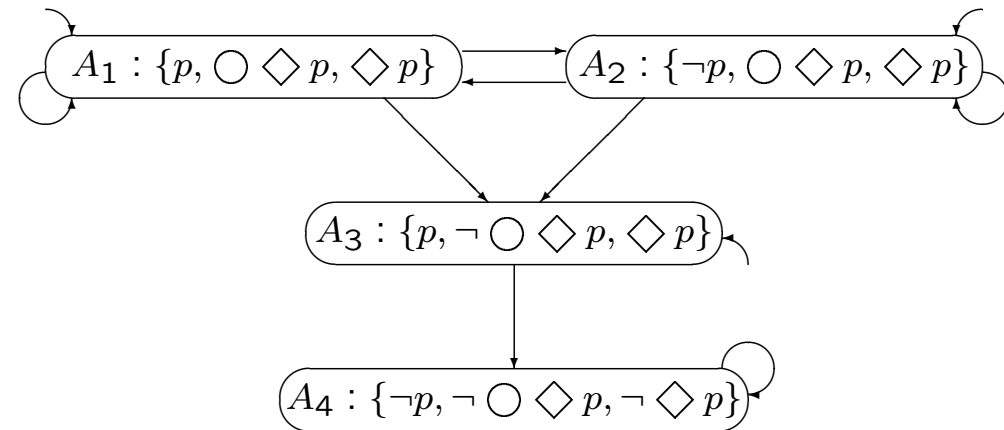


CS256/Winter 2009 Lecture #13

Zohar Manna

Example: $\varphi_0 : \Diamond p$

Tableau T_{φ_0} :



Promising Formula

In $T_{\diamond p}$, a path can start and stay forever in atom A_2 . But A_2 includes $\diamond p$, i.e., A_2 promises that p will eventually happen, but it is never fulfilled in the path. We want to exclude these paths.

The idea is that if a path contains an atom that includes a promising formula, then the path should fulfill the promise.

A formula $\psi \in \Phi_\varphi$ is said to promise the formula r if ψ is one of the forms:

$$\begin{array}{ccc} \diamond r & p \mathcal{U} r & \neg \square \neg r & \neg((\neg r) \mathcal{W} p) \\ & \underbrace{\hspace{2cm}} & \underbrace{\hspace{2cm}} & \underbrace{\hspace{2cm}} \\ & \approx \diamond r \wedge \dots & \approx \diamond r & \approx \diamond r \wedge \dots \end{array}$$

Example:

$$\begin{array}{c} \boxed{\varphi_1: \square p \wedge \diamond \neg p} \\ \Phi_{\varphi_1}: \left\{ \begin{array}{l} \varphi_1, \quad \square p, \quad \underline{\diamond \neg p}, \quad \bigcirc \square p, \quad \bigcirc \diamond p, \quad p \\ \neg \varphi_1, \quad \underline{\neg \square p}, \quad \neg \diamond \neg p, \quad \neg \bigcirc \square p, \quad \neg \bigcirc \diamond p, \quad \neg p \end{array} \right\} \end{array}$$

Only 2 promising formulas in Φ_φ

$$\begin{array}{l} \psi_1 : \neg \square p \text{ promises } r_1 : \neg p \\ \psi_2 : \diamond \neg p \text{ promises } r_2 : \neg p \end{array}$$

Promise Fulfillment

Property:

Let σ be an arbitrary model of φ ,
and $\psi \in \Phi_\varphi$ a formula that promises r .
If $(\sigma, j) \models \psi$ then $(\sigma, k) \models r$ for some $k \geq j$

Proof: Follows from the semantics of temporal formulas.

Claim: (promise fulfillment by models)

Let σ be an arbitrary model of φ ,
and $\psi \in \Phi_\varphi$ a formula that promises r .
Then σ contains infinitely many positions $j \geq 0$
such that

$$(\sigma, j) \models \neg\psi \quad \text{or} \quad (\sigma, j) \models r$$

Proof:

1. Assume σ contains infinitely many ψ -positions.
Then σ must contain infinitely many r -positions,
since ψ promises r .
2. Assume σ contains finitely many ψ -positions.
Then it contains infinitely many $\neg\psi$ -positions.

Fulfilling Atoms

Definition: Atom A fulfills $\psi \in \Phi_\varphi$
(which promises r)
if $\neg\psi \in A$ or $r \in A$.

Example: In $T_{\diamond p}$,

Only one promising formula:

