the book so far

basic modal logic
slides and MLOM chapter 2

bisimulations
slides and MLOM chapter 3

decidability
slides and MLOM chapter 4, translation to FOL not yet

extensions global box, difference, until
slides and MLOM chapter 7.4

temporal logic
mainly the slides, also chapter by Yde Venema
modally definable frame properties

property $P$ is modally definable if there exists a formula $\phi$ such that:

$\mathcal{F}$ has property $P$ iff $\mathcal{F} \models \phi$ (for every frame $\mathcal{F}$)

how do we prove this for given $P$ and $\phi$ usually?

assume a frame $\mathcal{F}$ with property $P$, prove that $\mathcal{F} \models \phi$

assume a frame $\mathcal{F}$ without property $P$, prove that $\mathcal{F} \not\models \phi$

that is, find a valuation $V$ and a world $w$ in $\mathcal{F}$ such that $\mathcal{F}, V, w \not\models \phi$
not modally definable frame properties

how do we prove that property $P$ is not modally definable?

suppose (towards a contradiction) that $P$ is modally definable by $\phi$

find ‘bisimilar’ frames $\mathcal{F}_1$ and $\mathcal{F}_2$ such that
$\mathcal{F}_1$ has property $P$ but $\mathcal{F}_2$ does not have property $P$, then

$\mathcal{F}_1 \models \phi$, but there is a valuation $V_2$ and a world $w_2$ such that $\mathcal{F}_2, V_2, w_2 \nvDash \phi$

use $V_2$ and $w_2$ to find $V_1$ and $w_1$ such that
$\mathcal{F}_1, V_1, w_1$ and $\mathcal{F}_2, V_2, w_2$ are bisimilar

by assumption on $\phi$ we have $\mathcal{F}_1, V_1, w_1 \models \phi$

by ‘bisimilar equivalent to modal equivalence’ we have $\mathcal{F}_2, V_2, w_2 \models \phi$

contradiction with $\mathcal{F}_2, V_2, w_2 \nvDash \phi$
operator definable

$\Delta$ a modal operator (modality) with $n$ arguments

$\Delta$ is definable if there is a formula $\zeta(p_1, \ldots, p_n)$ such that

$\Delta(\phi_1, \ldots, \phi_n)$ modally equivalent to $\zeta(\phi_1, \ldots, \phi_n)$

(for all formulas $\phi_1, \ldots, \phi_n$)

how to show that an operator is not modally definable?

suppose it is definable by some formula

find two bisimilar worlds such that
in one the formula should hold and in the other it shouldn’t hold
temporal logic: linear time and branching time

Moshe Vardi
paper

Rob van Glabbeek
paper
overview

- multi-modal logic
- towards propositional dynamic logic
overview

- multi-modal logic
- towards propositional dynamic logic
multi-modal logic

we assume a set of labels $\mathcal{I}$

we consider for every label $i$ a relation $R_i$

we consider for every label $i$ a box-formula $\langle i \rangle \phi$

we already know various instances of multi-modal logic:

$\mathcal{I} = \emptyset$ gives propositional logic

$\mathcal{I} = \{0\}$ gives basic modal logic

$\mathcal{I} = \{F, P\}$ gives temporal logic

and we will see $\mathcal{I} = Prog(A)$ gives propositional dynamic logic
especially interesting if there is some connection between the $R_i$

such as past is the inverse of future
multi-modal logic: frames and models

let $\mathcal{I}$ be a set of indices or labels

an $\mathcal{I}$-frame is a pair $(\mathcal{W}, \{R_i \mid i \in \mathcal{I}\})$ with

$\mathcal{W} \neq \emptyset$ a set of worlds or states

$R_i \subseteq \mathcal{W} \times w$ for every $i \in \mathcal{I}$

an $\mathcal{I}$-model is a triple $(\mathcal{W}, \{R_i \mid i \in \mathcal{I}\}, V)$ with

$(\mathcal{W}, \{R_i \mid i \in \mathcal{I}\})$ an $\mathcal{I}$-frame and $V : \text{Var} \rightarrow \mathcal{P}(\mathcal{W})$ a valuation
multi-modal logic: truth and validity

let $\mathcal{M} = (W, \{R_i \mid i \in \mathcal{I}\}, V)$ be an $\mathcal{I}$-model

$\mathcal{M}, w \models \phi$ is defined by induction on the definition of formulas

important clauses:

$\mathcal{M}, w \models \langle \alpha \rangle \phi$ iff $\mathcal{M}, v \models \phi$ for some $v$ with $R_\alpha Wv$

