Vol.2015-SE-187 No.23
2015/3/12

リアクティブシステム仕様の外部環境制約式に関する研究

深谷 悠一[†1,a)]　吉浦 紀晃[†1,b)]

概要：時相論理で記述されたリアクティブシステム仕様の満たすべき性質の一つに強充足可能性がある．これは「将来生起する環境からの入力が与えられたとき，いかなる入力に対しても仕様を満たす応答が存在する」という性質である．リアクティブシステムは環境に対して開いたシステムであるので，その仕様は環境からのすべての入力パターンを考慮する必要がある．そのため，強充足可能性はリアクティブシステム仕様の満たすべき重要な性質である．仕様が強充足不能であると判明した場合，仕様を修正する必要がある．このとき，仕様の欠陥情報を理解しやすい表現で得ることができれば，仕様を修正する助けとなる．そこで，本論文では強充足不能な仕様の外部環境制約式の導出手続きを提案する．外部環境制約式とは仕様を満たせない環境からの入力の集合を表す時相論理式である．本手続きでは，得られる制約式が単純で直感的な形を保つよう制約式の形を限定する．得られる制約式はその形において最も多くの欠陥情報を表現した式である．

1. はじめに

リアクティブシステムとは環境とインタラクションをとりながらサービスを提供し続けるシステムである．身近な例としては，自動販売機やオペレーティングシステムなどがリアクティブシステムに分類される．これらの中には，エレベータや自動車の制御システムなど，高い安全性が求められるシステムもある．そのため，欠陥のないリアクティブシステムの構築はシステム開発における重要な課題の一つである．

一般的に高い安全性が求められるシステムを設計する際，システムがどのように動作すべきかを分析し，システム仕様が策定される．このとき仕様に欠陥が含まれると仕様に沿って実装されたシステムにも欠陥が含まれてしまう．そのため，システム設計段階で仕様自体を検証することは重要である．

リアクティブシステム仕様は「将来生起する環境からの入力が与えられたとき，いかなる入力に対しても仕様を満たす応答が存在する」という性質を満たす必要がある．この性質は強充足可能性と呼ばれている [4]．もし仕様が強充足不能と判明した場合，仕様の欠陥を明らかにし，仕様を修正する必要がある．仕様が強充足不能になる原因は仕様記述者が環境からのすべての入力を想定することが困難なところにある．そのため，強充足不能な仕様には，仕様を満たせない環境からの入力が生じてしまう．これは別の見方をすると，リアクティブシステムが環境に対して開いたシステムであるにも関わらず，仕様記述者が環境からの入力に対して暗黙の前提条件をつけていることを意味する．この前提条件は仕様が強充足不能に陥る欠陥原因を指し示しているので，これを理解しやすい表現で仕様記述者に提供できれば，仕様を修正する際の助けとなる．

[8], [9] では強充足不能な仕様から，その仕様に含まれる環境からの入力に対する暗黙の前提条件を線形時相論理式で表現し導出する手続きが提案された．この式は外部環境制約式と呼ばれる．このとき，導出される外部環境制約式を時相演算子が 2 つ連続して出現する 2 種類の形に限定することで，仕様記述者が直感的に理解できる外部環境制約式を導出した．一方で，外部環境制約式は仕様の欠陥情報をより詳細に表現することが求められる．もし，より詳細な欠陥情報を単純で直感的な式で表現できれば，仕様記述者により多くの欠陥情報を提供できる．

そこで本論文では [8], [9] で提案された外部環境制約式導出手続きに比べ，より多くの欠陥情報を表現する外部環境制約式の導出手続きを提案する．ただし，式の単純さを保つため，導出される式の形を [8], [9] とは異なる形に制限する．手続きに関わる性質として，手続きの停止性および健全性を示す．さらに，得られる外部環境制約式が制限された式の形の中で最も多くの欠陥情報を表現する外部環境制約式であることを示し，既存の手続きで得られる外部環境制約式との比較を行う．

本論文の構成を次に示す．2 章では，リアクティブシス

†1 現在，埼玉大学大学院理工学研究科
Presently with Saitama Uniersity
a) fukaya@fmx.ics.saitama-u.ac.jp
b) yoshiura@fmx.ics.saitama-u.ac.jp

テムとその仕様の記述言語として線形時相論理 LTL を紹介し，リアクティブシステム仕様の強充足可能性と外部環境制約式について述べる．3 章では，既存の外部環境制約式導出手続きについて述べる．4 章では，本論文で提案する外部環境制約式導出手続きについて述べる．5 章では，4 章で提案する外部環境制約式導出手続きに関する性質について述べる．5 章では，既存の外部環境制約式導出手続きで得られる外部環境制約式と 4 章で提案する外部環境制約式導出手続きで得られる外部環境制約式の強弱関係について述べる．最後に 6 章で本論文をまとめる．

2. リアクティブシステム仕様と外部環境制約式

2.1 リアクティブシステム

リアクティブシステムは，環境とインタラクションをとりながらサービスを提供し続けるシステムであり，次のように定義される．

定義 2.1 (リアクティブシステム)．リアクティブシステム RS は三組み $RS = \langle X, Y, r\rangle$ である．ここで，X は環境が生起する外部イベントの集合，Y はシステムが生起する応答イベントの集合，$r : (2^X)^+ \mapsto 2^Y$ は過去に生起した外部イベントから現在生起させる応答イベント集合を決定するリアクション関数である．ただし，$(2^X)^+$ は外部イベント集合の有限列である．

2.2 リアクティブシステムの仕様

リアクティブシステムの仕様はイベント生起の時間順序を記述し，システムの許可された動作範囲を定める．本論文では仕様の記述言語として線形時相論理 LTL を用いる．命題変数として外部イベントに対応した外部イベント命題変数と応答イベントに対応した応答イベント命題変数を用い，各命題変数が真となることは対応するイベントが生起することを表す．以下では，外部イベント命題変数の集合を $\mathcal{X}$，応答イベント命題変数の集合を $\mathcal{Y}$ で表す．

2.2.1 構文

定義 2.2 (LTL 式)．LTL 式を次のように定義する．

- $p \in \mathcal{X} \cup \mathcal{Y}$ ならば，p は LTL 式である
- φ, ψ が LTL 式ならば，$\neg\varphi, \varphi \wedge \psi, \bigcirc\varphi, \varphi U \psi$ も LTL 式である

略記として $\bot, \top, \vee, \rightarrow, \leftrightarrow$ を通常のように用いる．また，$\Diamond, \Box$ を $\Diamond\varphi \equiv \top U \varphi, \Box\varphi \equiv \neg\Diamond\neg\varphi$ とする．

2.2.2 意味論

外部イベント集合及び応答イベント集合の無限列 $\sigma \in (2^{X\cup Y})^\omega$ を振る舞いとする．LTL 式は振る舞い上で評価される．σ の i 番目のイベント集合を $\sigma[i]$ で表し，$\sigma[i]$ が LTL 式 φ を満たすことを $\sigma, i \models \varphi$ と表す．LTL 式の意味を次のように定義する．