$$\psi : \diamond p \text{ promises } r : p$$

$$A_1^+ : \{p, \bigcirc \diamond p, \diamond p\}$$

fulfills $\diamond p$ since $p \in A_1$

$$A_3^+ : \{p, \neg \bigcirc \diamond p, \diamond p\}$$

fulfills $\diamond p$ since $p \in A_3$

$$A_4^+ : \{\neg p, \neg \bigcirc \diamond p, \neg \diamond p\}$$

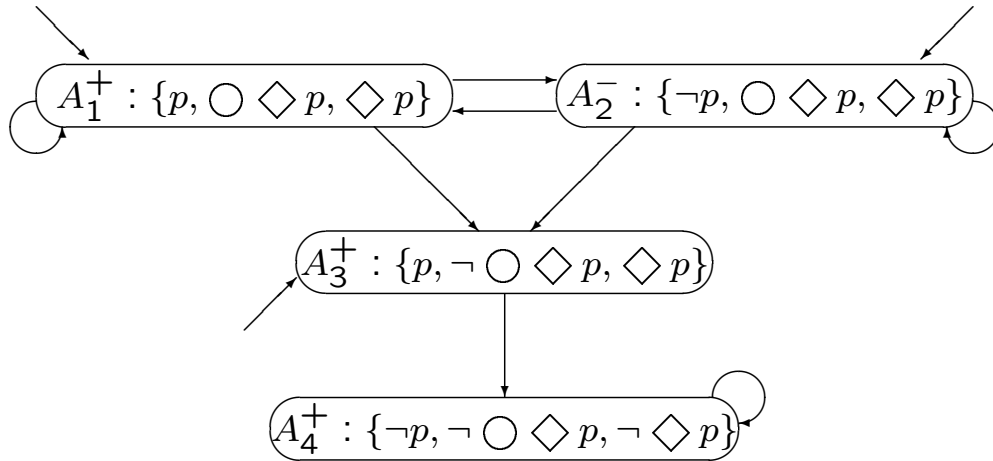
fulfills $\diamond p$ since $\neg \diamond p \in A_4$

But

$$A_2^- : \{\neg p, \bigcirc \diamond p, \diamond p\}$$

does not fulfill $\diamond p$ since $\diamond p, \neg p \in A_2$

Tableau $T_{\diamond p}$



Fulfilling Paths

Definition: A path $\pi : A_0, A_1, \dots$ is fulfilling if for every promising formula $\psi \in \Phi_\varphi$ it contains infinitely many A_j that fulfill ψ .

Example: In $T_{\diamond p}$,

$$A_2^-, A_2^-, A_2^-, A_3^+, A_4^+, A_4^+, \dots$$

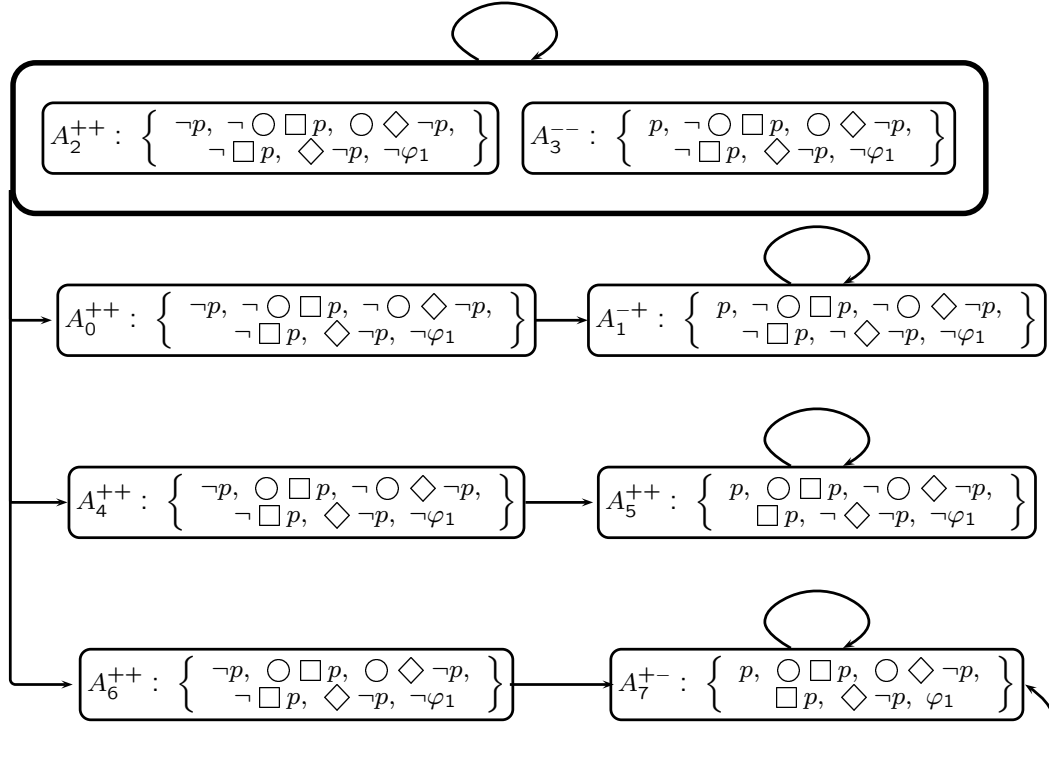
$$A_2^-, A_1^+, A_2^-, A_1^+, A_1^+, A_1^+, \dots$$

are fulfilling paths, but

$$A_2^-, A_2^-, A_2^-, A_2^-, A_2^-, A_2^-, A_2^-, \dots$$

is not a fulfilling path.

