

組合せ論理回路のハザード検出問題の計算複雑さについて

京都大学工学部 石浦 菜岐佐 (Nagisa Ishiura)

京都大学工学部 安浦 寛人 (Hiroto Yasuura)

1. はじめに

近年の大規模論理回路は大部分が同期式順序回路で設計されるため、タイミングに関する検証は、レジスタ間の遅延解析を行う程度で十分である。しかし、通信制御などの周辺論理、記憶素子など非同期回路として設計されるものに対しては、仕様通りの動作をするかどうか、あるいはハザード、発信、競合によるエラーが発生しないかどうかを調べるために、論理的動作との関係をも考慮した精密なタイミング解析を行う必要がある。論理回路のタイミング検証の手法として最も広く用いられているのは論理シミュレータを利用する方法である。論理シミュレーションによる検証は、代表的な入力パターンに対する回路の振る舞いを調べるものなので、可能な全ての場合を尽くす検証にはならないことが多い。また、遅延のあいまいさを扱うために、5~9値の論理値を用いた最大/最小遅延シミュレーションの手法が知られているが[2]、悲観的な結果を出力する(誤りのない設計に対しても誤りが有ると判定する)という問題点がある。この他にも、時相論理やオートマトン理論に基づく検証手法が提案されているが[3][4]、実用に耐えるものは少ない。また、ほとんどの検証系は離散時間を扱っているが、離散時間が現実の連続時間の近似として十分な精度を持つかどうかについての厳密な議論は著者らの知る限り無い。

我々は、遅延・時間のモデルと検証の精度、及び検証に必要な計算時間の関係を明らかにしたいという観点から、ハザード検出問題を例にとりタイミング解析の研究を行っている[1]。組合せ回路におけるハザード検出問題を、種々の時間・遅延のモデルの下で解くのに必要な計算量の評価を行った結果、ゲート遅延のあいまいさ、ゲート遅延の大きさ、及び時間を離散値とするか連続値とするか等のモデルの違いにより、ハザードの発生を検出するのに必要な計算量は、決定的多項式時間から多項式領域のクラスまで、様々に変化することが明らかになった。

2. 諸定義

2.1 ハザード検出問題

本稿では組合せ論理回路を対象とするハザード検出問題を考える。組合せ論理回路C中のゲートのファンイン数やファンアウト数は、Cに含まれるゲートの数

とは無関係な定数以下であるとする。Cの各外部入力に対する論理値($B = \{0, 1\}$ の要素)の割当てを入力パターンと呼ぶ。回路Cにおいて、入力パターン変化 $v_x \rightarrow v_y$ に対してハザードが起こるとは、Cが v_x に対して安定している状態で、入力パターンを v_y に変えた時、 v_y に対してCが安定するまでに、2回以上値を変化させる出力線が少なくとも1本存在することである。ハザード検出問題には次に示す特定入力変化に対するものと、全入力変化に対するものが考えられる。

1) 特定入力変化(specific input change)に対するハザード検出問題

Instance: 回路CとCへの入力パターン v_x と v_y 。

Question: Cにおいて入力パターン変化 $v_x \rightarrow v_y$ に対してハザードが起こりうるか?

2) 全入力変化(all input change)に対するハザード検出問題

Instance: 回路C。

Question: Cにおいてハザードが起こる入力パターン変化が存在するか?

本稿では前者の特定入力変化に対するハザード検出問題を中心に考える。特定入力変化を考える場合には、一般性を失うことなく、「回路Cの外部入力は唯一つで、この外部入力に対する信号値が変化する」ものとする事ができる。本稿では簡単の為、回路Cの外部出力も唯一つである場合を考える。即ち、回路Cを構成するゲートの集合を $G = \{g_0, g_1, \dots, g_n\}$ とし、 g_0 を外部入力、 g_n を外部出力に信号値を供給するゲートとする。

