Title: Temporal Logic and Model Checking

Lecturer: Mike Gordon

Class: Computer Science Tripos, Part II

Term: Lent Term 2015

Lecture 1: 10:00 on Thu, 15 Jan, 2015
Lecture 2: 10:00 on Tue, 20 Jan, 2015
Lecture 3: 10:00 on Thu, 22 Jan, 2015
Lecture 4: 10:00 on Tue, 27 Jan, 2015
Lecture 5: 10:00 on Thu, 29 Jan, 2015
Lecture 6: 10:00 on Tue, 03 Feb, 2015
Lecture 7: 10:00 on Thu, 05 Feb, 2015
Lecture 8: 10:00 on Tue, 10 Feb, 2015

Location: Lecture Theatre 2, WGB

Duration: Eight lectures

Document created December 1, 2014
<table>
<thead>
<tr>
<th>Topic</th>
<th>Slides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction to models</td>
<td>1 - 9</td>
</tr>
<tr>
<td>Atomic properties</td>
<td>10</td>
</tr>
<tr>
<td>Trees and paths</td>
<td>11 - 12</td>
</tr>
<tr>
<td>Examples of properties</td>
<td>13 - 16</td>
</tr>
<tr>
<td>Reachability</td>
<td>17</td>
</tr>
<tr>
<td>Introduction to model checking</td>
<td>18 - 26</td>
</tr>
<tr>
<td>Symbolic model checking</td>
<td>27 - 32</td>
</tr>
<tr>
<td>Disjunctive partitioning of BDDs</td>
<td>33 - 35</td>
</tr>
<tr>
<td>Generating counter-examples</td>
<td>36 - 42</td>
</tr>
<tr>
<td>Introduction to temporal logic</td>
<td>43 - 45</td>
</tr>
<tr>
<td>Linear Temporal Logic (LTL)</td>
<td>46 - 58</td>
</tr>
<tr>
<td>Computation Tree Logic (CTL)</td>
<td>59 - 75</td>
</tr>
<tr>
<td>CTL model checking</td>
<td>75 - 83</td>
</tr>
<tr>
<td>History of model checking</td>
<td>84</td>
</tr>
<tr>
<td>Expressibility of LTL and CTL</td>
<td>57 - 58, 85 - 87</td>
</tr>
<tr>
<td>CTL*</td>
<td>88 - 90</td>
</tr>
<tr>
<td>Fairness</td>
<td>91 - 92</td>
</tr>
<tr>
<td>Propositional modal $\mu$-calculus</td>
<td>93</td>
</tr>
<tr>
<td>Sequential Extended Regular Expressions (SEREs)</td>
<td>94 - 95</td>
</tr>
<tr>
<td>Assertion Based Verification (ABV) and PSL</td>
<td>96 - 107</td>
</tr>
<tr>
<td>Dynamic verification: event semantics</td>
<td>108 - 116</td>
</tr>
<tr>
<td>Bisimulation</td>
<td>117 - 119</td>
</tr>
<tr>
<td>Abstraction</td>
<td>120 - 124</td>
</tr>
<tr>
<td>Counterexample Guided Abstraction Refinement (CEGAR)</td>
<td>125</td>
</tr>
<tr>
<td>Summary</td>
<td>126</td>
</tr>
</tbody>
</table>
Temporal Logic and Model Checking

- **Model**
  - mathematical structure extracted from hardware or software

- **Temporal logic**
  - provides a language for specifying functional properties

- **Model checking**
  - checks whether a given property holds of a model

---

- Model checking is a kind of **static verification**
  - dynamic verification is simulation (HW) or testing (SW)
A model is (for now) specified by a pair \((S, R)\)
- \(S\) is a set of states
- \(R\) is a transition relation

Models will get more components later
- \((S, R)\) also called a transition system

\(R\ s\ s'\) means \(s'\) can be reached from \(s\) in one step
- here \(R: S \to (S \to \mathbb{B})\) (where \(\mathbb{B} = \{\text{true}, \text{false}\}\))
- more conventional to have \(R \subseteq S \times S\), which is equivalent
- i.e. \(R_{\text{(this course)}}\ s\ s' \iff (s, s') \in R_{\text{(some textbooks)}}\)
A simple example model

A simple model: \[(\{0, 1, 2, 3\}, \lambda n \rightarrow n'. n' = n + 1 (mod 4))\]

- where “\(\lambda x. \cdots x \cdots\)” is the function mapping \(x\) to \(\cdots x \cdots\)
- so \(R n n' = (n' = n + 1 (mod 4))\)
- e.g. \(R 0 1 \land R 1 2 \land R 2 3 \land R 3 0\)

 Might be extracted from:

DIV: a software example

Perhaps a familiar program:

```
0:  R := X;
1:  Q := 0;
2:  WHILE Y \leq R DO
3:   (R := R - Y;
4:     Q := Q + 1)
5:   
```

State \((pc, x, y, r, q)\)
- \(pc \in \{0, 1, 2, 3, 4, 5\}\) program counter
- \(x, y, r, q \in \mathbb{Z}\) are the values of \(X, Y, R, Q\)

Model \((S_{DIV}, R_{DIV})\) where:

\[ S_{DIV} = [0..5] \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \quad \text{(where } [m..n] = \{m, m+1, \ldots, n\}\text{)} \]

\[ R_{DIV} (pc, x, y, r, q) (pc', x', y', r', q') = \]
- \((pc = 0) \Rightarrow (pc', x', y', r', q') = (1, x, y, x, q)) \quad \wedge \]
- \((pc = 1) \Rightarrow (pc', x', y', r', q') = (2, x, y, r, 0)) \quad \wedge \]
- \((pc = 2) \Rightarrow (pc', x', y', r', q') = \)
  if \(y \leq r\) then \((3, x, y, r, q)\) else \((5, x, y, r, q)) \quad \wedge \]
- \((pc = 3) \Rightarrow (pc', x', y', r', q') = (4, x, y, (r - y), q)) \quad \wedge \]
- \((pc = 4) \Rightarrow (pc', x', y', r', q') = (2, x, y, r, (q + 1))\)
Deriving a transition relation from a state machine

- State machine transition function: \( \delta : \text{Inp} \times \text{Mem} \rightarrow \text{Mem} \)
  - \( \text{Inp} \) is a set of inputs
  - \( \text{Mem} \) is a memory (set of storable values)

- Model: \((S_\delta, R_\delta)\) where:
  \[
  S_\delta = \text{Inp} \times \text{Mem}
  \]
  \[
  R_\delta (i, m) (i', m') = (m' = \delta(i, m))
  \]
  and
  - \( i' \) arbitrary: determined by environment not by machine
  - \( m' \) determined by input and current state of machine

- Deterministic machine, non-deterministic transition relation
  - inputs unspecified (determined by environment)
  - so called “input non-determinism”
**RCV: a state machine specification of a circuit**

- Part of a handshake circuit:

![Handshake Circuit Diagram]

- Input: \( \text{dreq} \), Memory: \((q_0, \text{dack})\)

- Relationships between Boolean values on wires:
  
  \[
  \begin{align*}
  q_{0\text{bar}} &= \neg q_0 \\
  a_0 &= q_{0\text{bar}} \land \text{dack} \\
  \text{or0} &= q_0 \lor a_0 \\
  a_1 &= \text{dreq} \land \text{or0}
  \end{align*}
  \]

- State machine: \(\delta_{\text{RCV}} : \mathbb{B} \times (\mathbb{B} \times \mathbb{B}) \rightarrow (\mathbb{B} \times \mathbb{B})\)

  \[
  \delta_{\text{RCV}} (\text{dreq}, (q_0, \text{dack})) = (\text{dreq}, \text{dreq} \land (q_0 \lor (\neg q_0 \land \text{dack})))
  \]

- RTL model – could have lower level model with clock edges
RCV: a model of the circuit

- Circuit from previous slide:

- State represented by a triple of Booleans \((dreq, q0, dack)\)
- By De Morgan Law: \(q0 \lor (\neg q0 \land dack) = q0 \lor dack\)
- Hence \(\delta_{RCV}\) corresponds to model \((S_{RCV}, R_{RCV})\) where:
  \[
  S_{RCV} = B \times B \times B
  \]
  \[
  R_{RCV} (dreq, q0, dack) (dreq', q0', dack') = (q0' = dreq) \land (dack' = (dreq \land (q0 \lor dack))))
  \]
  [Note: we are identifying \(B \times B \times B\) with \(B \times (B \times B)\)]
Some comments

- $R_{RCV}$ is non-deterministic and total
  - $R_{RCV} (1, 1, 1) (0, 1, 1)$ and $R_{RCV} (1, 1, 1) (1, 1, 1)$
    (where $1 = true$ and $0 = false$)
  - $R_{RCV} (dreq, q0, dack) (dreq', dreq, (dreq \land (q0 \lor dack)))$

- $R_{DIV}$ is deterministic and partial
  - at most one successor state
  - no successor when $pc = 5$

Non-deterministic models are very common, e.g. from:

- asynchronous hardware
- parallel software (more than one thread)

Can extend any transition relation $R$ to be total:

$$R_{total} s s' = \text{if } (\exists s''. R s s'') \text{ then } R s s' \text{ else } (s' = s)$$

$$= R s s' \lor (\lnot(\exists s''. R s s'') \land (s' = s))$$

- sometimes totality required
  (e.g. in the book *Model Checking* by Clarke et. al)
JM1: a non-deterministic software example

- From Jhala and Majumdar’s tutorial:

<table>
<thead>
<tr>
<th>Thread 1</th>
<th>Thread 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
</tr>
<tr>
<td>1: X:=1;</td>
<td>1: X:=2;</td>
</tr>
<tr>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
</tr>
<tr>
<td>3:</td>
<td>3:</td>
</tr>
</tbody>
</table>

- Two program counters, state: \((pc_1, pc_2, lock, x)\)

\[
S_{JM1} = [0..3] \times [0..3] \times \mathbb{Z} \times \mathbb{Z}
\]

\[
R_{JM1} (0, pc_2, 0, x) \quad (1, pc_2, 1, x)
\]

\[
R_{JM1} (1, pc_2, lock, x) (2, pc_2, lock, 1)
\]

\[
R_{JM1} (2, pc_2, 1, x) \quad (3, pc_2, 0, x)
\]

\[
R_{JM1} (pc_1, 0, 0, x) \quad (pc_1, 1, 1, x)
\]

\[
R_{JM1} (pc_1, 1, lock, x) (pc_1, 2, lock, 2)
\]

\[
R_{JM1} (pc_1, 2, 1, x) \quad (pc_1, 3, 0, x)
\]

- Not-deterministic:

\[
R_{JM1} (0, 0, 0, x) (1, 0, 1, x)
\]

\[
R_{JM1} (0, 0, 0, x) (0, 1, 1, x)
\]

- Not so obvious that \(R_{JM1}\) is a correct model
Atomic properties (properties of states)

- Atomic properties are true or false of individual states
  - an atomic property $p$ is a function $p : S \rightarrow \mathbb{B}$
  - can also be regarded as a subset of state: $p \subseteq S$

- Example atomic properties of $\text{RCV}$ (where $1 = \text{true}$ and $0 = \text{false}$)
  - $\text{Dreq}(\text{dreq}, q_0, \text{dack}) = (\text{dreq} = 1)$
  - $\text{NotQ0}(\text{dreq}, q_0, \text{dack}) = (q_0 = 0)$
  - $\text{Dack}(\text{dreq}, q_0, \text{dack}) = (\text{dack} = 1)$
  - $\text{NotDreqAndQ0}(\text{dreq}, q_0, \text{dack}) = (\text{dreq} = 0) \land (q_0 = 1)$

- Example atomic properties of $\text{DIV}$
  - $\text{AtStart}(\text{pc}, x, y, r, q) = (\text{pc} = 0)$
  - $\text{AtEnd}(\text{pc}, x, y, r, q) = (\text{pc} = 5)$
  - $\text{InLoop}(\text{pc}, x, y, r, q) = (\text{pc} \in \{3, 4\})$
  - $\text{YleqR}(\text{pc}, x, y, r, q) = (y \leq r)$
  - $\text{Invariant}(\text{pc}, x, y, r, q) = (x = r + (y \times q))$
Model behaviour viewed as a computation tree

- Atomic properties are true or false of individual states
- General properties are true or false of whole behaviour
- Behaviour of \((S, R)\) starting from \(s \in S\) as a tree:

- A path is shown in red
- Properties may look at all paths, or just a single path
  - CTL: Computation Tree Logic (all paths from a state)
  - LTL: Linear Temporal Logic (a single path)
Paths

- A path of \((S, R)\) is represented by a function \(\pi : \mathbb{N} \rightarrow S\)
  - \(\pi(i)\) is the \(i\)th element of \(\pi\) (first element is \(\pi(0)\))
  - might sometimes write \(\pi i\) instead of \(\pi(i)\)
  - \(\pi\downarrow i\) is the \(i\)-th tail of \(\pi\) so \(\pi\downarrow i(n) = \pi(i + n)\)
  - successive states in a path must be related by \(R\)

- Path \(R \ s \ \pi\) is true if and only if \(\pi\) is a path starting at \(s\):
  \[
  \text{Path } R \ s \ \pi = (\pi(0) = s) \land \forall i. \ R(\pi(i))(\pi(i+1))
  \]
  where:

\[
\text{Path} : (S \rightarrow S \rightarrow \mathbb{B}) \rightarrow S \rightarrow (\mathbb{N} \rightarrow S) \rightarrow \mathbb{B}
\]

transition relation

initial state

path
Consider this timing diagram:

- Following a rising edge on \( \text{dreq} \), the value of \( \text{dreq} \) remains 1 (i.e. \textit{true}) until it is acknowledged by a rising edge on \( \text{dack} \).
- Following a falling edge on \( \text{dreq} \), the value on \( \text{dreq} \) remains 0 (i.e. \textit{false}) until the value of \( \text{dack} \) is 0.

A property language is used to formalise such properties.
Example properties of the program DIV.

