Relational Semantics for Modal Logics*

Bernd–Holger Schlingloff
Institut für Informatik,
Technische Universität München,
e-mail: schlingl@informatik.tu-muenchen.de

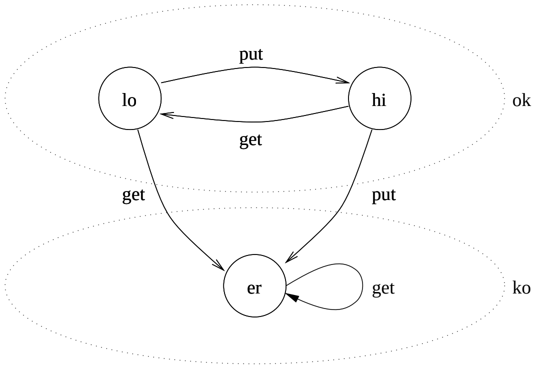
Wolfgang Heinle
Institut für angewandte Mathematik,
Universität Bern,
e-mail: heinle@iam.unibe.ch

Abstract

In this work we survey the connections between modal logic and relation algebra. We compare various modal and relational languages for the specification of reactive systems by giving new translation algorithms between these languages. We then characterize the expressiveness of the languages algebraically with p-morphisms (or bisimulations). Furthermore, we show how completeness and incompleteness proofs of modal logic can be transferred to relation algebra, and give a relation algebraic treatment of modal correspondence theory. We show how our methods can be applied to stronger languages like those containing derivation rules or fixpoint operators.

1 Introduction

In the design of safety-critical software systems formal semantics and proofs are mandatory. Whereas for *functional systems* (computing a certain function) usually denotational semantics and Hoare-style reasoning is employed, *reactive systems* (reacting to an environment) mostly are modelled in an automata-theoretic framework, with a modal or temporal logic proof system. Much of the success of these logics in the specification and verification of reactive systems is due to their ability to express properties without explicit use of first-order variables. For example, consider a program defined by the following transition system:



In this picture lo, hi and er denote states, and put and get are binary relations between states. Ok is the set $\{lo, hi\}$ of states, and ko is $\{er\}$. (The program is just for demonstration and does not have any particular purpose.) Let $R \triangleq put \cup get$ be the transition relation of this program; then e.g. nontermination from an initial state x is described by the first-order formula $\forall y\,[R^*(x,y) \rightarrow \exists z\,[R(y,z)]]$. It can also be expressed by the multimodal formula $[R^*]\langle R\rangle\top$, which does not contain individual variables x, y. However, the same virtue is shared by the more expressive relational calculus, which was introduced as a means to formalize mathematics without variables. In the example, the relational equation $R^* \circ -(R \circ 1) =$

*This article is a preliminary version of a chapter to appear in the forthcoming handbook "Relational Methods in Computer Science", edited by Ch. Brink and G. Schmidt

0 expresses the same condition as above for all x. As we will see, relational algebra thus can serve as a natural semantics for modal logics, resulting in some easy completeness and correspondence results. Vice versa, in many cases techniques developed for modal logics can be extended to relational algebra, yielding new insights and opening new areas of interest.

2 Formulas and properties

To begin with, we give definitions of all logical languages used in this chapter, and their respective translations into one another. Then, we describe how properties, i.e., classes of semantical structures for our formulas, can be characterized with relational means. We presuppose elementary knowledge of relation algebra as described, e.g., in the appendix of [SS89].

2.1 Logics and their Standard Translations

The basic modal logic **K** is built from propositions and boolean connectives $\neg$, $\vee$, with an additional unary connective $\Diamond$, called possibility operator. The necessity operator $\Box$ can be defined as its dual by $\Box\varphi = \neg\Diamond\neg\varphi$.

A *Kripke structure* consists of a nonempty set W of 'worlds', a binary relation R and a valuation h from propositions into $\mathcal{P}(W)$. Satisfaction of a sentence φ in a Kripke strukture (W, R, h) and a world $w \in W$ is defined inductively:

$W, R, h, w \models p_i$ if $w \in h(p_i)$.

$W, R, h, w \models (\varphi \vee \psi)$ if $W, R, h, w \models \varphi$ or $W, R, h, w \models \psi$.

$W, R, h, w \models \neg\varphi$ if $W, R, h, w \not\models \varphi$.

$W, R, h, w \models \Diamond\varphi$ if $W, R, h, w' \models \varphi$ for some $w' \in W$ with wRw'.

A sentence φ is valid in a Kripke structure (W, R, h), if $W, R, h, w \models \varphi$ for all $w \in W$.

To get a complete deductive system for the modal logic **K**, start with the set of all propositional tautologies, and add the following axioms and rules:

***monotonicity*:** $\Box(\varphi \rightarrow \psi) \rightarrow (\Box\varphi \rightarrow \Box\psi)$

***necessitation*:** $\varphi \vdash \Box\varphi$

***modus ponens*:** φ, $(\varphi \rightarrow \psi) \vdash \psi$

An alternative choice is to add the following axioms and rule to propositional logic with modus ponens:

***normality*:** $\Diamond\bot \leftrightarrow \bot$

***additivity*:** $\Diamond(\varphi \vee \psi) \leftrightarrow (\Diamond\varphi \vee \Diamond\psi)$

***replacement*:** $(\varphi \leftrightarrow \psi) \vdash (\Diamond\varphi \leftrightarrow \Diamond\psi)$

The language of basic modal logic defined above contains besides the boolean connectives only propositions and one unary modal operator. Propositions are interpreted as unary predicates (subsets) of worlds, and the diamond operator corresponds to a binary accessibility relation between worlds. However, already in the above example formula we used the reflexive transitive closure relation R^* of R. In general, we will want to express properties of several relations R, R^*, *put*, *get*,... Moreover, the restriction to unary predicates and binary relations sometimes is artificial. Therefore we define the modal language over an arbitrary algebraic type τ. Function symbols in τ are called *operators*; unary operators include $\Diamond$ and $\langle R \rangle$, where R is from some index set. Propositions are modal constants, i.e., zero-ary operators. *Modal formulas* (of type τ with variables from V) are defined as terms of type τ with additional boolean connectives:

- Every $v \in V$ is a modal formula,
- $\bot$ is a modal formula,
- If φ_1 and φ_2 are modal formulas, then $(\varphi_1 \to \varphi_2)$ is a modal formula,
- if $\varphi_1, \ldots, \varphi_n$ are modal formulas and $\triangle \in \mathcal{F}_\tau$ is an n-ary operator, then $\triangle\varphi_1 \ldots \varphi_n$ is a modal formula.

Variables are denoted by lowercase letters $\{v, p, q, ...\}$; formulas not containing any variables are called *sentences*. Whenever we wish to emphasize the fact that φ contains proposition variables we call φ an *axiom*. Other boolean connectives $\neg$, $\vee$, $\wedge$, $\leftrightarrow$ are defined as usual; for every operator $\triangle$ its *dual* operator ∇ is given by $\nabla\varphi_1 \ldots \varphi_n \triangleq \neg\triangle\neg\varphi_1 \ldots \neg\varphi_n$. The dual of $\langle R \rangle$ is $[R]$. The *basic* modal language is the set of modal sentences of type $\{P, \Diamond\}$, where P is the set of propositions. In *basic multimodal* formulas the arity of operators is at most one.

To define a semantics for the modal language, there are several choices. The most obvious idea is to extend the notion of Kripke structure to include n-ary relations:

A *standard frame* of type τ consists of a nonempty set W of 'worlds', and an interpretation $\mathcal{R}$ assigning to every n-ary operator from τ an $(n+1)$–ary relation on W. A *standard model* for formulas of type τ with variables from V is a standard frame $(W, \mathcal{R})$ of type τ together with a *valuation* $\mathcal{V}$ assigning to every variable from V a subset of W. The model $(W, \mathcal{R}, \mathcal{V})$ is said to be *based* on the frame $(W, \mathcal{R})$. Validity of a formula φ in a standard model $(W, \mathcal{R}, \mathcal{V})$ and a world $w \in W$ is defined inductively:

$W, \mathcal{R}, \mathcal{V}, w \models v$ if $w \in \mathcal{V}(v)$;

$W, \mathcal{R}, \mathcal{V}, w \not\models \bot$;

$W, \mathcal{R}, \mathcal{V}, w \models (\varphi_1 \to \varphi_2)$ if $W, \mathcal{R}, \mathcal{V}, w \models \varphi_1$ implies $W, \mathcal{R}, \mathcal{V}, w \models \varphi_2$;

$W, \mathcal{R}, \mathcal{V}, w \models \triangle\varphi_1 \ldots \varphi_n$ if there exist $w_1, ..., w_n \in W$ such that $(w, w_1, ..., w_n) \in \mathcal{R}(\triangle)$ and $W, \mathcal{R}, \mathcal{V}, w_i \models \varphi_i$ for all $i = 1, ..., n$.

The formula φ is *valid* in the model $(W, \mathcal{R}, \mathcal{V})$ if $W, \mathcal{R}, \mathcal{V}, w \models \varphi$ for all $w \in W$; it is valid in the frame $(W, \mathcal{R})$ if it is valid in all models $(W, \mathcal{R}, \mathcal{V})$ based on $(W, \mathcal{R})$. Note that any sentence is valid in a frame iff it is valid in some model based on that frame.

To get an intuitive understanding of how relations are coded as modal operators, consider a binary relation R on W. Define for any $w' \in W$ the set $\langle R \rangle(w') \triangleq \{w \in W : (w, w') \in R\}$, and for any $\varphi \subseteq W$, the set $\langle R \rangle(\varphi) \triangleq \bigcup\{\langle R \rangle(w') : w' \in \varphi\}$. Then we have $(w, w') \in R$ iff $w \in \langle R \rangle(w')$; therefore there is $w' \in \varphi$ with $(w, w') \in R$ iff there is $w' \in \varphi$ with $w \in \langle R \rangle(w')$, i.e., iff $w \in \langle R \rangle\varphi$.

In our example, $\langle get \rangle(\{er\}) = \{er, lo\}$, and $\langle put \rangle(\{lo, hi\}) = \langle put \rangle(lo) \cup \langle put \rangle(hi) = \emptyset \cup \{lo\}$. Thus $w \models \langle get \rangle ko$ iff $w \in \{er, lo\}$, and $w \models \langle put \rangle ok$ iff $w = lo$. As an example of a valid sentence, consider $\langle get \rangle\langle get \rangle ko$; as an axiom, $(\langle put \rangle p \to [put]p)$ is valid since it is valid for every substitution of p with some subset of $\{lo, hi, er\}$.

Standard frames of type τ are nothing else than relational structures for the algebraic type τ', where in τ' the arity of all operators is increased by one: $\tau'(\triangle) \triangleq \tau(\triangle) + 1$. But, relational structures of type τ' are also the semantical basis for the first and second order language of type τ'. The *standard translation* of modal formulas of type τ with variables from V into predicate logic formulas of type τ' with proposition variables from V and one free individual variable x is defined as follows:

$ST(v) \triangleq v(x)$;

$ST(\bot) \triangleq (x \neq x)$;

$ST((\varphi_1 \to \varphi_2)) \triangleq (ST(\varphi_1) \to ST(\varphi_2))$;

$ST(\triangle\varphi_1 \ldots \varphi_n) \triangleq \exists x_1 ... x_n \, [\triangle(x, x_1, ..., x_n) \wedge ST(\varphi_1)[x/x_1] \wedge \ldots \wedge ST(\varphi_n)[x/x_n]]$

Here $\varphi[x/y]$ denotes the formula derived by simultaneously substituting y and x for all occurrences of x and y in φ, respectively. If the highest arity of any operator in φ is n, then $ST(\varphi)$ contains one free variable x and at most $n+1$ bound variables $\{x, x_1, ..., x_n\}$. The number of free individual variables of a first-order formula is usually called its *dimension*; hence the standard translation of any modal formula is one-dimensional. Note that $ST(\varphi)$ is a first order formula iff φ is a modal sentence; if φ contains free proposition variables then so does $ST(\varphi)$. (In this case φ represents a *monadic* Π_1^1*–property*.)