- $\sigma, i \models p$ **iff** $p' \in \sigma[i]$　($p' \in X \cup Y$ は $p \in \mathcal{X} \cup \mathcal{Y}$ に対応するイベント)
- $\sigma, i \models \neg\varphi$ **iff** $\sigma, i \not\models \varphi$
- $\sigma, i \models \varphi \wedge \psi$ **iff** $\sigma, i \models \varphi$ かつ $\sigma, i \models \psi$
- $\sigma, i \models \bigcirc\varphi$ **iff** $\sigma, i+1 \models \varphi$
- $\sigma, i \models \varphi U \psi$ **iff** $(\exists j \geq 0)\Big(\sigma, i+j \models \psi$ かつ $\forall k\,(0 \leq k < j)\,\sigma, i+k \models \varphi\Big)$

2.3 強充足可能性

強充足可能性とは，「将来生起する環境からの入力が与えられたとき，いかなる入力に対しても仕様を満たす応答が存在する」という仕様の性質である．強充足可能性は次のように定義される．

定義 2.3 (強充足可能性)．仕様 $Spec$ が以下を満たすとき，$Spec$ は強充足可能であるという．

$$\forall\tilde{x}\exists\tilde{y}(\langle\tilde{x},\tilde{y}\rangle \models Spec)$$

ここで，$\tilde{x}$ は外部イベント集合の無限列であり，$\tilde{y}$ は応答イベント集合の無限列である．さらに，$\langle\tilde{x},\tilde{y}\rangle$ は振る舞いであり，$\tilde{x} = x_0x_1\ldots, \tilde{y} = y_0y_1\ldots$ であるとき，次のように定義される．

$$\langle\tilde{x},\tilde{y}\rangle = (x_0 \cup y_0)(x_1 \cup y_1)\ldots$$

2.4 外部環境制約式

強充足不能な仕様の外部環境制約式とは，仕様に含まれる環境からの入力に対する暗黙の前提条件を表現する LTL 式である．直感的には「外部イベント列が外部環境制約式を満たすならば，仕様を満たす応答イベント列が存在するような式」である．外部環境制約式は次のように定義される．

定義 2.4 (外部環境制約式)．$Spec$ を仕様，ψ を外部イベント命題変数のみからなる式とする．ψ が以下を満たすとき，ψ は仕様 $Spec$ に対する外部環境制約式であるという．

$$\forall\tilde{a}(\tilde{a} \models \psi \Rightarrow \exists\tilde{b}\langle\tilde{a},\tilde{b}\rangle \models Spec)$$

一般に，仕様に対する外部環境制約式は複数存在する．仕様 $Spec$ の外部環境制約式の集合を $EC(Spec)$ と表す．ここで，外部環境制約式の強弱を次のように定義する．

定義 2.5 (制約式の強弱)．式 ψ_1, ψ_2 を仕様 $Spec$ の外部環境制約式とする．ψ_1, ψ_2 が以下を満たすとき，ψ_2 が ψ_1 より弱いあるいは ψ_1 が ψ_2 より強いといい，$\psi_1 \leq \psi_2$ と表す．

$$\forall\sigma(\sigma \models \psi_1 \Rightarrow \sigma \models \psi_2)$$

ただし，$\psi_1 \leq \psi_2$ かつ $\psi_2 \leq \psi_1$ であるとき，ψ_1 と ψ_2 は同値であるといい，$\psi_1 \equiv \psi_2$ で表す．

さらに，ある式集合 $\mathcal{L}$ の中で最も弱い外部環境制約式を $\mathcal{L}$ における最弱な外部環境制約式という．外部環境制約式の最弱性を次のように定義する．

定義 2.6 (最弱性)．$\mathcal{L}$ を式の集合とする．$Spec$ を仕様とし，$\psi \in (\mathcal{L} \cap EC(Spec))$ であるとする．以下を満たすとき，ψ は $\mathcal{L}$ において最弱な外部環境制約式であるという．

$$\forall \psi'(\psi' \in (\mathcal{L} \cap EC(Spec)) \Rightarrow \psi' \leq \psi)$$

3. 既存の外部環境制約式導出手続き

本章では [8], [9] で提案された外部環境制約式の導出手続きについて述べる．[8], [9] で提案された外部環境制約式の導出手続きでは，導出される外部環境制約式の形を以下で定義されるクラス $\mathcal{L}_1, \mathcal{L}_2$ の形に限定することで，単純で理解しやすい外部環境制約式を得ることができる．さらに，導出される外部環境制約式は $\mathcal{L}_1, \mathcal{L}_2$ において最弱なものである．

定義 3.1 (制約式のクラス $\mathcal{L}_1, \mathcal{L}_2$)．クラス $\mathcal{L}_1, \mathcal{L}_2$ は以下のように定義される．

- $\mathcal{L}_1$ は次の形をした式の集合である

$$\bigwedge \Box\Diamond f$$

- $\mathcal{L}_2$ は次の形をした式の集合である

$$\bigwedge((\bigvee \Diamond\Box f) \vee \Box\Diamond(\bigwedge g))$$

ただし，f, g は古典命題論理式である．

ここで，以下に示す強充足不能な仕様 φ に対して [8], [9] で提案された外部環境制約式導出手続きを適用して得られる $\mathcal{L}_1, \mathcal{L}_2$ において最弱な外部環境制約式 $\psi_{\varphi,1}, \psi_{\varphi,2}$ を示す．以下では，x_1, x_2 を外部イベント命題変数，y を応答イベント命題変数とする．

$$\varphi = \Box((x_1 \wedge x_2) \rightarrow (yU(\neg x_1 \wedge \bigcirc(\neg x_1 \wedge x_2))))$$

φ は強充足不能である．なぜならば，x_1 と x_2 が同時に生起したとき，$\neg x_1 \wedge \bigcirc(\neg x_1 \wedge x_2)$ を満たす外部イベントの生起を暗黙の前提条件としてしまっている．そのため，この条件を満たさない外部イベント列に φ を満たすような応答イベント列は存在しない．φ に対する外部環境制約式 $\psi_{\varphi,1}, \psi_{\varphi,2}$ は以下の通りである．

$$\psi_{\varphi,1} = \bot$$

$$\psi_{\varphi,2} = (\Diamond\Box(x_1 \vee x_2) \vee \Box\Diamond(x_1 \vee x_2)) \wedge (\Diamond\Box\neg x_1)$$

$\psi_{\varphi,1}$ は $\bot$ であり，最も強い外部環境制約式である．このように強い外部環境制約式が導出されてしまう原因はクラス $\mathcal{L}_1, \mathcal{L}_2$ にイベントの生起順序に関して表現できる Next オペレータと Until オペレータが含まれていないためである．φ の環境からの入力に対する暗黙の前提条件は外部イベントがある順序で出現することを要求するものであり，このような前提条件に対してクラス $\mathcal{L}_1, \mathcal{L}_2$ の式では表現力が足りない．

4. 提案手続き

本章では本論文で提案する外部環境制約式の導出手続きを述べる．提案する外部環境制約式導出手続きではそれぞれ $\Box\Diamond(\bigwedge(f \vee \bigcirc g))$ と $\bigwedge((\bigvee \Diamond\Box f) \vee \Box\Diamond(\bigwedge(g \vee \bigcirc h)))$ の形において最弱な外部環境制約式を導出する．ここで，f, g, h は古典命題論理式である．まず，4.1 節で手続きへの入力である非決定性 Büchi オートマトンを定義し，LTL 式から非決定性 Büchi オートマトンへの変換について述べる．4.2 節で導出される外部環境制約式のクラス $\mathcal{L}_3, \mathcal{L}_4$ を定義する．4.3 節で $\mathcal{L}_3$ において最弱な外部環境制約式の導出手続きを述べ，4.4 節で $\mathcal{L}_4$ において最弱な外部環境制約式の導出手続きを述べる．4.5 節で手続きの適用例を示す．

