

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2011年3月3日(03.03.2011)

PCT

(10) 国際公開番号
WO 2011/024314 A1

- (51) 国際特許分類:
G06F 11/36 (2006.01) G06F 11/28 (2006.01)
- (21) 国際出願番号: PCT/JP2009/065209
- (22) 国際出願日: 2009年8月31日(31.08.2009)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (71) 出願人(米国を除く全ての指定国について): 株式会社 東芝(KABUSHIKI KAISHA TOSHIBA) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人(米国についてのみ): 太田 暁率(OHTA Akinori) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP). 遠藤 侑介(ENDOH Yusuke) [JP/JP]; 〒1058001 東京都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP). 進 博正(SHIN Hiromasa) [JP/JP]; 〒1058001 東京

都港区芝浦一丁目1番1号 株式会社 東芝 知的財産部内 Tokyo (JP).

- (74) 代理人: 吉武 賢次, 外(YOSHITAKE Kenji et al.); 〒1000005 東京都千代田区丸の内三丁目2番3号 富士ビル323号 協和特許法律事務所 Tokyo (JP).
- (81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア

[続葉有]

(54) Title: STATE-TRANSITION VERIFYING DEVICE, AND METHOD THEREFOR

(54) 発明の名称: 状態遷移検証装置およびその方法

[図1]

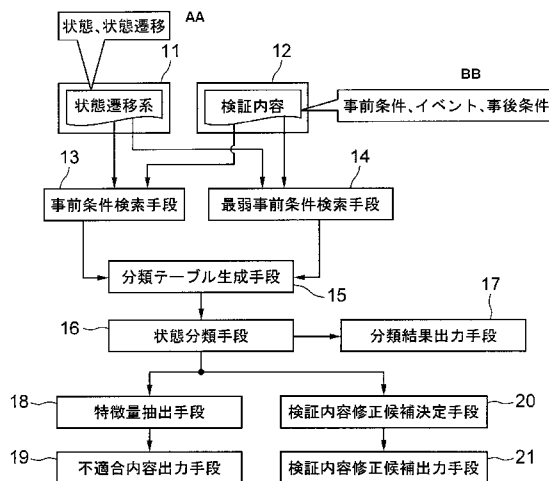


FIG. 1:
AA STATE, AND STATE TRANSITION
11 STATE TRANSITION SYSTEM
12 VERIFICATION CONTENT
BB PRIOR-CONDITION, EVENT, AND POST-CONDITION
13 PRIOR-CONDITION RETRIEVING MEANS
14 WEAKEST PRIOR-CONDITION RETRIEVING MEANS
15 CLASSIFICATION-TABLE GENERATING MEANS
16 STATE CLASSIFYING MEANS
17 CLASSIFIED-RESULT OUTPUTTING MEANS
18 FEATURE-QUANTITY EXTRACTING MEANS
19 NONCONFORMING-CONTENT OUTPUTTING MEANS
20 VERIFIED-CONTENT CORRECTION CANDIDATE DETERMINING MEANS
21 VERIFIED-CONTENT CORRECTION CANDIDATE OUTPUTTING MEANS

(57) Abstract: Disclosed is a state-transition verifying device for easily grasping the feature of a state which causes nonconformance. The state-transition verifying device comprises: a means for inputting a state transition system containing states defined by the combination of the values of one or more internal variables, events, and state transitions to be caused by the occurrence of the events; a means for inputting the verified content which is defined by a set of prior-conditions, the events, and post-conditions; a means for retrieving a state set (P) satisfying the prior-condition from the state transition system; a means for retrieving a state set (WP), from the state transition system, which transits to a transition target state which satisfies the post-condition when the event of the verification content occurs; a means for generating a classification table which describes all the internal variables and the belonging/not-belonging to the state sets (P and WP) with regard to all the individual states of the state transition system; a means for generating a classification tree for classifying all the states into the belonging/not-belonging to the state sets (P and WP) on the basis of those internal variables; and a means for applying nonconformance-state labels to leaf nodes indicating the belonging to the state set (P) and the not-belonging to the state set (WP).

(57) 要約:

[続葉有]



(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ
(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,
GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL,
NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ,
CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN,
TD, TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

〔課題〕 不適合を発生する状態の特徴を容易に把握する。〔解決手段〕 本発明の装置は、1 つ以上の内部変数の値の組合せで定義される複数の状態と、複数のイベントと、イベントの発生に起因して生じる状態遷移とを含む状態遷移系を入力する手段と、事前条件とイベントと事後条件との組により定義される検証内容を入力する手段と、事前条件を満たす状態集合 P を状態遷移系から検索する手段と、検証内容のイベントが発生したときに事後条件を満たす遷移先状態に遷移する状態集合 WP を状態遷移系から検索する手段と、状態遷移系の全ての状態の各々に関して、全ての内部変数と、状態集合 P、WP への所属有無とを記述した分類テーブルを生成する手段と、前記全ての状態をそれらの内部変数に基づき、状態集合 P、WP への所属有無へ分類する分類木を生成する手段と、状態集合 P に所属し状態集合 WP に所属しないことを示す葉ノードに不適合状態ラベルを付与する手段とを備える。

明 細 書

発明の名称： 状態遷移検証装置およびその方法

技術分野

[0001] 本発明は、例えばソフトウェアを始めとするシステムの設計工程における、状態遷移系と検証内容との適合性を検証する状態遷移検証装置およびその方法に関する。

背景技術

[0002] 「状態遷移系と検証内容との適合性検証」とは、設計対象システムの振舞いを表す状態遷移系が、当該システムの仕様である検証内容を満たすかを検証する事である。

[0003] 文献1 (E. Dijkstra, “A Discipline of Programming”, Chap. 3 “The Characterization of Semantics”, 1976) に記載されるように、検証内容は一般的に事前条件Pre、イベントEvent、事後条件Postの組合せ (Pre, Event, Post) で定義され、検証内容を満たすとは論理式「 $\text{Pre} \Rightarrow \text{WP}(\text{Event}, \text{Post})$ 」が成り立つ事である。ここで最弱事前条件 $\text{WP}(\text{Event}, \text{Post})$ は、状態のイベントEventが発生した後に事後条件Postを満たす状態に遷移する為の、状態遷移系の状態に関する必要十分条件である。

[0004] つまり、状態遷移系が検証内容を満たす事は、状態遷移系の任意の状態に対して、事前条件Preを満たすならば、イベントEventが発生した後に事後条件Postを満たす状態に必ず遷移する事である。この際、検証内容は、事前条件Preを満たす任意の状態でイベントEventの発生を前提としている。

[0005] 上記の論理式を集合論で言い換えると、事前条件を満たす状態集合をP、最弱事前条件 $\text{WP}(\text{Event}, \text{Post})$ を満たす状態集合をWPで表したとき、検証内容を満たすとは $P \subseteq \text{WP}$ が成り立つ事である。

[0006] 従来の検証技術では、適合性を検証するために差集合 $P - \text{WP}$ を計算し、 $P - \text{WP}$ が空集合であれば状態遷移系は検証内容を満たすとし、空集合でないときは $P - \text{WP}$ の要素を反例として出力する。

発明の概要

発明が解決しようとする課題

[0007] 従来の検証方法では、不適合が発生した場合の反例として、不適合が発生する状態のリストを出力していた。その為、不適合が発生する状態の特徴の把握（つまり状態のどの内部変数が、どの値のときに不適合が発生するか）と、不適合を解決する修正案の検討が困難であった。

[0008] 本発明は、不適合が発生する状態の特徴を容易に把握することが可能な情報を生成および出力する状態遷移検証装置およびその方法を提供する。

課題を解決するための手段

[0009] 本発明の状態遷移検証装置は、

それぞれ1つ以上の内部変数の値の組合せで定義される複数の状態と、複数のイベントと、各前記イベントの発生に起因して生じる状態遷移とにより定義される状態遷移系を入力する第1入力手段と、

遷移元状態の前記内部変数の値が満たすべき事前条件と、前記複数のイベントのうちの1つのイベントと、前記遷移元状態で前記1つのイベントが発生したときに遷移先状態の前記内部変数の値が満たすべき事後条件との組により定義される検証内容を入力する第2入力手段と、

前記事前条件を満たす状態集合Pを前記状態遷移系から検索する第1検索手段と、

前記1つのイベントが発生したときに前記事後条件を満たす遷移先状態に遷移する状態集合WPを前記状態遷移系から検索する第2検索手段と、

前記状態遷移系の全ての状態に関して、前記全ての状態のそれぞれの全ての内部変数と、前記状態集合Pおよび前記状態集合WPへの所属有無とを記述した分類テーブルを生成する分類テーブル生成手段と、

前記分類テーブルを用いて、前記全ての状態を、前記全ての状態のそれぞれに含まれる内部変数の値に基づき、前記状態集合Pおよび前記状態集合WPへの所属有無へ分類する分類木を生成する状態分類手段と、

