렬보간법에 기초한 추상화세련화에 의한 검증모형구축

신춘옥, 한은주

모형검사를 비롯한 유한상태검증기술에서는 추상화기술을 적용하여 검증모형을 작성하며 여기서 추상화의 적당한 정밀도를 찾아내는것이 매우 어려운 과제로 나선다.

CEGAR프레임워크[1]는 대략적인 추상화로부터 시작하여 적당한 정밀도를 얻을 때까지 추상화를 반복적으로 세련화하는 일반적인 알고리듬이며 여기에 술어추상화[2]와 값추상화[1]를 비롯하여 여러 추상화방법들을 적용할수 있다.

보간법을 리용하여 추상화를 세련화하는 새로운 술어를 추리할수 있다. 크레이그(Crag)보간법은 하나의 술어를 생성하지만 그것의 확장인 렬보간법은 술어들의 렬을 생성한다.

론문에서는 원천프로그람의 모형검사를 위한 CEGAR프레임워크를 구성하기 위하여 렬보간법으로 추상화세련화를 진행하는 방법을 제안하였다.

1. 렬보간법의 형식적정의

정의 1 기호이행체계 T는 $T=(V, Inv, Tran, Init)$이다. 여기서 $V=\{v_1, v_2, \cdots, v_n\}$은 각각 정의역 $D_{v_1}, D_{v_2}, \cdots, D_{v_n}$을 가지는 변수들의 모임이며 Inv는 V에 관한 불변식이다. 그리고 $Tran$은 $V \cup V'$우에서 정의된 식으로서 현재상태(V)와 계승상태(V')사이의 이행관계이며 $Init$는 초기상태들의 모임을 정의하는 V에 관한 식이다.

정의 2 구체적인 상태이행체계 $Q=(S, S_0, R)$에서 구체적인 상태들의 모임 S, 구체적인 이행들의 모임 R, 구체적인 초기상태들의 모임 S_0을 다음과 같이 정의한다.

① $S=\{s \mid s \models Inv\}$이다. 즉 S는 변수 $v_i \in V$가 불변식 Inv를 만족시키는 모든 가능한 상태(정의역 D_{v_i})를 가질 때 그 매 변수에 값 $s(v_i)=d_i \in D_{v_i}$를 할당하는 다부류해석이다. 즉 값들의 조 $(d_1, d_2, \cdots, d_n)$들의 모임이다.

② $R=\{(s, s') \mid (s, s') \models Inv \wedge Tran \wedge Inv'\}$이다. 즉 S'는 s의 계승상태이다.

③ $S_0=\{s \mid s \models Inv \wedge Init\}$이다. 즉 S_0은 초기의 식이 참인 S의 부분모임이다.

④ 구체적인 경로는 $(s_1, s_2, \cdots, s_n) \models Init_1 \wedge \bigwedge_{1 \le i \le n} Inv_i \wedge \bigwedge_{1 \le i \le n} Tran_{i, i+1}$이 성립하며 유한이고 순환이 없는 구체적인 상태들의 렬 $\sigma=(s_1, s_2, \cdots, s_n)$이다.

하나의 구체적인 상태 s는 어떤 n에 대하여 $s=s_n$인 경로 $\sigma=(s_1, s_2, \cdots, s_n)$이 존재하면 도달가능하다.

V에 관한 1계술어론리식으로 정의되는 안전성속성 φ에 대하여 론의하자. $S_n \not\models \varphi_n$인 경로 $\sigma=(s_1, s_2, \cdots, s_n)$을 반례라고 한다.

술어추상화에서는 1계술어론리식의 모임에 대한 평가에 기초하여 구체적인 상태이행

체계를 추상적인 상태이행체계로 넘긴다.

정의 3 구체적인 상태이행체계 $Q=(S, S_0, R)$에 대하여 술어추상화에 의하여 결정되는 추상적인 상태이행체계 $\overline{Q}=(\overline{S},\overline{S}_0,\overline{R},Label(\overline{s}))$는 다음과 같다.