- on every execution if AtEnd is true then Invariant is true and YleqR is not true
- on every execution there is a state where AtEnd is true
- on any execution if there exists a state where YleqR is true then there is also a state where InLoop is true

Compare these with what is expressible in Hoare logic

- execution: a path starting from a state satisfying AtStart
Recall **JM1**: a non-deterministic program example

<table>
<thead>
<tr>
<th>Thread 1</th>
<th>Thread 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
</tr>
<tr>
<td>1: X:=1;</td>
<td>1: X:=2;</td>
</tr>
<tr>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
</tr>
<tr>
<td>3:</td>
<td>3:</td>
</tr>
</tbody>
</table>

\[
R_{JM1}(0, pc_2, 0, x) \quad (1, pc_2, 1, x) \\
R_{JM1}(1, pc_2, lock, x) \quad (2, pc_2, lock, 1) \\
R_{JM1}(2, pc_2, 1, x) \quad (3, pc_2, 0, x) \\
R_{JM1}(pc_1, 0, 0, x) \quad (pc_1, 1, 1, x) \\
R_{JM1}(pc_1, 1, lock, x) \quad (pc_1, 2, lock, 2) \\
R_{JM1}(pc_1, 2, 1, x) \quad (pc_1, 3, 0, x) \\
\]

- **An atomic property:**
  - \( \text{NotAt}_{11}(pc_1, pc_2, lock, x) = \neg((pc_1 = 1) \land (pc_2 = 1)) \)

- **A non-atomic property:**
  - all states reachable from \((0, 0, 0, 0)\) satisfy \( \text{NotAt}_{11} \)
  - this is an example of a reachability property
State satisfying $\text{NotAt11}$ unreachable from $(0,0,0,0)$

<table>
<thead>
<tr>
<th>Thread 1</th>
<th>Thread 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
</tr>
<tr>
<td>1: X:=1;</td>
<td>1: X:=2;</td>
</tr>
<tr>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
</tr>
<tr>
<td>3:</td>
<td></td>
</tr>
</tbody>
</table>

\[
\begin{align*}
R_{JM1}(0,pc_2,0,x) &\rightarrow (1,pc_2,1,x) \\
R_{JM1}(1,pc_2,lock,x) &\rightarrow (2,pc_2,lock,1) \\
R_{JM1}(2,pc_2,1,x) &\rightarrow (3,pc_2,0,x) \\
R_{JM1}(pc_1,0,0,x) &\rightarrow (pc_1,1,1,x) \\
R_{JM1}(pc_1,1,lock,x) &\rightarrow (pc_1,2,lock,2) \\
R_{JM1}(pc_1,2,1,x) &\rightarrow (pc_1,3,0,x)
\end{align*}
\]

- NotAt11$(pc_1, pc_2, lock, x) = \neg((pc_1 = 1) \land (pc_2 = 1))$

- Can only reach $pc_1 = 1 \land pc_2 = 1$ via:
  - $R_{JM1}(0,pc_2,0,x) \rightarrow (1,pc_2,1,x)$
  - $R_{JM1}(pc_1,0,0,x) \rightarrow (pc_1,1,1,x)$

- But:
  - $R_{JM1}(pc_1,pc_2,lock,x) \rightarrow (pc'_1,pc'_2,lock',x') \land pc'_1=0 \land pc'_2=1 \Rightarrow lock'=1$
  - $R_{JM1}(pc_1,pc_2,lock,x) \rightarrow (pc'_1,pc'_2,lock',x') \land pc'_1=1 \land pc'_2=0 \Rightarrow lock'=1$

- So can never reach $(0,1,0,x)$ or $(1,0,0,x)$

- So can’t reach $(1,1,1,x)$, hence never $(pc_1 = 1) \land (pc_2 = 1)$

- Hence all states reachable from $(0,0,0,0)$ satisfy NotAt11
Reachability

- $R \ s \ s'$ means $s'$ reachable from $s$ in one step
- $R^n \ s \ s'$ means $s'$ reachable from $s$ in $n$ steps
  \[ R^0 \ s \ s' = (s = s') \]
  \[ R^{n+1} \ s \ s' = \exists s''. \ R \ s \ s'' \land R^n \ s'' \ s' \]
- $R^* \ s \ s'$ means $s'$ reachable from $s$ in finite steps
  \[ R^* \ s \ s' = \exists n. \ R^n \ s \ s' \]
- Note: $R^* \ s \ s' \iff \exists \pi \ n. \ Path \ R \ s \ \pi \land (s' = \pi(n))$
- The set of states reachable from $s$ is $\{s' \mid R^* \ s \ s'\}$
- Verification problem: all states reachable from $s$ satisfy $p$
  - verify truth of $\forall s'. \ R^* \ s \ s' \Rightarrow p(s')$
  - e.g. all states reachable from $(0, 0, 0, 0)$ satisfy $\text{NotAt11}$
  - i.e. $\forall s'. \ R_{JM1}^* (0, 0, 0, 0) \ s' \Rightarrow \text{NotAt11}(s')$
Models and model checking

- Assume a model \((S, R)\)
- Assume also a set \(S_0 \subseteq S\) of initial states
- Assume also a set \(AP\) of atomic properties
- Assume a labeling function \(L : S \rightarrow \mathcal{P}(AP)\)
  - \(p \in L(s)\) means “\(s\) labelled with \(p\)” or “\(p\) true of \(s\)”
  - previously properties were functions \(p : S \rightarrow \mathbb{B}\)
  - now \(p \in AP\) is distinguished from \(\lambda s. p \in L(s)\)
  - assume \(T, F \in AP\) with forall \(s: T \in L(s)\) and \(F \notin L(s)\)
- A Kripke structure is a tuple \((S, S_0, R, L)\)
  - often the term “model” is used for a Kripke structure
  - i.e. a model is \((S, S_0, R, L)\) rather than just \((S, R)\)
- Model checking computes whether \((S, S_0, R, L) \models \phi\)
  - \(\phi\) is a property expressed in a property language
  - informally \(M \models \phi\) means “wff \(\phi\) is true in model \(M\)”
Minimal property language: $\phi$ is $\text{AG} p$ where $p \in AP$

- Consider properties $\phi$ of form $\text{AG} p$ where $p \in AP$
  - “AG” stands for “Always Globally”

- Assume $M = (S, S_0, R, L)$

- Reachable states of $M$ are $\{s' \mid \exists s \in S_0. R^* s s'\}$
  - i.e. the set of states reachable from an initial state
  - define $\text{Reachable } M = \{s' \mid \exists s \in S_0. R^* s s'\}$

- $M \models \text{AG} p$ means $p$ true of all reachable states of $M$

- If $M = (S, S_0, R, L)$ then $M \models \phi$ formally defined by:

\[
M \models \text{AG} p \iff \forall s'. s' \in \text{Reachable } M \Rightarrow p \in L(s')
\]
Model checking $M \models AGp$

- $M \models AGp \iff \forall s'. s' \in \text{Reachable } M \Rightarrow p \in L(s')$
  \iff \text{Reachable } M \subseteq \{ s' \mid p \in L(s') \}$

so:

- compute Reachable $M$ i.e. compute $\{ s' \mid \exists s \in S_0. R^* s s' \}$
- check $p$ true of all its members

Let $S = \{ s' \mid \exists s \in S_0. R^* s s' \}$

- Compute $S$ iteratively: $S = S_0 \cup S_1 \cup \cdots \cup S_n \cup \cdots$
  - i.e. $S = \bigcup_{n=0}^{\infty} S_n$
  - where: $S_0 = S_0$ (set of initial states)
  - and inductively: $S_{n+1} = S_n \cup \{ s' \mid \exists s \in S_n \land R s s' \}$

- Clearly $S_0 \subseteq S_1 \subseteq \cdots \subseteq S_n \subseteq \cdots$

- Hence if $S_m = S_{m+1}$ then $S = S_m$

- Algorithm: compute $S_0, S_1, \ldots$, until no change; check all members of computed set labelled with $p$
compute $S_0, S_1, \ldots$, until no change; check $p$ holds of all members of computed set

- Does the algorithm terminate?
  - yes, if set of states is finite, because then no infinite chains:
    \[ S_0 \subset S_1 \subset \cdots \subset S_n \subset \cdots \]

- How to represent $S_0, S_1, \ldots$?
  - explicitly (e.g. lists or something more clever)
  - symbolic expression

- Huge literature on calculating set of reachable states
Example: \( RCV \)

- Recall the handshake circuit:

![Handshake Circuit Diagram]

- State represented by a triple of Booleans \((dreq, q0, dack)\)

- A model of \( RCV \) is \( M_{RCV} \) where:

\[
M = (S_{RCV}, \{(1, 1, 1)\}, R_{RCV}, L_{RCV})
\]

and

\[
R_{RCV} (dreq, q0, dack) (dreq', q0', dack') = \\
(q0' = dreq) \land (dack' = (dreq \land (q0 \lor dack)))
\]
Possible states for $\text{RCV}$:
\{000, 001, 010, 011, 100, 101, 110, 111\}
where $b_2 b_1 b_0$ denotes state
\[\text{dreq} = b_2 \land q0 = b_1 \land \text{dack} = b_0\]
Computing Reachable $M_{RCV}$

Define:

\[
S_0 = \{ b_2 b_1 b_0 \mid b_2 b_1 b_0 \in \{111\} \} = \{111\}
\]

\[
S_{i+1} = S_i \cup \{ s' \mid \exists s \in S_i. R_{RCV} s s' \}
= S_i \cup \{ b'_2 b'_1 b'_0 \mid \\
\exists b_2 b_1 b_0 \in S_i. (b'_1 = b_2) \land (b'_0 = b_2 \land (b_1 \lor b_0)) \}
\]
Computing \( \text{Reachable } \mathcal{M}_{\text{RCV}} \) (continued)

Compute:

\[
\begin{align*}
S_0 &= \{111\} \\
S_1 &= \{111\} \cup \{011\} \\
&= \{111, 011\} \\
S_2 &= \{111, 011\} \cup \{000, 100\} \\
&= \{111, 011, 000, 100\} \\
S_3 &= \{111, 011, 000, 100\} \cup \{010, 110\} \\
&= \{111, 011, 000, 100, 010, 110\} \\
S_i &= S_3 \quad (i > 3)
\end{align*}
\]

Hence \( \text{Reachable } \mathcal{M}_{\text{RCV}} = \{111, 011, 000, 100, 010, 110\} \)
Model checking $M_{\text{RCV}} \models AG\, p$

- $M = (S_{\text{RCV}}, \{111\}, R_{\text{RCV}}, L_{\text{RCV}})$

- To check $M_{\text{RCV}} \models AG\, p$
  - compute Reachable $M_{\text{RCV}} = \{111, 011, 000, 100, 010, 110\}$
  - check Reachable $M_{\text{RCV}} \subseteq \{s \mid p \in L_{\text{RCV}}(s)\}$, i.e. check:
    
    $p \in L_{\text{RCV}}(111)$
    $p \in L_{\text{RCV}}(011)$
    $p \in L_{\text{RCV}}(000)$
    $p \in L_{\text{RCV}}(100)$
    $p \in L_{\text{RCV}}(010)$
    $p \in L_{\text{RCV}}(110)$
Symbolic Boolean model checking of reachability

- Assume states are \( n \)-tuples of Booleans \((b_1, \ldots, b_n)\)
  - \( b_i \in \mathbb{B} = \{\text{true}, \text{false}\} \)
  - \( S = \mathbb{B}^n \), so \( S \) is finite: \( 2^n \) states

- Assume \( n \) distinct Boolean variables: \( v_1, \ldots, v_n \)
  - e.g. if \( n = 3 \) then could have \( v_1 = x, v_2 = y, v_3 = z \)

- Boolean formula \( f(v_1, \ldots, v_n) \) represents a subset of \( S \)
  - \( f(v_1, \ldots, v_n) \) only contains variables \( v_1, \ldots, v_n \)
  - \( f(b_1, \ldots, b_n) \) denotes result of substituting \( b_i \) for \( v_i \)
  - \( f(v_1, \ldots, v_n) \) determines \( \{(b_1, \ldots, b_n) | f(b_1, \ldots, b_n) \Leftrightarrow \text{true}\} \)

- Example \( \neg(x = y) \) represents \( \{(\text{true, false}), (\text{false, true})\} \)

- Transition relations also represented by Boolean formulae
  - e.g. \( R_{RCV} \) represented by:
    
    \[
    (q_0' = dreq) \land (dack' = (dreq \land (q_0 \lor (\neg q_0 \land dack))))
    \]
Symbolically represent Boolean formulae as BDDs

Key features of Binary Decision Diagrams (BDDs):

- canonical *(given a variable ordering)*
- efficient to manipulate

Variables:
\[ v = \text{if } v \text{ then } 1 \text{ else } 0 \]
\[ \neg v = \text{if } v \text{ then } 0 \text{ else } 1 \]

Example: BDDs of variable \( v \) and \( \neg v \)

Example: BDDs of \( v_1 \land v_2 \) and \( v_1 \lor v_2 \)
More BDD examples

- BDD of $v_1 = v_2$

- BDD of $v_1 \neq v_2$
BDD of a transition relation

- BDDs of

\[(v' = (v = v)) \land (v' = (v \neq v))\]

with two different variable orderings

- **Exercise:** draw BDD of \(R_{RCV}\)
Standard BDD operations

- If formulae $f_1, f_2$ represents sets $S_1, S_2$, respectively then $f_1 \land f_2, f_1 \lor f_2$ represent $S_1 \cap S_2, S_1 \cup S_2$ respectively

- Standard algorithms compute Boolean operation on BDDs

- Abbreviate $(v_1, \ldots, v_n)$ to $\vec{v}$

- If $f(\vec{v})$ represents $S$ and $g(\vec{v}, \vec{v}')$ represents $\{(\vec{v}, \vec{v}') \mid R \vec{v} \vec{v}'\}$ then $\exists \vec{u}. f(\vec{u}) \land g(\vec{u}, \vec{v})$ represents $\{\vec{v} \mid \exists \vec{u}. \vec{u} \in S \land R \vec{u} \vec{v}\}$

- Can compute BDD of $\exists \vec{u}. h(\vec{u}, \vec{v})$ from BDD of $h(\vec{u}, \vec{v})$
  - e.g. BDD of $\exists v_1. h(v_1, v_2)$ is BDD of $h(T, v_2) \lor h(F, v_2)$

- From BDD of formula $f(v_1, \ldots, v_n)$ can compute $b_1, \ldots, b_n$ such that if $v_1 = b_1, \ldots, v_n = b_n$ then $f(b_1, \ldots, b_n) \iff \text{true}$
  - $b_1, \ldots, b_n$ is a satisfying assignment (SAT problem)
  - used for counterexample generation (see later)
Reachable States via BDDs

- Assume $M = (S, S_0, R, L)$ and $S = \mathbb{B}^n$
- Represent $R$ by Boolean formulae $g(\vec{v}, \vec{v}')$
- Iteratively define formula $f_n(\vec{v})$ representing $S_n$
  
  $f_0(\vec{v}) = \text{formula representing } S_0$
  $f_{n+1}(\vec{v}) = f_n(\vec{v}) \lor (\exists \vec{u}. f_n(\vec{u}) \land g(\vec{u}, \vec{v}))$

- Let $B_0, B_R$ be BDDs representing $f_0(\vec{v}), g(\vec{v}, \vec{v}')$
- Iteratively compute BDDs $B_n$ representing $f_n$
  
  $B_{n+1} = B_n \lor (\exists \vec{u}. B_n[\vec{u}/\vec{v}] \land B_R[\vec{u}, \vec{v}/\vec{v}, \vec{v}'])$
  
  - efficient using (blue underlined) standard BDD algorithms (renaming, conjunction, disjunction, quantification)
  - BDD $B_n$ only contains variables $\vec{v}$: represents $S_n \subseteq S$

- At each iteration check $B_{n+1} = B_n$ efficient using BDDs
  
  - when $B_{n+1} = B_n$ can conclude $B_n$ represents Reachable $M$
  - we call this BDD $B_M$ in a later slide (i.e. $B_M = B_n$)
Example BDD optimisation: disjunctive partitioning