前記分類木において前記状態集合Pに所属し前記状態集合WPに所属しないこ

とを示す葉ノードに、前記検証内容との不適合を表すラベルを付与し、前記ラベルが付与された分類木を出力する第1出力手段と、
を備える。

発明の効果

[0010] 本発明により、不適合を発生する状態の特徴を容易に把握することが可能な情報を生成および出力することが可能となる。

図面の簡単な説明

[0011] [図1]本発明の一実施形態としての状態遷移検証装置のブロック図。

[図2]状態表の例を示す図。

[図3]状態遷移表の例を示す図。

[図4]実施例1に係る全体の処理の流れを示すフローチャート。

[図5]実施例1に係る事前条件集合Pを示す図。

[図6]実施例1に係る処理2の詳細フローチャート。

[図7]実施例1に係るイベントフィルタ処理を説明する図。

[図8]実施例1に係る事後条件フィルタ処理を説明する図。

[図9]実施例1に係る最弱事前条件集合WPを示す図。

[図10]実施例1に係る分類テーブルを示す図。

[図11]実施例1に係る分類木を示す図。

[図12]実施例1に係る出力例を示す図。

[図13]実施例2に係る全体の処理の流れを示すフローチャート。

[図14]実施例2に係る分類テーブルを示す図。

[図15]実施例2に係る分類木を示す図。

[図16]実施例2に係る出力例を示す図。

[図17]実施例3に係る全体の処理の流れを示すフローチャート。

[図18]図17の処理5を説明する図。

[図19]実施例4に係る全体の処理の流れを示すフローチャート。

[図20]図19の処理5を説明する図。

[図21]クルーズコントローラの状態遷移系の一部を示す図。

[図22] 反例状態集合P-WPの出力例を示す図。

発明を実施するための形態

- [0012] 以降に記載する本発明の実施例1～4は、単純なクルーズコントローラを題材にして説明される。ここでは、各実施例の説明に先立ち、クルーズコントローラの概要と、本件発明者が本発明を着想するに至った技術的背景について説明する。
- [0013] クルーズコントローラは、アクセルペダルを踏まなくても自動的に一定車速を維持する車両制御システム的一种である。目標車速を維持する為に、現在の車速に対して適切にスロットルの開度を調整する。例えば、現在の車速が目標車速よりも遅ければ、スロットル開度を上げる。また、加速ボタンが押されれば、目標車速を一定量加算する。
- [0014] クルーズコントローラは、これらの機能を実現するために、現在車速や目標車速などを表す複数の内部変数を保持する。また、加速ボタンを押すなどの各種イベントに対して、定められた通り内部変数を更新する処理を実行する。
- [0015] 図21はクルーズコントローラの状態遷移系の一部分を取り出して示したものである。
- [0016] 状態遷移系は、対象システム（ここではクルーズコントローラ）の振舞いを網羅的に記述したものであり、システムが保持する全内部変数値のスナップショットである状態と、各種イベント発生に伴う状態の移り変わりである状態遷移とで定義される。図21では丸が状態を、二つの状態を結ぶ矢印が状態遷移を表す。
- [0017] 状態1は内部変数OpMode(動作モード)が“PowerOFF”、CRNe(目標車速)が0、Vel(車速)が130、CruiseLamp(クルーズランプ)が“OFF”の状態である。イベント“CruiseSwitch=ON”の発生後に、別の状態15に遷移する(状態遷移359)。状態15は内部変数OpMode(動作モード)“Standby”、CRNe(目標車速)が0、Vel(車速)が130、CruiseLamp(クルーズランプ)が“ON”の状態である。OpMode(動作モード)が“PowerOFF”から“Standby”へ、CruiseLamp(クルーズラン

プ)が“OFF”から“ON”へ変化している。

[0018] また状態10は、内部変数OpMode(動作モード)が“PowerOFF”、CRNe(目標車速)が0、Vel(車速)が40、CruiseLamp(クルーズランプ)が“OFF”の状態である。イベントCruiseSwitch=“ON”の発生後に、別の状態24に遷移する(状態遷移143)。状態24は内部変数OpMode(動作モード)が“PowerOFF”、CRNe(目標車速)が0、Vel(車速)が40、CruiseLamp(クルーズランプ)が“OFF”の状態である。

[0019] ここで上記クルーズコントローラに対する検証内容を以下のように設定したとする。

Pre(事前条件): 「OpMode(動作モード)= “PowerOFF” && Vel(車速) ≥ 40」

Event(イベント): 「CruiseSwitchON」

Post(事後条件): 「OpMode(動作モード)= “Standby” && CruiseLamp(クルーズランプ)= “ON”」

この検証内容は、事前条件Preを満たすならば、イベントEventが発生した後に事後条件Postを満たす状態に遷移することを要求する。この際、検証内容は、事前条件Preを満たす任意の状態イベントEventの発生を前提としている。

[0020] 図21の状態1は事前条件を満たし、イベント“CruiseSwitchON”の発生後に状態遷移359により事後条件を満たす状態15へ遷移している。従って、状態1は検証内容を満たす。一方で、図21の状態10は、事前条件を満たすものの、イベント“CruiseSwitch=ON”による遷移先である状態24は、内部変数OpMode(動作モード)が“PowerOFF”、CruiseLamp(クルーズランプ)が“OFF”であるため、事後条件を満たさない。従って、状態10は検証内容を満たさない。

[0021] 上記状態遷移系が検証内容を満たすか否かの検証は、事前条件Preを満たす状態集合P、最弱事前条件WP(Event, Post)を満たす状態集合WPを計算し、差集合P-WPを求める事で行われる。差集合P-WPは、事前条件を満たすがイベントの発生後に事後条件を満たさない状態に遷移する状態と、事前条件を満た

すが当該イベントが発生しない状態との集合である。差集合 $P-WP$ が空集合ではない場合は、差集合 $P-WP$ を、検証の反例の状態集合として出力する。

[0022] 本例では、状態10が検証内容を満たさない反例の1つとなる。図22に反例の状態集合の出力結果例を示す。表の一行目は状態を一意に識別する状態番号、二行目以降は状態の各内部変数の値である。この表からでは、差集合 $P-WP$ の状態の特徴、つまり内部変数がどのような値のときに状態が検証内容を満たさないのか、を把握する事は困難である。実際の製品開発等では、反例の状態数も内部変数の数も更に多くなり、問題は更に深刻化する。

[0023] 本発明は、このような問題を解決して、差集合 $P-WP$ の状態の特徴を容易に把握できるようにしようとするものである。

実施例 1

[0024] 図1は本発明の一実施形態に係る状態遷移検証装置の構成を示すブロック図である。

[0025] この状態遷移検証装置は、状態遷移系を入力する第1入力手段11、検証内容のデータを入力する第2入力手段12、事前条件検索手段（第1検索手段）13、最弱事前条件検索手段（第2検索手段）14、分類テーブル生成手段15、状態分類手段16、分類結果出力手段（第1出力手段）17、特徴量抽出手段（抽出手段）18、不適合内容出力手段（第2出力手段）19、検証内容修正候補決定手段（取得手段）20、検証内容修正候補出力手段（第3出力手段）21を備える。

[0026] ただし、特徴量抽出手段18、不適合内容出力手段19は主に実施例3に関連する要素であり、検証内容修正候補決定手段20、検証内容修正候補出力手段21は主に実施例4に関連する要素であるため、これらの要素については本実施例での説明は行わず、それぞれの実施例3、4の中で説明する。

[0027] 第1入力手段11は、状態表と、状態遷移表とで定義される状態遷移系を、例えばメモリ、ハードディスク、光ディスク等から読み込み、本装置へ入力する。

[0028] 状態表は、各状態の識別子（状態番号）と、全内部変数の変数値とを含む。状態表の一例を図2に示す。例えば、状態1は内部変数OpMode（動作モード）

が“PowerOFF”、CRNe(目標車速)が0、CruiseLamp(クルーズランプ)が“OFF”、SetLamp(セットランプ)が“OFF”、CruiseSwitch(クルーズスイッチ)が“OFF”、Vel(車速)が130、Throttle(スロットル)が0、の状態である。初期状態は状態0である。

[0029] 状態遷移表は各状態遷移の識別子(遷移番号)と状態遷移元の状態識別子(遷移元)と状態遷移先の状態識別子(遷移先)と遷移の内容(イベント)とを含む。状態遷移表の一例を図3に示す。例えば、状態遷移表の状態遷移23(遷移番号)は、イベント「CruiseSwitchOn」による遷移であり、状態0のときに当該イベントの発生により状態14に遷移する。

[0030] 第2入力手段12は、事前条件Pre、イベントEvent、事後条件Postの組合せで定義される検証内容のデータを、例えばメモリ、ハードディスク、光ディスク等の記録媒体から読み出して入力する。事前条件は遷移元状態の内部変数の値が満たすべき条件式であり、イベントEventは状態遷移系に含まれるイベントのうちの1つであり、事後条件は、遷移元状態でイベントEventが発生したときに遷移先状態の内部変数の値が満たすべき条件式である。

[0031] 本実施例1では検証内容として、先に示した下記のものを用いる。

[0032] Pre(事前条件): 「OpMode(動作モード)= “PowerOFF” && Vel(車速) ≥ 40
」

Event(イベント): 「CruiseSwitchON」

Post(事後条件): 「OpMode(動作モード)= “Standby” && CruiseLamp(クルーズランプ)= “ON” 」

事前条件検索手段(第1検索手段)13は、状態表と検証内容の事前条件とを読み込み、検証内容の事前条件を満たす状態遷移系の状態集合Pを検索する。検索した状態集合Pを分類テーブル生成手段15に出力する。事前条件検索手段13は、状態遷移系記憶手段11からデータを読み込む読み込み手段、検証内容記憶手段12からデータを読み込む読み込み手段を有してもよい。

[0033] 最弱事前条件検索手段(第2検索手段)14は、状態表と、状態遷移表と、検証内容のイベントおよび事後条件とを読み込み、検証内容の最弱事前条件(イ

ベントが発生したときに事後条件を満たす状態に遷移する状態の必要十分条件)を満たす状態遷移系の状態集合WPを検索する。最弱事前条件検索手段14は、検索した状態集合WPを分類テーブル生成手段15に出力する。

[0034] 分類テーブル生成手段15は、状態表と、状態集合Pと、状態集合WPとに基づき、状態遷移系の全ての状態に関して状態の全ての内部変数と、状態集合Pと状態集合WPそれぞれへの所属有無とを記述した分類テーブルを生成する。分類テーブル生成手段15は、分類テーブルを状態分類手段16に出力する。

[0035] 状態分類手段16は、分類テーブル生成手段15で生成された分類テーブルを用いて、各状態をその内部変数値に基づき状態集合P、WPへの所属有無へ分類する分類木を生成する。分類木の生成には既に知られている任意のアルゴリズムを用いることができ、例えばID3アルゴリズム(J. R. Quinlan, “Induction of Decision Trees”, Chap. 4 “ID3”, 1986)を用いることができる。このID3では、状態の各内部変数に対し状態集合Pと状態集合WPの所属有無を決定した場合における平均情報量の期待値を計算し、その中で平均情報量が最大になる内部変数を選び、それを木のノードにする操作を再帰的に行う。

