マルチメディア通信と分散処理　82－12
（１９９７．４．２４）

命題論理に基づく要求仕様の詳細化とその支援

福沢 尚司＊　郷 健太郎＊　高橋 薫†　白鳥 則郎＊
＊東北大学電気通信研究所 / 情報科学研究科　〒980-77 仙台市青葉区片平 2-1-1　Tel: (022)217-5454
E-mail: {fukuzawa,go,norio}@shiratori.riec.tohoku.ac.jp
† 仙台電波工業高等専門学校　〒989-31 仙台市青葉区上愛子字北原 1　Tel: (022)392-4761
E-mail: kaoru@cc.sendai-ct.ac.jp

あらまし　大規模なシステムの開発では，システムの機能・性質に対するユーザの要求からシステムの動作仕様を得るために多大な労力を必要とする．このため，命題論理に基づく機能要求記述を単位とする要求仕様から，有限状態機械に基づくシステム仕様を導出する手法が提案されている．本稿ではこの手法に基づき，要求仕様の詳細化による段階的要求獲得の枠組みとして，(1) 要求仕様の階層化と (2) 機能要求記述の置換の２つを提案し，また，詳細化の具体的支援法として，(3) 要求仕様の分割による詳細化対象の明確化を提案する．さらに，簡易 TV システムへの適用例を用いて本支援法の有効性を示す．

Refinement of a Requirement Specification based on Propositional Logic and Its Support Method

Shoji Fukuzawa*, Kentaro Go*, Kaoru Takahashi† and Norio Shiratori*
*Research Institute of Electrical Communication / Graduate School of Information Sciences, Tohoku University, 2-1-1 Katahira, Aoba, Sendai 980-77, Japan　Tel: +81-22-217-5454
E-mail: {fukuzawa,go,norio}@shiratori.riec.tohoku.ac.jp
†Sendai National College of Technology, 1 Kitahara, Kamiayashi, Aoba, Sendai 989-31, Japan
Tel: +81-22-392-4761　E-mail: kaoru@cc.sendai-ct.ac.jp

Abstract　In the development of a large system, it is difficult to obtain a system specification from user's requirements such as system's functions or its property. A method to derive a system specification based on finite state machine from a requirement specification based on propositional logic has been proposed. In this paper, based on this method, we propose some frameworks of refinement method of a requirement specification. We also propose some support methods for refinement of the requirement specification along with those frameworks. Finally, we present a real application of our method to simple TV system, in order to demonstrate the effectiveness of our method.

1 はじめに

システム開発サイクルの要求仕様とシステム仕様を記述する工程に形式仕様を導入することで，仕様記述工程におけるシステムのエラー混入を防ぐことができる．これは，通信システムなどの高い信頼性が要求されるシステムを開発する場合に有効である．文献[1]は，命題論理に基づいてシステムの持つべき性質・機能を宣言的に記述する要求仕様と，有限状態機械に基づくシステム仕様の定義を与え，要求仕様からシステム仕様を導出する手法を提案している．この要求仕様は機能要求記述の集合で与えられるため，部分的な記述が行なわれている要求仕様に対し，機能要求記述の付加・削除を繰り返し行なって徐々に目的の要求仕様の完成に近付けていくという要求仕様の段階的記述が可能である．

本稿では文献[1]に基づいて以下の提案を行ない，要求仕様の詳細化法とその支援法を与える．

(1) 階層化と置換のための要求仕様の拡張．
(2) 階層化による詳細化と，置換による詳細化の枠組みの提案．
(3) 要求仕様の分割による詳細化対象の明確化．

本稿の構成は，以下の通りである．まず第2節で命題論理に基づく要求仕様の定義を示す．第3節では要求仕様の詳細化とその支援について述べる．第4節では適用例を示し，最後に第5節でまとめと課題を述べる．

2 命題論理に基づく要求仕様

本稿では文献[1]の手法に従い，命題論理に基づいて機能を記述する機能要求記述と，その集合で与えられる要求仕様を用いる．

$\mathcal{P}$ を素命題の有限集合とする．システムの状態は，その状態が満たしている条件を記述する命題論理式 $\gamma_1 \vee ... \vee \gamma_i \vee ... \vee \gamma_n$ ($\gamma_i = l_1 \wedge ... \wedge l_j \wedge ... \wedge l_m$ または $\gamma_i = 1$) で示される．ここで l_j は A のリテラル（素命題 A あるいは素命題の否定 $\neg A$）であり，A のリテラル同士の連言は禁止する．また，1は常に成立する条件である．

