社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
MSS2011-62 SS2011-47 (2012-1)

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ついて

坂井　利光† 　酒井　正彦†† 　坂部　俊樹†† 　西田　直樹†† 　草刈圭一朗††

† 名古屋大学　工学部　電気電子・情報工学科
〒 464–8603 名古屋市千種区不老町
†† 名古屋大学大学院 情報科学研究科
〒 464–8603 名古屋市千種区不老町
E-mail: †toshimitsu@trs.cm.is.nagoya-u.ac.jp, ††{sakai,sakabe,nishida,kusakari}@is.nagoya-u.ac.jp

あらまし　等式集合の語問題は，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．本論文では線形，シャロー，変数非消去かつ非崩壊な規則からなる等式集合の語問題が，等式集合と2つの項から定められる基底項を各等式に代入する変換を用いることにより，変数を持たない等式集合の語問題へ帰着可能であることを示す．この結果より，変数を持たない等式集合の語問題判定アルゴリズムを用いて，目的の語問題を解くことが可能となる．

キーワード　等式理論，語問題，合同閉包

On class of equation sets whose word problems are reducible to those of ground equation sets

Toshimitsu SAKAI†, Masahiko SAKAI††, Toshiki SAKABE††,
Naoki NISHIDA††, and Keiichirou KUSAKARI††

† Department of Information Engineering, School of Engineering, Nagoya University
Furo-cho, Chikusa-ku, Nagoya, 464–8603
†† Graduate School of Information Science, Nagoya University
Furo-cho, Chikusa-ku, Nagoya, 464–8603
E-mail: †toshimitsu@trs.cm.is.nagoya-u.ac.jp, ††{sakai,sakabe,nishida,kusakari}@is.nagoya-u.ac.jp

Abstract　The word problem of an equation set is to decide, given two terms, whether the two terms are equivalent under the equations. In this paper, we show that word problems of linear, shallow, non-erasing and non-collapsing equation sets are reducible to those of equation sets having no variables, where we use a transformation that substitutes ground terms determined from the equation set and the given two terms into each equation. This result allows us to use decision algorithms for the word problem of an equation set without variables to solve the target problem.

Key words　equational theory, word problem, congruence closure

1. はじめに

近年，ソフトウェアやハードウェアのシステム検証に関する議論が盛んである．その中でも特に，命題論理式の充足可能性を判定するSATソルバや，特定の理論において論理式の充足可能性を判定するSMTソルバを用いて検証を行う形式的証明手法についての関心が高まっている．システム検証において，システムの仕様や挙動は等式によって定められているが多い．したがって，検証を行うには，等式を推論する必要がある．またシステム検証だけでなく，関数型プログラミングにおいても，その意味論は等式に基づいて与えられているため，プログラミング検証にも等式推論は必要である．

そのような等式推論の問題として，等式集合の語問題がある．等式集合の語問題とは，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という問題である．しかし一般には，語問題は決定不能な問題として知られている．したがって，語問題が決定可能であるようなクラスが研究されている．そのようなクラスとして，等式集合が基底等式集合，すなわち変数を持たない等式の集合が知られている [1].

基底等式集合の語問題に対しては，高速な合同閉包（Congruence Closure）アルゴリズム [3], [5], [7], [8] を用いた効率的な決定手続きが存在する．例えば Barcelogic [6] などのいくつかの SMT ソルバでは，等式理論を扱うためにこの合同閉包アルゴリズムが実装されている．しかし，この方法は基底等式集合に対してしか用いることができないため，基底等式集合よりも大きなクラスの語問題を，基底等式集合の語問題に帰着することが可能であれば，高速な合同閉包アルゴリズムを用いて効率的に等式推論を行うことができる可能性がある．

本論文では語問題を解くことができる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発見することを目的とし，基底等式集合よりも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．

