CS256/Spring 2008 — Lecture #12

Zohar Manna

Chapter 5

Algorithmic Verification

(of General Formulas)

Algorithmic Verification of Finite-state Systems

Given finite-state program P,
i.e., each $x \in V$ assumes only finitely many values
in all P-computations.

> `Example:` MUX-PET1 (Fig. 3.4) is finite-state
>
> $s = 1, 2$
>
> $y_1 = \text{T}, \text{F} \qquad y_2 = \text{T}, \text{F}$
>
> π can assume at most 36 different values.

We present an algorithm (decision procedure)
for establishing properties specified by
an arbitrary (quantifier-free) temporal formula.

Example: Program mux-pet1 (Fig. 3.4)

(Peterson's Algorithm for mutual exclusion)

$$
\begin{array}{l}
\textbf{local}\ \ y_1, y_2 : \ \textbf{boolean}\ \ \textbf{where}\ y_1 = \text{F}, y_2 = \text{F} \\
\qquad\quad s \quad\ \ : \ \textbf{integer}\ \ \ \textbf{where}\ s = 1 \\[1em]
P_1 :: \quad \begin{array}{l} \ell_0 : \ \textbf{loop forever do} \\ \quad \left[\begin{array}{ll} \ell_1 : & \textbf{noncritical} \\ \ell_2 : & (y_1,\ s) := (\text{T},\ 1) \\ \ell_3 : & \textbf{await}\ (\neg y_2) \lor (s \neq 1) \\ \ell_4 : & \textbf{critical} \\ \ell_5 : & y_1 := \text{F} \end{array} \right] \end{array} \\[1em]
\| \\[1em]
P_2 :: \quad \begin{array}{l} m_0 : \ \textbf{loop forever do} \\ \quad \left[\begin{array}{ll} m_1 : & \textbf{noncritical} \\ m_2 : & (y_2,\ s) := (\text{T},\ 2) \\ m_3 : & \textbf{await}\ (\neg y_1) \lor (s \neq 2) \\ m_4 : & \textbf{critical} \\ m_5 : & y_2 := \text{F} \end{array} \right] \end{array}
\end{array}
$$

Overview

Given a temporal formula φ

1) Is φ satisfiable?
   i.e., is there a model σ such that $\sigma \vDash \varphi$?

   Apply algorithm for φ:

   YES: φ satisfiable
   produce a model σ satisfying φ

   NO: φ unsatisfiable
   there exists no model σ satisfying φ

2) Is φ valid? [Is $\neg\varphi$ unsatisfiable?]

   Apply algorithm for $\neg\varphi$:

   YES: $\neg\varphi$ satisfiable = φ not valid
   produce a model σ satisfying $\neg\varphi$
   (counterexample)

   NO: $\neg\varphi$ unsatisfiable = φ is valid

Overview (Cont'd)

Given a temporal formula φ and
a finite-state program P

3) Is φ P-satisfiable?
i.e., is there a P-computation σ such that $\sigma \vDash \varphi$?

Apply algorithm for φ and P:

YES: φ P-satisfiable
produce a P-computation σ
satisfying φ

NO: φ P-unsatisfiable
there exists no such computation

Overview (Cont'd)

Given a temporal formula φ and
a finite-state program P

4) Is φ P-valid? [Is $\neg\varphi$ P-unsatisfiable?]

Apply algorithm for $\neg\varphi$ and P:

YES: $\neg\varphi$ P-satisfiable = φ not P-valid
(Computation produced is a counterexample)

NO: $\neg\varphi$ P-unsatisfiable = φ is P-valid

Idea of algorithm

Construct a directed graph ("tableau") T_φ that exactly embeds all models of φ,
i.e., σ is embedded in T_φ iff $\sigma \vDash \varphi$.

