추상령역의 직적에서 상한산법구성의 한가지 방법

김태웅, 조철만

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.》

우리는 프로그람의 수값적성질검증을 위한 방법의 하나인 추상해석에 대한 리론연구를 심화시켜 추상령역의 직적에서 선행한 방법보다 정확한 상한산법을 구성하는 방법에 대하여 연구하였다.

선행연구[1, 3]에서는 추상령역들의 직적으로 이루어진 령역에서의 상한산법구성방법을 내놓았으나 련관정보를 반영하지 않은것으로 하여 정확성이 보장되지 못하였다.

선행연구[2]에서는 특수한 경우로서 구간추상령역과 그라프에 기초한 추상령역과의 직적으로 이루어진 령역에서 련관정보를 반영하여 상한산법의 정확성을 높이기 위한 방법에 대하여 연구하였다.

론문에서는 련관이 있는 추상령역들의 직적으로 이루어진 령역에서 련관정보를 반영하여 상한산법을 구성하기 위한 한가지 방법에 대하여 연구하였다.

추상령역우에서 상한산법은 다음과 같이 정의한다.

정의 1[1](추상령역우에서의 상한산법) 추상령역 $D^{\#}$이 구체화령역 D^{b}와 갈롸련결 (α, γ)가 존재하고 $D^{\#}$ 우에서의 산법 $\cup^{\#}$이 정의되여있다고 하자. 이때 조건 $\forall x_1^{\#}, x_2^{\#} \in D^{\#}$, $\gamma(x_1^{\#}) \cup \gamma(x_2^{\#}) \subseteq \gamma(x_1^{\#} \cup^{\#} x_2^{\#})$를 만족시킬 때 $\cup^{\#}$를 추상령역 $D^{\#}$에서의 상한산법이라고 부른다.

정의로부터 알수 있는것처럼 추상령역에는 상한산법들이 여러가지로 구성될수 있다.

같은 추상령역우에서 구성된 두 상한산법들의 정확성은 다음과 같이 비교한다.

정의 2[1](추상령역우에서의 상한산법의 정확성) 추상령역 $D^{\#}$ 우에서 두 상한산법 $\cup_1^{\#}, \cup_2^{\#}$이 정의되여있다고 하자.

$$\forall x_1^{\#},\ x_2^{\#} \in D^{\#},\ \gamma(x_1^{\#} \cup_1^{\#} x_2^{\#}) \subseteq \gamma(x_1^{\#} \cup_2^{\#} x_2^{\#})$$

이 성립하면 $\cup_1^{\#}$는 $\cup_2^{\#}$보다 더 정확하다고 말한다.

특히 $\gamma(x_1^{\#}) \cup \gamma(x_2^{\#}) = \gamma(x_1^{\#} \cup_1^{\#} x_2^{\#})$일 때 $\cup_1^{\#}$를 가장 정확한 상한산법이라고 부른다.

선행연구에서 밝힌 추상령역의 직적우에서 상한산법구성방법은 다음과 같다.

추상령역 $D^{\#} = D_1^{\#} \times D_2^{\#}$에서 반순서관계 $\subseteq_{1\times 2}$는 다음과 같이 정의하였다.

$$(i_1,\ f_1) \subseteq_{1\times 2} (i_2,\ f_2) := (i_1 \subseteq_1 i_2,\ f_1 \subseteq_2 f_2)$$

구체화넘기기와 추상화넘기기는 개개의 구체화 및 추상화넘기기들에 기초하여 다음과 같이 정의하였다.

$$\alpha_{1\times 2}(i,\ f) := (\alpha_1(i),\ \alpha_2(f))$$
$$\gamma_{1\times 2}(i,\ f) := \gamma_1(i) \cap \gamma_2(f)$$

α_1, α_2가 단조이므로 넘기기 $\alpha_{1\times 2}$도 우에서 정의된 반순서관계에 의하여 단조인 넘기기이다. γ_1, γ_2가 단조이므로 넘기기 $\gamma_{1\times 2}$도 단조인 넘기기이다.

추상령역의 직적으로 얻어진 추상령역에서 두 원소의 상한, 하한산법은 다음과 같이 정의하였다.

$$(i_1,\ f_1)\bigcup_{1\times 2}(i_2,\ f_2) := (i_1 \bigcup_1 i_2,\ f_1 \bigcup_2 f_2)$$
$$(i_1,\ f_1)\bigcap_{1\times 2}(i_2,\ f_2) := (i_1 \bigcap_1 i_2,\ f_1 \bigcap_2 f_2)$$

선행한 상한산법은 두 추상령역을 독립적으로 취급하므로 련관정보를 전혀 반영하지 않은것으로 하여 해석에서 정확성이 떨어진다.

