Model Checking of Real-Time Properties of Resource-Bound Process Algebra

Jungjae Lee

Theory and Formal Methods Lab.

Korea University

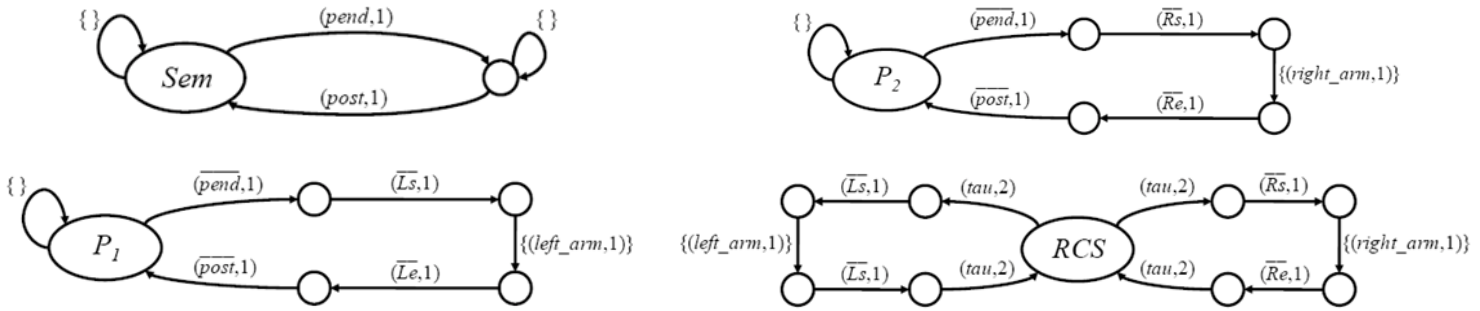
ACSR 소개

- **A**lgebra of **C**ommunicating **S**hared **R**esources
  - 이산 시간(discrete time), 자원(resource), 우선 순위(priority)가 고려된 실시간 프로세스 대수(Process Algebra)

- Robot Control System(RCS)의 ACSR 모델 예제

$$Sem \stackrel{\text{def}}{=} \emptyset : Sem + (pend, 0).rec\ X.(\emptyset : X + (post, 0).Sem)$$
$$P_1 \stackrel{\text{def}}{=} \emptyset : P_1 + (\overline{pend}, 1).(\overline{Ls}, 1).\{(left\_arm, 1)\} : (\overline{Le}, 1).(\overline{post}, 1).P_1$$
$$P_2 \stackrel{\text{def}}{=} \emptyset : P_2 + (\overline{pend}, 1).(\overline{Rs}, 1).\{(right\_arm, 1)\} : (\overline{Re}, 1).(\overline{post}, 1).P_2$$
$$RCS \stackrel{\text{def}}{=} (P_1 \| P_2 \| Sem) \backslash \{pend, post\}$$

- ACSR 모델에 대한 (Timed) Labeled Transition System



ACSR 분석 기법

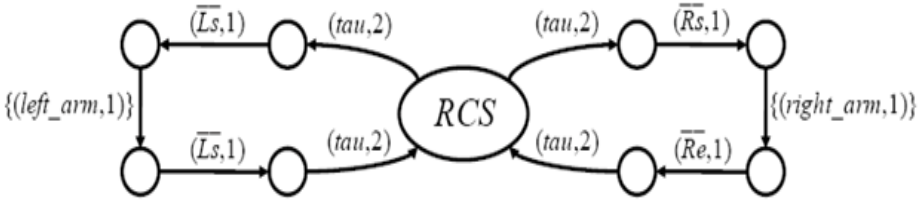
- Bisimulation checking

$$Sem \stackrel{\text{def}}{=} \emptyset : Sem + (pend, 0).rec\ X.(\emptyset : X + (post, 0).Sem)$$
$$P_1 \stackrel{\text{def}}{=} \emptyset : P_1 + (\overline{pend}, 1).(\overline{Ls}, 1).\{(left\_arm, 1)\} : (\overline{Le}, 1).(\overline{post}, 1).P_1$$
$$P_2 \stackrel{\text{def}}{=} \emptyset : P_2 + (\overline{pend}, 1).(\overline{Rs}, 1).\{(right\_arm, 1)\} : (\overline{Re}, 1).(\overline{post}, 1).P_2$$
$$RCS \stackrel{\text{def}}{=} (P_1 \| P_2 \| Sem) \backslash \{pend, post\}$$

$$Spec_1 \stackrel{\text{def}}{=} Spec_1' + Spec_1''$$
$$Spec_1' \stackrel{\text{def}}{=} (\tau, 2).(\overline{Rs}, 1)\{(right\_arm, 1)\} : (\overline{Re}, 1).(\tau, 2).Spec_1$$
$$Spec_1'' \stackrel{\text{def}}{=} (\tau, 2).(\overline{Ls}, 1)\{(left\_arm, 1)\} : (\overline{Le}, 1).(\tau, 2).Spec_1$$

$$Spec_2 \stackrel{\text{def}}{=} Spec_2' + Spec_2''$$
$$Spec_2' \stackrel{\text{def}}{=} (\overline{Rs}, 1)\{(right\_arm, 1)\} : (\overline{Re}, 1).Spec_2$$
$$Spec_2'' \stackrel{\text{def}}{=} (\overline{Ls}, 1)\{(left\_arm, 1)\} : (\overline{Le}, 1).Spec_2$$

- HML_u Model checking



Rs 와 ***Re*** 사이에 ***Ls*** 가 발생하지 않는다.