Embedding in a graph

In the simplest version, the nodes of the graph are labelled by assertions. A model

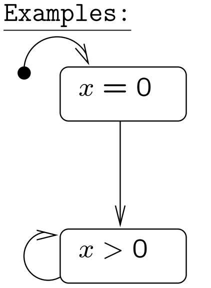
$$\sigma : s_0, s_1, \ldots s_i, \ldots$$

is embedded in the graph if there exists a path

$$\pi\colon\ n_0, n_1, \ldots n_i, \ldots$$

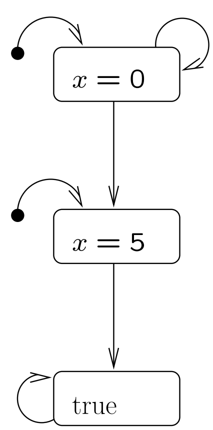
(where n_0 is an initial node)
such that for all $i \geq 0$,
s_i satisfies the assertion A_i labeling node n_i,
i.e., $s_i \Vdash A_i$.

Examples:



embeds all sequences that satisfy

$$(x = 0) \wedge \bigcirc \square (x > 0)$$



embeds all sequences that satisfy

$$(x = 0)\ \mathcal{W}\ (x = 5)$$

<u>`Example:`</u> Construct a graph that embeds exactly all sequences that satisfy

$$p \Rightarrow p \,\mathcal{W}\, q$$

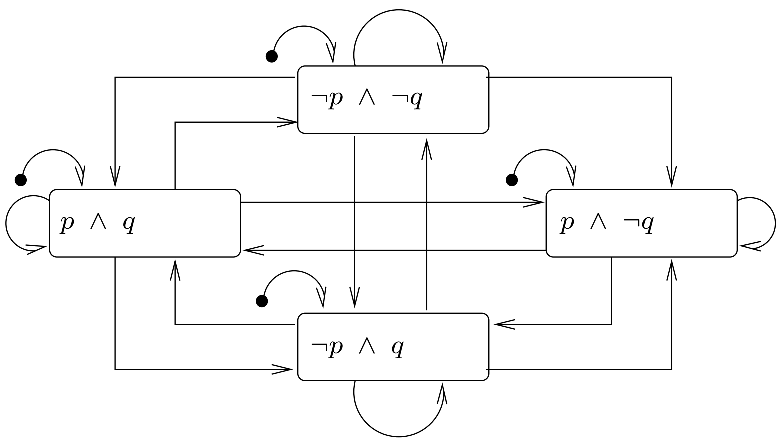


Tableau: Motivation

Note that $\Box(p \wedge \neg q)$ is embedded in the graph (as it should be since $\Box(p \wedge \neg q)$ implies $(p \Rightarrow p \,\mathcal{W}\, q)$.

How do we construct a graph that embeds all sequences that satisfy $p \Rightarrow p \,\mathcal{U}\, q$?
Now sequences that satisfy $\Box(p \wedge \neg q)$ should be excluded.

Temporal Tableau vs. ω-Automata

To be able to embed exactly all sequences that satisfy a formula like $p \Rightarrow p \,\mathcal{U}\, q$, we need some additional conditions on embeddings. The two most popular ways of doing this are:

1. <u>ω-Automata</u>:
   Add Muller or Streett-like acceptance conditions and interpret the graph as an ω-automaton.
2. <u>Temporal Tableau</u>:
   In addition to assertions, label the nodes with <u>temporal formulas</u> that determine not only what happens in the current state but also what must happen in the future (i.e., that make promises) and then exclude paths that don't fulfill their promises.

Now we will only use the temproal tableau and we will not further consider the ω-automata approach. We distinguish between 2 types of Temporal Tableaux:
<u>Atom Tableau</u> and <u>Particle Tableau</u>.

Satisfiability of a temporal formula

We consider temporal formulas that consist of

T F

$\neg \quad \vee \quad \wedge$
(logical connectives)

$\bigcirc \quad \Diamond \quad \Box \quad \mathcal{U} \quad \mathcal{W}$
(temporal operators)

Note: In this class we will only deal with future temporal operators. The book covers both past and future temporal operators.