As an example for the standard translation, we calculate $ST(\langle get\rangle\langle get\rangle ko)$

$= \exists x_1\,[get(x, x_1) \wedge ST(\langle get\rangle ko)[x/x_1]]$
$= \exists x_1\,[get(x, x_1) \wedge (\exists x_1\,[get(x, x_1) \wedge (ST(ko)[x/x_1])])[x/x_1]]$
$= \exists x_1\,[get(x, x_1) \wedge (\exists x_1\,[get(x, x_1) \wedge ko(x_1)])[x/x_1]]$
$= \exists x_1\,[get(x, x_1) \wedge \exists x\,[get(x_1, x) \wedge ko(x)]]$

Validity of a modal formula φ in a standard model $(W, \mathcal{R}, \mathcal{V})$ and world w could have been defined as validity of the predicate logic formula $ST(\varphi)$ in the relational structure $(W, \mathcal{R})$ with first order assignment $g : x \mapsto w$ and second order assignment $\mathcal{V}$. Of course this new definition for the semantics matches the old one, i.e.,

$$W, \mathcal{R}, \mathcal{V}, w \models \varphi \quad \text{iff} \quad (W, \mathcal{R}), g, \mathcal{V} \models ST(\varphi), \qquad \text{where } g : x \mapsto w.$$

The above standard translation maps modal sentences into first order formulas, and modal axioms into a restricted class of second order formulas. However, there is another formalism in between modal logic and predicate logic, which is equally well suited to serve as semantics for the modal language: the relational calculus.

Since in general we are working with relations of different arities, we have to extend the underlying relation algebra appropriately. There are several approaches to do so.

In the first approach, which is followed e.g. in [BBS92], boolean algebras and relation algebras are combined into *Peirce algebras*, that is, two sorted algebras of type $(B, A, \langle\ \rangle, ?)$, where B is a boolean algebra, A is a relation algebra, $\langle\ \rangle$ is a mapping $A \times B \to B$ and $?$ is a *cylindrification* mapping $B \to A$ such that

- $\langle r\rangle(a \vee b) = \langle r\rangle a \vee \langle r\rangle b$
- $\langle r \vee s\rangle a = \langle r\rangle a \vee \langle s\rangle a$
- $\langle r\rangle\langle s\rangle a = \langle r \circ s\rangle a$
- $\langle id\rangle a = a$
- $\langle 0\rangle a = 0$
- $\langle r^{\smile}\rangle(-\langle r\rangle a) \leq -a$
- $\langle a?\rangle 1 = a$
- $(\langle r\rangle 1)? = r \circ 1$

Any formula of the basic multimodal language can be regarded as a term of a Peirce algebra, consisting of a boolean algebra built from propositions and a relation algebra built from unary operators. Of course, Peirce algebras provide a much richer algebraic structure than modal formulas, since they include a relation type with operations on operators. However, since complementation of relations is present, the representation problem for Peirce algebras is undecidable.

Peirce algebras can be mapped into ordinary relation algebras by identifying each element a of the boolean algebra with a right ideal element $(a \circ 1)$ of the relation algebra. This is also the approach to a relational semantics followed, e.g., in [Orl88]. To extend this approach to n-ary operators, we extend the dimension of any relation or predicate to the maximum dimension of any relation in the signature.

The *projection* $\Pi_i(R)$ of an $(n+1)$-ary relation R onto its i-th component $(0 \leq i \leq n)$ is defined by

$$\Pi_i(R) \triangleq \{(x_0, ..., x_n) : \exists y_1, ..., y_n\,[R(x_i, y_1, ..., y_n)]\}$$

For a binary relation R we have $\Pi_0(R) = \{(x_0, x_1) : \exists y_1 [R(x_0, y_1)]\} = R \circ 1$, and $\Pi_1(R) = \{(x_0, x_1) : \exists y_1 [R(x_1, y_1)]\} = (R \circ 1)^{\smile} = 1 \triangleleft R$.

Using these operations, a *relational translation* RT of modal formulas into relation algebraic terms can be defined. If φ is a modal formula of type τ with variables from V, then $RT(\varphi)$ is a term of type τ'' with variables from V, where τ'' contains boolean operations, unary projections Π_i, and for every modal operator $\triangle$ a relation constant $\triangle$.

$RT(v) \triangleq \Pi_0(v)$ for every proposition variable from V;

$RT(\bot) \triangleq 0$;

$RT((\varphi_1 \to \varphi_2)) \triangleq RT(\varphi_1) \leq RT(\varphi_2)$;

$RT(\triangle\varphi_1 \ldots \varphi_n) \triangleq \Pi_0(\triangle \wedge \Pi_1(RT(\varphi_1)) \wedge \ldots \wedge \Pi_n(RT(\varphi_n)))$

For the basic (multi)modal language we have

$RT(P) = \Pi_0(P) = P \circ 1$ for any proposition P, and

$RT(\Diamond\varphi_1) = \Pi_0(\Diamond \wedge \Pi_1(RT(\varphi_1)) = (\Diamond \wedge (RT(\varphi_1) \circ 1)^{\smile}) \circ 1 = \Diamond \circ RT(\varphi_1)$

In the last transformation we used the fact that $RT(\varphi)$ is a right ideal relation, i.e. $RT(\varphi) = RT(\varphi) \circ 1$, which is proved by induction on φ. Thus this relational translation conforms with cylindrification by right ideals.

The relational translation of the necessity operator $\Box$ becomes

$RT(\Box\varphi_1) = RT(\neg\Diamond\neg\varphi_1) = RT(\varphi_1) \backslash \Diamond^{\smile}$

where $\backslash$ denotes right residuation of relations. For the above example formula we have $RT(\langle get\rangle\langle get\rangle ko) = get \circ get \circ ko \circ 1$.

A model for terms of type τ'' with projections $\Pi_0, ..., \Pi_n$ assigns an $(n+1)$-ary relation to every operator and proposition variable. Validity of a term $RT(\varphi)$ in a model M and worlds $w_0, ..., w_n$ is defined inductively according to the above clause for the projection operation. Now any standard model M can be extended to a model M'' for terms of type τ'' by setting, for an m-ary connective $\triangle$ (where $m \leq n$),

$$\mathcal{R}''(\triangle) \triangleq \{(x_0, ..., x_n) : (x_0, ..., x_m) \in \mathcal{R}(\triangle)\},$$

and similar for $v \in \mathcal{V}$. (E.g., ko becomes the binary relation $\{(er, lo), (er, hi), (er, er)\}$.) Then it is an easy exercise to prove that $M \models \varphi$ iff $M'' \models RT(\varphi)$. Thus the above relational translation preserves satisfiability. Moreover, since $RT(\varphi) = \Pi_0(RT(\varphi))$, we conclude: If $M'' \models RT(\varphi)$ for all M'' which are extensions of some standard model, then $M \models RT(\varphi)$ for all models M. Hence the translation is also validity-preserving: $\models \varphi$ iff $\models RT(\varphi)$.

The third approach to a relational semantics for modal logics uses an algebra of n-ary operations for n-ary operators. The set of modal formulas with operators from τ and variables from V can be seen as the term algebra of type $\tau \cup \{\vee, -, 0\}$ generated by V. A *modal algebra* or *boolean algebra with operators* is any relational structure $(A, \vee, -, 0, \tau)$ for this type, such that $(A, \vee, -, 0)$ forms a boolean algebra, and every operator $\triangle \in \tau$ of arity $n > 0$ is normal and additive, i.e. satisfies

$\triangle(p_1, ..., 0, ..., p_n) = 0$ and

$\triangle(p_1, ..., p_i \vee p_i', ..., p_n) = \triangle(p_1, ..., p_i, ..., p_n) \vee \triangle(p_1, ..., p_i', ..., p_n)$.

As usual, a relational expression is called *valid* in the algebra, if it is (equal to) the unit element 1. A term t containing free relation variables v is valid in A, if $t[v/R]) = 1$ for all substitutions of variables with elements of A.

An *ultrafilter* on a modal algebra is any maximal nontrivial meet-closed upset, i.e., a subset u of A satisfying

$p \in u$ or $-p \in u$ for each $p \in A$,

$0 \notin u$,

if $p, q \in u$ then $p \wedge q \in u$, and

if $p \in u$ and $p \leq q$ then $q \in u$.

A subset u of A is said to have the *finite intersection property*, if for any finite subset $\{p_1, ..., p_n\} \subseteq u$ it holds that $p_1 \wedge ... \wedge p_n \neq 0$. Any such subset can be extended to an ultrafilter of A by repeatedly adding either p or $-p$ for each $p \in A$. (Note that for uncountable A the axiom of choice is needed in this construction.) In particular, for any atom a of A there is exactly one ultrafilter u containing a, namely $u \triangleq \{p : a \leq p\}$. Now the ultrafilters of a modal algebra can serve as atoms of another algebra: consider the powerset algebra on the set U_A of ultrafilters of A. According to a fundamental result of Stone[Sto36], the function $\sigma : A \rightarrow \mathcal{P}(U_A)$, mapping every $p \in A$ to $\sigma(p) \triangleq \{u \in U_A : p \in u\}$, is a boolean embedding. That is, $\sigma(p \vee q) = \sigma(p) \cup \sigma(q)$, $\sigma(-p) = -\sigma(p)$, and $\sigma(0) = \emptyset$. The definition of σ can be extended such that it assigns an $(n+1)$-ary relation $\sigma(\triangle)$ on U_A to every n-ary operator $\triangle$:

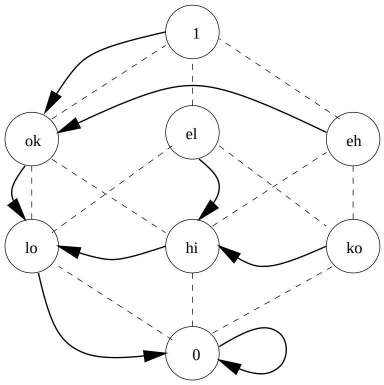
$$\sigma(\triangle) \triangleq \{(u_0, ..., u_n) : p_1 \in u_1 \wedge ... \wedge p_n \in u_n \rightarrow \triangle(p_1, ..., p_n) \in u_0\}$$

Dually, we have $\sigma(\nabla)(u_0, ..., u_n)$ iff $\nabla(p_1, ..., p_n) \in u_0 \rightarrow p_1 \in u_1 \vee ... \vee p_n \in u_n$. Again, $\sigma(\triangle)$ can be regarded as an n-ary operator on $\mathcal{P}(U_A)$ in the usual way; $\sigma(\triangle)(x_1, ...x_n) \triangleq \{u_0 : \exists u_1, ..., u_n\, [\triangle(u_0, ..., u_n) \wedge u_1 \in x_1 \wedge ... \wedge u_n \in x_n]\}$. Jónsson and Tarski[JT50] proved that this definition yields a modal homomorphism from $(A, \vee, \neg, 0, \tau)$ into $(\mathcal{P}(U_A), \cup, -, \emptyset, \sigma(\tau))$:

$$\sigma(\triangle(p_1, ..., p_n)) = \sigma(\triangle)(\sigma(p_1), ..., \sigma(p_n)).$$

Hence every modal algebra is isomorphic to a subalgebra of a powerset algebra. As a corollary, any term valid in A is valid in its ultrafilter algebra. Furthermore, if A is finite, then σ constitutes an isomorphism. This *representation theorem* is fundamental to modal duality theory.

Let us try to illustrate the ultrafilter construction with our example program and $\tau = \{ok, ko, \langle put \rangle\}$. The modal algebra A contains at least the elements $\{0, 1, ok, ko\}$. Other elements of A can be constructed as $lo \triangleq \langle put \rangle ok$, $el \triangleq ko \vee lo$, and $hi \triangleq -el$, and $eh \triangleq ko \vee hi$. A validates the following terms: $lo \leq \langle put \rangle hi$, $hi \leq \langle put \rangle ko$, and $ko \leq [put](0)$. Therefore A can be pictured as follows:



The ultrafilters of A are $u_{lo} \triangleq \{lo, ok, el, 1\}$, $u_{er} \triangleq \{ko, el, eh, 1\}$, and $u_{hi} \triangleq \{hi, ok, eh, 1\}$. The representation function σ is obvious: it maps e.g. $lo \mapsto \{u_{lo}\}$ and $ok \mapsto \{u_{lo}, u_{hi}\}$. It is easy to see that this map defines a modal isomorphism. Note that for the type $\tau = \{ok, ko, \langle R \rangle\}$, no additional elements besides $\{0, 1, ok, ko\}$ are generated; lo and hi cannot be distinguished in this language.