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



Example:

$$\varphi_1: \Box p \wedge \Diamond \neg p$$

T_{φ_1} in Fig 5.3

There are two promising formulas in Φ :

$$\psi_1: \neg \Box p \text{ promises } r_1: \neg p$$

$$\psi_2: \Diamond \neg p \text{ promises } r_2: \neg p$$

$$A_0^{++} : \{ \neg p, \neg \Box p, \Diamond \neg p, \dots \}$$

$$A_1^{-+} : \{ p, \neg \Box p, \neg \Diamond \neg p, \dots \}$$

$$A_2^{++} : \{ \neg p, \neg \Box p, \Diamond \neg p, \dots \}$$

$$A_3^{--} : \{ p, \neg \Box p, \Diamond \neg p, \dots \}$$

$$A_4^{++} : \{ \neg p, \neg \Box p, \Diamond \neg p, \dots \}$$

$$A_5^{++} : \{ p, \Box p, \neg \Diamond \neg p, \dots \}$$

$$A_6^{++} : \{ \neg p, \neg \Box p, \Diamond \neg p, \dots \}$$

$$A_7^{+-} : \{ p, \Box p, \Diamond \neg p, \dots \}$$

Example: (Cont'd)

- path $(A_7^{+-})^\omega$ not fulfilling.
- path $(A_2^{++})^\omega$ is fulfilling.
- path $(A_2^{++}, A_3^{--})^\omega$ is fulfilling.
- path $A_4^{++}, (A_5^{++})^\omega$ is fulfilling.
- For arbitrary m , path
 $\pi: (A_2^{++}, A_3^{--})^m, A_4^{++}, (A_5^{++})^\omega$
is fulfilling.

Models vs. fulfilling paths

Claim 2 (model \rightarrow fulfilling path):

If

$$\pi_\sigma : A_0, A_1, \dots$$

is a path induced by a model σ of φ ,
then π_σ is fulfilling.

Claim 3 (fulfilling path \rightarrow model):

If

$$\pi_\sigma : A_0, A_1, \dots$$

is a fulfilling path in T_φ ,
then there exists a model σ of φ that induces π_σ .

Proposition 1 (satisfiability by path)

Formula φ is satisfiable

iff

the tableau T_φ contains a fulfilling path

$\pi : A_0, A_1, A_2, \dots$ such that $\varphi \in A_0$

Proof:

(\Leftarrow) $\pi : A_0, A_1, \dots$ is a fulfilling path in T_φ with $\varphi \in A_0$

Then, by Claim 3, there exists model σ such that

$\forall j \geq 0, \forall p \in \Phi_\varphi: (\sigma, j) \models p \quad \text{iff} \quad p \in A_j$

Since $\varphi \in A_0$, $(\sigma, 0) \models \varphi$ and thus $\sigma \models \varphi$.

(\Rightarrow) $\sigma \models \varphi$. Then by Claims 1, 2, there exists a fulfilling path π_σ in T_φ that is induced by σ .

Since $(\sigma, 0) \models \varphi$, by the definition of induced, $\varphi \in A_0$.

Examples

In the examples below we use the following optimization: A path starting in A can only visit nodes that are reachable from A in T_φ . So we only need to consider nodes that are reachable from nodes labeled by atoms A such that $\varphi \in A$.

Example:

$$\varphi: \boxed{\Box p \wedge \neg \bigcirc p}$$

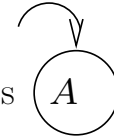
$$\Phi_\varphi = \{ \varphi, \Box p, \bigcirc \Box p, p, \bigcirc p, \neg \varphi, \neg \Box p, \neg \bigcirc \Box p, \neg p, \neg \bigcirc p \}$$

Basic formulas: $\{\bigcirc p, \bigcirc \Box p, p\} \rightarrow 8$ atoms

There is only one atom such that $\varphi \in A$:

$$A : \{ \neg \bigcirc p, \bigcirc \Box p, p, \Box p, \varphi \}$$

Any successor of A requires $\neg p$, $\Box p$, but these cannot coexist in any atom.



So the part of T_φ reachable from A is

So there is no fulfilling path (no path at all, as A does not have a successor).

Hence, $\boxed{\varphi \text{ is not satisfiable.}}$

Example:

$$\varphi_1: \Box p \wedge \Diamond \neg p$$

$\Phi_{\varphi_1} =$

$$\{ \varphi_1, \Box p, \Diamond \neg p, p, \bigcirc \Box p, \bigcirc \Diamond \neg p, \neg \varphi_1, \underbrace{\neg \Box p}_{\Diamond \neg p}, \neg \Diamond \neg p, \neg p, \neg \bigcirc \Box p, \neg \bigcirc \Diamond \neg p \}$$

$\neg \Box p$ and $\Diamond \neg p$ promise $\neg p$.

Basic formulas:

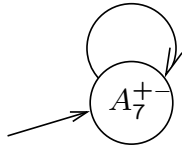
$$\{p, \bigcirc \Box p, \bigcirc \Diamond \neg p\} \rightarrow 8 \text{ atoms}$$

There is only one atom s.t. $\varphi_1 \in A$:

$$A_7: \{p, \bigcirc \Box p, \bigcirc \Diamond \neg p, \Box p, \Diamond \neg p, \varphi_1\}$$

Any successor of A_7 requires $\Box p$, $\Diamond \neg p$, and therefore φ_1 .

