## Model Checking

Given a Kripke structure $M = (S, R, L)$, which states in $S$ satisfy the temporal logic formula $f$?

Depending on f:

- CTL Model checking
- LTL Model checking
- CTL* Model checking



## CTL Model Checking

CTL formulas express properies of *states*.

We label each state with the set of subformulas of $f$ that are satisfied in this state in the set $label(s)$.

When all subformulas of f are handled, we have $M, s \models f$ iff $f \in label(s)$.

Does the microwave-oven finally get heated when we start it?

$f = \mathbf{AG}(start \rightarrow \mathbf{AF}heat)$



Each step gives 6 cases:

- $f_1 \in L(s)$ What's already known
- $\neg f_1$
- $f_1 \vee f_2$
- $\mathbf{EX}f_1$
- $\mathbf{E}[f_1 \mathbf{U} f_2]$ Mark backwards.
- $\mathbf{EG}f_1$ Find strongly connected components.

Complexity for finding SCC: $O(|S|+|R|)$. One round for each subformula $O(|f| \cdot (|S| + |R|))$.



## Fairness

Can not express fairness in CTL formulas.

We define a *fair* Kripke structure $M = (S, R, L, F)$. $F \subseteq \mathcal{P}(S)$ is a set of fairness constraints.

A path $\pi = s_1, s_2, \ldots$ is *fair* iff for each $P \in F$, $inf(\pi) \cap P \neq \emptyset$

$$inf(\pi) = \{s | s = s_i \text{ for infinitely many } i\}$$

No change for $\neg f_1$, $f_1 \vee f_2$ or $\mathbf{EX}f_1$.

$\mathbf{EG}f_1$ - Only consider fair SCC. $C$ is fair iff for each $P_i \in F$ there is some state $s_i \in (C \cap P_i)$.

$\mathbf{E}[f_1 \mathbf{U} f_2]$ - Define $fair = \mathbf{EG}true$. To check $M, s \models_F \mathbf{E}[f_1 \mathbf{U} f_2]$ we check $M, s \models \mathbf{E}[f_1 \mathbf{U} f_2 \wedge fair]$

Complexity $O(|F| \cdot (|S| + |R|) \cdot |f|)$

# LTL

Want to check $M, s \models \mathbf{A}f$ for some *restricted path formula* $f$.

$f = \mathbf{A}((\neg heat)\mathbf{U}close)$

We check $M, s \models \neg\mathbf{E}\neg f$. That is, we try to find a counterexample.

Which components of a given $f$ holds in a state $s$?

- We consider subformulas and negations ($CL(f)$)
- To hold they must be consistent with $L(s)$

Define atom as a pair $(s_A, F_A)$ of a state and a consistent set of formulas. (also consistent with the labeling.)

We want interesting formulas so $F_A \subseteq CL(f) \cup AP$.



## The closure, $CL(f)$, of $f$.

$CL(f)$ is the smallest set of formulas containing $f$ and satisfying:

- $\neg f_1 \in CL(f)$ iff $f_1 \in CL(f)$
- if $f_1 \vee f_2 \in CL(f)$, then $f_1, f_2 \in CL(f)$
- if $\mathbf{X}f_1 \in CL(f)$ then $f_1 \in CL(f)$
- if $\neg\mathbf{X}f_1 \in CL(f)$ then $\mathbf{X}\neg f_1 \in CL(f)$
- if $f_1\mathbf{U}f_2 \in CL(f)$ then $f_1, f_2, \mathbf{X}[f_1\mathbf{U}f_2] \in CL(f)$



# Atoms

An atom is a pair $A = (s_A, F_A)$ with $s_A \in S$ and $F_A \subseteq CL(f) \cup AP$ such that:

- for each proposition $p \in AP$, $p \in F_A$ iff $p \in L(s_A)$
- for every $f_1 \in CL(f)$, $f_1 \in F_A$ iff $\neg f_1 \notin F_A$
- for every $f_1 \vee f_2 \in CL(f)$, $f_1 \vee f_2 \in F_A$ iff $f_1 \in F_A$ or $f_2 \in F_A$
- for every $\neg\mathbf{X}f_1 \in CL(f)$, $\neg\mathbf{X}f_1 \in F_A$ iff $\mathbf{X}\neg f_1 \in F_A$
- for every $f_1\mathbf{U}f_2 \in CL(f)$, $f_1\mathbf{U}f_2 \in F_A$ iff $f_2 \in F_A$ or $f_1, \mathbf{X}[f_1 U f_2] \in F_A$.



## Building the graph

Construct a graph G with all the atoms as verticies.

$(A, B)$ is an edge iff $(s_A, s_B) \in R$ and for every $f_1$, $\mathbf{X}f_1 \in F_A$ iff $f_1 \in F_B$

An *eventuality sequence* is an infinite path in G where if for some node A on the path, $f_1\mathbf{U}f_2 \in F_A$, then there is an atom B where $f_2 \in F_B$.

To use G for model checking:

> $M, s \models \mathbf{E}f$ iff there exists an eventuality sequence starting at an atom $(s, F)$ such that $f \in F$.

A strongly connected component C in G is *self fulfilling* iff for every atom $A$ in C with some $f_1 \mathbf{U} f_2 \in F_A$ there exists a $B$ in C such that $f_2 \in F_B$.

> There exists an eventuality sequence starting at an atom $(s, F)$ iff there is a path in G from $(s, F)$ to a self-fulfilling strongly connected component.



## Algorithm for LTL model checking

$M, s \models \mathbf{E}f$ iff there exists an atom $A = (s, F)$ in G such that $f \in F$ and there exists a path in G from A to a self-fulfilling strongly connected component.

Complexity: $O((|S| + |R|) \cdot 2^{O(|f|)})$.

The complexity is inherent in the problem. Finding a Hamiltonian path is reducible to determining if $M, s \models f$

$$f = \mathbf{E}[\mathbf{F}p_1 \wedge \ldots \wedge \mathbf{F}p_n \wedge \mathbf{G}(p_1 \rightarrow \mathbf{XG}\neg p_1 \wedge \ldots \wedge p_n \rightarrow \mathbf{XG}\neg p_n)$$



## CTL* model checking

If $f$ has any CTL subformula, use the CTL algorithm. Then substitute the subformula with a fresh atomic proposition.

Otherwise use the LTL algorithm.

Repeat until all of $f$ is processed.



## Example

$f = \mathbf{AG}((\neg close \wedge start) \rightarrow \mathbf{A}(\mathbf{G}\neg heat \vee \mathbf{F}\neg error))$

$f = \neg\mathbf{EF}(\neg close \wedge start \wedge \mathbf{E}(\mathbf{F}heat \wedge \mathbf{G}error))$