例として，規則 $f(x,a) \approx g(x,b)$ からなる等式集合 E において，$f(g(a,b),a) \overset{*}{\leftrightarrow}_E g(f(a,a),b)$ が成立するかを考える．実際には，$f(g(a,b),a) \leftrightarrow_E g(g(a,b),b) \leftrightarrow_E g(f(a,a),b)$ であり成立するが，各書換えにおいては問題に出現する項の変数を持たない部分項のみが規則に代入されている．本論文ではこのような観測から，問題から定められる基底項を各等式の変数に代入して基底等式集合を作ることで，基底等式集合の語問題に帰着する．

以下 2 節では，本論文で必要となる基本的な定義を与える．3 節では，上で述べた等式集合に対する変換を提案し，その変換に対する性質を示す．4 節では，3 節で与えた変換を用いて，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．5 節では，本論文のまとめと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予想を述べる．

2. 準　　備

文献 [2] の記法に従って，本論文で必要となる基本的な定義を与える．

関数記号の集合を Σ，変数記号の集合を V で記す．ここで，$\Sigma \cap V = \emptyset$ であるとする．各関数記号 f は固有の引数個数を持ち，これを $\mathrm{arity}(f)$ で記す．項を以下のように再帰的に定義し，項の全体からなる集合を $T(\Sigma, V)$ で記す．

- 変数 $x \in V$ は項である．
- $f \in \Sigma$ かつ $\mathrm{arity}(f) = n$ かつ $t_1, t_2, \ldots, t_n$ が項ならば，$f(t_1, t_2, \ldots, t_n)$ も項である．

特に $\mathrm{arity}(a) = 0$ となる関数記号を定数記号と呼び，$a()$ を単に a と記す．また，2 つの項 s と t が等しいことを $s \equiv t$ で表し，項 t に出現する変数の全体からなる集合を $\mathcal{V}\mathrm{ar}(t)$ で表す．項 t が基底項であるとは，t が変数を含まないときである．基底項の集合 $T(\Sigma, \emptyset)$ を $T(\Sigma)$ と記す．

項 t における位置の集合 $\mathcal{P}\mathrm{os}(t)$ を正整数の列（空列を ε で表現）を用いて以下のように定義する．

- $t \in V$ のとき，$\mathcal{P}\mathrm{os}(t) = \{\varepsilon\}$
- $t \equiv f(t_1, \ldots, t_n)$ のとき，$\mathcal{P}\mathrm{os}(t) = \{\varepsilon\} \cup \{i.u \mid 1 \leq i \leq n, u \in \mathcal{P}os(t_i)\}$

文脈とは，ホールと呼ばれる特別な定数記号 $\Box$ を一つだけ含む項である．ホール自身も文脈であり，このような文脈を空の文脈と呼ぶ．文脈 $C[\,]$ に出現する $\Box$ を項 t で置き換えることによって得られる項を $C[t]$ と記す．特に，文脈 $C[\,]$ におけるホール $\Box$ の出現位置 p を明記したいときは，$C[\,]_p$ のように添字 p で明示する．項 t, u に対して，$t \equiv C[u]_p$ となる文脈 $C[\,]$，位置 p が存在するとき，u を t の位置 p における部分項と呼び，$t|_p$ で記す．

項 t の大きさ $|t|$ は，$|\mathcal{P}\mathrm{os}(t)|$ として定義される．

$s|_p \equiv t$ かつ $|p| = d$ となる $p \in \mathcal{P}\mathrm{os}(s)$ が存在するとき，t が s 中の深さ d に出現するという．

代入とは，変数から項への写像で，その定義域 $\mathcal{D}\mathrm{om}(\sigma) = \{x \in V \mid \sigma(x) \neq x\}$ が有限の写像である σ の値域を $\mathcal{R}\mathrm{an}(\sigma) = \{\sigma(x) \mid x \in \mathcal{D}\mathrm{om}(\sigma)\}$ で定義する．また，代入 σ に対して項上の代入 $\hat{\sigma}$ を以下で再帰的に定義する．

- $t \equiv x \in V$ のとき，$\hat{\sigma}(t) = \sigma(x)$
- $t \equiv f(t_1, \ldots, t_n)$ のとき，$\hat{\sigma}(t) = f(\hat{\sigma}(t_1), \ldots, \hat{\sigma}(t_n))$