Atom Tableau

Closure

The closure of a formula φ

Φ_φ

is the smallest set of formulas satisfying:

- $\varphi \in \Phi_\varphi$
- For every $\psi \in \Phi_\varphi$ and subformula ξ of ψ,
$$\xi \in \Phi_\varphi$$
- For every $\psi \in \Phi_\varphi$,
  $\neg\psi \in \Phi_\varphi$
  ($\neg\neg\psi$ is considered identical to ψ)
- For every ψ of the form
$$\Box\,\psi_1,\ \Diamond\,\psi_1,\ \psi_1\,\mathcal{U}\,\psi_2,\ \psi_1\,\mathcal{W}\,\psi_2,$$
  if $\psi \in \Phi_\varphi$ then $\bigcirc\,\psi \in \Phi_\varphi$

Definition: Formulas in Φ_φ are called the closure formulas of φ

Example: The closure of

$$\boxed{\varphi_0 :\ \Diamond\ p}$$

is Φ_{φ_0}: $\{\Diamond\,p,\ p,\ \bigcirc\,\Diamond\,p,\ \neg\,\Diamond\,p,\ \neg\,p,\ \neg\,\bigcirc\,\Diamond\,p\}$.

`Example:` The closure of

$$\boxed{\varphi_1:\quad \Box\,p\ \wedge\ \Diamond\,\neg p}$$

is $\Phi_{\varphi_1} = \Phi^+_{\varphi_1} \cup \Phi^-_{\varphi_1}$:

$$\{\ \varphi_1,\quad \Box\,p,\quad \Diamond\,\neg p,\quad p,\quad \bigcirc\,\Box\,p,\quad \bigcirc\,\Diamond\,\neg p$$
$$\neg\varphi_1,\ \neg\,\Box\,p,\ \neg\,\Diamond\,\neg p,\ \neg p,\ \neg\,\bigcirc\,\Box\,p,\ \neg\,\bigcirc\,\Diamond\,\neg p\,\}$$

`Example:` The closure of

$$\boxed{\varphi_2:\quad \Box\,\underbrace{(\neg p\ \vee\ (p\,\mathcal{W}\,q))}_{\psi}}$$

is $\Phi_{\varphi_2} = \Phi^+_{\varphi_2} \cup \Phi^-_{\varphi_2}$:

$$\{\ \varphi_2,\quad \psi,\quad p,\quad p\,\mathcal{W}\,q,\quad q,\quad \bigcirc\,\varphi_2,\quad \bigcirc(p\,\mathcal{W}\,q),$$
$$\neg\varphi_2,\ \neg\psi,\ \neg p,\ \neg(p\,\mathcal{W}\,q),\ \neg q,\ \neg\,\bigcirc\,\varphi_2,\ \neg\,\bigcirc(p\,\mathcal{W}\,q)\,\}$$

Size of Closure

The size of the closure is bounded by

$$|\Phi_\varphi| \le 4|\varphi|$$

where

$|\Phi_\varphi|$ – # of formulas

$|\varphi|$ – size of formula
(# of occ. of connectives, operators
+ # of occ. of propositions, variables)

Typically a temporal operator contributes 4 formulas to the closure, e.g., for $\Box\,p$:

$$\Box\,p,\quad \bigcirc\,\Box\,p,\quad \neg\,\Box\,p,\quad \neg\,\bigcirc\,\Box\,p$$

and a state formula contributes two, e.g., for p:

$$p,\quad \neg p$$

`Example:` $\boxed{\varphi_1:\quad \Box\,p\ \wedge\ \Diamond\,\neg p}$

$$|\varphi_1| = 6 \qquad |\Phi_{\varphi_1}| = 12$$
$$12 \le 4 \cdot 6$$

Atoms (Motivation)

Atoms are maximal "consistent" subsets of closure formulas that may hold together at some position in the model.

How do we identify consistent subsets?

Intuition: Based on the "Expansion Congruences".
We decompose temporal formulas into
what must hold current state, and/or
what must hold in the next state.

