김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제11호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 11 JUCHE105(2016).

시간속성을 가지는 UML도식들의 모형검사에 대한 연구

한석민, 승남철

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《과학연구부문에서는 나라의 경제발전과 인민생활향상에서 전망적으로 풀어야 할 문제들과 현실에서 제기되는 과학기술적문제들을 풀고 첨단을 돌파하여 지식경제건설의 지름길을 열어놓아야 합니다.》

체계모형의 정확성을 담보하는것은 쏘프트웨어의 품질을 높이고 그 개발에 드는 전체적인 비용을 줄이는것으로 하여 많은 연구들이 진행되고있다.

선행연구[1]에서는 시간상태도들의 의미론들에 대하여, 선행연구[2]에서는 시간상태도를 실시간명세서언어 TRIO로 변환하는 방법에 대하여 론의하였으나 이 방법들로는 직접적인 모형검사가 불가능하다. 선행연구[3]에서는 PVS로 UML시간상태도들에 대한 검증방법에 대하여 론의하였으나 이 방법 역시 복합상태들에 대하여서는 검증이 불가능하다.

론문에서는 시간속성을 가지는 UML상태도와 순차도를 시간자동체로 변환하고 모형검사도구 UPPAAL을 리용하여 체계모형의 정확성을 검증하기 위한 리론적기초들을 밝히였다.

1. 시간속성을 가지는 UML상태도를 시간자동체에로의 변환

1) 계층적자동체와 시간자동체의 정의

정의 1 순서자동체 A는 4원조 $(\sigma_A, s_A^0, \lambda_A, \delta_A)$이다. 여기서 σ_A는 $s_A^0 \in \sigma_A$인 초기상태를 가지는 상태들의 유한모임, λ_A는 이행표식들의 유한모임이고 $\delta_A \subseteq \sigma_A \times \lambda_A \times \sigma_A$는 이행관계이다. 매 이행들에 대한 표식들은 5원조 (sr, ev, g, ac, td)로 이루어지는데 여기서 sr는 원천제약, ev는 촉발사건, g는 감시조건, ac는 활동들의 목록, td는 목표결정을 나타낸다. 즉 이행들은 t=(s, (sr, ev, g, ac, td), s')로 표시된다.

정의 2 계층적자동체 H는 4원조 (F, E, ρ, Λ)이다. 여기서 F는 상태들의 모임이 사귀지 않는 순서자동체들의 유한모임이다. 즉 $\forall A_1, A_2 \in F$, $\sigma_{A_1} \cap \sigma_{A_2} = \phi$이다. 그리고 E는 사건들의 유한모임이며 $\rho: \bigcup_{A \in F} \sigma_A \to 2^F$는 F에 대한 나무구조를 만든다. 즉 유일한 뿌리상태가 존재하고 뿌리가 아닌 상태들에 대하여서는 그것의 선조상태가 존재하며 순환을 포함하지 않는다. 또한

$$\Lambda = \bigcup_{A \in F} \lambda_A$$

이다.

정의 3 시간자동체 C는 5원조 $(S_C, S_{C_{init}}, A_C, T_C, \Gamma_C)$이다.

여기서 S_C는 유한상태모임이며 매개 상태는 $S \in S_C$이다. 그리고 $S_{C_{init}} \in S_C$는 초기상태, A_C는 유한동작모임으로서 입력모임 A_{CI}, 출력모임 A_{CO}와 내부동작모임 A_{CP}를 포함한다.

또한 T_C는 유한시간제약모임이며 이때 2개의 시간변수 x와 y에 대하여 시간제약은 $\alpha ::= x \prec c \mid x - y \prec c \mid \neg\alpha \mid \alpha \wedge \alpha,\ c \in N,\ \prec \in \{<, \leq\}$로 된다. 한편 $\Gamma_C \subseteq S_C \times A_C \times T_C \times S_C$는 유한이행모임이며 동작 $a \in A_{CI}, A_{CO}, A_{CP}$에 대응하는 이행 (s, a, t, s′)는 입력, 출력, 내부이행으로 구분된다.

2) 시간속성을 가지는 UML상태도를 시간자동체에로의 변환

시간속성을 가지는 UML상태도를 계층적자동체로 표현하고 이 계층적자동체를 시간자동체로 변환하여 상태도에 대한 모형검사를 진행할수 있다.

UML상태도를 계층적자동체로 표현하기 위하여 상태들의 모임과 초기상태들의 모임, 이행표식들의 모임, 이행들의 모임을 얻는다. 이를 위하여 다음과 같은 모임론적인 표기를 정의하고 리용한다.

정의 4 상태를 11원조 (Name, Type, Region, Trigger, EnB, ExB, Do, EnP, ExP, PR, AFlag)로 표시한다. 매 기호의 의미는 다음과 같다.