Consider the special case that the boolean algebra $(A, \vee, \neg, 0)$ is a relation algebra, providing additional operators $\circ$, $\smile$, and id. That is, we regard relations as objects rather than transitions between objects. As usual we write $\circ$ and $\smile$ in infix and postfix notation and assume that the axioms of relational algebra are valid. It is easy to verify from these axioms that $\circ$ and $\smile$ are normal and additive, so $(A, \vee, \neg, 0, \circ, ^{\smile}, id, \tau)$ is indeed a modal algebra. We call such a structure a *modal relation algebra*.

Under which conditions can the operators from τ be represented in the relation algebra? A *relational representation* ρ of the n-ary operator $\triangle$ is any relational expression $\rho(\triangle)$ containing n variables such that for all $a_1, ..., a_n \in A$ we have $\triangle(a_1, ..., a_n) = \rho(\triangle)(a_1, ..., a_n)$. According to this definition, propositions (0-ary operators) must be represented by their denotation in the algebra. In general, most binary operators will not admit a relational representation.

Call a unary operator $\Diamond$ *associative* if $\Diamond(p \circ q) = \Diamond(p) \circ q$. Then $\Diamond$ is associative if and only if $\Diamond(p)$ is represented by $R \circ p$, where $R = \Diamond(id)$ is an element of A.

Every associative operator is conjugated: If $\Diamond(p) = R \circ p$, then $\Diamond(p) \wedge q = 0 \;\leftrightarrow\; p \wedge \Diamond^{\smile}(q) = 0$ for $\Diamond^{\smile}(q) \triangleq R^{\smile} \circ q$.

In the modal encoding of relations as operators we defined for any binary relation R an operator $\langle R \rangle$ by requiring for all $x, y \in W$ that $x \in \langle R \rangle(y)$ iff $(x, y) \in R$. Call a unary operator $\Diamond$ in a modal relation algebra A *internal*, if there exists a relation $R \in A$ such that for all points $x, y \in A$ we have $x \leq \Diamond(y)$ iff $x \circ y^{\smile} \leq R$. (Recall that a *point* is any element $y \neq 0$ with $y = y \circ 1$ and $y \circ y^{\smile} \leq id$.)

Any associative operator is internal. For, if y is a point, then for all x it holds that $x \leq R \circ y$ iff $x \circ y^{\smile} \leq R$. Proof: Let $x \leq R \circ y$. Then $x \circ y^{\smile} \leq R \circ y \circ y^{\smile}$, which implies $x \circ y^{\smile} \leq R$ since y is a point. To prove the other direction, we note that for any point y, it holds that $1 \circ y = 1 \circ y \circ 1 = 1$. Therefore $(R \circ y) \vee (-R \circ y) = 1$, which can be written as $x \wedge -(R \circ y) \leq x \wedge (-R) \circ y$ by boolean transformations. Assuming $x \circ y^{\smile} \leq R$, or, equivalently, $x \wedge (-R) \circ y = 0$, we have $x \wedge -(R \circ y) = 0$, showing that $x \leq R \circ y$. To sum up, $\Diamond$ is internal if for all y which are points, $\Diamond(y) = R \circ y$.

Any relational representation ρ of all modal operators in τ induces a translation PT^{ρ} of modal formulas into relation algebraic terms. Since in general $PT^{\rho}(\varphi)$ is not a right ideal, we call the translation *purely relational*.

$PT^{\rho}(P) = P$ for any proposition or variable P, and

$PT^{\rho}(\Diamond\varphi) = \Diamond \circ PT^{\rho}(\varphi)$ for associative operators.

2.2 Algebraic Characterizations of Definability

Any formula φ *defines* the set of models or frames g with $g \models \varphi$. Can the class of models or frames defined by a given formula be characterized with algebraic means?

We introduced several languages which can be compared with respect to definability:

- *MS:* basic multimodal sentences of type τ,
- *ML:* basic multimodal formulas (with propositional variables),
- *RA:* the language of variable-free relation algebraic terms,
- *qRA:* the language of relation algebraic terms with relation variables,
- $\mathcal{L}_o$: first order predicate logic of type τ'
- $q\mathcal{L}_o$: universal monadic second order logic of type τ'.

Standard translations like those of Section 2.1 establish a syntactic containment between these languages as follows:

$$\begin{array}{ccc} \mathcal{L}_o & \longrightarrow & q\mathcal{L}_o \\ \uparrow & & \uparrow \\ RA & \longrightarrow & qRA \\ \uparrow & & \uparrow \\ MS & \longrightarrow & ML \end{array}$$

As we will see, all of the above inclusions are proper.

Since in no formula from *MS*, *RA*, or $\mathcal{L}_o$ proposition variables apppear, with these formalisms there is no difference between definability of frame classes or model classes: A class $\mathcal{K}$ of frames is defined by, e.g., a modal sentence φ iff the class $\mathcal{M}(\mathcal{K})$ of all models based on $\mathcal{K}$ is defined by φ. Thus, we only have to consider definability of classes of frames.

A first characterization of the expressivity of modal sentences can be given as follows: precisely those classes are definable which are defined by first order sentences elementary equivalent (i.e., equivalent for all first-order sentences) to the standard translation of a modal sentence.

Equivalence to standard translations of modal sentences, however, can also be formulated without the notion of elementary equivalence. For frames $g = (W, \mathcal{R})$, $g' = (W', \mathcal{R}')$ and $x \in W$, $y \in W'$, we say that (g, x) and (g', y) are *modally equivalent* ($(g, x) \equiv_{\text{MS}} (g', y)$), if $g, x \models \varphi$ iff $g', y \models \varphi$ for all modal sentences φ. A function $f : W \to W'$ between frames $g = (W, \mathcal{R})$ and $g' = (W', \mathcal{R}')$ is called a *p–morphism*[Seg71], if for all $\triangle \in \tau$ and all $x_0 \in W$, $y_0 \in W'$ such that $f(x_0) = y_0$ we have

For all $x_1, ..., x_n \in W$ with $\mathcal{R}(\triangle)(x_0, x_1, ..., x_n)$ there are $y_1, ..., y_n \in W'$ such that $\mathcal{R}'(\triangle)(y_0, y_1, ..., y_n)$ and $f(x_i) = y_i$ for $1 \leq i \leq n$;

For all $y_1, ..., y_n \in W'$ with $\mathcal{R}'(\triangle)(y_0, y_1, ..., y_n)$ there are $x_1, ..., x_n \in W$ such that $\mathcal{R}(\triangle)(x_0, x_1, ..., x_n)$ and $f(x_i) = y_i$ for $1 \leq i \leq n$;

A frame g' is called a p–morphic image of g, if there is a p–morphism $f : W \to W'$. We write $g \hookrightarrow g'$ or $(g, x) \overset{f}{\hookrightarrow} (g', y)$ if g' is a p–morphic image of g with $f(x) = y$. For the basic monomodal language, $(g, x) \overset{f}{\hookrightarrow} (g', y)$ iff

$R \circ f = f \circ R'$, and

$g, x \models P$ iff $g', y \models P$ for all propositions P.

In computer science, *bisimulations* are a concept which often replace p–morphisms. Bisimulations are equivalence relations satisfying the same conditions as above (i.e., instead of requiring f to be a function with $f(x_i) = y_i$, for a bisimulation we require f to be an equivalence relation with $f(x_i, y_i)$). Thus p–morphism can be seen as special bisimulations. Vice versa, if f is a bisimulation between g and g', then the function mapping any x in the domain of f to the equivalence class of some bisimilar w' is a p–morphism.

Now, p–morphisms are precisely those homomorphisms which preserve modal equivalence: If $(g, x) \hookrightarrow (g', y)$, then $(g, x) \equiv_{\text{MS}} (g', y)$. This can be easily shown by induction on the structure of φ.

For any set Φ of modal formulas, we write $g, x \models \Phi$ if $g, x \models \varphi$ for all $\varphi \in \Phi$. Note that $g, x \models \Phi$ only if $g, x \models \Phi_o$ for all finite $\Phi_o \subseteq \Phi$. A frame $g = (W, R)$ for the basic modal language is *modally saturated* if for all $x \in W$ and all sets Φ of modal formulas the following holds: there is a $y \in W$ with $R(x, y)$ and $g, y \models \Phi$ iff $g, x \models \langle R \rangle \bigwedge \Phi_0$ for all finite $\Phi_o \subseteq \Phi$. The frame g is *image finite* if for all $x \in W$ the set $\{y : R(x, y)\}$ is finite. All finite frames are image finite; all image finite frames are modally saturated.

Let g, and g' be modally saturated frames such that (g, x) and (g', y) are modally equivalent. Then there is a p–morphism $(g, x) \hookrightarrow (g', y)$. This can be proved by an indirect argument: let $(g, z) \equiv_{\text{MS}} (g', z')$, and assume that not $(g, z) \hookrightarrow (g', z')$. That is, for any morphism $f : x \mapsto x'$ we can find y or y' such that

i: $R(x, y)$ and for all y' with $R'(x', y')$ is $y' \neq f(y)$, or

ii: $R'(x', y')$ and for all y with $R(x, y)$ is $y' \neq f(y)$.

We derive a contradiction from case i, case ii being essentially symmetric. Assume that for any y' with $R'(x', y')$ we have $y' \neq f(y)$. Then by induction hypothesis for any such y' there is a sentence $\varphi_{y'}$ with $g', y' \models \varphi_{y'}$, but $g, y \not\models \varphi_{y'}$. Now, let $\Phi \triangleq \{\neg\varphi_{y'} : R'(x', y')\}$. Per construction $g, y \models \Phi$, and thus for every finite $\Phi_o \subseteq \Phi$ we have $g, x \models \langle R \rangle \bigwedge \Phi_o$. Furthermore, for any y' with $R'(x', y')$ it holds that $g', y' \not\models \Phi$, since $g', y' \models \varphi_{y'}$, and $\neg\varphi_{y'} \in \Phi$. By modal saturation, there is a finite $\Phi_o \subseteq \Phi$ with $g', x' \not\models \langle R \rangle \bigwedge \Phi_o$, in contradiction to the assumption.

We have shown that modally saturated frames can be characterized "up to p–morphism" by modal sentences. The restriction to modally saturated frames reflects the finiteness of the language; it provides a compactness argument, which could be dropped if modal languages contained infinite conjunctions. Another way to arrive at an exact algebraic characterization of modal sentences is to weaken the notion of p–morphism:

A *partial* p–morphism is a partial function which is a p–morphism on its domain. Let $g = (W, \mathcal{R})$ and $g' = (W', \mathcal{R}')$ be frames. Then (g', x') is a *finitely p–morphic image* of (g, x), if there is a sequence (F_n) of sets of partial p–morphisms $(g, x) \hookrightarrow (g', x')$ such that

> for any $f \in F_{n+1}$, and $x_0, ..., x_n \in W$ such that $x_0 \in dom(f)$ and $\mathcal{R}(\triangle)(x_0, ..., x_n)$ for some $\triangle \in \tau$, there is an $f' \in F_n$ such that $domf \subseteq domf'$, $ranf \subseteq ranf'$ and $x_1, ..., x_n \in domf'$, and
>
> for any $f \in F_{n+1}$, and $y_0, ..., y_n \in W$ such that $y_0 \in ranf$ and $\mathcal{R}(\triangle)(y_0, ..., y_n)$ for some $\triangle \in \tau$, there is an $f' \in F_n$ such that $domf \subseteq domf'$, $ranf \subseteq ranf'$ and $y_1, ..., y_n \in ranf'$.

If (g, x) is a finitely p–morphic image of (g', x'), then it can be shown by induction on the nesting of modal operators, that for any sentence φ it holds that $g, x \models \varphi$ iff $g', x' \models \varphi$. Vice versa, if (g, x) and (g', x') are modally equivalent, then we can construct a sequence of sets of partial p–morphisms with extending domains and ranges, asserting that (g', x') is a finitely p–morphic image of (g, x).

