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
SS2007-61(2008-3)

等式を規則化する変換の停止条件

水野 清貴† 西田 直樹†† 坂部 俊樹†† 酒井 正彦†† 草刈 圭一朗††

†,†† 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: †kiyomizuno@trs.cm.is.nagoya-u.ac.jp, ††{nishida,sakabe,sakai,kusakari}@is.nagoya-u.ac.jp

あらまし 項書換え系（TRS）と等式集合から等価なTRSを得る変換手続きが様々な目的で提案されている．これらの手続きを活用するにはその停止性を明らかにすることが必要であるが，これまでに手続きの停止性に関する研究はほとんどなされていない．本稿では，TRSと等式集合の変換手続きに共通する特徴を捉えて，共通して適用できる停止性の十分条件を与える．具体的には，手続きの停止性をナローイング到達可能集合の有限性に帰着させる．そして，等式付き書換え系の等式数削減手続き [10] と正規化手続き [2] について停止性の十分条件を与える．

キーワード 項書換え系，等式付き書換え，等価変換，ナローイング

A Sufficient Condition for Termination of Transformations from Equations to Rewrite Rules

Kiyotaka MIZUNO†, Naoki NISHIDA††, Toshiki SAKABE††,
Masahiko SAKAI††, and Keiichirou KUSAKARI††

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

Abstract Several procedures which transform pairs of term rewriting systems (TRSs, for short) and sets of equations into equivalent TRSs have been proposed so far for different purposes. There has been few works on termination of these procedures, while we need some criteria assuring termination in applying them. In this paper, we show a common sufficient condition for the termination of those procedures. We reduce the termination of the procedures to finiteness of sets of narrowing reachable terms. In particular, we discuss sufficient conditions for the termination of the equation elimination procedure [10] and the normalization procedure [2].

Key words term rewriting system, rewriting modulo equations, equivalent transformation, narrowing

1. はじめに

項書換え系（TRS）と等式集合から等価なTRSを得る変換手続きが様々な目的で提案されている．等式付き書換え系の等式数削減手続き [10] は，アンビエント計算をTRSへ変換した際により扱いやすいTRSへ変換するために利用できる．等式付き書換え系の正規化手続き [2] は，等式理論付きπ計算で記述された暗号プロトコルの安全性検証で利用されている．その他に，拡張等式付き書換え系の変換手続き [4]，弱最内戦略が完全となるTRSを得る手続き [9] などがある．これらの手続きを活用するにはその停止性を明らかにすることが必要であるが，これまでに手続きの停止性に関する研究はほとんどなされていない．

本稿の目的は，TRSと等式集合の変換手続きに共通する特徴を捉えて，共通して使える停止性の十分条件を与えることである．このような十分条件は，同じ特徴を持つ手続きに対して応用できる．

上述のTRSと等式集合の変換手続きに共通する操作として，TRSおよび等式の左辺（の部分項）と右辺（の部分項）との単一化がある．特に，三浦らの等式数削減手続きとBlanchetらの正規化手続きは，単一化により定義されるナローイング [7] を基本操作としている．これらの手続きでは，項の有限集合からナローイング関係で到達可能な項集合が有限であることが手続きの停止性の重要な鍵となることが分かる．ここで，ナローイング到達可能集合が有限か否かは一般には決定不能な問題である．

本稿ではまず，ナローイング到達可能集合が有限であるための判定可能な十分条件を与える．次に，等式数削減手続きと正規化手続きについて上記の十分条件の適用可能性を明らかにする．

等式数削減手続きの停止性は，ナローイング到達可能集合の有限性だけでは保障できない．このため，ナローイング到達可能集合の有限性が手続きの停止条件となる入力条件を明らかにする．等式数削減手続きの適用例としてあげられているアンビエント計算の場合は，この入力条件を満たしているため，本稿の十分条件により停止性が証明できる．

正規化手続きは手続き1と手続き2から構成されており，既に手続き1の停止性の十分条件は示されている [2]．本稿では，手続き2の停止性がナローイング到達可能集合の有限性で保障できることを示す．

また，その他の類似の手続きの停止性に関して考察する．

本稿は次のように構成される．2節に本稿で扱う項書換え系，ナローイングに関する諸定義を与える．3節では，ナローイング到達可能集合を定義し，それが有限であるための判定可能な十分条件を示す．4節では，等式数削減手続きの停止性をナローイング到達可能集合の有限性を用いて保障する．5節では，正規化手続きを構成する手続き2の停止性をナローイング到達可能集合の有限性を用いて保障する．6節では，その他の類似の手続きの停止性についての考察を記す．7節では，まとめと今後の課題を記す．