システムの動作は，外部からある入力が行われたとき，外部への出力，状態の遷移によって示される．また，システムの動作は，システムが何らかの条件を満たすとき可能であるとみなせる．これにより，ある動作の後に次の動作が可能になる連続的な動作を，動作に伴いシステムの条件が変更されることで表せる．このとき，システムの状態集合は，ある動作が可能な状態の部分集合と不可能な状態の部分集合とによって与えられる．以上の概念から，システムの機能要求記述は次の形式で定義される．

定義 2.1 （機能要求記述）
機能要求記述は5項組 $\rho = \langle id, a, f_{in}, o, f_{out} \rangle$ で定義される．ここで，id は機能名，a は入力，f_{in} は実行前条件，o は出力，f_{out} は機能実行後条件である．id, a, o は文字列（o は空出力 ε の場合がある），f_{in} は選言標準形，f_{out} は連言形の命題論理式である． □

省略記法として，機能要求記述 ρ を $id : f_{in} \overset{a/o}{\Rightarrow} f_{out}$ と記述する．特に o が空出力 ε の場合，$id : f_{in} \overset{a}{\Rightarrow} f_{out}$ と記述する．

要求仕様は，機能要求記述の集合を使って表現される．これにより，機能要求記述の付加・削除を他の機能要求記述と独立に行うことができる．

定義 2.2 （要求仕様）
要求仕様は3項組 $\mathcal{R} = \langle R, \gamma_0, \gamma_e \rangle$ で定義される．ここで，R は機能要求記述の有限集合，γ_0 は全ての素命題のリテラルを含む連言形の命題論理式で記述される初期条件，γ_e は選言標準形の命題論理式で記述される最終条件である．γ_e は省略可能であるとし，省略された場合は初期条件と同一であるとする． □

3 要求仕様の詳細化とその支援法

要求仕様の詳細化は，要求仕様に情報を付加する作業である．詳細化により，部分的な要求仕様から徐々に目的のシステムの要求仕様に近付けていくという要求仕様の段階的な獲得が可能である．要求仕様は機能要求記述の集合を使って表現されるため，集合の性質から，段階的に機能要求記述を追加することが可能である．

情報の付加を効果的に行なうために，まず詳細化のための要求仕様の拡張を行ない，それに基づき詳細化の枠組みを与える．また，詳細化の支援法を構成する．

3.1 要求仕様の拡張

要求仕様の詳細化のため，(1) 階層化，(2) 置換に関して要求仕様の拡張を行う．

3.1.1 階層化

階層化は，「ある条件が成立しているシステムにおける要求の記述」を表現するものである．要求仕様を階層化するために，条件付き要求仕様を定義する．

定義 3.1 （条件付き要求仕様）
条件付き要求仕様は3項組 $\mathcal{CR} = \langle \eta, \mathcal{P}, \mathcal{R} \rangle$ で定義される．ここで，η は連言形の命題論理式，$\mathcal{P}$ は素命題の有限集合，$\mathcal{R}$ は要求仕様であり，以下の条件を満たす．

(1) $\mathcal{R}$ に現れる素命題は，$\mathcal{P}$ に含まれるものだけである．
(2) 任意の $\rho \in \mathcal{P}$ は η に現れない． □

条件付き要求仕様 $\langle \eta, \mathcal{P}, \mathcal{R} \rangle$ の意味は，要求仕様 $\mathcal{R}$ の実行後条件を除く全ての条件を，元の条件と η の連言で置き換えた要求仕様 $\mathcal{R}'$ によって与えられる．

条件付き要求仕様を用い，階層化要求仕様を定義する．

定義 3.2 （階層化要求仕様）

階層化要求仕様は $\mathcal{HR} = \{\mathcal{CR}_i\}$ で与えられる．ここで，$\mathcal{CR}_i = \langle \eta_i, \mathcal{P}_i, \mathcal{R}_i \rangle$ は条件付き要求仕様であり，$\eta_i = 1$ である i が唯一存在する．また，$\eta_i \neq 1$ である $\mathcal{CR}_i = \langle \eta_i, \mathcal{P}_i, \mathcal{R}_i \rangle$ は以下の条件を満たす．

(1) $i \neq j$ なる $\langle \eta_j, \mathcal{P}_j, \mathcal{R}_j \rangle \in \mathcal{HR}$ について，$\mathcal{P}_i \cap \mathcal{P}_j = \phi$

(2) η_i を満たす η_j を持ち，かつ η_i に現れて η_j に現れない全ての素命題を含む $\mathcal{P}_j$ $(i \neq j)$ を持つ条件付き要求仕様 $\langle \eta_j, \mathcal{P}_j, \mathcal{R}_j \rangle$ が $\mathcal{HR}$ に唯一存在する．

