김일성종합대학학보
수 학

주체107(2018)년
제64권 제4호

계단시간지속론리의 한가지 성질과 그것의 모형검사 알고리듬에 대한 연구

림권, 조영선

현실에서 제기되는 과학기술적문제들을 첨단수준에서 해결하는데서 실시간체계들의 안전성담보는 매우 중요한 문제로 나선다.

선행연구[1, 2]에서는 실시간체계의 실시간요구들을 형식적으로 서술하고 검사하는 도구로 지속론리가 연구되였다. 선행연구[1, 3]에서는 시간구간의 유한성과 무한성 그리고 어떤 시점에서의 상태변화를 고찰하면서 통신이나 계산과정이 매우 짧은 상태들에 대하여서는 그 경과시간을 령으로 처리하였다.

그러나 엄밀한 의미에서는 그 시간이 매우 짧아도 령으로는 될수 없으며 또 령이라고 보는 시각에도 체계내부에서는 여러가지 상태변화들이 일어나는 경우가 있다.

론문에서는 $\mathbf{R}^+$를 시간구조로 한 종전의 지속론리를 보존적으로 확장하여 계단시간이라는 새로운 시간구조우에서 지속론리를 정의하고 모형검사를 진행하였다.

1. 계단시간지속론리

계단시간구조를 정의하기 위해 다음의 표현들을 약속한다. $\mathbf{R}^+$를 부아닌 실수전부의 모임, $\mathbf{Z}^+$를 부아닌 웅근수전부의 모임이라고 하자. 시간구조에서 $\mathbf{R}^+$는 련속시간을, $\mathbf{Z}^+$는 리산시간을 의미하며 $\mathbf{R}^+$를 매크로시간구조, $\mathbf{Z}^+$를 마이크로시간구조라고도 한다. $\mathbf{R}^+$의 원소들을 $t_1, t_2, \cdots$, $\mathbf{Z}^+$의 원소들을 $i_1, i_2, \cdots$으로 표시한다.

정의 1 다음의 조건 ①－④를 만족시키는 쌍 $(ST, <)$을 계단시간구조라고 한다.

① $ST \subseteq \mathbf{R}^+ \times \mathbf{Z}^+$이다.

② $<$는 ST우의 사전식순서이다. 즉

$$(t_1, i_1) < (t_2, i_2) \quad \text{iff} \quad t_1 < t_2 \vee (t_1 = t_2 \wedge i_1 < i_2)$$

이다.

③ $<$는 단조성을 가진다. 즉

$$t_1 < t_2 \wedge (t_1, i_1) \in ST \wedge (t_2, i_2) \in ST$$

이면 $i_1 \le i_2$이다.

④ ST는 무한경과성을 가진다. 즉

$$\pi_1(t, i) = t, \ \pi_2(t, i) = i$$

라고 할 때 $\pi_1(ST) = \mathbf{R}^+, \ \pi_2(ST) = \mathbf{Z}^+$이다.

한편 ST우에서의 구간모임은 다음과 같이 령시간구간도 포함되게 정의한다.

$$\mathrm{Intv}(ST, <) \overset{def}{=} \{[b, e] \mid b, e \in ST, \ b \le e\}$$

이때 시간구간 $[b,\ e]$의 길이는 $e-b=(\pi_1(e)-\pi_1(b),\ \pi_2(e)-\pi_2(b))$ 이며

$$l=\pi_1(e)-\pi_1(b),\ \eta=\pi_2(e)-\pi_2(b)$$

일 때 $l\in\mathbf{R}^+$ 이고 $\eta\in\mathbf{Z}^+$ 이다.

계단시간구조우에서의 지속론리를 다음과 같이 정의한다.

이제 고찰하는 체계의 원자적인 성질들을 표시하는 원자공식전부의 모임을 $Pvar$ 로, 원자공식들을 $p,\ q,\ r,\ \cdots$ 등으로 표시하면 $Pvar$ 는 체계의 어떤 측면을 고찰하려고 하는가에 따라 결정된다.

정의 2 계단시간지속론리의 공식은 다음과 같이 구성된다.

$$P ::= p \mid \neg P \mid P_1\wedge P_2 \mid P_1\vee P_2 \mid P_1\to P_2$$

$$F ::= \lceil P\rceil^0 \mid \lceil P\rceil \mid \eta\ op\ k \mid \left(k_1\cdot\sum P_1+\cdots+k_m\cdot\sum P_m\right) op\ k \mid$$

$$l\ op\ c \mid \left(c_1\cdot\int P_1+\cdots+c_n\cdot\int P_n\right) op\ c$$

$$\Phi ::= \mid F \mid \neg\Phi \mid \Phi_1\wedge\Phi_2 \mid \Phi_1\vee\Phi_2 \mid \Phi_1\to\Phi_2 \mid \Phi_1\frown\Phi_2$$

여기서 $op\in\{=,\ \le,\ \ge\}$, $k\in\mathbf{Z}^+$, $c\in\mathbf{R}^+$ 이다.

