시간자동체에서의 선형지속제한식검증을 위한 한가지 방법

차명혁, 최창일

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《과학기술을 확고히 앞세우고 과학기술과 생산을 밀착시키며 경제건설에서 제기되는 모든 문제들을 과학기술적으로 풀어나가는 기풍을 세워 나라의 경제발전을 과학기술적으로 확고히 담보하여야 합니다.》

론문에서는 콤퓨터체계의 정확성검증에서 제기되는 한가지 문제를 연구하였다.

선행연구[1]에서는 시간자동체의 임의의 거동이 선형지속제한식을 만족시키는가를 판정하는 문제가 임의의 웅근수거동이 선형지속제한식을 만족시키는가를 판정하는 문제와 같다는것을 밝히고 그라프탐색법으로 검증할수 있다는것을 제시하였다.

선행연구[3]에서는 련속값을 취하는 실시간자동체에서 선형지속제한식의 검증문제를 선형계획법을 리용하여 푸는 방법을 제기하였다.

선행연구[2]에서는 실시간자동체의 확장인 적분실시간자동체에서 확장된 선형지속제한식의 검증문제를 선형계획법을 리용하여 푸는 방법을 제기하였다.

론문에서는 련속값을 취하는 시간자동체에서 선형지속제한식의 검증문제를 선형계획법을 리용하여 푸는 한가지 방법을 제기한다.

시계변수들의 모임을 X로 표시하자. $c \le x$ 또는 $x \le c$ 형태의 식들을 시간제한이라고 부른다. 여기서 $x \in X$ 이고 $c \in N \cup \{0\}$ 이다.

시간제한들의 유한모임을 $\Phi(X)$로 표시하자.

정의 1 다음의 조건을 만족시키는 $A := \langle L, s_0, \Sigma, X, E, I \rangle$를 시간자동체라고 부른다.[1] 여기서 L은 상태들의 유한모임, $s_0 \in L$은 초기상태, Σ는 기호들의 유한모임, X는 시계변수들의 유한모임, I는 매 상태 $s \in L$에 상태불변식이라고 부르는 시간제한들의 모임 $I(s) \subset \Phi(X)$를 대응시키는 넘기기이다.

직관적으로 볼 때 시간자동체는 시계의 값이 $I(s)$를 만족시킬 때만 s에 머무른다.

$E \subseteq L \times \Phi(X) \times \Sigma \times 2^X \times L$은 스위치들의 모임이다. 스위치 $\langle s, \varphi, a, \lambda, s' \rangle$는 자동체가 상태 s에 머무르다가 φ라는 조건이 만족될 때 a라는 신호를 받아 상태 s'로 이행하면서 $\lambda(\subseteq X)$에 속하는 시계들의 값을 0으로 재설정한다는것을 의미한다.

시간자동체 $A = \langle L, s_0, \Sigma, X, E, I \rangle$가 다음과 같은 형태의 지속론리공식

$$D : 0 \le l \Rightarrow \sum_{s \in L} b_s \int s \le M$$

를 만족시키면 A는 선형지속제한식 D를 만족시킨다고 말하고 $A \models D$로 표시한다. 여기서 b_s, M은 실수이다. 항 $\int s$는 상태 s의 지속을 의미하는 항이고 l은 관찰구간의 길이를 의미하는 항이다.

편리상 시계들이 $X=\{x_1,\ x_2,\cdots,\ x_k\}$와 같이 순서화되여있다고 가정하자. $i=1,\cdots,\ k$에 대하여 $c_i\geq 0$일 때 벡토르 $v=(c_1,\ c_2,\cdots,\ c_k)$를 시계값벡토르라고 부른다. 시계값벡토르 $v=(c_1,\ c_2,\cdots,\ c_k)$는 시간자동체의 상태이행과정의 어떤 순간에 시계변수 x_i의 값이 c_i라는것을 의미한다. 시계값벡토르 $v=(c_1,\ c_2,\cdots,\ c_k)$와 부아닌 실수 d, $\lambda\subset X$에 대하여 새로운 시계값벡토르$(c_1+d,\ c_2+d,\cdots,\ c_k+d)$를 $v+d$로, $(c_1,\ c_2,\cdots,\ c_k)$에서 λ에 속하는 시계들의 값을 0으로 준 새로운 시계값벡토르를 $v[\lambda:=0]$으로 표시한다.