$\mathcal{M}, w \models [\alpha] \phi$ iff $\mathcal{M}, v \models \phi$ for all $v$ with $R_\alpha Wv$

truth in a model, valid in a frame, universal validity are defined as before
use index set \{a, b, c\}

give a model with a world where the formula

\(\langle a \rangle (\langle b \rangle [a] p \land [c] \neg \langle a \rangle p)\) is true
multi-modal logic: bisimulation

we use one index set $I$

let $\mathcal{M} = (W, \{R_i | i \in I\}, V)$ and $\mathcal{M}' = (W', \{R'_i | i \in I\}, V')$ be $I$-models

$\emptyset \neq Z \subseteq W \times W'$ is a bisimulation if for every $(w, w') \in Z$

$w \in V(p)$ if and only if $w' \in V'(p)$

if $R_i w v$ then there is $v'$ with $R'_i w' v'$ and $(v, v') \in Z$

if $R'_i w' v'$ then there is $v$ with $R_i w v$ and $(v, v') \in Z$
bisimulation and modal equivalence

if two worlds are bisimilar, then they are modally equivalent

we work with multi-modal formulas and \( \mathcal{I} \)-models
modal equivalence and bisimulation

under the restriction that every $R_i$ is finitely branching

(which does not imply that the model is finitely branching)

two worlds are bisimilar if and only if they are modally equivalent

theorem by Hennessy and Milner (1985)
until and next

until not definable in basic modal logic in temporal frames

until not definable in temporal modal logic in temporal frames

next not definable in basic modal logic in temporal frames
overview

- multi-modal logic
- towards propositional dynamic logic
towards propositional dynamic logic

for program verification

prove that a program meets its specification
while programs: example gcd

```
while y ≠ 0 do
    begin
        z := x mod y;
        x := y;
        y := z;
    end
```

$x, y, z$ are program variables running over integers

a state assigns values to program variables

a trace is a sequence of states, example:

$((15, 27, 0), (15, 27, 15), (27, 27, 15), (27, 15, 15), (27, 15, 12), (15, 15, 12), (15, 12, 12), (15, 12, 3), (12.12, 3), (12, 3, 3), (3, 3, 0), (3, 0, 0))$
while programs: definition

basic program: assignment
\[ x := t \]

test

a formula

sequential composition
\[ \alpha; \beta \]

conditional or guarded choice
\[ \textbf{if } \phi \textbf{ then } \alpha \textbf{ else } \beta \]

while or iteration
\[ \textbf{while } \phi \textbf{ do } \alpha \]
program correctness: first ideas

correctness specification:
formal description of how the program is supposed to behave

for our gcd program:
if the input values of $x$ and $y$ are positive integers $c$ and $d$,
then the output value of $x$ is the gcd of $c$ and $d$, and
the program terminates
We restrict attention to input-output behaviour.

A specification consists of an input condition $\phi$ and an output condition $\psi$.

**Partial correctness:**
- If the program starts satisfying $\phi$, and if it halts,
- Then when it halts $\psi$ is satisfied.

**Total correctness:**
- It is partially correct,
- And it terminates whenever started satisfying $\phi$. 
Hoare Logic

introduced by Tony Hoare (1934) in 1969
following work by Floyd from 1967
there is already work by Turing

Turing Award 1980
quicksort, Hoare Logic, Communicating Sequential Processes (CSP)
Hoare Logic
towards dynamic logic

we use the programs as indices in multi-modal logic

the possible worlds are viewed as states

\( \langle \alpha \rangle \phi \)

we can execute \( \alpha \) and halt in state satisfying \( \phi \)

\( [\alpha] \phi \)

if \( \alpha \) halts then in a state satisfying \( \phi \)

\( \{ \phi \} \alpha \{ \psi \} \) is encoded as \( \phi \to [\alpha] \psi \)
regular programs

atomic

\( a \) from a set of atomic programs

test

\( \phi \)? with \( \phi \) a test

sequential composition

\( \alpha; \beta \)

non-deterministic choice

\( \alpha \cup \beta \)

iteration

\( \alpha^* \)
while programs and regular programs

while programs can be encoded as regular programs:

\[
\text{if } \phi \text{ then } \alpha \text{ else } \beta = \phi?; \alpha \cup \neg\phi?; \beta
\]

\[
\text{while } \phi \text{ do } \alpha = (\phi?; \alpha)^*; \neg\phi?
\]
two approaches: exogenous logic and endogenous logic

exogenous: programs are explicit in the language

dynamic logic and Hoare Logic are exogenous

temporal logic and method by Floyd are endogenous

MLOM chapter 14.2