通例に従い代入 σ と対応する項上の代入 $\hat{\sigma}$ を同一視する．また，$\sigma(t)$ を $t\sigma$ で記す．

代入の合成 $\circ$ を，$\tau \circ \sigma(t) = \tau(\sigma(t))$ で定義し，これを $t\sigma\tau$ で記す．

書換え規則とは，項の対であり，$s \to t$ と記す．項書換え系とは，書換え規則の集合である．項書換え系 R における書換え関係 $\to_R$ を以下で定義する．

$$s \to_R t \overset{\mathrm{def}}{\iff} \exists l \to r \in R,\ \exists C[\,]_p,\ \exists \sigma,\ s \equiv C[l\sigma]_p,\ t \equiv C[r\sigma]_p$$

書換えの位置を明記する場合には，$s \overset{p}{\to}_R t$ と記す．特に，$s \overset{\varepsilon}{\to}_R t$ をルートでの書換えといい，ルート以外での書換えの場合には，$s \overset{>\varepsilon}{\to}_R t$ と記す．

$\to$ を二項関係とする．このとき，$\leftarrow$ を逆，$\leftrightarrow$ を対称閉包，$\overset{n}{\to}$ を n 回合成，$\overset{+}{\to}$ を推移閉包，$\overset{*}{\to}$ を反射推移閉包とする．

項 t が線形であるとは，すべての変数が高々 1 度しか出現しないときである．シャローであるとは，t 中のすべての変数の出現が深さ 0 か 1 のときである．

書換え規則 $l \to r$ が線形（シャロー）であるとは，l と r がともに線形（シャロー）であるときである．変数非消去であるとは，$\mathcal{V}\mathrm{ar}(l) \supseteq \mathcal{V}\mathrm{ar}(r)$ のときである．非崩壊であるとは，r が変数ではないときである．基底規則であるとは，l も r も基底項であるときである．

項書換え系 R が線形（シャロー，変数非消去，非崩壊，基底項書換え系）であるとは，R 中のすべての書換え規則が線形（シャロー，変数非消去，非崩壊，基底規則）であるときである．

項書換え系 R の語問題 $\langle s, t \rangle$ とは，2 つの項 s, t が与えられて，$s \overset{*}{\leftrightarrow}_E t$ が成立するかという問題である．項書換え系 R の基底語問題とは，s, t が基底項である語問題である．

項書換え系 R から導かれる等式集合 E を，$E = R \cup R^{-1}$ で定義する．なお本論文中では，項書き換え系 R を明記せず単に等式集合 E と記す．また，等式 $s \approx t$ を $s \to t$ と $t \to s$ の両方の規則を表す略記として用いる．等式集合 E の語問題 $\langle s,t \rangle$ とは，2つの項 s,t が与えられて，$s \overset{*}{\to}_E t$ が成立するかどうかという問題である．一般に，等式集合の（基底）語問題は決定不能である．等式集合の語問題について，次の定理が知られている．

定理 1. ([1]) 有限な基底等式集合の語問題は決定可能である．

3. 等式集合の語問題の変換

本節では，等式集合の語問題の変換を定義する．この変換は，変数を問題に出現する基底項で置き換えるものである．

定義 2. 等式集合 E の語問題 $\langle s,t \rangle$ は，次の Inst と GS により，等式集合 $\mathrm{Inst}(E, \mathrm{GS}(\{s \to t\} \cup E))$ の語問題 $\langle s,t \rangle$ に変換される．ここで $\mathrm{Inst}(E,T)$ は，E に含まれる等式を T に含まれる項によってインスタンス化して得られる等式集合を表し，次のように定義される．

$$\mathrm{Inst}(E,T) = \{l\sigma \to r\sigma \mid l \to r \in E, \mathcal{V}\mathrm{ar}(l) \cup \mathcal{V}\mathrm{ar}(r) \subseteqq \mathcal{D}\mathrm{om}(\sigma), \mathcal{R}\mathrm{an}(\sigma) \subseteqq T\}$$

