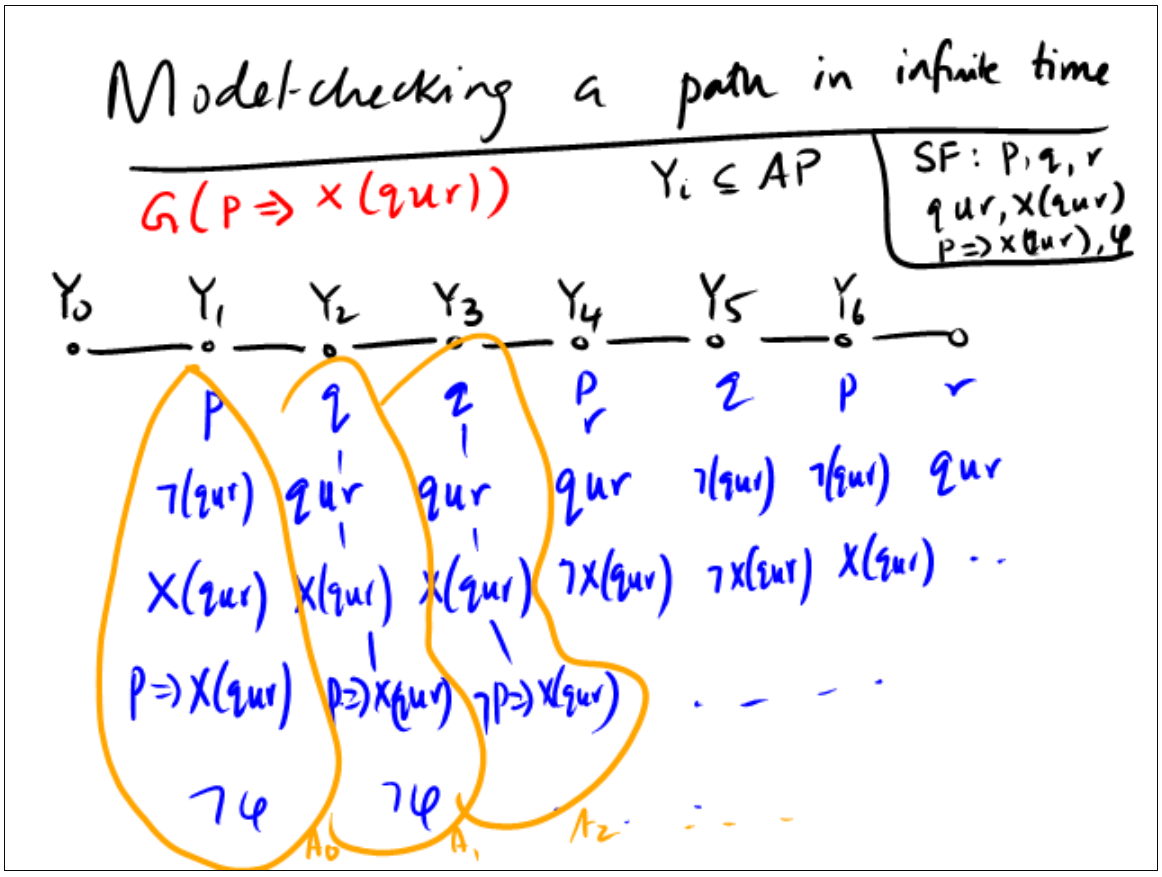
Lecture #8

LTL $\longrightarrow$ Automata

Model-checking LTL


Model-checking a path in infinite time
$G(p \Rightarrow X(qUr))$
$Y_i \subseteq AP$
SF: p, q, r, qUr, X(qUr), p ⇒ X(qUr), φ
Y_0 Y_1 Y_2 Y_3 Y_4 Y_5 Y_6
p
¬(qUr)
X(qUr)
p ⇒ X(qUr)
¬φ
q
qUr
X(qUr)
p ⇒ X(qUr)
¬φ
A0
q
qUr
X(qUr)
¬p ⇒ X(qUr)
A1
p
r
qUr
¬X(qUr)
A2
q
¬(qUr)
¬X(qUr)
p
¬(qUr)
X(qUr)
r
qUr
. . .