시간자동체의 상태 s와 $I(s)$를 만족시키는 시계값벡토르 v의 쌍$(s,\ v)$를 배치라고 부르며 배치들전부의 모임을 배치공간이라고 부른다. 스위치 $sw=<s,\ \varphi,\ a,\ \lambda,\ s'>$에 대하여 $(s,\ v)\xrightarrow{d,a}(s',\ v')$는 배치 $(s,\ v)$에서 $(s',\ v')$에로의 이행을 보여준다. 이때 $v'=v+d[\lambda:=0]$이여야 하며 $v+d$는 $I(s)$와 φ를 만족해야 한다.

시간자동체에서 상태 s_0으로부터 시작되는 상태들의 렬에 그 상태에 들어간 시점을 붙인 렬 $\rho:(s_0,\ t_0)(s_1,\ t_1)\cdots(s_m,\ t_m)$을 거동이라고 부르며 매 $t_i\ (1\leq i\leq m)$가 웅근수인 거동을 웅근수거동이라고 부른다. 시간자동체 A의 거동전부의 모임을 B_A, 웅근수거동전부의 모임을 B_A^I로 표시하자.

거동 $\rho:(s_0,\ t_0)(s_1,\ t_1)\cdots(s_m,\ t_m)$에 대하여 $D(\rho)$를 다음과 같이 정의하자.

$$D(\rho)=\sum_{i=1}^{m}b_{s_{i-1}}(t_i-t_{i-1})$$

$B\subset B_A$라고 하자. $\forall\rho\in B$에 대하여 $D(\rho)\leq M$일 때 거동모임 B는 D를 만족시킨다고 말하고 $B\models D$로 표시한다. 시간자동체 A가 선형지속제한식 D를 만족시키는가를 판정하는 문제는 $B_A\models D$인가를 판정하는 문제이다.

보조정리 1 임의의 거동 ρ에 대하여 어떤 웅근수거동 ρ'가 있어서 $D(\rho)\leq D(\rho')$가 성립한다.[1]

보조정리로부터 $B_A\models D$이기 위해서는 $B_A^I\models D$일것이 필요하고 충분하다는것을 알수 있다.

론문에서는 우의 보조정리결과에 기초하여 다음과 같이 새로운 실시간자동체를 구성한다.

K_i를 $x_i\in X$에 대한 시간제한식들에서 나오는 상수들가운데서 최대수라고 하고 $K=\max\limits_{1\leq i\leq k}K_i+1$이라고 하자. 시계값벡토르들사이의 동등성을 다음과 같이 정의한다.

정의 2 $v_1,\ v_2$를 2개의 웅근수시계값벡토르라고 하자. $i=1,\ 2,\cdots,\ k$에 대하여 $v_1(x_i)=v_2(x_i)$이거나 $v_1(x_i)\geq K_i+1\wedge v_2(x_i)\geq K_i+1$일 때 2개의 시계값벡토르는 동등하다고 말하며 $v_1\cong v_2$로 표시한다.

$\cong$가 A의 시계값벡토르모임에서의 동등관계로 된다는것은 분명하다. v를 포함하는 동등류를 $[v]$로 표시하고 웅근수시계값묶음 간단히 시계값묶음이라고 부른다.

시계모임 $X=\{x_1,\ x_2,\cdots,\ x_k\}$에 대하여 시계값묶음을 $[c_1,\ c_2,\ \cdots,\ c_k]$와 같이 표시한다. 여기서 c_i는 $x_i=c_i$를 만족시키는 웅근수이거나 $x_i\geq K_i+1$을 만족시키는 x_i에 대하여 기호 *로 표시한다. 다시말하여 시계값묶음 $[c_1,\ c_2,\ \cdots,\ c_k]$는 $c_i\neq *$이면 $v_i=c_i$이고 $c_i=*$이면 $v_i\geq K_i+1$인 시계값벡토르 $v=(v_1,\ v_2,\cdots,\ v_k)$들의 모임이다. 실례로 [2, 0, *, 1]

은 $p \geq K_3+1$일 때 $(2,\ 0,\ p,\ 1)$형태의 시계값벡토르들을 포함하는 시계값묶음을 표시한다. 시계값묶음들의 개수는 $(K+1)^k$를 넘지 않는다. 여기서 k는 시계의 개수이다.

$\pi_0 := [0,\ 0, \cdots,\ 0]$이고 $\pi_K := [*,\ *, \cdots,\ *]$로 표시하자. π_0은 모든 시계변수들값이 0인 시계값벡토르를 포함하고 π_K는 매 시계변수 x_i의 값이 K_i보다 큰 값을 가지는 무한개의 시계값벡토르들을 포함한다.