Three state transition functions in parallel

\[ \delta_x, \delta_y, \delta_z : B \times B \times B \rightarrow B \]

- Transition relation (asynchronous interleaving semantics):

\[
R (x, y, z) (x', y', z') = \\
(x' = \delta_x (x, y, z) \land y' = y \land z' = z) \lor \\
(x' = x \land y' = \delta_y (x, y, z) \land z' = z) \lor \\
(x' = x \land y' = y \land z' = \delta_z (x, y, z))
\]
Avoiding building big BDDs

Transition relation for three transition functions in parallel
\[ R(x, y, z) (x', y', z') = \]
\[ (x' = \delta_x(x, y, z) \land y' = y \land z' = z) \lor \]
\[ (x' = x \land y' = \delta_y(x, y, z) \land z' = z) \lor \]
\[ (x' = x \land y' = y \land z' = \delta_z(x, y, z)) \]

Recall symbolic iteration:
\[ f_{n+1}(\vec{v}) = f_n(\vec{v}) \lor (\exists \vec{u}. f_n(\vec{u}) \land g(\vec{u}, \vec{v})) \]

For this particular \( R \) (see next slide):
\[ f_{n+1}(x, y, z) \]
\[ = f_n(x, y, z) \lor (\exists \overline{x} \overline{y} \overline{z}. f_n(\overline{x}, \overline{y}, \overline{z}) \land R(\overline{x}, \overline{y}, \overline{z}) (x, y, z)) \]
\[ = f_n(x, y, z) \lor (\exists \overline{x}. f_n(\overline{x}, y, z) \land x = \delta_x(\overline{x}, y, z)) \lor \]
\[ (\exists \overline{y}. f_n(x, \overline{y}, z) \land y = \delta_y(x, \overline{y}, z)) \lor \]
\[ (\exists \overline{z}. f_n(x, y, \overline{z}) \land z = \delta_z(x, y, \overline{z})) \]

Don’t need to calculate BDD of \( R \)!
Disjunctive partitioning – Exercise: understand this

\[ \exists x \ y \ z. \ f_n(x, y, z) \land R(x, y, z)(x, y, z) \]

\[ = \exists x \ y \ z. \ f_n(x, y, z) \land ((x = \delta_x(x, y, z) \land y = \bar{y} \land z = \bar{z}) \lor \\
(\bar{x} = x \land y = \delta_y(x, y, z) \land z = \bar{z}) \lor \\
(\bar{x} = x \land y = \bar{y} \land z = \delta_z(x, y, z))) \]

\[ = (\exists x \ y \ z. \ f_n(x, y, z) \land x = \delta_x(x, y, z) \land y = \bar{y} \land z = \bar{z}) \lor \\
(\exists x \ y \ z. \ f_n(x, y, z) \land \bar{x} = x \land y = \delta_y(x, y, z) \land z = \bar{z}) \lor \\
(\exists x \ y \ z. \ f_n(x, y, z) \land \bar{x} = x \land y = \bar{y} \land z = \delta_z(x, y, z))) \]

\[ = ((\exists x. \ f_n(x, y, z) \land x = \delta_x(x, y, z)) \land (\exists \bar{y}. \ y = \bar{y}) \land (\exists \bar{z}. \ z = \bar{z})) \lor \\
((\exists x. \ x = \bar{x}) \land (\exists \bar{y}. \ f_n(x, y, z) \land y = \delta_y(x, y, z)) \land (\exists \bar{z}. \ z = \bar{z})) \lor \\
((\exists x. \ x = \bar{x}) \land (\exists \bar{y}. \ y = \bar{y}) \land (\exists \bar{z}. \ f_n(x, y, z) \land z = \delta_z(x, y, z)))) \]

\[ = (\exists x. \ f_n(x, y, z) \land x = \delta_x(x, y, z)) \lor \\
(\exists \bar{y}. \ f_n(x, y, z) \land y = \delta_y(x, y, z)) \lor \\
(\exists \bar{z}. \ f_n(x, y, z) \land z = \delta_z(x, y, z)) \]
Verification and counterexamples

- Typical safety question:
  - is property $p$ true in all reachable states?
  - i.e. check $M \models \text{AG} p$
  - i.e. is $\forall s. s \in \text{Reachable } M \Rightarrow p(s)$

- Check using BDDs
  - compute BDD $B_M$ of Reachable $M$
  - compute BDD $B_p$ of $p(\vec{v})$
  - check if BDD of $B_M \Rightarrow B_p$ is the single node $1$

- Valid because $true$ represented by a unique BDD (canonical property)

- If BDD is not $1$ can get counterexample
Generating counterexamples (general idea)

BDD algorithms can find **satisfying assignments** (SAT)

- Suppose not all reachable states of model $M$ satisfy $p$
- i.e. $\exists s \in \text{Reachable } M. \neg(p(s))$
- Set of reachable state $S$ given by: $S = \bigcup_{n=0}^{\infty} S_n$
- Iterate to find least $n$ such that $\exists s \in S_n. \neg(p(s))$
- Use SAT to find $b_n$ such that $b_n \in S_n \land \neg(p(b_n))$
- Use SAT to find $b_{n-1}$ such that $b_{n-1} \in S_{n-1} \land R b_{n-1} b_n$
- Use SAT to find $b_{n-2}$ such that $b_{n-2} \in S_{n-2} \land R b_{n-2} b_{n-1}$
  - ... 
- Iterate to find $b_0, b_1, \ldots, b_{n-1}, b_n$ where $b_i \in S_i \land R b_{i-1} i$
- Then $b_0 \ b_1 \ \cdots \ b_{n-1} \ b_n$ is a path to a counterexample
Use SAT to find \( s_{n-1} \) such that \( s_{n-1} \in S_{n-1} \land R s_{n-1} s_n \)

- Suppose states \( s, s' \) symbolically represented by \( \vec{v}, \vec{v}' \)
- Suppose BDD \( B_i \) represents \( \vec{v} \in S_i (1 \leq i \leq n) \)
- Suppose BDD \( B_R \) represents \( R \vec{v} \vec{v}' \)
- Then BDD
  \[
  (B_{n-1} \land B_R[\vec{b}_n/\vec{v}'])
  \]
  represents
  \( \vec{v} \in S_{n-1} \land R \vec{v} \vec{b}_n \)
- Use SAT to find a valuation \( \vec{b}_{n-1} \) for \( \vec{v} \)
- Then BDD
  \[
  (B_{n-1} \land B_R[\vec{b}_n/\vec{v}'])[\vec{b}_{n-1}/\vec{v}]
  \]
  represents
  \( \vec{b}_{n-1} \in S_{n-1} \land R \vec{b}_{n-1} \vec{b}_n = 1 \)
Generating counterexamples with BDDs

BDD algorithms can find satisfying assignments (SAT)

- \( M = (S, S_0, R, L) \) and \( B_0, B_1, \ldots, B_M, B_R, B_p \) as earlier
- Suppose \( B_M \Rightarrow B_p \) is not 1
- Must exist a state \( s \in \text{Reachable } M \) such that \( \neg(p \ s) \)
- Let \( B_{\neg p} \) be the BDD representing \( \neg(p \ \vec{v}) \)
- Iterate to find first \( n \) such that \( B_n \triangle \neg B_p \)
- Use SAT to find \( \vec{b}_n \) such that \( (B_n \triangle \neg B_p)[\vec{b}_n/\vec{v}] \)
- Use SAT to find \( \vec{b}_{n-1} \) such that \( (B_{n-1} \triangle B_R[\vec{b}_{n}/\vec{v}'])[\vec{b}_{n-1}/\vec{v}] \)
- For \( 0 < i < n \) find \( \vec{b}_{i-1} \) such that \( (B_{i-1} \triangle B_R[\vec{b}_{i}/\vec{v}'])[\vec{b}_{i-1}/\vec{v}] \)
- \( \vec{b}_0, \ldots, \vec{b}_i, \ldots, \vec{b}_n \) is a counterexample trace
- Sometimes can use partitioning to avoid constructing \( B_R \)
Consider a 3x3 array of 9 switches

Suppose each switch 1, 2, ..., 9 can either be on or off, and that toggling any switch will automatically toggle all its immediate neighbours. For example, toggling switch 5 will also toggle switches 2, 4, 6 and 8, and toggling switch 6 will also toggle switches 3, 5 and 9.

(a) Devise a state space [4 marks] and transition relation [6 marks] to represent the behavior of the array of switches

You are given the problem of getting from an initial state in which even numbered switches are on and odd numbered switches are off, to a final state in which all the switches are off.

(b) Write down predicates on your state space that characterises the initial [2 marks] and final [2 marks] states.

(c) Explain how you might use a model checker to find a sequences of switches to toggle to get from the initial to final state. [6 marks]

You are not expected to actually solve the problem, but only to explain how to represent it in terms of model checking.
A state is a vector \((v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9)\), where \(v_i \in \mathbb{B}\). A transition relation \(\text{Trans}\) is then defined by:

\[
\text{Trans}(v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8, v_9)(v_1', v_2', v_3', v_4', v_5', v_6', v_7', v_8', v_9') =
\begin{align*}
&((v_1' = \neg v_1) \land (v_2' = \neg v_2) \land (v_3' = v_3) \land (v_4' = \neg v_4) \land (v_5' = v_5) \land \\
&(v_6' = v_6) \land (v_7' = v_7) \land (v_8' = v_8) \land (v_9' = v_9)) \tag{toggle switch 1} \\
\lor ((v_1' = v_1) \land (v_2' = \neg v_2) \land (v_3' = \neg v_3) \land (v_4' = v_4) \land (v_5' = v_5) \land \\
&(v_6' = v_6) \land (v_7' = v_7) \land (v_8' = v_8) \land (v_9' = v_9)) \tag{toggle switch 2} \\
\lor ((v_1' = \neg v_1) \land (v_2' = v_2) \land (v_3' = v_3) \land (v_4' = \neg v_4) \land (v_5' = \neg v_5) \land \\
&(v_6' = v_6) \land (v_7' = \neg v_7) \land (v_8' = v_8) \land (v_9' = v_9)) \tag{toggle switch 3} \\
\lor ((v_1' = v_1) \land (v_2' = v_2) \land (v_3' = v_3) \land (v_4' = v_4) \land (v_5' = \neg v_5) \land \\
&(v_6' = v_6) \land (v_7' = \neg v_7) \land (v_8' = v_8) \land (v_9' = v_9)) \tag{toggle switch 4} \\
\lor ((v_1' = \neg v_1) \land (v_2' = v_2) \land (v_3' = v_3) \land (v_4' = \neg v_4) \land (v_5' = \neg v_5) \land \\
&(v_6' = v_6) \land (v_7' = v_7) \land (v_8' = \neg v_8) \land (v_9' = v_9)) \tag{toggle switch 5} \\
\lor ((v_1' = v_1) \land (v_2' = v_2) \land (v_3' = \neg v_3) \land (v_4' = v_4) \land (v_5' = \neg v_5) \land \\
&(v_6' = \neg v_6) \land (v_7' = v_7) \land (v_8' = v_8) \land (v_9' = \neg v_9)) \tag{toggle switch 6} \\
\lor ((v_1' = v_1) \land (v_2' = v_2) \land (v_3' = \neg v_3) \land (v_4' = \neg v_4) \land (v_5' = v_5) \land \\
&(v_6' = v_6) \land (v_7' = \neg v_7) \land (v_8' = \neg v_8) \land (v_9' = v_9)) \tag{toggle switch 7} \\
\lor ((v_1' = \neg v_1) \land (v_2' = v_2) \land (v_3' = \neg v_3) \land (v_4' = \neg v_4) \land (v_5' = v_5) \land \\
&(v_6' = v_6) \land (v_7' = \neg v_7) \land (v_8' = \neg v_8) \land (v_9' = v_9)) \tag{toggle switch 8} \\
\lor ((v_1' = v_1) \land (v_2' = v_2) \land (v_3' = \neg v_3) \land (v_4' = \neg v_4) \land (v_5' = v_5) \land \\
&(v_6' = \neg v_6) \land (v_7' = v_7) \land (v_8' = \neg v_8) \land (v_9' = v_9)) \tag{toggle switch 9}
\end{align*}
\]
Solution (continued)

Predicates $\text{Init}$, $\text{Final}$ characterising the initial and final states, respectively, are defined by:

$$\text{Init}(v_1,v_2,v_3,v_4,v_5,v_6,v_7,v_8,v_9) = \neg v_1 \land v_2 \land \neg v_3 \land v_4 \land \neg v_5 \land v_6 \land \neg v_7 \land v_8 \land \neg v_9$$

$$\text{Final}(v_1,v_2,v_3,v_4,v_5,v_6,v_7,v_8,v_9) = \neg v_1 \land \neg v_2 \land \neg v_3 \land \neg v_4 \land \neg v_5 \land \neg v_6 \land \neg v_7 \land \neg v_8 \land \neg v_9$$

Model checkers can find counter-examples to properties, and sequences of transitions from an initial state to a counter-example state. Thus we could use a model checker to find a trace to a counter-example to the property that

$$\neg \text{Final}(v_1,v_2,v_3,v_4,v_5,v_6,v_7,v_8,v_9)$$
Properties

- \( \forall s \in S_0. \forall s'. R^* s s' \Rightarrow p s' \) says \( p \) true in all reachable states

- Might want to verify other properties
  1. DeviceEnabled holds infinitely often along every path
  2. From any state it is possible to get to a state where Restart holds
  3. After a three or more consecutive occurrences of Req there will eventually be an Ack

- Temporal logic can express such properties
- There are several temporal logics in use
  - LTL is good for the first example above
  - CTL is good for the second example
  - PSL is good for the third example

- Model checking:
  - Emerson, Clarke & Sifakis: Turing Award 2008
  - widely used in industry: first hardware, later software
Temporal logic (originally called “tense logic”)

Originally devised for investigating: “the relationship between tense and modality attributed to the Megarian philosopher Diodorus Cronus (ca. 340-280 BCE)”. Mary Prior, his wife, recalls “I remember his waking me one night [in 1953], coming and sitting on my bed, ... and saying he thought one could make a formalised tense logic”.

A. N. Prior
1914-1969

- Temporal logic: deductive system for reasoning about time
  - temporal formulae for expressing temporal statements
  - deductive system for proving theorems
- Temporal logic model checking
  - uses semantics to check truth of temporal formulae in models
- Temporal logic proof systems also important in CS
  - use pioneered by Amir Pnueli (1996 Turing Award)
  - not considered in this course

Recommended: http://plato.stanford.edu/entries/prior/
Temporal logic formulae (statements)

- Many different languages of temporal statements
  - linear time (LTL)
  - branching time (CTL)
  - finite intervals (SEREs)
  - industrial languages (PSL, SVA)

- Prior used linear time, Kripke suggested branching time:

  ... we perhaps should not regard time as a linear series ... there are several possibilities for what the next moment may be like - and for each possible next moment, there are several possibilities for the moment after that. Thus the situation takes the form, not of a linear sequence, but of a 'tree'.