So the only successor is A_7 itself, and the part of T_{φ_1} reachable from A_7 is

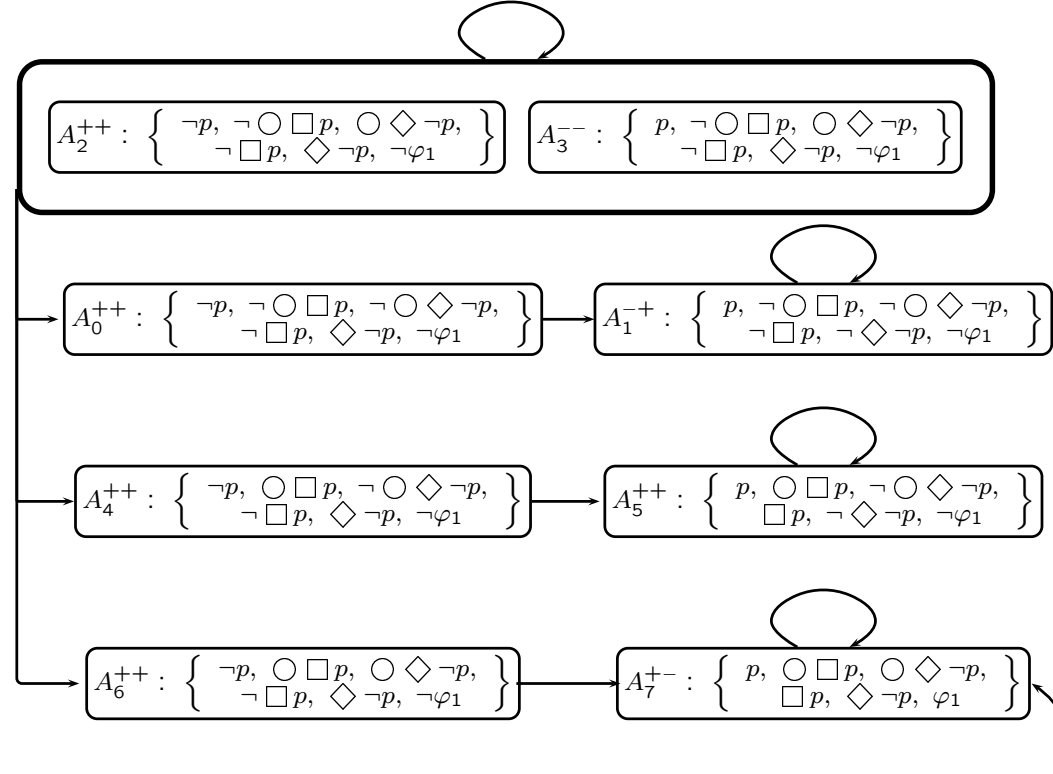


which has the infinite path A_7^ω .

However, A_7^{+-} does not fulfill the promising formula $\Diamond \neg p$, and thus A_7^ω is not a fulfilling path. Hence, φ_1 is not satisfiable.

Fig. 5.3: Tableau T_{φ_1} for formula

$$\varphi_1: \Box p \wedge \Diamond \neg p$$



Strongly Connected Subgraphs (SCS's)

Definitions

- A subgraph $S \subseteq T_\varphi$ is called strongly connected subgraph (SCS) if for every 2 distinct atoms $A, B \in S$, there exists a path from A to B which only passes through atoms of S

Note: a single-node subgraph is an SCS

- A single-node SCS is called transient (“bad”) if it is not connected to itself



- A non-transient (“good”) SCS S is fulfilling if every promising formula $\psi \in \Phi_\varphi$ is fulfilled by some atom $A \in S$, i.e.

$$\neg\psi \in A \quad \text{or} \quad r \in A$$

- SCS S is φ -reachable if there exist a path and $k \geq 0$

$$B_0, B_1, \dots, B_k, \dots$$

such that $\varphi \in B_0$ and $B_k \in S$.

Example: In $T_{\diamond p}$,

$\{A_1^+\}$, $\{A_1^+, A_2^-\}$, $\{A_4^+\}$ are fulfilling

$\{A_2^-\}$ is not fulfilling

All SCSs are $(\diamond p)$ -reachable.

A_3 is a transient SCS. All others are good SCSs.

Example: In T_{φ_1} (Fig. 5.3),

$\{A_4\}$ transient SCS

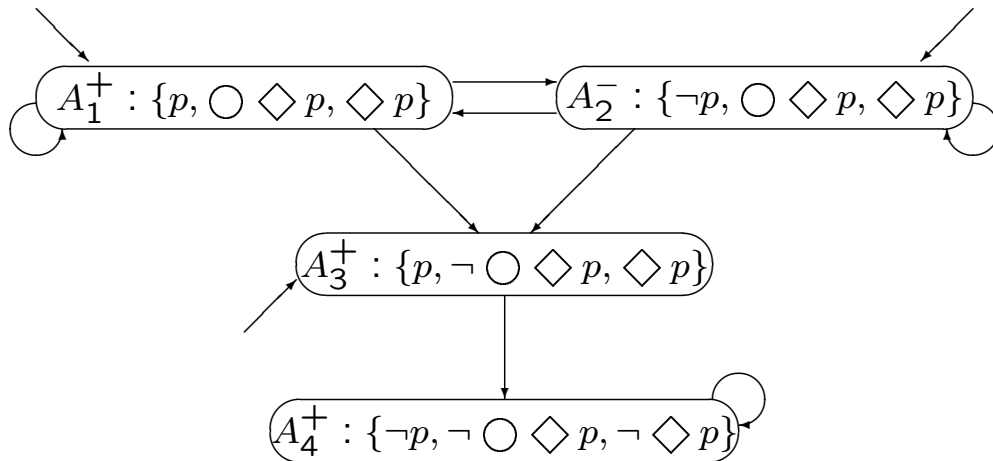
$\{A_5\}$ good SCS

$\{A_7\}$ is the only φ_1 -reachable SCS

$\{A_2^{++}, A_3^{--}\}$ $\{A_5^{++}\}$ fulfilling SCS's

$\{A_1^{-+}\}$ $\{A_7^{+-}\}$ SCS's but not fulfilling

Tableau $T_{\diamond p}$



Why SCS's?