계단시간지속론리공식의 의미는 형태별로 다음과 같이 정의한다.

우선 ST 를 계단시간구조, $[b,\ e]$를 ST 의 시간구간이라고 하면 $[b,\ b]$ 는 ST 의 한점구간을 의미한다. 조건《마이크로시점이 같은 ST 의 시점들의 모임은 어떤 유한개의 구간으로 분할되며 매개 구간의 점들에 대하여 L 의 값은 같다.》를 만족시키는 넘기기 $L: ST\to 2^{Pvar}$ 를 ST 의 해석이라고 한다.

정의 3 P 형태의 계단시간지속론리공식의 의미는 다음과 같이 정의된다.

$(ST,\ [b,\ b]) \models p$ iff $p\in L(b)$ 이다.

$(ST,\ [b,\ b]) \models \neg P$ iff $(ST,\ [b,\ b]) \not\models P$ 이다.

$(ST,\ [b,\ b]) \models P_1\wedge P_2$ iff $(ST,\ [b,\ b]) \models P_1$ 이고 $(ST,\ [b,\ b]) \models P_2$ 이다.

$(ST,\ [b,\ b]) \models P_1\vee P_2$ iff $(ST,\ [b,\ b]) \models P_1$ 이거나 $(ST,\ [b,\ b]) \models P_2$ 이다.

$(ST,\ [b,\ b]) \models P_1\to P_2$ iff $(ST,\ [b,\ b]) \models P_1$ 이면 $(ST,\ [b,\ b]) \models P_2$ 이다.

정의 4 F 형태의 계단시간지속론리공식의 의미는 다음과 같이 정의된다.

$(ST,\ [b,\ e]) \models \lceil P\rceil^0$ iff $b=e$ 이고 P 가 b 에서 참이다.

$(ST,\ [b,\ e]) \models \lceil P\rceil$ iff $b\le i\le e$ 인 임의의 점 i 에서 P 가 참이다.

$(ST,\ [b,\ e]) \models \eta\ op\ k$ iff $(\pi_2(e)-\pi_2(b))\ op\ k$ 이다.

$(ST,\ [b,\ e]) \models \left(k_1\cdot\sum P_1+\cdots+k_m\cdot\sum P_m\right) op\ k$ iff $(k_1\cdot eval(\sum P_1,\ [b,\ e])+$

$+\cdots+k_m\cdot eval\ (\sum P_m,\ [b,\ e]))\ op\ k$ 이다.

여기서 $eval(\sum P,\ [b,\ e])$ 는 $[b,\ e]$에서 P 가 참이 된 총회수라고 하자.

$(ST,\ [b,\ e]) \models l\ op\ c$ iff $(\pi_1(e)-\pi_1(b))\ op\ c$ 이다.

$$(ST,\ [b,\ e]) \models \left(c_1\cdot\int P_1+\cdots+c_n\cdot\int P_n\right) op\ c \text{ iff } \left(c_1\cdot\int_{\pi_1(b)}^{\pi_1(e)} P_1+\cdots+c_n\cdot\int_{\pi_1(b)}^{\pi_1(e)} P_n\right) op\ c$$ 이다.

정의 5 Φ형태의 계단시간지속론리공식의 의미는 다음과 같이 정의된다.

$(ST, [b, e]) \models \mathrm{F}$의 의미는 정의 3에서와 같다.

$(ST, [b, e]) \models \neg\Phi$ iff $(ST, [b, e]) \not\models \Phi$이다.

$(ST, [b, e]) \models \Phi_1 \wedge \Phi_2$ iff $(ST, [b, e]) \models \Phi_1$이고 $(ST, [b, e]) \models \Phi_2$이다.

$(ST, [b, e]) \models \Phi_1 \vee \Phi_2$ iff $(ST, [b, e]) \models \Phi_1$이거나 $(ST, [b, e]) \models \Phi_2$이다.

$(ST, [b, e]) \models \Phi_1 \rightarrow \Phi_2$ iff $(ST, [b, e]) \models \Phi_1$이면 $(ST, [b, e]) \models \Phi_2$이다.

$(ST, [b, e]) \models \Phi_1 \frown \Phi_2$ iff 어떤 $m(b \le m \le e)$이 있어서

$(ST, [b, m]) \models \Phi_1$이고 $(ST, [b, m]) \models \Phi_2$이다.

2. 모형검사알고리듬

아래에 임의로 주어진 시간자동체가 다음과 같은 형태의 계단시간지속론리의 공식을 만족시키는가를 검사하는 모형검사알고리듬을 제기한다.

