김일성종합대학학보 주체108(2019)년
정보과학 제65권 제2호

정확성검증을 위한 시간속성명세서작성의 한가지 방법

김철, 신춘옥

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《대학교육에서 리론교육과 실천교육을 밀접히 결합하여 진행하여야 합니다.》

(《**김정일**선집》 증보판 제21권 45페지)

선행연구들에서는 시간속성명세서작성방법을 세가지 방향에서 진행하였다.

① 자연언어로 서술된 시간속성을 시제론리식으로 넘기는 기계번역방법

② 사용자가 그라프적인 대본표기(시각언어)로 시간속성을 표현하면 그것을 속성명세서로 변환하는 방법

③ 사용자가 속성의 패턴과 적용범위를 선택하게 하고 그것에 해당한 론리식형타로부터 속성식을 자동적으로 편성해주는 방법

선행연구들에서 제일 많이 리용된것이 3번째 방법이다.

시간속성명세서작성을 위한 패턴체계 SPS는 계층화된 패턴분류와 적용범위, 시제론리식형타들의 모임으로 구성된다. 여기서 사용자는 패턴과 적용범위를 지적하는것으로 시간속성식을 얻을수 있다.

속성패턴들을 확장하거나 전문화하여 속성명세서의 표현능력을 높이기 위한 여러가지 방법[1, 2]도 제안되였다.

패턴체계 Prospec에서는 련속적이며 병행적인 행동들을 서술하도록 패턴들과 적용범위파라메터들을 분류하여 SPS를 확장하였다. 특히 여러 형태의 CP클라스(합성명제클라스)들을 정의하고 그것들의 의미를 LTL로 서술하였다. 그러나 SPS가 기초적인 패턴들과 적용범위에 대한 LTL식들과 Prospec에서 CP클라스들을 위한 LTL의미론을 제공하였지만 일부 CP클라스의 LTL정의를 패턴과 적용범위의 조합에 대하여 직접 대입시켜 계층적으로 세련화할 때 정확하지 못한 LTL식이 생성되는 경우가 있다. 그것은 SPS의 원자명제는 어느 한 시점에서의 조건 또는 사건을 의미하고 Prospec에서 제기한 CP클라스의 합성명제는 일정한 시간령역의 조건 또는 사건들의 조합을 나타내기때문이다.

론문에서는 패턴들과 적용범위, CP클라스들의 조합에 의한 LTL명세서의 작성에서 론리식형타로 리용할수 있는 추상적인 LTL식을 구성하는 방법을 제안하였다.

1. 합성명제를 파라메터로 가지는 시간속성패턴과 적용범위의 정의

패턴분류와 적용범위의 정의는 SPS에 따르며 CP클라스의 정의는 Prospec에 따른다.

대역적범위내에서 SPS의 시간속성패턴들중에서 다음의 패턴들에 대하여 보기로 하자.

① P가 전혀 출현하지 않음

② P가 적어도 한번 출현

③ Q가 P를 앞섬

④ Q가 P를 엄격히 앞섬

⑤ Q가 P에 응답

여기서 P는 단순명제 혹은 합성명제이고 그것에 대한 LTL론리식을 P_{ltl}로 표시한다.

매 패턴들을 구체적으로 보면 다음과 같다.

· 패턴《P가 전혀 출현하지 않음》은 속성 P가 전혀 성립하지 않는다는것을 나타낸다. 즉 모든 상태 s에서 P가 성립하지 않는다는것을 의미한다. 따라서 패턴《P가 전혀 출현하지 않음》에 대한 LTL식은 $[]\neg P_{ltl}$이다.

· 패턴《P가 적어도 한번 출현》은 (단순 혹은 합성)속성 P가 어떤 상태 s에서 성립하며 CP클라스의 경우에는 단순히 계산의 어떤 상태에서 P가 참이라는것을 의미한다. 따라서 패턴《P가 적어도 한번 출현》에 대한 LTL식은 $<>P_{ltl}$이다.

· 단순명제에 대한《앞섬》,《엄격히 앞섬》,《응답》과 같은 패턴들의 의미는 SPS에서 정의한 그대로이다.