[0036] 分類結果出力手段(第1出力手段)17は、分類木において、状態集合P、WP共に属するとの分類を示す葉ノードに、検証内容と適合する状態を意味する「適合状態」をラベル付けし、状態集合Pに属するが状態集合WPに属しないとの分類を示す葉ノードに、検証内容との不適合な状態を意味する「不適合状態」をラベル付けし、状態集合Pに所属しないとの分類を示す葉ノードに検証内容と無関係な状態を意味する「無関係」をラベル付けする。分類結果出力手段17は、ラベル付けした分類木を出力する。分類木は、表示装置またはプリンタ等の出力インターフェースに出力して、ユーザに提示されてもよい。本装置は分類木を記憶する記憶装置をさらに備えてもよい。

[0037] 以下、図2の状態表、図3の状態遷移表、上記した検証内容の例に基づき、本装置の動作を具体的に説明する。

[0038] 図4は、実施例1に係る装置の全体処理のフローチャートである。

[0039] Step1 (処理1: 事前条件検索)

事前条件検索手段13が、図2の状態表と、上記の検証内容（事前条件）とを読み込み、検証内容の事前条件を満たす、状態遷移系の状態集合Pを検索する。

[0040] 具体的に、事前条件検索手段13は、図5に示すように、図2の状態表における事前条件を満たす状態番号を逐次特定し、特定した状態番号の集合である状態集合 $P = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 24, \dots\}$ を得る。例えば状態0は事前条件を満たさないで状態集合Pには含まれないが、状態1は事前条件を満たすので状態集合Pに含まれる。

[0041] 事前条件検索手段13は、このようにして得た事前条件状態集合Pを分類テーブル生成手段15に出力する。

[0042] Step2（処理2：最弱事前条件検索）

最弱事前条件検索手段14は、図2の状態表および状態遷移表と、上記検証内容（イベント、事後条件）とを読み込み、検証内容の最弱事前条件を満たす状態遷移系の状態集合WPを検索する。

[0043] 図6は本処理の詳細フローを示す。

[0044] 処理2-1（イベントフィルタ）では、状態遷移表から検証内容のイベントを含む遷移（行）のみを抽出した状態遷移表（イベントフィルタ後）を得る。例えば図7に示すように、状態遷移0から22は、これらのイベントが検証内容のイベント(Event)「CruiseSwitchON」と異なるので抽出されない。一方で状態遷移23はこのイベントが検証内容のイベント(Event)「CruiseSwitchON」と一致するため抽出される。このようにして図7の右に示す状態遷移表（イベントフィルタ後）が得られる。

[0045] 処理2-2（事後条件フィルタ）では、状態遷移表（イベントフィルタ後）において、検証内容の事後条件を満たす遷移先をもつ遷移（行）のみを抽出した状態遷移表（事後条件フィルタ後）を得る。例えば、状態遷移23の遷移先状態14は、図8下の状態表（図2の一部を参考のために切り出したもの）から分かるように事後条件(Post)「OpMode(動作モード) = “Standby” && CruiseLamp(クルーズランプ) = “ON”」を満たさないため抽出されない。一方で状態

遷移167の遷移先状態23は、検証内容の事後条件(Post)を満たすため抽出される。同様に状態遷移191、215なども抽出される。このようにして図8の右に示す状態遷移表（事後条件フィルタ後）が得られる。

[0046] 処理2-3（状態リスト取得）では、図9に示すように、状態遷移表（事後条件フィルタ後）の全ての状態遷移から遷移元の状態番号を取得し、取得した状態番号の集合である最弱事前条件集合WP = {7, 8, 9, ...} を得る。

[0047] 最弱事前条件検索手段14はこのようにして得た最弱事前条件集合WPを分類テーブル生成手段15に出力する。

[0048] Step3(処理3：分類テーブル生成)

分類テーブル生成手段15は、図2の状態表と、図5下の状態集合Pと、図9下の状態集合WPとに基づき、状態遷移系の全ての状態に関して、状態の全ての内部変数と、事前条件状態集合Pおよび状態集合WPへの所属有無とを記述した分類テーブルを生成する。生成された分類テーブルを図10に示す。

[0049] 図10の分類テーブルは、状態表の全項目（状態番号、全内部変数）と、事前条件状態集合Pへの所属有無を示す項目と、最弱事前条件状態集合WPへの所属有無を示す項目を持つ。例えば状態0は状態集合P、WP共に含まれないので、各項目は共に「FALSE」となる。状態1は状態集合P、WP共に含まれるので、各項目は共に「TRUE」となる。状態10は状態集合Pに含まれ、WPに含まれないので、事前条件集合Pへの所属が「TRUE」、最弱事前条件集合WPへの所属が「FALSE」となる。

[0050] Step4（処理4：状態分類）

状態分類手段16は、図10の分類テーブルに基づき、状態集合を事前条件集合Pと最弱事前条件集合WPへの所属有無へ分類するための分類木を生成する。生成された分類木を図11に示す。分類木の葉ノードは事前条件集合Pと最弱事前条件集合WPへの所属有無を表し、葉ノード以外のノード（トップノード、中間ノード）は複数の内部変数のうちの一つに対応し、子ノードへ延びる枝はその内部変数の取り得る値である。葉ノードは、トップノードから一意に定まる経路によって表される内部変数値に対する分類結果（P、WPへの所属有

無)を表す。

[0051] 図11の分類木から、例えば、OpMode(動作モード)が“PowerOFF”、Vel(車速)が50以上である状態は、事前条件集合Pと最弱事前条件集合WP共に所属すると判定される。また、OpMode(動作モード)が“PowerOFF”、Vel(車速)が40である状態は、事前条件集合Pに所属するが、最弱事前条件集合WPには所属しないと判定される。

[0052] Step5 (処理5: 分類結果出力)

分類結果出力手段17は、図11の分類木で、状態集合P、WPへの所属が共に「TRUE」である葉ノードに“適合状態”ラベルを、状態集合Pへの所属が「TRUE」であり、状態集合WPへの所属が「FALSE」である葉ノードに“不適合状態”ラベルを、そして状態集合Pへの所属が「FALSE」である葉ノードに“無関係”ラベルを付する。このようにラベル付けされた分類木を図12に示す。なお状態集合Pへの所属が「FALSE」である葉ノードは、状態集合WPへの所属が「True」であるものも「False」であるものも両方含む。図11の例では後者のみが存在する。

[0053] したがって、この分類木は、状態集合を適合状態(状態集合Pにも状態集合WPにも属する状態)、不適合状態(状態集合Pに属するが状態集合WPに属さない状態)、無関係(状態集合Pに属さない状態)に分類する。不適合状態は、差集合P-WPの要素であり、差集合P-WPは不適合状態集合とも称される。不適合状態集合が空集合でない事は、検証内容と不適合な状態が存在することを意味する。

[0054] 図11の分類木において例えば、OpMode(動作モード)が“PowerOFF”、Vel(車速)が50以上である状態は適合状態、即ち事前条件を満たし検証内容を満たす状態と判定される。また、OpMode(動作モード)が“PowerOFF”、Vel(車速)が40である状態は不適合状態、即ち事前条件を満たすが検証内容を満たさない状態と判定される。それらの以外の状態は事前条件を満たさず、検証内容に無関係な状態であると判定される。尚、これらの分類に関して、OpMode(動作モード)、Vel(車速)以外の内部変数は、検証内容と無関係である事も確認

できる。

- [0055] 分類結果出力手段17は、ラベル付けされた分類木を出力インターフェース等に出力して、ユーザに提示する。ユーザはこの分類木を参照することで、特にトップノードから不適合状態を示す葉ノードへ至るパス上の内部変数と変数値とを参照することで、不適合内容（不適合状態に共通する内部変数と変数値の組合せ）を容易に把握できる。すなわち従来は単に不適合状態のリストを出力していたのに対し、本実施例では状態を適合状態と不適合状態に分類する分類木を可視的に表示することで、不適合内容を可視的に容易に把握できる。

実施例 2

- [0056] 本実施例2は、不適合状態への分類のみを含み、それ以外への状態（適合状態および無関係な状態）への分類を省略した分類木を生成および出力することを特徴し、これにより不適合内容の把握をより容易化しようとするものである。本実施例2の装置構成は、図1と同じ要素11～17に関連する。以下実施例1との差分を中心に説明し、実施例1と重複する説明は省略する。
- [0057] 分類テーブル生成手段15は、状態表と、状態集合P、WPに基づき、状態遷移系の全ての状態に関して、状態の全ての内部変数と、条件「状態集合Pに所属して状態集合WP所属しない」の充足有無（TRUE or FALSE）を記述した分類テーブルを生成する。
- [0058] 状態分類手段16は、この分類テーブルに基づき「状態集合Pに所属して状態集合WP所属しない」への所属有無を分類する分類木を生成する。
- [0059] 分類結果出力手段17は、この分類木で、「TRUE」（状態集合Pに所属して状態集合WPに所属しない）を示す葉ノードに不適合状態ラベルを付する。そして、「FALSE」を示す全ての葉ノードと、当該葉ノードとその親ノードとを接続するエッジを削除する。更に、子ノードを持たない非葉ノード（葉ノード以外のノード）と、その非葉ノードと親ノードを接続するエッジとを削除する操作を、子ノードを持たない非葉ノードが存在しなくなるまで繰り返す。分類結果出力手段17はこのようにして得た分類木を出力する。

[0060] 図13は実施例2に係る装置の全体処理のフローチャートである。大半の処理は実施例1と同じである。実施例1と異なる処理を、図13ではハッチング付きのブロックで示す。Step1（処理1：事前条件検索）およびStep2（処理2：最弱事前条件検索）は実施例1と同じである。ここではStep3以降を説明する。

[0061] Step3(処理3：分類テーブル生成)

分類テーブル生成手段15は、Step2で得た集合P, WPに基づき、状態表の全状態について、条件「状態集合Pに所属して状態集合WPに所属する」の充足有無を判定し、判定結果（TRUE or FALSE）の項目を状態表に追加することにより、図14に示す分類テーブルを得る。

[0062] したがって、図14の分類テーブルは、状態表(図2)の全項目(状態番号、全内部変数)と、条件「状態集合Pに所属して状態集合WPに所属しない」の充足有無を表す項目を持つ。例えば状態0は状態集合P、WP共に含まれないので「FALSE」となる。状態1は状態集合P、WP共に含まれるので「FALSE」となる。状態2～9も同様に「FALSE」となる。状態10は状態集合Pに含まれ、状態集合WPに含まれないので「TRUE」となる。

