

明 細 書

発明の名称： 検証処理装置、検証処理方法およびプログラム

技術分野

[0001] 本開示は、検証処理装置、検証処理方法およびプログラムに関する。本願は、2020年6月3日に、日本に出願された特願2020-096792号に基づき優先権を主張し、その内容をここに援用する。

背景技術

[0002] 特許文献1には、モデル検査を用いて、データ処理システムの動作ロジックの網羅的検証を行うことが記載されている。

先行技術文献

特許文献

[0003] 特許文献1：特開2008-071135号公報

発明の概要

発明が解決しようとする課題

[0004] 例えば、モデル検査でリレー回路の動作ロジックを検証する場合、当該リレー回路の基本動作ロジックを検証するだけでは不十分であり、当該リレー回路に含まれる信号線や回路素子に不具合が発生し得ることを加味して検証を行う必要がある。

[0005] 信号線や回路素子の不具合（例えば、信号線の混触、断線、回路素子の故障）はリレー回路の基本動作ロジックによらず同時多発的かつ非同期的に発生し得ることを考慮すると、モデル検査においては、基本動作中に起こり得る状態遷移に加え、基本動作中の各状態から発生し得る不具合の全ての組み合わせを網羅的に検証する必要がある。

[0006] しかしながら、そうした場合、リレー回路に含まれる各信号線及び各回路素子で生じた複数の不具合の組み合わせを含む反例が出力されたとしても、当該不具合の組み合わせの中には、不安全事故に至ったことに必ずしも寄与しない（クリティカルでない）不具合が含まれている可能性がある。

[0007] つまり、モデル検査は、BDD (Binary Decision Diagram) などにより、検査対象モデルが取り得る全状態を論理式で表現することにより、不安全事故に至る条件（パターン）を網羅的に検査するものであり、その不安全事故に至った過程においては、必ずしもクリティカルでない状態遷移をも含み得る。そのため、不安全事故に関してクリティカルでない不具合をも含み得る反例について反例解釈を行わざるを得ず、モデル検査の反例解釈の作業に要する負担が大きかった。

[0008] 本開示の目的は、モデル検査の反例解釈の作業に要する負担を軽減可能な検証処理装置、検証処理方法及びプログラムを提供することにある。

課題を解決するための手段

[0009] 本開示の一態様によれば、検証処理装置は、複数の要素を含む検査対象モデルに対してモデル検査を実施する検査部と、前記モデル検査の結果として出力された反例に含まれる複数の要素のうちの一つ以上を選択する選択部と、複数の要素ごとの除外頻度を示す除外履歴情報を生成する除外履歴生成部と、を備え、前記検査部は、更に、前記選択された要素を除外してなる検査対象モデルに対して再度のモデル検査を実施し、前記除外履歴生成部は、前記再度のモデル検査の結果として再度の反例が出力された場合に、前記選択された要素の前記除外頻度を増加させて前記除外履歴情報を更新し、前記選択部は、前記除外履歴情報に基づき、前記除外頻度が高い要素を選択する。

[0010] また、本開示の一態様によれば、検証処理方法は、複数の要素を含む検査対象モデルに対してモデル検査を実施するステップと、前記モデル検査の結果として出力された反例に含まれる複数の要素のうちの一つ以上を選択するステップと、複数の要素ごとの除外頻度を示す除外履歴情報を生成するステップと、前記選択された要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、前記再度のモデル検査の結果として再度の反例が出力された場合に、前記選択された要素の前記除外頻度を増加させて前記除外履歴情報を更新するステップと、を有し、前記選択するステップでは、前記除外履歴情報に基づき、前記除外頻度が高い要素を選択する。

[0011] また、本開示の一態様によれば、プログラムは、コンピュータに、複数の要素を含む検査対象モデルに対してモデル検査を実施するステップと、前記モデル検査の結果として出力された反例に含まれる複数の要素のうちの一つ以上を選択するステップと、複数の要素ごとの除外頻度を示す除外履歴情報を生成するステップと、前記選択された要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、前記再度のモデル検査の結果として再度の反例が出力された場合に、前記選択された要素の前記除外頻度を増加させて前記除外履歴情報を更新するステップと、を実行させ、前記選択するステップでは、前記除外履歴情報に基づき、前記除外頻度が高い要素を選択する。

