Lecture Notes*

Prof. Dr. Ernst-Erich Doberkat
eed@doberkat.de

13 aprile 2019

We will

- show how to specify change through a suitable logic,
- provide a relational interpretation for it, thus giving life to transition systems,
- look at (co-)algebraic aspects of the corresponding models.

1 Modal Logics

Describe the dynamics of a system through the states the system will be in. This description is done through formulas, starting from a given set Φ of primitives. The grammar for the formulas looks like this:

$$\varphi ::= p \mid \bot \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi_1 \mid \Diamond\varphi_1$$

with $p \in \Phi$. Thus a formula is either a primitive formula, taken from Φ, or the bottom element $\bot$, the conjunction of two formulas, the negation of another formula, or of the form $\Diamond\varphi_1$ for formula φ_1. This symbol $\Diamond$ is new and pronounced as *sometimes*, thus $\Diamond\varphi_1$ reads *sometimes* φ_1.
Note that for convenience and easier legibility we do without parentheses, so we really specify trees here. However, we'll set parentheses whenever necessary, just for readability and for disambiguating formulas. Bear with me. We let unary operations bind stronger than binary operations.
We derive other operations:

Disjunction The disjunction $\varphi_1 \vee \varphi_2$ of formulas φ_1 and φ_2 is defined as $\neg\big(\neg\varphi_1 \wedge \neg\varphi_2\big)$.

top The top element $\top$ is defined as $\neg\bot$. While $\bot$ may be thought of representing false, $\top$ may be thought of representing true.

Implication Put $\varphi_1 \to \varphi_2$ as $\neg\varphi_1 \vee \varphi_2$, and the equivalence as $\varphi_1 \leftrightarrow \varphi_2$ as $(\varphi_1 \to \varphi_2) \wedge (\varphi_2 \to \varphi_1)$.

Box Define the box operator $\Box$ through $\Box\varphi$ as $\neg(\Diamond\neg\varphi)$. This may be thought of *necessity*, read $\Box\varphi$ as φ *holds by necessity*.

*These are the brief notes for my even briefer course on *Modal logics and their coalgebraic interpretation*, April 2 – April 10, 2019. Main sources are [1] and [2].

Example 1.1 Let $\Phi := \{p, q\}$ with the informal understanding that p means *it rains*, and q means *the street is wet*.

- $\Diamond p$ - it sometimes rains,
- $\Box(p \to q)$ - it is necessary the case that if it rains, then the street is wet.

How would you verbally describe $\Box(p \to q) \wedge p \to q$ and $\Box(\Box p \to p) \to \Box q$?
✌

The primitive formulas serve as the basic building blocks, they come from the outside, i.e., are external to the logic.
What do the formulas mean? The operators *sometimes* and *necessarily* indicate that some change is about to happen, which is modelled through transitions of states.

2 Relations and Transitions

Fix a set S of states, and write a transition from state s to state s' as $s \to s'$. This sets up a directed graph with elements from S as nodes and transitions as directed edges. Put

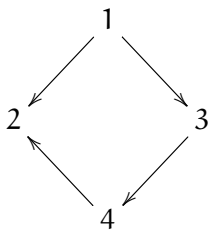
$$R := \{\langle s, s'\rangle \mid s \to s' \text{ is a transition}\},$$

then $R \subseteq S \times S$ is a relation on S. One writes sometimes aRb instead of $\langle a, b\rangle \in R$, in case of ambiguity one sometimes puts R as an index to the arrow: $a \to_R b$ is then equivalent to aRb.

Example 2.1 Let $S := \{1, 2, 3, 4\}$ and assume the transitions $1 \to 2$, $1 \to 3$, $3 \to 4$, $4 \to 2$. This yields the relation

$$\{\langle 1, 2\rangle, \langle 1, 3\rangle, \langle 3, 4\rangle, \langle 4, 2\rangle\}.$$

The corresponding graph looks like this:



✌

A relation $R \subseteq S \times S$ induces a map from $S \to \mathcal{P}(S)$, where $\mathcal{P}(S)$ is the power set of S. We denote this map also by R (it will be clear from the context whether we address a relation or the associated map). Put for $s \in S$

$$R(s) := \{s' \mid s \to s'\}$$

Evidently the representations above are equivalent in the sense that one may be derived from one of the others. These are the well-known operations on relations (R, R' relations on S):

Composition: $R \circ R' := \{\langle s, s''\rangle \mid \exists s' : sRs' \text{ and } s'R's''\}$. Thus $s \to_{R\circ R'} s''$ iff there exists some $s' \in S$ with $s \to_R s' \to_{R'} s''$.

Inversion: $R^{-1} := \{\langle b, a\rangle \mid \langle a, b\rangle \in R\}$. Thus $s \to_{R^{-1}} s'$ iff $s' \to_R s$, i.e., transitions are reversed.