Name: 상태를 유일하게 식별할수 있는 이름이다.

Type: 단순상태인가, 령역인가, 합성상태인가, 부분상태인가를 나타내는 4원조의 2진값들의 모임이다.

Region: 상태에 의하여 직접 포함되는 령역들의 모임이다. 단순상태인 경우에는 빈모임이다.

Trigger: 상태와 관련되는 촉발사건들의 모임이다.

EnB: 상태에로 들어올 때 동작이다.

ExB: 상태에서 나갈 때의 동작이다.

Do: 상태의 do동작이다.

EnP: 상태에로 들어오는 점이다.

ExP: 상태에서 나가는 점이다.

PR: 부분상태에 속하는 련결점들의 모임이다.

AFlag: 현재상태가 활성인가 비활성인가를 나타내는 2진값이다.

정의 5 이행을 8원조(Name, S, D, R, A, T, Y, PFlag)로 표시한다.

여기서 Name은 이행식별자이름, S는 이행의 원천상태, D는 촉발조건들의 부분모임, R는 이행의 감시조건, A는 이행의 동작, T는 이행의 목표상태, Y는 이행을 포함하는 상태, PFlag는 가상상태이행을 나타내는 2진값을 표시한다.

이러한 정의에 기초하여 UML상태도를 모임론적인 표기의 의미에 맞게 우선 해당한 정보들을 분류하고 시간자동체로 직접넘기기를 진행한다. 여기서 중요한것은 상태도의 이행표식모임이 시간속성을 포함하여야 한다는것이다. 그러면 UML상태도의 모든 이행들은 시간자동체의 이행들로 표현된다.

다음 계층적자동체로 표현된 UML상태도의 구성나무로부터 나무의 잎들에로 들어가는 이

행들에서 시간제약을 포함하는 촉발조건과 사건들의 모임을 얻는다. 매 사건 e에 대하여 e에 의하여 일어나는 이행들의 모임과 이행들의 원천, 목적상태들을 구하여 이행들의 모임을 얻는다.

그리고 모든 관련있는 감시조건들은 시간자동체모형의 이행에 복사한다. 또한 UML모형의 클라스도에서 정의된 변수들은 시간자동체모형의 국부변수들로 그대로 복사한다.

UML모형에서 매 신호보내기에 대하여 시간자동체모형의 동기화가 진행되도록 중간상태들을 생성한다. 이행의 목적상태는 활성화되고 임의의 입장동작은 실시간체계모형에서 대응하는 동작으로 변환된다. 이 조작은 목적상태에서 뿌리로 내려가는 방향으로 처리된다.

한편 촉발사건이 없는 UML상태도의 이행은 완전사건에 의하여 일어난다. 그리고 단순상태의 모든 내부활동이 결정된 후에 완전사건이 일어난다.

시간속성을 가지는 UML상태도의 이행은 d가 부아닌 웅근수인 after(d)형식의 표기에 의하여 표기된 시간의 경과에 의하여 촉발될수 있다. 시간자동체에서는 시간이행을 가지는 매 상태 s에 대하여 박자 c_s를 정의한다. s를 포함하는 상태구조에 대응하는 시간자동체의 매 위치는 불변량 $c_s \le d$를 만족시킬것을 요구한다. 임의의 그러한 위치들로 들어오는 이행들은 c_s를 0으로 재설정한다. 시간사건은 s로부터 중간상태에로 이행하는 동안 일어나며 조건 $c_s = d$에 의하여 감시된다. UML상태도에서는 시간제한표기를 리용할수 있으며 d시간이 후라는것을 나타내는 after(d)형식의 기초적인 시간사건들만을 리용하여 실시간체계에 대한 모형화를 지원할수 있다. UML클라스도에서 이것을 반영하여 박자변수들을 리용하도록 한다. 이러한 박자들은 이행감시에서 검사될수 있고 이행의 효과로 재설정할수 있는데 이것을 시간자동체로 서술할수 있다.

2. GRC체계에 대한 UML설계의 실시간모형검사

제기한 방법을 GRC문제에 적용하여 체계의 정확성을 검사하자.

GRC(General Railroad Control)문제는 철길교차에서 개폐기를 조작하는 체계에 대한 문제이다. 여러개의 철길로선들에 대한 개폐기는 로선들의 위험부분들에 놓인다. 모든 렬차들은 같은 방향에서 위험부분을 지난다. 매 로선에 대하여 위험부분은 렬차가 위험부분에 들어오는가 혹은 나가는가를 가리키는 2개의 검출기에 의하여 감시된다. 매 로선에 대하여 기껏 하나의 렬차가 위험부분을 지나야 하는데 서로 다른 로선들에서 렬차들은 서로 다른 속도로 지나갈수 있고 그러므로 위험부분을 통과하는 시간들은 서로 다를수 있다. 개폐기는 열려있다가 어떤 렬차가 개폐기를 통과하는 동안에는 닫겨야 한다.(안전성속성)

다른 하나의 유용한 속성은 일정한 시간구간에 대하여 그 이전과 이후에 개폐기가 열려야 한다는것이다. 개폐기가 열림상태로 초기화될 때 그것은 완전히 열려야 하고 일정한 시간동안 열림상태가 지속되여야 한다.