주어진 시계값묶음 $\pi = [c_1,\ c_2, \cdots,\ c_k]$와 웅근수 $d \geq 0$, $\lambda \subset X$에 대하여 $\pi + d$는 $i = 1,\ 2, \cdots,\ k$에 대하여 $c_i \neq *$이고 $c_i + d \leq K_i$이면 $c_i' = c_i + d$이고 그렇지 않으면 $c_i' = *$인 시계값묶음 $[c_1',\ c_2', \cdots,\ c_k']$를 표시한다.

$\pi[\lambda := 0]$은 $x_i \in \lambda$이면 $c_i' = 0$이고 그렇지 않으면 $c_i' = c_i$인 시계값묶음 $[c_1',\ c_2', \cdots,\ c_k']$를 표시한다.

만일 $v_1 \cong v_2$이면 임의의 웅근수 $d \geq 0$에 대하여 $v_1 + d \cong v_2 + d$이고 임의의 $\lambda \subset X$에 대하여 $v_1[\lambda := 0] \cong v_2[\lambda := 0]$이라는것을 알수 있다. 그러므로 $v' = v + d$이면 $[v'] = [v] + d$이고 $v' = v[\lambda := 0]$이면 $[v'] = [v][\lambda := 0]$이라는것을 쉽게 증명할수 있다. 즉 $v' = (v + d)[\lambda := 0]$이면 $[v'] = ([v] + d)[\lambda := 0]$이다. 또한 $\pi + d = \pi_K$를 만족시키는 웅근수 $d \geq 0$이 존재한다면 모든 $d' \geq d$에 대하여 $\pi + d' = \pi_K$이다. 또한 $\pi + K = \pi_K$이며 임의의 $d \geq 0$에 대하여 $\pi_K + d = \pi_K$이다.

시계값묶음 π에 속하는 임의의 시계값벡토르가 시간제한 φ를 만족시키면 π는 φ를 만족시킨다고 말하고 $\pi \models \varphi$로 표시한다. 동등관계 $\cong$의 정의로부터 어떤 $v \in \pi$가 φ를 만족하게 되면 $\pi \models \varphi$이다.

시계값벡토르들사이의 동등관계 $\cong$는 A의 배치공간에서의 동등관계 $\equiv$로 다음과 같이 확장된다.

정의 3 A의 두 배치 $q_1 = (s_1,\ v_1)$과 $q_2 = (s_2,\ v_2)$에 대하여 $v_1 \cong v_2$이고 $s_1 = s_2$일 때 두 배치는 동등하다고 말하고 $q_1 \equiv q_2$로 표시한다.

$\equiv$가 A의 배치공간에서 동등관계로 된다는것은 분명하다. 동등관계 $\equiv$는 A의 배치공간을 여러개의 동등류로 분할하는데 이 동등류를 배치묶음이라고 부른다. 배치묶음을 상태 s와 시계값묶음 π의 쌍 $<s,\ \pi>$로 표시한다. 배치묶음의 개수가 $|L|(K+1)^k$를 넘지 않는다는것을 쉽게 알수 있다.

주어진 배치묶음 $<s,\ \pi>$와 스위치 $sw = <s,\ \varphi,\ a,\ \lambda,\ s'>$에 대하여 $<s,\ \pi>$의 뒤에 오는 배치묶음을 다음과 같이 정의한다. $0 \leq d \leq K$인 웅근수 d에 대하여 만일 $\pi + d \models (I(s) \wedge \varphi)$이고 $\pi' = (\pi + d)[\lambda := 0] \models I(s')$이면 새로운 배치묶음 $<s',\ \pi'>$를 $<s,\ \pi>$뒤에 오는 배치묶음이라고 부른다. 이것을 $<s,\ \pi> \xrightarrow{d,a} <s',\ \pi'>$로 표시한다. 동등관계 $\cong$의 성질들은 $\equiv$에서도 그대로 성립한다.

보조정리 2 $(s,\ v) \xrightarrow{d,a} (s',\ v')$이면 $<s,\ [v]> \xrightarrow{d,a} <s',\ [v']>$이고 반대로 $<s,\ \pi> \xrightarrow{d,a} <s',\ \pi'>$이면 매 $v \in \pi$에 대하여 어떤 $v' \in \pi'$가 있어서 $(s,\ v) \xrightarrow{d,a} (s',\ v')$가 성립한다.

이제 시간자동체 A의 배치그라프 $CG = (V,\ E)$를 다음과 같이 귀납적으로 정의한다.

① E 는 초기에는 빈모임이고 V 는 초기에 한 원소모임 $\{<s_0,\ \pi_0>\}$ 이다. 여기서 s_0 은 시간자동체 A 의 초기상태이고 π_0 은 모든 시계들이 0인 시계값묶음이다.