4.1 非決定性 Büchi オートマトン

本論文で提案する外部環境制約式の導出手続きは，仕様を満たす振る舞いの集合を受理言語とする非決定性 Büchi オートマトンを入力とする．LTL 式から非決定性 Büchi オートマトンへの変換は [2] 等で効率的な変換手続きが提案されている．さらに，[7] 等で LTL 式から非決定性 Büchi オートマトンへの変換およびオートマトンの様々な操作を行えるツールが提案されている．本論文ではこれらを用いて予め仕様を非決定性 Büchi オートマトンに変換しておくものとする．非決定性 Büchi オートマトンを次に定義する．

定義 4.1 (非決定性 Büchi オートマトン)．P を命題変数の集合とする．アルファベット 2^P 上の非決定性 Büchi オートマトン $\mathcal{A} = \langle Q, q_0, \delta, F \rangle$ は，状態の有限集合 Q，初期状態 q_0，遷移関係 $\delta \subseteq Q \times B(P) \times Q$，受理状態集合 $F \subseteq Q$ からなる．ここで，$B(P)$ は P 中の命題変数と $\neg, \vee, \wedge$ からなる古典命題論理式の集合である．2^P 上の無限列 $\alpha \in (2^P)^\omega$ に対する $\mathcal{A}$ の行程とは状態の無限列 $\gamma = \gamma[0]\gamma[1]\ldots$ で，$\gamma[0] = q_0$ かつすべての $i \geq 0$ について，古典命題論理式 b が存在し，$(\gamma[i], b, \gamma[i+1]) \in \delta$ かつ $\alpha, i \models b$ となるものである．$In(\gamma) \cap F \neq \emptyset$ であるとき，行程 γ は成功するという．ここで，$In(\gamma)$ は γ 中に無限回出現する状態の集合である．α 上の $\mathcal{A}$ の成功行程が存在するとき，$\mathcal{A}$ が α を受理するという．$\mathcal{A}$ が受理する ω 語の集合を $\mathcal{A}$ の受理言語といい，$L(\mathcal{A})$ で表す．

4.2 制約式のクラス

定義 4.2 (制約式のクラス $\mathcal{L}_3, \mathcal{L}_4$)．クラス $\mathcal{L}_3, \mathcal{L}_4$ は以下のように定義される．

- $\mathcal{L}_3$ は次の形をした式の集合である．

$$\bigwedge \Box\Diamond(\bigwedge(f \vee \bigcirc g))$$

- $\mathcal{L}_4$ は次の形をした式の集合である．

$$\bigwedge((\bigvee \Diamond\Box f) \vee \Box\Diamond(\bigwedge(g \vee \bigcirc h)))$$

ただし，f, g, h は古典命題論理式である．

本論文で設定した外部環境制約式のクラス $\mathcal{L}_3, \mathcal{L}_4$ は，[8], [9] で設定された外部環境制約式のクラス $\mathcal{L}_1, \mathcal{L}_2$ の拡張である．$\mathcal{L}_1, \mathcal{L}_2$ では式に Next オペレータと Until オペレータが出現しないため，イベント生起の時間順序を記述することができない．そこで，$\mathcal{L}_3, \mathcal{L}_4$ では Next オペレータを導入することで，ある時刻とその次の時刻のイベント生起の時間順序を表現できるよう拡張する．

4.3 $\mathcal{L}_3$ において最弱な制約式の導出手続き

手続き 4.1 ($\mathcal{L}_3$ の制約式の導出手続き)．

入力: $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトン $\mathcal{A}_{Spec} = \langle Q, q_0, \delta, F\rangle$

出力: $\psi_3 \in \mathcal{L}_3 \cap EC(Spec)$

STEP1(命題変数の制限) $\mathcal{A}_{Spec}$ を外部イベント命題変数のみに制限した非決定性 Büchi オートマトン $\mathcal{A}'_{Spec} = \langle Q, q_0, \delta', F\rangle$ を構成する．ここで，$\delta' = \{(q, E(b), q') \mid (q, b, q') \in \delta\}$ であり，$E(b)$ は b 中に出現する応答イベント命題変数に $\top$ と $\bot$ をすべての組合せで代入し，その結果を $\vee$ で結んだ式である．ただし，δ' の定義より，$L(\mathcal{A}'_{Spec}) = \{\tilde{a} \mid \exists \tilde{b} \langle \tilde{a}, \tilde{b}\rangle \models Spec\}$ が成り立つ．

STEP2(補集合を受理するオートマトンを構成) $L(\mathcal{A}'_{Spec})$ の補集合を受理する非決定性 Büchi オートマトン $\overline{\mathcal{A}'_{Spec}}$ を構成する．

STEP3(極大強連結成分の探索) $\overline{\mathcal{A}'_{Spec}}$ で初期状態から到達可能な受理状態を含む極大強連結成分を探索し，得られた極大強連結成分の集合を MSC とする．

STEP4(外部環境制約式の導出) MSC の各極大強連結成分 msc に対して式 ψ_{msc} を以下のように定義する．

$$\psi_{msc} = \Diamond\Box(\bigvee_{s \in q(msc)} ((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})))$$

ただし，$q(msc)$ は msc に含まれる状態の集合，$in(s)$ は状態 s に入る msc 内のエッジについたラベルの集合，$out(s)$ は状態 s から出る msc 内のエッジについたラベルの集合である．このとき以下の外部環境制約式 ψ_3 を導出する．

$$\begin{aligned}\psi_3 &= \neg(\bigvee_{msc \in MSC} \psi_{msc}) \\ &= \bigwedge_{msc \in MSC} \Box\Diamond(\bigwedge_{s \in q(msc)} ((\bigwedge_{c_{in} \in in(s)} \neg c_{in}) \vee \bigcirc(\bigwedge_{c_{out} \in out(s)} \neg c_{out})))\end{aligned}$$

4.4 $\mathcal{L}_4$ において最弱な制約式の導出手続き

手続き 4.2 ($\mathcal{L}_4$ の制約式の導出手続き)．

入力: $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトン $\mathcal{A}_{Spec} = \langle Q, q_0, \delta, F\rangle$

出力: $\psi_4 \in \mathcal{L}_4 \cap EC(Spec)$

STEP1，STEP2 は手続き 4.1 と同様．

STEP3(強連結成分の探索) $\overline{\mathcal{A}'_{Spec}}$ で初期状態から到達可能な受理状態を含む強連結成分を探索し，得られた強連結成分の集合を SC とする．

STEP4(外部環境制約式の導出) SC の各強連結成分 sc に対して式 ψ_{sc} を以下のように定義する．

$$\begin{aligned}\psi_{sc} = (&\bigwedge_{c \in l(sc)} \Box\Diamond c) \wedge \\ &\Diamond\Box(\bigvee_{s \in q(sc)} ((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})))\end{aligned}$$