(3) η_i を満たすような η_j を持つ全ての条件付き要求仕様 $\langle \eta_j, \mathcal{P}_j, \mathcal{R}_j \rangle \in \mathcal{HR}$ について，η_j に現れる任意の素命題は $\mathcal{P}_i$ の要素でない． □

定義3.2において，条件付き要求仕様 $\mathcal{CR}_i$ を，階層化要求仕様 $\mathcal{HR}$ における階層と呼ぶ．特に定義3.2 (2) に関して，$\mathcal{CR}_j$ を $\mathcal{CR}_i$ の上階層，$\mathcal{CR}_i$ を $\mathcal{CR}_j$ の下階層と呼ぶ．また，$\eta_i = 1$ の階層を最上階層と呼ぶ．

定義3.2は，階層化要求仕様の階層間で記述に用いる素命題の重複がないこと，各階層は高々1つの上階層を持ち，階層 $\langle \eta_i, \mathcal{P}_i, \mathcal{R}_i \rangle$ が上階層 $\langle \eta_j, \mathcal{P}_j, \mathcal{R}_j \rangle$ を持つとき，η_i は上階層の η_j と，上階層の $\mathcal{P}_j$ に含まれる素命題だけを用いて記述されるある条件 η_i' の連言 $\eta_j \wedge \eta_i'$ であること，そして，ある階層の上階層の，さらに上階層をたどっていくと，元の階層に戻ることなく，最上階層にたどりついて停止することを示している．

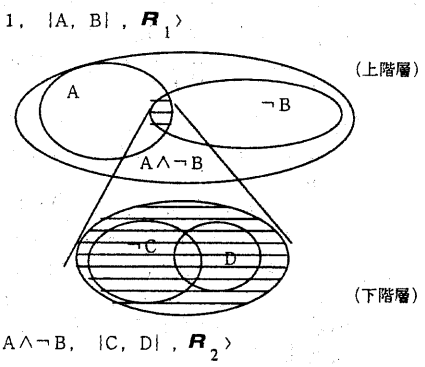

図 1: 階層化要求仕様

階層化要求仕様 $\mathcal{HR} = \{\mathcal{CR}_i\}$ の意味は，条件付き要求仕様 $\mathcal{CR}_i = \langle \eta_i, \mathcal{P}_i, \mathcal{R}_i \rangle$ の意味が要求仕様 $\langle R_i, \gamma_{oi}, \gamma_{ei} \rangle$ で与えられるとき，要求仕様 $\langle \bigcup_i R_i, \bigwedge_i \gamma_{oi}, \bigwedge_i \gamma_{ei} \rangle$ で与えられる．

3.1.2 置換

機能要求記述の集合を，より多くの要素を含んだ別の機能要求記述の集合で置き換えることにより，詳細化することが可能である．

置換のための構造化として，機能要求記述に一括化の機能を加える．

定義 3.3 （機能要求記述の一括化）

機能要求記述 $id_1 : f_{in} \overset{a/o}{\Rightarrow} f_{out1}, ..., id_n : f_{in} \overset{a/o}{\Rightarrow} f_{outn}$ が以下の条件を満たすとき，これらの機能要求記述を1つの機能要求記述として扱う．

(1) $id_1 = ... = id_n = id$

(2) $f_{out1}, ..., f_{outn}$ の全てに関して，ある素命題 A と $\neg A$ の両方が現れることはない．

このとき，機能要求記述 $id_1, ..., id_n$ は全体で $id : f_{in} \overset{a/o}{\Rightarrow} \bigwedge_i f_{outi}$ と等しい意味を持つとみなす．これを機能要求記述の一括化という． □

次に，1つの機能要求記述を新たな情報を加えた2つの機能要求記述で置換する方法として機能要求記述の場合分けを定義する．

定義 3.4 （機能要求記述の場合分け）

機能要求記述 $id : f_{in} \overset{a/o}{\Rightarrow} f_{out}$ を，f_{in} に現れない素命題を用いた連言形の命題論理式で記述される条件 g を用い，$f_{in} \wedge g, f_{in} \wedge \neg g$ のそれぞれを実行前条件に持つ機能要求記述 $id : f_{in} \wedge g \overset{a/o}{\Rightarrow} f_{out}$, $id : f_{in} \wedge \neg g \overset{a/o}{\Rightarrow} f_{out}$ で置換する操作を機能要求記述の場合分けという． □

f_{in} が成り立つ場合，$f_{in} \wedge g$ と $f_{in} \wedge \neg g$ とは必ずどちらか一方が成立し，かつ同時に成立することはない．よって，場合分けによって，機能要求記述全体の表す意味は変化しない．