CP를 리용할수 있게 이 패턴들의 의미를 확장하자면 단어《이전》,《이후》의 의미를 보다 명백하게 규정하여야 한다.

단순명제는 하나의 상태에서 평가되지만 CP는 상태들의 렬과 시간구간에 관계된다.

특히 CP(합성명제)

$$P=T(p_1, \cdots, p_n)$$

에 대하여 시작상태 b_p(p_i가 참으로 되는 첫상태)와 끝상태 e_p(조건 T가 성립될 때의 첫상태)가 있다.

매 상태 s와 CP에 대하여 s에서 성립하는 $P=T(p_1, \cdots, p_n)$에 대하여 시작상태 $b_p(s)$와 끝상태 $e_p(s)$를 다음과 같이 정의한다.

상태 s에서 성립하는 CP클라스 $P=$《적어도 하나의 조건》$(p_1, \cdots, p_n)$에 대하여

$$b_p(s)=e_p(s)=s$$

로 한다.

상태 s에서 성립하는 CP클라스 $P=$《적어도 하나의 사건》$(p_1, \cdots, p_n)$에 대하여 $e_p(s)$로는 명제들중의 하나인 p_i가 참으로 되는 첫상태 $s'>s$, $b_p(s)$를

$$b_p(s)=e_p(s)-1$$

로 한다.

상태 s에서 성립하는 CP클라스 $P=$《병렬조건》$(p_1, \cdots, p_n)$에 대하여

$$b_p(s)=e_p(s)=s$$

로 한다.

상태 s에서 성립하는 CP클라스 $P=$《병렬사건》$(p_1, \cdots, p_n)$에 대하여 $e_p(s)$는 명제 p_i들모두가 참으로 되는 첫상태 $s'>s$이고

$$b_p(s)=e_p(s)-1$$

로 한다.

상태 s에서 성립하는 CP클라스 $P=$《잇달은 조건》$(p_1, \cdots, p_n)$에 대하여

$$b_p(s)=s,\ e_p(s)=s+(n-1)$$

로 한다.

상태 s에서 성립하는 CP클라스 $P=$《잇달은 조건》$(p_1, \cdots, p_n)$에 대하여 $b_p(s)$로서는 모든 명제가 거짓이고 다음상태에서 p_1이 참으로 되는 마지막상태 $s'>s$를

$$e_p(s)=s'+(n)$$

으로 한다.

상태 s에서 성립하는 CP클라스 $P=$《최종적조건》$(p_1, \cdots, p_n)$에 대하여 $b_p(s)=s$로 하고 $e_p(s)$로는 마지막명제 p_n이 참이고 $p_2, \cdots, p_{n-1}$이 대응하는 상태들

$$s_2, \cdots, s_{n-1}(s<s_2<\cdots<s_{n-1}<s_n)$$

에서 참인 첫 상태 $s_n>s$를 취한다.

상태 s에서 성립하는 CP클라스 $P=$《최종적사건》$(p_1, \cdots, p_n)$에 대하여 $b_p(s)$로는 모든 명제가 거짓이고 다음상태에서 첫 명제 p_1이 참인 첫상태 s_1을, $e_p(s)$로는 마지막명제 p_n이 참인 첫상태 s_n을 취한다.

우에서 정의한 시작상태와 끝상태의 개념을 사용하여 대역적인 적용범위에서의《앞섬》,《엄격히 앞섬》,《응답》패턴을 다음과 같이 정의한다.

정의 1 P, Q가 CP클라스라고 하자.

P가 어떤 상태 s에서 성립하고 Q도 $e_Q(s')\le b_p(s)$인 어떤 상태 s'에서 성립하면《Q는 P를 앞선다.》라고 말한다. 다시말하여 Q의 마지막상태가 P의 시작상태와 같거나 P의 시작상태전의 상태이면《Q는 P를 앞선다.》라고 한다.

정의 2 P, Q가 CP클라스라고 하자.