2. 準　　備

本稿では，項書換え系，ナローイングの一般的な記法に従う [1,7]．

$\mathcal{F}$ を関数記号，$\mathcal{X}$ を変数の加算無限集合とし，$\mathcal{F}\cap\mathcal{X}=\emptyset$ とする．**項**は関数記号と変数から構成され，項の集合を $\mathcal{T}(\mathcal{F},\mathcal{X})$ と記す．項 s と t が構造的に等しいことを $s\equiv t$ と記す．項 t に現れるすべての変数の集合を $\mathcal{V}ar(t)$ と記す．集合 $\mathcal{T}(\mathcal{F},\emptyset)$ 中の項を**基礎項**という．本稿では，項の組 (t_1,t_2) や $(t_1,\cdots,t_n)$ も項とみなす．

項 t における**位置**の集合 $\mathcal{O}(t)$ を以下のように定義する．

- $t\equiv x\in\mathcal{X}$ のとき，$\mathcal{O}(t)=\{\varepsilon\}$.
- $t\equiv f(t_1,\cdots,t_n)$ のとき，$\mathcal{O}(t)=\{\varepsilon\}\cup\{ip \mid 1\leqq i\leqq n, p\in\mathcal{O}(t_i)\}$.

ここで，ε は項の先頭の位置を表す．位置 $p,q\in\mathcal{O}(t)$ に対して，$pp'=q$ を満たす位置 p' が存在するとき，$p\leqq q$ と記す．特に，$p\neq q$ のときは $p<q$ と記す．項 t に対して，t の関数記号の位置を $\mathcal{O}_{\mathcal{F}}(t)$ と記す．項 s の大きさ $|s|$ は，$|s|=|\mathcal{O}(s)|$ である．文脈 C はホールと呼ばれる特別な記号 $\Box$ を含む項であり，文脈 C 中の位置 p の $\Box$ を項 t で置き換えて得られた項を $C[t]_p$ と記す．位置 p が特に本質的ではないときは，$C[t]_p$ を $C[t]$ と略記する．項 s,t，位置 p に対して $s\equiv C[t]_p$ であるとき，t は s の位置 p の**部分項**であるといい，特に $p\neq\varepsilon$ であるとき，t は s の**真部分項**であるという．項 t の位置 p の部分項を $t|_p$ と記す．項 t の位置 p の部分項を項 s で置き換えて得られた項を $t[s]_p$ と記す．

$\mathcal{X}$ から $\mathcal{T}(\mathcal{F},\mathcal{X})$ への写像 σ で，その定義域 $\mathcal{D}om(\sigma)=\{x|x\sigma\neq x\}$ が有限であるものを**代入**という．$x\sigma$ は $\sigma(x)$ を表す．項 t に現れるすべての変数に代入 σ を適用したものを $t\sigma$ と記す．σ の定義域を $X\subseteqq\mathcal{X}$ に制限した代入 $\{x\mapsto x\sigma \mid x\in\mathcal{D}om(\sigma)\cap X\}$ を $\sigma|_X$ と記す．代入 σ,θ に対して $\sigma\delta=\theta$ となる代入 δ が存在するとき，$\sigma\lesssim\theta$ と記す．項 $t\sigma$ を t の具体項という．項 s,t が互いの具体項であるとき，s と t は**名前替え**であるという．項 s，t は，$s\sigma\equiv t\sigma$ となる代入 σ が存在するとき，**単一化可能**であるといい，σ を s と t の**単一化子**という．さらに，s と t の任意の単一化子 σ' に対して $\sigma\lesssim\sigma'$ であるとき，σ を s と t の**最汎単一化子**といい，$mgu(s,t)$ と記す．

$\mathcal{T}(\mathcal{F},\mathcal{X})$ 上の**書換え規則**は $l\notin\mathcal{X}$ かつ $\mathcal{V}ar(l)\supseteqq\mathcal{V}ar(r)$ を満たす項の組 (l,r) であり，これを $l\to r$ と記す．**項書換え系（TRS）**は書換え規則 $l\to r$ の集合である．TRS R で定まる**書換え関係** $\to_R$ は，$\to_R=\{(C[l\sigma],C[r\sigma]) \mid l\to r\in R, C\in\mathcal{T}(\mathcal{F}\cup\{\Box\},\mathcal{X})\}$ である．$\to_R$ の推移閉包，反射推移閉包をそれぞれ $\xrightarrow{+}_R$，$\xrightarrow{*}_R$ と記す．書換え規則 $l\to r$ と $l'\to r'$ は，$\pi\in\mathcal{O}_{\mathcal{F}}(l)$ で $l|_\pi$ と l' が単一化可能であるとき，π において**重なりを持つ**という．

等式集合 E に基づく関係 $\to_E$ は，$\to_E=\{(C[u\sigma]_\pi,C[v\sigma]_\pi) \mid u\approx v\in E, C\in\mathcal{T}(\mathcal{F}\cup\{\Box\},\mathcal{X})\}$ である．$\to_E$ の対称閉包を $\leftrightarrow_E$ と記し，$\leftrightarrow_E$ の反射推移閉包を $\approx_E$ と記す．