The above idea can be transformed into an algorithm that checks whether two finite frames are modally equivalent: Start with all mappings $x \mapsto x'$ such that x and x' satisfy the same propositions, and systematically try to extend this mapping for all worlds reachable from any world in the domain or range of any already constructed mapping. Upon termination this algorithms delivers a partial p–morphism from the strongly connected component containing x, or a modal sentence distinguishing the two frames. Many computer aided verification systems incorporate an algorithm for checking bisimulation equivalence which is based on this method.

Using the notion of p–morphism, [Ben89] gives a characterization of definability of basic multimodal sentences relative to first order logic: Any $\mathcal{L}_o$–formula is invariant for p–morphisms iff it is equivalent to (the standard translation of) a modal sentence.

As an example we prove that the term $R^{\smile} \circ R \leq R$, or, equivalently, the first-order sentence E : $\forall xyz\,[R(x, y) \wedge R(x, z) \rightarrow R(y, z)]$ cannot be expressed by a modal sentence. We give two frames $g = (W, R)$ and $g' = (W', R')$ such that g is the p–morphic pre–image of g', and g' satisfies E, but g does not. Let $W \triangleq \{a, b, c, d, e\}$ with $R \triangleq \{(a, b), (a, c), (b, c), (c, b), (b, e), (c, d), (d, e), (e, d)\}$, and $W' \triangleq \{1, 2, 3\}$ with $R' \triangleq \{(1, 2), (1, 3), (2, 3), (3, 2)\}$. The mapping f given by $a \mapsto 1$, $b \mapsto 2$, $c \mapsto 3$, $d \mapsto 2$, $e \mapsto 3$ is the required p–morphism $g \rightarrow g'$. However, even though the validity of E is not preserved under p–morphic pre–images, it can be proved that it is preserved under p–morphic *images*; that is, if $g, x \models E$ and $(g, x) \hookrightarrow (g', y)$, then $g', y \models E$.

In the case of modal formulas with propositional variables, axioms essentially are Π^1_1–sentences. For this language the theorem above could be used to characterize definability of sets of models; however, axioms usually are used to define classes of frames. Although axioms in general are not invariant under p–morphisms, they are preserved: If $(g, x) \hookrightarrow (g', y)$ and $g, x \models \varphi$, then $g', y \models \varphi$.

Further invariances are for generated subframes, disjoint unions, and ultrafilter expansions:

Let $g = (W, \mathcal{R})$ be a standard frame for the basic multimodal language, and S be the reflexive transitive closure of $\bigcup\{\mathcal{R}(R) : \langle R\rangle \in \tau\}$. For any world $x \in W$, the *generated subframe* $g_x = (W_x, \mathcal{R}_x)$ of g is defined by $W_x \triangleq \{y : S(x, y)\}$, and $\mathcal{R}_x(R) \triangleq R_x$, where R_x is the restriction of R to $W_x \times W_x$. It is easy to see that any modal formula is valid in a frame only if it is true in all of its generated subframes.

As a sideline, invariance of first order sentences under generated subframes can be characterized itself. This was was shown by Goldblatt and Feferman: *Existentially restricted* $\mathcal{L}_o$–formulas are built from propositions and negated propositions using conjunction, disjunction, universal quantification and restricted existential quantification of the form $\exists y\,[R(x, y) \wedge ...]$. (Note that any modal sentence is an existentially restricted $\mathcal{L}_o$–formula using only restricted universal quantification.) An $\mathcal{L}_o$ sentence is preserved under generated subframes iff it is equivalent to an existentially restricted $\mathcal{L}_o$ sentence.

The *disjoint union* of two frames $g = (W_g, \mathcal{R}_g)$ and $h = (W_h, \mathcal{R}_h)$ is the frame $g+h = (W_g \dot{\cup} W_h, \mathcal{R}_{g+h})$, where $W_g \dot{\cup} W_h$ is the disjoint union of W_g and W_h and $\mathcal{R}_{g+h}(R)(x,y)$ iff $\mathcal{R}_g(R)(x,y)$ or $\mathcal{R}_h(R)(x,y)$. Modal formulas are invariant under disjoint unions: $g+h \models \varphi$ iff $g \models \varphi$ and $h \models \varphi$.

Recalling the construction of the ultrafilter extension from 6.1.1, we can characterize definability of modal axioms with respect to first order logic. Let $\mathcal{K}$ be a frame class which is closed under elementary equivalence. Then $\mathcal{K}$ is definable by a modal formula iff $\mathcal{K}$ is closed under generated subframes, disjoint unions, and p–morphic images, and the complement of $\mathcal{K}$ is closed under ultrafilter extensions.

This theorem can be used to disprove modal definability. For example, there is no basic modal formula defining all frames with $R = 1$. It is immediate, that the disjoint union of the universal relations of two frames g and h is not universal in the frame $g+h$. Another example of a relational property which is not definable by any modal axiom is irreflexivity: $R \leq -Id$. This can be shown using preservation of modal formulas by p–morphisms: The frame $(\{a\}, \{(a,a)\})$ is a reflexive p–morphic image of the frame (ω, S), where ω is the set of natural numbers, S is the successor relation (irreflexive), and $f(i) = a$ for all $i \in \omega$.

The above definability considerations can be extended from modal logic to relational or predicate logic. Whereas "modal equivalence" can be checked by means of (partial) p–morphisms, in first order logic elementary equivalence can be checked by means of partial isomorphisms. Let $g = (W, \mathcal{R})$ and $g' = (W', \mathcal{R}')$ be frames. A partial function $f : g \rightarrow g'$ is called a *partial isomorphism*, if

f is injective, i.e., $x_0 = x_1$ iff $f(x_0) = f(x_1)$, and

$\mathcal{R}(R)(x_0, \ldots, x_n)$ iff $\mathcal{R}'(R)(f(x_0), \ldots, f(x_n))$

Two frames g, g' are called *finitely isomorphic*, if there is a sequence (F_n) of sets of partial isomorphisms $g \rightarrow g'$ with:

for $f \in F_{n+1}$ and $x \in W$ there is an $f' \in F_n$ with $f' \supseteq f$ and $x \in dom f'$;

for $f \in F_{n+1}$ and $y \in W'$ there is an $f' \in F_n$ with $f' \supseteq f$ and $y \in ran f'$.

Compared to partial p–morphisms, partial isomorphisms yield a stronger condition on f, as they additionally require $\mathcal{R}'(R)(f(x_0), ..., f(x_n)) \rightarrow \mathcal{R}(R)(x_0, ..., x_n)$. Finite isomorphisms are to elementary equivalence what finite p–morphisms are to modal equivalence: Fraissé proved that two frames satisfy the same first-order formulas iff they are finitely isomorphic. Van Benthem and Doets use this theorem to show that a class $\mathcal{K}$ of models is definable by a first order sentence iff there exists an n such that $\mathcal{K}$ is invariant for finite isomorphisms of level n.

For relation algebras we mention another approach to characterize its expressivity: As we have seen, the standard translation of a basic multimodal formula yields a first order formula with at most two individual variables. Similarly, the calculus of relations can be understood as a proper subformalism of first order logic. Every relation algebraic term t can be translated into an $\mathcal{L}_o$ formula $ST(t)$ with two free variables x_0, x_1 and one bounded variable. Thus this term is valid in a frame iff the universal closure of the translation is valid in this frame: $g \models t$ iff $g \models \forall x_0, x_1 [ST(t)]$. We say that RA is contained in the *3–variable fragment* of $\mathcal{L}_o$.

As an example, $(Q \wedge S \circ R^{\smile}) \circ R \leq Q$ can be translated into
$\forall x_0, x_1 [\exists x_2 [Q(x_0, x_2) \wedge \exists x_1 [S(x_0, x_1) \wedge R(x_2, x_1)] \wedge R(x_2, x_1) \rightarrow Q(x_0, x_1)]]$.

Givant and Tarski[GT87] showed that also the converse direction is true: For every $\mathcal{L}_o$–sentence with at most three variables there is an equivalent variable-free relation algebraic term. Put differently, relation algebra is *expressively complete* with respect to the 3–variable fragment of $\mathcal{L}_o$. (To be more specific, relation algebra is expressively complete w.r.t. the 3–variable fragment of $\mathcal{L}_o$ with at most two free individual variables.) As the proof of this theorem is constructive, an algorithm may be given which computes the relation algebraic translation of any 3–variable formula.

From this theorem, an algebraic characterization of definability with relational terms can be developed by defining a suitable restricted version of finite isomorphisms. Additionally, this theorem can be used to show non-definability of certain properties in relation algebra. For example consider the first order frame property XX: $\forall x, y, z, u [Q(x,y) \wedge R(x,z) \wedge S(x,u) \rightarrow \exists v [T(y,v) \wedge U(z,v) \wedge V(u,v)]]$ It can be shown that XX needs at least four individual variables, so it cannot be expressed in RA. However, it can be defined in qRA with the following axiom: $\forall p,q\,[R\circ -(U\circ -p)\wedge S\circ -(V\circ -p)\rightarrow -(Q\circ -(T\circ(p\wedge q)))]$. These matters will be pursued further in Section 3.2.

3 Modal Logic as Relational Algebra

In this section we regard modal formulas as a special class of relational terms. First we present some well-known modal completeness and incompleteness results with implications for the relational language; then we describe how some modal axioms can be translated into variable–free relational terms.

3.1 Completeness and Incompleteness

Whereas in the previous section we focussed on the definitional power of modal formulas, in this section we will describe their deductive capabilities.

Let any type τ and set of variables V be given. Formally, a *modal logic* $\mathcal{L}$ is any set of modal formulas closed under propositional tautologies, modus pones, normality, additivity, replacement, and substitution of formulas for propositional variables. The smallest modal logic is $\mathbf{K}$; the largest logic is the one containing $\perp$, which consists of all formulas. If $\mathbf{X}$ is any set of formulas, then $\mathcal{L}(\mathbf{X})$ denotes the smallest logic containing $\mathbf{X}$.

This definition allows us to identify a logic $\mathcal{L}(\mathbf{X})$ with its axioms $\mathbf{X}$: For a formula φ, a set Φ of sentences and a set $\mathbf{X}$ of axioms, we write $\Phi \overset{\mathbf{X}}{\vdash} \varphi$, if $\varphi\in\mathcal{L}$, where $\mathcal{L}$ is the smallest logic with $\Phi\cup\mathbf{X}\subseteq\mathcal{L}$. If Φ is empty, it is omitted; also $\mathbf{X}$ is omitted whenever no confusion can arise. Note that in contrast to predicate logic, modal logic does not provide a deduction theorem: From $\Phi\cup\{\varphi\}\vdash\psi$ we are not allowed to conclude $\Phi\vdash(\varphi\rightarrow\psi)$.

To prove $\Phi \overset{\mathbf{X}}{\vdash} \varphi$ one has to give a *derivation* of φ from the assumptions Φ, i.e., a sequence of formulas such that the last element of this sequence is φ, and every element of this sequence is either from Φ, or a substitution instance of an axiom from $\mathbf{X}$, or the substitution instance of the consequence of a rule, where all premisses of the rule for this substitution appear already in the derivation.

As an example, let us derive monotonicity in $\mathbf{K}$. First, we note that the rule of replacement of provably equivalent subformulas (**Repl**: $(p \leftrightarrow q)\vdash(\varphi(p)\leftrightarrow\varphi(q))$) is *admissible*, i.e., does not increase the number of derivable formulas. We proceed as follows:

1.	$(\Diamond\neg q\rightarrow\Diamond\neg p\vee\Diamond\neg q)$	(**taut**)
2.	$(\Diamond\neg q\rightarrow\Diamond(\neg p\vee\neg q))$	(1,**add**)
3.	$(\Diamond\neg q\rightarrow\Diamond(\neg p\vee(p\wedge\neg q)))$	(2,**Repl**)
4.	$(\Diamond\neg q\rightarrow\Diamond\neg p\vee\Diamond(p\wedge\neg q)))$	(3,**add**)
5.	$(\neg\Diamond\neg p\wedge\Diamond\neg q\rightarrow\Diamond(\neg(p\rightarrow q)))$	(4,**Repl**)
6.	$(\Box(p\rightarrow q)\rightarrow(\Box p\rightarrow\Box q)$	(5,taut)

A formula φ *follows* from a set Φ of sentences in a class G of standard frames or models ($\Phi \overset{G}{\Vdash} \varphi$), if φ is valid in every frame or model of G which validates all $\psi\in\Phi$. $\mathbf{X}$ is called *correct* for G, if $\overset{G}{\Vdash}\varphi$ whenever $\overset{\mathbf{X}}{\vdash}\varphi$. Note that since any deduction can use only finitely many premisses, $\mathbf{X}$ is correct for G iff for all Φ it holds that $\Phi\overset{G}{\Vdash}\varphi$ whenever $\Phi\overset{\mathbf{X}}{\vdash}\varphi$.