Transitive closure: Put

$$\begin{aligned} \Delta &:= \{\langle s, s\rangle \mid s \in S\}, \\ R^0 &:= \Delta, \\ R^{n+1} &:= R^n \circ R, \end{aligned}$$

and define

$$\begin{aligned} R^+ &:= \bigcup_{n=1}^{\infty} R^n, \\ R^* &:= \Delta \cup R^+. \end{aligned}$$

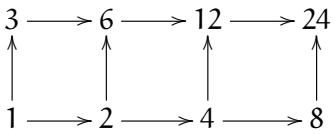
Then R^+ is the smallest transitive relation that contains R, and R^* is the smallest reflexive and transitive relation which contains R (remember: Relation Q is reflexive iff $\Delta \subseteq Q$ and transitive iff $Q \circ Q \subseteq Q$). Proof as a fai da te.

Example 2.2 Put

$$S := \{1, \ldots, 24\},$$

$R_1 := \{\langle a, b\rangle \mid a \text{ divides } b\}$,

R_2 is given through the graph below.



Another fai da te: $R_2^* = R_1$.

This observation is helpful since one sometimes provides only the skeleton of a relation, e.g., by omitting the transitive edges, as in this example. 🐰

3 Morphisms

Morphisms help comparing objects structurally. Consider as an example group morphisms. Let $(G, +)$ and $(H, *)$ be groups, then a map $f : G \to H$ is a group morphism iff $f(a + b) = f(a) * f(b)$ always holds (group morphisms are called usually group homomorphisms, but never mind). Let's write this a bit more complicated: put $m_+(a, b) := a + b$, thus $m_+ : G \times G \to G$, similarly $n_*(x, y) := x * y$, hence $n_* : H \times H \to H$. Finally, define $f \times f : G \times G \to H \times H$

as $(f \times f)(a, b) := \langle f(a), f(b)\rangle$, thus propagating f into the Cartesian product. Then f is a morphism iff this diagram commutes:

$$\begin{array}{ccc} G \times G & \xrightarrow{f\times f} & H \times H \\ {\scriptstyle m_+}\downarrow & & \downarrow{\scriptstyle n_*} \\ G & \xrightarrow[f]{} & H \end{array}$$

Check it out: $n_* \circ (f \times f) = f \circ m_+$ means for each $\langle a, b\rangle \in G$ that

$$\begin{aligned} f(a + b) &= f\big(m_+(a, b)\big) \\ &= \big(f \circ m_+\big)(a, b) \\ &= \big(n_* \circ (f \times f)\big)(a, b) \text{ (the diagram commutes)} \\ &= n_*\big((f \times f)(a, b)\big) \\ &= n_*(f(a), f(b)) \\ &= f(a) * f(b). \end{aligned}$$

Ok. For defining a morphism in our setting, we need to modify a map accordingly (just as we just fiddled around with f propagating it into the Cartesian product); this times we need sets, since we are dealing with sets and power sets. Assume that $f : M \to N$ is a map (for sets M and N), then f induces a map $\mathcal{P}(f) : \mathcal{P}(M) \to \mathcal{P}(N)$ upon setting

$$\mathcal{P}(f)(A) := \{f(a) \mid a \in A\},$$

so $\mathcal{P}(f)(A)$ collects all images from elements of A. This is also written as $f[A]$. Sometimes one needs also the inverse image $f^{-1}[B]$ of a set $B \subseteq T$:

$$f^{-1}[B] := \{a \in M \mid f(a) \in B\},$$

thus $m \in f^{-1}[B]$ iff $f(m) \in B$.

But now:

Definition 3.1 *Let R and R' be relations on the sets S and S', and $f : S \to S'$ be a map. Then f is said to be a* morphism $R \to R'$ *iff this diagram commutes*

$$\begin{array}{ccc} S & \xrightarrow{f} & S' \\ {\scriptstyle R}\downarrow & & \downarrow{\scriptstyle R'} \\ \mathcal{P}(S) & \xrightarrow[\mathcal{P}(f)]{} & \mathcal{P}(S') \end{array}$$

Thus a morphism $f : R \to R'$ is characterized by $R' \circ f = \mathcal{P}(f) \circ R$, this means that we have for each state $s \in S$

$$\begin{aligned} R'(f(s)) &= (R' \circ f)(s) \\ &= (\mathcal{P}(f) \circ R)(s) \\ &= \{f(s') \mid s' \in R(s)\} \\ &= \{f(s') \mid s \to_R s'\}. \end{aligned}$$

Rephrasing, we find that $f(s) \to_{R'} t$ iff there exists s' such that $s \to_R s'$ and $t = f(s)$.

This gives a characterization of morphisms which leans towards transitions.