In general a tableau may have infinitely many paths, so we cannot directly determine whether there are any fulfilling paths.

What needs to hold?

- When does a graph have an infinite path?
 - it must have a *non-transient* SCS.
- When is such an infinite path induced by a model of φ ?
 - SCS must be *φ -reachable*,
i.e., reachable from a node labeled by A , s.t. $\varphi \in A$
 - SCS must be *fulfilling*,
i.e., for every promising formula $\psi \in \Phi_\varphi$ the SCS must have at least one atom that fulfills ψ .

Proposition (satisfiability by SCS)

Formula φ is satisfiable

iff

the tableau T_φ contains a φ -reachable fulfilling SCS

The number of SCS's in a graph is finite, but may be exponential in the size of the graph!

Example: $\varphi_0 : \diamond p$

In T_{φ_0} , the fulfilling SCS's

$$\{A_1^+\} \quad \{A_1^+, A_2^-\} \quad \{A_4^+\}$$

are reachable from an initial node.

Thus, $\varphi_0 : \diamond p$ is satisfiable.

Satisfying models:

$$p^\omega \quad (p, \neg p)^\omega \quad p, (\neg p)^\omega.$$

Maximal Strongly Connected Subgraphs (MSCS's)

Definition: An SCS is maximal (MSCS) if it is not properly contained in any larger SCS

Example: In T_{φ_1} (Fig. 5.3),

$$\underbrace{\{A_2\} \{A_3\}}_{\text{not MSCS}} \quad \underbrace{\{A_2, A_3\}}_{\text{MSCS}}$$

In fact, it is sufficient to determine whether there exists a fulfilling reachable MSCS in T_φ . The number of MSCS in T_φ is bounded by $|T_\varphi|$.

Decomposition into MSCS's

There exists an efficient algorithm [Hopcroft&Tarjan] to decompose T_φ into subgraphs G_1, \dots, G_N such that

- each G_i is an MSCS (and therefore disjoint)
- $G_1 \cup \dots \cup G_N = T_\varphi$
- whenever there is an edge from a node in G_i to a node in G_j then $i \leq j$.

Algorithm SAT

(check satisfiability of arbitrary temporal formula φ)

- construct T_φ
- construct $\underline{T_\varphi^-}$ by removing all atoms that are not reachable from φ -atom
- decompose T_φ^- into MSCS's U_1, \dots, U_k
- check whether U_1, \dots, U_k is fulfilling:
 - if some U_i is fulfilling: φ is satisfiable.
A model is defined by the path leading from a φ -atom to U_i and staying in U_i forever from then on.
 - if no U_i is fulfilling: φ is not satisfiable.

Proposition (satisfiability and MSCS)

Formula φ is satisfiable
iff

The tableau T_{φ}^{-} contains a φ -reachable
fulfilling MSCS

Check validity of φ

Apply algorithm SAT to $\neg\varphi$

Algorithm reports success:

$\neg\varphi$ is satisfiable = φ is not valid
(the produced σ is a counterexample)

Algorithm reports failure:

$\neg\varphi$ is unsatisfiable = φ is valid

Example: Check satisfiability of

$$\varphi_1: \Box p \wedge \Diamond \neg p$$

T_{φ_1} (Fig 5.3)

$T_{\varphi_1}^{-} = \{A_7^{+-}\}$ MSCS of $T_{\varphi_1}^{-} = \{A_7^{+-}\}$

nonfulfilling \implies φ_1 is unsatisfiable

Example:

$$\psi_1 = \neg\varphi_1: \neg(\Box p \wedge \Diamond \neg p)$$

T_{ψ_1} (Fig 5.3)

$T_{\psi_1}^{-}$: all atoms

MSCS's:

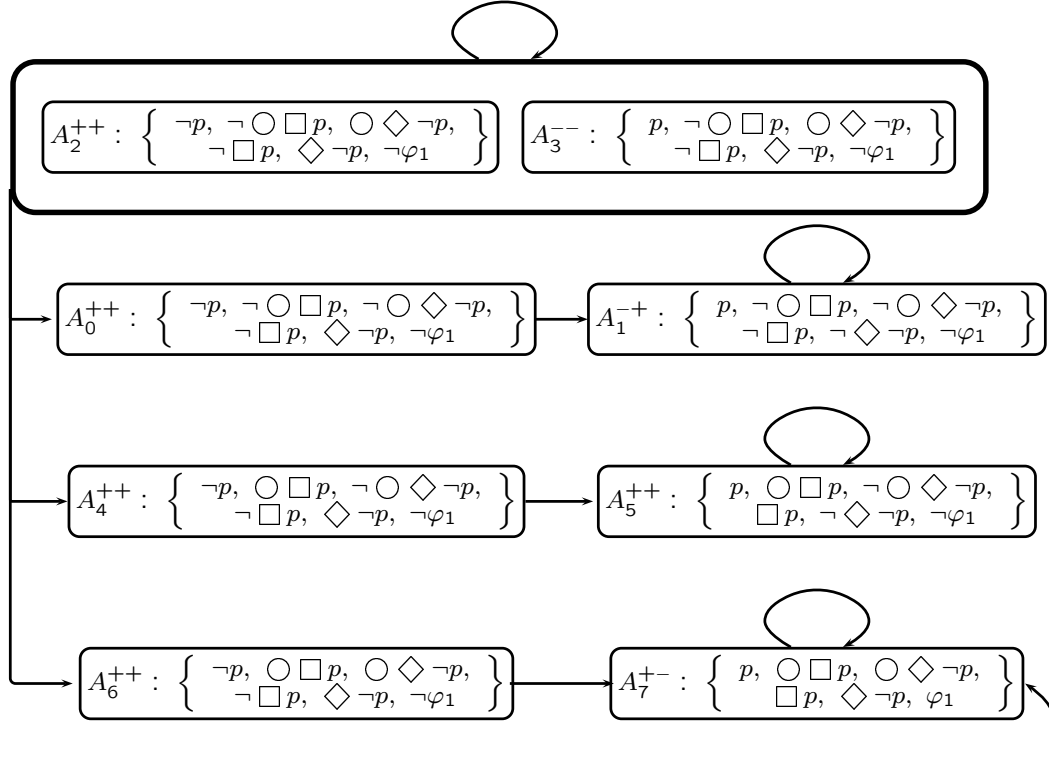
$\{A_0\}, \{A_4\}, \{A_6\}$	transient
$\{A_1^{-+}\}, \{A_7^{+-}\}$	non-fulfilling
$\{A_2^{++}, A_3^{-}\}, \{A_5^{++}\}$	fulfilling

ψ_1 satisfiable

For A_5^{++} : A_5^{ω} model $\langle p: T \rangle^{\omega}$
For $\{A_2^{++}, A_3^{-}\}$: $(A_2, A_3)^{\omega}$ model $(\langle p: F \rangle \langle p: T \rangle)^{\omega}$

each satisfies ψ_1

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



Example: Check satisfiability of

$$\varphi_2: \Box (\underbrace{\neg at_l_2 \vee \Diamond at_l_3}_{p_2})$$

$$\Phi_{\varphi_2}^+ : \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad at_l_2, \\ \Diamond at_l_3, \quad \circ \Diamond at_l_3, \quad at_l_3 \}$$

φ_2 -reachable atoms

$$\{ \underbrace{\Box p_2, \circ \Box p_2, p_2}_{\varphi_2}, \\ \underbrace{\quad}_{\text{fixed}} \\ \underbrace{at_l_2, at_l_3, \circ \Diamond at_l_3, \Diamond at_l_3, \neg \Diamond at_l_3}_{8 \text{ possibilities}}, \underbrace{\quad}_{\text{followed}} \}$$

One promising formula in Φ : $\Diamond at_l_3$ (and $\neg \Box p_2$)

$$\begin{aligned} A_0^+ &: \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad \neg at_l_2, \quad \neg at_l_3, \quad \neg \circ \Diamond at_l_3, \quad \neg \Diamond at_l_3 \} \\ A_1^- &: \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad \neg at_l_2, \quad \neg at_l_3, \quad \circ \Diamond at_l_3, \quad \Diamond at_l_3 \} \\ A_2^+ &: \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad \neg at_l_2, \quad at_l_3, \quad \neg \circ \Diamond at_l_3, \quad \Diamond at_l_3 \} \\ A_3^+ &: \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad \neg at_l_2, \quad at_l_3, \quad \circ \Diamond at_l_3, \quad \Diamond at_l_3 \} \\ A_4^- &: \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad at_l_2, \quad \neg at_l_3, \quad \circ \Diamond at_l_3, \quad \Diamond at_l_3 \} \\ A_5^+ &: \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad at_l_2, \quad at_l_3, \quad \neg \circ \Diamond at_l_3, \quad \Diamond at_l_3 \} \\ A_6^+ &: \{ \Box p_2, \quad \circ \Box p_2, \quad p_2, \quad at_l_2, \quad at_l_3, \quad \circ \Diamond at_l_3, \quad \Diamond at_l_3 \} \end{aligned}$$

Example: (Cont'd)

Atom #8

$\{ \underline{\Box p_2}, \underline{\bigcirc \Box p_2}, \underline{p_2}, at_{-l_2}, \neg at_{-l_3}, \neg \bigcirc \Diamond at_{-l_3}, \dots \}$