3.2 詳細化の枠組み

要求仕様の詳細化の枠組みを，階層化と置換による方法で与える．階層化による詳細化では条件付き要求仕様の条件を詳細化し，置換による詳細化では条件付き要求仕様の機能要求記述を詳細化する．

3.2.1 階層化による詳細化

条件付き要求仕様と階層化要求仕様の定義に基づき，階層化による詳細化は以下の手順で行なわれる．

手順 3.5 （階層化による詳細化）

(1) 条件付き要求仕様 $\mathcal{CR}_1 = \langle 1, \mathcal{P}_1, \mathcal{R}_1 \rangle$ を記述する．以下では変数 n は階層の個数を表し，その初期値を1とする．

(2) 目的仕様が得られていれば終了．

(3) ある i $(1 \leq i \leq n)$ を選び，$\mathcal{CR}_i = \langle \eta_i, \mathcal{P}_i, \mathcal{R}_i \rangle$ の $\mathcal{P}_i$ に含まれる素命題を用いて詳細化の対象としたい条件 η を構成する．

(4) $n \leftarrow n+1$, $\eta_n \leftarrow \eta$ とする．条件 η_n による階層 $\mathcal{CR}_n = \langle \eta_n, \mathcal{P}_n, \mathcal{R}_i \rangle$ を以下のように構成する．

(a) 素命題の集合 $\mathcal{P}_n$ を，$\mathcal{CR}_j = \langle \eta_j, \mathcal{P}_j, \mathcal{R}_j \rangle$ $(1 \leq j \leq n-1)$ の $\mathcal{P}_j$ に対し，$\mathcal{P}_n \cap \mathcal{P}_j = \phi$ となるように与える．

(b) $\mathcal{P}_n$ を用いて $\mathcal{R}_n$ を記述する．

(5) (2) へ戻る． □

3.2.2 置換による詳細化

一括化と場合分けの定義に基づき，置換による詳細化は以下の手順で行なわれる．

手順 **3.6** （置換による詳細化）

(1) 階層化要求仕様 $\mathcal{HR} = \{\mathcal{CR}_i\}$ を仮定する．

(2) 目的仕様が得られていれば終了．

(3) ある $\mathcal{CR}_i = \langle \eta_i, \mathcal{P}_i, \langle R_i, \gamma_{0i}, \gamma_{ei} \rangle \rangle$ に対し，機能要求記述 $\rho \in R_i$ を選ぶ（ρ は空機能要求記述の場合もありうる）

(4) 以下の (a)(b)(c)(d) のいずれかの操作を行なう．

(a) ρ を R_i から取り除き，新たな機能要求記述 $\rho_1, ..., \rho_n$ を R_i に加える．

(b) ρ を R_i から取り除き，新たな機能要求記述 ρ, ρ' を R_i に加える．ここで，ρ' は ρ と一括化される機能要求記述である．

(c) ρ を R_i から取り除き，新たな機能要求記述 ρ', ρ'' を R_i に加える．ここで，ρ' と ρ'' は一括化される機能要求記述であり，かつ ρ と同じ意味になる．

(d) ρ を場合分けする．すなわち，ρ を R_i から取り除き，新たな機能要求記述 ρ', ρ'' を R_i に加える．

(5) (2) に戻る． □

手順 3.6 において，(4)(a),(b) は $\mathcal{CR}_i$ の意味を変え，(4)(c),(d) は $\mathcal{CR}_i$ の意味を変えない．

3.3 支援法

要求仕様の詳細化を行なう上で困難な作業の1つは，詳細化する対象を決定することである．要求仕様の性質から，その対象が（半）自動的に決定されることが望ましい．本節では要求仕様の構文的性質を利用し，要求仕様の分割を用いて詳細化対象を（半）自動的に決定する手法を与える．

以下では，分割による詳細化対象の選定支援法を述べる．

3.3.1 分割による詳細化対象の選定支援

A. 素命題集合に関する分割法，B. 階層化による分割法，C. 特定素命題の成否に関する分割法の3つの分割法と，それらを円滑に行なうための D. 一括化を用いた分割の支援法を与える．

A. 素命題集合に関する分割法は，機能要求記述に現れる素命題が共通するもの同士をまとめて，要求仕様の機能要求記述集合を，同じ素命題を含まない部分機能要求記述集合の集合に自動的に分割する．

B. 階層化による分割法は，A. 素命題集合に関する分割法と同様に要求仕様の機能要求記述の分割を行なった後，さらに実行前・実行後条件である一定の共通した条件 η' が満たされる機能要求記述同士をまとめ，このまとまりと残りの機能要求記述のまとまりで機能要求記述集合を2つに分割し，要求仕様を η' を用いて階層化する．