Proposition 3.2 $f : S \to S'$ *is a morphisms* $R \to R'$ *iff these conditions hold:*

1. sRs' *implies* $f(s)R'f(s')$ *(the* forward *condition),*

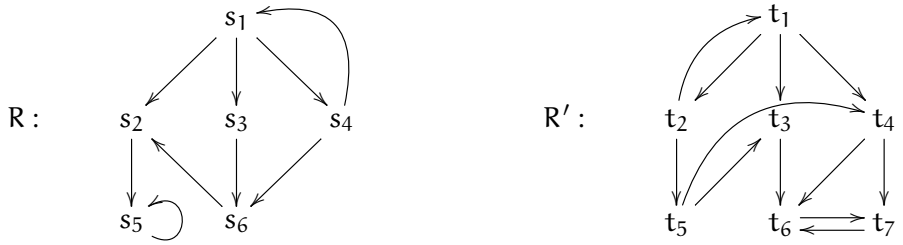
2. *if* $f(s)R't$*, then there exists* s' *with* sRs' *and* $t = f(s')$ *(the* backward *condition).*

The forward condition means that edges (or transitions) are preserved, the backward condition says that edges (or transitions) in the image can be traced.
Proof 1 $\Rightarrow$ 2: Assume that $R' \circ f = \mathcal{P}(f) \circ R$, hence that the diagram is commutative. The forward condition is satisfied: if $s \to_R s'$, then $s' \in R(s)$, so that $f(s') \in f[R(s)] = \mathcal{P}(f)(R(s))$. Thus $f(s') \in R'(f(s))$, so that $f(s) \to_{R'} f(s')$.
The discussion above shows that the backward condition is satisfied as well.
2 $\Rightarrow$ 1: Assume that both the forward and the backward condition hold, we want to show that for $s \in S$

$$R'(f(s)) = f[R(s)]\,.$$

" $\subseteq$ ": Assume that $t \in R'(f(s))$, which means $f(s)R't$, thus we find by the backward condition $s' \in R(s)$ with $f(s) \to_{R'} t = f(s')$, so that $t \in f[R(s)]$.
" $\supseteq$ ": If $t \in f[R(s)]$, we find $s' \in R(s)$ with $t = f(s)$, but this means $t \in R'(f(s))$, because $f(s) \to_{R'} f(s') = t$.
Because we have shown $f[R(s)] = \mathcal{P}(f)(R(s))$, the assertion that the diagram commutes follows immediately. $\dashv$
The diagram definition is algebraically more attractive, the forward/backward definition is sometimes more handy.

Example 3.3 Let $S = \{s_1, \ldots s_7\}$ and $S' = \{t_1, \ldots, t_7\}$.



Then there does not exist a morphism $R \to R'$. Why? A morphism $f : R \to R'$ would transport the loop s_5Rs_5 into a loop $f(s_5)R'f(s_5)$, which, however, does not exist.
We find, however, a morphism $R' \to R$; try this:

t	t_1	t_2	t_3	t_4	t_5	t_6	t_7
$f(t)$	s_1	s_4	s_3	s_2	s_1	s_6	s_5

The forward condition is satisfied: $\{\langle f(a), f(b)\rangle \mid aR'b\} \subseteq R$ by inspection. For checking the backward condition, we compute $R(f(t))$ and compare the result against $\mathcal{P}(f)(R'(t))$, for example:

- $t = t_1$, then $R(f(t_1)) = R(s_1) = \{s_2, s_3, s_4\}$, and $\mathcal{P}(f)(R'(t_1)) = f[\{t_2, t_3, t_4\}] = \{s_2, s_3, s_4\}$,
- $t = t_4$, then $R(s_2) = \{s_5, s_6\} = f[\{t_6, t_7\}] = \mathcal{P}(f)(R'(t_4))$.

Fai da te: Complete the comparisons on your own. ✌

4 Interpretations

Given a state space S (sometimes also called a set of *possible worlds*) and a relation $R \subseteq S \times S$, for interpreting the modal logic we need informations about the behavior of the primitive symbols. Since these symbols are external, we should expect that their interpretation, i.e., information on where they are valid, is external as well. For this, we assume that a map $V : \Phi \to \mathcal{P}(S)$ is given with the understanding that $V(p) \subseteq S$ is the set of all states in which p is true.
We now define inductively the validity relation $\models$ between states and formulas:

- $s \models p$ iff $s \in V(p)$, provided $p \in \Phi$,
- $s \models \bot$ is always false,
- $s \models \varphi_1 \wedge \varphi_2$ iff $s \models \varphi_1$ and $s \models \varphi_2$,
- $s \models \neg\varphi$ iff $s \models \varphi$ is false,
- $s \models \Diamond\varphi$ iff there exists a state s' with $s \to_R s'$ such that $s_1 \models \varphi$.

The interesting definition is of course the one for $s \models \Diamond\varphi$; it says that formula $\Diamond\varphi$ holds in state s iff we can find a transition from s to a state s' in which formula φ holds.

Example 4.1 Look at these formulas

- $s \models \varphi_1 \vee \varphi_2$ iff $s \models \varphi_1$ or $s \models \varphi_2$.
- $s \models \varphi_1 \to \varphi_2$ iff $s \models \varphi_1$ implies $s \models \varphi_2$.
- $s \models \Box\varphi$ iff $t \models \varphi$ for all t with $s \to_R t$, so φ must hold for all successors t of s: fai da te.