  [Saul Kripke, 1958 (aged 17, still at school)]

- CS issues different from philosophical issues
  - Moshe Vardi: “Branching vs. Linear Time: Final Showdown”
    
    [Hyperlink: http://www.computer.org/portal/web/awards/Vardi]

---

Moshe Vardi
www.computer.org

“For fundamental and lasting contributions to the development of logic as a unifying foundational framework and a tool for modeling computational systems”

2011 Harry H. Goode Memorial Award Recipient
Linear Temporal Logic (LTL)

- Grammar of well formed formulae (wff) $\phi$

  $\phi ::= p$ \quad (Atomic formula: $p \in AP$)
  $\mid \neg \phi$ \quad (Negation)
  $\mid \phi_1 \lor \phi_2$ \quad (Disjunction)
  $\mid X\phi$ \quad (successor)
  $\mid F\phi$ \quad (sometimes)
  $\mid G\phi$ \quad (always)
  $\mid [\phi_1 U \phi_2]$ \quad (Until)

- Details differ from Prior’s tense logic – but similar ideas

- Semantics define when $\phi$ true in model $M$

  - where $M = (S, R, S_0, L)$ – a Kripke structure
  - notation: $M \models \phi$ means $\phi$ true in model $M$
  - model checking algorithms compute this (when decidable)
$\models \phi$ means “wff $\phi$ is true in model $M$”

- If $M = (S, S_0, R, L)$ then
  $\pi$ is an $M$-path starting from $s$ iff Path $R s \pi$

- If $M = (S, S_0, R, L)$ then we define $M \models \phi$ to mean:
  $\phi$ is true on all $M$-paths starting from a member of $S_0$

- We will define $\llbracket \phi \rrbracket_{M(\pi)}$ to mean
  $\phi$ is true on the $M$-path $\pi$

- Thus $M \models \phi$ will be formally defined by:
  $M \models \phi \iff \forall \pi \ s. \ s \in S_0 \land \text{Path } R s \pi \Rightarrow \llbracket \phi \rrbracket_{M(\pi)}$

- It remains to actually define $\llbracket \phi \rrbracket_{M}$ for all wffs $\phi$
Definition of $\llbracket \phi \rrbracket_M(\pi)$

- $\llbracket \phi \rrbracket_M(\pi)$ is the application of function $\llbracket \phi \rrbracket_M$ to path $\pi$
  - thus $\llbracket \phi \rrbracket_M : (\mathbb{N} \rightarrow S) \rightarrow \mathbb{B}$

- Let $M = (S, S_0, R, L)$
  
  $\llbracket \phi \rrbracket_M$ is defined by structural induction on $\phi$

\[
\begin{align*}
\llbracket p \rrbracket_M(\pi) &= p \in L(\pi \ 0) \\
\llbracket \neg \phi \rrbracket_M(\pi) &= \neg(\llbracket \phi \rrbracket_M(\pi)) \\
\llbracket \phi_1 \lor \phi_2 \rrbracket_M(\pi) &= \llbracket \phi_1 \rrbracket_M(\pi) \lor \llbracket \phi_2 \rrbracket_M(\pi) \\
\llbracket X \phi \rrbracket_M(\pi) &= \llbracket \phi \rrbracket_M(\pi \downarrow 1) \\
\llbracket F \phi \rrbracket_M(\pi) &= \exists i. \llbracket \phi \rrbracket_M(\pi \downarrow i) \\
\llbracket G \phi \rrbracket_M(\pi) &= \forall i. \llbracket \phi \rrbracket_M(\pi \downarrow i) \\
\llbracket [\phi_1 U \phi_2] \rrbracket_M(\pi) &= \exists i. \llbracket \phi_2 \rrbracket_M(\pi \downarrow i) \land \forall j. j < i \Rightarrow \llbracket \phi_1 \rrbracket_M(\pi \downarrow j)
\end{align*}
\]

- We look at each of these semantic equations in turn
\[ [p]_M(\pi) = p(\pi 0) \]

- Assume \( M = (S, S_0, R, L) \)

- We have: \( [p]_M(\pi) = p \in L(\pi 0) \)
  - \( p \) is an atomic property, i.e. \( p \in AP \)
  - \( \pi : \mathbb{N} \to S \) so \( \pi 0 \in S \)
  - \( \pi 0 \) is the first state in path \( \pi \)
  - \( p \in L(\pi 0) \) is \textit{true} iff atomic property \( p \) holds of state \( \pi 0 \)

\( [p]_M(\pi) \) means \( p \) holds of the first state in path \( \pi \)

- Assume \( T, F \in AP \) with for all \( s \): \( T \in L(s) \) and \( F \not\in L(s) \)
  - \( [T]_M(\pi) \) is always true
  - \( [F]_M(\pi) \) is always false
\[ \lbrack \neg \phi \rbrack_M(\pi) = \neg (\lbrack \phi \rbrack_M(\pi)) \]

\[ \lbrack \phi_1 \lor \phi_2 \rbrack_M(\pi) = \lbrack \phi_1 \rbrack_M(\pi) \lor \lbrack \phi_2 \rbrack_M(\pi) \]

- \[ \lbrack \neg \phi \rbrack_M(\pi) \] true iff \[ \lbrack \phi \rbrack_M(\pi) \] is not true

- \[ \lbrack \phi_1 \lor \phi_2 \rbrack_M(\pi) \] true iff \[ \lbrack \phi_1 \rbrack_M(\pi) \] is true or \[ \lbrack \phi_2 \rbrack_M(\pi) \] is true
$$[X\phi]_M(\pi) = [\phi]_M(\pi\downarrow 1)$$

- $$[X\phi]_M(\pi) = [\phi]_M(\pi\downarrow 1)$$
  - $$\pi\downarrow 1$$ is $$\pi$$ with the first state chopped off
    - $$\pi\downarrow 1(0) = \pi(1 + 0) = \pi(1)$$
    - $$\pi\downarrow 1(1) = \pi(1 + 1) = \pi(2)$$
    - $$\pi\downarrow 1(2) = \pi(1 + 2) = \pi(3)$$
    - $$\vdots$$

- $$[X\phi]_M(\pi)$$ true iff $$[\phi]_M$$ true starting at the next state of $$\pi$$
\[[F\phi]_M(\pi) = \exists i. [\phi]_M(\pi \downarrow i)\]

- \([F\phi]_M(\pi) = \exists i. [\phi]_M(\pi \downarrow i)\)
  - \(\pi \downarrow i\) is \(\pi\) with the first \(i\) states chopped off
    - \(\pi \downarrow i(0) = \pi(i + 0) = \pi(i)\)
    - \(\pi \downarrow i(1) = \pi(i + 1)\)
    - \(\pi \downarrow i(2) = \pi(i + 2)\)
    - \(\vdots\)
  - \([\phi]_M(\pi \downarrow i)\) true iff \([\phi]_M\) true \textit{starting} \textit{i} states along \(\pi\)

- \([F\phi]_M(\pi)\) true iff \([\phi]_M\) true \textit{starting somewhere} along \(\pi\)

- “\(F\phi\)” is read as “sometimes \(\phi\)”
\[ \text{[G} \phi \text{]}_M(\pi) = \forall i. \text{[}\phi\text{]}_M(\pi \downarrow i) \]

- \text{[G} \phi \text{]}_M(\pi) = \forall i. \text{[}\phi\text{]}_M(\pi \downarrow i)
  - \pi \downarrow i \text{ is } \pi \text{ with the first } i \text{ states chopped off}
  - \text{[}\phi\text{]}_M(\pi \downarrow i) \text{ true iff } \text{[}\phi\text{]}_M \text{ true starting } i \text{ states along } \pi

- \text{[G} \phi \text{]}_M(\pi) \text{ true iff } \text{[}\phi\text{]}_M \text{ true starting anywhere along } \pi

- "G} \phi \text{" is read as "always } \phi \text{" or "globally } \phi \text{"

- \( M \models \text{AG} \rho \) defined earlier: \( M \models \text{AG} \rho \iff M \models \text{G}(\rho) \)

- G\ is\ definable\ in\ terms\ of\ F\ and\ \neg:\ G} \phi = \neg(F(\neg\phi))

  \[ \text{[\neg(F(\neg\phi))]}_M(\pi) = \neg(\text{[F(\neg\phi)}]_M(\pi)) \]
  \[ = \neg(\exists i. \text{[}\neg\phi\text{]}_M(\pi \downarrow i)) \]
  \[ = \neg(\exists i. \neg(\text{[}\phi\text{]}_M(\pi \downarrow i))) \]
  \[ = \forall i. \text{[}\phi\text{]}_M(\pi \downarrow i) \]
  \[ = \text{[G} \phi \text{]}_M(\pi) \]
$$[[\phi_1 U \phi_2]]_M(\pi) = \exists i. [[\phi_2]]_M(\pi \downarrow i) \land \forall j. j<i \Rightarrow [[\phi_1]]_M(\pi \downarrow j)$$

- $$[[\phi_1 U \phi_2]]_M(\pi) = \exists i. [[\phi_2]]_M(\pi \downarrow i) \land \forall j. j<i \Rightarrow [[\phi_1]]_M(\pi \downarrow j)$$
  - $$[[\phi_2]]_M(\pi \downarrow i)$$ true iff $$[[\phi_2]]_M$$ true starting $$i$$ states along $$\pi$$
  - $$[[\phi_1]]_M(\pi \downarrow j)$$ true iff $$[[\phi_1]]_M$$ true starting $$j$$ states along $$\pi$$

- $$[[\phi_1 U \phi_2]]_M(\pi)$$ is true iff
  - $$[[\phi_2]]_M$$ is true somewhere along $$\pi$$ and up to then $$[[\phi_1]]_M$$ is true

- “$$[[\phi_1 U \phi_2]]$$” is read as “$$\phi_1$$ until $$\phi_2$$”

- $$F$$ is definable in terms of $$[- U -]$$: $$F\phi = [[T U \phi]]_M(\pi)$$
  
  $$[[T U \phi]]_M(\pi)$$
  
  $$= \exists i. [[\phi]]_M(\pi \downarrow i) \land \forall j. j<i \Rightarrow [[T]]_M(\pi \downarrow j)$$
  
  $$= \exists i. [[\phi]]_M(\pi \downarrow i) \land \forall j. j<i \Rightarrow true$$
  
  $$= \exists i. [[\phi]]_M(\pi \downarrow i) \land true$$
  
  $$= \exists i. [[\phi]]_M(\pi \downarrow i)$$
  
  $$= [[F\phi]]_M(\pi)$$
Review of Linear Temporal Logic (LTL)

- Grammar of *well formed formulae* (wff) $\phi$

  $$\phi ::= p \quad \text{(Atomic formula: } p \in AP)$$

  $$\neg \phi \quad \text{(Negation)}$$

  $$\phi_1 \lor \phi_2 \quad \text{(Disjunction)}$$

  $$\text{X} \phi \quad \text{(successor)}$$

  $$\text{F} \phi \quad \text{(sometimes)}$$

  $$\text{G} \phi \quad \text{(always)}$$

  $$[\phi_1 \text{ U } \phi_2] \quad \text{(Until)}$$

- $M \models \phi$ means $\phi$ holds on all $M$-paths

- $M = (S, S_0, R, L)$

- $\llbracket \phi \rrbracket_M(\pi)$ means $\phi$ is true on the $M$-path $\pi$

- $M \models \phi \iff \forall \pi \ s. \ s \in S_0 \land \text{Path } R \ s \ \pi \Rightarrow \llbracket \phi \rrbracket_M(\pi)$
LTL examples

- “DeviceEnabled holds infinitely often along every path”
  \[ G(F \text{DeviceEnabled}) \]

- “Eventually the state becomes permanently Done“
  \[ F(G \text{Done}) \]

- “Every Req is followed by an Ack”
  \[ G(\text{Req} \Rightarrow F \text{Ack}) \]
  Number of Req and Ack may differ - no counting

- “If Enabled infinitely often then Running infinitely often”
  \[ G(F \text{Enabled}) \Rightarrow G(F \text{Running}) \]

- “An upward going lift at the second floor keeps going up if a passenger requests the fifth floor”
  \[ G(\text{AtFloor2} \land \text{DirectionUp} \land \text{RequestFloor5} \Rightarrow [\text{DirectionUp} U \text{AtFloor5}]) \]

(acknowledgement: http://pswlab.kaist.ac.kr/courses/cs402-2011/temporal-logic2.pdf)
A property not expressible in LTL

Consider models $M$ and $M'$ below

$M = (\{s_0, s_1\}, \{s_0\}, \{(s_0, s_0), (s_0, s_1), (s_1, s_1)\}, L)$

$M' = (\{s_0\}, \{s_0\}, \{(s_0, s_0)\}, L)$

where: $L = \lambda s. \text{if } s = s_0 \text{ then } \emptyset \text{ else } \{P\}$

Every $M'$-path is also an $M$-path

So if $\phi$ true on every $M$-path then $\phi$ true on every $M'$-path

Hence for any $\phi$ if $M \models \phi$ then $M' \models \phi$

Consider property “can always reach a state satisfying $P$”

true: $M \models \text{"can always reach a state satisfying $P"}$

false: $M' \models \text{"can always reach a state satisfying $P"}$

“can always reach a state satisfying $P$” not expressible in LTL
LTL expressibility

“can always reach a state satisfying $P$”

- In LTL $M \models \phi$ says $\phi$ holds of all paths of $M$

- LTL formulae $\phi$ are evaluated on paths . . . . path formulae

- Want to say there exists a path to $p \in AP$
  - $\exists \pi. \text{Path } R s \pi \land \exists i. p \in L(\pi(i))$

- CTL properties are evaluated at a state . . . state formulae
  - they can talk about both some or all paths
  - starting from the state they are evaluated at
Computation Tree Logic (CTL)

- LTL formulae $\phi$ are evaluated on paths .... path formulae
- CTL formulae $\psi$ are evaluated on states .. state formulae