$\Box p \quad \approx \quad p \wedge \bigcirc \Box p$

$\Diamond p \quad \approx \quad p \vee \bigcirc \Diamond p$

$p\, \mathcal{U}\, q \;\approx\; q \vee [p \wedge \bigcirc (p\, \mathcal{U}\, q)]$

$p\, \mathcal{W}\, q \approx\; q \vee [p \wedge \bigcirc (p\, \mathcal{W}\, q)]$

For this purpose, we classify formulas as

- α-formulas (conjunctive flavor) and
- β-formulas (disjunctive flavor)

based on the top-level connective/operator of the formula.

α-formulas

α	$\kappa(\alpha)$
$p \wedge q$	$p,\ q$
$\Box p$	$p,\ \bigcirc \Box p$

intended meaning:

An α-formula holds at position j
iff
all $\kappa(\alpha)$-formulas hold at j

`Example:`

$\Box p$ holds at position j in σ
iff
both p and $\bigcirc \Box p$ hold at j

β-formulas

β	$\kappa_1(\beta)$	$\kappa_2(\beta)$
$p \vee q$	p	q
$\Diamond p$	p	$\bigcirc \Diamond p$
$p\, \mathcal{U}\, q$	q	$p,\ \bigcirc (p\, \mathcal{U}\, q)$
$p\, \mathcal{W}\, q$	q	$p,\ \bigcirc (p\, \mathcal{W}\, q)$

Intended meaning:

A β-formula holds at position j
iff
$\kappa_1(\beta)$-formula holds at j
or all $\kappa_2(\beta)$-formulas hold at j (or both)

`Example:`

$p\, \mathcal{U}\, q$ holds at position j
iff
q holds at j
or both p and $\bigcirc (p\, \mathcal{U}\, q)$ hold at j

Atoms

atom over φ (φ-atom) is a subset $A \subseteq \Phi_\varphi$ satisfying the following requirements:

- R_{sat}: $state(A)$, the conjunction of all state formulas in A is satisfiable
- $R_\neg$: For every $\psi \in \Phi_\varphi$,
  $\psi \in A \quad \text{iff} \quad \neg\psi \notin A$
- R_α: For every α-formula $\psi \in \Phi_\varphi$,
  $\psi \in A \quad \text{iff} \quad \kappa(\psi) \subseteq A$

  [e.g., $\Box p \in A$ iff both $p \in A$ and $\bigcirc \Box p \in A$]
- R_β: For every β-formula $\psi \in \Phi_\varphi$,
  $\psi \in A \quad \text{iff} \quad \kappa_1(\psi) \in A$,
  or $\kappa_2(\psi) \subseteq A$ (or both)

  [e.g., $p\mathcal{U}q \in A$ iff $q \in A$ or $\{p, \bigcirc(p\mathcal{U}q)\} \subseteq A$]

Note: Due to $R_\neg$, φ-atom must contain ψ or $\neg\psi$ for every ψ of Φ_φ. Thus the number of formulas in an atom is always half the number of formulas in the closure.

`Example:`

$\boxed{\varphi_1: \quad \Box p \ \wedge \ \Diamond \neg p}$

closure

$$\Phi_{\varphi_1}: \ \{\varphi_1, \ \Box p, \ \Diamond \neg p, \ \bigcirc \Box p, \ \bigcirc \Diamond \neg p, \ p \ \neg\varphi_1, \ldots\}$$

A: $\{\varphi_1, \ \Box p, \ \Diamond \neg p, \ \bigcirc \Box p, \ \bigcirc \Diamond \neg p, \ p\}$

is an atom

$$B: \ \{\varphi_1, \ \underset{\uparrow}{\Box p}, \ \Diamond \neg p, \ \underset{\uparrow}{\bigcirc \Box p}, \ \neg \bigcirc \Diamond \neg p, \ \underset{\uparrow}{\neg p}\}$$

is not an atom since by α-table,

$$\Box p \in B \quad \text{iff} \quad \{p, \ \bigcirc \Box p\} \subseteq B$$

Basic Formula

Definition: A formula is called basic if it is an atomic formula (i.e., no operators or connectives) or a formula of the form $\bigcirc \psi$

`Example:`

$\boxed{\varphi_0: \ \Diamond p}$

basic formulas in Φ_{φ_0}:

$$p, \ \bigcirc \Diamond p$$

`Example:`

$\boxed{\varphi_1: \ \Box p \ \wedge \ \Diamond \neg p}$

basic formulas in Φ_{φ_1}:

$p, \quad \bigcirc \Box p, \quad \bigcirc \Diamond \neg p$

`Example:`

$\boxed{\varphi_2: \quad \Box(\neg p \ \vee \ (p \ \mathcal{W} \ q))}$

basic formulas in Φ_{φ_2}:

$p, \quad q, \quad \bigcirc \varphi_2, \quad \bigcirc (p \, \mathcal{W} \, q)$

Why important?