P가 어떤 상태 s에서 성립하고 Q도 $e_Q(s')<b_p(s)$인 어떤 상태 s'에서 성립하면《Q는 P를 엄격히 앞선다.》라고 말한다. 다시말하여 Q의 마지막상태가 P의 시작상태전의 상태이면《Q는 P를 엄격히 앞선다.》라고 한다.

정의 3 P, Q가 CP클라스라고 하자.

P가 어떤 상태 s에서 성립하고 그다음 Q도 $e_p(s)\le b_Q(s')$인 어떤 상태 s'에서 성립하면《Q는 P에 응답한다.》라고 말한다. 다시말하여 Q의 시작상태가 P의 끝상태와 같거나 P의 끝상태를 따르는 상태이면《Q는 P에 응답한다.》라고 한다.

SPS에서 지적된 비대역적인 적용범위들을 형식적으로 다음과 같이 정의한다.

《R이전》적용범위는 구간 $[0, b_R(s_f)]$에 놓이며 여기서 s_f는 R가 참인 첫상태이다. 이 적용범위는 계산을 시작하는 상태를 포함하지만 $b_R(s_f)$와 련관된 상태를 포함하지 않는다.

《L이후》적용범위는 구간 $[e_L(s_f), \infty)$에 놓이며 여기서 s_f는 L이 참으로 되는 첫상태이다. 이 적용범위는 $e_L(s_f)$와 관련되는 상태를 포함한다.

《L과 R사이》적용범위는 $[e_L(s_L), b_R(s_R))$이며 여기서 s_L은 L이 성립하는 상태이고 s_R는 R가 참인 $e_L(s_L)$보다 뒤에 놓이는 첫상태이다.

《L부터 R까지》적용범위는 적용범위《L과 R사이》에 대한 범위에 구간 $[e_L(s_L), \infty)$를 보충한것이며 여기서 s_L은 L이 성립하고 상태 $s>e_L(s_L)$에서는 R가 성립하지 않는 상태

이다.

정의 4 P가 CP클라스이고 S는 적용범위라고 하자.

P가 상태 $s_p \in S$ 와 $e_p(s) \in S$ 에서 성립하면(즉 끝상태 $e_p(s_p)$ 는 같은 적용범위 S에 속한다.) P는 S에서 $s-$성립한다고 말한다.

적용범위내에서 패턴의 서술을 다음의 표에 보여주었다.

표. 적용범위내에서 패턴의 서술

패턴	서술내용
P가 적어도 한번 출현	P가 이 범위내의 어떤 상태에서 $s-$성립하면 《P가 적어도 한번 출현》은 적용범위 S내에 있다고 한다.
P가 전혀 없음	P_s 가 적용범위내의 임의의 상태에서 $s-$성립하지 않으면 《P가 전혀 없음》은 S범위내에 있다고 한다.
Q가 P를 앞섬	P가 어떤 상태 s에서 $s-$성립하고 Q도 $e_Q(s') \le b_p(s)$ 에 대해서 어떤 상태 s' 에서 $s-$성립하면 S범위내에서 Q가 P를 앞선다고 한다.
Q가 P를 엄격히 앞섬	P가 어떤 상태 s에서 주어지고 Q도 $e_q(s') < b_p(s)$ 에 대해서 어떤 상태 s' 에서 $s-$성립하면 S범위내에서 《Q는 P를 엄격히 앞선다.》고 한다.
Q는 P에 응답	P가 어떤 상태 s에서 성립하고 Q도 $b_Q(s') \ge e_p(s)$ 인 어떤 상태 s' 에서 $s-$성립하면 《Q는 P에 응답》은 S범위내에 있다고 한다.

2. CP를 가지는 패턴과 적용범위에 대한 LTL식형타

일반적으로 LTL식 A는 비시간론리식과는 달리 A의 일부 부분식들이 상태 s에서 성립하고 다른 부분식들이 다른 상태에서 성립해도 성립한다.

CP를 포함한 패턴에 대해 A의 여러 부분식이 성립하는 모든 상태들에서 B가 성립한다는것을 담보하는 and연산자를 새로 정의한다.