Any set of formulas $\mathbf{X}$ is correct for the set $G(\mathbf{X})$ of frames in which all elements of $\mathbf{X}$ are valid: $\overset{\mathbf{X}}{\vdash}\varphi$ implies $\overset{G(X)}{\Vdash}\varphi$.

The converse direction of this statement is called the completeness problem: $\mathbf{X}$ is called *complete* for G if $\overset{G}{\Vdash}\varphi$ implies $\overset{\mathbf{X}}{\vdash}\varphi$. $\mathbf{X}$ is *strongly complete* for G if for all Φ, if $\Phi\overset{G}{\Vdash}\varphi$ then $\Phi\overset{\mathbf{X}}{\vdash}\varphi$. In contrast to the correctness statement, the two notions of completeness do not coincide: there are axiom systems complete for a certain class of models, but not strongly complete. The situation is the same as in more expressive languages like predicate logic or relational calculus: Some (classes of) models can be described by an infinite set of formulas, but not by any finite subset thereof.

The minimal logic $\mathbf{K}$ is strongly complete for the class G of all standard models, i.e., $\Phi\Vdash\varphi$ iff $\Phi\vdash\varphi$. The proof follows the so–called Henkin/Hasenjäger construction and is completely analogous to the proof of the representation theorem for boolean algebras sketched in 6.1.1: A set Ψ of formulas is *inconsistent with* Φ, if there is a finite subset $\{\psi_1, ..., \psi_n\} \subseteq \Psi$ such that $\Phi \vdash (\psi_1 \wedge ... \wedge \psi_n \rightarrow \bot)$. To prove strong completeness, we have to show that every formula consistent with Φ is satisfiable in a model validating Φ. For, if $\Phi \mid\!\models \varphi$, then no model validating Φ satisfies $\{\neg\varphi\}$; therefore $\{\neg\varphi\}$ is inconsistent with Φ, hence $\Phi \vdash \varphi$. (Without loss of generality, we can assume here Φ to be consistent with itself, or else $\Phi \vdash \varphi$ holds). Lindenbaum's extension lemma states that any set of formulas consistent with Φ can be extended to a maximal consistent set including Φ (by repeatedly adding ψ or $\neg\psi$, respectively).

The quotient algebra of modal formulas with respect to provable equivalence is called the *Lindenbaum algebra*, named LINDA in [DP90]. Maximal consistent sets are ultrafilters in this algebra. Now we define the analogon of the ultrafilter algebra: The *canonical model* for Φ is $(W, \mathcal{R}, \mathcal{V})$, where W is the set of maximal consistent sets which include Φ, $\mathcal{R}(\triangle) \triangleq \{(w_0, ..., w_n) : p_1 \in w_1 \wedge ... \wedge p_n \in w_n \rightarrow \triangle(p_1, ..., p_n) \in w_0\}$, and $\mathcal{V}(v) \triangleq \{w : v \in w\}$. The fundamental 'truth' or 'killing' lemma states that for any formula φ and maximal consistent set w it holds that $\varphi \in w$ iff $W, \mathcal{R}, \mathcal{V}, w \models \varphi$. In the inductive step for this lemma, we have to show that $\triangle\varphi_1...\varphi_n \in w$ iff $W, \mathcal{R}, \mathcal{V}, w \models \triangle\varphi_1...\varphi_n$. The 'if' direction being a direct consequence of the definition, assume that $\triangle\varphi_1...\varphi_n \in w$. We have to find maximal consistent sets $w_1, ..., w_n$ such that $(w, w_1, ..., w_n) \in \mathcal{R}(\triangle)$ and $\varphi_i \in w_i$ for $i \leq n$. Since $\vdash (\triangle\varphi_1...\varphi_n \wedge \nabla\psi_1...\psi_n \rightarrow (\triangle(\varphi \wedge \psi_1)\varphi_2...\varphi_n) \vee ... \vee (\triangle\varphi_1...\varphi_{n-1}(\varphi_n \wedge \psi_n)))$, for every $\nabla\psi_1...\psi_n$ in w there exists some k such that $\triangle\varphi_1...(\varphi_k \wedge \psi_k)...\varphi_n$ is in w. Fix an enumeration (j) of all formulas $\nabla\psi_1...\psi_n$ in w, and define n sequences u_i of consistent sets $u_{i,j}$ such that $\triangle \bigvee u_{1j} ... \bigvee u_{nj}$ is in w for all j. Let $u_{i,0} \triangleq \varphi_i$, and $u_{i,j+1} \triangleq u_{i,j} \cup \psi_i$ if $i = k$, or else $u_{i,j+1} \triangleq u_{i,j}$. (In the basic monomodal language, u_{1j} is just $\{\varphi_1\} \cup \{\psi_j : \Box\psi_j \in w\}$.) Let w_i be any maximal consistent extension of u_{ij}. Then $(w, w_1, ..., w_n) \in \mathcal{R}(\triangle)$, since for formulas $\varphi_1, ...\varphi_n$ the assumptions $\varphi_i \in w_i$ and not $\triangle\varphi_1, ..., \varphi_n \in w_0$ lead to a contradiction. Thus we have achieved our goal of constructing a model for any consistent set.

In fact, we have shown that any set of formulas is strongly complete for its canonical model. To show that a set of formulas is complete for a set G of models, a useful strategy is to show that the canonical model belongs to G, or, that the canonical model can be transformed into a model belonging to G. Such transformations include the unfolding of models into trees, and the collapse of the model with respect to bisimulation equivalence.

Note that the completeness proof can be improved: It is not necessary that maximal consistent sets are maximal in the space of all formulas; it is sufficient to consider maximality with respect to all subformulas of the given consistent set. This idea can be used to transform the above completeness proof into a decision algorithm: For any formula, there are only finitely many different subformulas, and hence only finitely many sets of subformulas. Call such a set w of subformulas *locally maximal consistent*, if

for any subformula ψ, either $\psi \in w$ or $\neg\psi \in w$, and

$\bot \notin w$, and

$(\psi_1 \rightarrow \psi_2) \in w$ iff $\neg\psi_1 \in w$ or $\psi_2 \in w$.

There are two approaches to deciding whether a given formula φ is satisfiable: The first, 'local' algorithm, is tableaux-based. We start with the set of all locally maximal consistent sets containing φ and try to systematically extend one of these to a model. Given a locally maximal consistent set w, we construct for any formula $\triangle p_1...p_n \in w$ as successors all n–tuples of locally maximal consistent sets $(w_1...w_n)$ which arise in the completeness proof. If there are no such successors, then w is unsatisfiable and we backtrack; otherwise we proceed to extend the successors. Since there are only finitely many locally maximal consistent sets, the process stabilizes. Either all initial nodes are unsatisfiable, or we have constructed a model for the formula.

The second, 'global' algorithm for testing satisfiability starts with the set W of all locally maximal consistent sets and the set of all $n+1$-tuples for any n-ary operator. It then iteratively deletes 'bad arcs' and 'bad nodes' until stabilization is reached. Bad arcs are tuples $(w, w_1, ..., w_n)$ such that w contains $\nabla\psi_1...\psi_n$, but for all $i \leq n$ it is not the case that $\psi_i \in w_i$. Bad nodes w contain a formula $\triangle p_1...p_n$, but there does no longer exist a tuple $(w, w_1, ..., w_n)$ with $\psi_i \in w_i$ for all $i \leq n$. The given formula is satisfiable iff upon termination there is a node left in which it is contained.

These two algorithms can be extended to yield more general algorithms for relational structures.

We proved completeness with respect to sets of models. However, axioms are usually used to define sets of frames. Thus we are looking for completeness statements of the kind "$\Vdash^{G} \varphi$ implies $\vdash^{\mathbf{X}} \varphi$", where G is a class of frames. We know that $\vdash^{\mathbf{X}} \varphi$ iff φ is valid in the set $G(\mathit{Subst}(X))$ of all models satisfying all substitution instances (of propositional variables with formulas) of $\mathbf{X}$. But, this set is much bigger than the set $G(X)$ of all models based on some frame for $\mathbf{X}$, because the latter models have to satisfy all substitution instances of $\mathbf{X}$, where variables are substituted with subsets of worlds. Since in general not all subsets of worlds are described by sentences, we can not infer that validity in all frames for $\mathbf{X}$ implies derivability from $\mathbf{X}$. In fact, there is a finite axiom set $\mathbf{X}$ and formula φ such that the question whether $\Vdash^{G(X)} \varphi$ is Σ_1^1–hard (and thus not recursively enumerable):

Consider our example program as the state transition diagram of a counter machine, which increments and decrements its counter with every *put* and *get* operation, respectively. We show how this machine can be coded by a finite set of formulas, such that every model of these formulas describes the sequence of memory states of a complete run.

Let $\tau \triangleq \{hi, lo, er, put, get, eoq, \langle X\rangle, \langle F\rangle, \langle M\rangle\}$. The operator $\langle X\rangle$ will be used to describe the execution steps of the program in time, the operator $\langle F\rangle$ to denote the transitive closure of $\langle X\rangle$, and the operator $\langle M\rangle$ to access the content of the memory. As we will see in the next section, the following axioms describe that X and M are functional ($X^{\smile} \circ X \leq id$ and $M^{\smile} \circ M \leq id$), form a half–grid ($M \circ X \leq X \circ M$), and that F is the transitive closure of X:

$$\langle X\rangle p \rightarrow [X]p, \qquad \langle M\rangle p \rightarrow [M]p$$

$$\langle M\rangle\langle X\rangle p \rightarrow \langle X\rangle\langle M\rangle p$$

$$\langle X\rangle p \vee \langle X\rangle\langle F\rangle p \rightarrow \langle F\rangle p, \qquad [F](p \rightarrow [X]p) \rightarrow ([X]p \rightarrow [F]p)$$

Using these relations, we will fix the propositions such that

the number of M^*–successors in any world labelled eoq is the value of the counter,

every world is labelled hi,lo, or er, according to the machine state it denotes,

every world is labelled put or get, according to which action is executed next.

So, here are the relevant sentences:

put increases the length of the counter by one:
$(put \wedge [M]\bot \rightarrow \langle X\rangle\langle M\rangle[M]\bot)$

get decreases the length of the counter by one:
$(\langle M\rangle(get \wedge [M]\bot) \rightarrow \langle X\rangle[M]\bot)$

Every world is exactly one of $\{put, get\}$ and $\{hi, lo, er\}$:
$(put \text{ xor } get) \wedge (hi \text{ xor } lo \text{ xor } er)$

All worlds reachable by M^* have the same marking:
$(P \rightarrow [M]P)$ for $P \in \{put, get, hi, lo, er\}$

eoq propagates only in one dimension:
$(eoq \rightarrow [X]eoq), \qquad [M]\neg eoq$

Transitions:
$(lo \wedge put \rightarrow [X]hi), \qquad (hi \wedge get \rightarrow [X]lo),$
$(lo \wedge get \rightarrow [X]er), \qquad (hi \wedge put \rightarrow [X]er),$
$(er \wedge get \rightarrow [X]er), \qquad (er \wedge put \rightarrow [X]\bot)$

For a conditional transition like "from er go to lo if counter is zero" we could use the sentence $(er \wedge eoq \wedge [M]\bot \rightarrow [X]lo)$. For a multiple counter machine, we can use a similar encoding with several memory access functions $\langle M_i \rangle$. Now there is a computation in which such a machine reaches a certain state (say, hi) infinitely often from its initial state iff the sentence $(lo \wedge eoq \wedge [M]\bot \wedge [F]\langle F\rangle hi)$ is satisfiable in a model validating all of the above axioms and sentences. Of course, for our example machine, we easily see that the formula is satisfiable; for all single counter machines this *recurrence problem* is decidable. But, for multiple counter machines the problem is Σ^1_1 complete, therefore also the problem whether any sentence follows from a set of axioms is Σ^1_1 hard. Recall that axioms are monadic Π^1_1-properties, so the problem is in Σ^1_1 as well.