項 t のすべての真部分項が変数か基礎項であるとき，t は**シャロー**（shallow）であるという．また，書換え規則の左辺がシャローである場合，その書換え規則は**左シャロー**であるという．TRS R に対して，R に含まれるすべての書換え規則が左シャローであるとき，R は**左シャロー**であるという．項 t に2回以上出現する変数がないとき，t は**線形**であるという．書換え規則（等式）の両辺が線形であるとき，その規則（等式）は**線形**であるという．右辺が変数である書換え規則（等式）は，**崩壊**（collapsing）であるという．

TRS R，等式集合 E，項 s,t に対して，$s\approx_E s'\to_R t'\approx_E t$ を満たす項 s',t' が存在するとき，s から t へ等式付き書換え可能であるといい，$s\to_{R/E}t$ と記す．$\to_{R/E}$ で定まる抽象書換え系を**等式付き書換え系**という．また，$\to_{R/E}$ の部分関係に $\to_{R,E}$ がある．$\to_{R,E}$ で定まる抽象書換え系を**拡張等式付き書換え系**という．

（狭義の）半順序 $\succ$ は推移的かつ非反射的な二項関係である．$s\succ t$ ならば $\forall\sigma.\ s\sigma\succ t\sigma$ であるとき半順序 $\succ$ が**代入に閉じている**という．$s\succ t$ ならば $\forall C[\,].\ C[s]\succ C[t]$ であるとき半順序 $\succ$ が文脈に閉じているという．関係 $\succ$ の無限減少列が存在しないとき，$\succ$ は整礎であるという．代入と文脈に閉じた整礎な半順序を簡約化順序という．

TRS R，項 s,t に対して，$s|_p\notin\mathcal{X}$ かつ $t\equiv(C[r]_p)\sigma$ を満たす $\sigma=mgu(s,C[l]_p)$，$p\in\mathcal{O}(s)$，$l\to r\in R$ が存在するとき，s は σ,p,R のもとで t に**ナローイング可能である**といい，$s\ {}_\sigma\!\rightsquigarrow^p_R\ t$ と記す．ただし，$l\to r$ 中の変数は常に新しい変数に名前替えされているとする．文脈から明らかなときは σ，p は省略可能である．$\rightsquigarrow_R$ によって定まる関係を R の**ナローイング**という．$s\equiv t_0\ {}_{\sigma_0}\!\rightsquigarrow_R t_1\ {}_{\sigma_1}\!\rightsquigarrow_R\cdots\ {}_{\sigma_{n-1}}\!\rightsquigarrow_R t_n\equiv t$ をナ

ローイング系列といい，$s \ {}_{\sigma}\!\rightsquigarrow^{n}_{R} \ t$ または $s \ {}_{\sigma}\!\rightsquigarrow^{*}_{R} \ t$ と記す．このとき $\sigma = \sigma_0\sigma_1\cdots\sigma_{n-1}$ であり，$n=0$ のときは $\sigma = \emptyset$ とする．また，このとき s から R のナローイングで t に**到達可能**であるという．

3. ナローイング到達可能集合の有限性

本節では，ナローイング到達可能集合が名前替えを法として有限であるための判定可能な十分条件を2つ示す．4-6節では，手続きの停止性をナローイング到達可能集合の有限性に帰着させることで，手続きが停止するための判定可能な十分条件を与える．

まず，ナローイング到達可能集合に位置の指定による制限も可能にするために，ナローイングに位置の制限を導入する．

定義 3.1 R を TRS，s,t を項，$p,q \in \mathcal{O}(s)$ とする．$s \ {}_{\sigma}\!\rightsquigarrow^{q}_{R} \ t$ かつ $p \leqq q$ のとき，$s \ {}_{\sigma}\!\rightsquigarrow^{p\leqq}_{R} \ t$ と記す．このとき $p \in \mathcal{O}(t)$ である．また，$s_1 \ {}_{\sigma_1}\!\rightsquigarrow^{p\leqq}_{R} \ t_1 \ {}_{\sigma_2}\!\rightsquigarrow^{p\leqq}_{R} \ t_2 \cdots \ {}_{\sigma_n}\!\rightsquigarrow^{p\leqq}_{R} \ t_n$ のとき $s_1 \ {}_{\sigma}\!\rightsquigarrow^{*p\leqq}_{R} \ t_n$ と記す（ただし，$\sigma = \sigma_1\sigma_2\cdots\sigma_n$）．□

以下で，項の集合からある位置 p 以上におけるナローイングで到達可能なすべての項の集合を定義する．

定義 3.2 (ナローイング到達可能集合) R を TRS，T を項の集合，p を位置とする．

$$\rightsquigarrow^{*p}_{R}(T) = \{t' \mid t \in T,\ t \ {}_{\sigma}\!\rightsquigarrow^{*p\leqq}_{R} \ t'\}$$