✌

Example 4.2 Put $\Phi := \{p, q, r\}$ as the set of propositional letters, $S := \{1, 2, 3, 4, 5\}$ as the set of states; relation R is given through

$$1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5$$

Finally, put

$$V(\ell) := \begin{cases} \{2, 3\}, & \ell = p \\ \{1, 2, 3, 4, 5\}, & \ell = q \\ \emptyset, & \ell = r \end{cases}$$

Then we have for (S, V, R) for example

$1 \models \Diamond\Box p$**:** This is so since $3 \models p$ (because $3 \in V(p)$), thus $2 \models \Box p$, hence $1 \models \Diamond\Box p$.

$1 \not\models \Diamond\Box p \to p$**:** Since $1 \notin V(p)$, we have $1 \not\models p$.

$2 \models \Diamond(p \wedge \neg r)$**:** The only successor to 2 in R is state 3, and we see that $3 \in V(p)$ and $3 \notin V(r)$.

$1 \models q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond q)))$**:** Because $1 \in V(q)$ and 2 is the successor to 1, we investigate whether $2 \models q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond q))$ holds. Since $2 \in V(q)$ and $\langle 2,3\rangle \in R$, we look at $3 \models q \wedge \Diamond(q \wedge \Diamond q)$; now $\langle 3,4\rangle \in R$ and $3 \models q$, so we investigate $4 \models q \wedge \Diamond q$. Since $4 \in V(q)$ and $\langle 4,5\rangle \in R$, we find that this is true. Let φ denote the formula $q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond(q \wedge \Diamond q)))$, then this peeling off layers of parentheses shows, however, that $2 \not\models \varphi$, because $5 \models \Diamond p$ does not hold.

$1 \not\models \Diamond\varphi \wedge q$**:** Since $2 \not\models \varphi$, and since state 2 is the only successor to 1, we see that $1 \not\models \varphi$.

$s \models \Box q$**:** This is true for all states $s \in S$, because $s' \in V(q)$ for all s' which are successors to some $s \in S$.

✌

It is sensible to put the state space, the map V and the relation R into one joint structure.

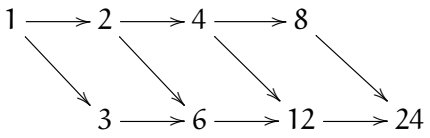
Definition 4.3 *The triplet* (S, V, R) *is called a* Kripke model *iff* S *is a set of states,* $V : \Phi \to \mathcal{P}(S)$ *is a map and* $R \subseteq S \times S$ *is a relation.*

Sometimes we talk only about a *model* (because we do deal only with this kind of models here). If we are working with more than one model, say, $\mathcal{M}$ and $\mathcal{M}'$, we emphasize validity by mentioning the model which we are working in, e.g., $\mathcal{M}, s \models \varphi$.

Example 4.4 We have two propositional letters p and q, as set of states we put $S := \{1,2,3,4,6,8,12,24\}$, and we say

$$x \to_R y \text{ iff } x \neq y \text{ and } x \text{ divides } y.$$

This is what R looks like without transitive arrows (see page 3):



Put $V(p) := \{4,8,12,24\}$ and $V(q) := \{6\}$. Define the Kripke model (S, V, R). We obtain for example

$4 \models \Box p$**:** The set of successor to state 4 is just $\{8,12,24\}$ which is a subset of $V(p)$.

$6 \models \Box p$**:** Here we may reason in the same way.

$2 \not\models \Box p$**:** State 6 is a successor to 2, but $6 \notin V(p)$.

$2 \models \Diamond(q \wedge \Box p) \wedge \Diamond(\neg q \wedge \Box p)$**:** State 6 is a successor to state 2 with $6 \models q \wedge \Box p$, and state 4 is a successor to state 2 with $4 \models \neg q \wedge \Box p$

✌

We denote for a given Kripke model (S, V, R) and for a formula φ the set

$$[\![\varphi]\!] := \{s \in S \mid s \models \varphi\}$$

as the set of all states in which formula φ holds, the validity set for φ. If the specific model is important, we add it as an index.
Fix a Kripke model $S, V, R)$, and put

$$R(A) := \{s \mid sRt \text{ for some } t \in A\}$$

for $A \subseteq S$. This is the set of all states which permit a transition into A.
We want to characterize the validity sets through set operations, and here we obtain

- $[\![\bot]\!] = \emptyset$ and $[\![\top]\!] = S$,
- $[\![p]\!] = V(p)$ for all primitive formulas $p \in \Phi$,
- $[\![\varphi_1 \wedge \varphi_2]\!] = [\![\varphi_1]\!] \cap [\![\varphi_2]\!]$,
- $[\![\neg\varphi]\!] = S \setminus [\![\varphi]\!]$,
- $[\![\Diamond\varphi]\!] = R([\![\varphi]\!])$.

Only the last equation is non-trivial. Let's see: Since $s \models \Diamond\varphi$ iff there exists s' with $s \to_R s'$ and $s \models \varphi$, we infer that $s \in [\![\diamond\varphi]\!]$ iff we can find a transition from s into an element of $[\![\varphi]\!]$.

We port the notion of a morphism now to Kripke models.