発明の効果

[0012] 上述の各態様によれば、モデル検査の反例解釈の作業に要する負担を軽減できる。

図面の簡単な説明

[0013] [図1]本開示の少なくとも一実施形態に係る検証処理装置の全体構成を示す図である。

[図2]本開示の少なくとも一実施形態に係る検証処理装置のCPUの機能構成を示す図である。

[図3]本開示の少なくとも一実施形態に係る検査対象モデルの例を示す図である。

[図4]本開示の少なくとも一実施形態に係る検証処理装置の処理フローを示す図である。

[図5]本開示の少なくとも一実施形態に係る検証処理装置による除外履歴情報の更新処理を示す図である。

[図6]本開示の少なくとも一実施形態に係る除外履歴情報の例を示す図である。

[図7]本開示の少なくとも一実施形態に係る検証処理装置の処理フローを示す図である。

[図8]本開示の少なくとも一実施形態に係る検証処理装置の処理フローを示す図である。

[図9]本開示の少なくとも一実施形態に係る検証処理装置の処理フローを示す図である。

[図10]本開示の少なくとも一実施形態に係る検証処理装置の処理フローを示す図である。

[図11]本開示の少なくとも一実施形態に係る検証処理装置のCPUの機能構成を示す図である。

[図12]本開示の少なくとも一実施形態に係る閾値決定部の処理の内容を示す図である。

発明を実施するための形態

[0014] <第1の実施形態>

以下、第1の実施形態に係る検証処理装置について、図1～図10を参照しながら説明する。

[0015] (検証処理装置の構成)

図1は、第1の実施形態に係る検証処理装置の構成を示す図である。

図2は、第1の実施形態に係る検証処理装置のCPUの機能構成を示す図である。

[0016] 図1に示すように、検証処理装置1は、CPU10と、メモリ11と、ディスプレイ12と、入力デバイス13と、ストレージ14とを備え、一般的なコンピュータとして構成されている。

[0017] メモリ11は、いわゆる主記憶装置であって、CPU10がプログラムに基づいて動作するための命令及びデータが展開される。

[0018] ディスプレイ12は、情報を視認可能に表示する表示デバイスであって、例えば、液晶ディスプレイや有機ELディスプレイなどであってよい。

[0019] 入力デバイス13は、検証処理装置1の使用者の操作を受け付ける入力デバイスであって、例えば、一般的なマウス、キーボード、タッチセンサなどであってよい。

[0020] ストレージ 14 は、いわゆる補助記憶装置であって、例えば、HDD (Hard Disk Drive)、SSD (Solid State Drive) 等であってよい。ストレージ 14 には、例えば、検査対象とするリレー回路を示す検査対象モデルMODなどが記録される。

[0021] CPU 10 は、検証処理装置 1 の動作全体の制御を司るプロセッサである。本実施形態に係るCPU 10 は、図 2 に示すように、検査部 100、選択部 101 及び除外履歴生成部 102 としての機能を発揮する。

[0022] 検査部 100 は、検査対象モデルMODに対してモデル検査を実施（実行）する。ここで実施されるモデル検査とは、BDD (Binary Decision Diagram) などにより検査対象モデルが取り得る全状態を論理式で表現することで、不安全事故に至る条件（パターン）を網羅的に検査するものである。本実施形態において実施されるモデル検査のアルゴリズムは、一般によく知られているものであってよい。

検査対象モデルMODとは、検査対象とするシステム（例えば、鉄道の保安システム）の動作ロジックが規定された情報であり、モデル検査では、ここで規定された動作ロジックにしたがって、システムの網羅的な動作検証が実施される。

また、不安全事故とは、検査対象とするシステムがいかなる場合であっても遷移してはならない状態として定義される状態である。例えば、鉄道の保安システムにおいては、“車両の自動運転制御中に非常ブレーキが効かない”状態、“車両が踏切を走行しているにもかかわらず遮断機が下りていない”状態などが不安全事故として定義される。

[0023] 選択部 101 は、検査部 100 によって実施されたモデル検査の結果に基づき、不安全事故に至る過程で状態が変化した要素の中から一つの要素を選択する。「要素」とは、検査対象モデルMODの動作ロジック及び状態を規定する最小単位であって、例えば、保安システムのリレー回路に実装されている信号線や回路素子などである。後述するように、「要素」には、現実のリレー回路に実装されている信号線や回路素子の動作そのものを模擬するも