C. 特定素命題の成否に関する分割法は，ある機能要求記述の集合中の，ある素命題 A に関して，機能要求記述の集合を以下の3つに分割する．*i.* 実行前条件，実行後条件ともに A を満たす場合．*ii.* 実行前条件，実行後条件ともに $\neg A$ を満たす場合．*iii.* 実行前条件，実行後条件で A の成否が異なる場合．

D. 一括化を用いた分割の支援法は，一括化を用いて1つの機能要求記述を，それと同じ働きをする複数の機能要求記述で置換し，A. 素命題に関する分割法と，B. 階層化による分割法を支援する．

A. 素命題集合に関する分割法: 素命題集合に関する分割は以下のアルゴリズムで行なわれる．

アルゴリズム **3.7** （素命題集合に関する分割法）

条件付き要求仕様 $\mathcal{CR} = \langle \eta, \mathcal{P}, \langle R, \gamma_0, \gamma_e \rangle \rangle \in \mathcal{HR}$ に対し，機能要求記述集合 R を以下の手順で n 個の機能要求記述集合 R_i $(1 \leq i \leq n)$ に分割して，全ての R_i からなる集合 $S_R = \{R_i\}$ を得る．

(1) $S_R = \phi$ とし，m の初期値を 0 とする．

(2) $R \neq \phi$ のとき，以下を実行する．

(a) $\rho \in R$ を R から取り除く．$m \leftarrow m+1$ とし，$S_R \leftarrow S_R \cup \{\{\rho\}\}$ とする．以下，$R_m = \{\rho\}$ とする．

(b) P_i を R_i に現れる全ての素命題の集合であるとする．$P_i \cap P_j \neq \phi$ である全ての $R_i, R_j \in T$ について，$m \leftarrow m+1$ とし，$S_R \leftarrow (S_R - \{R_i, R_j\}) \cup \{R_i \cup R_j\}$ とする．以下，$R_m = R_i \cup R_j$ とする．

(3) すべての $R_i \in S_R$ に対し，重複しないように $1 \leq k \leq n$ の数値を割り当て，i を k に変更する名前の付け替えを行なう．ここで，n は S_R の要素数である． □

本分割法により，素命題の重複がない形で機能要求記述集合を分割できる．

B. 階層化による分割法: 階層化による分割は以下のアルゴリズムで行なわれる．

アルゴリズム **3.8** （階層化による分割法）

条件付き要求仕様 $\mathcal{CR} = \langle \eta, \mathcal{P}, \langle R, \gamma_0, \gamma_e \rangle \rangle \in \mathcal{HR}$ を以下の手順で生成される2個の条件付き要求仕様 $\mathcal{CR}', \mathcal{CR}''$ に分割する．

(1) $\mathcal{CR} = \langle \eta, \mathcal{P}, \langle R, \gamma_0, \gamma_e \rangle \rangle$ の機能要求記述集合 R を，アルゴリズム 3.7 の R に対して行なっ

たのと同様の手順で n 個の機能要求記述集合 R_i $(1 \leq i \leq n)$ に分割し，全ての R_i からなる集合 $S_R = \{R_i\}$ を得る．

(2) $flag = 0$ とする．

(3) $flag = 0$ のとき，すべての $R_i \in S_R$ について，以下を実行する．

  (a) ある条件 η' を実行前・実行後条件ともに満たす m 個の機能要求記述 $\rho_k \in R_i$ $(1 \leq k \leq m)$ が存在するような η' をみつける．R_i に現れる全ての素命題の集合を P_i，$\{\rho_k\}$ に現れる全ての素命題の集合を P'，η' に現れる全ての素命題の集合を $P_{\eta'}$ とする．

  (b) $P' - P_{\eta'}$ の要素である素命題が $R_i - \{\rho_k\}$ に現れるとき，(a) に戻って別の η' を探す．

  (c) $flag = 1$ とする．

(4) $flag = 0$ のときは終了．

(5) 機能要求記述集合 $\{\rho_k\}$ の全ての ρ_k から条件 η' を除いた機能要求記述の集合を R' とする．γ_0 から $P' - P_{\eta'}$ の要素である素命題による条件だけを取り出した条件を γ_0'，γ_e から $P' - P_{\eta'}$ の要素である素命題による条件だけを取り出した条件を γ_e' とする．