In an atom, the positive/negative presence of the basic formulas uniquely determine the rest of the atom.

Thus, if a closure has b basic formulas, then there are 2^b distinct atoms.

Systematic Construction of Atoms

Suppose we know only the presence/absence of the basic formulas – the full atom A can be constructed following the definition of atom

Example: $\boxed{\varphi_1\colon\ \Box\, p\ \wedge\ \Diamond\, \neg p}$

Suppose we know

$\bigcirc\,\Box\, p,\ \bigcirc\,\Diamond\,\neg p\ \in A \qquad \neg p \in A$ (i.e., $p \notin A$)

The full atom can be constructed as follows

- $\neg p \in A\ \rightarrow$ place $\neg\,\Box\, p$ in A
- $\neg p \in A\ \rightarrow$ place $\Diamond\,\neg p$ in A
- $\neg\,\Box\, p \in A\ \rightarrow$ place $\neg(\underbrace{\Box\, p\ \wedge\ \Diamond\,\neg p}_{\varphi_1})$ in A

Final atom A:

$$\{\underbrace{\neg p,\ \bigcirc\,\Box\, p,\ \bigcirc\,\Diamond\,\neg p}_{\text{chosen independently}},\ \underbrace{\neg\,\Box\, p,\ \Diamond\,\neg p,\ \neg\varphi_1}_{\text{follow from the rules}}\}$$

Example:

$\boxed{\varphi_2\colon\ \ \Box\,(\neg p\ \vee\ (p\,\mathcal{W}\,q))}$

Φ_{φ_2} has four basic formulas

$p,\quad q,\quad \bigcirc\,\varphi_2,\quad \bigcirc(p\,\mathcal{W}\,q)$

Two atoms are:

$$\begin{array}{ll} \{\ \neg p,\ \neg q,\ \bigcirc\,\varphi_2,\ \bigcirc(p\,\mathcal{W}\,q), & \neg(p\,\mathcal{W}\,q),\ \neg p \vee (p\,\mathcal{W}\,q),\ \varphi_2\ \} \\ \{\ \neg p,\ \ q,\ \bigcirc\,\varphi_2,\ \bigcirc(p\,\mathcal{W}\,q), & p\,\mathcal{W}\,q,\ \neg p \vee (p\,\mathcal{W}\,q),\ \varphi_2\ \} \\ \underbrace{\hphantom{\{\ \neg p,\ \neg q,\ \bigcirc\,\varphi_2,\ \bigcirc(p\,\mathcal{W}\,q),}}_{\text{chosen independently}} & \underbrace{\hphantom{\neg(p\,\mathcal{W}\,q),\ \neg p \vee (p\,\mathcal{W}\,q),\ \varphi_2\ \}}}_{\text{follow from the rules}} \end{array}$$

Atom Construction

- let $p_1, p_2, \ldots, p_b$ be all basic formulas in Φ_φ
- construct all 2^b combinations

$$\left\{\begin{array}{c} p_1 \\ \neg p_1 \end{array}\right\},\ \ldots,\ \left\{\begin{array}{c} p_b \\ \neg p_b \end{array}\right\}$$

- complete each combination into a full atom using the α-table and the β-table.