실례로 새로운 and연산자에 대해 식 $(p_1 \wedge Xp_2)$ and B는 B가 s상태와 $s+1$상태에서 성립한다는것을 의미한다.(LTL식으로 표현하면 $(p_1 \wedge B \wedge X(p_2 \wedge B))$ 이다.) 이와 류사하게 $(p_1 \wedge X <> p_2)$ and B는 B가 s상태와 $s_2 > s$ 상태에서 성립한다는것을 의미한다. 다시말하여 원래 s상태에서 $p_1 \wedge B$ 이여야 하고 어떤 미래의 상태 $s_2 > s$ 에서는 $p_2 \wedge B$ 이여야 한다는것이다.(이것을 LTL로 표현하면 $(p_1 \wedge B) \wedge X <> (p_2 \wedge B)$ 이다.)

LTL연산자 $\wedge$과 and연산을 구별하기 위하여 기호 $\&_r$를 사용하며 그외에 다음과 같은 2개의 연산자를 더 도입한다.

① 새로운 연산 $A \&_l B$ 는 B가 A관련순간의 마지막에 성립한다는것을 의미한다.

② 새로운 연산 $A \&-_l B$ 는 B가 마지막순간을 제외한 모든 A관련순간에서 성립한다는것을 의미한다.

새로운 연산자들을 리용하여 패턴, 적용범위, CP를 조합한 LTL명세서를 작성할수 있는 LTL식형타들을 다음과 같이 정의한다.

① 대역적인 적용범위에 대한 론리식생성형타

② 《R이전》범위에 대한 식생성형타

③ 나머지 적용범위들에 대한 식생성형타

여기서 나머지 적용범위에 대한 식생성형타는 대역적인 형타와 《R이전》형타를 리용한다.

세가지 그룹에 대한 LTL식형타들을 실례를 통하여 보기로 하자.

· 대역적범위내의 LTL식형타의 실례는 패턴 《Q는 P에 응답한다.》에 대한 LTL식형타이다.

$$[](P_{ltl} \rightarrow (P_{ltl} \,\&_l <> Q_{ltl}))$$

· 적용범위 《R이전》내에서 LTL식형타의 실례는 《Q는 R_c이전에 P_c에 앞섬》에 대한 LTL식형타이다.

$$(<> R_{ltl}) \rightarrow ((\neg(P_{lt}^{L} \,\&_r \neg R_{ltl})) \cup ((Q_{ltl} \,\&_{-l} \neg P_{ltl}) \vee R_{ltl}))$$

· 나머지 세가지 적용범위내에 대한 식형타는 대역적인 적용범위와 《R이전》적용범위의 형타에 기초한다.

실례로 적용범위 《L이후》의 식은 《대역적》범위의 식을 리용하여 구성할수 있다.

$$\neg((\neg L_{ltl}) \cup (L_{ltl} \,\&_l \neg P_{ltl}^{G}))$$

이것은 임의의 패턴에 대하여 《L이후》적용범위에 대한 식들은 우의 식을 리용하며 대역범위내의 패턴들에 대한 식들은 항 P_{ltl}^{G}를 치환하는것으로 생성할수 있다는것을 의미한다.

맺 는 말

합성명제를 가지는 패턴에 기초하여 시간속성명세서작성을 지원하는 패턴체계의 정확성을 높이기 위해 합성명제를 파라메터로 가지는 시간속성패턴과 적용범위를 보다 엄밀하게 정의하고 그것에 기초하여 LTL식형타들을 구성하였다.

참 고 문 헌

[1] Marco Autili et al.; IEEE Trans. Software Engineering, **41**, 7, 620, 2015.

[2] John D. Backes et al.; NASA Formal Methods 8th International Symposium, NFM 2016 Minneapolis, 19, 2016.

주체108(2019)년 2월 5일 원고접수

A Method of Supporting Temporal Property Specification for Correctness Verifications

Kim Chol, Sin Chun Ok

In this paper, an approach that supports temporal property specification using pattern system for source code model checking is proposed.

Key words: property specification, temporal logic, pattern-based specification