However, there is a notion of completeness for frame consequences, which is inspired by the algebraic approach. Even though not every modal algebra is isomorphic to its ultrafilter algebra, modal algebras can be regarded as models in their own right. This viewpoint gives rise to a semantics more general than standard semantics:

A *general frame* is a structure $(W, \mathcal{R}, \mathcal{B})$, where $(W, \mathcal{R})$ is a standard frame, and $\mathcal{B}$ is a *domain for quantification*: a modal subalgebra of the powerset algebra on W. That is, $\mathcal{B}$ is a set of subsets of W closed under boolean operations as well as under modal operators: If $p_1, ..., p_n \in \mathcal{B}$, then $\triangle p_1...p_n \in \mathcal{B}$, where again $\triangle p_1...p_n \triangleq \{x_0 \in W : \exists x_1...x_n\, [\mathcal{R}(\triangle)(x_0, ..., x_n) \wedge x_i \in p_i, 1 \leq i \leq n]\}$. A model $(W, \mathcal{R}, \mathcal{V})$ is *based on* a general frame $(W, \mathcal{R}, \mathcal{B})$, if $\mathcal{V}(v) \in \mathcal{B}$ for every propositional variable v. An axiom φ is valid in a general frame g, if it is valid in all models based on g. Note that there are many more general frames than standard frames satisfying a given axiom; in fact, standard frames can be seen as the special case of general frames where $\mathcal{B} = \mathcal{P}(W)$.

For every consistent set of modal formulas there is a nontrivial modal algebra. Using this algebra as domain for quantification, we can construct for every consistent set $\mathbf{X}$ of axioms a general frame validating all elements from $\mathbf{X}$. Hence $\Vdash^{G} \varphi$ iff $\vdash^{\mathbf{X}} \varphi$, where G is the class of all general frames validating all elements of $\mathbf{X}$. This idea can even be extended to yield completeness results for more expressive formalisms like relational terms with variables or Σ^1_1 formulas.

3.2 Second-order to First-order

Standard translations of modal axioms can be regarded as universal second order formulas. We say that a modal axiom *corresponds to* some monadic Π^1_1 frame property. Sometimes, such a property can be expressed by a first order sentence. Vice versa, first order logic is a proper extension of the language of modal sentences; however, in some cases a first order formula which has no equivalent modal sentence can be described by a modal axiom. The important questions are: given a modal axiom, does it define a first-order property? And: given a first order property, is there a modal axiom describing it? In general, the complexity of these questions is not known. Thus, none of the methods for deriving first-order correspondences can be proved complete, they are proved relatively complete w.r.t. each other.

In this section we give a brief survey of the existing theory on modal correspondences, and investigate first order definability in relation algebras with propositional variables.

Consider the modal axiom $\mathbf{U}$: $(\Diamond p \rightarrow \Box p))$, which we met several times in the previous sections. It defines the first-order property of *functionality*, i.e., $\forall xyz\, [R(x, y) \wedge R(x, z) \rightarrow y = z]$. This correspondence can be established as follows: Assume a frame g for $\mathbf{U}$ such that $R(x, y)$ for some x, and a valuation assigning $\{y\}$ to p. Then x satisfies $\Box p$. Hence every z with xRz must satisfy p. But, given the choice of p, we see that z must be equal to y, establishing functionality. Now, assume a functional frame and a valuation for p which validates the antecedent of $\mathbf{U}$ in x. Thus, we have a successor y of x in p. Functionality establishes that y is the only successor of x, hence all successors of x are in p, establishing validity of $\mathbf{U}$. This proof displays the role of the proposition variables: they can be used as a kind of register for a certain individual variable.

U can also be defined by the relation algebraic sentence $R^{\smile} \circ R \leq id$. This can be shown with the relational translation of modal formulas from Section 2.1: $\mathbf{U}$ is translated into $R \circ p \leq -(R \circ -p)$, which is equivalent to $(R \circ -p) \wedge (R \circ p) = 0$, which is $conR \circ R \circ p \wedge -p = 0$, or, equivalently, $R^{\smile} \circ R \circ p \leq p$. Since the relation variable p can be substituted with any relation, this is equivalent to $R^{\smile} \circ R \leq id$.

Incompleteness of modal axioms w.r.t. standard frames can be obtained easily by certain correspondences:

$$(\Diamond\Diamond p \rightarrow \Diamond p) \qquad \mathbf{4}$$

$$(\Box(\Box p \rightarrow p) \rightarrow \Box p) \qquad \mathbf{W}$$

$$\Diamond(\Box\neg p \vee \Box p) \qquad \mathbf{M}$$

As we shall see, **4** corresponds to transitivity ($R \circ R \leq R$), every standard frame satisfying **W** must be irreflexive, and **4** and **M** imply the existence of certain reflexive worlds. So, there is no standard frame satisfying all of the above axioms, that is, their conjunction defines the first order frame property $\perp$. Nevertheless, the axioms are satisfiable in the general frame having the natural numbers as worlds, the usual "$<$"–relation as accessibility relation and the boolean algebra of finite and cofinite sets as domain for quantification. Hence $\perp$ cannot be derivable from **4**, **M** and **W**.

For a systematical approach to first order correspondences attention is restricted to those axioms for which the standard semantics is appropriate, that is, which are complete w.r.t. the property they define. Let φ be a modal axiom corresponding to the first order sentence ε. Then φ is *canonical* if the canonical frame for φ satisfies ε.

Normal modal logics, constructed from canonical axioms φ (with modus ponens and replacement as the only rules) are complete: the canonical frame for φ invalidates any formula which is not derivable from φ. If φ is canonical, the canonical frame is an ε–frame, thus φ is complete for ε.

Examples of non-canonical axioms are **W** and **M**. A detailed account on canonicity and correspondence can be found in [Gol88]. A very wide class of canonical axioms, which has a direct syntactical characterization, are the *Sahlqvist axioms*: conjunctions of formulas of the following kind: $(\psi(p_1, ..., p_k) \rightarrow \varphi(p_1, \ldots, p_k))$, where φ is positive in all of its arguments, and ψ is built from sequences $[R_1]...[R_j]\, p_i$ and $\top$ and $\perp$, using only conjunction and existential modalities.

Sahlqvist correspondences can be calculated automatically, see e.g. [OS95] for a detailed presentation. In this section we follow an alternative approach of second order quantifier elimination using certain extensionality priciples. The canonical frame satisfies the following two conditions:

$$x = y \;\leftrightarrow\; \forall p\,[p(y) \;\leftrightarrow\; p(x)]$$

$$R(x, y) \;\leftrightarrow\; \forall p\,[p(y) \rightarrow \exists y\,[R(x, y) \wedge p(y)]] \qquad Ext_R$$

the latter one being developed from the definition of the accessibility relation in the canonical frame. This idea is generalized into the following second order axiom system $\mathcal{C}$:

i: All first order tautologies;

ii: $A \rightarrow \forall p\,[A]$, if p is not free in A;

iii: $x = y \;\leftrightarrow\; \forall p\,[p(y) \;\leftrightarrow\; p(x)]$;

iv: $\forall p\,[A] \rightarrow A[p/\eta]$, for η any standard translation of a modal formula;

v: $\forall p\,[ST(p \rightarrow [R]\langle R^{\smile}\rangle p)]$ and $\forall p\,[ST(p \rightarrow [R^{\smile}]\langle R\rangle p)]$ for all $\langle R\rangle \in \tau$;

vi: $\forall p\,[ST([R^{\smile}]p \rightarrow \varphi)] \;\leftrightarrow\; ST(\varphi)[p(z)/R(z, x)]$ (φ positive in p)

The axiom Ext_R mentioned above is an instantiation of item *vi* in this list.

The correspondence problem in terms of $\mathcal{C}$ reduces to whether for a first order sentence ε and a modal axiom φ,

$$\vdash^{\mathcal{C}} \varepsilon \;\leftrightarrow\; \forall p_1...p_n\,[ST(\varphi)].$$

An induction on deductions in $\mathcal{C}$ shows that $\mathcal{C}$ is correct for canonical frames. Thus, for any $\mathcal{C}$–derivable equivalence of the type above, φ corresponds to ε, and φ is canonical and hence complete for ε. The system $\mathcal{C}$ is relatively complete: $\mathcal{C}$ proves all Sahlqvist correspondences[Hei95].

We now consider modal correspondences in a relation algebraic environment. To be conservative w.r.t. the treatment given above, we assume relation algebras with operators, where all $\Diamond$–operators are internal, that is, represented by the term $R \circ p$ for some element R of the relation algebra. Internal operators are residuated, thus continuous and conjugated.

Let (A, τ) be a relation algebra A with internal operators $\langle R \rangle$. An relation algebraic term t containing free variables v was defined to be valid in A, if $t[v/R]) = 1$ for all substitutions of variables with relations from A. However, we can define a weaker notion of validity by allowing only substitutions of variables with right ideal elements of A. Let qRA_r denote an internal qRA with variables from the subalgebra of right ideal elements of A, and qRA_g an internal qRA with quantification on all of A.

Furthermore there are several possibilities as to which terms are allowed as internal representation of operators:

conservative internal qRA: only relation constants R, S, 1, id, ... are allowed for operators;

liberal internal qRA: every variable-free relation algebraic term is allowed as an operator.

The expressivity of liberal qRAs is considerably stronger than that of conservative ones, as here for instance irreflexivity is defined by $\langle R \wedge id \rangle p \rightarrow \bot$. We will come back to this point in Section 4.

Now, we consider the correspondence problem for qRA_g. Compared to qRA_r, here we have additional structure on the algebra of the variables. In qRA_g, the following quantifier elimination principle holds:

$$\forall p\,[Q \circ p \rightarrow R \circ p] \quad \text{iff} \quad Q \leq R \qquad \textbf{qep}$$

The proof is immediate: from right to left it is monotonicity of the relational product; the other direction is achieved by specialization of p to the identity relation id. An immediate consequence is the modal correspondent to the relational product:

$$\langle Q \rangle \langle R \rangle p \;\leftrightarrow\; \langle S \rangle p \quad \text{iff} \quad Q \circ R = S$$

Even in liberal qRA_r, **qep** can be derived only under additional assumptions, such as the point-axiom. Many common modal first order correspondences can be obtained from **qep**. For instance, *reflexivity* ($id \rightarrow R$) translates into **T**: $p \rightarrow \langle R \rangle p$, and *transitivity* ($R \circ R \leq R$) becomes **4**: $\langle R \rangle \langle R \rangle p \rightarrow \langle R \rangle p$. We already gave a derivation of the corresponding axiom **U** for functionality. In Section 3.1 we defined the property that M and X form a half grid ($M \circ X \leq X \circ M$). By **qep**, this is equivalent to $\langle M \rangle \langle X \rangle p \rightarrow \langle X \rangle \langle M \rangle p$.

Conjugated operators reflect relational converses via the Prior-McTaggart axiom **PMcT**: $(p \rightarrow [Q] \langle R \rangle p \wedge [R] \langle Q \rangle p)$ iff $Q = R^{\smile}$ The proof is an easy relation algebraic deduction: Let $(p \rightarrow [Q] \langle R \rangle p)$, or equivalently $Q \circ -(S \circ p) \leq -p$. Thus we get $Q^{\smile} \circ p \leq R \circ p$, and with **qep**: $Q^{\smile} \leq R$. Symmetrically, the second axiom gives $R^{\smile} \leq Q$, together: $Q^{\smile} = R$.

Next, we prove a generic correspondence scheme **X**:

$$Q^{\smile} \circ V \leq S \circ U^{\smile} \quad \text{iff} \quad \langle V \rangle [U] p \rightarrow [Q] \langle S \rangle p\ .$$

By **qep** we have $Q^{\smile} \circ V \leq S \circ U^{\smile}$ iff $\langle Q^{\smile} \rangle \langle V \rangle p \rightarrow \langle S \rangle \langle U^{\smile} \rangle p$. This formula is equivalent to the required axiom.

