (2007)
5. J. van Benthem, F. Liu: Dynamic logic of preference upgrade. Manuscript 2004. To appear in J. Applied Non-Classical Logics 2006
6. J.A. Bergstra, W. Fokkink, A. Ponse: Process algebra with recursive operations. In J.A. Bergstra, S. Smolka, A. Ponse (eds.): Handbook of process algebra. North-Holland 2001, 333–389
7. E. Cohen: Separation and reduction. In R. Backhouse, J. Oliveira (eds.): Mathematics of Program Construction (MPC 2000). LNCS 1837. Springer 2000, 45–59.

8. J. Desharnais, B. Möller and G. Struth. Kleene algebra with domain. Institute of Computer Science, University of Augsburg, Technical Report 2003-7. Revised version: ACM Transaction on Computational Logic 7:4, 798–833 (2006)
9. J. Desharnais, B. Möller, G. Struth: Modal Kleene algebra and applications — A survey. Journal on Relational Methods in Computer Science 1, 93–131 (2004)
10. J. Desharnais, B. Möller, G. Struth: Termination in modal Kleene algebra. In J.-J. Lévy, E. Mayr, J. Mitchell (eds): Exploring new frontiers of theoretical informatics. IFIP Series 155. Kluwer 2004, 653–666. Extended version: Institute of Computer Science, University of Augsburg, Technical Report 2006-23
11. E. Dijkstra: A discipline of programming. Prentice-Hall 1976
12. D. Harel, D. Kozen, J. Tiuryn: Dynamic logic. MIT Press 2000
13. P. Höfner, G. Struth: Automated reasoning in Kleene algebra. In F. Pfenning (ed.): CADE 2007. LNAI 4603. Springer 2007, 279-294
14. M. Huth, M. Ryan: Logic in computer science — Modelling and reasoning about systems, 2nd Edition. Cambridge University Press 2004
15. B. Jónsson, A. Tarski: Boolean algebras with operators, Part I. American Journal of Mathematics 73:891–939 (1951)
16. D. Kozen: A completeness theorem for Kleene algebras and the algebra of regular events. Inf. Comput. 110:2, 366–390 (1994)
17. D. Kozen: Kleene algebra with tests. ACM Transactions on Programming Languages and Systems, 19(3), 427–443 (1997)
18. W.Kuich,A.Salomaa: Semirings, automata, languages. EATCS Monographs on Theore- ticalComputerScience, Vol.5. Springer 1986
19. J. McCarthy: Formalization of two puzzles involving knowledge. `http://www-formal.stanford.edu/jmc/puzzles/puzzles.html`
20. `W. McCune: Prover9 and Mace4. http://www.cs.unm.edu/ mccune/mace4/`
21. B. Möller: Lazy Kleene algebra. In D. Kozen (ed.): Mathematics of Program Construction. LNCS 3125. Springer 2004, 252-273. Revised Version: B. Möller: Kleene getting lazy. Science of Computer Programming (in Press)
22. B. Möller, P. Höfner, G. Struth: Quantales and temporal logics. In: M. Johnson, V. Vene (eds.): Algebraic Methodology and Software Technology (AMAST 2006). LNCS 4019. Springer 2006, 263–277
23. B. Möller, G. Struth: Algebras of modal operators and partial correctness. Theoretical Computer Science 351, 221-239 (2006)
24. G. Nelson: A generalization of Dijkstra's calculus. *ACM Transactions on Programming Languages and Systems* 11:517–561 (1989)
25. R. Parikh: Propositional logics of programs: new directions. In M. Karpinski (ed.): Fundamentals of Computation Theory. LNCS 158. Springer 1983, 347–359
26. M. Pauly, R. Parikh: Game logic – An overview. Studia Logica 75, 165-182 (2003)
27. K. Solin: Dynamic epistemic semirings. Institute of Computer Science, University of Augsburg, Technical Report, 2006-17. June 2006
28. K. Solin, J. von Wright: Refinement algebra with operators for enabledness and termination. In: T. Uustalu (Ed.): Mathematics of Program Construction. LNCS 4014. Springer 2006, 397–415
29. Wikipedia: Unexpected hanging paradox. `http://en.wikipedia.org/wiki/Unexpected_hanging_paradox`

Appendix

First we prove an auxiliary lemma about relative complements.

Lemma A Assume in a Boolean algebra $r \leq p \wedge q \ \wedge \ s \leq p \wedge \neg q \ \wedge \ r \vee s = p$. Then $r = p \wedge q \ \wedge \ s = p \wedge \neg q$.

Proof. Observe that $s \wedge q \leq p \wedge \neg q \wedge q = p \wedge 0 = 0$, i.e., $s \wedge q = 0$. Hence $p \wedge q = (r \vee s) \wedge q = r \wedge q \vee s \wedge q = r \wedge q \leq r$, which shows $r = p \wedge q$. Symmetrical reasoning applies to s. □

Now we can give the

Proof of Lemma 9.1:

1. ($\Leftarrow$) By definition, $f \leq id$. A straightforward calculation shows that the complement of f relative to id is $g(p) =_{df} p \wedge \neg f(1)$.
   ($\Rightarrow$) Let $g \in \mathrm{ISO}(B)$ be the complement of $f \leq id$ relative to id, i.e., $f \vee g = id$ and $f \wedge g = \mathbf{0}$. First, $f \leq id$ means $f(p) \leq p$. Second, $f \in \mathrm{ISO}(B)$ means $f(p) \leq f(1)$. Hence $f(p) \leq p \wedge f(1)$. From $f \vee g = id$ we conclude $g(1) = \neg f(1)$ and hence, by symmetrical reasoning, $g(p) \leq p \wedge \neg f(1)$. Since
   $$\begin{aligned} p \wedge f(1) \vee p \wedge \neg f(1) \ &= \ p \wedge (f(1) \vee \neg f(1)) \ = \ p \wedge 1 \ = \ p \ , \\ p \wedge f(1) \wedge p \wedge \neg f(1) \ &= \ p \wedge f(1) \wedge \neg f(1) \ = \ p \wedge 0 \ = \ 0 \ , \end{aligned}$$
   we obtain $f(p) = p \wedge f(1)$ and $g(p) = p \wedge \neg f(1)$ by Lemma A.
2. By (4) and 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 $\langle p \rangle$. □

We conclude by explaining the relation between tests and assumptions. We first introduce a test-based conditional as $\mathsf{if}\, p\, \mathsf{then}\ a\ \mathsf{else}\ b \Leftrightarrow_{df} p \cdot a + \neg p \cdot b$. With its help assertions and assumptions can be defined as

$$\mathsf{assert}\ p =_{df} \mathsf{if}\, p\, \mathsf{then}\ 1\ \mathsf{else}\ 0 \qquad \mathsf{assume}\ p =_{df} \mathsf{if}\, p\, \mathsf{then}\ 1\ \mathsf{else}\ \top \ ,$$

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

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

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

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

which is the expression given in Section 9.