(6) γ_0 から $P' - P_{\eta'}$ の要素である素命題による条件を全て除いた条件を γ_0''，γ_e から $P' - P_{\eta'}$ の要素である素命題による条件を全て除いた条件を γ_e'' とする．

(7) 条件付き要求仕様 $\mathcal{CR}' = \langle \eta', P' - P_{\eta'}, \langle R', \gamma_0', \gamma_e' \rangle \rangle$ と，$\mathcal{CR}'' = \langle \eta, P_i - (P' - P_{\eta'}), \langle R - \{\rho_k\}, \gamma_0'', \gamma_e'' \rangle \rangle$ を得る． □

階層化による詳細化では，詳細化対象条件はすべて設計者自身が記述しなければならなかった．本分割法により，階層の構築を自動的に行なえる．

C. 特定の素命題の成否に関する分割法: 特定の素命題の成否に関する分割は，以下のアルゴリズムで行なわれる．

アルゴリズム 3.9 (特定の素命題の成否に関する分割法)

機能要求記述集合の分割の基準として，設計者により指定される素命題を用い，この素命題の実行前・実行後条件での成立・不成立の種類別の分割を行なう．

素命題 A が与えられたとき，条件付き要求仕様 $\mathcal{CR} = \langle \eta, \mathcal{P}, \langle R, \gamma_0, \gamma_e \rangle \rangle \in \mathcal{HR}$ に対し，機能要求記述集合 R を以下の手順で 3 個の機能要求記述集合 R_1, R_2, R_3 に分割する．

(1) A が現れない全ての機能要求記述 $\rho \in R$ を A を用いた場合分けにより，機能要求記述 ρ_1, ρ_2 で置換する．

(2) $R \neq \phi$ のとき，以下を実行する．

  (a) R から ρ を取り出す．

  (b) 以下の条件のどれを満たすかによって，ρ を機能要求記述集合 R_1, R_2, R_3 のどれかの要素に加える．

    i. 実行前・実行後条件ともに A が成立する場合，$R_1 \leftarrow R_1 \cup \{\rho\}$.

    ii. 実行前・実行後条件ともに $\neg A$ が成立する場合，$R_2 \leftarrow R_2 \cup \{\rho\}$.

    iii. 実行前・実行後条件で A の成否が異なる場合，$R_3 \leftarrow R_3 \cup \{\rho\}$. □

本分割法は任意の要求仕様に適用可能である．

D. 一括化を用いた分割支援法: 一括化の仕組みを用い，1 つの機能要求記述を複数の機能要求記述で置換する．

機能要求記述 $id : f_{in} \overset{a/o}{\Rightarrow} f_{out}$ において，f_{out} を 2 つの条件 f_{out1}, f_{out2} の連言とみて，$id : f_{in} \overset{a/o}{\Rightarrow} f_{out1} \wedge f_{out2}$ を，一括化される 2 つ機能要求記述 $id : f_{in} \overset{a/o}{\Rightarrow} f_{out1}$, $id : f_{in} \overset{a/o}{\Rightarrow} f_{out2}$ で置き換える．

本分割支援法により，それぞれの機能要求記述に含まれる素命題の数を減らし，A. 素命題集合に関する分割法，および B. 階層化による分割法について，分割の条件を満たしやすくする．

4 適用例

以下に簡易 TV の要求仕様とその分割例を示す．

簡易 TV は (1) 電源の on, off, (2) 音声ミュートの on, off, (3) ボリュームの上下，(4) チャンネルの上下の機能を持つ．これらの機能に対応する機能要求記述の機能名は (1) $Power\_on$, $Power\_off$, (2) $Mute\_on$, $Mute\_off$, (3) $Volume\_up$, $Volume\_down$, (4) $Channel\_up$, $Channel\_down$ である．また，素命題は「電源が on である」ことを示す $Power$ と，「ミュート機能が働いていて音声が off である」ことを示す $Mute$ である．電源 on する機能を機能要求記述として書くと，次のようになる．$Power\_on : \neg Power \overset{pw/ch}{\Rightarrow} Power$. これは，「電源が off のとき，電源キーによる入力があったら，電源を on にして画面にチャンネル番号を出力する」ことを意味する．同様に電源 off する機能を機能要求記述として書くと，次のようになる．$Power\_off : Power \overset{pw}{\Rightarrow} \neg Power \wedge \neg Mute$. これは，「電源が on のとき，電源キーによる入力があったら，電源を off にして，ミュート機能も off にする」ことを意味する．同様に簡易 TV の全ての機能の機能要求記述を記述し，要求仕様を構成すると，次のようになる．