[0063] Step4（処理4：状態分類）

状態分類手段16は、Step3で得た分類テーブル(図14)から、状態集合を条件「状態集合Pに所属して状態集合WPに所属しない」の充足有無へ分類する分類木を生成する。生成した分類木を図15に示す。OpMode(動作モード)が“Power OFF”、Vel(車速)が40である状態は、この条件を満たすと判定され（TRUE）、それ以外の状態は条件を満たさないと判定される（FALSE）。

[0064] Step5（処理5：分類結果出力）

分類結果出力手段17は、Step5で得た分類木(図15)において、「TRUE」（条件「状態集合Pに所属して状態集合WPに所属しない」）を示す葉ノードに、状態遷移系と検証内容の不適合を意味する不適合状態ラベルを付する。また「FALSE」を示す全ての葉ノードと、当該葉ノードとその親ノードとを接続するエッジを削除する。この結果、図16に示す分類木が得られる。

[0065] 図16において、OpMode(動作モード)が“PowerOFF”、Vel(車速)が40である

状態は不適合状態に分類される。不適合状態以外への分類は分類木上から省略される。

[0066] このように本実施例2では、不適合状態への分類のみを含む分類木を出力することで、不適合内容(不適合状態を特徴付ける内部変数と変数値の組合せ)の把握をより容易化することができる。

[0067] (変形例)

実施例1の状態分類生成手段で生成した分類木(例えば図11参照)を用いて、本実施例2と同様の出力を得ることも可能である。すなわち、実施例1の分類木で、「P:True, WP:False」(状態集合Pに所属して状態集合WPに所属しない)を示す葉ノードに不適合状態ラベルを付する。そして、それ以外の全ての葉ノード(すなわち「P:False, WP:False」または「P:True, WP:True」または「P:False, WP:True」を示す葉ノード)と、当該葉ノードとその親ノードとを接続するエッジを削除する。更に、子ノードを持たない非葉ノード(葉ノード以外のノード)と、その非葉ノードと親ノードを接続するエッジとを削除する操作を、子ノードを持たない非葉ノードが存在しなくなるまで繰り返す。このようにしても図11の分類木から、図16に示す分類木を得ることができる。

実施例 3

[0068] 本実施例3は、不適合状態(状態集合Pに属して状態集合WPに属さない状態)の特徴である不適合内容(状態の内部変数と、各内部変数の値との組)を出力することを特徴とし、これにより不適合内容の把握をより容易化しようとするものである。

[0069] 本実施例3の装置構成は、図1の要素11~16、18、19に関連し、特徴量抽出手段18と不適合内容出力手段19を用い、分類結果出力手段17を用いないことが実施例1と大きく異なる。以下実施例1との差分を中心に説明し、実施例1と重複する部分の説明は省略する。

[0070] 特徴量抽出手段(抽出手段)18は、状態分類手段16で生成された分類木のトップノードから、不適合状態(状態集合Pに属して状態集合WPに属さない状

態)への分類を示す葉ノードを一意に結ぶパス上に存在する全ての非葉ノード(トップノード、中間ノード)と、各非葉ノードの直下のエッジのラベル(値)との組合せを得る事で、不適合状態を特徴付ける内部変数と変数値の組合せ(不適合内容)を取得する。

[0071] 不適合内容出力手段(第2出力手段)19は、特徴量抽出手段18で得た不適合内容を入力する。不適合内容は例えば出力インターフェースを介してユーザに提示される。

[0072] 図17は本実施例3に係る装置の全体処理のフローチャートである。大半の処理は実施例1と同じである。実施例1と異なる処理を、図17ではハッチング付きのブロックで示す。Step1(処理1:事前条件検索)からStep4(処理4:状態分類)までは実施例1と同じである。ここではStep5以降を説明する。

[0073] Step5(処理5:特徴量抽出)

特徴量抽出手段18は、図11の分類木を対象に特徴量抽出処理を行う。図18にこの処理内容の一例を示す。最上部のトップノードから、最下部の不適合状態への分類を示す葉ノードを一意に結ぶパスが、点線で囲まれている。

[0074] このパスにおいて例えば、ノード1「OpMode(動作モード)」とノード1直下のエッジ「PowerOFF」から、内部変数と変数値の組合せ(OpMode、“PowerOFF”)が得られる。同様にパス上のノード2「Vel(車速)」とノード2直下のエッジ「40」から、内部変数と変数値の組合せ(Vel、40)が得られる。これらを合わせる事で、不適合状態を特徴付ける内部変数と変数値の組合せである不適合内容「OpMode=“PowerOFF”、Vel=40」が得られる。

[0075] Step6(処理6:不適合内容出力)

不適合内容出力手段19は、特徴量抽出手段18で得られた不適合内容「OpMode(動作モード)=“PowerOFF”、Vel(車速)=40」を出力する。

[0076] 以上、本実施例3によれば、不適合状態を特徴づける内部変数と変数値の組合せ(不適合内容)を出力することにより、不適合内容の把握がより容易になる。

実施例 4

- [0077] 状態遷移系と検証内容との適合性検証において不適合が発生する場合、状態遷移系に誤りが含まれる可能性と、検証内容(仕様)が誤っている可能性、両方の可能性が存在する。本実施例4は検証内容(仕様)が誤っている可能性に絞って、検証内容の事前条件の修正候補を検出して出力することを特徴とする。修正候補である事前条件は、実施例3の不適合内容と同じ形式、即ち状態の内部変数と各内部変数の値の組で表現される。
- [0078] 本実施例3の装置構成は、図1の要素11~16、20、21に関連し、検証内容修正候補決定手段20、検証内容修正候補出力手段21を用い、分類結果出力手段17を用いないことが実施例1と大きく異なる。以下実施例1との差分を中心に説明し、実施例1と重複する部分の説明は省略する。
- [0079] 検証内容修正候補決定手段(取得手段)20は、状態分類手段16で生成した分類木でトップノードから、状態集合WPへの所属を示す葉ノードを一意に結ぶパス上に存在する全ての非葉ノード(トップノード、中間ノード)と、非葉ノード直下のエッジのラベル(値)との組合せを得る事で、検証内容の事前条件の修正候補を取得する。状態集合WPへの所属を示す葉ノードは、状態集合Pへの所属が「True」のものと「False」のものとの両方を含む。
- [0080] 検証内容修正候補出力手段(第3出力手段)21は、検証内容修正候補決定手段20で得た、検証内容の修正候補を出力する。検証内容の修正候補は例えば出力インターフェースを介してユーザに提示されてもよい。この修正候補を用いることで不適合の解消が期待される。
- [0081] 図19は本実施例4に係る装置の全体処理のフローチャートである。大半の処理は実施例1と同じである。実施例1と異なる処理を、図19ではハッチング付きのブロックで示す。Step1(処理1:事前条件検索)からStep4(処理4:状態分類)までは実施例1と同じである。ここではStep5以降を説明する。
- [0082] Step5(処理5:検証内容修正候補決定)
- 検証内容修正候補決定手段20は、図11の分類木を対象に処理を行う。図20に処理内容の一例を示す。
- [0083] 最上部のトップノードから、最下部の最弱事前条件WPへの所属を示す葉ノ

ードを一意に結ぶパスが点線で囲まれている。このパスにおいて、例えば、ノード1「OpMode(動作モード)」とノード1直下のエッジ「PowerOFF」から、内部変数と変数値の組合せ(OpMode、“PowerOFF”)が得られる。同様にパス上のノード2「Vel(車速)」とノード2直下のエッジ「50以上」から、内部変数と変数値の組合せ(Vel、“50以上”)が得られる。これら合わせる事で、検証内容の事前条件の修正候補「OpMode：“PowerOFF”、Vel：“50以上”」が得られる。この修正候補を事前条件として用いることで不適合が解消される可能性が高まる。

[0084] Step6 (処理6:検証内容修正候補出力)

検証内容修正候補出力手段21は、検証内容修正候補決定手段20で得られた修正候補「OpMode：“PowerOFF”、Vel：“50以上”」を出力する。

[0085] 以上、本実施例4によれば、不適合を解決する修正候補を出力することにより、検証内容の修正作業を容易化することができる。

[0086] なお図1の状態遷移検証は、例えば、汎用のコンピュータ装置を基本ハードウェアとして用いることでも実現することが可能である。すなわち、図1の装置が備える各要素は、各要素の処理を行う指示を記述したプログラムをコンピュータに実行させることにより実現してもよい。このとき、状態遷移検証装置は、上記のプログラムをコンピュータ装置にあらかじめインストールすることで実現してもよいし、ハードディスク、メモリ装置、光ディスク等の記憶媒体に記憶して、あるいはネットワークを介して上記のプログラムを配布して、このプログラムをコンピュータ装置に適宜インストールすることで実現してもよい。

請求の範囲

[請求項1]

それぞれ1つ以上の内部変数の値の組合せで定義される複数の状態と、複数のイベントと、各前記イベントの発生に起因して生じる状態遷移とにより定義される状態遷移系を入力する第1入力手段と、

遷移元状態の前記内部変数の値が満たすべき事前条件と、前記複数のイベントのうちの1つのイベントと、前記遷移元状態で前記1つのイベントが発生したときに遷移先状態の前記内部変数の値が満たすべき事後条件との組により定義される検証内容を入力する第2入力手段と、

前記事前条件を満たす状態集合Pを前記状態遷移系から検索する第1検索手段と、

前記1つのイベントが発生したときに前記事後条件を満たす遷移先状態に遷移する状態集合WPを前記状態遷移系から検索する第2検索手段と、

前記状態遷移系の全ての状態に関して、前記全ての状態のそれぞれの全ての内部変数と、前記状態集合Pおよび前記状態集合WPへの所属有無とを記述した分類テーブルを生成する分類テーブル生成手段と、

前記分類テーブルを用いて、前記全ての状態を、前記全ての状態のそれぞれに含まれる内部変数の値に基づき、前記状態集合Pおよび前記状態集合WPへの所属有無へ分類する分類木を生成する状態分類手段と、