のその他、不具合発生時におけるリレー回路の動作を模擬するために規定された仮想の素子を含む。

本実施形態に係る選択部101は、除外履歴情報（後述）に基づき、除外頻度（除外履歴値）が相対的に高い要素を選択する。

[0024] 除外履歴生成部102は、複数の要素ごとの除外頻度を示す除外履歴情報を生成する。除外履歴生成部102は、選択部101によって選択された要素を除外してなる検査対象モデルMODに対し再度のモデル検査が行われた場合において、その結果として再度の反例が出力された場合（つまり、要素を除外しても反例が消えなかった場合）に、当該選択部101が選択した要素の除外頻度を増加させるように除外履歴情報を更新する。

[0025] （検査対象モデルの例）

図3は、第1の実施形態に係る検査対象モデルの例を示す図である。

図3に示す検査対象モデルMODは、例として、鉄道の保安システムを構成するリレー回路の動作ロジックを模擬する。

図3に示す配線V及び配線Gは、それぞれ、電源線及び接地線（グラウンド）である。また、要素A1、A2、・・・はリレースイッチであり、通電に応じてOFF状態またはON状態に遷移する（0（FALSE）＝OFF／1（TRUE）＝ON）。また、要素D1、D2、・・・は、マニュアルスイッチであり、人の操作によってOFF状態またはON状態に遷移する（0＝OFF／1＝ON）。

要素X1、X2、・・・は、各信号線で発生し得る不具合（断線及び混触）を再現するために規定された仮想素子である。例えば、配線V（電源線）と要素D1（マニュアルスイッチ）とを結ぶ信号線上には、要素X1が規定されている。この要素X1は、当該信号線における不具合の一つとして“断線の発生”を再現する（0＝断線／1＝非断線）。また、要素D1と要素D2（マニュアルスイッチ）とを結ぶ信号線上には、2つの要素X2、X3が規定されている。このうち、要素X2は、当該信号線における“断線の発生”を再現し（0＝断線／1＝非断線）、要素X3は、当該信号線における“電

源線との混触の発生”を再現する（0＝非混触／1＝混触）。同様に、要素D2と要素A1（リレースイッチ）とを結ぶ信号線上には、2つの要素X4、X5が規定されている。このうち、要素X4は、当該信号線における“断線の発生”を再現し（0＝断線／1＝非断線）、要素X5は、当該信号線における“電源線との混触の発生”を再現する（0＝非混触／1＝混触）。

[0026] 実際の検査対象モデルMODは、論理式（言語）によって記述される。例えば、要素A1（リレースイッチ）に関しては、マニュアルスイッチD1、D2の他、各信号線に生じ得る不具合（断線、混触）を加味して、式（1）のように記述される。

[0027]
$$A1 = (X1 \& D1 \& X2 \& D2 \& X4) \text{ or } (X3 \& D2 \& X4) \text{ or } (X5) \cdots (1)$$

[0028] 他の要素についても同様の論理式によって記述される。

[0029] マニュアルスイッチである要素D1、D2、・・・は、人の操作に従って状態遷移する要素であるため、モデル検査においては、不具合の発生を規定する要素X1、X2、・・・と同様に、あらゆるタイミングで同時多発的かつ非同期的な状態遷移が起こり得るものとして規定される。

[0030] 後述するように、このような検査対象モデルMODは、複数の設計図面に渡って構成される。設計図面は、主に、機能ごと（例えば、車両のブレーキについての設計図面、空調についての設計図面など）に分けて作成される。

[0031] （検査および結果解釈の流れ）

図4は、第1の実施形態に係る検証処理装置の処理フローを示す図である。

図4に示す処理フローは、検証処理装置1を用いたモデル検査および結果解釈のおおまかな流れを示している。

[0032] まず、不具合が発生する要素（不具合設定素子）を設定し、検査対象モデルMODを構築する（ステップS1）。図4に示す例では、不具合設定素子として、要素X1～要素X9が設定される。そして、不安全事象を示す条件A（以下、「検査式A」とも表記する。）を設定し、モデル検査を行う。

[0033] モデル検査の結果、反例（例えば、X 1 & X 2 & X 4 & X 5 & X 6）が出力される（ステップS 2）。上述した通り、通常のモデル検査は、不安全事故（検査式A）に至るまで、不具合設定素子X 1～X 9についての状態遷移を網羅的に検査し、たまたま検査式Aに至った遷移過程を出力するものであるから、ここで出力される反例には、必ずしも主要因（クリティカル）でない不具合設定素子の状態遷移をも含み得る。つまり、反例出力の結果は、検査式Aに至ったことについての主要因のみが出力されるとは限らない。