2.2 遅延と時間のモデル

ゲートの遅延は、製造条件や使用条件によってばらつく。本稿では、このような遅延のばらつきをモデル化するために、遅延の値を最大値と最大値により表す。即ち、ゲート g_k の遅延は2つの非負整数 d_k^{\min} と d_k^{\max} で指定され、閉区間 $[d_k^{\min}, d_k^{\max}]$ のある値 d_k (但し、 $d_k \in \mathbf{Z}$ (整数)または $d_k \in \mathbf{R}$ (実数))をとるものとする。本稿では、 d_k^{\min} 、 d_k^{\max} の値や d_k のとりうる値によって、次に示す遅延や時間のモデルを考える。

(1) 遅延のあいまいさのモデル

$d_k^{\min} = d_k^{\max}$ である場合を正確遅延モデル(accurate delay model)、このような制限がないものをあいまい遅延モデル(ambiguous delay model)という。本稿では、さらに現実的な遅延モデルとして、限定あいまい遅延モデル(bounded ambiguous delay model)を考える。これは、非負の定数 c^{\min} 、 c^{\max} があって、すべてのゲート g_k が $c^{\min} \leq (d_k^{\max} - d_k^{\min}) / (d_k^{\max} + d_k^{\min}) \leq c^{\max}$ を満たすというものであり、遅延のあいまいさが遅延の大きさに対して、極端に大きかったり小さかったりすることはないというモデルである。

(2) 時間のモデル

$d_k \in \mathbf{Z}$ (整数)である場合を離散時間モデル、 $d_k \in \mathbf{R}$ (実数)である場合を連続時間モデルという。ゲートの遅延時間の大きさ(d_k^{\min} 、 d_k^{\max})は整数で指定されるため、正確遅延モデルにおいては両者に差は生じないが、あいまい遅延の場合には差が生じる。二つの時刻 t_1 と t_2 の間に、離散時間モデルでは有限個の時刻しか存在しないのに対し、連続時間モデルでは無限の時刻が考えられるためである。

(3) 遅延の大きさのモデル

現実の回路では、ゲート遅延の大きさはゲート数 n には依存しない。即ち、 $d_k^{\max} = O(1)$ であり、これを定数遅延モデルという。しかし、本稿では連続時間と離散時間の相違を考察する際に、理論上 $d_k^{\max} \leq O(2^{\text{poly}(n)})$ (但し $\text{poly}(n)$ は n の多項式)のような遅延を許す場合も考える。この遅延モデルを指数遅延モデルという。

その他、あいまい遅延モデルがモデル化している遅延の静的なばらつきに対し、現実にはゲートの履歴や環境の変化によりもたらされる動的な遅延のばらつきも存在するが、今回は考えない。立上り/立下り遅延、慣性遅延についても本稿では考えないことにする。

2.3 表記法

以下では簡便の為、下記のような略記を用いる。

$$\begin{bmatrix} S \\ A \end{bmatrix} \text{HD} \begin{bmatrix} \text{Cnst} \\ \text{Exp} \end{bmatrix} \begin{bmatrix} \text{Acc} \\ \text{Amb} \\ \text{Bamb} \end{bmatrix} \begin{bmatrix} \text{Dscr} \\ \text{Cont} \end{bmatrix}$$

S/Aは、Specific/Allで、特定/全入力変化を、

Cnst/Expは、Constant/Exponentialの略で、定数/指数遅延を、

Acc/Amb/Bambは、Accurate/Ambiguous/Bounded-Ambiguousの略で正確/あいまい/限定あいまい遅延を、

Disc/Contは、Discreat/Continuousの略で、離散/連続時間を、それぞれ指定するものである。例えばSHDCnstBambContは、定数遅延・連続時間・限定あいまい遅延における特定入力変化に対するハザード検出問題を表わす。

3. 定数遅延の離散遅延モデル(SHDCnstXDscr)

3.1 離散時間モデル

この節では、現実的な大きさの遅延を仮定する定数遅延モデルのハザード検出問題を、離散時間モデルのもとで解くのに必要な計算量を考える。この仮定のもとで、1) 正確遅延モデル、2) 非限定あいまい遅延モデル、3) 限定あいまい遅延モ