また $\mathrm{GS}(t)$ は，項 t の部分項のうち基底項であるものの集合を表し，次のように定義される．

$$\mathrm{GS}(t) = \{t|_p \mid p \in \mathcal{P}\mathrm{os}(t),\ t|_p \in T(\Sigma)\}$$

これは等式集合 E に対して自然に拡張される．

$$\mathrm{GS}(E) = \bigcup_{l \to r \in E} (\mathrm{GS}(l) \cup \mathrm{GS}(r))$$

例 3. 次の等式集合 E_1 の語問題 $\langle s,t \rangle$ を考える．

$$E_1 = \{f(x,a) \approx g(x,a)\},\ \langle s,t \rangle = \langle f(b,a), g(b,a) \rangle$$

このとき，

$$\mathrm{GS}(\{s \to t\} \cup E_1) = \{a,\ b,\ f(b,a),\ g(b,a)\}$$

$$\mathrm{Inst}(E_1, \mathrm{GS}(\{s \to t\} \cup E_1))$$

$$= \{f(a,a) \approx g(a,a),\ f(b,a) \approx g(b,a),$$

$$f(f(b,a),a) \approx g(f(b,a),a),\ f(g(b,a),a) \approx g(g(b,a),a)\}.$$

まず Inst に関する性質を述べる．等式集合 $\mathrm{Inst}(E,T)$ の書換え関係は，等式集合 E の書換え関係に含まれている．すなわち，次の命題が成り立つ．

命題 4. 等式集合 E，項の集合 T に対して，以下が成立する．

$$\to_{\mathrm{Inst}(E,T)} \subseteqq \to_E$$

証明. $s \to_{\mathrm{Inst}(E,T)} t$ とする．書換え関係の定義より，書換え規則 $l \to r \in \mathrm{Inst}(E,T)$，文脈 $C[\,]_p$，代入 σ が存在して，$s \equiv C[l\sigma]_p$，$t \equiv C[r\sigma]_p$ である．また Inst の定義より，$l' \to r' \in E$ を満たす項 l,r と $\mathcal{V}\mathrm{ar}(l') \cup \mathcal{V}\mathrm{ar}(r) \subseteqq \mathcal{D}\mathrm{om}(\sigma')$，$\mathcal{R}\mathrm{an}(\sigma) \subseteqq T$ を満たす代入 σ' に対して，$l \equiv l'\sigma'$，$r \equiv r'\sigma'$ である．よって，$s \equiv C[l'\sigma'\sigma]_p$，$t \equiv C[r'\sigma'\sigma]_p$ であることから，$s \to_E t$ が成り立つ．□

$\mathrm{GS}(E)$ は部分項に閉じている．すなわち，次の命題が成り立つ．

命題 5. 等式集合 E に対して，以下が成立する．

$$t \in \mathrm{GS}(E) \text{ ならば } \forall p \in \mathcal{P}\mathrm{os}(t), t|_p \in \mathrm{GS}(E)$$

証明. $l \to r \in E$ に対して，$t \in \mathrm{GS}(l)$ としても一般性を失わない．このとき $\mathrm{GS}(l)$ の定義より，$q \in \mathcal{P}\mathrm{os}(l)$ に対して，$t \equiv l|_q$ と書ける．よって，$p \in \mathcal{P}\mathrm{os}(t)$ に対して，$t|_p \equiv l|_{q.p}$ と書ける．ゆえに，$q.p \in \mathcal{P}\mathrm{os}(l)$ であるから，$t|_p \in \mathrm{GS}(l)$ が成り立つ．□

