# 平成23年度 情報工学コース卒業研究報告要旨

| 酒井 研究室 | 氏　　名 | 坂 井　利 光 |
|---|---|---|
| 卒業研究題目 | 語問題を基底等式集合の語問題に帰着可能な等式集合のクラスに関する研究 | |

形式的手法を用いた検証に関する研究が活発になされており，そのような検証を行うツールとして，特定の理論のもとで充足可能性を判定するSMTソルバがある．システム検証においては，システムの仕様や挙動は等式によって定められていることが多いため，多くのSMTソルバには等式理論を扱うためのモジュールが組み込まれている．等式理論の重要な問題として，2つの項を与えたときに等式集合のもとで2つの項が等しいかどうかを決定する問題である語問題がある．いくつかのSMTソルバには，基底等式集合（変数を持たない等式の集合）の語問題に対する決定手続きとして，高速な合同閉包（Congruence Closure）アルゴリズムが組み込まれている．語問題を解く手続きは頻繁に呼び出されるため重要であるが，合同閉包アルゴリズムは基底等式集合の語問題にしか用いることができない．

本研究では，合同閉包アルゴリズムを用いることが可能な等式集合のクラスを発見することを目的とし，基底等式集合より大きなクラスである線形，シャロー，変数非消去かつ非崩壊な等式集合の語問題を，基底等式集合の語問題に帰着可能であることを示す．

まずはじめに，等式集合の語問題に対する変換を定義し，線形，シャロー，変数非消去かつ非崩壊な等式集合の語問題を基底等式集合の語問題に変換する．線形，シャロー，変数非消去かつ非崩壊な等式集合は一般に変数を含んでいるため，基底等式集合に変換する際に無限集合になってしまう．そこで，ある観測に基づき変換する基底等式集合を有限に抑える．

つぎに，変換を適用して作成された基底等式集合の語問題が，変換を適用する前の線形，シャロー，変数非消去かつ非崩壊な等式集合の語問題と等価であることを示す．しかし，そのままでは書換えの順序に関する問題が発生する．変換前の等式集合のもとでは等しかった2つの項が，変換後の等式集合のもとでは書換えの順序に起因して等しくならない書換え系列になってしまうという問題である．そこで，線形，シャロー，変数非消去かつ非崩壊な等式集合においては順序を意図的に制限した書換え系列を必ず得ることができるということを示すことで，この困難性に対処する．

これにより．基底等式集合より大きなクラスである線形，シャロー，変数非消去かつ非崩壊な等式集合の語問題を，基底等式集合の語問題に帰着可能であることを示す．この結果から，変換を用いることで線形，シャロー，変数非消去かつ非崩壊な等式集合の語問題に対して合同閉包アルゴリズムが利用することができ，このクラスの語問題を高速に解くことができる可能性がある．

本研究で定義した変換は未実装であるため，実際に線形，シャロー，変数非消去かつ非崩壊な等式集合の語問題を高速に解くことができるかどうかは不明である．したがって，変換を実装し実験することは今後の課題である．また，基底等式集合の語問題に帰着可能であるより大きなクラスを発見することも課題である．