デルの問題の計算量を考える。正確遅延モデルの場合(SHDCnstAccDscr)は、現実的な時間でハザードを検出する方法が存在する。

定理1. SHDCnstAccDscrは決定的に多項式時間で解ける。

[証明] 論理シミュレーションを行う。計算時間は $O(n^2)$ で済む。□

ゲートの遅延のあいまいさを考慮したタイミング・シミュレーションには、5値以上の論理値を用いる最大/最小遅延シミュレーションが用いられるが、ハザードの検出に関しては結果が悲観的になることが知られている。遅延の大きさに幅がある場合でも、時間が離散的であれば、許される遅延値の全ての組合せについて通常のシミュレーションを行えばよいので、次の上界は自明である。

補題3.1 SHDCnstAmbDscr、SHDCnstBambDscrはいずれも非決定的に多項式時間で解ける。□

一方、SHDCnstAmbDscr、SHDCnstBambDscrの計算量の下界に対しては、次の結果が得られている。

補題3.2 SHDCnstAmbDscr、SHDCnstBambDscrはNP困難である。

[証明] SAT(論理式の充足可能性判定問題)をこの問題に帰着できることを示す。このために、図3.1に示すような回路を構成する。回路は入力生成部と論理式計算部からなる。入力生成部は(c)のようなパルス生成回路により構成される。パルス生成回路は、安定している時にはいずれの出力も常に0であるが、入力が0から1に変化した時にはいずれか一方の出力に1パルスが発生しうる(g_1 の遅延がaより小さい時には g_4 の出力に、大きい時には g_5 の出力に1パルスを生成しうる)回路である。論理式計算部はSATの論理式Fに対し、

$$F'(x_0, \overline{x_0}, \overline{x_1}, x_1, \dots, \overline{x_n}, x_n) = F(x_0, x_1, \dots, x_n)$$

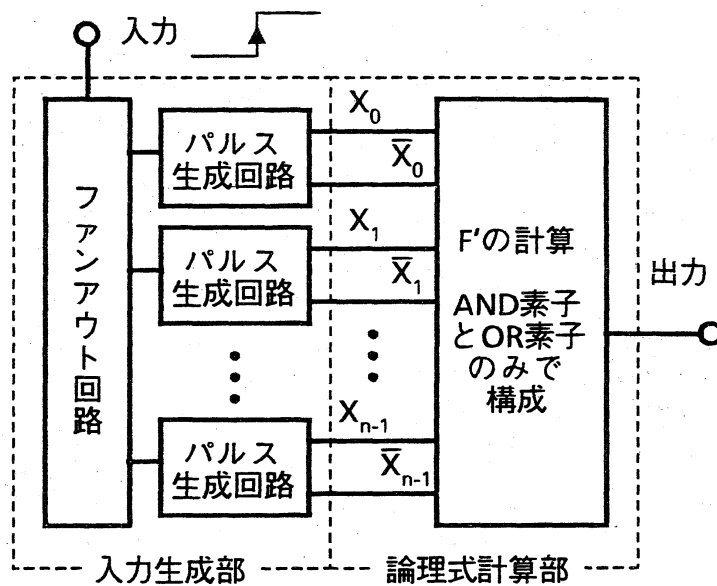
を満たす $2n$ 入力の論理関数 F' を実現する組合せ回路ある。この部分は、AND素子とOR素子のみで構成されており、内部は適当に同期化されているものとする。

さて、この回路の出力は安定状態では常に0である。もしFが充足可能であれば、 F' も充足可能であり、入力生成部で F' を充足する割当てに対応するパルスが発生したとき、出力にはハザードが発生しうる。逆に、この回路のハザード検出問題がYESであれば、 F' 及びFを充足する入力割当てが存在することになる。□

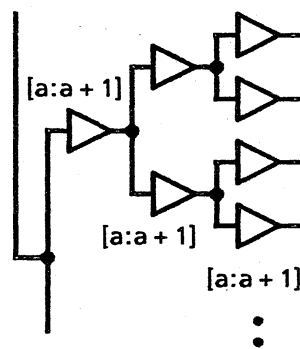
定理2. SHDCnstAmbDscr、SHDCnstBambDscrはNP完全である。□