Generalized Büchi automaton.

$$A = (Q, Q_{in}, \delta, \{F_1, \ldots F_n\})$$

A run ρ is accepting if

$$\forall i. \left(Inf(\rho) \cap F_i \neq \emptyset \right)$$

$$CL(\varphi) = SF(\varphi) \cup \{X(\alpha \cup \beta) \mid \alpha \cup \beta \in SF(\varphi)\} \cup \{\neg\alpha \mid \alpha \in SF(\varphi)\}$$

where $\neg\neg\alpha$ is identified with α.

Atoms

An atom $A \subseteq CL(\varphi)$ such that

- $\alpha \in A \iff \neg\alpha \notin A$
- $\alpha \vee \beta \in A \iff (\alpha \in A \text{ or } \beta \in A)$
- $\alpha \cup \beta \in A \iff \begin{cases} (\beta \in A) \text{ or} \\ (\alpha \in A \text{ and } X(\alpha \cup \beta) \in A) \end{cases}$

Automaton for φ : A_φ

States : Atoms of φ — $2^{cl(\varphi)}$

$A \xrightarrow{Y} A' \quad Y \subseteq AP$

$\forall p \in AP : \quad p \in Y \iff p \in A \quad [A \cap AP = Y]$

$\forall \alpha \in CL(\varphi) \quad X\alpha \in A \iff \alpha \in A'$

$\forall (\alpha U \beta) \in CL(\varphi)$ — i'th until formula

$F_i = \{ A \mid \alpha U \beta \notin A \text{ or } \beta \in A \}$

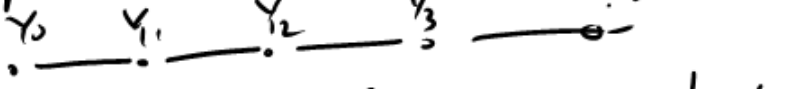
Initial states

$$Init = \{ A \mid \varphi \in A \}$$

$$\forall \omega \in (2^{AP})^{\omega} . \left(\omega \models \varphi \text{ iff } \omega \in A_{\varphi} \right)$$

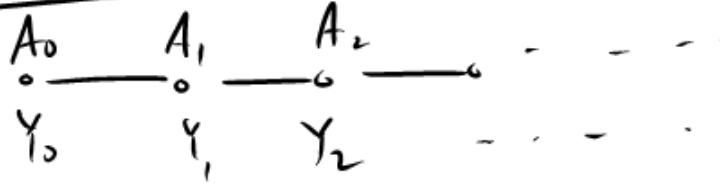
Proof outline

Suppose $\omega \models \varphi$



$$A_i = \{ \alpha \in CL(\varphi) \mid \alpha \text{ holds at position } i \}$$

The other way



φ

Induction on subformulas $\alpha \in CL(\varphi)$.

Argue that $w, i \models \alpha$ iff $\alpha \in A_i$

Model-checking

Model : S Spec : φ

All runs of S satisfy φ.

$\neg\varphi \longrightarrow A_{\neg\varphi}$

$(\text{Runs of } S) \cap \mathcal{L}(A_{\neg\varphi}) \stackrel{?}{\neq} \emptyset$

if yes then error
else S model-checks against φ.

Capture $Runs(S)$ using another automaton A_S with no winning condition.

$$\mathcal{L}(A_S) \cap \mathcal{L}(A_{\neg\varphi}) \neq \emptyset$$

$$\Leftrightarrow \mathcal{L}(A_S \cap A_{\neg\varphi}) \neq \emptyset$$

which is decidable in linear time in $|A_S| \cdot |A_{\neg\varphi}|$

$|S| \times 2^{O(|\varphi|)}$

Moreover, if $\mathcal{L}(A_S) \wedge \mathcal{L}(A_{\neg\varphi}) \neq \emptyset$,
model-checker will return

u, v s.t.

$uv^\omega \in \mathcal{L}(A_S)$

$uv^\omega \in \mathcal{L}(A_{\neg\varphi})$

i.e. $uv^\omega \not\models \varphi$