이를 위하여 다음과 같은 시간속성들을 리용한다.

T_a: 렬차가 지점 A에서 위험지점 D로 들어오면서 개폐기를 통과하는데 걸리는 최대시간이다.

t_a: 렬차가 지점 A에서 위험지점 D로 들어오면서 개폐기를 통과하는데 걸리는 최소시간이다.

T_g : 렬차가 위험지점 D에서 지점 E로 나가면서 개폐기를 통과하는데 걸리는 최대시간이다.

t_g : 렬차가 위험지점 D에서 지점 E로 나가면서 개폐기를 통과하는데 걸리는 최소시간이다.

g_u : 개폐기가 완전히 닫긴상태로부터 완전히 열린상태로 되는데 걸리는 시간이다.

g_d : 개폐기가 완전히 열린상태로부터 완전히 닫긴상태로 되는데 걸리는 시간이다.

g_o : 개폐기가 열린상태에 머무르는 최소지속시간이다.

Δ : 개폐기에서 통신으로 인한 지연시간이다.

한편 시간자동체의 최종상태가 UML상태도를 표현하는 시간자동체와 순차도로부터 생성된 자동체에 도달가능한가를 검증하여야 한다.

체계의 어떤 정확성속성들은 순차도를 통하여 정확한 실행을 요구하는것으로 표현된다. 그러나 모든 속성들이 시간제약을 가지는 UML순차도를 리용하여 표현가능한것은 아니다. 특히 UML순차도들은 신호들의 결여가 나타나는지 검사하는것을 허용하지 않는다. 그러므로 GRC체계에 대한 안전성속성을 검증하기 위하여 모형검사에 불변량을 도입한다. 기초적인 안전성속성 즉 개폐기는 렬차가 지나가자마자 닫겨야 한다는것을 다음의 식으로 표시할수 있다.

$$\forall \square((\text{Track1.Crossing} \vee \text{Track2.Crossing}) \Rightarrow \text{Gate.Closed})$$

먼저 이 식을 리용하여 렬차가 지나가고있는데 개폐기가 닫기고있다는것을 검증하자. 이를 위해 Closing상태가 일어난 다음 개폐기가 닫기는데 g_d 시간 걸린다는 안전성속성을 추가하여 검사를 진행한다. 렬차가 통과한 후에 두번째 렬차가 같은 경로에 들어선다고 하자. 이것은 상태가 활성화된 후에 NoTrain상태에 대한 완전사건이 즉시에 일어날수 있다면 허용된다.

대응되는 enter신호는 앞선 exit신호 이전에 Control에 도착한다. 즉 ctl의 부합되는 령역이 Critical상태에 있을 동안 일어난다. 상태는 enter신호에 대하여 이행을 정의하지 않기때문에 그것은 무시되며 개폐기는 exit신호가 도착할 때 두번째 렬차가 접근하고 통과하는 동안 열려있는채로 남아있는다. 이것은 개폐기조종기에서 오유를 나타낸다. 오유는 Control상태도에 Critical로부터 Entered상태에로의 이행을 추가하여 수정할수 있는데 enter신호에 의하여 촉발되여 trains속성을 증가시키고 doOpen신호를 일으킨다.

맺 는 말

시간속성을 가지는 UML설계의 정확성을 검사하기 위한 한가지 방법을 제기하였다. 즉 UML상태도와 순차도를 시간자동체로 변환하기 위하여 UML도식들에 대한 모임론적표기를 새로 정의하였으며 계층적자동체를 시간자동체로 변환하기 위한 방법론을 제기하고 GRC문제에 적용하였다.

참 고 문 헌

[1] Rodolphe Arthaud et al.; http://wooddes.intranet.gr/workshop.htm., 2000.

[2] Atle Refsdal et al.; Journal of Computer and System Science, 81, 1221, 2015.

[3] Samir Ouchani et al.; Expert System with Applications, 41, 2713, 2014.

주체105(2016)년 7월 5일 원고접수

On Model Checking of UML Diagrams with Time Property

Han Sok Min, Sung Nam Chol

We researched theoretical bases to check its correctness by transforming UML state diagrams with time property and sequence diagram to timed automata using model check tool UPPAAL.

Key words: UML, model checking