3.2 連続時間モデル(SHDCnstXCont)問題に対するアプローチ

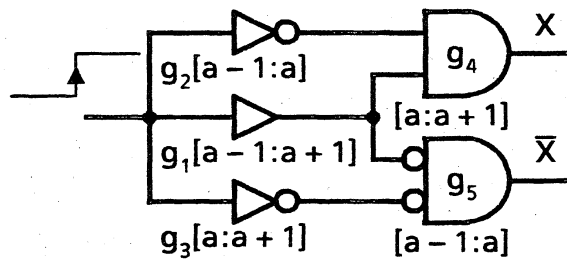
ゲートの遅延時間(の上下限)は整数で与えられると仮定しているので、正確遅延モデルにおいては、離散時間モデルと連続時間モデルの相違はないが、あいま



(a) 回路の全体構成



(b) ファンアウト回路



(c) パルス生成回路

図3.1 SATを解く回路

い遅延を考える場合には差が生じる。図3.2は、実際に離散時間モデルと連続時間モデルでハザードの発生の有無に差が生じる例である。この例においては、連続時間モデルでは発生するハザードが離散時間モデルでは発生しない。

しかし、この例において $1/2$ 時刻を単位と考えるなら、ハザードは発生する。即ち、離散時間モデルは時間の刻み幅を小さくすれば、連続時間と同じ能力を持つと考えられる。本稿では、離散時間モデルがどの程度まで時間の刻み幅を細かくすれば、連続時間モデルと同じ能力をもつかというアプローチにより、連続時間モデルにおける計算量を考える。指数遅延モデルは、ゲート遅延の値を指数オーダーまで許すことにより、相対的に極めて細かい単位時間を実現するものであるが、次節ではこの指数遅延モデルにおける計算量について考察する。

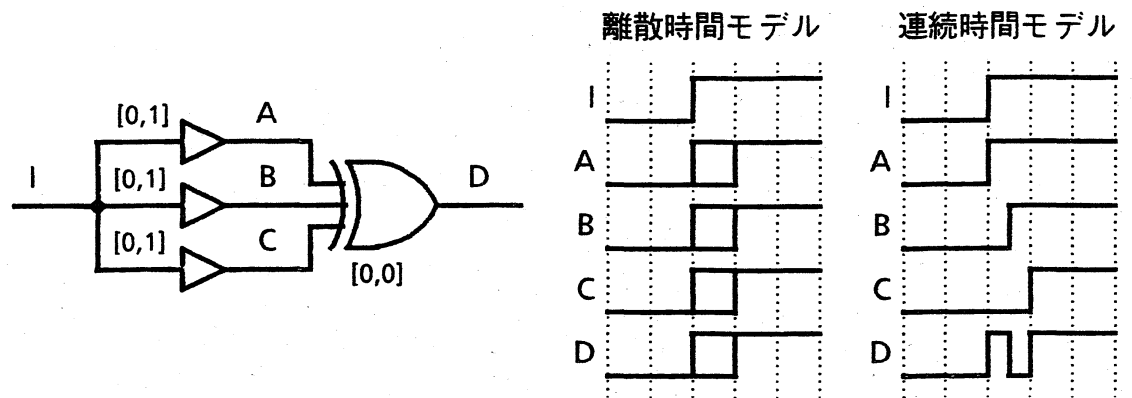


図3.2 離散時間モデルと連続時間モデルの差

4. 指数遅延の離散時間モデル(SHDExpXDscr)

まず、正確遅延モデルの場合(SHDExpAccDscr)について考える。定数遅延モデルに関しては、論理シミュレーションにより決定的に多項式時間で解けることを定理1.で示した。指数遅延モデルの場合には、ゲートの遅延の最大値が $O(2^{\text{poly}(n)})$ になり得るので、多項式時間でシミュレーションを行うことはできない。実際に、指数遅延モデルでは次の結果の通り、計算量は飛躍的に増大する。