① 기호이행체계 $T=(V, Inv, Tran, Init)$와 V 우에서의 1계술어들의 모임 P가 주어졌을 때 있을수 있는 $2^{|P|}$개의 추상상태들의 모임을 $\overline{S}$로 표시한다. 추상상태 $\overline{s}\in\overline{S}$를 $Label(\overline{s})=\wedge_{p\in\overline{s}}\ p$로 즉 $\overline{s}$를 술어 혹은 그것의 부정의 론리적으로 표시한다. 구체적인 상태 s를 $s\models Label(\overline{s})$가 성립하도록 추상상태 $\overline{s}$에로 넘긴다.

② 추상이행관계 $\overline{R}=\{(\overline{s},\overline{s}')\in\overline{S}\times\overline{S}\mid\exists s, s'.(s, s')\models Inv\wedge Inv'\wedge Lavel(\overline{s})\wedge Lavel(\overline{s}')'\wedge Tran$이다. 즉 s는 $\overline{s}$로, s'는 $\overline{s}'$에로 넘기는 구체적인 계승상태의 이행관계 (s,s')가 존재한다.

③ 추상적인 초기상태들의 모임 $\overline{S}_0=\{\overline{s}\in\overline{S}\mid\exists s.s\models Inv\wedge Init\wedge Lavel(\overline{s})\}$이다. 즉 $\overline{s}$에로 넘어가는 구체적인 초기상태 s가 존재한다.

④ 추상경로는 $\overline{s}_1\in S_0$이고 $(\overline{s}_i, \overline{s}_{i+1})\in\overline{R}(1\le i<n)$인 유한이며 비순환인 추상상태들의 렬 $\overline{\sigma}=(\overline{s}_1, \overline{s}_2, \cdots, \overline{s}_n)$이다.

추상경로 $\overline{\sigma}=(\overline{s}_1, \overline{s}_2, \cdots, \overline{s}_n)$에 대하여

$$(s_1, s_2, \cdots, s_n)\models Init_1\wedge\wedge_{1\le i\le n} Label(\overline{s}_i)_i\wedge\wedge_{1\le i\le n} Inv_i\wedge\wedge_{1\le i\le n} Tran_{i,\,i+1}$$

인 상태들의 렬 $\sigma=(s_1, s_2, \cdots, s_n)$이 존재할 때 구체화할수 있다.

정의 4 $\psi_1, \psi_2, \cdots, \psi_n$은 $\psi_1\wedge\psi_2\wedge\cdots\wedge\psi_n$이 충족불가능한 1계론리식들의 렬이라고 할 때 다음의 성질이 성립하는 식들의 렬 $I_0, I_1, \cdots, I_n$은 $\psi_1, \psi_2, \cdots, \psi_n$에 대한 보간렬이다.

① $I_0=\top$, $I_n=\bot$

② $I_j\wedge\psi_{j+1}$은 $0\le j<n$에 대하여 I_{j+1}을 암시한다.

③ I_j는 $0<j<n$에 대하여 $\psi_1, \psi_2, \cdots, \psi_j$와 $\psi_{n+1}, \cdots, \psi_n$에서 공통인 기호들만을 포함한다.(론리연산기호들을 제외한다.)

2. 렬보간법에 기초한 추상화세련화

이행체계의 모형검사를 위한 CEGAR알고리듬에서 초기추상화, 모형검사, 반례의 구체화와 추상화세련화를 다음과 같이 구성한다.

① 초기추상화

초기추상화단계에서는 값추상화에서의 값할당으로 하여 성립하는 등식들을 술어로 보고 술어추상화에서의 술어모임에 포함시켜 추상화를 진행한다.

$T=(V, Inv, Tran, Init)$는 변수 $V=\{v_1, v_2, \cdots, v_n\}$을 가지는 기호이행체계, P는 V우에서의 1계술어들의 모임, $V_E\subseteq V$를 명백한 값변수들의 모임이라고 하자. 그리고 이 변수들은 m까지의 첨수($0\le m\le n$)들에 의하여 표시된다. 즉 $V_E=\{v_1, v_2, \cdots, v_m\}$이라고 가정한다.

