

平成 19 年度 情報工学コース卒業研究報告要旨

坂部 研究室	氏 名	石 垣 達 也
卒業研究題目	手続き型プログラムから 書換え系への変換における プログラムの微差の吸収に関する研究	
<p>手続き型プログラムの主な検証手法として、モデル検査やホーア論理に基づく手法がある。これらの手法では、ループ不変式の発見は原理的に不可能であることや、事前条件、事後条件は人が与える必要があるなど、検証の自動化は困難である。一方、関数型プログラムに対する検証法として、潜在帰納法や書換え帰納法などの自動証明手法が広く研究されている。また、最近、手続き型プログラムをそれと等価な制約付き TRS に変換し、潜在帰納法を利用して検証を行う手法も提案された。この手法では、制約付き TRS の完備化手続きを、変換によって生成した制約付き TRS に適用することで、仕様として与えられた制約付き TRS との等価性を検証する。しかし、多くの場合で、完備化が成功するためには、証明に必要な補題等式を発見的に与える必要があり、検証には高いコストを要する。この手法での証明の戦略を開発するために行われた検証実験では、同じ仕様に沿ったプログラムと仕様として与えられた制約付き TRS の等価性が検証された。しかし、変換対象の手続き型プログラムには、<code>return</code> 文は関数の末尾にのみ記述されるという構文上の制約が存在したため、実際に変換できたプログラムは少なかった。一方で、変換に成功したプログラムは、制御文の構造によって 3 種類の制約付き TRS に大別された。</p> <p>本研究では、構文上に違いがあっても本質的に等しいプログラムを、等しい制約付き TRS に変換することで、同じ仕様に沿って作られた複数のプログラムの検証の効率化を目指す。複数の手続き型プログラムの等価性を検証する際には、それらから変換で生成された制約付き TRS の種類の数だけ完備化を行う必要がある。しかし、先に述べたように、この完備化手続きは検証に掛かるコストの大部分を占める。ここで、等しい制約付き TRS を、各規則の両辺が構文的に等価であるとする、等しい制約付き TRS に変換できた手続き型プログラムは当然等しく、この場合は完備化手続きによる等価性検証は不要である。従って、変換による手続き型プログラムの差の吸収は、等価性検証全体のコストの低下を期待できる。</p> <p>本研究ではまず、制約付き TRS に変換可能な手続き型プログラムの構文の制約を緩和した。前述の検証実験で変換できなかったプログラムは、その大部分が <code>return</code> 文の位置に関する構文上の制約が原因であった。よって、この制約を取り除いた手続き型プログラムの構文と意味論を再定義した。そして、新たな構文上のプログラムを変換できるよう変換アルゴリズムを改良し、変換実験を行った。等価な手続き型プログラムでは、制御構造は 2, 3 種類に大別できるが、ループの初期値 (0 か 1) や条件分岐の条件 ($>$ か \geq) という違いがあると、本質的な意味の評価が等しいにもかかわらず、変換後の制約付き TRS にこの差は影響した。</p> <p>本研究では次に、手続き型プログラムを制約付き TRS へ変換する際に、手続き型プログラムの微差を吸収するように変換アルゴリズムを改良した。この改良により、これまでの変換では別の制約付き TRS へと変換されていた手続き型プログラムの一部を、等しい制約付き TRS へと変換できた。また、ループの構造に関して別の改良方法も実現し、これらの改良方法が効果的である制御構造について考察した。</p>		