以下では，変換で得られた等式集合の技術的な性質を述べる．

補題 6. シャローな等式集合 E，基底項 s,t，等式集合 $\mathrm{Inst}(E, \mathrm{GS}(\{s \to t\} \cup E))$ を E' と書く．このとき，以下が成立する．

$$f(u_1, \ldots, u_\alpha) \in \mathrm{GS}(\{s \to t\} \cup E')$$

$$\text{ならば } \forall i, u_i \in \mathrm{GS}(\{s \to t\} \cup E)$$

証明. $f(u_1, \ldots, u_\alpha) \in \mathrm{GS}(\{s \to t\})$ のときは明らかであるので，$f(u_1, \ldots, u_\alpha) \in \mathrm{GS}(E')$ のときを考える．このとき，$l' \to r' \in E'$，位置 p が存在して，一般性を失わず，$f(u_1, \ldots, u_\alpha) \equiv l'|_p$ と書ける．E' の作り方より，$l \to r \in E$，$\mathcal{R}\mathrm{an}(\sigma) \subseteqq \mathrm{GS}(\{s \to t\} \cup E)$ を満たす σ が存在して，$l' \equiv l\sigma$ と書ける．

$p = \varepsilon$ のときを考える．

- $l|_i \in V$ のとき，$u_i \equiv l'|_i \equiv (l\sigma)|_i \equiv l|_i\sigma \in \mathcal{R}\mathrm{an}(\sigma) \subseteqq \mathrm{GS}(\{s \to t\} \cup E)$ である．
- $l|_i \notin V$ のとき，l はシャローであるから，$l|_i$ は基底項である．よって $u_i \equiv l'|_i \equiv (l\sigma)|_i \equiv l|_i \in \mathrm{GS}(\{s \to t\} \cup E)$ である．

$p = j.p'$ $(1 \leqq j \leqq \mathrm{arity}(l) \wedge p' \in \mathcal{P}\mathrm{os}(l|_j))$ のときを考える．

- $l|_j \in V$ のとき，$l'|_j \equiv (l\sigma)|_j \equiv l|_j\sigma \in \mathcal{R}\mathrm{an}(\sigma) \subseteqq \mathrm{GS}(\{s \to t\} \cup E)$ であるから，命題 5 より $u_i \equiv l'|_{j.p'.i} \in \mathrm{GS}(\{s \to t\} \cup E)$ である．
- $l|_j \notin V$ のとき，l はシャローであるから，$l|_j$ は基底項である．よって $l'|_j \equiv (l\sigma)|_j \equiv l|_j \in \mathrm{GS}(\{s \to t\} \cup E)$ であるから，命題 5 より $u_i \equiv l'|_{j.p'.i} \in \mathrm{GS}(\{s \to t\} \cup E)$ である．

以上より，題意は成り立つ．□

例 7. 次の等式集合 E_2 の語問題 $\langle s,t \rangle$ を考える．

$$E_2 = \{f(x,a) \approx g(b)\},\ \langle s,t \rangle = \langle f(a,a), g(b) \rangle$$

このとき以下のようになるので，補題 6 が成り立っているのがわかる．

$\mathrm{GS}(\{s \to t\} \cup E_2) = \{a, b, f(a,a), g(b)\}$

$E_2' = \{f(u,a) \approx g(b) \mid u \in \{a, b, f(a,a), g(b)\}\}$

$\mathrm{GS}(\{s \to t\} \cup E_2') = \{a, b, f(a,a), f(f(a,a),a), f(g(b),a), g(b)\}$

4. 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

本節では，線形，シャロー，変数非消去かつ非崩壊な等式集合 E の語問題 $\langle s,t\rangle$ が，3 節の変換で得られる基底等式集合 $\mathrm{Inst}(E, \mathrm{GS}(\{s \to t\} \cup E))$ の語問題 $\langle s,t\rangle$ と等価であることを示す．

証明の準備として，線形かつシャローな等式集合に関する補題を示す．

補題 8. E は線形かつシャローな等式集合，$t \xrightarrow{n,>\varepsilon}_E l\sigma \xrightarrow{\varepsilon}_E r\sigma$ とする．このとき，次の 2 つを満たす代入 σ' が存在する．

（1） $t \xrightarrow{m,>\varepsilon}_E l\sigma' \xrightarrow{\varepsilon}_E r\sigma' \xrightarrow{m'}_E r\sigma \ \wedge\ m + m' \leqq n$

（2） $\forall p \in \mathcal{P}\mathrm{os}(l), (l|_p \in V \implies t|_p \equiv l|_p\sigma')$