The following correspondences can be proved by instanciating Q, V, S, and U in **X** with appropriate relations:

1.	$id \leq R$	$p \to \langle R \rangle p$	**T**
2.	$R \circ R \leq R$	$\langle R \rangle \langle R \rangle p \to \langle R \rangle p$	**4**
3.	$R^{\smile} = R$	$p \to [R]\langle R \rangle p$	**B**
4.	$R^{\smile} \circ R \leq id$	$\langle R \rangle p \to [R]p$	**U**
5.	$R^{\smile} \circ R \leq R$	$\langle R \rangle [R]p \to [R]p$	**E**
6.	$R^{\smile} \circ R \leq S$	$\langle R \rangle [S]p \to [R]p$	
7.	$R^{\smile} \circ R \leq R \vee R^{\smile}$	$[R]([R]p \to q) \vee [R]([R]q \to p)$	**Lem**
8.	$R^{\smile} \circ R \leq id \vee S \vee R$	$\langle R \rangle p \to [R](p \vee \langle R \rangle p \vee \langle S \rangle p)$	
9.	$R^{\smile} \circ R \leq R \circ R^{\smile}$	$\langle R \rangle [R]p \to [R]\langle R \rangle p$	**G**
10.	$R^{\smile} \circ R \leq Q \circ Q^{\smile}$	$\langle R \rangle [Q]p \to [R]\langle Q \rangle p$	
11.	$R^{\smile} \circ R \leq id \vee R \vee R^{\smile} \vee R \circ R^{\smile}$	$\langle R \rangle (p \wedge [R]p) \to [R](p \vee \langle R \rangle p)$	
12.	$id \leq R \circ R^{\smile}$	$[R]p \to \langle R \rangle p$	**D**
13.	$id \vee S \vee R \leq R \circ R^{\smile}$	$[R]p \vee \langle R \rangle [R]p \vee \langle S \rangle [R]p \to \langle R \rangle p$	
14.	$R^{\smile} \circ (R \wedge -(R^{\smile})) \leq R$	$(\langle R \rangle [R]p \to q) \vee [R]([R]q \to p)$	**F**
15.	$R^{\smile} \circ (R \wedge -(R^{\smile})) \leq R$	$\langle R \rangle [R]p \to (p \to [R]p)$	**R**
16.	$Q \circ (R \wedge -S) \leq U$	$\langle Q \rangle (\langle R \rangle p \wedge \neg \langle S \rangle p) \to \langle U \rangle p$	**Y**

We give a proof of **Y**. The variable-free version is obtained by substitution of p with id, and the other direction is proved by the following relational derivation:

1.	$-(S \circ p) \circ p^{\smile} \leq -S$	(ax)
2.	$R \circ p \wedge -(S \circ p) \leq (R \wedge -(S \circ p) \circ p^{\smile}) \circ (p \wedge R^{\smile} \circ -(S \circ p))$	
3.	$R \circ p \wedge -(S \circ p) \leq (R \wedge -(S \circ p) \circ p^{\smile}) \circ p$	(2)
4.	$R \circ p \wedge -(S \circ p) \leq (R \wedge -S) \circ p$	(1,3))
5.	$Q \circ (R \wedge -S) \leq U$	(ass)
6.	$Q \circ (R \wedge -S) \circ p \leq U \circ p$	(5,**qep**)
7.	$Q \circ (R \circ p \wedge -(S \circ p)) \leq U \circ p$	(4,6)

Using the same methods, we can derive correspondences even for richer modal languages such as liberal qRA_g with universal or difference operators. Even though completeness may be lost, correctness is guaranteed: we can derive only correspondences which are valid in all standard frames. This is because **qep** with quantification over right-ideals is correct for standard frames and can be proved in relation algebras with point-axiom.

4 Relational Algebra as Modal Logic

In the previous section we reviewed modal logics *per se* and scetched the impact of the results for more expressive formalisms. Now we try to extend the modal language according to the guidelines given in the relational approach. First we extend the semantics by the use operators with a fixed interpretation, and the syntax by admitting several kinds of deduction rules. Then we allow also recursive definitions of operators and relations.

4.1 Extensions of the Modal Language

As we have seen, various relational concepts like the universal relation cannot be characterized in modal logic. Thus we can try to extend the latter with these concepts. Doing so, we have to be careful to preserve the advantages we gained by using a restricted language (e.g., decidability).

A first obvious idea is to include special operators $\langle L \rangle$ (universal operator) or $\langle D \rangle$ (difference operator) into the type τ, with additional semantic clauses:

- $W, \mathcal{R}, \mathcal{V}, w \models \langle L \rangle \varphi$ iff there exists $w' \in W$ such that $W, \mathcal{R}, \mathcal{V}, w' \models \varphi$
- $W, \mathcal{R}, \mathcal{V}, x \models \langle D \rangle \varphi$ iff there exists $w' \neq w \in W$ such that $W, \mathcal{R}, \mathcal{V}, w' \models \varphi$

These operators were investigated in [Gor90] and [Rij93]. To get an impression of their defining power, consider the following examples:

($\langle L \rangle \langle R \rangle \top$) corresponds to $R \neq \emptyset$, which is undefinable in basic modal logic,

($[L][R]p \rightarrow p$) corresponds to $id \leq R^{\smile} \circ R$, or, equivalently, to $\langle R^{\smile} \rangle \top$,

($\langle L \rangle p \leftrightarrow p \vee \langle D \rangle p$), thus $\langle L \rangle$ is definable from $\langle D \rangle$,

($\langle R \rangle p \rightarrow \langle D \rangle p$) corresponds to irreflexivity $R \cap Id = \emptyset$, and

$R \cap Id \neq \emptyset$ has no correspondent axiom even with $\langle D \rangle$–operator.

A relation algebra is called *simple*, if it satisfies the *Tarski–rule*: $R \neq 0 \ / \ 1 \circ R \circ 1 = 1$. Similarly, we can extend the expressivity of the modal language by admitting modal derivation rules as a means of specification. A *standard rule* $\rho : \psi \ / \ \varphi$ consists of two modal formulas ψ and φ and closes the set of formulas of logic $\mathcal{L}$ under the condition: For any substitution *Subst* of propositional variables with formulas, $Subst(\psi)$ is in $\mathcal{L}$ implies that $Subst(\varphi)$ is in $\mathcal{L}$. E.g., the rule $p \rightarrow \langle R \rangle p \ / \ p \rightarrow \langle S \rangle p$ allows to derive $\langle S \rangle \top$ from $\langle R \rangle \top$.

A *modal sequent rule*([Kap87]) $\rho : \psi_1, ..., \psi_n \ / \ \varphi_1, ..., \varphi_m$ imposes the condition: $Subst(\psi_1) \in \mathcal{L}$ and ... and $Subst(\psi_n) \in \mathcal{L}$, implies $Subst(\varphi_1) \in \mathcal{L}$ or ... or $Subst(\varphi_m) \in \mathcal{L}$. Since modal logic is an extension of propositional logic, $Subst(\psi_1) \in \mathcal{L}$ and $Subst(\psi_2) \in \mathcal{L}$ iff $Subst(\psi_1 \wedge \psi_2) \in \mathcal{L}$. Thus rules with a finite set of antecedents $\{\psi_1, ..., \psi_n\}$ are equivalent to rules with a single antecedent $(\psi_1 \wedge ... \wedge \psi_n)$. Any axiom can be regarded a standard rule with antecedent $\top$, and every standard rule can be regarded a sequent rule with one consequent.

Let $\mathbf{X}$ be a set of (axioms or) rules. The formula φ is *derivable* from a set Φ of formulas in the system $\mathbf{X}$ ($\Phi \Vdash^{\mathbf{X}} \varphi$), if there is a *derivation tree* for φ. This is a finite tree of formulas, such that every leaf in this tree is φ, and every node of this tree is either from Φ, or one of the n children of a node x which are substitution instances of a consequence of a rule, such that all antecedents of this rule occur above x in the tree.

We define a (sequent) rule $\rho : \psi_1, ..., \psi_n \ / \ \varphi_1, ..., \varphi_m$ to be derivable in $\mathbf{X}$ ($\Vdash^{\mathbf{X}} \rho$), if there is a derivation tree with leafs from $\{\varphi_1, ..., \varphi_m\}$ from the assumptions $\{\psi_1, ..., \psi_n\}$. For standard rules, $\vdash^{\mathbf{X}} \psi \ / \ \varphi$ iff $\{\psi\} \Vdash^{\mathbf{X}} \varphi$. Note the difference to $\Vdash^{\mathbf{X} \cup \psi} \varphi$, which is $\Psi \Vdash^{\mathbf{X}} \varphi$ for the set Ψ of substitution instances of ψ!

A (sequent) rule $\rho : \psi_1, ..., \psi_n \ / \ \varphi_1, ..., \varphi_m$ is *valid* in an class of models G ($||\!\!\models^{G} \rho$), if for any $g \in G$ we have that $g \models \psi_1$ and ... and $g \models \psi_n$ implies $g \models \varphi_1$ or ... or $g \models \varphi_m$. It is valid in a class of frames, if it is valid in every model based on that class.

Thus " / " is interpreted as *global* consequence relation: $||\!\!\models^{G} \psi \ / \ \varphi$ iff for any frame g of G with $g \models \psi$ also $g \models \varphi$ holds; this in turn is true iff for all Φ, if $\Phi \ ||\!\!\models^{G} \psi$ then $\Phi \ ||\!\!\models^{G} \varphi$. Thus $||\!\!\models^{G} \psi \ / \ \varphi$ and $G \supseteq G'$ imply $||\!\!\models^{G'} \psi \ / \ \varphi$. The rule of replacement is valid in the class of all frames. A standard rule $\psi \ / \ \varphi$ is called *locally valid* in a class of frames G, if φ is valid *in every world* of every model of G in which ψ is valid. It is easy to see that $\psi \ / \ \varphi$ is locally valid in G iff $||\!\!\models^{G} (\psi \rightarrow \varphi)$. Thus, with local validity there is no difference in definability between axioms and standard rules. Furthermore, there are frames locally invalidating the rule of replacement, enforcing yet another interpretation for this rule. φ is called a *global frame consequence* of ψ in G ($||\!\!\models^{G} \psi \Rrightarrow \varphi$), if $||\!\!\models^{G} \psi$ implies $||\!\!\models^{G} \varphi$. Clearly, we have $||\!\!\models^{G} \psi \Rrightarrow \varphi$ if $||\!\!\models^{G} \psi \ / \ \varphi$ if $||\!\!\models^{G} \psi \rightarrow \varphi$.

Some observations about definability with rules are:

$\Box p \ / \ p$ corresponds to $id \leq R^{\smile} \circ R$, $[R]p \ / \ p$ is equivalent to $\langle R^{\smile} \rangle \top$,

the $\langle L \rangle$–operator is undefinable with standard rules: $R = 1$ has no correspondent standard rule, with $\langle L \rangle$–operator, every rule $\rho = \psi_1, ..., \psi_n \ / \ \varphi_1, ..., \varphi_m$ is equivalent to $([L]\psi_1 \wedge ... \wedge [L]\psi_n \rightarrow [L]\varphi_1 \vee ... \vee [L]\varphi_m)$,

$(p \vee [R]q) \ / \ p, q$ corresponds to $R = 1$ and is complete for this condition on models,

$\langle D \rangle$ is not definable from $\langle L \rangle$ even with rules.

In summary, standard rules give only a limited access to universal and converse relation, sequent rules and $\langle L \rangle$–operator are alternative choices to reason about a universal relation in modal logic, whereas the $\langle D \rangle$–operator is a further step towards more general logics.

Nevertheless, standard rules can be used to give simple correspondences for certain second order properties relevant to computer science, such as terminality, discreteness, and transitive closure. We develop axioms for these properties from intuitive rule characterizations.

A paths in a frame is a sequence of R–successors of any world for the given accessibility relation R. A frame is called *terminal* if it contains no infinite paths. Any terminal image finite frame is finite by Königs lemma. Finite frames may contain infinite paths: if R contains a world x such that $R(x, x)$, this trivial loop gives rise to an infinite path. A frame is called *strongly terminal* if in every infinite path each two neighbors are different. (This notion could be generalized to finite loops of arbitrary fixed length.)