本稿では，すべての $t \in T$ について，$p \in \mathcal{O}(t)$ と仮定する．□

例 3.3 項 $t = (f(f(x,y),z),g(x,y))$，TRS R_1 について，2つナローイング到達可能集合を名前替えを法として与える．

$$R_1 = \left\{ \begin{array}{l} f(x,a) \to x \\ g(x,y) \to g(y,x) \end{array} \right\}$$

$$\rightsquigarrow^{*1}_{R_1}(\{t\}) = \left\{ \begin{array}{ll} (f(f(x,y),z),g(x,y)), & (f(x,y),g(x,y)) \\ (f(x,z),g(x,a)), & (x,g(x,a)) \end{array} \right\}$$

$$\rightsquigarrow^{*2}_{R_1}(\{t\}) = \{\,(f(f(x,y),z),g(x,y)),\ (f(f(x,y),z),g(y,x))\,\}$$

□

次に，ナローイング到達可能集合が名前替えを法として有限であるための判定可能な十分条件を2つ示す．1つはナローイングの停止性に基づく条件であり，もう1つは，ナローイングの停止性とは無関係に成り立つ構文的条件である．

1つめの十分条件を次の定理 3.6 に示す．この十分条件はナローイングの停止性に基づいている．以下ではまず，定理 3.6 で利用する停止性順序の定義 3.4 とナローイングの停止性を示した定理 3.5 を示す．

定義 3.4 (停止性順序 [3]) 代入に閉じた整礎な基礎項上の半順序 $\succ$ を**停止性順序**（termination ordering）という．□

定理 3.5 ([3]) R を左シャロー TRS とする．$R \subseteqq \succ$ となる停止性順序 $\succ$ が存在するならば，R のナローイングは停止性を持つ．□

定理 3.6 R を左シャロー TRS，T を項の有限集合，p を位置とする．$R \subseteqq \succ$ となる停止性順序 $\succ$ が存在するならば，$\rightsquigarrow^{*p}_{R}(T)$ は名前替えを法として有限である．

[証明] 定義 3.2 より，ナローイングが停止性を持つならば，ナローイング到達可能集合が名前替えを法として有限であることは明らかである．よって，定理 3.5 より成り立つ．□

例 3.7 例 3.3 の R_1 の $f(x,a) \to x$ は，左シャローである．また，停止性順序である辞書式経路順序 $\succ_{lpo}$ を記号上の半順序を $f \succ a$ として用いると $f(x,a) \succ_{lpo} x$ である．よって，任意の項の有限集合 T，任意の位置 p について $\rightsquigarrow^{*p}_{\{f(x,a)\to x\}}(T)$ は名前替えを法として有限である．□

簡約化順序や停止性を持つ TRS R の書換え関係は停止性順序である．よって，左シャローな R の書換えの停止性が証明できれば，R のナローイングの停止性は証明できる．よって，以下の系が得られる．

系 3.8 R を左シャロー TRS，T を項の有限集合，p を位置とする．このとき，$\to_R$ が停止性を持つならば，$\rightsquigarrow^{*p}_{R}(T)$ は名前替えを法として有限である．

[証明] $\to_R$ が停止性を持つとき，$\to_R$ は停止性順序であるため，定理 3.6 より成り立つ．□

既存の TRS の停止性の証明ツール（AProVE [5]，TTT [6]）を用いれば，TRS の停止性は判定できる．実際，例 3.7 の $f(x,a) \to x$ の停止性は TTT で確認できた．

次に，ナローイング到達可能集合が名前替えを法として有限であるためのもう1つの判定可能な十分条件を次の定理 3.9 で示す．この十分条件は，ナローイングの停止性とは無関係に成り立つ．

定理 3.9 R を TRS，T を項の有限集合，p を位置とする．このとき，R のすべての書換え規則が以下の条件を満たすならば，$\rightsquigarrow^{*p}_{R}(T)$ は名前替えを法として有限である．

1. 線形である．
2. 両辺のすべての真部分項が変数である．
3. 左辺の変数集合と右辺の変数集合が等しい．

[証明] $l \to r \in R$ とする．R が条件1と2を満たすとき，位置 π で l と重なる任意の項 s に対して $\sigma = mgu(s|_\pi, l)$ かつ $s|_\pi = l\sigma$ である．よって，$\rightsquigarrow_R = \to_R$ である．また R が条件2と3を満たすとき，任意の項 s,t に対して $s \to_R t$ ならば $|s| = |t|$ である．項の有限集合 T における関数記号と変数は有限個であるため，$t \in T$ から到達できる項の候補はたかだか有限個である．したがって，$\rightsquigarrow^{*p}_{R}(T)$ は名前替えを法として有限である．□