Example: $\varphi_0:\ \Diamond\, p$

$\Phi_{\varphi_0}:\ \{\Diamond\, p,\ p,\ \bigcirc\,\Diamond\, p,\ \neg\,\Diamond\, p,\ \neg p,\ \neg\,\bigcirc\,\Diamond\, p\}$

Basic formulas: $\{p,\ \bigcirc\,\Diamond\, p\}$

Atoms:

$$A_1:\ \{\underline{p},\ \underline{\bigcirc\,\Diamond\, p},\ \Diamond\, p\ \}$$

$$A_2:\ \{\underline{\neg p},\ \underline{\bigcirc\,\Diamond\, p},\ \Diamond\, p\ \}$$

$$A_3:\ \{\underline{p},\ \underline{\neg\,\bigcirc\,\Diamond\, p},\ \Diamond\, p\ \}$$

$$A_4:\ \{\underline{\neg p},\ \underline{\neg\,\bigcirc\,\Diamond\, p},\ \neg\,\Diamond\, p\ \}$$

Example:

Generate all atoms of

$\boxed{\varphi_1\colon\ \Box\, p\ \wedge\ \Diamond\,\neg p}$

basic formulas

$p \quad \bigcirc\,\Box\, p \quad \bigcirc\,\Diamond\,\neg p$

8 possible combinations = 8 atoms

$$\begin{array}{lrrrrrl} A_0\colon\ \{ & \neg p, & \neg\bigcirc\Box\, p, & \neg\bigcirc\Diamond\neg p, & \neg\Box\, p, & \Diamond\neg p, & \neg\varphi_1\} \\ A_1\colon\ \{ & p, & \neg\bigcirc\Box\, p, & \neg\bigcirc\Diamond\neg p, & \neg\Box\, p, & \neg\Diamond\neg p, & \neg\varphi_1\} \\ A_2\colon\ \{ & \neg p, & \neg\bigcirc\Box\, p, & \bigcirc\Diamond\neg p, & \neg\Box\, p, & \Diamond\neg p, & \neg\varphi_1\} \\ A_3\colon\ \{ & p, & \neg\bigcirc\Box\, p, & \bigcirc\Diamond\neg p, & \neg\Box\, p, & \Diamond\neg p, & \neg\varphi_1\} \\ A_4\colon\ \{ & \neg p, & \bigcirc\Box\, p, & \neg\bigcirc\Diamond\neg p, & \neg\Box\, p, & \Diamond\neg p, & \neg\varphi_1\} \\ A_5\colon\ \{ & p, & \bigcirc\Box\, p, & \neg\bigcirc\Diamond\neg p, & \Box\, p, & \neg\Diamond\neg p, & \neg\varphi_1\} \\ A_6\colon\ \{ & \neg p, & \bigcirc\Box\, p, & \bigcirc\Diamond\neg p, & \neg\Box\, p, & \Diamond\neg p, & \neg\varphi_1\} \\ A_7\colon\ \{ & p, & \bigcirc\Box\, p, & \bigcirc\Diamond\neg p, & \Box\, p, & \Diamond\neg p, & \varphi_1\} \end{array}$$

$$\underbrace{\hphantom{p,\ \neg\bigcirc\Box\, p,\ \neg\bigcirc\Diamond\neg p,}}_{\text{chosen independently}} \qquad \underbrace{\hphantom{\neg\Box\, p,\ \neg\Diamond\neg p,\ \neg\varphi_1\}}}_{\text{follow from the rules}}$$

Tableau Construction T_φ

Given formula φ,
construct directed graph T_φ (tableau of φ):

- create a node for each atom of φ and label the node with that atom.

- A node is initial if $\varphi \in A$.

  $\rightarrow A$

- Create an edge:
  Atom A_1 is connected to atom A_2 by directed edge,

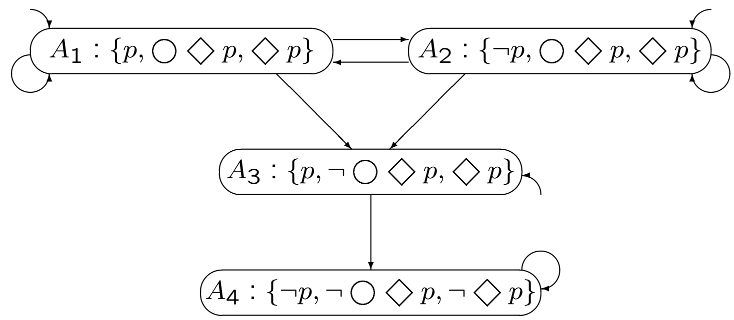
  $A_1 \longrightarrow A_2$

  If for every $\bigcirc\psi \in \Phi_\varphi$,
  $\bigcirc\psi \in A_1$ iff $\psi \in A_2$

