平成20年度 情報工学コース卒業研究報告要旨

坂部 研究室	氏　　名	馬 場 達 也
卒業研究題目	プログラムの述語抽象化におけるループ不変式の利用について	

プログラムの述語抽象化とは，モデル検査に基づくプログラム検証において，プログラムを抽象化してラベル付き状態遷移系（LTS）を得る手法の一つであり，得られるLTSは述語抽象化モデル（$\mathcal{MP}$）と呼ばれる．CMUのグループで開発されているプログラム検証システムMAGICでは，プログラムCが仕様$Spec$を満たすことの検証は次のように進められる．

$$\mathrm{C} \rightarrow \mathrm{CFG} \rightarrow \mathcal{MP} \rightarrow \mathcal{MA} \Leftrightarrow Spec$$

まず，プログラムCから流れ図CFG（Control Flow Graph）を作成し，CFGから述語抽象化により$\mathcal{MP}$を得る．$\mathcal{MP}$からさらにもう一段抽象化したモデル$\mathcal{MA}$を構成する．次に，モデル検査手法により$\mathcal{MA}$が$Spec$を満たすことを検証する．成功すればCは$Spec$を満たすとして終了する．真の反例が得られたときはCは$Spec$を満たさないとして終了する．偽の反例が得られたときは，偽の反例を除外するように$\mathcal{MP}$を再構成し，以下は同じことを繰り返す．このような検証が成功するには，述語抽象化モデルの状態数を抑えることが鍵となっている．

本論文の目的は，CFGから$\mathcal{MP}$を得る過程でプログラムのループ不変式を利用することにより，$\mathcal{MP}$の状態数削減にどのような効果があるかを明らかにすることである．

MAGICではCFGから$\mathcal{MP}$を構成するとき，CFGの各頂点sに，プログラム中の条件式として出現する述語からなる集合$\mathcal{P}_s$を割り当てる．プログラム中にループがあるとき，そのループ中の頂点に割り当てられる述語集合のサイズは限りなく大きくなるため，MAGICでは適当な上限を定めて，途中で打ち切る．$\mathcal{MP}$の状態として，CFGの各頂点sに対して$2^{|\mathcal{P}_s|}$個の状態が作られる．このため，$\mathcal{P}_s$の大きさを抑えることができれば，$\mathcal{MP}$の状態数を削減できる．

本論文では，扱うプログラムを逐次的なプログラムに限定し，プログラムの一部のループにループ不変式が与えられていると仮定する．これらの仮定の下で，ループ不変式を用いてCFGから述語抽象化モデル$\mathcal{MP}_{inv}$を構成するアルゴリズムを提案する．そのアルゴリズムでは，ループ不変式pが与えられたループ中の各頂点sに対しては述語の集合のサイズは高々ループ中に現れる条件式の数とし，ループヘッドの頂点はそれにpを加える．このとき，$\mathcal{MP}_{inv}$は次のような性質を持つことを示す．

1. MAGICの$\mathcal{MP}$から$\mathcal{MP}_{inv}$への準同型写像が存在する．
2. すべてのループ不変式を自明なループ不変式$TRUE$としたときの述語抽象化モデルを$\mathcal{MP}_{TRUE}$とすると，$\mathcal{MP}_{TRUE}$と$\mathcal{MP}_{inv}$は同型となる．

性質1は，$\mathcal{MP}_{inv}$をMAGICの$\mathcal{MP}$の代わりに用いてもよいこと，また，$\mathcal{MP}$より$\mathcal{MP}_{inv}$の方が状態数が少ないことを意味する．性質2は，$\mathcal{MP}_{inv}$の構造はループ不変式の与え方に依存しないことを意味するが，各状態に付随する述語集合に依存しているMAGICの後段では$\mathcal{MP}_{inv}$の方が有効であると予想される．