定理 3.9 の条件は，容易に判定できる．

例 3.10 例 3.3 の R_1 の $g(x,y) \to g(y,x)$ は，定理 3.9 のすべての条件を満たす．よって，任意の項の有限集合 T，任意の位置 p について $\rightsquigarrow^{*p}_{\{g(x,y)\to g(y,x)\}}(T)$ は有限である．□

項の対は，関数記号の集合に現れていない新しい2引数記号を用いることで，項として表現できる．以降では，T の候補として項の対の集合である TRS も許すこととする．

入力 規則集合 R, 等式 $u = v$
出力 規則集合 R_k
1. $R_0 := R$, $R_{-1} := \phi$, $i := 0$.
2. $R_{i+1} := R_i \cup \{l' \to r\sigma \mid l \to r \in R_i \setminus R_{i-1},\ l\ {}_\sigma\!\rightsquigarrow_{\{u\to v\}}\ l'\}$
$\cup \{v\sigma \to u' \mid l \to r \in R_i \setminus R_{i-1},\ u\ {}_\sigma\!\rightsquigarrow_{\{l\to r\}}\ u'\}$.
3. $R_{i+1} \neq R_i$ ならば $i := i+1$ として手順 2 へ戻る.
$R_{i+1} = R_i$ ならば $R_k := R_i \cup \{u \to v\}$ として終了.

図 1 RED と RED$^-$ (RED$^-$ は下線部を除去した手続き)

4. 等式数削減手続きの停止性

本節では, 等式付き書換え系の等式数削減手続き [10] の停止性をナローイング到達可能集合の有限性に帰着させることで, 3 節で示したナローイング到達可能集合の有限性の十分条件から, 手続きが停止するための判定可能な十分条件を導く. 以降, 等式数削減手続きを **RED** と呼ぶ.

図 1 に RED を記す. ここで, 以降の議論を簡潔に行うため RED はナローイングを用いた定義で記述している. RED は, TRS と等式を入力すると, 等式を規則化し, それと重なる TRS の規則からその等式を法として等価な左辺を持つ規則を生成する. 与えられた項から 1 ステップで到達可能なすべての項を決定することができない等式付き書換え系に対して, RED を複数回実行し等式数を削減していくと, 等式集合の語問題が決定可能となる等式のみを持つ等価な等式付き書換え系に変換できる可能性がある. 変換できた場合, 計算不能だった 1 ステップの計算結果を決定することが可能となる. RED は, プロセス計算の 1 つであるアンビエント計算を TRS へ変換した際により扱いやすい TRS へ変換するために利用できる. RED は必ずしも停止するとは限らない手続きであり, その停止条件は示されていない.

RED の停止性をナローイング到達可能集合の有限性に直接帰着させることは非常に困難である. また, アンビエント計算に RED を適用する実用例では下線部の処理は常に規則を生成しない. そこで, RED から下線部の処理を取り除いた手続きを **RED**$^-$ と定義する (図 1). RED$^-$ は RED の機能を弱くした手続きであり, RED$^-$ は拡張等式付き書換え系の等式数の削減に利用できる. RED$^-$ の停止性はナローイング到達可能集合の停止性に帰着することができる.

以降ではまず, RED$^-$ が停止するための判定可能な十分条件を導く. 補題 4.2 は, RED$^-$ の R_i の規則の左辺は, 入力の TRS R の規則の左辺から i ステップのナローイングで到達可能であることを示す. まず, 補題 4.2 で用いる補題 4.1 を示す.

補題 4.1 RED$^-$ において, R を入力の TRS とする. このとき, すべての i について以下が成り立つ.

$$R_i \setminus R_{i-1} = \{l' \to r\delta \mid l \to r \in R,\ l\ {}_\delta\!\rightsquigarrow^{i}_{\{u\to v\}}\ l'\}$$

[証明] i に関する帰納法で証明できる. □

補題 4.2 RED$^-$ において, R を入力の TRS とする. このとき, すべての i について以下が成り立つ.

$$R_i = \{l' \to r\delta \mid l \to r \in R,\ l\ {}_\delta\!\rightsquigarrow^{j}_{\{u\to v\}}\ l',\ j \leqq i\}$$

[証明] 補題 4.1 を用いることで証明できる. □

次の補題は, RED$^-$ の R_i の総和が, 入力の TRS R と等式 $u \to v$ から定義されるナローイング到達可能集合と等しいことを示す.

補題 4.3 RED$^-$ において, R を入力の TRS, $u \to v$ を入力の等式とする. このとき, 以下が成り立つ.

$$\bigcup_{i=0}^{\infty} R_i = {\rightsquigarrow}^{*1}_{\{u\to v\}}(R)$$

[証明] 定義 3.2 と補題 4.2 より明らかである. □

次の補題は, RED$^-$ の R_i が単調増加することを示す.