is not considered since

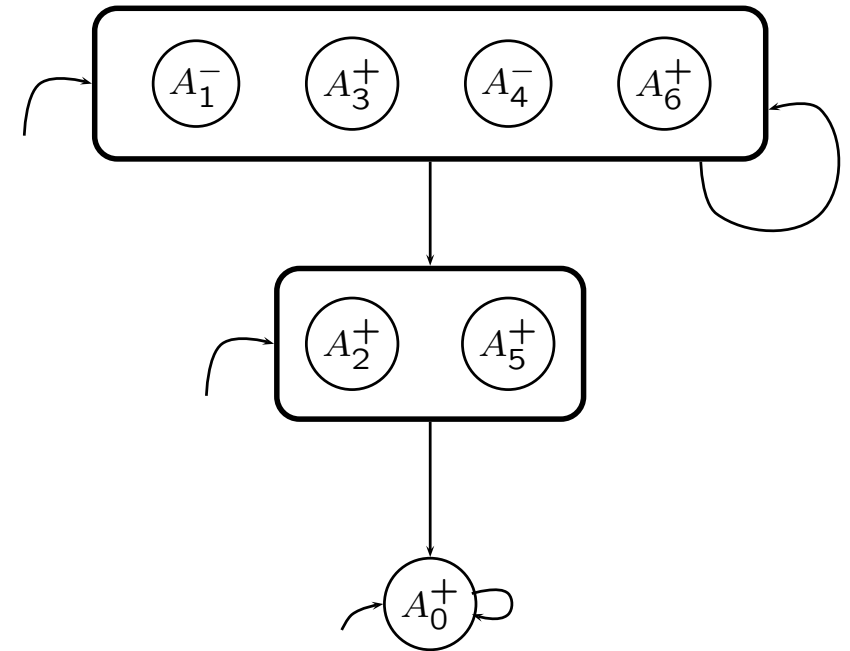
$\underbrace{\neg at_{-l_2} \vee \Diamond at_{-l_3}}_{p_2}$ and $at_{-l_2} \rightarrow \Diamond at_{-l_3}$

$\neg at_{-l_3}$ and $\neg \bigcirc \Diamond at_{-l_3} \rightarrow \neg \Diamond at_{-l_3}$

Tableau T_{φ_2} (Fig 5.4) = $T_{\varphi_2}^-$

formula $\Diamond at_{-l_3}$ promising at_{-l_3}

Fig. 5.4. Tableau for φ_2 : $\Box(\neg at_{-l_2} \vee \Diamond at_{-l_3})$



Decomposition to MSCS's

$\{A_1^-, A_3^+, A_4^-, A_6^+\} \{A_2^+\} \{A_5^+\} \{A_0^+\}$

fulfilling MSCS's: $\{A_0^+\}$, $\{A_1^-, A_3^+, A_4^-, A_6^+\}$
($\{A_2^+\}$ and $\{A_5^+\}$ are transient)

φ_2 is satisfiable

model (by A_0^ω)

$\langle at_{-l_2}: f, at_{-l_3}: f \rangle^\omega$

Pruning the tableau

Definition: MSCS S is terminal if

there are no edges leading from
atoms of S to atoms outside S

Example: Consider $\psi_1 = \neg\varphi_1 : \neg(\Box p \wedge \Diamond \neg p)$

In T_{ψ_1} (same as T_{φ_1} , Fig 5.3, except for initial nodes)

$\{A_1\} \{A_5\} \{A_7\}$ are terminal MSCS's

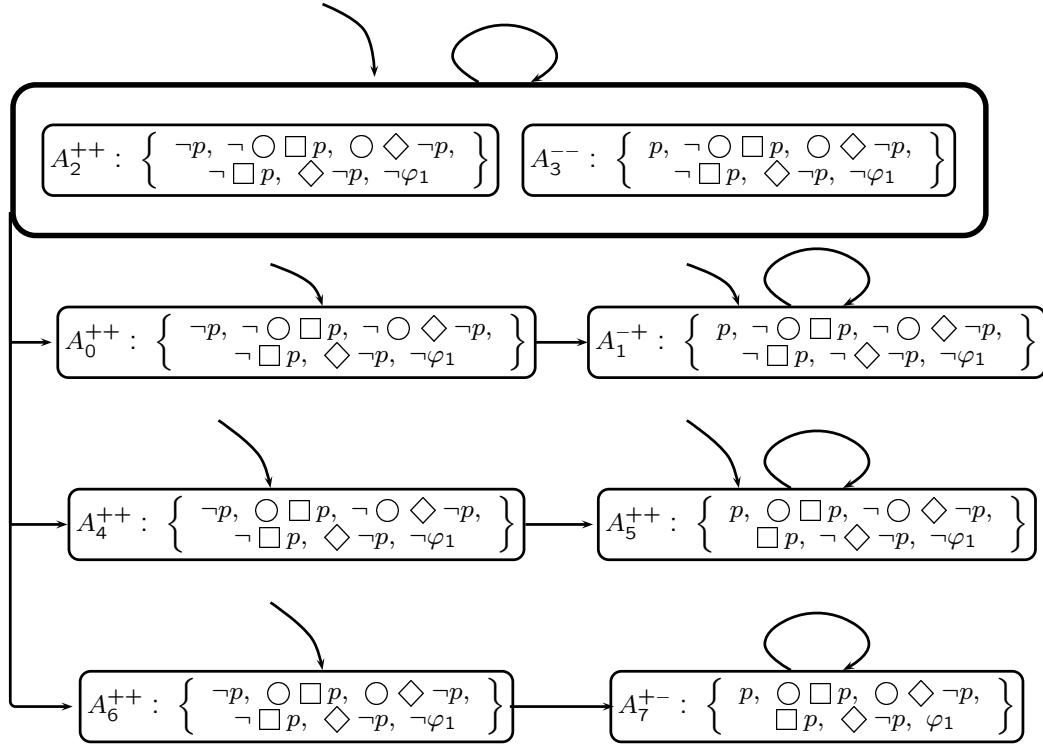
$\{A_6\} \{A_2, A_3\}$ are not

After constructing T_φ , remove useless atoms:

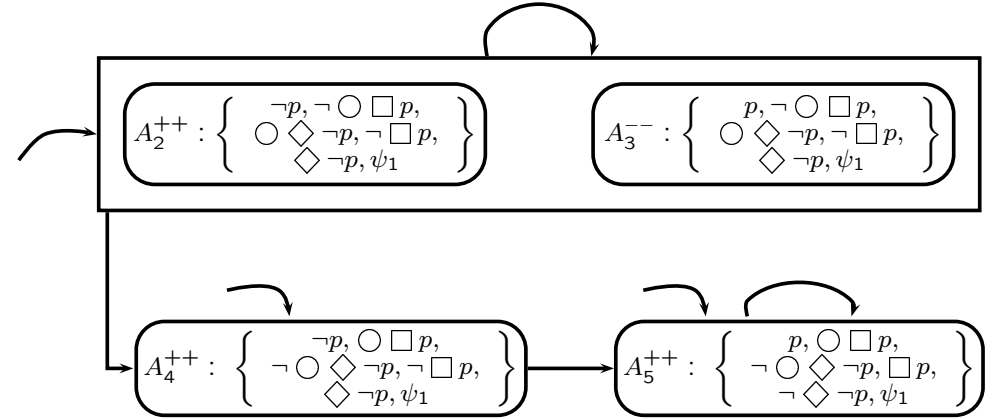
- Remove an MSCS that is not φ -reachable.
- Remove a terminal MSCS that is not fulfilling.

Iterate until no further atoms can be removed.

Fig. 5.3: Tableau T_{ψ_1} for formula
 $\psi_1: \neg(\Box p \wedge \Diamond \neg p)$.



Pruned Tableau $T_{\psi_1}^-$ for
 $\psi_1 : \neg(\Box p \wedge \Diamond \neg p)$



Fulfilling MSC's: $\{A_2^{++}, A_3^{--}\}, \{A_5^{++}\}$
 $\psi_1 : \neg(\Box p \wedge \Diamond \neg p)$ is satisfiable.

Example:

$$\varphi_3: \square \diamond (x = 3)$$

$$\Phi_{\varphi_3}^+: \{ \varphi_3, \diamond (x = 3), x = 3, \bigcirc \diamond (x = 3), \bigcirc \varphi_3 \}$$

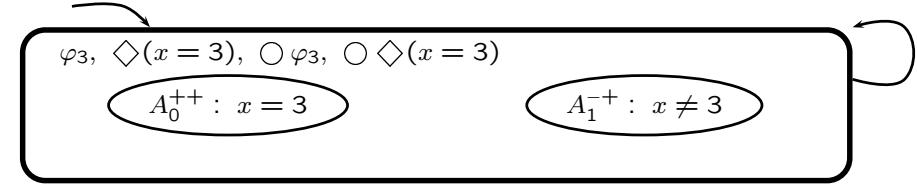
8 atoms A_0, \dots, A_7 (see list)

$$\{ \underbrace{x = 3, \bigcirc \diamond (x = 3), \bigcirc \varphi_3, \dots}_{8 \text{ possibilities}} \}$$

Promising formulas: $\diamond (x = 3)$ and $\neg \underbrace{\square \diamond (x = 3)}_{\varphi_3}$

$$\begin{array}{l} A_0^{++}: \{x = 3, \quad \bigcirc \diamond (x = 3), \quad \bigcirc \varphi_3, \quad \diamond (x = 3), \quad \varphi_3\} \\ A_1^{-+}: \{x \neq 3, \quad \bigcirc \diamond (x = 3), \quad \bigcirc \varphi_3, \quad \diamond (x = 3), \quad \varphi_3\} \\ A_2^{++}: \{x = 3, \quad \neg \bigcirc \diamond (x = 3), \quad \bigcirc \varphi_3, \quad \diamond (x = 3), \quad \varphi_3\} \\ A_3^{++}: \{x \neq 3, \quad \neg \bigcirc \diamond (x = 3), \quad \bigcirc \varphi_3, \quad \neg \diamond (x = 3), \quad \neg \varphi_3\} \\ A_4^{+-}: \{x = 3, \quad \bigcirc \diamond (x = 3), \quad \neg \bigcirc \varphi_3, \quad \diamond (x = 3), \quad \neg \varphi_3\} \\ A_5^{-}: \{x \neq 3, \quad \bigcirc \diamond (x = 3), \quad \neg \bigcirc \varphi_3, \quad \diamond (x = 3), \quad \neg \varphi_3\} \\ A_6^{+-}: \{x = 3, \quad \neg \bigcirc \diamond (x = 3), \quad \neg \bigcirc \varphi_3, \quad \diamond (x = 3), \quad \neg \varphi_3\} \\ A_7^{++}: \{x \neq 3, \quad \neg \bigcirc \diamond (x = 3), \quad \neg \bigcirc \varphi_3, \quad \neg \diamond (x = 3), \quad \neg \varphi_3\} \end{array}$$

Fig. 5.6. Pruned tableau $T_{\varphi_3}^-$



The φ_3 -reachable MSCS's: $\{A_0^{++}, A_1^{-+}\}$

$\{A_0^{++}, A_1^{-+}\}$ is fulfilling.

Therefore, φ_3 is satisfiable.

Model (by $(A_0, A_1)^\omega$): $(\langle x: 3 \rangle, \langle x: 0 \rangle)^\omega$

↑
arbitrary $x \neq 3$