Syntax of CTL well-formed formulae:

$$\psi ::= p \quad (\text{Atomic formula } p \in AP)$$
$$\quad \quad \quad \quad \quad \neg \psi \quad (\text{Negation})$$
$$\quad \quad \quad \quad \quad \psi_1 \land \psi_2 \quad (\text{Conjunction})$$
$$\quad \quad \quad \quad \quad \psi_1 \lor \psi_2 \quad (\text{Disjunction})$$
$$\quad \quad \quad \quad \quad \psi_1 \Rightarrow \psi_2 \quad (\text{Implication})$$
$$\quad \quad \quad \quad \quad \text{AX}\psi \quad (\text{All successors})$$
$$\quad \quad \quad \quad \quad \text{EX}\psi \quad (\text{Some successors})$$
$$\quad \quad \quad \quad \quad \text{A}[\psi_1 \text{ U } \psi_2] \quad (\text{Until – along all paths})$$
$$\quad \quad \quad \quad \quad \text{E}[\psi_1 \text{ U } \psi_2] \quad (\text{Until – along some path})$$
Assume $M = (S, S_0, R, L)$ and then define:

\[
\begin{align*}
\sem{p}_{M}(s) & = p \in L(s) \\
\sem{\neg \psi}_{M}(s) & = \neg(\sem{\psi}_{M}(s)) \\
\sem{\psi_1 \land \psi_2}_{M}(s) & = \sem{\psi_1}_{M}(s) \land \sem{\psi_2}_{M}(s) \\
\sem{\psi_1 \lor \psi_2}_{M}(s) & = \sem{\psi_1}_{M}(s) \lor \sem{\psi_2}_{M}(s) \\
\sem{\psi_1 \Rightarrow \psi_2}_{M}(s) & = \sem{\psi_1}_{M}(s) \Rightarrow \sem{\psi_2}_{M}(s) \\
\sem{Ax \psi}_{M}(s) & = \forall s'. R s s' \Rightarrow \sem{\psi}_{M}(s') \\
\sem{Ex \psi}_{M}(s) & = \exists s'. R s s' \land \sem{\psi}_{M}(s') \\
\sem{A[\psi_1 U \psi_2]}_{M}(s) & = \forall \pi. \text{Path } R s \pi \\
& \quad \Rightarrow \exists i. \sem{\psi_2}_{M}(\pi(i)) \\
& \quad \land \forall j. j < i \Rightarrow \sem{\psi_1}_{M}(\pi(j)) \\
\sem{E[\psi_1 U \psi_2]}_{M}(s) & = \exists \pi. \text{Path } R s \pi \\
& \quad \land \exists i. \sem{\psi_2}_{M}(\pi(i)) \\
& \quad \land \forall j. j < i \Rightarrow \sem{\psi_1}_{M}(\pi(j))
\end{align*}
\]
The defined operator $\textbf{AF}$

- Define $\textbf{AF} \psi = A[T \cup \psi]$

- $\textbf{AF} \psi$ true at $s$ iff $\psi$ true somewhere on every $R$-path from $s$

\[
[\textbf{AF} \psi]_M(s) = [A[T \cup \psi]]_M(s) \\
= \forall \pi. \text{Path } R s \pi \\
\Rightarrow \\
\exists i. [\psi]_M(\pi(i)) \land \forall j. j < i \Rightarrow [I]_M(\pi(j)) \\
= \forall \pi. \text{Path } R s \pi \\
\Rightarrow \\
\exists i. [\psi]_M(\pi(i)) \land \forall j. j < i \Rightarrow \text{true} \\
= \forall \pi. \text{Path } R s \pi \Rightarrow \exists i. [\psi]_M(\pi(i))
The defined operator \( \text{EF} \)

- **Define** \( \text{EF} \psi = \mathsf{E} [ \mathsf{T} \mathsf{U} \psi ] \)

- **\( \text{EF} \psi \) true at \( s \) iff \( \psi \) true *somewhere on some* \( R \)-path from \( s \)

\[
\llbracket \text{EF} \psi \rrbracket_M(s) = \llbracket \mathsf{E} [ \mathsf{T} \mathsf{U} \psi ] \rrbracket_M(s)
\]

\[
= \exists \pi. \text{Path } R \ s \ \pi
\]

\[
\land
\exists i. \llbracket \psi \rrbracket_M(\pi(i)) \land \forall j. j < i \Rightarrow \llbracket \mathsf{T} \rrbracket_M(\pi(j))
\]

\[
= \exists \pi. \text{Path } R \ s \ \pi
\]

\[
\land
\exists i. \llbracket \psi \rrbracket_M(\pi(i)) \land \forall j. j < i \Rightarrow \text{true}
\]

\[
= \exists \pi. \text{Path } R \ s \ \pi \land \exists i. \llbracket \psi \rrbracket_M(\pi(i))
\]

- “can reach a state satisfying \( p \in AP \)” is \( \text{EF} \ p \)
The defined operator \( \text{AG} \)

- Define \( \text{AG}\psi = \neg\text{EF}(\neg\psi) \)
- \( \text{AG}\psi \) true at \( s \) iff \( \psi \) true everywhere on every \( R \)-path from \( s \)

\[
\llbracket \text{AG}\psi \rrbracket_M(s) = \llbracket \neg\text{EF}(\neg\psi) \rrbracket_M(s)
= \neg(\llbracket \text{EF}(\neg\psi) \rrbracket_M(s))
= \neg(\exists \pi. \text{Path } R \ s \ \pi \land \exists i. \llbracket \neg\psi \rrbracket_M(\pi(i)))
= \neg(\exists \pi. \text{Path } R \ s \ \pi \land \exists i. \neg\llbracket \psi \rrbracket_M(\pi(i)))
= \forall \pi. \neg(\text{Path } R \ s \ \pi \land \exists i. \neg\llbracket \psi \rrbracket_M(\pi(i)))
= \forall \pi. \neg\text{Path } R \ s \ \pi \lor \neg(\exists i. \neg\llbracket \psi \rrbracket_M(\pi(i)))
= \forall \pi. \neg\text{Path } R \ s \ \pi \lor \forall i. \neg\llbracket \psi \rrbracket_M(\pi(i))
= \forall \pi. \text{Path } R \ s \ \pi \Rightarrow \forall i. \llbracket \psi \rrbracket_M(\pi(i))

- \( \text{AG}\psi \) means \( \psi \) true at all reachable states
- \( \llbracket \text{AG}(p) \rrbracket_M(s) \equiv \forall s'. R^* \ s \ s' \Rightarrow p \in L(s') \)
- “can always reach a state satisfying \( p \in AP \)” is \( \text{AG}(\text{EF } p) \)
The defined operator $\text{EG}$

- Define $\text{EG}\psi = \neg\text{AF}(\neg\psi)$

- $\text{EG}\psi$ true at $s$ iff $\psi$ true everywhere on some $R$-path from $s$

\[
\llbracket \text{EG}\psi \rrbracket_M(s) = \llbracket \neg\text{AF}(\neg\psi) \rrbracket_M(s) \\
= \neg(\llbracket \text{AF}(\neg\psi) \rrbracket_M(s)) \\
= \neg(\forall \pi. \text{Path } R s \pi \Rightarrow \exists i. \llbracket \neg\psi \rrbracket_M(\pi(i))) \\
= \neg(\forall \pi. \text{Path } R s \pi \Rightarrow \exists i. \neg\llbracket \psi \rrbracket_M(\pi(i))) \\
= \exists \pi. \neg(\text{Path } R s \pi \Rightarrow \exists i. \neg\llbracket \psi \rrbracket_M(\pi(i))) \\
= \exists \pi. \text{Path } R s \pi \land \neg(\exists i. \neg\llbracket \psi \rrbracket_M(\pi(i))) \\
= \exists \pi. \text{Path } R s \pi \land \forall i. \neg\llbracket \psi \rrbracket_M(\pi(i)) \\
= \exists \pi. \text{Path } R s \pi \land \forall i. \llbracket \psi \rrbracket_M(\pi(i))
\]
The defined operator $A[\psi_1 W \psi_2]$

- $A[\psi_1 W \psi_2]$ is a ‘partial correctness’ version of $A[\psi_1 U \psi_2]$
- It is true at $s$ if along all $R$-paths from $s$:
  - $\psi_1$ always holds on the path, or
  - $\psi_2$ holds sometime on the path, and until it does $\psi_1$ holds

Define

$$
[A[\psi_1 W \psi_2]]_M(s) = \neg E[(\psi_1 \land \neg \psi_2) U (\neg \psi_1 \land \neg \psi_2)]_M(s) = \neg E[(\psi_1 \land \neg \psi_2) U (\neg \psi_1 \land \neg \psi_2)]_M(s) = \neg (\exists \pi. \text{Path } R s \pi)
$$

- $\land$
- $\exists i. [\neg \psi_1 \land \neg \psi_2]_M(\pi(i))$
- $\land$
- $\forall j. j < i \Rightarrow [\psi_1 \land \neg \psi_2]_M(\pi(j))$

Exercise: understand the next two slides!
A[ψ₁ W ψ₂] continued (1)

Continuing:

¬(∃π. Path R s π)
∧
∃i. [¬ψ₁ ∧ ¬ψ₂]_M(π(i)) ∧ ∀j. j < i ⇒ [[ψ₁ ∧ ¬ψ₂]_M(π(j)))]

= ∀π. ¬(Path R s π)
∧
∃i. [¬ψ₁ ∧ ¬ψ₂]_M(π(i)) ∧ ∀j. j < i ⇒ [[ψ₁ ∧ ¬ψ₂]_M(π(j)))]

= ∀π. Path R s π
⇒
¬(∃i. [¬ψ₁ ∧ ¬ψ₂]_M(π(i)) ∧ ∀j. j < i ⇒ [[ψ₁ ∧ ¬ψ₂]_M(π(j)))]

= ∀π. Path R s π
⇒
∀i. ¬[¬ψ₁ ∧ ¬ψ₂]_M(π(i)) ∨ ¬(∀j. j < i ⇒ [[ψ₁ ∧ ¬ψ₂]_M(π(j)))]
\[A[\psi_1 \mathbf{W} \psi_2] \text{ continued (2)}\]

- Continuing:

\[= \forall \pi. \text{Path } R s \pi\]
\[\Rightarrow\]
\[\forall i. \neg \llbracket \neg \psi_1 \land \neg \psi_2 \rrbracket_M(\pi(i)) \lor \neg (\forall j. j<i \Rightarrow \llbracket \psi_1 \land \neg \psi_2 \rrbracket_M(\pi(j)))\]

\[= \forall \pi. \text{Path } R s \pi\]
\[\Rightarrow\]
\[\forall i. \neg (\forall j. j<i \Rightarrow \llbracket \psi_1 \land \neg \psi_2 \rrbracket_M(\pi(j))) \lor \neg \llbracket \neg \psi_1 \land \neg \psi_2 \rrbracket_M(\pi(i))\]

\[= \forall \pi. \text{Path } R s \pi\]
\[\Rightarrow\]
\[\forall i. (\forall j. j<i \Rightarrow \llbracket \psi_1 \land \neg \psi_2 \rrbracket_M(\pi(j))) \Rightarrow \llbracket \psi_1 \lor \psi_2 \rrbracket_M(\pi(i))\]

- Exercise: explain why this is \[\llbracket A[\psi_1 \mathbf{W} \psi_2] \rrbracket_M(s)\]?

- this exercise illustrates the subtlety of writing CTL!
Sanity check: \( \mathbf{A}[\psi \mathbf{W} F] = \mathbf{AG} \psi \)

- From last slide:
  \[
  \begin{align*}
  \llbracket \mathbf{A}[\psi_1 \mathbf{W} \psi_2] \rrbracket_M(s) &= \forall \pi. \text{Path } R s \pi \\
  &\implies \forall i. (\forall j. j < i \Rightarrow \llbracket \psi_1 \land \neg \psi_2 \rrbracket_M(\pi(j))) \Rightarrow \llbracket \psi_1 \lor \psi_2 \rrbracket_M(\pi(i))
  \end{align*}
  \]

- Set \( \psi_1 \) to \( \psi \) and \( \psi_2 \) to \( F \):
  \[
  \begin{align*}
  \llbracket \mathbf{A}[\psi \mathbf{W} F] \rrbracket_M(s) &= \forall \pi. \text{Path } R s \pi \\
  &\implies \forall i. (\forall j. j < i \Rightarrow \llbracket \psi \land \neg F \rrbracket_M(\pi(j))) \Rightarrow \llbracket \psi \lor \neg F \rrbracket_M(\pi(i))
  \end{align*}
  \]

- Simplify:
  \[
  \begin{align*}
  \llbracket \mathbf{A}[\psi \mathbf{W} F] \rrbracket_M(s) &= \forall \pi. \text{Path } R s \pi \Rightarrow \forall i. (\forall j. j < i \Rightarrow \llbracket \psi \rrbracket_M(\pi(j))) \Rightarrow \llbracket \psi \rrbracket_M(\pi(i))
  \end{align*}
  \]

- By induction on \( i \):
  \[
  \llbracket \mathbf{A}[\psi \mathbf{W} F] \rrbracket_M(s) = \forall \pi. \text{Path } R s \pi \Rightarrow \forall i. \llbracket \psi \rrbracket_M(\pi(i))
  \]

- **Exercises**
  1. Describe the property: \( \mathbf{A}[\top \mathbf{W} \psi] \).
  2. Describe the property: \( \neg \mathbf{E}[\neg \psi_2 \mathbf{U} (\neg \psi_1 \lor \psi_2)] \).
  3. Define \( \mathbf{E}[\psi_1 \mathbf{W} \psi_2] = \mathbf{E}[\psi_1 \mathbf{U} \psi_2] \lor \mathbf{EG} \psi_1 \).
     Describe the property: \( \mathbf{E}[\psi_1 \mathbf{W} \psi_2] \)?
Recall model behaviour computation tree

- Atomic properties are true or false of individual states
- General properties are true or false of whole behaviour
- Behaviour of \((S, R)\) starting from \(s \in S\) as a tree:

- A path is shown in red
- Properties may look at all paths, or just a single path
  - CTL: Computation Tree Logic (all paths from a state)
  - LTL: Linear Temporal Logic (a single path)
Summary of CTL operators (primitive + defined)

- **CTL formulae:**

  - $p$ (Atomic formula - $p \in AP$)
  - $\neg \psi$ (Negation)
  - $\psi_1 \land \psi_2$ (Conjunction)
  - $\psi_1 \lor \psi_2$ (Disjunction)
  - $\psi_1 \Rightarrow \psi_2$ (Implication)
  - $\textbf{A}X\psi$ (All successors)
  - $\textbf{E}X\psi$ (Some successors)
  - $\textbf{A}F\psi$ (Somewhere – along all paths)
  - $\textbf{E}F\psi$ (Somewhere – along some path)
  - $\textbf{A}G\psi$ (Everywhere – along all paths)
  - $\textbf{E}G\psi$ (Everywhere – along some path)
  - $A[\psi_1 U \psi_2]$ (Until – along all paths)
  - $E[\psi_1 U \psi_2]$ (Until – along some path)
  - $A[\psi_1 W \psi_2]$ (Unless – along all paths)
  - $E[\psi_1 W \psi_2]$ (Unless – along some path)
Example CTL formulae

- **EF(Started ∧ ¬Ready)**
  It is possible to get to a state where Started holds but Ready does not hold.

- **AG(Req ⇒ AFAck)**
  If a request Req occurs, then it will eventually be acknowledged by Ack.

- **AG(AFDeviceEnabled)**
  DeviceEnabled is always true somewhere along every path starting anywhere: i.e. DeviceEnabled holds infinitely often along every path.