Definition 4.5 *Let $\mathcal{M} = (S, V, R)$ and $\mathcal{M}' = (S', V', R')$ be Kripke models and $f : R \to R'$ be a morphism for the contributing relations. Then $f : \mathcal{M} \to \mathcal{M}'$ is said to be a* model morphism *iff $f^{-1}[V'(p)] = V(p)$ for each atomic proposition $p \in \Phi$ (this is sometimes called* celestial harmony*).*

Hence for a model morphism f $\mathcal{M}, w \models p$ iff $\mathcal{M}', f(w) \models p$ for each atomic proposition p. This observation extends to all formulas of the basic modal language, as we will see now.

Proposition 4.6 *Assume $\mathcal{M}$ and $\mathcal{M}'$ are models as above, and $f : \mathcal{M} \to \mathcal{M}'$ is a model morphism. Then*

$$\mathcal{M}, s \models \varphi \text{ iff } \mathcal{M}', f(s) \models \varphi$$

for all states s of $\mathcal{M}$, and for all formulas φ.

Proof 0. The assertion is equivalent to

$$[\![\varphi]\!]_{\mathcal{M}} = f^{-1}\,[[\![\varphi]\!]_{\mathcal{M}'}]$$

for all formulas φ. This is the claim which will be established by induction on the structure of a formula now.
1. If p is an atomic proposition, then this is just the definition of a morphism for relations to be a morphism for Kripke models:

$$[\![p]\!]_{\mathcal{M}} = V(p) = f^{-1}\,[Y(p)] = [\![p]\!]_{\mathcal{M}'}.$$

Assume that the assertion holds for φ_1 and φ_2, then

$$\begin{array}{ll} [\![\varphi_1 \wedge \varphi_2]\!]_{\mathcal{M}} & = [\![\varphi_1]\!]_{\mathcal{M}} \cap [\![\varphi_2]\!]_{\mathcal{M}} \qquad\quad = f^{-1}\,[[\![\varphi_1]\!]_{\mathcal{M}'}] \cap f^{-1}\,[[\![\varphi_2]\!]_{\mathcal{M}'}] \\ & = f^{-1}\,[[\![\varphi_1]\!]_{\mathcal{M}'} \cap [\![\varphi_2]\!]_{\mathcal{M}'}] \quad = f^{-1}\,[[\![\varphi_1 \wedge \varphi_2]\!]_{\mathcal{M}'}]\,. \end{array}$$

Similarly, one shows that $[\![\neg\varphi]\!]_{\mathcal{M}} = f^{-1}\,[[\![\neg\varphi]\!]_{\mathcal{M}'}]$.
2. Now consider $\Diamond\varphi$, assume that the hypothesis holds for formula φ, then we have

$$\begin{array}{lll} [\![\Diamond\varphi]\!]_{\mathcal{M}} & = \{s \mid \exists s' \in R(s) : s' \in [\![\varphi]\!]_{\mathcal{M}}\} & \\ & = \{s \mid \exists s' \in R(s) : f(s') \in [\![\varphi]\!]_{\mathcal{M}'}\} & \text{(by hypothesis)} \\ & = \{s \mid \exists s' : f(s') \in S(f(s)), f(s') \in [\![\varphi]\!]_{\mathcal{M}'}\} & \text{(by Lemma 4.7 below)} \\ & = f^{-1}\left[\{x \mid \exists x' \in S(x) : x' \in [\![\varphi]\!]_{\mathcal{M}'}\}\right] & \\ & = f^{-1}\,[[\![\Diamond\varphi]\!]_{\mathcal{M}'}]\,. & \end{array}$$

Thus the assertion holds for all formulas φ. ⊣
It remains to establish this auxiliar statement:

Lemma 4.7 *If* $f : R \to R'$ *and* $A \subseteq S'$, *then* $f^{-1}\,[R'(A)] = R(f^{-1}\,[A])$

Proof 0. Note that we cannot directly argue with the diagram from Definition 3.1 above, since $\left(\mathcal{P}(f)\right)^{-1}[\{A\}]$ does not necessarily coincide with $\{f^{-1}\,[A]\}$ (take a constant map as a counter example). But we are in a position to argue directly using the forward and the backward condition.
1. We establish two inclusions.
" $\subseteq$ " : If $f(s) \in R'(A)$, we find $s' \in A$ with $f(s) \to_{R'} s'$. From the backward condition we obtain s_0 with $f(s_0) = s'$ and $s \to_R s_0$, giving $s_0 \in f^{-1}\,[A]$ and $s \in R(f^{-1}\,[A])$.
" $\supseteq$ " : If $s \in R(f^{-1}\,[A])$, $s \to_R s_0$ for some $s_0 \in f^{-1}\,[A]$, which entails $f(s) \to_{R'} f(s_0)$ by the forward condition. Also $f(s_0) \in A$, which means $f(s) \in R'(A)$, so that $s \in f^{-1}\,[R'(A)]$. ⊣

Proposition 4.6 has the important consequence that morphisms preserve validity.