証明. 代入 σ' を次のように定め，(1) と (2) を満たすことを示す．

$$x\sigma' \equiv \begin{cases} t|_p & \text{if } \exists p \in \mathcal{P}\mathrm{os}(l),\ l|_p \equiv x \in V \\ x\sigma & \text{if } x \in \mathcal{V}\mathrm{ar}(r) - \mathcal{V}\mathrm{ar}(l) \end{cases}$$

ここで，l は線形であるから，σ' は矛盾なく定まる．

$t \xrightarrow{n,>\varepsilon}_E l\sigma$ より，書換えは深さ 1 以上でしかおこらない．ゆえに，$t \equiv f(t_1,\ldots,t_\alpha)$, $l \equiv f(l_1,\ldots,l_\alpha)$ と書ける．したがって，$\forall i, t_i \xrightarrow{n_i}_E l_i\sigma$ (ただし，$\sum n_i = n$) となる．

（1） 初めに，$t \xrightarrow{m,>\varepsilon}_E l\sigma'$ を示す．

- $l_i \in \mathcal{V}\mathrm{ar}(l)$ のとき，$t_i \equiv l_i\sigma'$ であるから，$t_i \xrightarrow{0} l_i\sigma'$ である．
- $l_i \notin \mathcal{V}\mathrm{ar}(l)$ のとき，l はシャローであるから，l_i は基底項である．よって，$l_i\sigma' \equiv l_i\sigma \equiv l_i$ である．したがって，$t_i \xrightarrow{n_i} l_i\sigma'$ である．

以上より，$l_i \notin \mathcal{V}\mathrm{ar}(l)$ なる i に対して，$m = \sum n_i$ とすると，$t \xrightarrow{m,>\varepsilon} l\sigma'$ である．

次に，$r\sigma' \xrightarrow{m'} r\sigma$ を示す．これを示すには，$\forall x \in \mathcal{V}\mathrm{ar}(r), x\sigma' \xrightarrow{m'_x} x\sigma$ を示せばよい．

- $x \in \mathcal{V}\mathrm{ar}(r) \cap \mathcal{V}\mathrm{ar}(l)$ のとき，$l_i \equiv x$ に対して，$t_i \equiv l_i\sigma' \xrightarrow{n_i} l_i\sigma$ であるので，$x\sigma' \xrightarrow{n_i} x\sigma$ である．
- $x \in \mathcal{V}\mathrm{ar}(r) - \mathcal{V}\mathrm{ar}(l)$ のとき，$x\sigma' \equiv x\sigma$ であるので，$x\sigma' \xrightarrow{0} x\sigma$ である．

以上より，$l_i \in \mathcal{V}\mathrm{ar}(l) \cap \mathcal{V}\mathrm{ar}(r)$ なる i に対して，$m' = \sum n_i$ とすると，$r\sigma' \xrightarrow{m'} r\sigma$ である．

さらに，m と m' で加算されている各 n_i はお互いにかぶらないので，$m + m' \leqq \sum n_i = n$ が成り立つ．

したがって，(1) は成り立つ．

（2） 代入 σ' の定め方より，σ' が $\forall p \in \mathcal{P}os(l), (l|_p \in V \implies t|_p \equiv l|_p\sigma')$ を満たすのは明らか．よって，(2) は成り立つ． □

例 9. 次の等式集合 E_3 を考える．

$$E_3 = \{f(x,y) \approx g(x), a \approx b\}$$

このとき，代入 $\sigma = \{x \mapsto b, y \mapsto a\}$ に対して，以下が成立する．

$$f(a,a) \xrightarrow{>\varepsilon}_{E_3} f(b,a) \xrightarrow{\varepsilon}_{E_3} g(b)$$

一方，代入 $\sigma' = \{x \mapsto a, y \mapsto a\}$ に対して，以下が成立する．

$$f(a,a) \xrightarrow{\varepsilon}_{E_3} g(a) \to_{E_3} g(b)$$

次の定理より，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が定義 2 の変換により，基底等式集合の語問題に帰着可能であることがわかる．