- **AG(EFRestart)**
  From any state it is possible to get to a state for which Restart holds.
  Can’t be expressed in LTL!
More CTL examples (1)

- \(\text{AG}(\text{Req} \Rightarrow \text{A}[\text{Req U Ack}])\)
  
  If a request Req occurs, then it continues to hold, until it is eventually acknowledged

- \(\text{AG}(\text{Req} \Rightarrow \text{AX}(\text{A}[\neg\text{Req U Ack}]))\)
  
  Whenever Req is true either it must become false on the next cycle and remains false until Ack, or Ack must become true on the next cycle
  
  Exercise: is the **AX** necessary?

- \(\text{AG}(\text{Req} \Rightarrow (\neg\text{Ack} \Rightarrow \text{AX}(\text{A}[\text{Req U Ack}]))))\)
  
  Whenever Req is true and Ack is false then Ack will eventually become true and until it does Req will remain true
  
  Exercise: is the **AX** necessary?
More CTL examples (2)

1. \( \text{AG}(\text{Enabled} \Rightarrow \text{AG}(\text{Start} \Rightarrow A[\neg \text{Waiting} U \text{ Ack}]))) \)
   
   If \( \text{Enabled} \) is ever true then if \( \text{Start} \) is true in any subsequent state then \( \text{Ack} \) will eventually become true, and until it does \( \text{Waiting} \) will be false.

2. \( \text{AG}(\neg \text{Req}_1 \land \neg \text{Req}_2 \Rightarrow A[\neg \text{Req}_1 \land \neg \text{Req}_2 U (\text{Start} \land \neg \text{Req}_2)]) \)
   
   Whenever \( \text{Req}_1 \) and \( \text{Req}_2 \) are false, they remain false until \( \text{Start} \) becomes true with \( \text{Req}_2 \) still false.

3. \( \text{AG}(\text{Req} \Rightarrow \text{AX}(\text{Ack} \Rightarrow \text{AF} \neg \text{Req})) \)
   
   If \( \text{Req} \) is true and \( \text{Ack} \) becomes true one cycle later, then eventually \( \text{Req} \) will become false.
Some abbreviations

- \( AX_i \psi \equiv AX(AX(\cdots(AX\psi)\cdots)) \)
  - \( i \) instances of \( AX \)
  - \( \psi \) is true on all paths \( i \) units of time later

- \( ABF_{i..j} \psi \equiv AX_i (\psi \lor AX(\psi \lor \cdots AX(\psi \lor AX\psi)\cdots)) \)
  - \( j - i \) instances of \( AX \)
  - \( \psi \) is true on all paths sometime between \( i \) units of time later and \( j \) units of time later

- \( AG(Req \Rightarrow AX(Ack_1 \land ABF_{1..6}(Ack_2 \land A[Wait U Reply]))) \)
  - One cycle after \( Req \), \( Ack_1 \) should become true,
  - and then \( Ack_2 \) becomes true 1 to 6 cycles later
  - and then eventually \( Reply \) becomes true, but until
  - it does \( Wait \) holds from the time of \( Ack_2 \)

- More abbreviations in ‘Industry Standard’ language PSL
CTL model checking

- For LTL path formulae $\phi$ recall that $M \models \phi$ is defined by:
  \[
  M \models \phi \iff \forall \pi. s \in S_0 \land \text{Path } R s \pi \Rightarrow [\phi]_M(\pi)
  \]

- For CTL state formulae $\psi$ the definition of $M \models \psi$ is:
  \[
  M \models \psi \iff \forall s. s \in S_0 \Rightarrow [\psi]_M(s)
  \]

- $M$ common; LTL, CTL formulae and semantics $[\_\_]_M$ differ

- CTL model checking algorithm:
  - compute $\{s \mid [\psi]_M(s) = \text{true}\}$ bottom up
  - check $S_0 \subseteq \{s \mid [\psi]_M(s) = \text{true}\}$
  - symbolic model checking represents these sets as BDDs
CTL model checking: $p$, $\text{AX}\psi$, $\text{EX}\psi$

- For CTL formula $\psi$ let $\{\psi\}_M = \{s \mid [\psi]_M(s) = \text{true}\}$

- When unambiguous will write $\{\psi\}$ instead of $\{\psi\}_M$

- $\{p\} = \{s \mid p \in L(s)\}$
  
  - scan through set of states $S$ marking states labelled with $p$
  - $\{p\}$ is set of marked states

- To compute $\{\text{AX}\psi\}$
  
  - recursively compute $\{\psi\}$
  - marks those states all of whose successors are in $\{\psi\}$
  - $\{\text{AX}\psi\}$ is the set of marked states

- To compute $\{\text{EX}\psi\}$
  
  - recursively compute $\{\psi\}$
  - marks those states with at least one successor in $\{\psi\}$
  - $\{\text{EX}\psi\}$ is the set of marked states
CTL model checking: $\{E[\psi_1 U \psi_2]\}, \{A[\psi_1 U \psi_2]\}$

- To compute $\{E[\psi_1 U \psi_2]\}$
  - recursively compute $\{\psi_1\}$ and $\{\psi_2\}$
  - mark all states in $\{\psi_2\}$
  - mark all states in $\{\psi_1\}$ with a successor state that is marked
  - repeat previous line until no change
  - $\{E[\psi_1 U \psi_2]\}$ is set of marked states

- More formally: $\{E[\psi_1 U \psi_2]\} = \bigcup_{n=0}^{\infty} \{E[\psi_1 U \psi_2]\}_n$ where:
  $\{E[\psi_1 U \psi_2]\}_0 = \{\psi_2\}$
  $\{E[\psi_1 U \psi_2]\}_{n+1} = \{E[\psi_1 U \psi_2]\}_n \cup \{s \in \{\psi_1\} | \exists s' \in \{E[\psi_1 U \psi_2]\}_n. R s s'\}$

- $\{A[\psi_1 U \psi_2]\}$ similar, but with a more complicated iteration
  - details omitted
Example: checking $\text{EF } p$

- $\text{EF } p = \text{E}[\text{T } \text{U } p]$
  - holds if $\psi$ holds along some path

- Note $\{\text{T}\} = S$

- Let $S_n = \{\text{E}[\text{T } \text{U } p]\}_n$ then:
  \[
  S_0 = \{\text{E}[\text{T } \text{U } p]\}_0 = \{p\} = \{s \mid p \in L(s)\}
  \]
  \[
  S_{n+1} = S_n \cup \{s \in \{\text{T}\} \mid \exists s' \in \{\text{E}[\text{T } \text{U } p]\}_n. R s s'\}
  \]
  \[
  = S_n \cup \{s \mid \exists s' \in S_n. R s s'\}
  \]
  - mark all the states labelled with $p$
  - mark all with at least one marked successor
  - repeat until no change
  - $\{\text{EF } p\}$ is set of marked states
Example: RCV

- Recall the handshake circuit:

- State represented by a triple of Booleans \((dreq, q0, dack)\)

- A model of \(RCV\) is \(M_{RCV}\) where:

\[
M = (S_{RCV}, S_{0_{RCV}}, R_{RCV}, L_{RCV})
\]

and

\[
R_{RCV} (dreq, q0, dack) (dreq', q0', dack') = (q0' = dreq) \land (dack' = (dreq \land (q0 \lor dack)))
\]
Possible states for RCV:
\{000, 001, 010, 011, 100, 101, 110, 111\}
where $b_2 b_1 b_0$ denotes state
\[\text{dreq} = b_2 \land \text{q0} = b_1 \land \text{dack} = b_0\]
Computing \( \{\text{EF } \text{At111}\} \) where \( \text{At111} \in L_{RCV}(s) \Leftrightarrow s = 111 \)

Define:

\[
S_0 = \{s \mid \text{At111} \in L_{RCV}(s)\} = \{s \mid s = 111\} = \{111\}
\]

\[
S_{n+1} = S_n \cup \{s \mid \exists s' \in S_n. \mathcal{R}(s, s')\} = S_n \cup \{b_2b_1b_0 \mid \exists b'_2b'_1b'_0 \in S_n. (b'_1 = b_2) \land (b'_0 = b_2 \land (b_1 \lor b_0))\}
\]
Computing $\{EF_{At111}\}$ (continued)

- **Compute:**
  
  $S_0 = \{111\}$
  
  $S_1 = \{111\} \cup \{101, 110\}$
  
  $S_1 = \{111, 101, 110\}$
  
  $S_2 = \{111, 101, 110\} \cup \{100\}$
  
  $S_2 = \{111, 101, 110, 100\}$
  
  $S_3 = \{111, 101, 110, 100\} \cup \{000, 001, 010, 011\}$
  
  $S_3 = \{111, 101, 110, 100, 000, 001, 010, 011\}$
  
  $S_n = S_3$ for $n > 3$
  
  $\{EF_{At111}\} = \mathbb{B}^3 = S_{RCV}$
  
  $M_{RCV} \models EF_{At111} \iff S_{0_{RCV}} \subseteq S$
Symbolic model checking

- Represent sets of states with BDDs
- Represent Transition relation with a BDD
- If BDDs of $\{\psi\}$, $\{\psi_1\}$, $\{\psi_2\}$ are known, then:
  - BDDs of $\{\neg\psi\}$, $\{\psi_1 \land \psi_2\}$, $\{\psi_1 \lor \psi_2\}$, $\{\psi_1 \Rightarrow \psi_2\}$ computed using standard BDD algorithms
  - BDDs of $\{AX\psi\}$, $\{EX\psi\}$, $\{A[\psi_1 U \psi_2]\}$, $\{E[\psi_1 U \psi_2]\}$ computed using straightforward algorithms (see textbooks)
- Model checking CTL generalises reachable states Iteration
History of Model checking

- CTL model checking due to Emerson, Clarke & Sifakis
- Symbolic model checking due to several people:
  - Clarke & McMillan (idea usually credited to McMillan’s PhD)
  - Coudert, Berthet & Madre
  - Pixley
- SMV (McMillan) is a popular symbolic model checker:
  - [http://www.cs.cmu.edu/~modelcheck/smv.html](http://www.cs.cmu.edu/~modelcheck/smv.html) (original)
  - [http://nusmv.irst.itc.it/](http://nusmv.irst.itc.it/) (new implementation)
- Other temporal logics
  - CTL*: combines CTL and LTL
  - Engineer friendly industrial languages: PSL, SVA
Expressibility of CTL

Consider the property

“on every path there is a point after which $p$ is always true on that path”

Consider

\[((\star) \text{ non-deterministically chooses } T \text{ or } F)\]

\[
\begin{array}{l}
0: \ P := 1; \\
s0 \ 1: \ \text{WHILE} \ (\star) \ \text{DO} \ \text{SKIP}; \\
s1 \ 2: \ P := 0; \\
s2 \ 3: \ P := 1; \\
4: \ \text{WHILE} \ T \ \text{DO} \ \text{SKIP}; \\
5: 
\end{array}
\]

Property true, but cannot be expressed in CTL

- would need something like $\text{AF}\psi$
- where $\psi$ is something like “property $p$ true from now on”
- but in CTL $\psi$ must start with a path quantifier $A$ or $E$
- cannot talk about current path, only about all or some paths
- $\text{AF}(\text{AG} \ p)$ is false (consider path $s0 s0 s0 \cdots$)
LTL can express things CTL can’t

- Recall:
  \[
  \begin{align*}
  \sem{F\phi}_M(\pi) &= \exists i. \sem{\phi}_{M(\pi \downarrow i)} \\
  \sem{G\phi}_M(\pi) &= \forall i. \sem{\phi}_{M(\pi \downarrow i)}
  \end{align*}
  \]

- \(FG\phi\) is true if there is a point after which \(\phi\) is always true
  \[
  \sem{FG\phi}_M(\pi) = \sem{F(G(\phi))}_M(\pi) = \exists m_1. \sem{G(\phi)}_{M(\pi \downarrow m_1)}
  = \exists m_1. \forall m_2. \sem{\phi}_{M((\pi \downarrow m_1) \downarrow m_2)}
  = \exists m_1. \forall m_2. \sem{\phi}_{M(\pi \downarrow (m_1 + m_2))}
  \]

- LTL can express things that CTL can’t express

- Note: it’s tricky to prove CTL can’t express \(FG\phi\)
CTL can express things that LTL can’t express

- \( \text{AG}(\text{EF } p) \) says:
  
  “from every state it is possible to get to a state for which \( p \) holds”

- Can’t say this in LTL (easy proof given earlier)

- Consider disjunction:
  
  “along every path there is a state from which \( p \) will hold forever
  or
  from every state it is possible to get to a state for which \( p \) holds”

- Can’t say this in either CTL or LTL!

- CTL* combines CTL and LTL and can express this property
Both state formulae ($\psi$) and path formulae ($\phi$)

- state formulae $\psi$ are true of a state $s$ like CTL
- path formulae $\phi$ are true of a path $\pi$ like LTL

Defined mutually recursively

$$\begin{align*}
\psi & ::= p \quad \text{(Atomic formula)} \\
& | \neg \psi \quad \text{(Negation)} \\
& | \psi_1 \lor \psi_2 \quad \text{(Disjunction)} \\
& | A\phi \quad \text{(All paths)} \\
& | E\phi \quad \text{(Some paths)} \\
\phi & ::= \psi \quad \text{(Every state formula is a path formula)} \\
& | \neg \phi \quad \text{(Negation)} \\
& | \phi_1 \lor \phi_2 \quad \text{(Disjunction)} \\
& | X\phi \quad \text{(Successor)} \\
& | F\phi \quad \text{(Sometimes)} \\
& | G\phi \quad \text{(Always)} \\
& | [\phi_1 U \phi_2] \quad \text{(Until)}
\end{align*}$$

- CTL is CTL* with $X$, $F$, $G$, $[\neg U \neg]$ preceded by $A$ or $E$
- LTL consists of CTL* formulae of form $A\phi$, where the only state formulae in $\phi$ are atomic
CTL* semantics

- Combines CTL state semantics with LTL path semantics:

\[
\begin{align*}
\lbrack p \rbrack_M(s) & = p \in L(s) \\
\lbrack \neg \psi \rbrack_M(s) & = \neg (\lbrack \psi \rbrack_M(s)) \\
\lbrack \psi_1 \lor \psi_2 \rbrack_M(s) & = \lbrack \psi_1 \rbrack_M(s) \lor \lbrack \psi_2 \rbrack_M(s) \\
\lbrack A\phi \rbrack_M(s) & = \forall \pi. \text{Path } R s \pi \Rightarrow \phi(\pi) \\
\lbrack E\phi \rbrack_M(s) & = \exists \pi. \text{Path } R s \pi \land \lbrack \phi \rbrack_M(\pi) \\
\lbrack \psi \rbrack_M(\pi) & = \lbrack \psi \rbrack_M(\pi(0)) \\
\lbrack \neg \phi \rbrack_M(\pi) & = \neg (\lbrack \phi \rbrack_M(\pi)) \\
\lbrack \phi_1 \lor \phi_2 \rbrack_M(\pi) & = \lbrack \phi_1 \rbrack_M(\pi) \lor \lbrack \phi_2 \rbrack_M(\pi) \\
\lbrack X\phi \rbrack_M(\pi) & = \lbrack \phi \rbrack_M(\pi \downarrow 1) \\
\lbrack F\phi \rbrack_M(\pi) & = \exists m. \lbrack \phi \rbrack_M(\pi \downarrow m) \\
\lbrack G\phi \rbrack_M(\pi) & = \forall m. \lbrack \phi \rbrack_M(\pi \downarrow m) \\
\lbrack [\phi_1 U \phi_2] \rbrack_M(\pi) & = \exists i. \lbrack \phi_2 \rbrack_M(\pi \downarrow i) \land \forall j. j < i \Rightarrow \lbrack \phi_1 \rbrack_M(\pi \downarrow j)
\end{align*}
\]