추상상태 $\overline{s}\in\overline{S}$는 술어들의 모임으로서 다음과 같이 정의한다.

· 매 $p_i\in P$에 대하여 $\overline{s}$는 p_i 혹은 $\neg p_i$를 포함한다.

· 매 $v_i \in V_E$에 대하여 $\bar{s}$는 $v_i = \bar{s}(v_i)$형태의 술어를 포함한다. 따라서 $\bar{S}$는

$$|\bar{S}| = 2^{|p|} \cdot |D_{v_1}| \cdot D_{v_2}| \cdot \cdots \cdot |D_{v_m}|$$

개의 추상상태를 가질수 있다.

추상관계 $\bar{R}$와 초기상태 $\bar{S}_0$도 술어추상화와 류사하게 계산한다.

② 모형검사

추상상태 $\bar{s} \in \bar{S}$는 $Label(\bar{s}) \wedge Inv \wedge \neg \varphi$가 충족가능할 때 안전성속성 φ를 위반한다. 즉 $\bar{s}$에 넘어가면서 φ를 위반하는 구체적인 상태가 존재하면 안전성속성을 위반한다. 추상이행체계에 대한 모형검사는 φ를 위반하는 추상상태가 도달가능한가 즉 $\bar{s}_n = \bar{s}$인 추상경로 $\bar{\sigma} = (\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_n)$가 존재하는가를 검사한다.

③ 반례의 구체화

안전성속성 φ에 대한 추상경로 $\bar{\sigma} = (\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_n)$는

$$(s_1, s_2, \cdots, s_n) \models Init_1 \wedge \bigwedge_{1 \le i \le n} Label(\bar{s}_i)_i \wedge \bigwedge_{1 \le i \le n} Inv_i \wedge \bigwedge_{1 \le i \le n} Tran_{i,\, i+1} \wedge \neg \varphi_n$$

이 성립하는 상태들의 렬 $\sigma = (s_1, s_2, \cdots, s_n)$이 존재하면 구체화할수 있다. 구체화가 가능한 반례는 구체적인 모형도 요구를 위반한다는 증거로 되며 구체화가 불가능한 반례를 가짜반례라고 한다.

모형검사에서 가짜반례가 다시 출력되는것을 막기 위하여 추상화를 세련화한다.

주어진 반례의 가장 긴 접두사는 세련화에 대하여 필요한 정보를 제공하므로 추상화반례

$$\bar{\varphi} = (\bar{s}_1, \bar{s}_2, \cdots, \bar{s}_n)$$

를 다음의 $n+1$개의 식으로 반복적으로 구체화한다.

$$F_i = \begin{cases} Init_1 \wedge Inv_1 \wedge Lavel(\bar{s}_1)_1, & i = 1\text{일 때} \\ Inv_i \wedge Lavel(\bar{s}_i)_i \wedge Tran_{i-1,\, i}, & 1 < i \le n\text{일 때} \\ \neg \varphi_n, & i = n+1\text{일 때} \end{cases}$$

$F_1 \wedge F_2 \wedge \cdots \wedge F_n$은 $\bar{\sigma}$로 넘겨진 구체적인 경로를 서술하며 F_{n+1}은 마지막상태가 그 속성을 위반한다는것을 담보한다. $F_1 \wedge F_2 \wedge \cdots \wedge F_{n+1}$이 충족가능하면 반례는 구체화가 가능하다.

$f\,(1 \le f \le n)$가 $F_1 \wedge F_2 \wedge \cdots \wedge F_f$를 충족시키는 가장 큰 첨수라고 하면 상태 $\bar{s}_f$를 실패상태라고 한다.

④ 추상화세련화

실패상태 $\bar{s}_f$에로 넘겨지는 구체적인 상태들의 모임을 초기상태로부터 도달할수 있는 상태(막힌 상태), $\bar{s}_{f+1}$에로의 이행을 가지거나 φ를 위반하는 상태(나쁜 상태), 그외 무관계한 상태들로 분할한다.