다음의 실례는 추상령역의 직적으로 이루어진 령역에서 선행한 상한산법에 의한 해석은 정확성이 떨어진다는것을 보여준다.

실례 1 선행한 방법으로 다음과 같은 프로그람을 해석해보자.

① if (…)

② {x=1; y=3;}

else

③ {x=0; y=1;}

우와 같은 프로그람을 변수들의 크기관계를 고려한 추상령역에 의하여 해석을 진행해보자.

②행이 끝나는 위치에서

$$(i,\ f) = (i[x \to 1,\ y \to 3],\ \lambda x.\emptyset)$$

이고 ③행이 끝나는 위치에서는

$$(i,\ f) = (i[x \to 0,\ y \to 1],\ \lambda x.\emptyset)$$

이다. 그러면 마지막위치에서는

$$(i,\ f) = (i[x \to [0,\ 1],\ y \to [1,\ 3]],\ \lambda x.\emptyset)$$

이다. $x = y = 1$인 경우가 없다는것을 선행한 상한산법만으로는 증명할수 없다.

추상령역의 직적에서 새로운 상한구성방법은 다음과 같다.

넘기기 $\rho : {D_1}^{\#} \times {D_2}^{\#} \to {D_1}^{\#} \times {D_2}^{\#}$가 다음의 조건을 만족시킨다고 하자.

$(d_1',\ d_2') = \rho((d_1,\ d_2))$라고 할 때

$$d_1' \subseteq_1^{\#} d_1,\ d_2' \subseteq_2^{\#} d_2,\ \gamma_1(d_1)\bigcap\gamma_2(d_2) = \gamma_1(d_1')\bigcap\gamma_2(d_2') \qquad (*)$$

이다. 추상령역의 직적으로 이루어진 령역에서 조건 (1)을 만족시키는 넘기기는 늘 존재한다. 실례로 추상령역의 직적으로 이루어진 임의의 령역에서 넘기기 $\alpha_{1\times 2}\circ\gamma_{1\times 2}$는 식 (1)을 만족시킨다.

우와 같은 넘기기 ρ를 생각하자. 그리고 추상령역 $D^{\#}$우에서의 상한산법 $\bigcup'_{1\times 2}$를 다음과 같이 구성한다.

$$(d_{11},\ d_{12})\bigcup'_{1\times 2}(d_{21},\ d_{22}) := (d'_{11} \bigcup_1 d'_{21},\ d'_{12} \bigcup_2 d'_{22})$$

여기서

$$(d'_{11},\ d'_{12}) = \rho(d_{11},\ d_{12}),\ (d'_{21},\ d'_{22}) = \rho(d_{21},\ d_{22})$$

이다.

정리

$$(\gamma_{1\times 2}(i_1,\ f_1)\bigcup\gamma_{1\times 2}(i_2,\ f_2)) \subseteq \gamma_{1\times 2}((i_1,\ f_1)\bigcup'_{1\times 2}(i_2,\ f_2)) \subseteq \gamma_{1\times 2}((i_1,\ f_1)\bigcup_{1\times 2}(i_2,\ f_2))$$

증명 넘기기 ρ의 성질로부터

$$(i_1',\ f_1')\bigcup_{1\times 2}(i_2',\ f_2')\subseteq_{1\times 2}(i_1,\ f_1)\bigcup_{1\times 2}(i_2,\ f_2)$$

이고 $\gamma_{1\times 2}$의 단조성으로부터

$$\gamma_{1\times 2}((i_1',\ f_1')\bigcup_{1\times 2}(i_2',\ f_2'))\subseteq^{b}\gamma_{1\times 2}((i_1,\ f_1)\bigcup_{1\times 2}(i_2,\ f_2))$$

이다. 또한

$$\gamma_{1\times 2}(i_1',\ f_1')\bigcup\gamma_{1\times 2}(i_2',\ f_2')=\gamma_{1\times 2}(i_1,\ f_1)\bigcup\gamma_{1\times 2}(i_2,\ f_2)$$

이고 $\bigcup_{1\times 2}$의 정의로부터

$$\gamma_{1\times 2}((i_1,\ f_1)\bigcup'_{1\times 2}(i_2,\ f_2))=\gamma_{1\times 2}(i_1',\ f_1')\bigcup\gamma_{1\times 2}(i_2',\ f_2')\subseteq\gamma_{1\times 2}((i_1',\ f_1')\bigcup_{1\times 2}(i_2',\ f_2'))$$

이므로

$$(\gamma_{1\times 2}(i_1,\ f_1)\bigcup\gamma_{1\times 2}(i_2,\ f_2))\subseteq\gamma_{1\times 2}((i_1',\ f_1')\bigcup_{1\times 2}(i_2',\ f_2'))$$

이다.(증명끝)

정리에서는 새롭게 구성한 산법이 추상령역의 직적으로 이루어진 령역우에서의 상한산법으로 되며 선행한 산법보다 정확하다는것을 보여주고있다.