補題4.1 SHDExpAccDscrはPSPACE困難である。

[証明] QBF(限定記号付きの論理式の充足可能性判定問題)[5]がSHDExpAccDscrに多項式時間帰着できることを示す。詳細は[1]参照。

逆にSHDExpAccDscrの計算量の上界については、次の補題4.2に示す結果が得られており、SHDExpAccDscrはPSPACE完全に属することがわかる。

補題4.2 SHDExpAccDscrは決定的に多項式領域で解ける。

[証明] 通常の論理シミュレーションではなく、回路の出力側からハザードの有無を調べる、逆方向シミュレーションを用いる。回路の入力パターンは時刻0に $v_x \rightarrow v_y$ に変化するものとし、入力パターン v に対する出力を $F(v)$ で表す。

1) 静的ハザードが発生する場合($F(v_x) = F(v_y)$ のとき)は、回路の入力から出力に至るパスを1つguessする。その遅延長(パス上にあるゲートの遅延の合計)を d_p とし、時刻 d_p に回路の出力、即ちゲート g_n の出力が時刻 d_p に $\sim F(v_x)$ になっているかどうかを次に示す手続き $\text{Val}(g_n, d_p, \sim F(v_x))$ によって調べる。

2) 動的ハザードが発生する場合($F(v_x) \neq F(v_y)$ のとき)は、回路の入力から出力に至るパスを2つguessする。その遅延長(パス上にあるゲートの遅延の合計)を d_{p1} 、 d_{p2} (但し $d_{p1} < d_{p2}$) とし、回路の出力、即ちゲート g_n の出力が時刻 d_{p1} に $\sim F(v_x)$ であり、かつ時刻 d_{p1} に $F(v_x)$ になっているかどうかを手続き $\text{Val}(g_n, d_{p1}, \sim F(v_x))$ 及び $\text{Val}(g_n, d_{p1}, F(v_x))$ によって調べる。

手続き $\text{Val}(g, t, v)$ は、ゲート g の出力が時刻 t に v になっていることを判定する再帰的な手続きである。ゲート g の実現する論理関数を f 、 g の遅延を d 、入力数を m 、 g に入力を供給するゲートを g_1^s, \dots, g_m^s とする。

手続き $\text{Val}(g, t, v)$

v1) $g = g_0$ (外部入力) のときは、 $(d < 0$ かつ $v = v_x$) または $(d \geq 0$ かつ $v = v_y)$ であれば YES、そうでなければ NO を返す。 $g \neq g_0$ (通常のゲート) のときは、v2)~v3) を実行する。

v2) $v = f(v_1, \dots, v_m)$ となる v_1, \dots, v_m を guess する。

v3) 再帰的に $\text{Val}(g_1^s, t-d, v_1)$ 、 \dots 、 $\text{Val}(g_m^s, t-d, v_m)$ を呼び出し、全ての結果が YES であれば YES を、そうでなければ NO を返す。

回路の段数は高々 n であるから、手続き Val を用いれば、静的ハザードの発生、動的ハザードの発生とも交代 Turing 機械によって多項式時間で判定できる。従って、SHDExpAccDscr は決定的に多項式領域で解ける。□

定理3. SHDExpAccDscr は PSPACE 完全である。□

次に、あいまい遅延や限定あいまい遅延に関しては、ハザードの発生するゲート遅延の組合せを guess すれば、正確遅延の場合に帰着できるので、直ちに次の結果を得ることができる。

補題4.3 SHDExpAmbDscr、SHDExpBambDscr は PSPACE に属する。□

補題4.4 SHDExpAmbDscr は PSPACE 困難である。

[証明] 正確遅延モデルはあいまい遅延の特殊な場合であるから自明。□

定理4. SHDExpAmbDscr は PSPACE 完全である。□

5. 定数遅延の連続時間モデル (SHDCnstXCont)