⇊

$$RCS \sim_\pi Spec_1$$
$$RCS \approx_\pi Spec_2$$

~(~((*tt* <*Rs*> *tt* ∧ ((*tt* <*Ls*> *tt*) <*A> ~(*tt* <*Re*> *tt*)))) <*A**> *tt***)

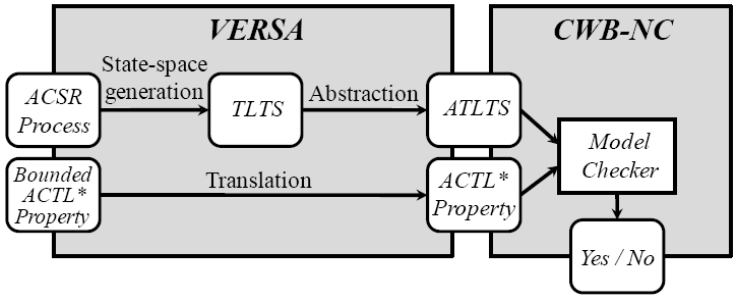
기존 분석 기법의 문제점

- Bisimulation checking
  - 시스템의 완전한 행위를 명세하여야 함.
  - 시스템을 명세하는 과정에 명세의 정확성을 따져 볼 수 없음.
  - 시스템의 크기가 커질 경우 상태 폭발 문제를 일으킴.
- HML_u Model checking
  - 속성을 직관적으로 기술하기 어려움.
  - 도구 지원이 되지 않음.

>> 속성을 쉽게 기술할 수 있는 시제 논리와 이를 확인할 수 있는 도구가 필요함.

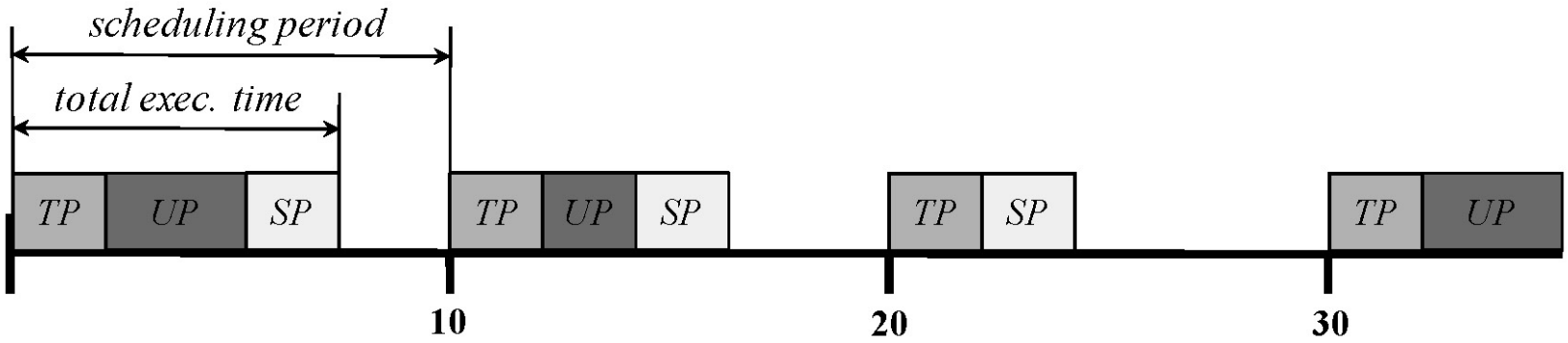
접근 방법

- Bounded ACTL* Model checking



  - VERSA , Concurrency Workbench of the New Century(CWB-NC) 사용.
  - Timed LTS을 Abstracted Timed LTS으로 변환 + Bounded ACTL*을 사용.
    - $\mathbf{G}^{<d}\,\varphi$, $\mathbf{G}^{\leq d}\varphi$, $\mathbf{F}^{<d}\varphi$, $\mathbf{F}^{\leq d}\varphi$, $\mathbf{G}^{\geq d}\,\varphi$, $\mathbf{G}^{>d}\varphi$, $\mathbf{F}^{\geq d}\varphi$, $\mathbf{F}^{>d}\varphi$, $\varphi_1\mathbf{U}^{\sim d}\varphi_2$ 사용.
      - Emmanuel Letier, et al., “Fluent Temporal Logic for Discrete-Time Event-Based Models”, ESEC/FSE 2005
  - 시제 명세 패턴(Temporal Specification Pattern)을 사용.
    - **AG** (*Rs*-> (~*Ls* **U** *Re*)) (Absence/Between Pattern)
      - Sacha Knrad, et al., “Real-time Specification Patterns”, ICSE 2005
      - Matthew B. Dwyer, et al., “Patterns in Property Specifications for Finite-State Verification”, ICSE 1999

사례 연구



TP is executed every scheduling period (*TPs* action occurs between two consecutive *TimeTick* actions).

» **AG** (*TimeTick* -> **X**(~ *TimeTick* **W** *TPs*))

TP finish its execution after at most 2 time units from the beginning of every scheduling period (If *TimeTick* occurs, then *TPe* occurs after at most 2 time units).

» **AG** (*TimeTick* -> $\mathbf{F}^{\leq 2}$*TPe*)

결론 및 향후 연구

- 결론
  - Bounded ACTL*를 사용하여 시스템의 실시간 속성을 명세 가능.
  - 명세한 속성의 확인이 가능한 도구 지원.
  - 시제 명세 패턴을 사용하여 속성을 정확하고 쉽게 명세 가능.

- 향후 연구
  - 상태 공간 축소 방안 연구
  - 자원 사용의 제약을 기술하는 시제논리 연구
  - 효율적인 모델체킹 알고리즘을 도구로 직접 구현