- Note $\lbrack \psi \rbrack_M : S \rightarrow \mathbb{B}$ and $\lbrack \phi \rbrack_M : (\mathbb{N} \rightarrow S) \rightarrow \mathbb{B}$
LTL and CTL as CTL*

- As usual: $M = (S, S_0, R, L)$
- If $\psi$ is a CTL* state formula: $M \models \psi \iff \forall s \in S_0. [\psi]_M(s)$
- If $\phi$ is an LTL path formula then: $M \models_{\text{LTL}} \phi \iff M \models_{\text{CTL}^*} A\phi$
- If $R$ is total ($\forall s. \exists s'. R s s'$) then (exercise):
  $\forall s s'. R s s' \iff \exists \pi. \text{Path } R s \pi \land (\pi(1) = s')$
- The meanings of CTL formulae are the same in CTL*

\[
\begin{align*}
[\mathbf{A}(\mathbf{X}\psi)]_M(s) &= \forall \pi. \text{Path } R s \pi \Rightarrow [\mathbf{X}\psi]_M(\pi) \\
&= \forall \pi. \text{Path } R s \pi \Rightarrow [\psi]_M(\pi(1)) \\
&= \forall \pi. \text{Path } R s \pi \Rightarrow [\psi]_M((\pi(1)(0))) \\
&= \forall \pi. \text{Path } R s \pi \Rightarrow [\psi]_M(\pi(1))
\end{align*}
\]

\[
\begin{align*}
[\mathbf{AX}\psi]_M(s) &= \forall s'. R s s' \Rightarrow [\psi]_M(s') \\
&= \forall s'. (\exists \pi. \text{Path } R s \pi \land (\pi(1) = s')) \Rightarrow [\psi]_M(s') \\
&= \forall s'. \forall \pi. \text{Path } R s \pi \land (\pi(1) = s') \Rightarrow [\psi]_M(s') \\
&= \forall \pi. \text{Path } R s \pi \Rightarrow [\psi]_M(\pi(1))
\end{align*}
\]

Exercise: do similar proofs for other CTL formulae
Fairness

- May want to assume system or environment is ‘fair’

- Example 1: fair arbiter
  - the arbiter doesn’t ignore one of its requests forever
    - not every request need be granted
    - want to exclude infinite number of requests and no grant

- Example 2: reliable channel
  - no message continuously transmitted but never received
    - not every message need be received
    - want to exclude an infinite number of sends and no receive
Handling fairness in CTL and LTL

- Consider: $p$ holds infinitely often along a path then so does $q$

- In LTL is expressible as $G(F \ p) \Rightarrow G(F \ q)$

- Can’t say this in CTL
  - why not – what’s wrong with $AG(AF \ p) \Rightarrow AG(AF \ q)$?
  - in CTL* expressible as $A(G(F \ p) \Rightarrow G(F \ q))$
  - fair CTL model checking implemented in checking algorithm
  - fair LTL just a fairness assumption like $G(F \ p) \Rightarrow \cdots$

- Fairness is a tricky and subtle subject
  - many kinds of fairness: ‘weak fairness’, ‘strong fairness’ etc
  - exist whole books on fairness
Propositional modal $\mu$-calculus

- You may learn this in *Topics in Concurrency*

- $\mu$-calculus is an even more powerful property language
  - has fixed-point operators
  - both maximal and minimal fixed points
  - model checking consists of calculating fixed points
  - many logics (e.g. CTL*) can be translated into $\mu$-calculus

- Strictly stronger than CTL*
  - expressibility strictly increases as allowed nesting increases
  - need fixed point operators nested 2 deep for CTL*

- The $\mu$-calculus is *very* non-intuitive to use!
  - intermediate code rather than a practical property language
  - nice meta-theory and algorithms, but terrible usability!
SEREs: Sequential Extended Regular Expressions

- SEREs are from the industrial PSL (more on PSL later)

**Syntax:**

\[
\begin{align*}
r &::= p \quad \text{(Atomic formula } p \in AP) \\
& | !p \quad \text{(Negated atomic formula } p \in AP) \\
& | r_1 | r_2 \quad \text{(Disjunction)} \\
& | r_1 \& r_2 \quad \text{(Conjunction)} \\
& | r_1 ; r_2 \quad \text{(Concatenation)} \\
& | r_1 : r_2 \quad \text{(Fusion)} \\
& | r[*] \quad \text{(Repeat)}
\end{align*}
\]

**Semantics:**

\( w \) ranges over finite lists of states \( s; |w| \) is length of \( w; w_1 . w_2 \) is concatenation; head \( w \) is head; \( \langle \rangle \) is empty word

\[
\begin{align*}
[p](w) &= p \in L(\text{head } w) \land |w| = 1 \\
[!p](w) &= \neg(p \in L(\text{head } w)) \land |w| = 1 \\
[r_1 | r_2](w) &= [r_1](w) \lor [r_2](w) \\
[r_1 \& r_2](w) &= [r_1](w) \land [r_2](w) \\
[r_1 ; r_2](w) &= \exists w_1 . w_2 . w = w_1 . w_2 \land [r_1](w_1) \land [r_2](w_2) \\
[r_1 : r_2](w) &= \exists w_1 . s . w_2 . w = w_1 . s . w_2 \land [r_1](w_1 . s) \land [r_2](s . w_2) \\
[r[*]](w) &= w = \langle \rangle \lor \exists w_1 . \cdots . w_l . w = w_1 . \cdots . w_l \land [r](w_1) \land \cdots \land [r](w_l)
\end{align*}
\]
Example SERE

Example

A sequence in which req is asserted, followed four cycles later by an assertion of grant, followed by a cycle in which abortin is not asserted.

Define $p[\ast 3] = p;p;p$

Then the example above can be represented by the SERE:

$$\text{req};\text{T[}\ast 3\text{]};\text{grant};!\text{abortin}$$

In PSL this could be written as:

$$\text{req};[\ast 3];\text{grant};!\text{abortin}$$

where $[\ast 3]$ abbreviates $\text{T[}\ast 3\text{]}$

more ‘syntactic sugar’ later

e.g. true, false for T, F
Assertion-Based Verification (ABV)

- It has been claimed that assertion based verification:
  “is likely to be the next revolution in hardware design verification”

- Basic idea:
  - document designs with formal properties
  - use simulation (dynamic) and model checking (static)

- Problem: too many languages
  - academic logics: LTL, CTL
  - tool-specific industrial versions:
    Intel, Cadence, Motorola, IBM, Synopsys

- What to do? Solution: a competition!
  - run by Accellera organisation
  - results standardised by IEEE
  - lots of politics
IBM’s *Sugar* and Accellera’s PSL

- **Sugar 1**: property language of IBM RuleBase checker
  - CTL plus *Sugar* Extended Regular Expressions (SEREs)
- Competition finalists: IBM’s *Sugar 2* and Motorola’s *CBV*
  - Intel/Synopsys ForSpec eliminated earlier (apparently industry politics involved)
- **Sugar 2** is based on LTL rather than CTL
  - has CTL constructs: “Optional Branching Extension” (OBE)
  - has clocking constructs for temporal abstraction
- Accellera purged “Sugar” from it property language
  - the word “Sugar” was too associated with IBM
  - language renamed to PSL
  - SEREs now *Sequential Extended Regular Expressions*
- Lobbying to make PSL more like ForSpec (align with SVA)
PSL Foundation Language (FL is LTL + SEREs)

Syntax:

\[
\begin{align*}
f & ::= p & \text{(Atomic formula - } p \in AP) \\
     & | !f & \text{(Negation)} \\
     & | f_1 \text{ or } f_2 & \text{(Disjunction)} \\
     & | \text{next } f & \text{(Successor)} \\
     & | \{r\}(f) & \text{(Suffix implication: } r \text{ a SERE)} \\
     & | \{r_1\} |\rightarrow \{r_2\} & \text{(Suffix next implication: } r_1, r_2 \text{ SEREs)} \\
     & | [f_1 \text{ until } f_2] & \text{(Until)}
\end{align*}
\]

Semantics (omits clocking, weak/strong distinction)

\[
\begin{align*}
[p]_M(\pi) &= p \in L(\pi(0)) \\
[!f]_M(\pi) &= \neg([f]_M(\pi)) \\
[f_1 \text{ or } f_2]_M(\pi) &= [f_1]_M(\pi) \lor [f_2]_M(\pi) \\
[\text{next } f]_M(\pi) &= [f]_M(\pi\downarrow 1) \\
[\{r\}(f)]_M(\pi) &= \forall \pi' w. (\pi = w.\pi' \land [r]_M(w)) \Rightarrow [f]_M(\pi') \\
[\{r_1\} |\rightarrow \{r_2\}]_M(\pi) &= \forall \pi' w_1 s. (\pi = w_1.s.\pi' \land [r_1]_M(w_1.s)) \\
& \quad \Rightarrow \exists \pi'' w_2. \pi' = w_2.\pi'' \land [r_2]_M(s.w_2) \\
[[f_1 \text{ until } f_2]]_M(\pi) &= \exists i. [f_2]_M(\pi\downarrow i) \land \forall j. j < i \Rightarrow [f_1]_M(\pi\downarrow j)
\end{align*}
\]

There is also an Optional Branching Extension (OBE)

- completely standard CTL: EX, E[\text{--- \text{U \text{---}}}], EG etc.
Combining SEREs with LTL formulae

- Formula \( \{r\}f \) means LTL formula \( f \) true after SERE \( r \)

- Example

  \( \text{After a sequence in which req is asserted, followed four cycles later by an assertion of grant, followed by a cycle in which abortin is not asserted, we expect to see an assertion of ack some time in the future.} \)

- Can represent by
  \[ \text{always} \ {\text{req;[}^*3{]};\text{grant;!abortin}}(\text{eventually} \ \text{ack}) \]

  where \( \text{eventually} \) and \( \text{always} \) are defined by:

  \[
  \text{eventually} \ f = [\text{true until} \ f] \\
  \text{always} \ f = !([\text{eventually} !f])
  \]

- N.B. Ignoring strong/weak distinction
  - strong/weak distinction important for dynamic checking
  - semantics when simulator halts before expected event
  - strictly should write \text{until!}, \text{eventually}!
SERE examples

- How can we modify

  \[
  \text{always reqin;ackout;!abortin } \rightarrow \text{ ackin;ackin}
  \]

  so that the two cycles of ackin start the cycle after !abortin

- Two ways of doing this

  \[
  \text{always\{reqin;ackout;!abortin\} } \rightarrow \text{\{true;ackin;ackin\}}
  \]

  \[
  \text{always\{reqin;ackout;!abortin\} } \Rightarrow \text{\{ackin;ackin\}}
  \]

- \( \Rightarrow \) is a defined operator

  \[
  \text{\{r1\}} \Rightarrow \text{\{r2\}} = \text{\{r1\}} \rightarrow \text{\{true;r2\}}
  \]

- Note: true and T are synonyms
Examples of defined notations: consecutive repetition

- Define
  
  \[ r[+] = r; r[*] \]
  
  \[ \text{false}[*] \text{ if } i=0 \]
  
  \[ r[*i] = | \]
  
  \[ r; \ldots; r \text{ otherwise (i repetitions)} \]
  
  \[ r[*i..j] = r[*i] \mid r[*](i+1)] \mid \ldots \mid r[*j] \]
  
  \[ [+]= \text{true}[+] \]
  
  \[ [\ast]= \text{true}[*] \]

- Example

Whenever we have a sequence of \text{req} followed by \text{ack}, we should see a full transaction starting the following cycle. A full transaction starts with an assertion of the signal \text{start\_trans}, followed by one to eight consecutive data transfers, followed by the assertion of signal \text{end\_trans}. A data transfer is indicated by the assertion of signal \text{data}.

\[
\text{always\{req;ack\}|=>\{start\_trans;data[*1..8];end\_trans\}}
\]
Fixed number of non-consecutive repetitions

Example

Whenever we have a sequence of \texttt{req} followed by \texttt{ack}, we should see a full transaction starting the following cycle. A full transaction starts with an assertion of the signal \texttt{start\_trans}, followed by eight not necessarily consecutive data transfers, followed by the assertion of signal \texttt{end\_trans}. A data transfer is indicated by the assertion of signal \texttt{data}.

Can represent by

\begin{verbatim}
always
{req;ack} |=>
{start_trans;
{{!data[*];data}[*8];!data[*]}};
end_trans
\end{verbatim}

Define: \texttt{b[i] = {!b[*];b}[*i];!b[*]}

Then have a nicer representation

\begin{verbatim}
always{req;ack} |=>{start_trans;data[= 8];end_trans}
\end{verbatim}
Variable number of non-consecutive repetitions

- Example

  Whenever we have a sequence of $req$ followed by $ack$, we should see a full transaction starting the following cycle. A full transaction starts with an assertion of the signal $start\_trans$, followed by one to eight not necessarily consecutive data transfers, followed by the assertion of signal $end\_trans$. A data transfer is indicated by the assertion of signal $data$.