Recall: $\neg\bigcirc\psi \approx \bigcirc\neg\psi$

Example: $\varphi: \Diamond p$

Tableau T_φ:



Example:

$\boxed{\varphi_1\colon \Box p \wedge \Diamond\neg p}$

Tableau T_{φ_1} (Fig 5.3)

Since

A_2: $\{\ldots,\ \neg\bigcirc\Box p,\ \bigcirc\Diamond\neg p,\ \ldots\}$

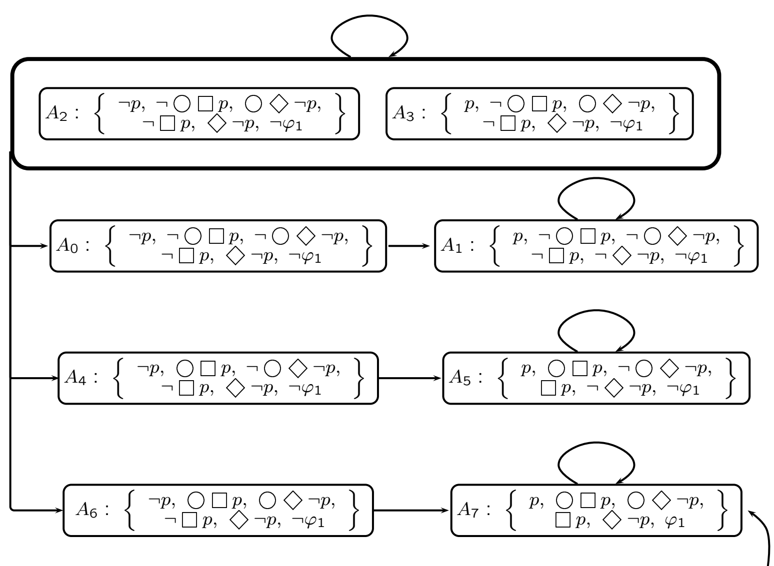
all successors of A_2 must have

$\{\ldots,\ \neg\Box p,\ \Diamond\neg p,\ \ldots\}$

$A_2 \ \rightarrow\ A_0, A_2, A_3, A_4, A_6$

$A_2 \ \not\rightarrow\ A_1, A_5, A_7$

Fig. 5.3: Tableau T_{φ_1} for formula
$\varphi_1\colon \Box p \wedge \Diamond\neg p$



Example:

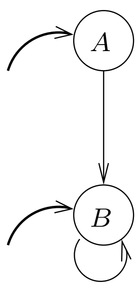
$\boxed{\varphi_2: \quad \square(\neg p \ \vee \ (p\,\mathcal{W}\,q))}$

Let A and B be the atoms:

$$A: \ \{\ \neg p,\ \neg q,\ \bigcirc\varphi_2,\ \bigcirc(p\,\mathcal{W}\,q),\ \neg(p\,\mathcal{W}\,q),\ \neg p \vee (p\,\mathcal{W}\,q),\ \varphi_2\ \}$$

$$B: \ \{\ \neg p,\ \ q,\ \bigcirc\varphi_2,\ \bigcirc(p\,\mathcal{W}\,q),\ p\,\mathcal{W}\,q,\ \neg p \vee (p\,\mathcal{W}\,q),\ \varphi_2\ \}$$

The tableau is:



Paths induced by models

Definition: An infinite path

$$\pi: \ A_0, A_1, \ldots$$

in the tableau T_φ is induced by a model

$$\sigma: \ s_0, s_1, \ldots$$

if for all $j \geq 0$ and for all $\psi \in \Phi_\varphi$:

$$\underset{(\sigma, j)}{\underset{\uparrow}{s_j}} \quad \vDash \psi \quad \text{iff} \quad \psi \in A_j$$

