# 시태론리모형검사도구 UPPAAL을 리용한 체계련동모의와 정확성검증

리승광, 최창일

론문에서는 여러개의 분체계들로 구성되는 체계의 련동모의와 정확성검증을 시태론리모형검사도구 UPPAAL을 리용하여 진행하는 방법을 제기하고 한가지 단순화된 비행기날개조종체계의 모의와 검증에 적용하였다.

## 1. UPPAAL에 의한 체계련동모의와 정확성검증

일반적으로 체계련동에서는 모의프로그람을 리용하여 각종 시험을 진행하는 방법으로 련동정확성을 확인한다. 그러나 모의는 어디까지나 공학적인 방법인것으로 하여 체계련동으로 발생하는 모든 가능한 경우들을 다 확인하는것은 불가능한 일이다. 이 문제를 해결하기 위하여 여러가지 수학적방법들이 제기되였지만 그것들은 모두 검증을 위하여 프로그람을 작성해야 하는것으로 하여 사용자들이 쓰기 불편해하는 결함이 있다.[2]

UPPAAL은 시태론리에 기초하여 프로그람의 정확성을 검증하는 직관성이 강한 도구이다.[1] 검증하려는 프로그람은 시간자동체 또는 시간자동체망으로 모형화되며 검증하려는 성질은 시태론리공식으로 서술된다. 이에 기초하여 모형의 가능한 모든 실행경로들을 자동으로 탐색하는 방법으로 검증을 진행한다. UPPAAL을 리용하여 병행성처리가 기본문제로 제기되는 여러가지 통신규약들과 프로그람들의 정확성이 검증되였다.

론문에서는 수감부와 촬영기, 조종프로그람, 수행기구로 구성되는 비행기날개조종체계의 련동과정을 실례로 하여 UPPAAL을 체계련동모의와 련동정확성검증에 적용하는 방법을 보여준다. 이 방법은 분체계들의 련동으로 발생하는 가능한 모든 거동을 다 검사할수 있는 방법인것으로 하여 제한된 개수의 검사밖에 할수 없는 공학적인 방법의 약점을 극복할뿐아니라 강한 직관성으로 하여 모의와 검증에서 쉽게 리용될수 있는 효과적인 방법이라고 본다.

0을 포함하는 자연수모임을 $\mathbf{N}$으로 표시하고 $\mathbf{N}$우에서 값을 취하는 변수 $x$를 시계라고 부른다. $c\in\mathbf{N}$일 때 $x\le c$ 또는 $x\ge c$를 $x$에 대한 시간제한 또는 간단히 $x$에 대한 제한이라고 부른다. $x$에 대한 제한전부의 모임을 $\Phi(x)$로 표시한다. $\Phi(x)$는 무한모임이다.

$X=\{x_1, x_2, \cdots, x_k\}$라고 할 때 $\Phi(x_1)\cup\Phi(x_2)\cup\cdots\cup\Phi(x_k)$의 원소들로 취할수 있는 론리적전부의 모임을 $\Phi(X)$로 표시한다. $\Phi(X)$에 속하는 론리적의 실례로는 $x_1\le 3\wedge x_2\ge 5$와 같은것을 들수 있다. $\Phi(X)$의 원소들을 표시하는데 $\varphi$를 리용한다.

정의 1 다음과 같이 구성되는 $\Gamma=\{L, s_0, \Sigma, X, E, I\}$를 시간자동체라고 부른다.

$L=\{s_0, s_1, \cdots, s_n\}$: 위치들의 유한모임

$s_0\in L$: 초기위치

$\Sigma=\{a_1, a_2, \cdots, a_m\}$: 신호들의 유한모임

$X=\{x_1, x_2, \cdots, x_k\}$: 시계들의 유한모임

$I: L \to \Phi(X)$: 위치지속함수

$E \subseteq L \times \Phi(X) \times \Sigma \times 2^X \times L$: 이행관계

정의에서 위치지속함수의 값 $I(s)$는 위치 $s$에서 자동체가 얼마만한 시간동안 머물러 있을수 있는가를 규정해준다. 이행관계 $E$의 원소 $(s, \varphi, a, \lambda, s') \in E$는 자동체가 위치 $s$에서 $I(s)$가 만족되는동안 머물러있을수 있으며 이 동안에 시계값이 $\varphi$를 만족시키는 어느 한 순간에 신호 $a$를 받아서 위치 $s'$로 이행하고 $\lambda$에 속하는 시계값들을 0으로 재설정한다는것을 의미한다.