ただし，$q(sc)$ は sc に含まれる状態の集合，$in(s)$ は状態 s に入る sc 内のエッジについたラベルの集合，$out(s)$ は状態 s から出る sc 内のエッジについたラベルの集合である．このとき以下の外部環境制約式 ψ_4 を導出する．

$$\begin{aligned}\psi_4 &= \neg(\bigvee_{sc \in SC} \psi_{sc}) \\ &= \bigwedge_{sc \in SC} ((\bigvee_{c \in l(sc)} \Diamond\Box\neg c) \vee \\ &\qquad \Box\Diamond(\bigwedge_{s \in q(sc)} ((\bigwedge_{c_{in} \in in(s)} \neg c_{in}) \vee \bigcirc(\bigwedge_{c_{out} \in out(s)} \neg c_{out}))))\end{aligned}$$

4.5 手続きの適用例

仕様 $\varphi = \Box((x_1 \wedge x_2) \rightarrow (yU(\neg x_1 \wedge \bigcirc(\neg x_1 \wedge x_2))))$ について，$L(\mathcal{A}_\varphi) = \{\sigma \mid \sigma \models \varphi\}$ を満たす非決定性 Büchi オートマトンを $\mathcal{A}_\varphi$ とする．$\mathcal{A}_\varphi$ に対して手続き 4.1 と手続き 4.2 を適用する．$\mathcal{A}_\varphi$ に STEP1 と STEP2 を適用して得られる非決定性 Büchi オートマトン $\overline{\mathcal{A}'_\varphi}$ を図 1 に示す．図中のエッジのラベルは横に並んだ式が $\wedge$ で結ばれ，縦に並んだ式が $\vee$ で結ばれた式を表している．さらに逆三角のついた状態が初期状態，二重の状態が受理状態を表す．

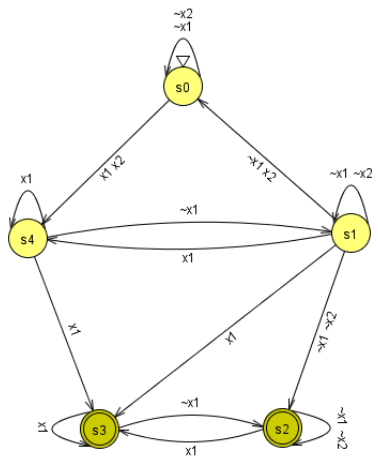

図 1 $\overline{\mathcal{A}'_\varphi}$

得られる外部環境制約式 $\psi_{\varphi,3}, \psi_{\varphi,4}$ を以下に示す．

$$\psi_{\varphi,3} = \Box\Diamond(\neg x_1 \wedge \bigcirc(\neg x_1 \wedge x_2))$$

$$\psi_{\varphi,4} = (\Diamond\Box(x_1 \vee x_2) \vee \Box\Diamond(x_1 \vee x_2)) \wedge (\Diamond\Box\neg x_1 \vee \Box\Diamond(\neg x_1 \wedge \bigcirc\neg x_1)) \wedge (\Diamond\Box\neg x_1 \vee \Diamond\Box(x_1 \vee x_2) \vee \Box\Diamond(\neg x_1 \wedge \bigcirc(\neg x_1 \wedge x_2)))$$

このとき，3 章で示した $\psi_{\varphi,1}, \psi_{\varphi,2}$ との強弱関係は以下に示す通りである．

$$\psi_{\varphi,1} \leq \psi_{\varphi,2} \leq \psi_{\varphi,3} \leq \psi_{\varphi,4}$$

5. 導出手続きの性質

本章では 4 章で述べた外部環境制約式導出手続きの正当性として停止性と健全性を示す．さらに，得られる外部環境制約式がそれぞれ $\mathcal{L}_3, \mathcal{L}_4$ において最弱であることを示し，既存の手続きで得られる外部環境制約式との強弱関係の比較を行う．まず 5.1 節で手続きの停止性を示す．次に 5.2 節で手続きの健全性を示す．5.3 節で手続き 4.1 と手続き 4.2 で導出される外部環境制約式の最弱性を示し，5.4 節で $\mathcal{L}_1, \mathcal{L}_2$ において最弱な外部環境制約式との強弱関係を明らかにする．

5.1 停止性

定理 5.1 (手続き 4.1 と手続き 4.2 の停止性)．$\mathcal{A}_{Spec}$ を $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトンとする．$\mathcal{A}_{Spec}$ に対して手続き 4.1 と手続き 4.2 を適用したとき，手続きは停止する．

証明. STEP1 は $\mathcal{A}_{Spec}$ のエッジ集合が有限であることから停止することは明らかである．STEP2 は [3] より，$L(\mathcal{A}'_{Spec})$ の補集合を受理するオートマトンは必ず存在し，その変換手続きは停止する．有向グラフの極大強連結成分の探索手続きは [6] などがあり，手続きは停止する．また，極大でない強連結成分の探索は極大強連結成分の部分グラフで強連結なものを探索することで得ることができる．したがって，手続き 4.1 と手続き 4.2 は停止する． □

5.2 健全性

定理 5.2 (手続き 4.1 の健全性)．$\mathcal{A}_{Spec}$ を $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトンとする．$\mathcal{A}_{Spec}$ に対して手続き 4.1 を適用して得られる式を ψ_3 とするとき，$\psi_3 \in \mathcal{L}_3 \cap EC(Spec)$ を満たす．

証明. $\psi_3 \in \mathcal{L}_3$ は式の形から明らかである．$\overline{\mathcal{A}'_{Spec}}$ で受理される外部イベント列 $\tilde{a}$ はいつか受理状態を含むある極大強連結成分に到達し，以後，その極大強連結成分内を遷移し続ける．さらにこのとき，極大強連結成分内の任意の状態 s を通るイベントの生起順序は $(\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})$ を満たす．これは，式 $\neg\psi_3$ を満たすことを意味する．したがって，以下により，$\psi_3 \in EC(Spec)$ である．

$$\begin{aligned}
&\forall\tilde{a}(\tilde{a} \in L(\overline{\mathcal{A}'_{Spec}}) \Rightarrow \tilde{a} \models \neg\psi_3)\\
\Leftrightarrow\ &\forall\tilde{a}(\tilde{a} \notin L(\mathcal{A}'_{Spec}) \Rightarrow \tilde{a} \not\models \psi_3)\\
\Leftrightarrow\ &\forall\tilde{a}(\tilde{a} \models \psi_3 \Rightarrow \tilde{a} \in L(\mathcal{A}'_{Spec}))\\
\Leftrightarrow\ &\forall\tilde{a}(\tilde{a} \models \psi_3 \Rightarrow \exists\tilde{b}\langle\tilde{a}, \tilde{b}\rangle \models Spec)\\
\Leftrightarrow\ &\psi_3 \in EC(Spec)
\end{aligned}$$

□

定理 5.3 (手続き 4.2 の健全性)．$\mathcal{A}_{Spec}$ を $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトンとする．$\mathcal{A}_{Spec}$ に対して手続き 4.2 を適用して得られる式を ψ_4 とするとき，$\psi_4 \in \mathcal{L}_4 \cap EC(Spec)$ を満たす．