補題 4.4 RED$^-$ において, すべての i に対して, $R_i \subseteqq R_{i+1}$.

[証明] RED$^-$ の定義より明らかである. □

補題 4.3 と補題 4.4 より, 以下の定理が成立する. この定理は, RED$^-$ の停止性がナローイング到達可能集合の有限性に帰着できることを示す.

定理 4.5 RED$^-$ において, R を入力の TRS, $u \to v$ を入力の等式とする. ${\rightsquigarrow}^{*1}_{\{u\to v\}}(R)$ が名前替えを法として有限のとき, かつそのときに限り, RED$^-$ は停止する.

[証明] 補題 4.3 と補題 4.4 を用いることで証明できる. □

この定理 4.5 と 3 節で示したナローイング到達可能集合の有限性の十分条件を示した定理 3.6, 定理 3.9 から RED$^-$ が停止するための判定可能な十分条件を以下の 2 つの系で示す.

系 4.6 入力の $u \to v$ において, $u \to v$ が左シャローかつ, $u \succ v$ となる停止性順序 $\succ$ が存在するならば, RED$^-$ は停止する.

[証明] 定理 3.6 と定理 4.5 より明らかである. □

系 4.7 入力の $u \to v$ が以下を満たすならば, RED$^-$ は停止する.
1. 線形である.
2. u, v のすべての真部分項が変数である.
3. $\mathcal{V}ar(u) = \mathcal{V}ar(v)$.

[証明] 定理 3.9 と定理 4.5 より明らかである. □

また, 以下の系も成り立つ.

系 4.8 入力の $u \to v$ において, $u \to v$ が左シャローかつ, 停止性を持つならば, RED$^-$ は停止する.

[証明] 系 3.8 と定理 4.5 より明らかである. □

次に, RED が停止するための判定可能な十分条件を導く. 次の命題は, RED と RED$^-$ の出力が等しくなるための入力条件を示す.

命題 4.9 以下の入力条件を満たす TRS R, 書換え規則 $u \to v$ を RED と RED$^-$ に入力するとき, RED と RED$^-$ の出力は等しい.

- すべての $l \to r \in R$ に対して, l の根記号が u に現れる場

合は，その記号は u の真部分項には現れない． □

系 4.6，4.7，4.8 で示した RED$^-$ の停止性の十分条件と命題 4.9 の入力条件の両方を満たすことが，RED が停止するための十分条件である．

文献 [10] には，アンビエント計算に RED を適用した実用例がいくつか記されている．これらの例は，本稿で示した停止性の十分条件を満たす．次の例は，そのうちの一つである．

例 4.10 アンビエント計算の遷移規則を TRS，構造等価関係を等式として捉えて，RED の入力とする．

- 遷移規則：$n[in\ m.P \mid Q] \mid m[R] \to m[n[P \mid Q] \mid R]$
- 構造等価関係：$P \mid 0 \equiv P$

ここで，$n[\,]$，$m[\,]$，$in\ m.$，$\mid$ を関数記号，P, Q, R を変数として捉える．この遷移規則と構造等価関係は，系 4.6（または系 4.8）と命題 4.9 の条件を満たすため，これらを入力するとき，RED は停止する． □

5. 正規化手続きの停止性

等式付き書換え系の正規化手続き [2] は，TRS と等式集合を入力すると，まず等式集合を規則化し，それらの規則による複数ステップの書換えを 1 ステップで行える規則を生成する．次に，その生成されたすべての規則と入力の TRS による複数ステップの書換えを 1 ステップで行える規則を生成する．この手続きは，等式理論付き π 計算（applied π calculus）で記述された暗号プロトコルの安全性検証において利用されている [2]．

正規化手続きは，上記のように等式付き書換え系の等式集合を正規化して規則集合を得る前半部分と，そこで得られた規則集合を用いて等式付き書換え系の TRS を正規化する後半部分から構成される．さらに前半部分は手続き 1 と**手続き 2** から構成される．入力の等式集合はその性質によって，手続き 1 で処理される集合と手続き 2 で処理される集合に分けられる．後半部分は必ず停止するように定義されているが，手続き 1 と 2 は必ずしも停止するとは限らない．そのため，手続き 1 が停止するための判定可能な十分条件は示されている [2]．しかし，手続き 2 の停止条件は示されていない．

本節では，等式付き書換え系の正規化手続きを構成する手続き 2 の停止性をナローイング到達可能集合の有限性に帰着させることで，3 節で示したナローイング到達可能集合の有限性の十分条件から，手続きが停止するための判定可能な十分条件を導く．以降，正規化手続きの手続き 2 を **NORM** と呼ぶ．

NORM は，崩壊でなく，かつ線形な等式集合を入力すると，その等式集合を規則化し，それらの規則による複数ステップの書換えを 1 ステップで行える規則を生成する．NORM を図 2 に記す．ここで，以降の議論を簡潔に行うため，NORM はナローイングを用いた定義で記述している(注1)．