The existence of infinite paths is expressed by the following second-order sentence:

$$\exists p \, [\exists x \, [p(x) \wedge (\forall y \, [p(y) \rightarrow \exists z \, [R(y, z) \wedge p(z)]])]]$$

Thus the frame g is terminal if the negation of that sentence holds:

$$\forall p \, [\forall y \, [p(y) \rightarrow \exists z \, [R(y, z) \wedge p(z)]] \rightarrow \forall x \, [\neg p(x)]]$$

This can be written in qRA_r as follows:

$$(p \leq \Diamond p) \ / \ \ p = 0 \qquad \textbf{(LR)}$$

Its dual version is the so-called Löb-rule: $(\Box p \rightarrow p) \ / \ p$.
Terminality implies irreflexivity $((R \wedge id) \circ p = 0)$:

1.	$(id \wedge R) \circ p = (id \circ id \wedge R) \circ p$	(ax)
2.	$(id \wedge R) \circ p \leq (id \wedge R) \circ (id \wedge R) \circ p$	(1)
3.	$(id \wedge R) \circ p \leq R \circ (id \wedge R) \circ p$	(2)
4.	$(id \wedge R) \circ p = 0$	(**LR**,3)

With transitivity, **(LR)** is equivalent to the already mentioned axiom **W**: $\Box(\Box p \rightarrow p) \rightarrow \Box p$
A frame contains an infinite path without trivial loops, if

$$\exists p \, [\exists x \, [p(x) \wedge (\forall x \, [p(x) \rightarrow \exists y \, [R(x, y) \wedge \neg p(y) \wedge \exists z \, [R(y, z) \wedge p(z)]]]])]]$$

Again, strong terminality can be described by the negation of this sentence, which can be translated into the following rule :

$$p \leq \Diamond(-p \wedge \Diamond p) \ / \ p = 0 \qquad \textbf{(Grz)}$$

An equivalent modal formula is the Grzegorczyk-axiom $\Box(\Box(p \rightarrow \Box p) \rightarrow p) \leq \Box p$

Every transitive standard frame for **(Grz)** is antisymmetrical $(R \wedge R^{\smile} \leq id)$. Antisymmetry can be derived in qRA_r from **4** and **(Grz)** with point-axiom. Using a nonrepresentable relation algebra, it can be shown that antisymmetry can not be derived from **4** and **(Grz)** alone. So, the *relational* **K4(Grz)** based on qRA_r is incomplete. However, antisymmetry can not be formulated as a modal formula. In fact, the *modal* **K4(Grz)** is complete.

Terminality is related to discreteness. A total-linear irreflexive frame is called *Dedekind-discrete* if it satisfies the following condition:

$$\forall p \, [((\exists x \, [p(x)] \wedge \exists x \, [\neg p(x)]) \wedge \forall x, y \, [p(x) \wedge \neg p(y) \rightarrow R(x, y)]) \rightarrow \exists uw \, [p(u) \wedge \neg p(w) \wedge \neg \exists v \, [R(u, v) \wedge R(v, w)]]]$$

This is defined in relation algebra with the following rule:

$$(1 \circ p) \wedge (1 \circ (-p)) = 1 \ , \quad p \circ -p^{\smile} \leq R \ / \ p^{\smile} \circ -(R \circ R) \circ -p = 1$$

A path p (on a linear frame) is *unbounded*, if every successor of any point in p has a successor which again is in p: $p \rightarrow [R]\langle R \rangle p$. A frame g is called *path-discrete*, if every infinite path is unbounded. So, path-discreteness is defined by the following pair of rules **(ZR)**:

$$p \leq \langle R \rangle p \ / \ p \leq [R]\langle R \rangle p \ , \qquad p \leq \langle R^{\smile} \rangle p \ / \ p \leq [R^{\smile}]\langle R^{\smile} \rangle p$$

In irreflexive, linear frames, these rules are equivalent to Dedekind-discreteness.

Let g be an irreflexive transitive standard frame. Then g has *greatest lower bounds* in every $w \in W$ iff g validates the first rule **(ZR)**, and, dually, g has *smallest upper bounds* in every $w \in W$ iff it satisfies the second one.

Changing the basic notion of path to paths without trivial loops allows us to generalize Dedekind-discreteness to reflexive (transitive, linear) frames as well:

A linear frame is *strongly path-discrete*, iff it satisfies the following Dummet rules **(DumR)**:

$$p \leq \langle R \rangle (-p \wedge \langle R \rangle p) \ / \ p \leq [R]\langle R \rangle p \ ,$$
$$p \leq \langle R^{\smile} \rangle (-p \wedge \langle R^{\smile} \rangle p) \ / \ p \leq [R^{\smile}]\langle R^{\smile} \rangle p$$

Again, with transitivity **(DumR)** is equivalent to the following axiom:

$$([R]([R](p \rightarrow [R]p) \rightarrow p) \wedge \langle R \rangle [R]p) \rightarrow [R]p$$

So, any linear frame g has *greatest lower bounds* iff it satisfies this axiom. Let R be the *next-step* relation of a program, and R^* its reflexive transitive closure . If R is functional, then R^* satisfies **(DumR)**.

4.2 Dynamic and Fixpoint Logic

We have seen that Peirce algebras extend modal algebras by admitting arbitrary operations on the operators. However, Peirce algebras do not provide a *Kleene star* for transitive closure of relations, which is a very important concept in computer science. To avoid undecidability caused by the nonrepresentability of relation algebras, in dynamic logic we start with a relation semilattice, i.e., we disallow complement and intersection of relations. A *Kleene algebra* is a relation semilattice A augmented with an additional operator $^* : A \rightarrow A$, such that

$$R \circ S^* \circ T = \sup{}_n R \circ S^n \circ T,$$

where $S^0 = id$ and $S^{i+1} = S \circ S^i$, and the supremum is with respect to the lattice order of A. A *dynamic algebra* is a Peirce algebra $(B, A, \langle\ \rangle, ?)$, where A is a Kleene algebra instead of a relation algebra, satisfying the following equality:

$$\langle R^* \rangle p = \sup{}_n \langle R^n \rangle p,$$

where the supremum is with respect to the lattice order in B.

Standard models for modal logics can be extended to standard models for dynamic algebras by defining R^* to be the reflexive transitive closure of R. A proof similar to the completeness proof sketched in Section 2.1 shows that every dynamic algebra is representable in a standard model. Hence propositional dynamic logic is complete; the following axioms and rule, in addition to **K**, give a complete deductive basis (see, e.g.,[Koz82]):

$$\langle R \vee S \rangle p \leftrightarrow (\langle R \rangle p \vee \langle S \rangle p)$$

$$\langle R \circ S \rangle p \leftrightarrow \langle R \rangle \langle S \rangle p$$

$$\langle p? \rangle q \leftrightarrow (p \wedge q)$$

$$\langle R^* \rangle p \leftrightarrow (p \vee \langle R \rangle \langle R^* \rangle p)$$

$\langle R\rangle p \to p \ / \ \langle R^*\rangle p \to p$

The last axiom and rule in this list are called *recursion axiom* and *induction rule*, respectively. To give a relational interpretation, the recursion axiom forces R^* to be any reflexive transitive relation containing R, and the induction rule determines R^* to be the smallest such relation: Let S be any relation with $id \le S$, $R \le S$ and $S \circ S \le S$. Then $R \circ S \le S \circ S$, hence $R \circ S \le S$. Assuming that from $R \circ p$ we can derive $R^* \circ p \le p$, we can infer $R^* \circ S \le S$. Since $id \le S$, we have $R^* \circ id \le R^* \circ S$, which gives $R^* \le S$.

Even with Kleene star, there are some properties of programs not expressible in dynamic logic. For example, our introductory example formula $[R^*]\langle R\rangle$ expresses that *every* execution of the program is nonterminating, its complement being the property that some execution halts. To assert that *every* computation halts, we extend the basic modal logic with recursive definitions of operators. By the above axioms, $\langle R^*\rangle$ is defined to be the smallest operator $\langle F\rangle$ satisfying $\langle F\rangle p \ \leftrightarrow\ (p \vee \langle R\rangle\langle F\rangle p)$ for all p. $\langle R^*\rangle p$ is the *least fixpoint* of the function f mapping every q onto $(p \vee \langle R\rangle q)$. We introduce a propositional quantification μ for least fixpoints and write $(\langle R^*\rangle p \ \leftrightarrow\ \mu q[p \vee \langle R\rangle q])$.

Formally, the μ–calculus can be seen as a sublanguage of monadic second order logic, via the standard translation:

$$ST(\mu q[\varphi]) \triangleq \forall q\,[\forall y\,[ST(\varphi)[x/y] \to q(y)] \to q(x)]$$

The property that every execution of a program terminates can be formulated in the propositional μ–calculus as $\mu q[[R]\top]$: The standard translation of this sentence amounts to $\forall q\,[q(x) \to \exists y\,[q(y) \wedge \forall z\,[R(y,z) \to \neg q(z)]]]$. Substituting for q the set of states of any complete execution sequence, we see that this sequence must be terminal.

All known program logics which are decidable can be embedded in the propositional μ–calculus. Moreover, this calculus itself is decidable and was recently shown to be complete by [Wal95]. The relevant recursion axiom and induction rule are:

$$\varphi[q/\mu q[\varphi]] \to \mu q[\varphi]$$

$$\varphi[q/p] \to p \ / \ \mu q[\varphi] \to p$$

The propositional μ-calculus is particularly useful for automatic program verification: Given a μ–calculus *specification* formula, and a model describing (the executions of) the program, we can give simple algorithms for testing whether the specification is satisfied by the program. This *model checking* problem has received much attention, and several elaborate data structures for the representation of relational models have been developed, see e.g. [BCMD+90].

References

[BBS92] C. Brink, K. Britz, R. Schmidt: Peirce algebras; Max-Planck-Institut für Informatik, Saarbrčken, Report MPI-I-92-229 (1992)

[BCMD+90] J. Burch, E. Clarke, K. McMillan, D. Dill, L. Hwang: Symbolic model checking, 10^{20} states and beyond, 5th LICS (1990)

[Ben89] J. van Benthem: Notes on modal definability; NDJFL 30(1):20-35 (1989)

[DP90] B. Davey, H. Priestley: Introduction to Lattices and Order; Cambridge Univ. Press (1990)

[Gol88] R. Goldblatt: Logics of Time and Computation; CSLI lecture notes 7, Stanford (1988)

[Gor90] V. Goranko: Modal definability in enriched languages; NDJFL 31(1):81-105 (1990)

[GT87] S. Givant, A. Tarski: A Formalization of Set Theory without Variables; AMS Quarterly Coll. Pub. 41, Providence, R.I. (1987)

[Hei95] W. Heinle, Expressivity and Definability in Extended Modal Languages; Verlag Shaker, Aachen (1995)

[JT50] B. Jonsson, A. Tarski: Boolean Algebras with operators; Trans AMS, pp.891-839 (1950)

[Kap87] B. Kapron: Modal sequents and definability; JSL 52(3):756-762 (1987)

[Koz82] D. Kozen: Results on the propositional μ-calculus; in: Proc. 9th ICALP, LNCS 140 (1982)

[Orl88] E. Orlowska: Relational interpretation of modal logics; in: Andreka, Monk, Nemeti (eds): Algebraic Logic, North Holland (1991)

[Rij93] M. de Rijke: Extending Modal Logic; ILLC Diss. Series 93-4, Univ. of Amsterdam (1993)

[Seg71] K. Segerberg: An essay in classical modal logic; Technical report, Dept. of Phil., Uppsala (1971)

[OS95] H.-J. Ohlbach, R. Schmidt: Functional translation and second-order frame properties of modal logics, Rep. MPI-I-95-2-002, Max-Planck-Inst., Stuttgart (1995)

[SS89] G. Schmidt, T. Ströhlein: Relationen und Graphen; Springer (1989)

[Sto36] M. Stone: The theory of representations for Boolean algebras; Trans AMS 40, pp.37-111 (1936)

[Wal95] I. Walukiewicz: Completeness of Kozens axiomatization of the propositional μ-calculus; LICS (1995)