$\{\langle 1, \{Power, Mute\},$

$\langle \{ Power\_on : \neg Power \overset{pw/ch}{\Rightarrow} Power,\ Power\_off : Power \overset{pw}{\Rightarrow} \neg Power \wedge \neg Mute,\ Mute\_on : Power \wedge \neg Mute \overset{mt/mt}{\Rightarrow} Mute,\ Mute\_off : Power \wedge Mute \overset{mt/vl}{\Rightarrow} \neg Mute,\ Volume\_up : Power \overset{vlup/vl}{\Rightarrow} \neg Mute,\ Volume$

$down$: $Power \overset{vldw/vl}{\Rightarrow} \neg Mute$, $Channel\_up$: $Power \overset{chup/ch}{\Rightarrow} 1$, $Channel\_down : Power \overset{chdw/ch}{\Rightarrow} 1\}$, $\neg Power \wedge \neg Mute, \neg Power \wedge \neg Mute\rangle\rangle\}$

ここで，初期条件と最終条件は，電源がoffであり，かつミュート機能がoffである．

以下では分割の最初の2ステップを説明する．

(1) C. 素命題 $Power$ の成否に関して要求仕様を分割する．ここで，D. $Power\_off$ に対し，一括化を用いた分割支援法を適用する．

(2) B. 条件 $Power$ に関する階層化により，要求仕様を，条件 $Power$ を持つ階層とそれ以外の階層に分割する．

まず(1)で，C. 特定の素命題に関する分割法を $Power$ に関して適用して，要求仕様の機能要求記述集合を3つに分割する．分割の結果，以下の要求仕様が得られる．

$\{\langle 1, \{Power, Mute\},$

$\langle \{ \{ Mute\_on : Power \wedge \neg Mute \overset{mt/mt}{\Rightarrow} Mute, Mute\_off : Power \wedge Mute \overset{mt/vl}{\Rightarrow} \neg Mute, Volume\_up : Power \overset{vlup/vl}{\Rightarrow} \neg Mute, Volume\_down : Power \overset{vldw/vl}{\Rightarrow} \neg Mute, Channel\_up : Power \overset{chup/ch}{\Rightarrow} 1, Channel\_down : Power \overset{chdw/ch}{\Rightarrow} 1\},$ ... *i.*

$\{\},$ ..... *ii.*

$\{ Power\_on : \neg Power \overset{pw/ch}{\Rightarrow} Power, Power\_off : Power \overset{pw}{\Rightarrow} \neg Power \wedge \neg Mute\}\},$ ..... *iii.*

$\neg Power \wedge \neg Mute, \neg Power \wedge \neg Mute\rangle\rangle\}$

ここで，*i.* は実行前・実行後条件ともに条件 $Power$ を満たす機能要求記述の集合であり，*ii.* は実行前・実行後条件ともに条件 $\neg Power$ を満たす機能要求記述の集合であり，*iii.* は実行前・実行後条件で条件 $Power$ の成否が異なる機能要求記述の集合である．

次に，D. 一括化を用いた分割支援法を用いて，機能要求記述 $Power\_off : Power \overset{pw}{\Rightarrow} \neg Power \wedge \neg Mute$ を，一括化される2つの機能要求記述 $Power\_off : Power \overset{pw}{\Rightarrow} \neg Power$, $Power\_off : Power \overset{pw}{\Rightarrow} \neg Mute$ で置換する．

以上から次の要求仕様 $\mathcal{HR}$ が得られる．

$\mathcal{HR} = \{\langle 1, \{Power, Mute\},$

$\langle \{ Mute\_on : Power \wedge \neg Mute \overset{mt/mt}{\Rightarrow} Mute, Mute\_off : Power \wedge Mute \overset{mt/vl}{\Rightarrow} \neg Mute, Volume\_up : Power \overset{vlup/vl}{\Rightarrow} \neg Mute, Volume\_down : Power \overset{vldw/vl}{\Rightarrow} \neg Mute, Channel\_up : Power \overset{chup/ch}{\Rightarrow} 1, Channel\_down : Power \overset{chdw/ch}{\Rightarrow} 1, Power\_on : \neg Power \overset{pw/ch}{\Rightarrow} Power, Power\_off : Power \overset{pw}{\Rightarrow} \neg Power, Power\_off : Power \overset{pw}{\Rightarrow} \neg Mute\},$