- Define

  \[
  b[= i..j] = \{b[= i]\} \mid \{b[= (i+1)]\} \mid \ldots \mid \{b[= j]\}
  \]

- Then

  \[
  \text{always } \{req;ack\} \implies \\
  \{start\_trans;data[= 1..8];end\_trans\}
  \]

- These examples are meant to illustrate how PSL/Sugar is much more readable than raw CTL or LTL.
Clocking

- Basic idea: $b@clk$ samples $b$ on rising edges of $clk$
- Can clock SEREs ($r@clk$) and formulae ($f@clk$)
- Can have several clocks
- Official semantics messy due to clocking
- Can ‘translate away’ clocks by pushing $@clk$ inwards
  - rules given in PSL manual
  - roughly: $b@clk \rightarrow \{!clk[*];clk \land b\}$
Model checking PSL (outline)

- SEREs checked by generating a finite automaton
  - recognise regular expressions
  - these automata are called “satellites”
- FL checked using standard LTL methods
- OBE checked by standard CTL methods
- Can also check formula for runs of a simulator
  - this is dynamic verification
  - semantics handles possibility of finite paths – messy!
- Commercial checkers only handle a subset of PSL
PSL layer structure

- **Boolean layer** has atomic predicates
- **Temporal layer** has LTL (FL) and CTL (OBE) properties
- **Verification layer** has commands for how to use properties
  - e.g. `assert`, `assume`
    ```
    assert always (!en1 & en2))
    | | |
    | | ------------ Boolean layer
    | |
    | ----------------- temporal layer
    | |
    |------------------- verification layer
    ```

- **Modelling layer**: HDL specification of e.g. inputs, checkers
  - e.g. augment `always(Req  ->  eventually! Ack)`
  - add counter to keep track of numbers of Req and Ack
PSL/Sugar summary

- Combines together LTL and CTL
- Regular expressions – SEREs
- LTL – Foundation Language formulae
- CTL – Optional Branching Extension
- Relatively simple set of primitives + definitional extension
- Boolean, temporal, verification, modelling layers
- Semantics for static and dynamic verification (needs strong/weak distinction)
Simulation semantics (a.k.a. event semantics)

- HDLs use discrete event simulation
  - changes to variables ⇒ threads enabled
  - enabled threads executed non-deterministically
  - execution of threads ⇒ more events

- Combinational thread:
  \[
  \text{always } @ (v_1 \text{ or } \cdots \text{ or } v_n) \quad v := E
  \]
  - enabled by any change to \( v_1, \ldots, v_n \)

- Positive edge triggered sequential threads:
  \[
  \text{always } @(\text{posedge } clk) \quad v := E
  \]
  - enabled by \( clk \) changing to \( T \)

- Negative edge triggered sequential threads:
  \[
  \text{always } @(\text{negedge } clk) \quad v := E
  \]
  - enabled by \( clk \) changing to \( F \)
Simulation

- Given
  - a set of threads
  - initial values for variables read or written by threads
  - a sequence of input values
    (inputs are variables not in LHS of assignments)

- simulation algorithm $\Rightarrow$ a sequence of states

- Simulation is non-deterministic
Combinational threads in series

\[
\begin{array}{c}
\text{in} \quad \rightarrow \ f \quad \rightarrow \ g \quad \rightarrow \ h \quad \rightarrow \ \text{out}
\end{array}
\]

- HDL-like specification:
  
  \[
  \begin{align*}
  \text{always} @ (\text{in}) & \quad l_1 := f(\text{in}) \quad \quad \text{................. thread T1} \\
  \text{always} @ (l_1) & \quad l_2 := g(l_1) \quad \quad \text{................. thread T2} \\
  \text{always} @ (l_2) & \quad \text{out} := h(l_2) \quad \quad \text{................. thread T3}
  \end{align*}
  \]

- Suppose \text{in} changes to \( x \) at simulation time \( t \)
  
  \begin{itemize}
    \item T1 will become enabled and assign \( f(x) \) to \( l_1 \)
    \item if \( l_1 \)'s value changes then T2 will become enabled (still simulation time \( t \))
    \item T2 will assign \( g(f(x)) \) to \( l_2 \)
    \item if \( l_2 \)'s value changes then T will become enabled (still simulation time \( t \))
    \item T3 will assign \( h(g(f(x))) \) to \( \text{out} \)
    \item simulation quiences (still simulation time \( t \))
  \end{itemize}

- Steps at same simulation time happen in “\( \delta\)-time” (VHDL jargon)
Semantic gap

- Designers use HDLs and verify via simulation
  - event semantics
- Formal verifiers use logic and verify via proof
  - path semantics
- Problem: do path and simulation semantics agree?
- Would like:
  
  paths = sequences of quiescent simulation states
Consider two Dtypes in series:

\[
\text{always } @(\text{posedge } clk) \ l := \ in \\
\text{always } @(\text{posedge } clk) \ out := \ l
\]

If \text{posedge} \ clk:

- both threads become enabled
- race condition

Right thread executed first:

- \text{out} gets previous value of \( l \)
- then left thread executed
- so \( l \) gets value input at \( \text{in} \)

Left thread executed first:

- \( l \) gets input value at \( \text{in} \)
- then right thread executed
- so \text{out} gets input value at \( \text{in} \)
Sequential threads – path semantics

- **Trace semantics:**
  
  ```
  in  aaaaaaaaaabbbbbbbccccccdddddddddddd . . . . . . .
  clk  00000111110000011111000001111100 . . . . . . .
  l   eeeeeeaaaaaaaaabbbbbbbbbdddddddddd . . . . . . .
  out ffffeeeeeeaaaaaaaaabbbbbbb . . . . . . .
  ```

- Corresponds to right thread executed first
- How to ensure event and path semantics agree?
  - **Method 1:** use non-blocking assignments:
    ```
    always @(posedge clk) l <= in;
    always @(posedge clk) out <= l;
    ```
    - non-blocking assignments (<=) in Verilog
    - RHS of all non-blocking assignments first computed
    - assignments done at end of simulation cycle
  - **Method 2:** make simulation cycle VHDL-like
Verilog versus VHDL simulation cycles

- **Verilog-like simulation cycle:**
  1. Choose an enabled thread
  2. Execute the chosen thread
  3. Fire event controls to enable new threads
  4. Execute until quiescent
  5. Advance simulation time

- **VHDL-like simulation cycle:**
  1. Execute all enabled threads in parallel
  2. Fire event controls to enable new threads
  3. Execute until quiescent
  4. Advance simulation time
Recall HDL:

\[
\begin{align*}
\text{always @ (posedge } clk \text{) } l & := in \\
\text{always @ (posedge } clk \text{) } out & := l
\end{align*}
\]

If \textit{posedge} \textit{clk}:

- both threads become enabled

VHDL semantics:

- both threads executed in parallel
- \textit{out} gets previous value of \textit{l}
- in parallel \textit{l} gets value input at \textit{in}

Now no race

Event semantics matches path semantics
Summary of dynamic versus static semantics

- Simulation (event) semantics different from path semantics
- No standard event semantics (Verilog versus VHDL)
- Verilog: need non-blocking assignments
- VHDL semantics closer path semantics
- Simulations are finite traces: better fit with LTL than CTL
Bisimulation equivalence: general idea

- $M$, $M'$ **bisimilar** if they have ‘corresponding executions’
  - to each step of $M$ there is a corresponding step of $M'$
  - to each step of $M'$ there is a corresponding step of $M$

- Bisimilar models satisfy same CTL* properties
- Bisimilar: same truth/falsity of model properties
- **Simulation** gives property-truth preserving abstraction (see later)
Let $R : S \to S \to B$ and $R' : S' \to S' \to B$ be transition relations.

$B$ is a bisimulation relation between $R$ and $R'$ if:

$B : S \to S' \to B$

1. $\forall s s'. B s s' \Rightarrow \forall s_1 \in S. R s s_1 \Rightarrow \exists s'_1. R' s' s'_1 \land B s_1 s'_1$
   (to each step of $R$ there is a corresponding step of $R'$)

2. $\forall s s'. B s s' \Rightarrow \forall s'_1 \in S. R' s' s'_1 \Rightarrow \exists s_1. R' s s_1 \land B s_1 s'_1$
   (to each step of $R'$ there is a corresponding step of $R$)
Bisimulation equivalence: definition and theorem

Let $M = (S, S_0, R, L)$ and $M' = (S', S'_0, R', L')$

$M \equiv M'$ if:

- there is a bisimulation $B$ between $R$ and $R'$
- $\forall s_0 \in S_0. \exists s'_0 \in S'_0. B s_0 s'_0$
- $\forall s'_0 \in S'_0. \exists s_0 \in S_0. B s_0 s'_0$
- there is a bijection $\theta : AP \rightarrow AP'$
- $\forall s s'. B s s' \Rightarrow L(s) = L'(s')$

Theorem: if $M \equiv M'$ then for any CTL* state formula $\psi$:
$M \models \psi \iff M' \models \psi$

See Q14 in the Exercises
Abstraction

- Abstraction creates a simplification of a model
  - separate states may get merged
  - an abstract path can represent several concrete paths

- $M \preceq \overline{M}$ means $\overline{M}$ is an abstraction of $M$
  - to each step of $M$ there is a corresponding step of $\overline{M}$
  - atomic properties of $M$ correspond to atomic properties of $\overline{M}$

- Special case is when $\overline{M}$ is a subset of $M$ such that:

  - $\overline{M} = (\overline{S_0}, \overline{S}, \overline{R}, \overline{L})$ and $M = (S_0, S, R, L)$
  - $\overline{S} \subseteq S$
  - $\overline{S_0} = S_0$
  - $\forall s, s' \in \overline{S}. \overline{R} s s' \iff R s s'$
  - $\forall s \in \overline{S}. \overline{L} s = L s$

  - $\overline{S}$ contain all reachable states of $M$
  - $\forall s \in \overline{S}. \forall s' \in S. R s s' \Rightarrow s' \in \overline{S}$

- All paths of $M$ from initial states are $\overline{M}$-paths
  - hence for all CTL formulas $\psi$: $\overline{M} \models \psi \Rightarrow M \models \psi$
Recall JM1

<table>
<thead>
<tr>
<th>Thread 1</th>
<th>Thread 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
<td>0: IF LOCK=0 THEN LOCK:=1;</td>
</tr>
<tr>
<td>1: X:=1;</td>
<td>1: X:=2;</td>
</tr>
<tr>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
<td>2: IF LOCK=1 THEN LOCK:=0;</td>
</tr>
<tr>
<td>3:</td>
<td></td>
</tr>
</tbody>
</table>

◮ Two program counters, state: \((pc_1, pc_2, lock, x)\)

\[
S_{JM1} = [0..3] \times [0..3] \times \mathbb{Z} \times \mathbb{Z}
\]

\[
R_{JM1}(0, pc_2, 0, x) \quad (1, pc_2, 1, x) \quad R_{JM1}(pc_1, 0, 0, x) \quad (pc_1, 1, 1, x)
\]

\[
R_{JM1}(1, pc_2, lock, x) \quad (2, pc_2, lock, 1) \quad R_{JM1}(pc_1, 1, lock, x) \quad (pc_1, 2, lock, 2)
\]

\[
R_{JM1}(2, pc_2, 1, x) \quad (3, pc_2, 0, x) \quad R_{JM1}(pc_1, 2, 1, x) \quad (pc_1, 3, 0, x)
\]

◮ Assume \(\text{NotAt}11 \in L_{JM1}(pc_1, pc_2, lock, x) \iff \neg((pc_1 = 1) \wedge (pc_2 = 1))\)

◮ Model \(M_{JM1} = (S_{JM1}, \{(0, 0, 0, 0)\}, R_{JM1}, L_{JM1})\)

◮ \(S_{JM1}\) not finite, but actually \(lock \in \{0, 1\}, x \in \{0, 1, 2\}\)

◮ Clear by inspection that \(M_{JM1} \preceq \overline{M}_{JM1}\) where:

\[
\overline{M}_{JM1} = (\overline{S}_{JM1}, \{(0, 0, 0, 0)\}, \overline{R}_{JM1}, \overline{L}_{JM1})
\]

◮ \(\overline{S}_{JM1} = [0..3] \times [0..3] \times [0..1] \times [0..3]\)

◮ \(\overline{R}_{JM1}\) is \(R_{JM1}\) restricted to arguments from \(\overline{S}_{JM1}\)

◮ \(\text{NotAt}11 \in \overline{L}_{JM1}(pc_1, pc_2, lock, x) \iff \neg((pc_1 = 1) \wedge (pc_2 = 1))\)

◮ \(\overline{L}_{JM1}\) is \(L_{JM1}\) restricted to arguments from \(\overline{S}_{JM1}\)
Simulation relations

- Let $R : S \rightarrow S \rightarrow \mathbb{B}$ and $\overline{R} : \overline{S} \rightarrow \overline{S} \rightarrow \mathbb{B}$ be transition relations.

- $H$ is a simulation relation between $R$ and $\overline{R}$ if:
  - $H$ is a relation between $S$ and $\overline{S}$ – i.e. $H : S \rightarrow \overline{S} \rightarrow \mathbb{B}$
  - to each step of $R$ there is a corresponding step of $\overline{R}$ – i.e.:
    \[
    \forall s \overline{s}. H s \overline{s} \Rightarrow \forall s' \in S. R s s' \Rightarrow \exists \overline{s}' \in \overline{S}. \overline{R} \overline{s} \overline{s}' \wedge H s' \overline{s}'
    \]

- Also need to consider abstraction of atomic properties
  - $H_{AP} : AP \rightarrow \overline{AP} \rightarrow \mathbb{B}$
  - details glossed over here
Simulation preorder: definition and theorem

- Let $M = (S, S_0, R, L)$ and $\overline{M} = (\overline{S}, \overline{S_0}, \overline{R}, \overline{L})$

- $M \preceq \overline{M}$ if:
  - there is a simulation $H$ between $R$ and $\overline{R}$
  - $\forall s_0 \in S_0. \ \exists \overline{s_0} \in \overline{S_0}. \ H \ s_0 \ \overline{s_0}$
  - $\forall s \ \overline{s}. \ \overline{H} \ s \ \overline{s} \ \Rightarrow \ L(s) = \overline{L}(\overline{s})$

- ACTL is the subset of CTL without E-properties
  - e.g. $\text{AG AF}p$ – from anywhere can always reach a $p$-state

- Theorem: if $M \preceq \overline{M}$ then for any ACTL state formula $\psi$:
  - $\overline{M} \models \psi \ \Rightarrow \ M \models \psi$

- If $\overline{M} \models \psi$ fails then cannot conclude $M \models \psi$ false
Example (Grumberg)

\[
H \text{ a simulation}
\]

\[
H \ RED \ STOP \ \land
H \ YELLOW \ GO \ \land
H \ GREEN \ GO
\]

\[
H_{AP} : \{r, y, g\} \rightarrow \{r, yg\} \rightarrow \Box
\]

\[
H_{AP} \ r \ r \ \land
H_{AP} \ y \ yg \ \land
H_{AP} \ g \ yg
\]

\[
\overline{M} \models AG \ AF \ \neg r \ \text{hence} \ M \models AG \ AF \ \neg r
\]

\[
\neg (\overline{M} \models AG \ AF \ r) \ \text{doesn’t entail} \ \neg (M \models AG \ AF \ r)
\]

\[
\neg [AG \ AF \ r]_{\overline{M}}(STOP) \ \text{is false}
\]

\[
\text{(consider } \overline{M}-\text{path } \pi' \ \text{where } \pi' = \text{STOP.GO.GO.GO.} \ldots )
\]

\[
[AG \ AF \ r]_{M}(RED) \ \text{is true}
\]

\[
\text{(abstract path } \pi' \ \text{doesn’t correspond to a real path in } M)
\]
- **Counter Example Guided Abstraction Refinement**

  - Lots of details to fill out (several different solutions)
    - how to generate abstraction
    - how to check counterexamples
    - how to refine abstractions

  - Microsoft SLAM driver verifier is a CEGAR system
Temporal Logic and Model Checking – Summary

- Various property languages: LTL, CTL, PSL (Prior, Pnueli)
- Models abstracted from hardware or software designs
- Model checking checks $M \models \psi$ (Clarke et al.)
- Symbolic model checking uses BDDs (McMillan)
- Avoid state explosion via simulation and abstraction
- CEGAR refines abstractions by analysing counterexamples
- Triumph of application of computer science theory
  - two Turing awards, McMillan gets 2010 CAV award
  - widespread applications in industry
THE END