証明. $\psi_4 \in \mathcal{L}_4$ は式の形から明らかである．$\overline{\mathcal{A}'_{Spec}}$ で受理される外部イベント列 $\tilde{a}$ はいつか受理状態を含むある強連結成分中のエッジのラベルを満たし続け，かつ，その強連結成分に存在するエッジを無限にしばしば通過する．さらにこのとき，強連結成分内の任意の状態 s を通るイベントの生起順序は $(\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})$ を満たす．これは，式 $\neg\psi_4$ を満たすことを意味する．したがって，以下により，$\psi_4 \in EC(Spec)$ である．

$$\begin{aligned}
&\forall\tilde{a}(\tilde{a} \in L(\overline{\mathcal{A}'_{Spec}}) \Rightarrow \tilde{a} \models \neg\psi_4)\\
\Leftrightarrow\ &\forall\tilde{a}(\tilde{a} \notin L(\mathcal{A}'_{Spec}) \Rightarrow \tilde{a} \not\models \psi_4)\\
\Leftrightarrow\ &\forall\tilde{a}(\tilde{a} \models \psi_4 \Rightarrow \tilde{a} \in L(\mathcal{A}'_{Spec}))\\
\Leftrightarrow\ &\forall\tilde{a}(\tilde{a} \models \psi_4 \Rightarrow \exists\tilde{b}\langle\tilde{a}, \tilde{b}\rangle \models Spec)\\
\Leftrightarrow\ &\psi_4 \in EC(Spec)
\end{aligned}$$

□

5.3 最弱性

ここでは，手続き 4.1 と手続き 4.2 で得られる外部環境制約式の最弱性を示す．

定理 5.4 (手続き 4.1 で得られる制約式の最弱性)．$\mathcal{A}_{Spec}$ を $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトンとする．$\mathcal{A}_{Spec}$ に対して手続き 4.1 を適用して得られる式を ψ_3 とする．このとき，ψ_3 は $\mathcal{L}_3$ において最弱である．

証明. 対偶，すなわち，$\psi' \in \mathcal{L}_3$ かつ $\psi' \not\leq \psi_3$ ならば，$\psi' \notin EC(Spec)$ を示す．ψ_3 を以下のようにおく．

$$\psi_3 = \bigwedge_{msc \in MSC} \Box\Diamond(\bigwedge_{s \in q(msc)} ((\bigwedge_{c_{in} \in in(s)} \neg c_{in}) \vee \bigcirc(\bigwedge_{c_{out} \in out(s)} \neg c_{out})))$$

さらに，ψ' を以下のようにおく．

$$\psi' = \bigwedge_{1 \leq i \leq n} (\Box\Diamond(\bigwedge_{j}(f_{ij} \vee \bigcirc g_{ij})))$$

$\psi' \not\leq \psi_3$ より $\tilde{a} \not\models \psi_3$ かつ $\tilde{a} \models \psi'_3$ となる $\tilde{a}$ が存在する．よって，ある msc が存在して $\tilde{a} \models \Diamond\Box(\bigvee_{s\in q(msc)}((\bigvee_{c_{in}\in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out}\in out(s)} c_{out})) \wedge \bigwedge_{1\leq i\leq n}(\Box\Diamond(\bigwedge_j(f_{ij} \vee \bigcirc g_{ij})))$ を満たす．これより，任意の i に対して，ある状態 $s_i \in q(msc)$ と外部イベント集合 a^i_{in}, a^i_{out} が存在し，$(a^i_{in}a^i_{out})\sigma \models ((\bigvee_{c_{in}\in in(s_i)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out}\in out(s_i)} c_{out})) \wedge (\bigwedge_j(f_{ij} \vee \bigcirc g_{ij}))$ である．ただし，σ は任意の外部イベント列である．このことから，任意の i に対して，s_i に入る msc 内のあるエッジ e^i_{in} とそのラベル $c^i_{in} \in in(s_i)$，s_i から出る msc 内のあるエッジ e^i_{out} とそのラベル $c^i_{out} \in out(s_i)$ が存在し，$(a^i_{in}a^i_{out})\sigma \models (c^i_{in} \wedge \bigcirc c^i_{out}) \wedge (\bigwedge_j(f_{ij} \vee \bigcirc g_{ij}))$ である．msc は初期状態から到達可能な受理状態を含む極大強連結成分なので，初期状態から状態 s_1 までの行程が存在する．その行程に対応する有限外部イベント列を $\overline{x}_{q_0,1}$ とする．さらに任意の $i(1 \leq i < n)$ に対して，状態 s_i からエッジ e^i_{out} を通って始まり，msc 内のみを通過し，最後にエッジ e^{i+1}_{in} を通って状態 s_{i+1} に至る行程とそのラベル列 $c^i_{out} \dots c^{i+1}_{in}$ が存在する．その行程に対応する有限外部イベント列を $\overline{x}_{i,i+1} = a^i_{out} \dots a^{i+1}_{in}$ とする．状態 s_n からエッジ e^n_{out} を通って始まり，msc 内のみを通過し，かつ msc 内の受理状態を通過し，最後にエッジ e^1_{in} を通って状態 s_1 に至る行程とそのラベル列 $c^n_{out} \dots c^1_{in}$ も存在する．その行程に対応する有限外部イベント列も同様に $\overline{x}_{n,1} = a^n_{out} \dots a^1_{in}$ とする．このとき次の外部イベント列を考える．

$$\tilde{x} = \overline{x}_{q_0,1} \cdot (\overline{x}_{1,2} \cdot \overline{x}_{2,3} \cdot \dots \cdot \overline{x}_{n-1,n} \cdot \overline{x}_{n,1})^\omega$$

明らかに $\overline{\mathcal{A}'_{Spec}}$ には $\tilde{x}$ に対する成功行程が存在し，$\tilde{x} \in L(\overline{\mathcal{A}'_{Spec}})$ である．また，$\tilde{x}$ には長さ 2 の有限外部イベント列 $(a^1_{in}a^1_{out}), \dots, (a^n_{in}a^n_{out})$ が無限にしばしば出現するため，任意の i に対して $(a^i_{in}a^i_{out})\sigma \models (\bigwedge_j(f_{ij} \vee \bigcirc g_{ij}))$ が成り立つ．したがって，$\tilde{x} \models \bigwedge_{1\leq i\leq n}(\Box\Diamond(\bigwedge_j(f_{ij} \vee \bigcirc g_{ij})))$ である．よって，以下により，$\psi' \notin EC(Spec)$ である．

$$\begin{aligned}
&\tilde{x} \models \psi' \quad \text{and} \quad \tilde{x} \in L(\overline{\mathcal{A}'_{Spec}}) \\
\Rightarrow\ &\neg(\forall\tilde{a}(\tilde{a} \models \psi' \Rightarrow \tilde{a} \notin L(\overline{\mathcal{A}'_{Spec}}))) \\
\Leftrightarrow\ &\neg(\forall\tilde{a}(\tilde{a} \models \psi' \Rightarrow \tilde{a} \in L(\mathcal{A}'_{Spec}))) \\
\Leftrightarrow\ &\neg(\forall\tilde{a}(\tilde{a} \models \psi' \Rightarrow \exists\tilde{b}\langle\tilde{a},\tilde{b}\rangle \models Spec)) \\
\Leftrightarrow\ &\psi' \notin EC(Spec)
\end{aligned}$$