$\neg Power \wedge \neg Mute, \neg Power \wedge \neg Mute\rangle\rangle$

ここで，一括化を用いた分割支援により，$Power\_off1$ つあたりに現れる素命題数が減らされている．

次に(2)で，B. 階層化による分割法を $Power$ に関して適用し，要求仕様を $Power$ に関する階層と，それ以外の階層とに分割する．

B. の(1)～(3)により，要求仕様 $\mathcal{HR}$ の機能要求記述集合を分割する．実行前・実行後条件で $Power$ を満たす機能要求記述をまとめ，次の R' を得る．

$R' = \{ Power\_off : Power \overset{pw}{\Rightarrow} \neg Mute, Mute\_on : Power \wedge \neg Mute \overset{mt/mt}{\Rightarrow} Mute, Mute\_off : Power \wedge Mute \overset{mt/vl}{\Rightarrow} \neg Mute, Volume\_up : Power \overset{vlup/vl}{\Rightarrow} \neg Mute, Volume\_down : Power \overset{vldw/vl}{\Rightarrow} \neg Mute, Channel\_up : Power \overset{chup/ch}{\Rightarrow} 1, Channel\_down : Power \overset{chdw/ch}{\Rightarrow} 1\}$

B. の(5)により，R' から条件 $Power$ を除いた機能要求記述の集合 R'' を，次のように得る．

$R'' = \{ Power\_off : 1 \overset{pw}{\Rightarrow} \neg Mute, Mute\_on : \neg Mute \overset{mt/mt}{\Rightarrow} Mute, Mute\_off : Mute \overset{mt/vl}{\Rightarrow} \neg Mute, Volume\_up : 1 \overset{vlup/vl}{\Rightarrow} \neg Mute, Volume\_down : 1 \overset{vldw/vl}{\Rightarrow} \neg Mute, Channel\_up : 1 \overset{chup/ch}{\Rightarrow} 1, Channel\_down : 1 \overset{chdw/ch}{\Rightarrow} 1\},$

$Power$ を用いて要求仕様を階層 $\langle Power, \{Mute\}, \langle R'', \neg Mute, \neg Mute\rangle\rangle$ と $\langle 1, \{Power\}, \langle R - R', \neg Power, \neg Power\rangle\rangle$ に分割する．以上により，以下のような階層化要求仕様が得られる．

$\{\langle 1, \{Power\}, \langle \{Power\_on : \neg Power \overset{pw/ch}{\Rightarrow} Power, Power\_off : Power \overset{pw}{\Rightarrow} \neg Power\}, \neg Power, \neg Power\rangle\rangle,$

$\langle Power, \{Mute\}, \langle \{ Power\_off : 1 \overset{pw}{\Rightarrow} \neg Mute, Mute\_on : \neg Mute \overset{mt/mt}{\Rightarrow} Mute, Mute\_off : Mute \overset{mt/vl}{\Rightarrow} \neg Mute, Volume\_up : 1 \overset{vlup/vl}{\Rightarrow} \neg Mute, Volume\_down : 1 \overset{vldw/vl}{\Rightarrow} \neg Mute, Channel\_up : 1 \overset{chup/ch}{\Rightarrow} 1, Channel\_down : 1 \overset{chdw/ch}{\Rightarrow} 1\}, \neg Mute, \neg Mute\rangle\rangle\}$

5 おわりに

本稿では命題論理に基づく機能要求記述と，その集合を使って表現される要求仕様の定義，その詳細化法について述べた．特に要求仕様の階層化と機能要求記述の置換による詳細化の枠組みを定義した．これにより，詳細化の方針を与えることができた．また，要求仕様の分割による，詳細化対象の選定支援法を提案した．

今後の課題としては，実際に様々なシステムの要求仕様開発に本詳細化法とその支援法を適用し，評価を行なうことが挙げられる．

参考文献

[1] Togashi,A., Usui,N., Song,K., Shiratori, N.: Synthesis of Formal Specifications from User Requirememts and its Flexibility, *Tech. Rep. of IEICE*,IN-95, 1995.

[2] 臼井伸幸, 高橋薫, 神長裕明, 白鳥則郎: "形式仕様の開発における機能要求への反映" 電子情報通信学会技術報告書 SSE95-65, pp.67–72, 1995.

[3] K. H. Song, A. Togashi, N. Shiratori: Verification and Refinement for System Requirements, IEICE Trans. on Fundementals of Electoronics, Communications and Computer Sciences, Vol. E78-A, No. 11, pp. 1468–1478, Nov. 1995.