前記分類木において前記状態集合Pに所属し前記状態集合WPに所属しないことを示す葉ノードに、前記検証内容との不適合を表すラベルを付与し、前記ラベルが付与された分類木を出力する第1出力手段と、

を備えた状態遷移検証装置。

[請求項2]

前記分類テーブル生成手段は、前記状態遷移系の全ての状態に関して、前記全ての状態のそれぞれの全ての内部変数と、前記状態集合P

に所属しかつ前記状態集合WPへ所属しないとの条件の充足有無とを記述した分類テーブルを生成し、

前記状態分類手段は、前記全ての状態を、前記全ての状態のそれぞれに含まれる内部変数に基づき、前記条件の充足有無へ分類する分類木を生成し、

前記第1出力手段は、

(A) 前記分類木において前記条件を充足することを示す葉ノードに前記ラベルを付与し、

(B) 前記条件を充足しないことを示す葉ノードと、前記葉ノードとその親ノード間に接続するエッジとを削除し、

(C) 子ノードを持たない非葉ノードと、前記非葉ノードとその親ノード間に接続するエッジとを削除する操作を、子ノードを持たない非葉ノードが存在しなくなるまで繰り返し、

(A) ～ (C) の処理によって得られた分類木を出力することを特徴とする請求項1に記載の装置。

[請求項3]

前記分類木のトップノードから、前記状態集合Pに属し前記状態集合WPに属さないことを示す前記葉ノードを一意に結ぶパス上に存在するすべての非葉ノードの内部変数と、前記非葉ノードの直下のエッジの変数値との組合せを抽出する抽出手段と、

前記組合せを出力する第2出力手段と、

をさらに備えたことを特徴とする請求項1に記載の装置。

[請求項4]

前記分類木のトップノードから、前記状態集合WPへの所属を示す葉ノードを一意に結ぶパス上に存在する全ての非葉ノードの内部変数と、前記非葉ノードの直下のエッジの変数値との組合せを取得する取得手段と、

前記組合せを、前記事前条件の修正候補として出力する第3出力手段と、

を備えたことを特徴とする請求項1に記載の装置。

[請求項5]

コンピュータにおいて実行する状態遷移検証方法であって、

それぞれ1つ以上の内部変数の値の組合せで定義される複数の状態と、複数のイベントと、各前記イベントの発生に起因して生じる状態遷移とによって定義される状態遷移系を入力する第1入力ステップと、

遷移元状態の前記内部変数の値が満たすべき事前条件と、前記複数のイベントのうちの1つのイベントと、前記遷移元状態で前記1つのイベントが発生したときに遷移先状態の前記内部変数の値が満たすべき事後条件との組により定義される検証内容を入力する第2入力ステップと、

前記事前条件を満たす状態集合Pを前記状態遷移系から検索する第1検索ステップと、

前記1つのイベントが発生したときに前記事後条件を満たす遷移先状態に遷移する状態集合WPを前記状態遷移系から検索する第2検索ステップと、

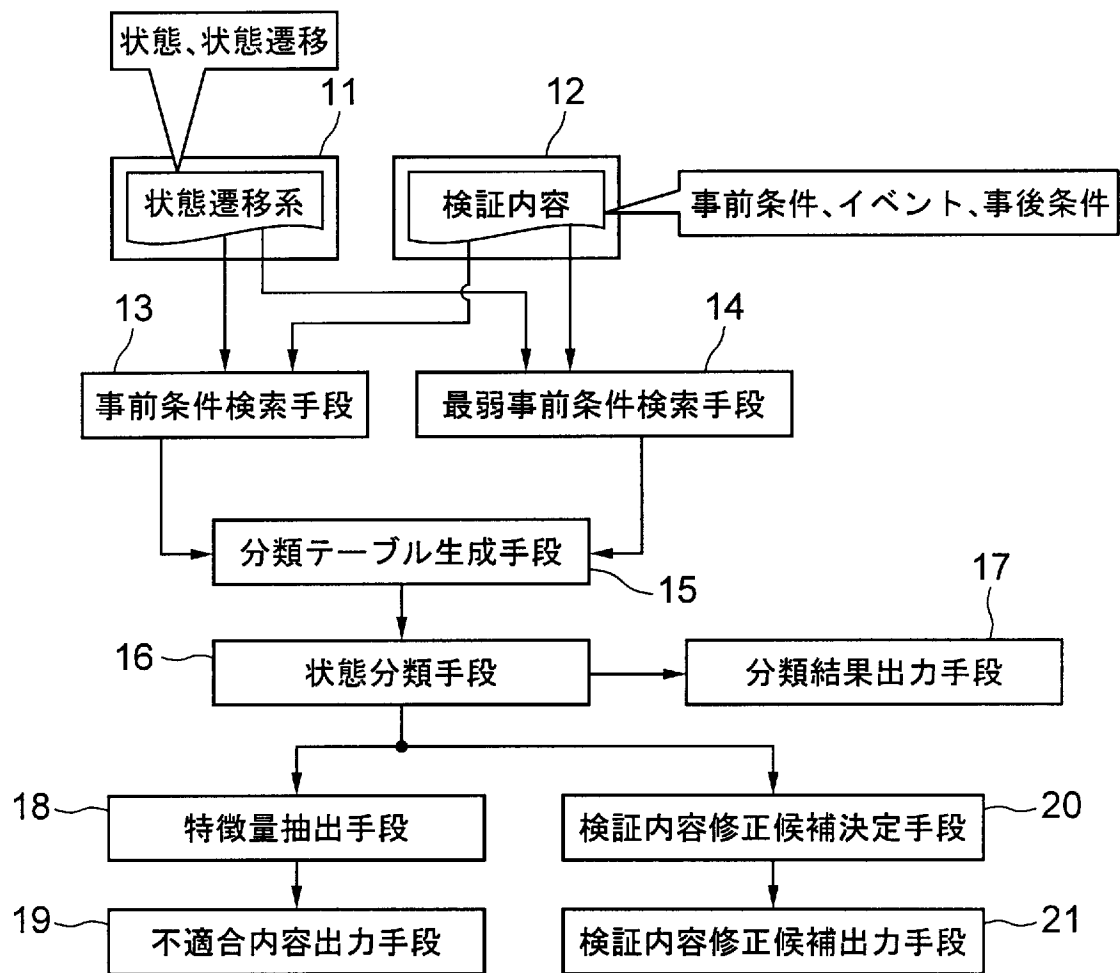
前記状態遷移系の全ての状態に関して、前記全ての状態のそれぞれの全ての内部変数と、前記状態集合Pおよび前記状態集合WPへの所属有無とを記述した分類テーブルを生成する分類テーブル生成ステップと、

前記分類テーブルを用いて、前記全ての状態を、前記全ての状態のそれぞれに含まれる内部変数の値に基づき、前記状態集合Pおよび前記状態集合WPへの所属有無へ分類する分類木を生成する状態分類ステップと、

前記分類木において前記状態集合Pに所属し前記状態集合WPに所属しないことを示す葉ノードに、前記検証内容との不適合を表すラベルを付与し、前記ラベルが付与された分類木を出力する第1出力ステップと、

を備えた状態遷移検証方法。

[図1]



[図2]

内部変数

状態表の例

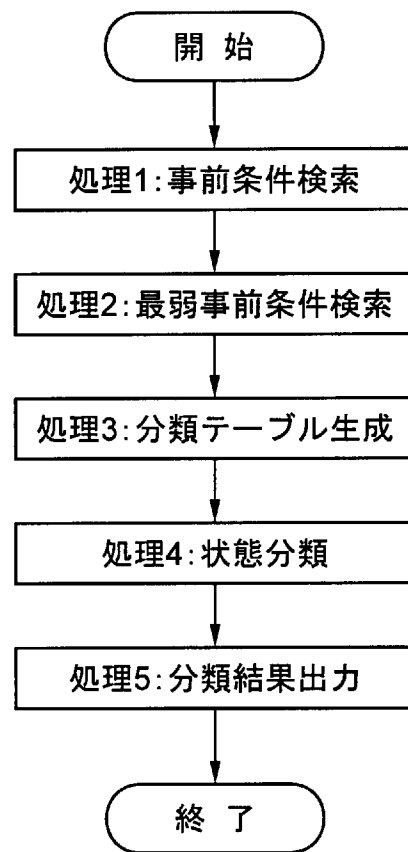
状態番号	OpMode (動作モード)	CRNe (目標車速)	CruiseLamp (クルーズランプ)	SetLamp (セットランプ)	CruiseSwitch (クルーズスイッチ)	Vel (車速)	Throttle (スロットル)
0	Power OFF	0	OFF	OFF	OFF	0	0
1	Power OFF	0	OFF	OFF	OFF	130	0
2	Power OFF	0	OFF	OFF	OFF	120	0
3	Power OFF	0	OFF	OFF	OFF	110	0
4	Power OFF	0	OFF	OFF	OFF	100	0
5	Power OFF	0	OFF	OFF	OFF	90	0
6	Power OFF	0	OFF	OFF	OFF	80	0
7	Power OFF	0	OFF	OFF	OFF	70	0
8	Power OFF	0	OFF	OFF	OFF	60	0
9	Power OFF	0	OFF	OFF	OFF	50	0
10	Power OFF	0	OFF	OFF	OFF	40	0
11	Power OFF	0	OFF	OFF	OFF	30	0
12	Power OFF	0	OFF	OFF	OFF	20	0
13	Power OFF	0	OFF	OFF	OFF	10	0
14	Power OFF	0	OFF	OFF	ON	0	0
15	Standby	0	ON	OFF	ON	130	0
16	Standby	0	ON	OFF	ON	120	0
17	Standby	0	ON	OFF	ON	110	0
18	Standby	0	ON	OFF	ON	100	0
19	Standby	0	ON	OFF	ON	90	0
20	Standby	0	ON	OFF	ON	80	0
...	...	...	...	...	...	...	...