추상화세련화의 목표는 막힌 상태와 나쁜 상태들을 서로 다른 추상상태로 넘겨 가짜반례가 다음번 반복에서 발생하지 않도록 하는것이다. 추상화를 세련화하는 새로운 술어를 추리하는데 렬보간법을 리용한다.

렬보간법에서 $\psi_1, \psi_2, \cdots, \psi_{n+1}$을 다음과 같이 정의한다.

$$\psi_i = \begin{cases} Init_1 \wedge Inv_1 \wedge Lavel(\bar{s}_1)_1, & i=1\text{일 때} \\ Inv_i \wedge Lavel(\bar{s}_i)_i \wedge Trans_{i-1,i}, & 1<i<n\text{일 때} \\ \neg\varphi_n, & i=n+1\text{일 때} \end{cases}$$

여기서 식 ψ_1은 $\bar{s}_1$에 대응하는 초기상태를 서술하며 $\psi_2, \cdots, \psi_n$은 각각 $\bar{s}_2, \cdots, \bar{s}_n$에 대응하는 도달가능한 상태들, ψ_{n+1}은 안전성속성을 위반하는 상태들을 서술한다.

$\psi_1 \wedge \psi_2 \wedge \cdots \wedge \psi_{n+1}$은 충족불가능하며 $\bar{\sigma}$는 가짜반례이므로 안전성속성을 위반한다.

이로부터 다음과 같은 성질을 가지는 보간렬 $I_0, I_1, \cdots, I_{n+1}$이 존재한다.

· $I_0 = \mathsf{T}, I_{n+1} = \perp$이다. 즉 반례에서 어떤 상태에 해당하지 않는 보간식은 정보를 포함하지 않는다.

· $0 \le j \le n$인 j에 대하여 $I_j \wedge \psi_{j+1} \rightarrow I_{j+1}$이다. 즉 보간식은 막힌 상태와 나쁜 상태들을 함께 일반화한다.

· I_j는 $\psi_1, \psi_2, \cdots, \psi_j$와 $\psi_{j+1}, \cdots, \psi_{n+1}$의 공통기호들 즉 첨수 j를 가지는 변수들만을 참조한다.

추상화는 매 $\bar{s}_i (1 \le i \le n)$를 $\bar{s}_i$의 술어에 I_i와 $\neg I_i$를 보충하여 얻어진 $\bar{s}_{i_1}$와 $\bar{s}_{i_2}$를 교체하는 방법으로 세련화한다. 즉 $\bar{s}_{i_1} = \bar{s}_i \cup \{I_i\}$이고 $\bar{s}_{i_2} = \bar{s}_i \cup \{\neg I_i\}$이다. $1 \le i \le n$인 어떤 i에 대하여 $I_i = \top$ 혹은 $I_i = \perp$가 발생할수 있다. 이 경우에 대응하는 추상상태 $\bar{s}_i$는 분할되지 않는다.

크레이그보간법은 세련화의 매 걸음에서 하나의 추상상태를 분할하지만 렬보간법은 매 걸음에서 여러 상태를 분할하므로 적은 회수의 세련화반복으로 보다 많은 가짜동작들을 소거할수 있다. 렬보간법은 크레이그보간법에 비하여 보다 단순한 보간식들을 생성한다.

맺 는 말

초기의 추상화단계에서 술어추상화와 값추상화를 조합하며 렬보간법을 리용하여 추상화세련화를 진행하는 CEGAR프레임워크의 구성을 제안하였다.

참 고 문 헌

[1] D. Beyer, S. Lowe; 10th International Conference on Formal Aspects of Software Engineering, FASE, 146, 2013.

[2] Tuva Yavuz; 14th International Conference on Software Engineering and Formal Method SEFM 104, 2016.

주체108(2019)년 2월 5일 원고접수

Construction of Verification Model by Sequence Interpolation-based Abstraction Refinement

Sin Chun Ok, Han Un Ju

This paper proposed a research on a configuration of CEGAR framework, to which we extended predicate abstraction in first stage of the algorithm and applied sequence interpolation in abstraction refinement stage.

Key words: model checking, abstraction refinement, predicate abstraction