변수들의 크기관계를 고려한 추상령역에서 우의 방법을 리용하여 상한산법을 새로 구성해보겠다.

변수들의 관계를 고려한 추상령역은 다음과 같이 구성된다.

$$D_1^{\#}=\{f\mid f:V\to Int\}$$

$$D_2^{\#}=\{f\mid f:V\to P(V)\}$$

$$D^{\#}=D_1^{\#}\times D_2^{\#}$$

명제 변수들사이의 크기관계를 고려한 추상령역에서 다음과 같이 정의되는 넘기기 ρ는 식 (∗)을 만족시킨다.

$$\rho:D_1^{\#}\times D_2^{\#}\to D_1^{\#}\times D_2^{\#}$$

$$(i,\ f)\mapsto(i',\ f')$$

여기서

$$i':x\mapsto\bigcap_{y\in f(x)}[\mid x<y\mid]i$$

$$f':x\mapsto f(x)\bigcup\{y\mid y\neq x,\ \sup(i(x))<\inf(i(y))\}$$

증명 i', f'의 정의와 추상령역들에서의 반순서관계에 의하여 다음과 같은 결과가 성립한다.

$$i'\subseteq_1 i,\ f'\subseteq_2 f$$

$$\gamma(i')\subseteq\gamma(i),\ \gamma(f')\subseteq\gamma(f)$$

이므로

$$\gamma(i')\bigcap\gamma(f')\subseteq\gamma(i)\bigcap\gamma(f)$$

이다. 또한 $\forall d\in\gamma(i)\bigcap\gamma(f)$에 대하여 $d\in\gamma(f)$이면 $\forall v\in V$에 대하여 $d(v)<d(f(v))$이므로 $d\in\gamma(i')$이다.

$$d\in\gamma(i)\Rightarrow\forall v_0\in V,\ V_1:=\{v\mid v\neq v_1,\ \sup(i(v_0))<\inf(i(v))\}$$

라고 하면 갈롸련결의 성질에 의하여 $\forall v\in V_1.d(v_0)<d(v)$이다.(증명끝)

아래의 실례는 변수들사이의 크기관계를 고려한 추상령역에서 새롭게 구성한 상한산

법이 선행한 상한산법보다 정확하다는것을 보여준다.

실례 2 새롭게 구성한 상한산법에 의하여 우에서 해석한 프로그람을 다시 해석해보자.

① if (…)

② {x=1; y=3;}

else

③ {x=0; y=1;}

②행이 끝나는 위치에서

$$(i_1,\ f_1) = (i[x \to 1,\ y \to 3],\ \lambda x.\emptyset)$$

$$(i_1',\ f_1') = \rho(i_1,\ f_1) = (i[x \to 1,\ y \to 3],\ f[x \to y,\ y \to \emptyset])$$

이고 ③행이 끝나는 위치에서는

$$(i_2,\ f_2) = (i[x \to 0,\ y \to 1],\ \lambda x.\emptyset)$$

$$(i_2',\ f_2') = \rho(i_2,\ f_2) = (i[x \to 0,\ y \to 1],\ f[x \to y,\ y \to \emptyset])$$

이다. 따라서 마지막위치에서는

$$(i,\ f) = (i[x \to [0,\ 1]],\ f[x \to y,\ y \to \emptyset])$$

이다. 즉 $x = y = 1$인 경우는 있을수 없다.

결국 새롭게 구성한 상한산법으로 하여 해석의 정확성이 높아진다는것을 보여준다.

참 고 문 헌

[1] P. Le Roux et al.; Electronic Notes in Theoretical Computer Science, **267**, 73, 2010.

[2] M. Maalej et al.; Science of Computer Programming, **152**, 161, 2017.

[3] I. Mariuca et al.; Electronic Notes in Theoretical Computer Science, **307**, 33, 2014.

주체108(2019)년 9월 15일 원고접수

A Method for Constructing a Least Upper Bound Operator over the Product of Abstract Domains

Kim Thae Ung, Jo Chol Man

In this paper, we introduce a new method to improve exactitude of precise abstraction operator over the product of abstract domains.

Keywords: abstraction operator, product of abstract domains