Morphisms help with important constructions. This will to be demonstrated for congruences now. Recall for analogy that an equivalence relation $\equiv$ on a group $(G, +)$ respects the algebraic structure, i.e., $a \equiv b$, and $x \equiv y$ together imply $(a + x) \equiv (x + y)$. This carries over to the observation that we can find a group structure on the equivalence classes, say, $(G/\equiv, +_{\equiv})$, such that this diagram commutes (π sends each element x to its class $[x]$):

$$\begin{array}{ccc} G \times G & \xrightarrow{\pi\times\pi} & G/\equiv \times\, G/\equiv \\ {\scriptstyle m_+}\downarrow & & \downarrow{\scriptstyle m_{+_\equiv}} \\ G & \xrightarrow[\pi]{} & G/\equiv \end{array}$$

The notations are analogous to the diagram on page 4.

Now let us have a look at the situation discussed here:

Example 4.8 Given a model $\mathcal{M} = (S, V, R)$, an equivalence relation $\equiv$ on S is said to be a *congruence* for $\mathcal{M}$ iff there exists a model $\mathcal{M}' = (S/\equiv, V', R')$ which renders this diagram commutative:

$$\begin{array}{ccc} S & \xrightarrow{\pi} & S/\equiv \\ {\scriptstyle R}\downarrow & & \downarrow{\scriptstyle R'} \\ \mathcal{P}(S) & \xrightarrow[\mathcal{P}(\pi)]{} & \mathcal{P}(S/\equiv) \end{array}$$

Again, π sends each element s to its class $[s]$.
Let us discuss how to define V' and R' on the set $S/\equiv$ of classes.

- $[s] \in V'(p)$ iff $s \in V(p)$ for all $p \in \Phi$: this implies that if $s \in V(p)$ and $s \equiv s'$, then $s' \in V(p)$ must also hold. Thus each set $V(p)$ is invariant under the equivalence relation, i.e., a union of $\equiv$-classes.

- Note first that $\mathcal{P}(\pi)(R(s)) = \{[s_0] \mid s \to_R s_0\}$. Then

$$\begin{aligned} [s] \to_{R'} [s'] \text{ iff } & [s'] \in R'([s]) \\ \text{iff } & [s'] \in R'(\pi(s)) \\ \text{iff } & [s'] \in \mathcal{P}(\pi)(R(s)) \text{ (since } \pi \text{ is a morphism)} \end{aligned}$$

  This means that $[s] \to_{R'} [s']$ iff there exists s_1, s_2 such that $s_1 \equiv s$ and $s_2 \equiv s'$ with $s_1 \to_R s_2$, and $R'([s]) = \{[s'] \mid s_1 \to_R s_2 \text{ for some } s_1 \equiv s \& s_2 \equiv s'\}$. In particular, each set $R(s)$ must be invariant with respect to $\equiv$.

✌

This is a special case (fai da te):

Example 4.9 Let $\mathcal{M}$ be a Kripke model and define $s_1 \equiv s_2$ iff $s_1 \models \varphi \Leftrightarrow s_2 \models \varphi$ for all formulas. Then $\equiv$ is a congruence for $\mathcal{M}$.
This model could be called a *reduced model*, because it has the minimal number of states among those models which display the same behavior as $\mathcal{M}$ with respect to the logic. ✌

The notion of bisimilarity permits the comparison of models as well, and we will soon see that bisimilarity and equivalent behavior are closely related. We start again with relations and extend the notion then to Kripke models.

Definition 4.10 *Let* R *and* R' *be relations over* S *resp.* S'. *Then* $B \subseteq S \times S'$ *is called a* bisimulation *for* R *and* R' *iff for all* $\langle s, s' \rangle \in B$ *these conditions are satisfied:*

1. *if* $s \to_R s_1$, *then there is a* $s_1' \in S'$ *such that* $s' \to_{R'} s_1'$ *and* $\langle s_1, s_1' \rangle \in B$,

2. *if* $s' \to_{R'} s_1'$, *then there is a* $s_1 \in S$ *such that* $s \to_R s_1$ *and* $\langle s_1, s_1' \rangle \in B$.

Thus, if you start with a set of friends, and one of them makes a move, then the other one will also make a move, and the targets are friends as well.

Example 4.11 Let relation B be defined as

$$B := \{\langle 1, a\rangle, \langle 2, b\rangle, \langle 2, c\rangle, \langle 3, d\rangle, \langle 4, e\rangle, \langle 5, e\rangle\}$$

with $V(p) := \{a, d\}, V(q) := \{b, c, e\}$.

The transitions for $\mathcal{M}$ are given through $\mathcal{M}'$ is given through

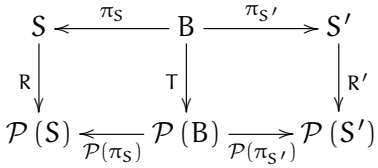
Then B is a bisimulation. ✌

The formulation from Definition 4.10 is relational, but there is also a characterization available through morphisms, as we establish now.