[図3]

状態遷移表の例

遷移番号	遷移元	遷移先	イベント
0	0	1	updateVelocity130
1	0	2	updateVelocity120
2	0	3	updateVelocity110
3	0	4	updateVelocity100
4	0	5	updateVelocity90
5	0	6	updateVelocity80
6	0	7	updateVelocity70
7	0	8	updateVelocity60
8	0	9	updateVelocity50
9	0	10	updateVelocity40
10	0	11	updateVelocity30
11	0	12	updateVelocity20
12	0	13	updateVelocity10
13	0	0	updateVelocity0
14	0	0	shiftPosIsDOFF
15	0	0	shiftPosIsDON
16	0	0	brakeOFF
17	0	0	brakeON
18	0	0	cancelSwitch
19	0	0	coastSetSwitchOFF
20	0	0	coastSetSwitchON
21	0	0	accelResSwitchOFF
22	0	0	accelResSwitchON
23	0	14	cruiseSwitchON
24	14	15	updateVelocity130
25	14	16	updateVelocity120
26	14	17	updateVelocity110
...	...	...	...

[図4]



[図5]

状態表

状態番号	OpMode (動作モード)	CRNe (目標車速)	CruiseLamp (クルーズランプ)	SetLamp (セットランプ)	CruiseSwitch (クルーズスイッチ)	Vel (車速)	Throttle (スロットル)
0	Power OFF	0	OFF	OFF	OFF	0	0
1	Power OFF	0	OFF	OFF	OFF	130	0
2	Power OFF	0	OFF	OFF	OFF	120	0
3	Power OFF	0	OFF	OFF	OFF	110	0
4	Power OFF	0	OFF	OFF	OFF	100	0
5	Power OFF	0	OFF	OFF	OFF	90	0
6	Power OFF	0	OFF	OFF	OFF	80	0
7	Power OFF	0	OFF	OFF	OFF	70	0
8	Power OFF	0	OFF	OFF	OFF	60	0
9	Power OFF	0	OFF	OFF	OFF	50	0
10	Power OFF	0	OFF	OFF	OFF	40	0
11	Power OFF	0	OFF	OFF	OFF	30	0
12	Power OFF	0	OFF	OFF	OFF	20	0
13	Power OFF	0	OFF	OFF	OFF	10	0
14	Power OFF	0	OFF	OFF	ON	0	0
15	Standby	0	ON	OFF	ON	130	0
16	Standby	0	ON	OFF	ON	120	0
17	Standby	0	ON	OFF	ON	110	0
18	Standby	0	ON	OFF	ON	100	0
19	Standby	0	ON	OFF	ON	90	0
20	Standby	0	ON	OFF	ON	80	0
...	...	...	...	...	...	...	...

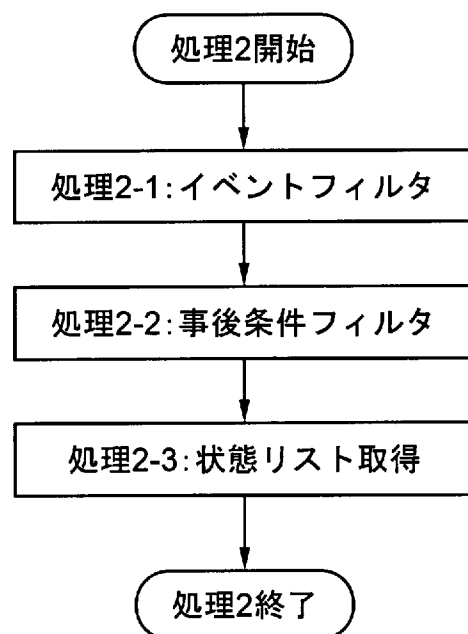
事前条件を
満たす

事前条件を
満たさない



事前条件集合P={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 24, ...}

[図6]



[図7]

状態遷移表

遷移番号	遷移元	遷移先	イベント
0	0	1	updateVelocity130
1	0	2	updateVelocity120
2	0	3	updateVelocity110
3	0	4	updateVelocity100
4	0	5	updateVelocity90
5	0	6	updateVelocity80
6	0	7	updateVelocity70
7	0	8	updateVelocity60
8	0	9	updateVelocity50
9	0	10	updateVelocity40
10	0	11	updateVelocity30
11	0	12	updateVelocity20
12	0	13	updateVelocity10
13	0	0	updateVelocity0
14	0	0	shiftPosIsDOFF
15	0	0	shiftPosIsDON
16	0	0	brakeOFF
17	0	0	brakeON
18	0	0	cancelSwitch
19	0	0	coastSetSwitchOFF
20	0	0	coastSetSwitchON
21	0	0	accelResSwitchOFF
22	0	0	accelResSwitchON
23	0	14	CruiseSwitchON
24	14	15	updateVelocity130
25	14	16	updateVelocity120
26	14	17	updateVelocity110
...	...	...	...

検証項目のイベント(Event)と異なるイベント

状態遷移表(イベントフィルタ後)

遷移番号	遷移元	遷移先	イベント
23	0	14	CruiseSwitchON
71	13	27	CruiseSwitchON
95	12	26	CruiseSwitchON
119	11	25	CruiseSwitchON
143	10	24	CruiseSwitchON
167	9	23	CruiseSwitchON
191	8	22	CruiseSwitchON
215	7	21	CruiseSwitchON
...	...	...	...

検証項目のイベント(Event)と等しいイベント

[図8]

状態遷移表(イベントフィルタ後)

遷移番号	遷移元	遷移先	イベント
23	0	14	CruiseSwitchON
71	13	27	CruiseSwitchON
95	12	26	CruiseSwitchON
119	11	25	CruiseSwitchON
143	10	24	CruiseSwitchON
167	9	23	CruiseSwitchON
191	8	22	CruiseSwitchON
215	7	21	CruiseSwitchON
...	...	...	...



状態遷移表(事後条件フィルタ後)

遷移番号	遷移元	遷移先	イベント
167	9	23	CruiseSwitchON
191	8	22	CruiseSwitchON
215	7	21	CruiseSwitchON
...	...	...	...

遷移先状態が事後条件Postを満たす状態遷移

状態表

状態番号	OpMode (動作モード)	CRNe (目標車速)	CruiseLamp (クルーズランプ)	SetLamp (セットランプ)	CruiseSwitch (クルーズスイッチ)	Vel (車速)	Throttle (スロットル)
14	PowerOFF	0	OFF	OFF	ON	0	0
21	Standby	0	ON	OFF	ON	70	0
22	Standby	0	ON	OFF	ON	60	0
23	Standby	0	ON	OFF	ON	50	0
24	PowerOFF	0	OFF	OFF	ON	40	0
25	PowerOFF	0	OFF	OFF	ON	30	0
26	PowerOFF	0	OFF	OFF	ON	20	0
27	PowerOFF	0	OFF	OFF	ON	10	0

事後条件Postを満たす状態

[図9]

状態遷移表(イベントフィルタ後)

遷移番号	遷移元	遷移先	イベント
167	9	23	CruiseSwitchON
191	8	22	CruiseSwitchON
215	7	21	CruiseSwitchON
...	...	...	...



最弱事前条件集合 $WP = \{7, 8, 9, \dots\}$

[図10]

分類テーブル

もともとの状態表

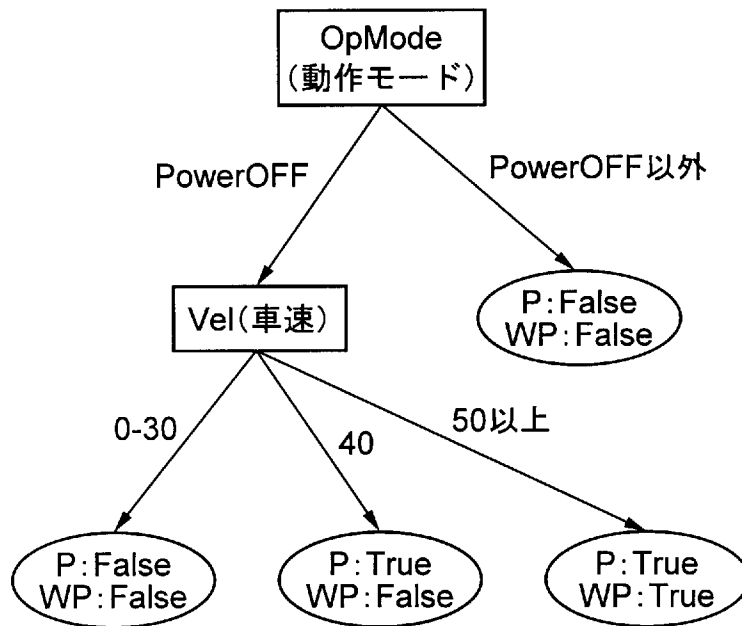
状態集合P, WPの所属有無
を示す新しい2つの例

状態番号	OpMode (動作モード)	CRNe (目標車速)	CruiseLamp (クルーズランプ)	SetLamp (セットランプ)	CruiseSwitch (クルーズスイッチ)	Vel (車速)	Throttle (スロットル)	事前条件 集合Pの所属	最弱事前条件 集合WPの所属
0	Power OFF	0	OFF	OFF	OFF	0	0	FALSE	FALSE
1	Power OFF	0	OFF	OFF	OFF	130	0	TRUE	TRUE
2	Power OFF	0	OFF	OFF	OFF	120	0	TRUE	TRUE
3	Power OFF	0	OFF	OFF	OFF	110	0	TRUE	TRUE
4	Power OFF	0	OFF	OFF	OFF	100	0	TRUE	TRUE
5	Power OFF	0	OFF	OFF	OFF	90	0	TRUE	TRUE
6	Power OFF	0	OFF	OFF	OFF	80	0	TRUE	TRUE
7	Power OFF	0	OFF	OFF	OFF	70	0	TRUE	TRUE
8	Power OFF	0	OFF	OFF	OFF	60	0	TRUE	TRUE
9	Power OFF	0	OFF	OFF	OFF	50	0	TRUE	TRUE
10	Power OFF	0	OFF	OFF	OFF	40	0	TRUE	FALSE
11	Power OFF	0	OFF	OFF	OFF	30	0	FALSE	FALSE
12	Power OFF	0	OFF	OFF	OFF	20	0	FALSE	FALSE
...	...	...	...	...	...	...	...	...	...