定理 10. 線形，シャロー，変数非消去かつ非崩壊な等式集合 E の語問題 $\langle s,t\rangle$ に対して，以下が成立する．

$$s \xrightarrow{*}_E t \iff s \xrightarrow{*}_{E'} t$$

ここで E' は $\mathrm{Inst}(E, \mathrm{GS}(\{s \to t\} \cup E))$ で表される基底等式集合である．

証明. ($\Longleftarrow$)：命題 4 より明らかである．

($\Longrightarrow$)：任意の $u, v \in \mathrm{GS}(\{s \to t\} \cup E')$ に対して，$u \xrightarrow{n}_E v \implies u \xrightarrow{n}_{E'} v$ が成り立つことを辞書式順序のもとで $(n, |u|)$ に関する帰納法で示す．

$n = 0$ のとき，$u \equiv v$ であるから明らかである．

$n > 0$ のとき，以下の二つの場合がある．

- ルートでの書換えがないとき，$u \equiv f(u_1,\ldots,u_\alpha)$, $v \equiv f(v_1,\ldots,v_\alpha)$ と書ける．

$1 \leqq i \leqq \alpha$ なる i に対して，$u_i \xrightarrow{n_i}_E v_i$ とする．$n_i \leqq n, |u_i| < |u|$ かつ $u_i, v_i \in \mathrm{GS}(\{s \to t\} \cup E')$ であるから，帰納法の仮定より，$u_i \xrightarrow{n_i}_{E'} v_i$ である．よって，$f(u_1,\ldots,u_\alpha) \xrightarrow{n}_{E'} f(v_1,\ldots,v_\alpha)$，すなわち，$u \xrightarrow{n}_{E'} v$ となる．

- ルートでの書換えがある，すなわち，$u \xrightarrow{n_1}_E u' \xrightarrow{\varepsilon}_E v' \xrightarrow{n_2}_E v$ のとき，等式集合 E は非崩壊であるから，$u' \equiv f(u'_1,\ldots,u'_\alpha)\sigma', v' \equiv g(v'_1,\ldots,v'_\beta)\sigma'$（ただし，$f(u'_1,\ldots,u'_\alpha) \to g(v'_1,\ldots,v'_\beta) \in E$ であり，σ' は代入）と書ける．ここで，$u \xrightarrow{n_1}_E u'$ において，ルートでの書換えがないとしても一般性を失わない．

このとき，$u \equiv f(u_1,\ldots u_\alpha)$ と書ける．ゆえに書換えは，以下のように書ける．

$$f(u_1,\ldots,u_\alpha) \xrightarrow{n_1,>\varepsilon}_E f(u'_1,\ldots,u'_\alpha)\sigma' \xrightarrow{\varepsilon}_E g(v'_1,\ldots,v'_\beta)\sigma' \xrightarrow{n_2}_E v$$

補題 8 より，書換えは次のようにすることが可能である．

$$f(u_1,\ldots,u_\alpha) \xrightarrow{m,>\varepsilon}_E f(u'_1,\ldots,u'_\alpha)\sigma \xrightarrow{\varepsilon}_E g(v'_1,\ldots,v'_\beta)\sigma \xrightarrow{m'+n_2}_E v$$

ただし，代入 σ と書換えステップ m, m' は補題 8 を満たすも

のである．

$f(u'_1,\ldots,u'_\alpha) \to g(v'_1,\ldots,v'_\beta) \in E$ であり，E は線形，シャローかつ変数非消去であるから，変数 x は $1 \leqq i_x \leqq \alpha$ なる i_x と $1 \leqq j_x \leqq \beta$ なる j_x を用いて u'_{i_x}, v'_{j_x} と表すことができる．よって，$u_{i_x} \equiv u'_{i_x}\sigma \equiv v'_{j_x}\sigma$ となる．