Theorem 4.12 *Given the transition systems* R *and* R' *as above. These statements are equivalent for* $B \subseteq S \times S'$*:*

1. B *is a bisimulation.*

2. *There exists relation* T *on* B *such that these diagrams commute*



Here π_S *and* $\pi_{S'}$ *are the corresponding projections.*

Proof
$1 \Rightarrow 2$: We have to construct a map $T : B \to \mathcal{P}(B)$ such that $f(\pi_S(s, s')) = \mathcal{P}(\pi_S)(T(s, s'))$ and $R(\pi_T(s, t)) = \mathcal{P}(\pi_T)(h(s, t))$ for all $\langle s, s'\rangle \in B$. The choice is somewhat obvious: put for $\langle s, t\rangle \in B$

$$T(s, s') := \{\langle s_1, s_1'\rangle \in B \mid s \to_R s_1, s' \to_{R'} s_1'\}.$$

Thus $T : B \to \mathcal{P}(B)$ is a map.
Now fix $\langle s, s'\rangle \in B$, then we claim that $R(s) = \mathcal{P}(\pi_S)(T(s, s'))$.

"$\subseteq$": Let $s_1 \in R(s)$, hence $s \to_R s_1$, thus there exists s_1' with $\langle s_1, s_1' \rangle \in B$ such that $s_1 \to_T s_1'$, hence

$$\begin{aligned} s_1 &\in \{\pi_S(s_0, t_0) \mid \langle s_0, t_0 \rangle \in T(s, s')\} \\ &= \{s_0 \mid \langle s_0, t_0 \rangle \in h(s, t) \text{ for some } t_0\} \\ &= \mathcal{P}(\pi_S)(T(s, s')). \end{aligned}$$

"$\supseteq$": If $s_1 \in \mathcal{P}(\pi_S)(T(s, s'))$, then in particular $s \to_R s_1$, thus $s_1 \in R(s)$.

Thus we have shown that $\mathcal{P}(\pi_S)(T(s, s')) = R(s) = R(\pi_S(s, s'))$. One shows $\mathcal{P}(\pi_{S'})(T(s, s')) = R'(s') = R'(\pi_{S'}(s, s'))$ in exactly the same way. We have constructed $T : B \to \mathcal{P}(T)$ such that the diagrams above commute.
$2 \Rightarrow 1$: Assume that T exists with the properties described in the assertion, then we have to show that B is a bisimulation. Now let $\langle s, s' \rangle \in B$ and $s \to_R s'$, hence $s' \in R(s) = R(\pi_S(s, s')) = \mathcal{P}(\pi_S)(T(s, s'))$. Thus there exists s_1' with $\langle s', s_1' \rangle \in T(s, t) \subseteq B$, and hence both $\langle s', s_1' \rangle \in B$ and $s' \to_{R'} s_1'$ hold.
A similar argument finds s' with $s \to_R s'$ with $\langle s', s_1' \rangle \in B$ in case $s' \to_{R'} s_1'$.
This completes the proof. $\dashv$
This characterization is important since it permits a description of bisimilarity in algebraic terms, i. e., in terms of morphisms and commutative diagrams. It opens an avenue for investigating bisimilar systems in which a purely relational description is either not available or inadequate.
The observation from Proposition 4.6 permits comparing states which are given through two models. Two states are said to be *modally equivalent* iff they cannot be separated by a formula, i.e., iff they satisfy exactly the same formulas.

Definition 4.13 *Let $\mathcal{M}$ and $\mathcal{M}'$ be models with state spaces S resp. S'. States $s \in S$ and $s' \in S'$ are called* modally equivalent *iff we have*

$$\mathcal{M}, s \models \varphi \text{ iff } \mathcal{M}', s' \models \varphi$$

for all formulas φ

Hence if $f : \mathcal{M} \to \mathcal{M}'$ is a model morphism, then s and $f(s)$ are modally equivalent for each state s of $\mathcal{M}$. One might be tempted to compare models with respect to their transition behavior; after all, underlying a model is a transition system. This leads directly to an extension of the notion of bisimilarity to Kripke models — note that we have to take the atomic propositions into account.

Definition 4.14 *Let $\mathcal{M} = (S, V, R)$ and $\mathcal{M}' = (S', V', R')$ be Kripke models, then a relation $B \subseteq S \times S'$ is called a* bisimulation *of $\mathcal{M}$ and $\mathcal{M}'$ iff*

1. *If $\langle s, s' \rangle \in B$, then s and s' satisfy the same propositional letters (this is called sometimes* atomic harmony*).*
2. *B is a bisimulation for the relations R and R'.*

States s *and* s' *are called* bisimilar *iff there exists a bisimulation* B *with* $\langle s, s' \rangle \in B$.

The first result relating bisimulation and modal equivalence is intuitively quite clear and fairly satisfying. Since a bisimulation reflects the structural similarity of the transition structure of the underlying transition systems, and since the validity of modal formulas is determined through this transition structure (and the behavior of the atomic propositional formulas), it does probably not come as a surprise that bisimilar states are modally equivalent.

Proposition 4.15 *Let* $\mathcal{M}$ *and* $\mathcal{M}'$ *be models with states* s *and* s'*. If* s *and* s' *are bisimilar, then they are modally equivalent.*

Proof 0. Let B be the bisimulation for which we know that $\langle s, s' \rangle \in B$. We have to show that

$$\mathcal{M}, s \models \varphi \Leftrightarrow \mathcal{M}', s' \models \varphi$$

for all formulas φ. This is done by induction on the formula.
1. Because of atomic harmony, the equivalence holds for propositional formulas. It is also clear that conjunction and negation are preserved under this equivalence, so that only the case of proving the equivalence for a formula $\Diamond\varphi$ under the assumption that it holds for φ remains to be taken care of.