□

定理 5.5 (手続き 4.2 で得られる制約式の最弱性)．
$\mathcal{A}_{Spec}$ を $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトンとする．$\mathcal{A}_{Spec}$ に対して手続き 4.2 を適用して得られる式を ψ_4 とする．このとき，ψ_4 は $\mathcal{L}_4$ において最弱である．

証明. 対偶，すなわち，$\psi' \in \mathcal{L}_4$ かつ $\psi' \not\leq \psi_4$ ならば，$\psi' \notin EC(Spec)$ を示す．ψ_4 を以下のようにおく．

$$\psi_4 = \bigwedge_{sc\in SC}((\bigvee_{c\in l(sc)} \Diamond\Box\neg c) \vee \Box\Diamond(\bigwedge_{s\in q(sc)}((\bigwedge_{c_{in}\in in(s)} \neg c_{in}) \vee \bigcirc(\bigwedge_{c_{out}\in out(s)} \neg c_{out}))))$$

さらに，ψ' を以下のようにおく．

$$\psi' = \bigwedge_i((\bigvee_j \Diamond\Box f_{ij}) \vee \Box\Diamond(\bigwedge_k(g_{ik} \vee \bigcirc h_{ik})))$$

$\psi' \not\leq \psi_4$ より $\tilde{a} \not\models \psi_4$ かつ $\tilde{a} \models \psi'$ となる $\tilde{a}$ が存在する．よって，ある sc が存在して $\tilde{a} \models (\bigwedge_{c\in l(sc)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{s\in q(sc)}((\bigvee_{c_{in}\in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out}\in out(s)} c_{out}))$ である．さらに任意の i に対して $\tilde{a} \models (\bigvee_j \Diamond\Box f_{ij}) \vee \Box\Diamond(\bigwedge_k(g_{ik} \vee \bigcirc h_{ik})$ を満たす．すなわち任意の i に対して，次の 1 または 2 のいずれかを満たす．

1. ある j_i が存在して，$\tilde{a} \models \Diamond\Box f_{ij_i}$
2. $\tilde{a} \models \Box\Diamond(\bigwedge_k(g_{ik} \vee \bigcirc h_{ik}))$

1 を満たす i を集めた集合を V とし，2 を満たす i を集めた集合を W とする．このとき，$\tilde{a} \models (\bigwedge_{v\in V} \Diamond\Box f_{vj_v}) \wedge (\bigwedge_{w\in W} \Box\Diamond(\bigwedge_k(g_{wk} \vee \bigcirc h_{wk})))$ である．よって，$\tilde{a} \models (\bigwedge_{v\in V} \Diamond\Box f_{vj_v}) \wedge (\bigwedge_{w\in W} \Box\Diamond(\bigwedge_k(g_{wk} \vee \bigcirc h_{wk}))) \wedge (\bigwedge_{c\in l(sc)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{s\in q(sc)}((\bigvee_{c_{in}\in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out}\in out(s)} c_{out}))$ を満たす．このことから，次の 3 と 4 が成り立つ．

3. 任意の $c \in l(sc)$ に対して，ある外部イベント集合 α_c が存在し，$\alpha_c \models (\bigwedge_{v\in V} f_{vj_v}) \wedge c$ を満たす．つまり，sc に含まれるすべてのエッジは $(\bigwedge_{v\in V} f_{vj_v})$ を満たすように遷移することができる．
4. 任意の $w \in W$ に対して，ある状態 $s_w \in q(sc)$ と外部イベント集合 a^w_{in}, a^w_{out} が存在し，$(a^w_{in}a^w_{out})\sigma \models (\bigwedge_{v\in V} f_{vj_v}) \wedge (\bigcirc(\bigwedge_{v\in V} f_{vj_v})) \wedge (\bigwedge_k(g_{wk} \vee \bigcirc h_{wk})) \wedge ((\bigvee_{c_{in}\in in(s_w)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out}\in out(s_w)} c_{out}))$ を満たす．ただし，σ は任意の外部イベント列である．このことから，任意の w に対して，s_w に入る sc 内のあるエッジ e^w_{in} とそのラベル c^w_{in}，s_w から出る sc 内のあるエッジ e^w_{out} とそのラベル c^w_{out} が存在し $(a^w_{in}a^w_{out})\sigma \models (\bigwedge_{v\in V} f_{vj_v}) \wedge (\bigcirc(\bigwedge_{v\in V} f_{vj_v})) \wedge (\bigwedge_k(g_{wk} \vee \bigcirc h_{wk})) \wedge (c^w_{in} \wedge \bigcirc c^w_{out})$ を満たす．

ここで，集合 W の各要素について言及するため，$W = \{w_1, w_2, \dots, w_{|W|}\}$ とする．sc は $\overline{\mathcal{A}'_{Spec}}$ の初期状態から到達可能な受理状態を含む強連結成分なので初期状態から状態 s_{w_1} までの行程が存在する．その行程に対応する有限外部イベント列を $\overline{x}_{q_0,1}$ とする．さらに任意の $n(1 \leq n < |W|)$ に対して，状態 s_{w_n} からエッジ $e^{w_n}_{out}$ を通って始まり，sc 内のみを通過し，最後にエッジ $e^{w_{n+1}}_{in}$ を通って状態 $s_{w_{n+1}}$ に至る行程とそのラベル列 $c^{w_n}_{out}c_1 \dots c_m c^{w_{n+1}}_{in}$ が存在する．その行程に対応する有限長の外部イベント列を $\overline{x}_{n,n+1} = a^{w_n}_{out}\alpha_{c_1} \dots \alpha_{c_m} a^{w_{n+1}}_{in}$ とする．状態 $s_{w_{|W|}}$ から

エッジ $e_{out}^{w_{|W|}}$ を通って始まり，sc 内のみを通過し，かつ sc 内の受理状態を通過し，最後にエッジ $e_{in}^{w_1}$ を通って状態 s_{w_1} に至る行程も存在する．その行程に対応するイベント集合列も同様に $\overline{x}_{|W|,1}$ とする．このとき次のような外部イベント列を考える．

$$\tilde{x} = \overline{x}_{q_0,1} \cdot (\overline{x}_{1,2} \cdot \overline{x}_{2,3} \cdot \ldots \cdot \overline{x}_{|W|-1,|W|} \cdot \overline{x}_{|W|,1})^{\omega}$$