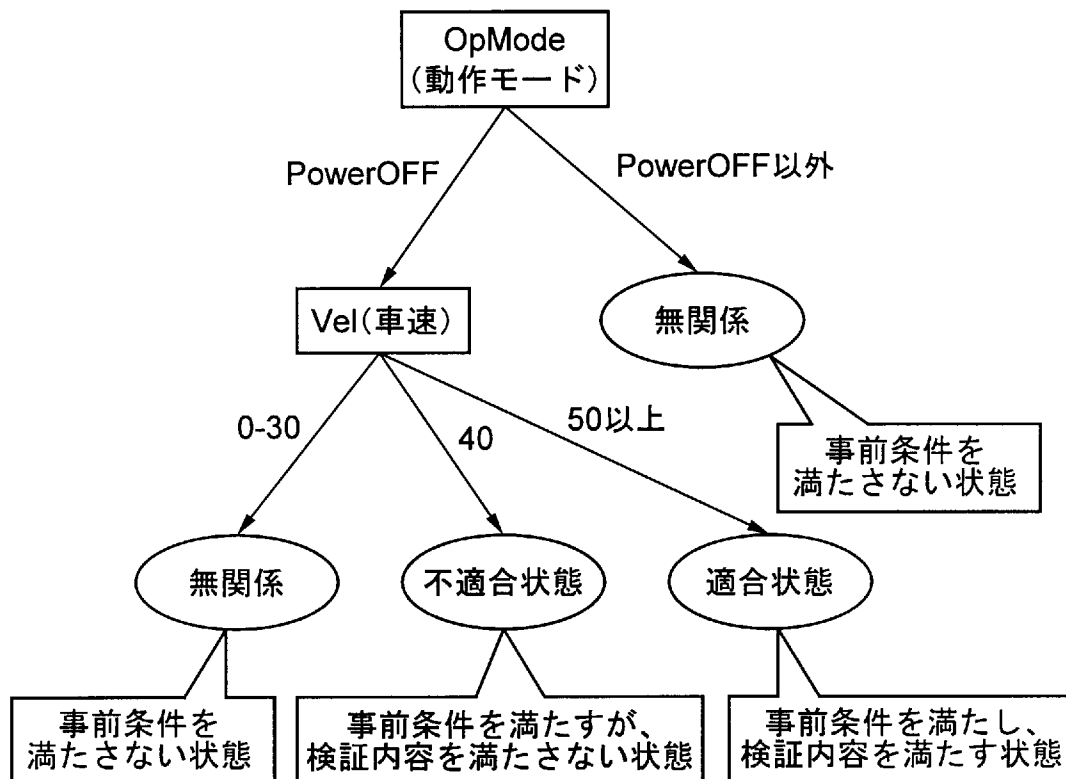
事前条件集合P={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 24, ...}

最弱事前条件集合WP={1, 2, 3, 4, 5, 6, 7, 8, 9, 53, 65, 77, ...}

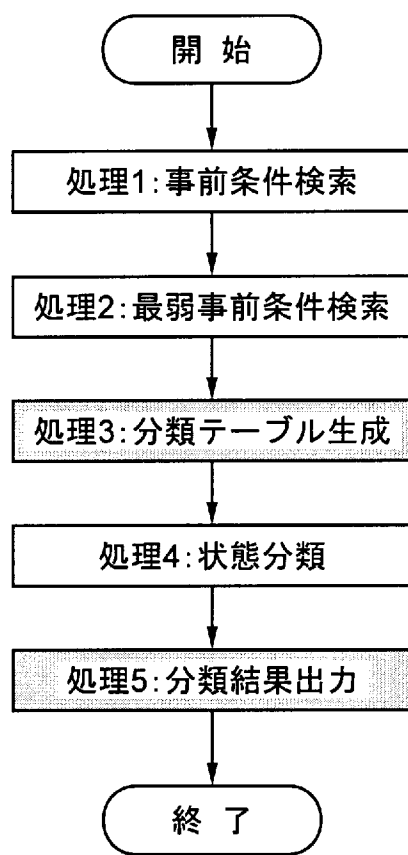
[図11]



[図12]



[図13]



[図14]

分類テーブル

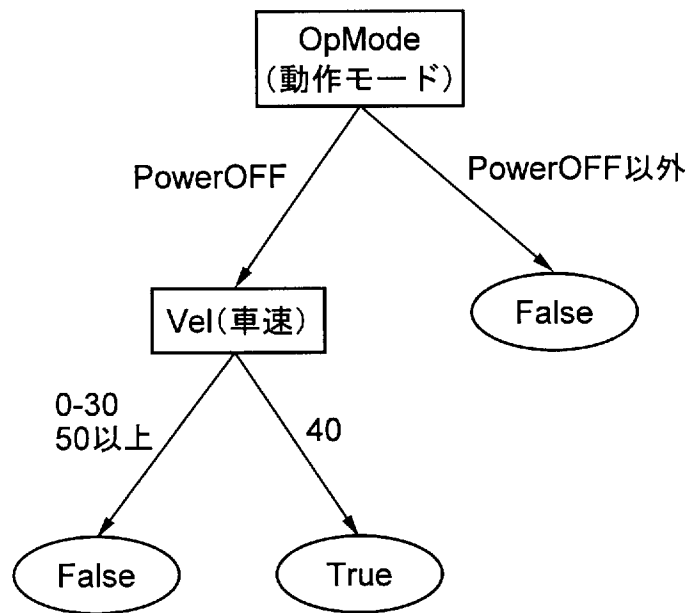
状態番号	OpMode (動作モード)	CRNe (目標車速)	CruiseLamp (クルーズランプ)	SetLamp (セットランプ)	CruiseSwitch (クルーズスイッチ)	Vel (車速)	Throttle (スロットル)	状態集合PIに所属して状態 集合WPに所属しない
0	Power OFF	0	OFF	OFF	OFF	0	0	FALSE
1	Power OFF	0	OFF	OFF	OFF	130	0	FALSE
2	Power OFF	0	OFF	OFF	OFF	120	0	FALSE
3	Power OFF	0	OFF	OFF	OFF	110	0	FALSE
4	Power OFF	0	OFF	OFF	OFF	100	0	FALSE
5	Power OFF	0	OFF	OFF	OFF	90	0	FALSE
6	Power OFF	0	OFF	OFF	OFF	80	0	FALSE
7	Power OFF	0	OFF	OFF	OFF	70	0	FALSE
8	Power OFF	0	OFF	OFF	OFF	60	0	FALSE
9	Power OFF	0	OFF	OFF	OFF	50	0	FALSE
10	Power OFF	0	OFF	OFF	OFF	40	0	TRUE
11	Power OFF	0	OFF	OFF	OFF	30	0	FALSE
12	Power OFF	0	OFF	OFF	OFF	20	0	FALSE
...	...	...	...	...	...	...	...	...

条件「状態集合PIに所属して
状態集合WPに所属する」の
充足有無を表す例

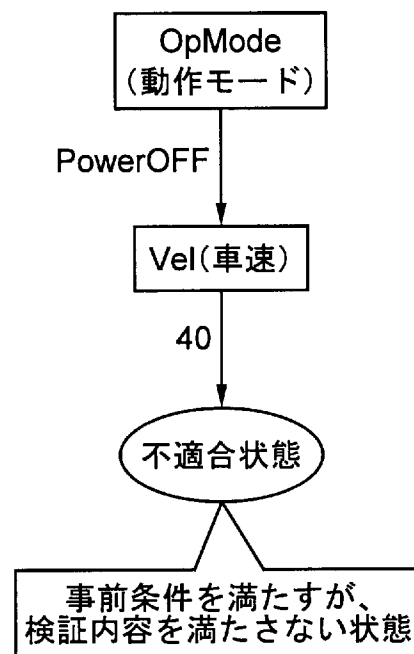
もともとの状態表

事前条件集合P={1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 24, ...}
最弱事前条件集合WP={1, 2, 3, 4, 5, 6, 7, 8, 9, 53, 65, 77, ...}

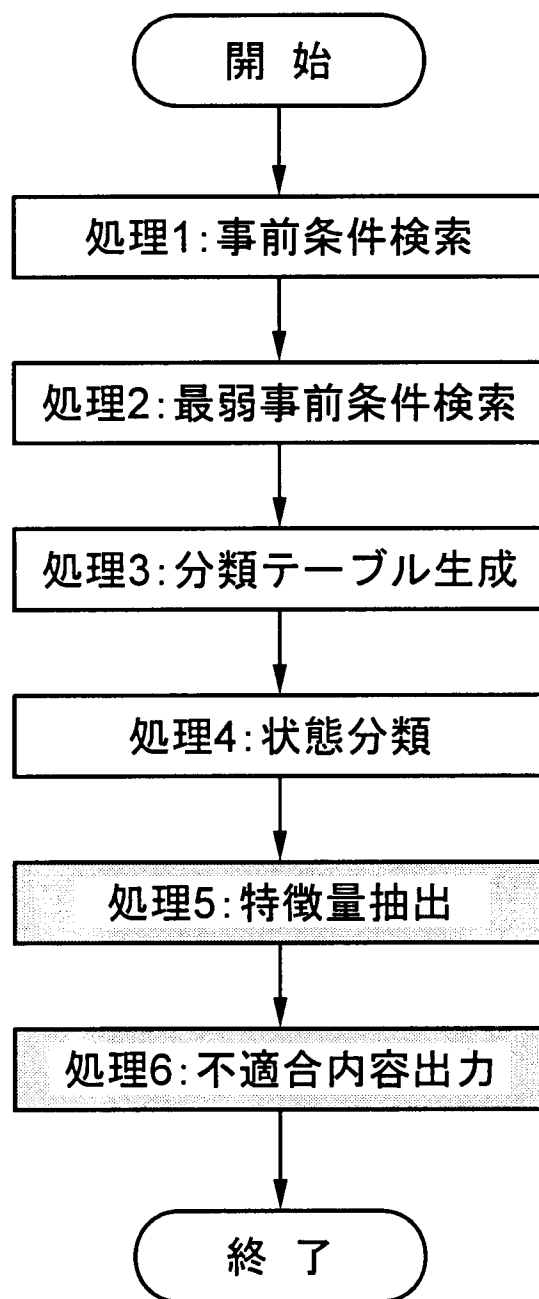
[図15]



