

CS 5090:
Software Fault Tolerance –
Modal/Temporal Logic

Ali Ebneenasir
Department of Computer Science
Michigan Technological University

S/W Fault-Tolerance – Ebneenasir – Spring
2008

Acknowledgement

- The contents of this lecture are adapted from

Anil Nerode and Richard A. Shore, “**Logic for Applications**”, Springer-Verlag, 1997.

MichiganTech
What Does Modal Mean?

- Reason about notions such as possibility, necessity, knowledge, belief and time
- An extension of predicate logic with additional modal operators
- Additional Syntax Rule:
 - If ψ is a formula, then so are $\Box\psi$ and $\Diamond\psi$, where \Box and \Diamond are new symbols
- \Box and \Diamond may have different meanings depending on where modal logic is applied

S/W Fault-Tolerance – Ebneenasir – Spring
2008

MichiganTech

Semantics

- Intuitively
 - \Box means
 - “It is necessary that” (philosophy)
 - It is always true that (temporal logic)
 - I know (believe) that (epistemic logic)
 - \Diamond means
 - It is possible that
 - It will eventually be true that
- \Diamond is the negation of \Box

S/W Faulstich-Tolerance – Ehrenmüller – Spring 2008

MichiganTech

Semantics

- Formally: A generalization of structures in predicate logic known as Kripke structures (frames)

- 1) Set of possible worlds \mathcal{W}^o with different views of reality
 - Worlds with different interpretations (structures) of reality
 - Let $w \in \mathcal{W}^o$. $w \models \varphi$ means that φ is true in world w ; i.e., φ is true in the structure associated with w
- $\Box \varphi$ means φ is true in all possible worlds (necessity)

S/W Faulstich-Tolerance – Ehrenmüller – Spring 2008

MichiganTech

Semantics

- 2) Accessibility of one world q from another p captured by a relation \mathfrak{S} among worlds
 - $p \mathfrak{S} q$ means q is a successor world of p
- 3) A labeling function that associates a structure with each possible world

- **Semantics:** A triple $(\mathcal{W}^o, \mathfrak{S}, \mathcal{L})$, where
 - \mathcal{W}^o is the set of possible worlds,
 - \mathfrak{S} is the accessibility relation on \mathcal{W}^o , and
 - \mathcal{L} is the labeling function

S/W Faulstich-Tolerance – Ehrenmüller – Spring 2008

MichiganTech

Example:


- Consider concurrent programs
 - \mathcal{W}^e is the set of program states,
 - \mathcal{R} is the reachability relation on states, and
 - \mathcal{I} is the function that associates a set of atomic propositions to each state
- Then, what does $\Box (x>1)$ mean?
- How about $\Diamond(z=0)$?

S/W Fault-Tolerance – Ehemasi – Spring 2008

MichiganTech

Example

- Does this state machine satisfy $\Box (x>1)$?




S/W Fault-Tolerance – Ehemasi – Spring 2008

MichiganTech

Example

- Does this state machine satisfy $\Diamond (z=0)$?



S/W Fault-Tolerance – Ehemasi – Spring 2008

MichiganTech

Example

- Does this state machine satisfy $\diamond(z=0)$?

```
graph LR; S1((X=1, Z=1)) --> S2((X=2, Z=4)); S2 --> S3((X=5, Z=2)); S3 --> S4((X=5, Z=0)); S3 --> S2;
```

S/W Fault-Tolerance - Ehemasi - Spring 2008

MichiganTech

Temporal Logic (TL)

S/W Fault-Tolerance - Ehemasi - Spring 2008

MichiganTech

Why do we need TL?

```
graph LR; I[Inputs] --> P[Transformational programs]; P --> O[Outputs];
```

- Transform inputs to outputs in a finite amount of time
- Finite computations
- Hoare logic to reason about transformational programs
- Inputs satisfy a Precondition
- Outputs satisfy a Postcondition
- $\{Pre\}p\{Post\}$

S/W Fault-Tolerance - Ehemasi - Spring 2008

MichiganTech

Why do we need TL?

- How about applications with non-terminating computations?
 - Operating systems (e.g., scheduler, memory manager, etc.)
 - Network protocols
 - Embedded systems in critical infrastructures
- Mostly in concurrent/distributed programs
- Reason about time-varying infinite computations

S/W Fault-Tolerance – Ehemusir – Spring 2008

MichiganTech

Structure of Time

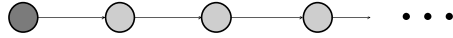
- Discrete time domain; current moment means current program state
 - Continuous time domain is used for modeling real-time systems
- Future time; mostly reason about the subsequent program behaviors
 - Past time has also been considered to simplify specifications

S/W Fault-Tolerance – Ehemusir – Spring 2008

MichiganTech

Semantics of Time

- **Linear** time: at any moment, there is only one possible next moment
 - Modalities capture events along a single timeline
 - A total order
 - Initial moment without any predecessor
 - Infinite into the future



S/W Fault-Tolerance – Ehemusir – Spring 2008