SHDCnstAmbCont、SHDCnstBambCont については、補題3.2 と同じ方法で次の下界が示せる。

補題5.1 SHDCnstAmbCont、SHDCnstBambCont は NP 困難である。□

本章では4章での結果を用いて、SHDCnstAmbCont、SHDCnstBambCont が決定的に多項式領域で解けることを示す。証明は、連続時間モデルの問題が、遅延の大きさの制限を緩めた離散時間の問題に帰着できることによっているが、遅延の大きさの制限を求めるために、あいまい(限定あいまい)遅延モデルにおけるハザード検出問題は、ある特殊な Presburger 文の充足可能性判定問題と等価であることを利用している。

5.1 ハザード検出問題と等価な連立不等式

定義5.1 ゲート g_i の遅延値を表す変数を x_1, \dots, x_n とし、 $\mathbf{x}=(x_1, \dots, x_n)$ とする。 x_i は離散時間モデルの時は整数値を、連続時間モデルのときは実数値をとる。また、 x_i は次のRを満たす。

$$R = \bigwedge_{i=1, n} [(d^{\min}_i \leq x_i) \wedge (x_i \leq d^{\max}_i)] \quad \square$$

定義5.2 D_n 及び D'_n を次のように定義する。

$$D_n = \{\delta_1 x_1 + \delta_2 x_2 + \dots + \delta_n x_n \mid \delta_i = 0, 1\}$$

$$D'_n = \{\eta_1 x_1 + \eta_2 x_2 + \dots + \eta_n x_n \mid \eta_i = 0, \pm 1\} \quad \square$$

定義5.3 3つ組 $a=(g, t, v)$ の集合Aが次の3つの条件を満たすとき、Aを回路Cに対する時間-値割当てと呼ぶ。

1) $g \in G, t \in D'_n, v \in \{0, 1, d\}$ 。(但し、 d はdon't careを表す。)

2) $(g, t, 0), (g, t, 1), (g, t, d)$ の2つ以上が同時にAに属しない。

3) $g_i \in G, g_i \neq g_0, g_i$ に入力を供給するゲートを g^s_1, \dots, g^s_m とする。 $(g_i, t, v) \in A$ ならば $j=1, \dots, m$ について $(g^s_j, t - x_i, v_j)$ かつ $f(v_1, \dots, v_m) = v$ が成立する。但し、 f_i はゲート g_i の実現する論理関数である。□

定義5.4 時間-値割当てAの要素のうち $g=g_0$ であるものを $a_1, \dots, a_k, a_j=(g_0, t_j, v_j)$ とする。外部入力の値が $v_x \rightarrow v_y$ に変化するものとする、次のように定義されるSをAの充足条件と呼ぶ。

$$S = s_1 \wedge s_2 \wedge \dots \wedge s_k,$$

$$s_j = \begin{cases} t_j < 0 & (v_j = v_x \text{ のとき}) \\ t_j \geq 0 & (v_j = v_y \text{ のとき}) \end{cases} \quad \square$$

与えられた回路Cの入力 v に対する出力を $F(v)$ で表すことにすると、定義より明らかに補題5.2、5.3が成立し、定理5.を得る。

補題5.2 静的ハザード($F(v_x) = F(v_y)$)の場合が発生する必要十分条件は、

$$R \wedge (S_1 \vee S_2 \vee \dots \vee S_k)$$

を満たす (x_1, \dots, x_n) が存在することである。但し、 S_i は $t \in D_n$ として、 $(g_n, t, \sim F(v_x))$ を含む時間-値割当て A_i に対する充足条件である。□

補題5.3 動的ハザード($F(v_x) \neq F(v_y)$)の場合が発生する必要十分条件は、

$$R \wedge (S'_1 \vee S'_2 \vee \dots \vee S'_k)$$

を満たす (x_1, \dots, x_n) が存在することである。但し、 S'_i は $s, t \in D_n$ として、 $(g_n, s, \sim C(v_x))$ 及び $(g_n, t, \sim C(v_y))$ を含む時間-値割当て A_i に対する充足条件に、