明らかに $\overline{\mathcal{A}'_{Spec}}$ には $\tilde{x}$ に対する成功行程が存在し，$\tilde{x} \in L(\overline{\mathcal{A}'_{Spec}})$ である．また，$\tilde{x}$ には長さ 2 の有限外部イベント列 $(a_{in}^{w_1} a_{out}^{w_1}), \ldots, (a_{in}^{w_{|W|}} a_{out}^{w_{|W|}})$ が無限にしばしば出現する．したがって，4 より $\tilde{x} \models \bigwedge_{w \in W} \Box\Diamond(\bigwedge_k (g_{wk} \vee \bigcirc h_{wk}))$ である． さらに，任意の n に対する有限外部イベント列 $\overline{x}_{n,n+1}$ と $\overline{x}_{|W|,1}$ 中に出現するすべての外部イベント集合は，3 と 4 より式 $\bigwedge_{v \in V} f_{vj_v}$ を充足させる．よって，$\tilde{x} \models \bigwedge_{v \in V} \Diamond\Box f_{vj_v}$ である．以上のことから $\tilde{x} \models \psi'$ が成り立つ．よって，以下により，$\psi' \notin EC(Spec)$ である．

$$\begin{aligned}
&\tilde{x} \models \psi' \quad \text{and} \quad \tilde{x} \in L(\overline{\mathcal{A}'_{Spec}}) \\
\Rightarrow\ &\neg(\forall \tilde{a}(\tilde{a} \models \psi' \Rightarrow \tilde{a} \notin L(\overline{\mathcal{A}'_{Spec}}))) \\
\Leftrightarrow\ &\neg(\forall \tilde{a}(\tilde{a} \models \psi' \Rightarrow \tilde{a} \in L(\mathcal{A}'_{Spec}))) \\
\Leftrightarrow\ &\neg(\forall \tilde{a}(\tilde{a} \models \psi' \Rightarrow \exists \tilde{b} \langle \tilde{a}, \tilde{b} \rangle \models Spec)) \\
\Leftrightarrow\ &\psi' \notin EC(Spec)
\end{aligned}$$

□

5.4 外部環境制約式の強弱関係

この節では各外部環境制約式導出手続きによって導出される外部環境制約式の強弱関係を示す．[8], [9] で提案された出手続きで得られる $\mathcal{L}_1, \mathcal{L}_2$ において最弱な外部環境制約式との比較では，手続きについて言及する必要があるため，まず [8], [9] で提案された外部環境制約式導出手続きを示す．以下に示す手続き 5.1 及び手続き 5.2 は [9] によるものである．

手続き 5.1 ($\mathcal{L}_1$ の制約式の導出手続き).
入力: $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトン $\mathcal{A}_{Spec} = \langle Q, q_0, \delta, F \rangle$
出力: $\psi_1 \in \mathcal{L}_1 \cap EC(Spec)$
STEP1，STEP2，STEP3 は手続き 4.1 と同様.
STEP4(外部環境制約式の導出) MSC の各極大強連結成分 msc に対して式 ψ_{msc} を以下のように定義する．

$$\psi_{msc} = \Diamond\Box(\bigvee_{c \in l(msc)} c)$$

ここで，$l(msc)$ は msc の各エッジについたラベルの集合である．このとき，以下の外部環境制約式 ψ_1 を導出する．

$$\begin{aligned}
\psi_1 &= \neg(\bigvee_{msc \in MSC} \psi_{msc}) \\
&= \bigwedge_{msc \in MSC} (\Box\Diamond(\bigwedge_{c \in l(msc)} \neg c))
\end{aligned}$$

手続き 5.2 ($\mathcal{L}_2$ の制約式の導出手続き).
入力: $L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトン $\mathcal{A}_{Spec} = \langle Q, q_0, \delta, F \rangle$
出力: $\psi_2 \in \mathcal{L}_2 \cap EC(Spec)$
STEP1，STEP2，STEP3 は手続き 4.2 と同様.
STEP4(外部環境制約式の導出) SC の各強連結成分 sc に対して式 ψ_{sc} を以下のように定義する．

$$\psi_{sc} = (\bigwedge_{c \in l(sc)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{c \in l(sc)} c)$$

このとき，以下の外部環境制約式 ψ_2 を導出する．

$$\begin{aligned}
\psi_2 &= \neg(\bigvee_{sc \in SC} \psi_{sc}) \\
&= \bigwedge_{sc \in SC} ((\bigvee_{c \in l(sc)} \Diamond\Box\neg c) \vee \Box\Diamond(\bigwedge_{c \in l(sc)} \neg c))
\end{aligned}$$

仕様 $Spec$ について，$L(\mathcal{A}_{Spec}) = \{\sigma \mid \sigma \models Spec\}$ を満たす非決定性 Büchi オートマトンを $\mathcal{A}_{Spec}$ とする．以下では $\mathcal{A}_{Spec}$ に対して手続き 5.1, 手続き 5.2 を適用して得られる外部環境制約式をそれぞれ ψ_1, ψ_2 とし，手続き 4.1, 手続き 4.2 を適用して得られる外部環境制約式をそれぞれ ψ_3, ψ_4 とする．

定理 5.6 (ψ_1, ψ_2 の強弱関係). ψ_1, ψ_2 は以下を満たす．

$$\psi_1 \leq \psi_2$$

証明. $\psi_1 \not\leq \psi_2$ と仮定し，矛盾を導くことで証明を行う．仮定より以下が成り立つ．

$$\begin{aligned}
&\neg(\forall \sigma(\sigma \models \psi_1 \Rightarrow \sigma \models \psi_2)) \\
\Leftrightarrow\ &\exists \sigma(\sigma \models \psi_1 \wedge \sigma \not\models \psi_2) \\
\Leftrightarrow\ &\exists \sigma(\sigma \not\models \neg\psi_1 \wedge \sigma \models \neg\psi_2)
\end{aligned}$$

このことより，$\sigma \not\models \neg\psi_1$ かつ $\sigma \models \neg\psi_2$ を満たす外部イベント列 σ が存在する．$\neg\psi_2 = \bigvee_{sc \in SC}((\bigwedge_{c \in l(sc)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{c \in l(sc)} c))$ なので，ある強連結成分 sc_T が存在して，$\sigma \models (\bigwedge_{c \in l(sc_T)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{c \in l(sc_T)} c)$ である．このとき，σ 上で初めて $\langle \sigma, i \rangle \models \Box(\bigvee_{c \in l(sc_T)} c)$ が成り立つ時刻 i が存在し，$j \geq 0$ について sc_T 内のあるエッジに付いたラベル c_{i+j} が存在し，$\sigma, i+j \models c_{i+j}$ を満たす．sc_T は強連結成分なので $sc_T \subseteq msc_T$ となる極大強連結成分 msc_T が存在し，msc_T に対応する $\neg\psi_1$ の部分式 $\psi_{msc_T} = \Diamond\Box(\bigvee_{c \in l(msc_T)} c)$ が存在する．$l(sc_T) \subseteq l(msc_T)$ であるので，式の構造より $\Diamond\Box(\bigvee_{c \in l(sc_T)} c)$ が真となる外部イベント列上で $\Diamond\Box(\bigvee_{c \in l(msc_T)} c)$ も真となる．よって，$\sigma \models \Diamond\Box(\bigvee_{c \in l(msc_T)} c)$ であることから，$\sigma \models \neg\psi_1$ が成り立ち矛盾する．したがって，$\psi_1 \leq \psi_2$ である． □

定理 5.7 (ψ_3, ψ_4 の強弱関係). ψ_3, ψ_4 は以下を満たす．

$$\psi_3 \leq \psi_4$$

証明. 証明は定理 5.6 と同様に行うことができる. □

定理 5.8 (ψ_1, ψ_3 の強弱関係). ψ_1, ψ_3 は以下を満たす.

$$\psi_1 \leq \psi_3$$

証明. $\psi_1 \not\leq \psi_3$ と仮定し，矛盾を導くことで証明を行う. 仮定より以下が成り立つ.