次の補題は，NORM の R_i の性質を示す．

(注1)：文献 [2] の NORM の定義と異なる点は，ナローイングによる表現以外に，$normalize$ の適用回数が異なる．しかし，文献 [2] の NORM と本稿の NORM は等価である．

入力 崩壊でなく，かつ線形な等式集合 E
出力 TRS R_E

R を TRS とするとき，関数 $normalize(R)$ を以下に定義する．

- $l \to l$ を削除する．
- すべての $l \to r \in R$ に対して $C[l\sigma] \to C[r\sigma]$ を削除する．

以下，手続きの内容

1. $R_0 := normalize(\{l \to r, r \to l \mid l \approx r \in E\})$，$i := 0$.
2. $R_{i+1} :=$ $normalize(R_i \cup \{l' \to r' \mid l \to r \in R_i,\ (l,r)\ {}_\sigma\!\rightsquigarrow_{R_i}\ (l',r')\})$.
3. $R_{i+1} \neq R_i$ ならば $i := i+1$ として手順 2 へ戻る．
   $R_{i+1} = R_i$ ならば $R_E := R_i$ として終了．

図 2 NORM

補題 5.1 NORM において，すべての i に対して，$l \to r \in R_i$ ならば $r \to l \in R_i$.

[証明] i に関する帰納法と背理法で証明できる． □

次の補題は，NORM の R_i の規則は R_0 の複数ステップの書換えを 1 ステップで行える規則であることを示す．

補題 5.2 NORM において，すべての i に対して，$l \to r \in R_i$ ならば $l \stackrel{+}{\to}_{R_0} r$

[証明] i に関する帰納法と補題 5.1 を用いて証明できる． □

補題 5.4 は，入力の E が補題の条件を満たすとき，NORM の R_i の規則もその条件を満たすことを示す．まず，補題 5.4 で用いる補題 5.3 を示す．

補題 5.3 ([8]) R を右線形の TRS とする．s は線形であり，かつ $s \stackrel{*}{\rightsquigarrow}_R t$ ならば，t は線形である． □

補題 5.4 NORM において，等式集合 E のすべての等式が以下の条件を満たすならば，すべての i に対して R_i のすべての規則も以下の条件を満たす．

1. 線形である．
2. 両辺のすべての真部分項は変数である．
3. 左辺の変数集合と右辺の変数集合が等しい．

[証明] 補題 5.3 を用いることで証明できる． □

定理 3.9 の証明での議論より，TRS R が補題 5.4 の条件 1,2 を満たすとき，$\rightsquigarrow_R = \to_R$ である．これと補題 5.2，5.4 より次の補題が成り立つ．この補題は，入力の E が補題 5.4 の条件 1,2,3 を満たすとき，NORM の R_i の規則は R_0 の規則の左辺または右辺を複数回ナローイングすることで得られることを示す．

補題 5.5 NORM において，等式集合 E のすべての等式が補題 5.4 の条件 1,2,3 を満たすならば，すべての i に対して以下が成り立つ．

$$R_i \subseteq \{l' \to r' \mid l \to r \in R_0,\ (l,r)\ {}_\sigma\!\stackrel{*}{\rightsquigarrow}_{R_0}\ (l',r')\}$$

[証明] i に関する帰納法で証明する． □

次の補題は，入力の E が補題 5.4 の条件 1,2,3 を満たすとき，NORM の R_i の総和が，R_0 のみから定義されるナローイング

到達可能集合の部分集合であることを示す.

補題 5.6 NORM において，等式集合 E のすべての等式が補題 5.4 の条件 1,2,3 を満たすとする．このとき，R_i において以下が成り立つ.

$$\bigcup_{i=0}^{\infty} R_i \subseteqq \overset{*}{\rightsquigarrow}^{\epsilon}_{R_0}(R_0)$$

[証明] 定義 3.2 と補題 5.5 より明らかである. □

次の補題は，入力の E が補題 5.4 の条件 1,2,3 を満たすとき，NORM の R_i が単調増加することを示す.

補題 5.7 NORM において，入力の等式集合 E のすべての等式が補題 5.4 の条件 1,2,3 を満たすとする．このとき，すべての i に対して，$R_i \subseteqq R_{i+1}$.

[証明] E が補題 5.4 の条件 1,2,3 を満たすとき，*normalize* は機能しない．そのため，R_i は定義より単調増加である. □

補題 5.6 と補題 5.7 より，以下の定理が成立する．この定理は，NORM の停止がナローイング到達可能集合の有限性に帰着できることを示す.

定理 5.8 NORM において，入力の等式集合 E のすべての等式が補題 5.4 の条件 1,2,3 を満たすとする．このとき，$\overset{*}{\rightsquigarrow}^{\epsilon}_{R_0}(R_0)$ が名前替えを法として有限であるならば，NORM は停止する.

