Rely/Guarantee and CTL*  

Joey Coleman  

5 July 2010
Context

- Expressions to extensions of CTL*  
  - Atomicity refinement of expressions  
    - Stable/unstable components  
    - \emph{SingleUnstableVar()} restriction  
  - Better way of reasoning  
  - Resemblance: interference paths and branching time  
  - So, cast R/G in CTL*  
- Exploratory work; primarily my own curiosity
Rely/Guarantee — Quick Introduction

- \{P, R\} \pi \{G, Q\}
  - \(P\) pre condition; predicate
  - \(R\) rely condition; relation
  - \(\pi\) the subject program
  - \(G\) guarantee condition; relation
  - \(Q\) post condition; relation

- Relational
- Undefinedness (LPF)
- Underpinned by an operational semantics
Basic Framework

Configns

Transitions
More Constraints

- \( \{P, R\} \pi \{G, Q\} \)
- Feasibility:
  - \( P \subseteq \text{dom} \ Q \)
  - \( P \subseteq \text{dom} \ G \)
- Progress: \( \text{rng} \ R \subseteq \text{dom} \ G \)
- [ Composability: \( \text{rng} \ G_i \subseteq \text{dom} \ G_j \) ]
CTL* — Quick Introduction

- Branching-time temporal logic
- Kripke model $M = (S, R, L)$ where
  - $S$ is the set of states
  - $R$ is the accessibility relation
  - $L$ is a mapping from propositions to their truth value(s)
(More) CTL*

- Notions of states and paths; two types of formula
  - state formula: $M, s \models \phi$
    $s$ is a state
  - path formula: $M, x \models \phi$
    $x$ is a sequence of states
State Formulae

\[ M, s \models A\phi \quad \text{\(\phi\) is true over all paths} \]

\[ M, s \models E\phi \quad \text{\(\phi\) is true over some paths} \]
Path Formulae

- $M, x \models F\phi$ \hspace{1cm} $\phi$ is true at some point along the path
- $M, x \models G\phi$ \hspace{1cm} $\phi$ is always true
- $M, x \models X\phi$ \hspace{1cm} $\phi$ is true in the next state along the path
- $M, x \models \phi U\psi$ \hspace{1cm} $\phi$ is true until $\psi$ is true
Extending CTL*

- R/G: relational; CTL*: single-place propositions
- R/G: LPF; CTL*: boolean logic
- Three steps:
  - 3-valued CTL*
  - Relational CTL*
  - 3-valued, relational CTL*
Extending CTL*

- R/G: relational; CTL*: single-place propositions
- R/G: LPF; CTL*: boolean logic
- Three steps:
  - 3-valued CTL*
  - Relational CTL* ← Only talking about this step
  - 3-valued, relational CTL*
Relational CTL*

- \( M, s \models \phi \) becomes \( M, s', s \models \phi \)
- \( M, x \models \phi \) becomes \( M, s', x \models \phi \)
- Propositions become two-place
  - \( M, s', s \models R \) iff \( R(s', s) \)
  - Predicates are encoded as relations ignoring \( s' \)
Relational Path Modalities

- Two versions of each of $F$, $G$, $X$
  
  $\dot{X}\phi$ \hspace{1cm} $X\phi$

  $M, s', x \models \dot{X}R$ iff $R(s', x^1)$
  
  $\bar{X}\phi$

  $M, s', x \models \bar{X}R$ iff $R(x^0, x^1)$
  
  $\dot{F}\phi$ \hspace{1cm} $\bar{F}\phi$

  $M, s', x \models \dot{F}R$ iff $\exists i \cdot R(s', x^i)$
  
  $M, s', x \models \bar{F}R$ iff $\exists i \cdot R(x^0, x^i)$
A Model for R/G and Relational CTL*

- $M$ becomes $(\text{Config}, \xrightarrow{\lambda}, L)$ where
  - Config is from the operational semantics
  - $\xrightarrow{\lambda}$ is the transition relation from the semantics
  - $L$ maps relational propositions to truth values

- Propositions include:
  - Pre, Rely, Guar, Post, Done, $\xrightarrow{p}$, $\xrightarrow{e}$
Encoded Framework Assumptions

- Pre condition holds

\[ M, c', c_0 \models Pre \]

- Rely condition holds over environmental steps

\[ M, c', c_0 \models AG\overline{X}(e \rightarrow) \Rightarrow Rely \]

- Weak fairness

\[ M, c', c_0 \models AG(\neg Done \Rightarrow EX(p \rightarrow)) \]
Encoded Framework Constraints

• Guarantee holds over program steps

\[ M, c', c_0 \models AG\overline{X} \left( (\overset{p}{\rightarrow}) \Rightarrow Gu\text{ar} \right) \]

• Post condition holds at termination (if the pre condition holds initially)

\[ M, c', c_0 \models Pre \Rightarrow AG \left( \neg Done \land \dot{X}\text{Done} \Rightarrow \dot{X}Post \right) \]
(More) Encoded Framework Constraints

- Feasibility:
  - $P \subseteq \text{dom } Q$

  $$M, c', c_0 \models Pre \implies EF Post$$

  $$M, c', c_0 \models Pre \implies EX Guar$$

- Progress: $\text{rng } R \subseteq \text{dom } G$

  $$M, c', c_0 \models AGX \left( (\text{Rely} \land \neg\text{Done}) \implies EX Guar \right)$$
Future Work

- Case studies & examples
- Atomicity refinement
- Axiomatization & soundness
- Model-checking
- Temporal logic within rely/guarantee conditions
Thank you. Questions?