② $<s,\ \pi>\in V$ 에 대하여 $<s',\ \pi'>$ 가 그것의 뒤에 오는 배치묶음이라면 $<s',\ \pi'>$ 를 V 에 추가하고 $e=(<s,\ \pi>,\ <s',\ \pi'>)$ 를 릉으로 E 에 추가한다. 매 릉 e 에는 구간 $[l(e),\ u(e)]$ 가 대응되는데 $l(e)$, $u(e)$ 는 각각 체계가 배치묶음 $<s,\ \pi>$ 에 머물수 있는 최소, 최대시간이다. 즉

$$l(e) := \inf\{d \geq 0 \mid d \in \mathbf{N},\ <s,\ \pi> \xrightarrow{d,a} <s',\ \pi'>\}$$

$$u(e) := \sup\{d \geq 0 \mid d \in \mathbf{N},\ <s,\ \pi> \xrightarrow{d,a} <s',\ \pi'>\}$$

이다. 이때 $0 < l(e) \leq u(e)$ 가 성립한다.($u(e)=+\infty$ 일수도 있다.)

배치그라프는 다음의 알고리듬을 리용하여 구성할수 있다.

```
Begin
V := {<s0, π0>}; E := φ; mark <s0, π0> as unexplored;
While (true) do begin
If all of vertexes in V are marked with "explored" then exit;
let unexplored vertex v = <s, π> ∈ V;
for each switch sw = (s, φ, λ, s') do
for d = 0 to K do begin
    if (π + d) ≠ I(s) ∧ φ then goto loop;
    if (π + d)[λ := 0] ≠ I(s') then goto loop;
    π' = (π + d)[λ := 0];
    If <s', π'> ∉ V then
        add <s', π'> into V;
        mark <s', π'> as unexplored
    end if;
    if (<s, π>, <s', π'>) ∉ E then
        add e = (<s, π>, <s', π'>) into E;
        l(e) = d;
        if π' = πK then u(e) = ∞ else u(e) = d
    else
        if u(e) ≠ ∞ then u(e) = d
    end if
loop: next d
next sw
end
end
```

이 배치그라프를 상태이행도로 하는 새로운 실시간자동체를 다음과 같이 구성한다.

배치그라프 $CG=(V,\ E)$ 의 매 정점 v 를 새로운 상태로 하고 릉 e 를 이행으로 하며 e 에 대응되는 시간구간 $[l(e),\ u(e)]$ 를 그 이행에 해당한 시간제한으로 한다. 이 실시간자

동체를 $A' =< V,\ E,\ low,\ up >$ 이라고 하자. 여기서 $low : E \to \mathrm{N} \cup \{0\}$ $(low(e) = l(e))$, $up : E \to \mathrm{N} \cup \{+\infty\}$ $(up(e) = u(e))$이다. 이 실시간자동체는 시계모임이 1개 원소로 이루어지고 이 시계가 다른 상태에로 넘어갈 때마다 매번 재설정되는 시간자동체로 볼수 있다.

이제 선형지속제한식 D로부터 얻어지는 새로운 선형지속제한식 D'를 다음과 같이 정의하자.

$$D' : 0 \le l \Rightarrow \sum_{<s,\pi>\in V} b_s \int < s,\ \pi > \le M$$

이때 다음의 정리가 성립한다.

정리 1 $A \models D$이기 위해서는 $A' \models D'$일것이 필요하고 충분하다.

실시간자동체 A'에 대한 론의는 선행연구[3]에서와 같다. 선행연구[3]에서는 실시간자동체가 선형지속제한식을 만족시키는가를 유한개의 선형계획법을 풀어서 판정하는 방법을 제기하였다. 따라서 다음의 정리가 성립한다.

정리 2 $A \models D$인가를 판정하는 문제는 유한개의 선형계획법을 푸는 문제로 귀착된다.

참 고 문 헌

[1] Zhao Jinhua et al.; J. Comput. Sci. & Technol, **15**, 423, 2000.

[2] Choe Changil et al.; CCIS, **476**, 62, 2014.

[3] Z. Chaochen et al.; A Formal Approach to Real-Time Systems, Springer, 125～144, 2004.

주체107(2018)년 6월 5일 원고접수

A Checking Method Timed Automata for Linear Duration Invariants

Cha Myong Hyok, Choe Chang Il

In this paper, the problem of checking timed automata for linear duration invariants is reduced to the problem of checking real-time automata for linear duration invariants and verified using linear programming.

Key words: timed automata, duration calculus, model checking, real-time system