체계가 여러개의 분체계들로 구성되는 경우 개개의 분체계들을 시간자동체로 모형화하고 이것들의 망을 구성하는 방법으로 체계를 시간자동체망으로 모형화할수 있다. 그림 1은 비행기날개조종체계의 네가지 분체계들을 시간자동체의 가장 단순한 경우인 이행체계로 모형화한 결과를 보여준다. 복잡성을 피하기 위하여 검증하려고 하는 성질인 비교착성과 활성에 관련이 없는 세부들은 반영하지 않았다.

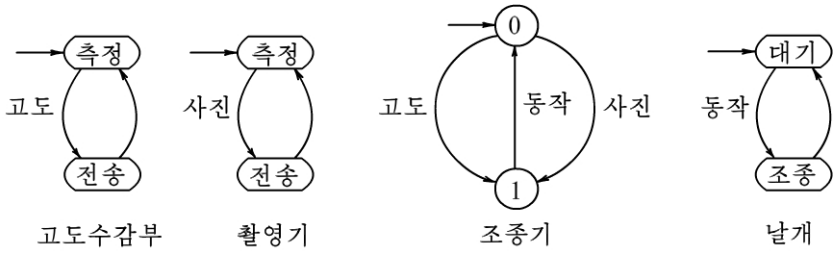


그림 1. 고도수감부, 촬영기, 조종기, 날개에 대한 이행체계

정의 2 UPPAAL의 요구명세언어는 BNF로 다음과 같이 정의된다.

Prop::=A[] Expression | E<> Expression | E[] Expression | A<> Expression | Expression--> Expression

정의에서 Expression은 명제론리의 공식이다.

UPPAAL을 리용하여 체계련동모의와 정확성을 검증하는 절차는 다음과 같다.

단계 1 편집기를 리용하여 검증하려는 체계의 매개 분체계들을 시간자동체로 모형화한다.

단계 2 모의기를 리용하여 분체계들에서 발생하는 신호들사이의 동기를 맞춘다.

단계 3 체계에서 만족하여야 하는 성질 즉 검증하려는 성질들을 명세언어로 서술한다.

단계 4 검증기를 가동시켜 작성한 모형이 검증하려는 성질을 만족하는가를 검사한다.

단계 5 검증하려는 성질이 만족되면 절차를 끝내고 만족되지 않으면 제시된 반례를 참고하여 모형을 수정하고 다시 검사를 진행한다.

## 2. 적 용 실 례

일반적으로 조종체계는 수감부와 조종프로그람, 수행기구로 구성된다. 그림 1에 제시한 비행기날개조종체계는 4개의 분체계 camera(촬영기), sensor(고도수감부), con(조종프로그람), wing(날개)로 구성된다. 이것들을 UPPAAL의 편집기로 체계모형화하고 동기를 맞추면 그림 2와 같다.

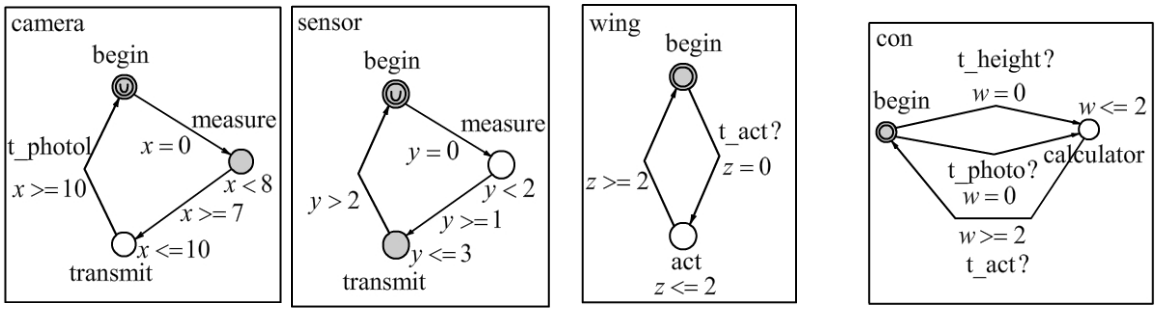


그림 2. 체계모형화

체계에서 검증하려는 성질들은 비교착성과 활성이며 이것들을 UPPAAL의 편집기로 서술하면 다음과 같다.