$$\begin{aligned}
&\neg(\forall\sigma(\sigma \models \psi_1 \Rightarrow \sigma \models \psi_3)) \\
\Leftrightarrow\ &\exists\sigma(\sigma \models \psi_1 \wedge \sigma \not\models \psi_3) \\
\Leftrightarrow\ &\exists\sigma(\sigma \not\models \neg\psi_1 \wedge \sigma \models \neg\psi_3)
\end{aligned}$$

このことより，$\sigma \not\models \neg\psi_1$ かつ $\sigma \models \neg\psi_3$ を満たす外部イベント列 σ が存在する. $\neg\psi_3 = \bigvee_{msc \in MSC} \Diamond\Box(\bigvee_{s \in q(msc)} ((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})))$ なので，ある極大強連結成分 msc_T が存在して，$\sigma \models \Diamond\Box(\bigvee_{s \in q(msc_T)} ((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})))$ である. このとき，σ 上で初めて $\sigma, i \models \Box(\bigvee_{s \in q(msc_T)}((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})))$ が成り立つ時刻 i が存在し，$j \geq 0$ について msc_T 内のあるエッジについたラベル c_{in}^{i+j} が存在し，$\sigma, i+j \models c_{in}^{i+j}$ を満たす. また，msc_T に対応する $\neg\psi_1$ の部分式 $\Diamond\Box(\bigvee_{c \in l(msc_T)} c)$ が存在し，すべての j について $c_{in}^{i+j} \in l(msc)$ が存在し $\sigma, i+j \models c_{in}^{i+j}$ を満たすことから $\sigma \models \Diamond\Box(\bigvee_{c \in l(msc)} c)$ が成り立つ. よって，$\sigma \models \neg\psi_1$ であり，矛盾する. したがって，$\psi_1 \leq \psi_3$ である. □

定理 5.9 (ψ_2, ψ_4 の強弱関係). ψ_2, ψ_4 は以下を満たす.

$$\psi_2 \leq \psi_4$$

証明. $\psi_2 \not\leq \psi_4$ と仮定し，矛盾を導くことで証明を行う. 仮定より以下が成り立つ.

$$\begin{aligned}
&\neg(\forall\sigma(\sigma \models \psi_2 \Rightarrow \sigma \models \psi_4)) \\
\Leftrightarrow\ &\exists\sigma(\sigma \models \psi_2 \wedge \sigma \not\models \psi_4) \\
\Leftrightarrow\ &\exists\sigma(\sigma \not\models \neg\psi_2 \wedge \sigma \models \neg\psi_4)
\end{aligned}$$

このことより，$\sigma \not\models \neg\psi_2$ かつ $\sigma \models \neg\psi_4$ を満たす外部イベント列 σ が存在する. $\neg\psi_4 = \bigvee_{sc \in SC}((\bigwedge_{c \in l(sc)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{s \in q(sc)}((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out}))))$ なので，ある強連結成分 sc_T が存在して，$\sigma \models (\bigwedge_{c \in l(sc_T)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{s \in q(sc_T)}((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})))$ である. このとき，σ 上で初めて $\sigma, i \models \Box(\bigvee_{s \in q(sc_T)} ((\bigvee_{c_{in} \in in(s)} c_{in}) \wedge \bigcirc(\bigvee_{c_{out} \in out(s)} c_{out})))$ が成り立つ時刻 i が存在し，$j \geq 0$ について sc_T 内のあるエッジについたラベル c_{in}^{i+j} が存在し，$\sigma, i+j \models c_{in}^{i+j}$ を満たす. また，sc_T に対応する $\neg\psi_2$ の部分式 $(\bigwedge_{c \in l(sc_T)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{c \in l(sc_T)} c)$ が存在し，すべての j について $c_{in}^{i+j} \in l(sc)$ が存在し $\sigma, i+j \models c_{in}^{i+j}$ を満たすことから $\sigma \models \Diamond\Box(\bigvee_{c \in l(sc)} c)$ が成り立つ. さらに，$\sigma \models \bigwedge_{c \in l(sc)} \Box\Diamond c$ であることから $\sigma \models (\bigwedge_{c \in l(sc_T)} \Box\Diamond c) \wedge \Diamond\Box(\bigvee_{c \in l(sc_T)} c)$ である. よって，$\sigma \models \neg\psi_2$ であり，矛盾する. したがって，$\psi_2 \leq \psi_4$ である. □

定理 5.6 及び定理 5.9 より定理 5.10 が成り立つ.

定理 5.10 (ψ_1, ψ_2, ψ_4 の強弱関係). ψ_1, ψ_2, ψ_4 は以下を満たす.

$$\psi_1 \leq \psi_2 \leq \psi_4$$

6. まとめ

本論文では強充足不能なリアクティブシステム仕様の外部環境制約式の導出手続きを提案した. 本手続きに関わる性質として，手続きの停止性と健全性，制限されたクラス内での最弱性を示した. さらに既存の手続きで得られる外部環境制約式より弱い外部環境制約式が得られることを示した.

参考文献

[1] Abadi, M., Lamport, L., and Wolper, P.: Realizable and Unrealizable Specifications of Reactive Systems, in *Proceedings of the 16th International Colloquium on Automata, Languages and Programing*, pp. 1-17, (1989).

[2] Gastin, P. and Oddoux, D.: Fast LTL to Büchi Automata Translation, in *Proc. of the 13th International Conference on Computer Aided Verification (CAV 2001)*, Lecture Notes in Computer Science, Vol.2102, pp. 53-65, Springer (2001).

[3] Grädel, E., Thomas, W. and Wilke, T.(Eds.): *Automata, Logics, and Infinite Games: A Guide to Current Research*, Lecture Notes in Computer Science, Vol.2500, Springer (2002).

[4] Mori, R. and Yonezaki, N.: Several Realizability Concepts in Reactive Objects, *Information Modeling and Knowledge Bases*, IOS Press (1993).

[5] Pnueli, A. and Rosner, R.: On the synthesis of a reactive module, in *Proceedings of the 16th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pp.179-190 (1989).

[6] Tarjan, R. E.: Depth-First Search and Linear Graph Algorithms, *SIAM Journal on Computing*, Vol.1, No.2, pp.146-160 (1972).

[7] Tsay, Y.-K., Chen, Y.-F., Tsai, M.-H., Wu, K.-N. and Chan, W.-C.: GOAL: A Graphical Tool for Manupulating Büchi Automata and Temporal Formulae, in *Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2007)*, Lecture Notes in Computer Science, Vol.4424, pp.466-471, Springer (2007).

[8] 北村佑介, 島川昌也, 萩原茂樹, 米崎直樹: リアクティブシステム仕様の外部環境制約について, 第五回システム検証の科学技術シンポジウム予稿集, pp. 7-18 (2008).

[9] 萩原茂樹, 北村佑介, 島川昌也, 関戸聡, 米崎直樹: リアクティブシステム仕様を実現可能にするための環境制約の抽出, コンピュータソフトウェア, Vol. 28, No.3, pp.132-146, 2011.

[10] 森亮靖, 友石正彦, 米崎直樹: 時相論理によるリアクティブシステム仕様の実現可能性に関する分類, コンピュータソフトウェア, Vol. 15, No.3, pp.25-37 (1998).