[証明] 補題 5.6 と補題 5.7 を用いることで証明できる. □

この定理 5.8 と 3 節で示したナローイング到達可能集合の有限性の十分条件を示した定理から NORM が停止するための判定可能な十分条件を与える．ここで，NORM の R_0 は $l \to r \in R_0$ ならば $r \to l \in R_0$ であるため，$R_0 \subseteqq \succ$ となる停止性順序 $\succ$ は存在しない．また，$\to_{R_0}$ は停止性を持たない．そのため，定理 3.6 と系 3.8 の十分条件は，NORM の停止条件とはならない．しかし，定理 3.9 の十分条件は，NORM の停止条件となる．それを次の系で示す.

系 5.9 入力の等式集合 E のすべての等式が以下の条件を満たすならば，NORM は停止する.

1. 線形である.
2. 両辺のすべての真部分項は変数である.
3. 左辺の変数集合と右辺の変数集合が等しい.

[証明] 定理 3.9 と定理 5.8 より明らかである. □

系 5.9 の停止条件は，次のように NORM の実用的な入力に対して NORM の停止性が保障できる.

例 5.10 以下の交換律を表す等式は，系 5.9 の停止条件を満たすため，この等式を入力とするとき，NORM は停止する.

$$g(x,y) \approx g(y,x)$$ □

6. その他の手続きの停止性に関する考察

本節では，その他の類似の手続きの停止性に関して考察する．拡張等式付き書換え系の変換手続き [4] の停止性はナローイング到達可能集合の有限性に帰着させることで，判定可能な十分条件を得られる．しかし，その停止条件を満たす入力に対しては手続きで変換を行う必要がないため，その停止条件は実用的でない．弱最内戦略が完全となる TRS を得る手続き [9] の停止性はその手続きの定義上，ナローイング到達可能集合の有限性に帰着させることができないため，停止条件を得ることができなかった．これは RED に対して帰着が困難であった場合と類似している.

7. おわりに

本稿では，まず，等式付き書換え系の等式数削減手続きと等式付き書換え系の正規化手続きを構成する手続き 2 は共にナローイングを使用して表せるということを見出した．次に，これらの手続きの停止性をナローイング到達可能集合の有限性に帰着させるために，ナローイング到達可能集合が名前替えを法として有限であるための判定可能な十分条件を与えた．そして，各手続きに対して，その停止条件がナローイング到達可能集合の有限性の十分条件となることを示した.

定理 3.9 の条件は制限が厳しい条件であるため，条件の緩和を行うことなどが今後の課題である.

謝辞 本研究は一部，科研費#16650005，#18500011，#17700009，及び栢森情報科学振興財団の補助を受けている.

文　献

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

[2] B. Blanchet and M. Abadi and C. Fournet. "Automated Verification of Selected Equivalences for Security Protocol". Journal of Logic and Algebraic Programming, volume 75, Issue 1, pp. 3–51, 2008.

[3] J. Christian. "Some Termination Criteria for Narrowing and E-Narrowing". In Proceedings of the 11th International Conference on Automated Deduction, pp. 582–588, 1992.

[4] J. Giesl and D. Kapur. "Dependency pairs for equational rewriting". In Proceedings of the 12th International Coference on Rewriting Techniques and Applications, volume 2051 of LNCS, pp. 93–108, 2001.

[5] J. Giesl, R. Thiemann, P. Schneider-Kamp and S. Falke. "Automated termination proofs with aprove". In Proceedings of the 15th International Conference on Rewriting Techniques and Applications, volume 3091 of LNCS, pp. 210–220, 2004.

[6] N. Hirokawa and A. Middeldorp. "Tsukuba termination tool". In Proceedings of the 14th International Conference on Rewriting Techniques and Applications, volume 2703 of LNCS, pp. 311–320, 2003.

[7] J. Hullot. "Canonical Forms and Unification". In Proceedings of the 5th International Conference on Automated Deduction, volume of 87 LNCS, pp. 318–334, 1980.

[8] N. Nishida and M. Sakai T. Sakabe. "Narrowing-Based Simulation of Term Rewriting Systems with Extra Variables and its Termination Proof". Functional and Constraint Logic Programming, volume 86 of ENTCS, Issue 3, pp. 1–18, 2003.

[9] 岡本晃治，酒井正彦，西田直樹，草刈圭一朗，坂部俊樹. "弱最内戦略を完全にする項書換え系の等価変換". 2004 年度 LA シンポジウム冬, pp. 21.1–21.8, 2005.

[10] 三浦浩一，西田直樹，酒井正彦，坂部俊樹，草刈圭一朗. "等式付き書換え系の等式数を削減する変換". 信学技報 SS2006-14, 電子情報通信学会, Vol. 106, No. 120, pp. 7–12, 2006.