비교착성(체계가 교착에 빠지지 않는다.)

A[] not deadlock

활성(요청이 실현되지 않는 일은 없다.)

camera.transmit - - > wing.act

sensor.transmit - - > wing.act

검사는 UPPAAL의 검사기를 리용하여 자동으로 진행한다. 검사결과 그림 2의 모형은 활성은 만족하지만 다른 어떤 리유로 하여 다음과 같은 교착상태에 빠진다는것을 보여준다.

(camera.tr ansmit, sensor.mea sure, con.calcul ator, wing.act)

UPPAAL은 그 이행과정을 그림 3과 같이 제시한다.

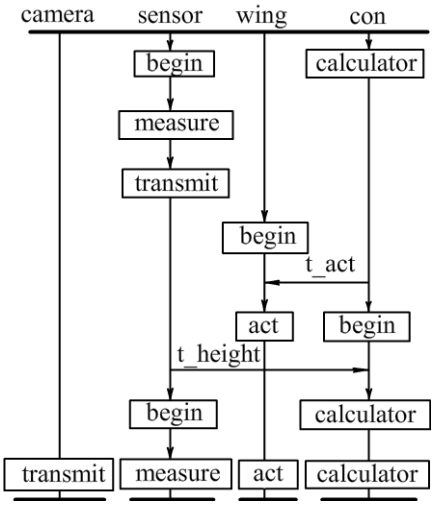


그림 3. 비교착성이 만족되지 않는 상태에로의 이행과정

그림 3에 보여준 이행과정을 분석해보면 비교착성이 만족되지 않는 상태에 도달하게 되는 리유를 알수 있다. 그것은 2개의 수감부자료들을 처리함에 있어서 1개 수감부가 보내온 자료들을 처리하는 과정에 다른 수감부가 자료를 보내오는 경우를 프로그람적으로 정확히 처리하지 못하였기때문이다.

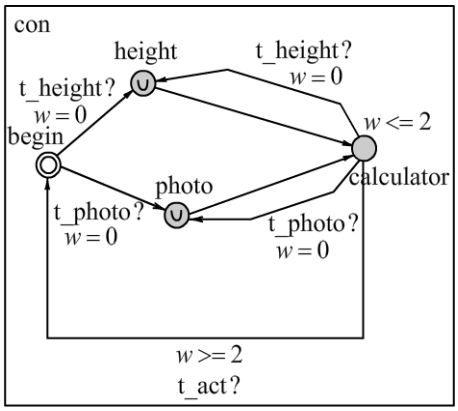


그림 4. 비교착성과 활성을 만족시키는 모형

이 문제를 해결하기 위하여 원래의 모형에서 con(조종프로그람)을 그림 4와 같이 수정한다. 그림에서 보는바와 같이 고도와 사진처리중에 사진이나 고도가 들어오는 경우를 처리하기 위해 새로운 상태들인 height와 photo를 추가하고 새로운 상태들과 상태 calculator사이에 가지들을 추가하였다.

우와 같이 조종프로그람을 수정하고 다시 검증을 진행하면 체계가 교착에 빠지지 않으며 활성도 만족하게 된다.

실례는 시태론리모형검사도구 UPPAAL이 여러개의 분체계들로 구성되는 체계의 련동과정을 모의하고 정확성을 검증하는데 효과적으로 리용될수 있다는것을 보여준다.

## 참 고 문 헌

[1] H. B. Mokadem et al.; IEEE Transactions on Automotion Science and Engineering, 7, 4, 921, 2010.
[2] Z. Chen et al.; Software: Practice and Experience, 45, 989, 2015.

주체107(2018)년 12월 5일 원고접수

## On the Interlocking Simulation and Verification of Systems using CTL Model Chekcer UPPAAL

*Ri Sung Gwang, Choe Chang Il*

In this paper, we present a method which simulates the interlocking of systems and verifies correctness of the simulation using CTL model checker UPPAAL.

Key words: simulation, verification