"⇒": Assume that $\mathcal{M}, s \models \Diamond\varphi$ holds. Thus there exists a state s_1 in $\mathcal{M}$ with $s \to_R s_1$ and $\mathcal{M}, s_1 \models \varphi$. Hence there exists by the forward condition a state s_1' in $\mathcal{M}'$ with $s' \to_{R'} s_1'$, and $\langle s_1, s_1' \rangle \in B$ such that $\mathcal{M}', s_1' \models \varphi$ by the induction hypothesis. Because s_1' is a successor to s', we conclude $\mathcal{M}', s' \models \Diamond\varphi$.

"⇐": This is shown in the same way, using the backward condition for B.

⊣
The converse of Proposition 4.15 holds only under the restrictive condition that the models are image finite. This means that each state has only a finite number of successor states. Formally, model (S, V, R) is called *image finite* iff for each state s the set $R(s)$ of successor states is finite.
Then the famous Hennessy-Milner Theorem says

Theorem 4.16 *If the models* $\mathcal{M}$ *and* $\mathcal{M}'$ *are image finite, then modal equivalent states are bisimilar.*

Proof 1. Given two modal equivalent states s^* and t^*, we have to find a bisimulation B with $\langle s^*, t^* \rangle \in B$. The only thing we know about the states is that they are modally equivalent, hence that they satisfy exactly the same formulas. This suggests to define somewhat audaciously

$$B := \{\langle s', t' \rangle \mid \ s' \text{ and } t' \text{ are modally equivalent}\}$$

and then to establish B as a bisimulation. Since by assumption $\langle s^*, t^* \rangle \in B$, this will then prove the claim.
2. Since $\langle s, t \rangle \in B$, both satisfy the same atomic propositions by the definition of modal equivalence. Now let $\langle s, t \rangle \in B$ and $s \to_R s'$. Assume that we cannot find t' with $t \to_{R'} t'$ and $\langle s', t' \rangle \in B$.

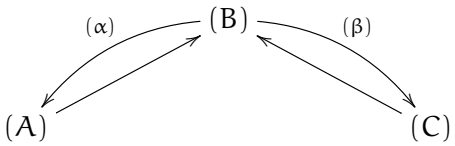
We know that $\mathcal{M}, s \models \Diamond\top$, because this says that there exists a successor to s, viz., s'. Since x and t satisfy the same formulas, $\mathcal{M}', t \models \Diamond\top$ follows, hence $R'(t) \neq \emptyset$. Let $R'(t) = \{t_1, \ldots, t_k\}$. Then, since s and t_i cannot be not modally equivalent, we can find for each $t_i \in R'(t)$ a formula ψ_i such that $\mathcal{M}, s' \models \psi_i$, but $\mathcal{M}', t_i \not\models \psi_i$. Hence $\mathcal{M}, s \models \Diamond(\psi_1 \wedge \cdots \wedge \psi_k)$, but $\mathcal{M}', t \not\models \Diamond(\psi_1 \wedge \cdots \wedge \psi_k)$. This is a contradiction, so the assumption is false, and we can find t' with $t \to_{R'} t'$ and $\langle s', t' \rangle \in B$.
The other conditions for a bisimulation are shown in exactly the same way.
⊣
Now look at these statements for the models $\mathcal{M}$ and $\mathcal{M}'$:

(A) $\mathcal{M}$ and $\mathcal{M}'$ are bisimilar.

(B) $\mathcal{M}$ and $\mathcal{M}'$ are modally equivalent (thus: for each state in one model there exists a modally equivalent state in the other model).

(C) There exists a model $\mathcal{N}$ and surjective morphisms $\mathcal{M} \xrightarrow{f} \mathcal{N} \xleftarrow{g} \mathcal{M}'$ (this is sometimes called *behavioral equivalence*: let $s \in S$, then $f(s) = g(s')$ for some $s' \in S'$, so that Proposition 4.6 implies $\mathcal{M}, s \models \varphi$ iff $\mathcal{M}', s' \models \varphi$ for each formula φ).

Then we have this picture:



with

(α) (B) → (A) if both models are image finite.

(β) (B) → (C) is always true. The proof is technically a bit involved and somewhat lengthy. It proceeds by factoring each model through the congruence from Example 4.9 and observes the isomorphism of the factor models.

Riferimenti bibliografici

[1] P. Blackburn, M. de Rijke, and Y. Venema, *Modal logic*, Cambridge Tracts in Theoretical Computer Science, no. 53, Cambridge University Press, Cambridge, UK, 2001.

[2] E.-E. Doberkat, *Special topics in Mathematics for Computer Scientists: Sets, categories, topologies and measures*, Springer International Publishing Switzerland, Cham, Heidelberg, New York, Dordrecht, London, December 2015.