$$s < t$$

を加えたものである。 □

定理5. あいまい(限定あいまい)遅延モデルでハザードの発生する必要十分条件は次の形で表される。

$$R \wedge (T_1 \vee T_2 \vee \dots \vee T_p) \dots \textcircled{1}$$

但し、

$$R = \bigwedge_{k=1, n} [(d_k^{\min} \leq x_k) \wedge (x_k \leq d_k^{\max})] \dots \textcircled{2},$$

$$T_i = t_1 \wedge t_2 \wedge \dots \wedge t_{p_i} \dots \textcircled{3},$$

$$t_j = (\eta_1 x_1 + \eta_2 x_2 + \dots + \eta_n x_n < 0), \text{ または} \\ (\eta_1 x_1 + \eta_2 x_2 + \dots + \eta_n x_n \leq 0).$$

但し $\eta_k = 0, \pm 1$. □

5.2 離散時間モデルへの帰着

前節の結果より、離散時間モデルにおいてハザードが発生することは①が整数解を持つことであり、連続時間モデルにおいてハザードが発生することは①が実数解を持つことである。線型代数の性質により補題5.4が示せるので、これより直ちに補題5.5が成立し、定理6.を得る。

補題5.4より次の2つの命題は同値である。

1') ①が実数解を持つ。

2') ある $m \leq n^n$ に対し、①の定数項を m 倍したものが整数解を持つ。 □

補題5.5 次の2つの命題は同値である。

1) 連続時間モデルでハザードが発生する。

2) ある $m \leq n^n$ に対し、遅延の値 (d_i^{\min} 、 d_i^{\max}) を m 倍した回路が離散時間モデルでハザードを発生する。 □

定理6. SHDCnstAmbCont、SHDCnstBambContは決定的に多項式領域で解ける。

[証明] 補題5.5より、 $2 \sim n^n$ の整数を1つguessし、遅延の上下限値を m 倍したものを離散時間で解けばよい。この問題は離散時間、指数遅延モデルのハザード検出問題SHDExpAmbDscr、SHDExpBambDscrであり、補題4.3により決定的に多項式領域で解ける。 □

6. むすび

種々の遅延、時間モデルの下でのハザード検出問題の計算複雑さについて考察した。結果を表6.1にまとめる。定数遅延の連続時間モデルに関しては、依然上界

と下界との間に大きな差があるが、これは、離散時間と連続時間で本質的に必要な計算量が異なるかどうかという重要な点であるため、考察を続けていきたい。

表6.1(a) 定数遅延モデルにおける計算複雑さ

	正確遅延	あいまい遅延	限定あいまい遅延
離散時間	in P	NP-complete	NP-complete
連続時間	-	NP-hard in PSPACE	NP-hard in PSPACE

表6.1(b) 指数遅延モデルにおける計算複雑さ

	正確遅延	あいまい遅延	限定あいまい遅延
離散時間	PSPACE-complete	PSPACE-complete	NP-hard in PSPACE

謝辞

補題5.4の導出にあたり、線型計画法の分解能について貴重なコメントを頂いた、本学数理工学教室の長持氏に感謝します。また、矢島脩三教授、平石裕実助教授、岡部寿男氏、安岡孝一氏はじめ御討論頂いた矢島研究室の諸氏に感謝します。

参考文献

- [1] 安浦寛人, 石浦菜岐佐: ハザード検出問題の計算複雑さについて, 電子通信学会技術研究報告COMP86-64, pp. 29~37, (Jan. 1987).
- [2] M. A. Breuer and A. D. Friedman: *Diagnosis and Reliable Design of Digital Systems*, Computer Science Press, (1976).
- [3] 平石裕実, 濱口清治, 矢島脩三: 正則時相論理の充足可能性判定アルゴリズム, 電子情報通信学会昭和62年総合全国大会1420, p. 6-98, (May 1987).
- [4] 木村晋二, 矢島脩三: 論理回路の入力制約および入出力仕様の記述とその検証, 電子通信学会論文誌, Vol. J69-D, No. 4, (April 1986).
- [5] J. E. Hopcroft and J. D. Ullman: *Introduction to Automata Theory, Languages, and Computation*, Addison Wesley, (1979).