Example:

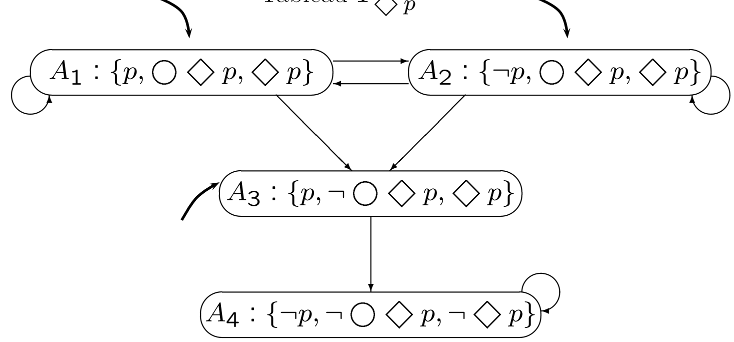
$\boxed{\varphi: \ \diamond\, p}$

$$\Phi_\varphi = \{\diamond\, p,\ p,\ \bigcirc\diamond\, p,\ \neg\diamond\, p,\ \neg p,\ \neg\bigcirc\diamond\, p\}$$

basic formulas: $\{p,\ \bigcirc\diamond\, p\}$

Atoms:
- A_1: $\{\underline{p},\ \underline{\bigcirc\diamond\, p},\ \diamond\, p\}$
- A_2: $\{\underline{\neg p},\ \underline{\bigcirc\diamond\, p},\ \diamond\, p\}$
- A_3: $\{\underline{p},\ \underline{\neg\bigcirc\diamond\, p},\ \diamond\, p\}$
- A_4: $\{\underline{\neg p},\ \underline{\neg\bigcirc\diamond\, p},\ \neg\diamond\, p\}$

Tableau $T_{\diamond\, p}$



Paths:

$$\begin{array}{l|cccccc c}
\sigma_1: & \neg p & \neg p & \neg p & p & \neg p & \neg p & \ldots \\ \hline
\pi_1: & A_2 & A_2 & A_2 & A_3 & A_4 & A_4 & \ldots
\end{array}$$

$$\begin{array}{l|cccccccc c}
\sigma_2: & \neg p & p & \neg p & p & \neg p & p & p & p & \ldots \\ \hline
\pi_2: & A_2 & A_1 & A_2 & A_1 & A_2 & A_1 & A_1 & A_1 & \ldots
\end{array}$$

π_1 is induced by σ_1
π_2 is induced by σ_2

Paths induced by models (Cont'd)

`Claim 1` (model $\rightarrow$ induced path):

Consider formula φ and its tableau T_φ.
For every model σ of φ (i.e., $\sigma \vDash \varphi$)
there exists an infinite path

$$\pi_\sigma\colon\ A_0, A_1, \ldots$$

in T_φ such that π_σ is induced by σ

Converse?

The converse of claim 1 is not true:
There may be a path π in T_φ that is not induced by any model σ of φ.

`Example:` In $T_{\diamondsuit p}$,

path $\pi : A_2^\omega$ is not induced by model $\sigma : (\neg p)^\omega$, since $\neg p, \diamondsuit p \in A_2$ should hold at all positions j, but there is no σ such that

$\diamondsuit p$ at position 0 and
$\neg p$ at all positions $j \geq 0$.

`Example:`

$$\boxed{\varphi_1\colon\quad \square p \ \wedge\ \diamondsuit \neg p}$$

In Fig 5.3,

A_7: $\{\ p,\ \bigcirc\square p,\ \bigcirc\diamondsuit\neg p,\ \square p,\ \diamondsuit\neg p,\ \varphi_1\ \}$

Path $\underline{A_7^\omega}$ is not induced by any model of φ_1,

since every $\psi \in A_7$ should hold at all positions j,
but there is no σ s.t.

$\diamondsuit \neg p$ at position 0 and
p at all positions $j \geq 0$

How do we exclude those "bad" paths?