성질 $0 < c < 1$, $\alpha = \{i \mid s_i = \neg P\}$라고 할 때

$$C_{\min} \le l \le C_{\max} \Rightarrow \left(\sum_{i \in \alpha} \int_{\pi_1(b_i)}^{\pi_1(e_i)} \neg P \le c \cdot l \right) \wedge \left(\sum_{i \in \alpha} \sum_{[\pi_2(b_i),\ \pi_2(b_i)]} \neg P \ \le m \cdot k \right)$$

이다. 이 공식을 간단히 $\boldsymbol{\Phi}$로 표시한다.

공식 $\boldsymbol{\Phi}$의 모형검사알고리듬

M을 임의로 주어진 시간자동체, $\boldsymbol{\Phi}$를 검사하여야 할 계단시간지속론리의 공식이라고 하자. 그리고 자동체 M은 부분순환이 없다고 가정한다. 즉 경로가 유한인 자동체에 대하여 검사를 진행한다. 이때 알고리듬을 다음과 같이 구성한다.

① 자동체 M의 정규표현식 $L(r)$를 찾는다.

② 정규표현식 $L(r)$에 의하여 생성되는 임의의 경로 $path$에 대하여 $path \models \boldsymbol{\Phi}$가 성립하는가를 다음과 같이 검사한다.

가정으로부터 정규표현식에 의하여 생성되는 경로는 유한개로서 그것을 $path_1, \cdots, path_k$라고 하자.

ㄱ) $C_{\min} \le l \le C_{\max}$에 대하여 $\exists S_j \in S$, $path_\tau\left(\int S_j\right) \le 0$ $(\tau = \overline{1,\ k})$이면 걸음 ㄴ)로 가고 $\forall S_j \in S$, $path_\tau\left(\int S_j\right) > 0$이면 검사를 중지한다.

ㄴ) $0 < \exists c < 1$에 대하여 $path_\tau\left(\int S_j\right) \le c \cdot l$이면 걸음 ㄷ)로 가고 $0 < \forall c < 1$에 대하여 $path_\tau\left(\int S_j\right) > c \cdot l$이면 검사를 중지한다.

ㄷ) $\exists k \in \omega$, $m = |\alpha|$에 대하여 $path_\tau(\eta) \le m \cdot k$이면 걸음 ㄹ)로 가고 $path_\tau(\eta) > m \cdot k$이면 검사를 중지한다.

ㄹ) $path_\tau\left(\sum_{i \in \alpha} S_i\right) = path_\tau(\eta)$이면 $path_\tau \models \boldsymbol{\Phi}$가 성립한다고 판정하고 $\tau = \tau + 1$로 증가시

킨 다음 걸음 ㄱ)부터 ㄹ)까지 반복한다. $path_\tau\left(\sum_{i\in\alpha} S_i\right) \neq path_\tau(\eta)$ 인 경우에는 $path_\tau \not\models \Phi$ 라고 판정하고 검사를 중지한다.

③ 모든 τ 에 대하여 $path_\tau \models \Phi$ 이면 $M \models \Phi$ 라고 판정하고 검사를 중지한다.

결국 계단시간지속론리공식 Φ 는 다음과 같이 구성된 자동체에서 접수된다는것을 알수 있다.

정리 $M=(S,\ T,\ L)$ 을 자동체, Φ 를 우에서 정의한 계단시간지속론리의 공식이라고 하자.

$S=\{S_1,\ S_2,\ S_3\}$ 은 상태들의 모임이고 $T=\{(S_1,\ t_1)\rightarrow S_2,\ (S_2,\ t_2)\rightarrow S_3,\ (S_3,\ t_3)\rightarrow S_1\}$ 은 이행규칙들의 모임이다. 여기서 $t_1>0,\ t_2=0,\ t_1>t_3>0$ 이다.

$L: S\rightarrow Atoms$ 인 함수이다. 여기서 $e_i,\ b_i\in ST$ 일 때 $t_i=e_i-b_i$ 이다.

이때 주어진 자동체에 대하여 $M\models\Phi$ 가 성립한다.

결국 계단시간지속론리를 리용하면 일부 실시간체계들의 모형화설계에서 지속시간이 대단히 짧아 무시되였던 상태들도 모두 체계의 모형화에 반영할수 있다.

참 고 문 헌

[1] Changil Choe et al.; UNU/IIST, 5, 375, 2007.

[2] Miaomiao Zhang et al.; UNU/IIST, 12, 332, 2005.

[3] Univan Ahn et al.; Communications in Computer and Information Science, 742, 211, 2014.

주체107(2018)년 6월 5일 원고접수

A Property of Step Time Frame Duration Calculus and Its Model Checking Algorithm

Rim Kwon, Jo Yong Son

Duration calculus represents a logical approach to formal design of real time systems.

In this paper, duration calculus is defined over step time frame, a new time frame which is an extended to design the states of real time systems in more detail and then we prove a property of this duration calculus.

Key words: duration calculus, model checking, real time system