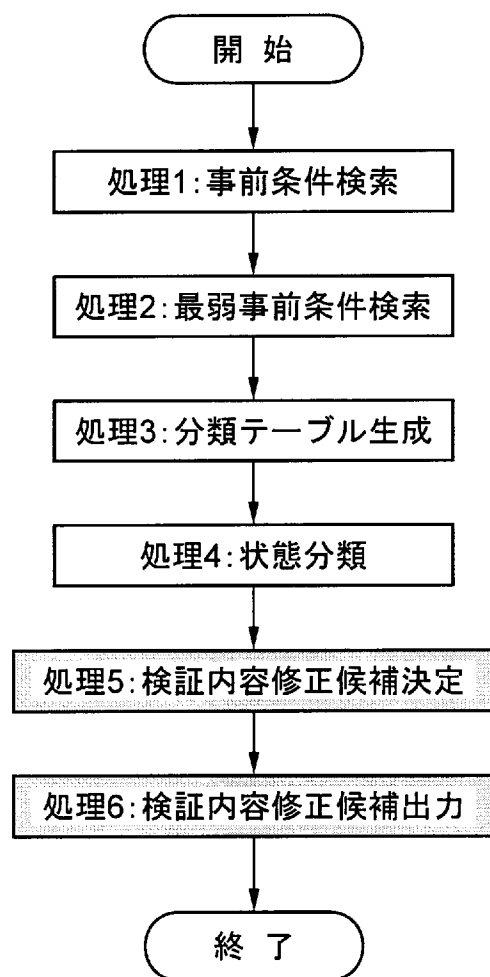
[図16]



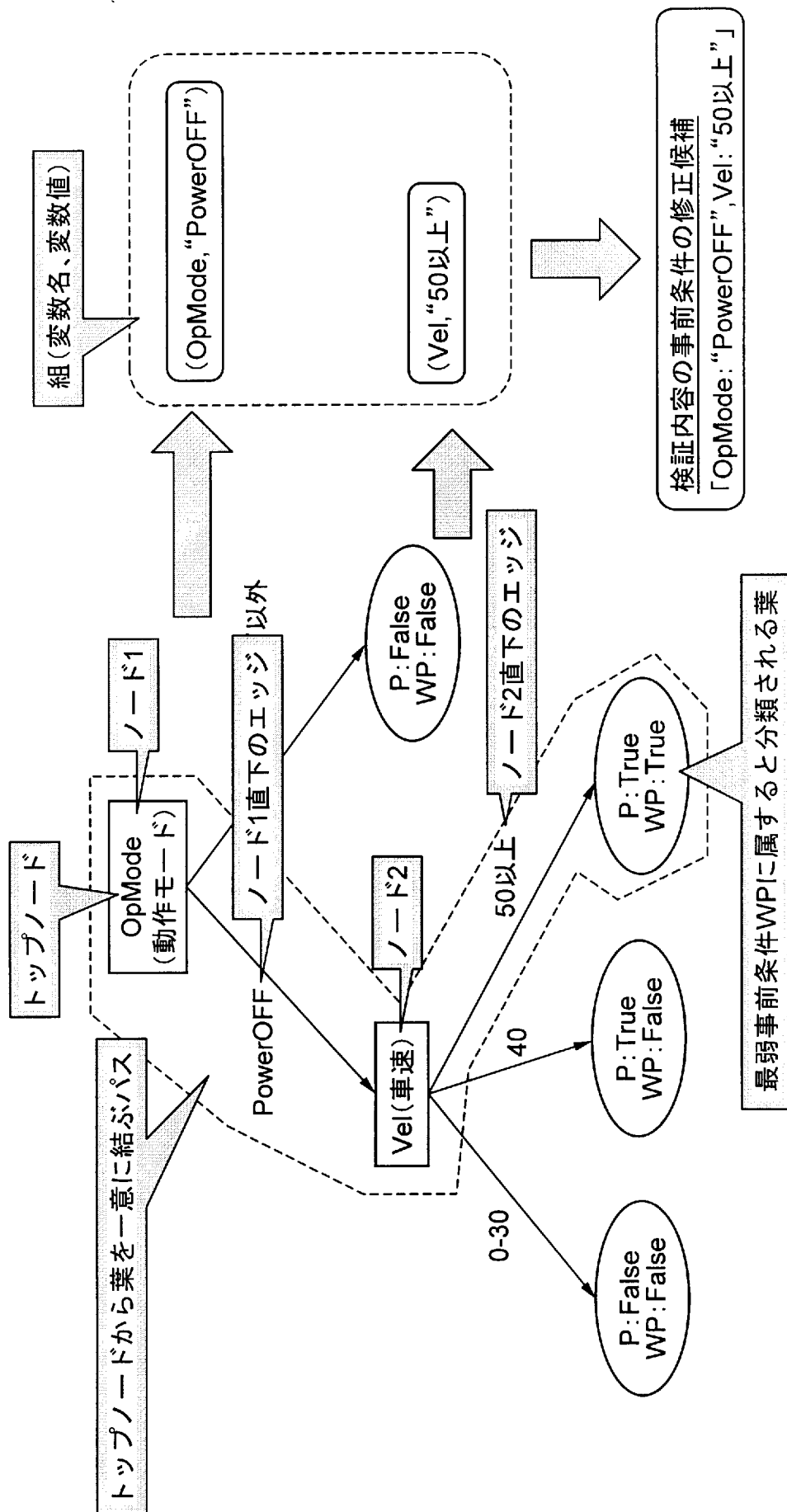
[図17]



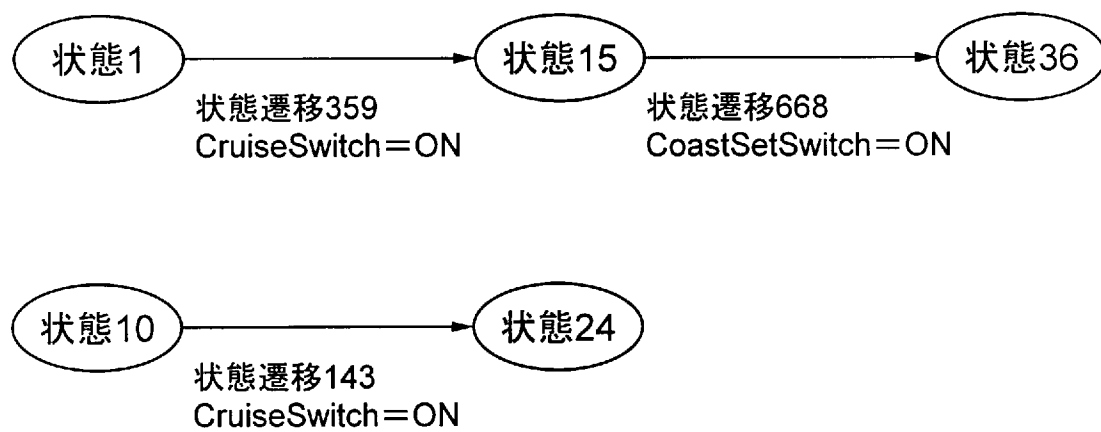
[図19]



[図20]



[図21]



[図22]

反例状態集合P-WPの出力例

状態番号	OpMode (動作モード)	CRNe (目標車速)	CruiseLamp (クルーズランプ)	SetLamp (セットランプ)	CruiseSwitch (クルーズスイッチ)	Vel (車速)	Throttle (スロットル)
10	Power OFF	0	OFF	OFF	OFF	40	0
24	Power OFF	0	OFF	OFF	ON	40	0
45	Power OFF	0	OFF	OFF	ON	40	0
119	Power OFF	0	OFF	OFF	OFF	40	0
131	Power OFF	0	OFF	OFF	ON	40	1
146	Power OFF	0	OFF	OFF	ON	40	-1
162	Power OFF	0	OFF	OFF	ON	40	0
343	Power OFF	0	OFF	OFF	OFF	40	1
357	Power OFF	0	OFF	OFF	ON	40	1
379	Power OFF	0	OFF	OFF	OFF	40	-1
402	Power OFF	0	OFF	OFF	ON	40	-1
417	Power OFF	0	OFF	OFF	OFF	40	0
431	Power OFF	0	OFF	OFF	ON	40	0
594	Power OFF	0	OFF	OFF	ON	40	1
605	Power OFF	0	OFF	OFF	OFF	40	1
635	Power OFF	0	OFF	OFF	ON	40	-1
651	Power OFF	0	OFF	OFF	OFF	40	-1
678	Power OFF	0	OFF	OFF	OFF	40	0
684	Power OFF	0	OFF	OFF	ON	40	0
726	Power OFF	0	OFF	OFF	OFF	40	1
734	Power OFF	0	OFF	OFF	OFF	40	-1
751	Power OFF	0	OFF	OFF	OFF	40	0

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/065209

A. CLASSIFICATION OF SUBJECT MATTER

G06F11/36(2006.01) i, G06F11/28(2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F11/36, G06F11/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2009
Kokai Jitsuyo Shinan Koho	1971-2009	Toroku Jitsuyo Shinan Koho	1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009-176246 A (International Business Machines Corp.), 06 August, 2009 (06.08.09), Full text; all drawings (Family: none)	1-5
A	JP 2007-11605 A (The Kansai Electric Power Co., Inc.), 18 January, 2007 (18.01.07), Full text; all drawings (Family: none)	1-5

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
09 September, 2009 (09.09.09)

Date of mailing of the international search report
29 September, 2009 (29.09.09)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類（国際特許分類（I P C））
Int.Cl. G06F11/36(2006.01)i, G06F11/28(2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F11/36, G06F11/28

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2009-176246 A（インターナショナル・ビジネス・マシーンズ・コーポレーション）2009.08.06, 全文, 全図（ファミリーなし）	1-5
A	JP 2007-11605 A（関西電力株式会社）2007.01.18, 全文, 全図（ファミリーなし）	1-5

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

0 9 . 0 9 . 2 0 0 9

国際調査報告の発送日

2 9 . 0 9 . 2 0 0 9

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官（権限のある職員）

坂庭 剛史

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 5

5 B

9 2 8 8