ここで $f(u_1,\ldots,u_\alpha) \in \mathrm{GS}(\{s \to t\} \cup E')$ であるから，補題 6 より $u_{i_x} \in \mathrm{GS}(\{s \to t\} \cup E)$ である．ゆえに，$u'_{i_x}\sigma, v'_{j_x}\sigma \in \mathrm{GS}(\{s \to t\} \cup E)$ である．E' の定義より，$\mathrm{GS}(\{s \to t\} \cup E)$ に含まれている項は必ず E 中の等式に出現する変数に代入される．ゆえに，$f(u'_1,\ldots,u'_\alpha)\sigma \to g(v'_1,\ldots,v'_\beta)\sigma \in E'$，すなわち $u' \to v' \in E'$ である．

さらに，E' は基底等式集合であるので，各等式は基底項である．したがって，すなわち $u', v' \in \mathrm{GS}(\{s \to t\} \cup E')$ である．$m + m' + n_2 \leqq n_1 + n_2 < n$ であるので，$m < n$ かつ $m' + n_2 < n$ である．したがって帰納法の仮定より，以下が成立する．

$$u \xrightarrow{m}_{E'} u' \to_E v' \xrightarrow{m'+n_2}_{E'} v$$

さらに，$u' \to v' \in E'$ であるので，以下が成立する．

$$u \xrightarrow{m}_{E'} u' \to_{E'} v' \xrightarrow{m'+n_2}_{E'}$$

□

次の系 11 が，定理 10 から導かれるが，新しい結果ではない．なぜなら，線形，シャロー，変数非消去かつ非崩壊な等式集合 E は線形シャロー項書換え系とみなすことができ，また線形シャロー項書換え系の到達可能性は決定可能である [4]．よって，線形，シャロー，変数非消去かつ非崩壊な有限等式集合に対する基底語問題の決定可能性が導かれるからである．

系 11. 線形，シャロー，変数非消去かつ非崩壊な等式集合に対する基底語問題は決定可能である．

証明. 定理 10 より，線形，シャロー，変数非消去かつ非崩壊な等式集合に対する基底語問題は，基底等式集合に対する語問題に帰着可能である．さらに定理 1 より，基底等式集合に対する語問題は決定可能である．ゆえに，系は成り立つ． □

5. おわりに

本論文では，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は，基底等式集合の語問題に帰着可能であることを示した．

本論文の手法による語問題の決定手続きでは，まだ実際に線形，シャロー，変数非消去かつ非崩壊な等式集合の語問題をより高速に解くことができるかは不明である．したがって，定義 2 の変換を実装し実験することは今後の課題である．

また，等式集合に対する条件の緩和も挙げられる．それに関して，以下のことを予想している．

予想 12. 線形，シャローかつ非崩壊な等式集合の語問題は，基底等式集合の語問題に帰着可能である．

これは，本論文における等式集合の条件から変数非消去を除いたものである．

謝辞 本研究は，一部，文部科学省科学研究費#20300010, #20500008, #21700011 の助成を受けたものである．

文　献

[1] Ackermann, W.: Solvable Cases of The Decision Problem, North Holland , 1954.

[2] Baader, F. and Nipkow, T.: Term Rewriting and All That, Cambridge University Press, 1998.

[3] Downey, P. J., Sethi, R. and Tarjan, R. E.: Variations on the common subexpressions problem, Journal of the ACM, J ACM 27 (4), pp.758–771, 1980.

[4] Jacquemard, F.: Decidable Approximations of Term Rewriting Systems. *Proc. 7th International Conference on Rewriting Techniques and Applications(RTA'96)*, pp.362–376, 1996.

[5] Nelson, G. and Oppen, D. C.: Fast decision procedures based on congruence closure, Journal of the ACM, J ACM 27 (2), pp.356–364, 1980.

[6] Nieuwenhuis, R. and Oliveras, A.: Decision procedures for SAT, SAT Modulo Theories and Beyond. The Barcelogic-Tools, *12th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR 2005)*, LNCS, Vol.3855, pp.23–46, 2005.

[7] Nieuwenhuis, R. and Oliveras, A.: Fast congruence closure and extentions. *Information and Computation*, Volume 205 Issue 4, pp.557–580, 2007.

[8] Shostak, R. E.: An algorithm for reasoning about equality, Communications of the ACM, Commun. ACM 21 (7), pp.583–585, 1978.