そこで、検証処理装置1は、不具合設定素子のうち反例に含まれる素子のいくつかを検査対象モデルMODから除外し、その検査対象モデルMODについて、再度、同じ検査式Aについてのモデル検査を行う。例えば、不具合設定素子X 6を除外した検査対象モデルMODに対するモデル検査の結果、再度の反例が出力された場合は、不具合設定素子X 6は不安全事故発生のものである（主要因は他の素子にある。）と判断できる。一方、不具合設定素子X 6を除外した検査対象モデルMODに対するモデル検査の結果、再度反例が出力されなくなった場合は、不具合設定素子X 6は、不安全事故発生のものであると判断できる。このような作業を繰り返すことで、主要因となる不具合設定素子を絞り込む。

[0034] 繰り返しのモデル検査の結果、主要因の特定（結果解釈）が行われる（ステップS 3）。図4の例では、主要因となる不具合設定素子は、X 1、X 2、X 5であり、X 4、X 6は、主要因ではなかったと解釈される。

[0035] 本実施形態に係る検証処理装置1は、1回の結果解釈において主要因ではないものとして除外された不具合設定素子X 4、X 6についての除外履歴値を増やし、除外履歴情報を更新する（ステップS 4）。このステップS 4の処理については後述する。

[0036] （除外履歴情報の更新処理）

図5は、第1の実施形態に係る検証処理装置による除外履歴情報の更新処理を示す図である。

まず、前提として、重故障と単故障について説明する。

重故障とは、単独で独立して発生し得る故障モードである。図3で説明した、混触や断線などを表す要素X1、X2、・・・は、いずれも重故障である。図5に示す例では、検査対象モデルMODに4種類の重故障X1、X2、X3、X4が含まれる。

一方、単故障は、複数の異常状態のうちいずれか一つのみが起こり得る故障モードである。例えば、単故障Y1、Y2、Y3、Y4、Y5が設定されている場合、これらY1～Y5のいずれか一つのみが発生する。

[0037] 実際の検査対象モデルMODは、重故障と単故障とを含んで構築される。

このような検査対象モデルMODに対してモデル検査を行う場合、以下のような手順で行う。

まず、単故障Y1～Y5のうちどの故障が発生するか（例えば、Y1）を選択し、当該単故障Y1が発生した条件下で重故障X1～X4についての網羅的検査を行う。単故障Y1の発生条件下でのモデル検査及び結果解釈が完了したら、次の単故障（例えば、Y2）が発生した条件下で、重故障X1～X4についての網羅的検査を行う。このように、本実施形態に係る検証処理装置1は、一つの検査式Aについて、単故障の発生条件別に複数回の網羅的検査およびその結果解釈を実施する。

[0038] 図5に示す例を用いて、本実施形態に係る除外履歴生成部102が行う図4のステップS4の処理について詳しく説明する。

まず、単故障Y1の発生条件下で行われたモデル検査の結果、最終的な結果解釈がY1 & X1（つまり、重故障X1が主要因であった）となった場合、除外履歴生成部102は、主要因ではなかった（つまり、検査対象モデルMODから除外された）重故障X2、X3、X4について、除外履歴値“1”を加算する。これは、1回の結果解釈で、除外された回数が1であることを意味している。

[0039] 続いて、単故障Y2の発生条件下で行われたモデル検査の結果、最終的な結果解釈がY2 & X1 & X3（つまり、重故障X1と重故障X3が主要因であった）となった場合、除外履歴生成部102は、主要因ではなかった（つ

まり、検査対象モデルMODから除外された)重故障X2、X4について、除外履歴値“1”を加算し、全体を2(結果解釈の完了回数)で除算する。この結果、例えば、重故障X3の除外履歴値は、“ $1/2$ ”となる。これは、2回の結果解釈が完了した時点で、除外された回数が1であることを意味している。

[0040] 単故障Y3、Y4、Y5についても同様の処理を行われると、除外履歴生成部102は、その都度、各重故障X1～X5についての除外履歴値を更新する。

このように、除外履歴値は、各要素(重故障X1～X5)の、これまでに行われたモデル検査および結果解釈にて主要因とならなかった頻度を示している。

[0041] (除外履歴情報の例)

図6は、第1の実施形態に係る除外履歴情報の例を示す図である。

本実施形態に係る除外履歴生成部102は、図6に示すような除外履歴情報を作成する。

図6に示すように、除外履歴情報には、「素子個別」、「図面単位」、「検査式単位」の除外履歴値が含まれる。

「素子個別」の欄に記録される除外履歴値(以下、素子個別除外履歴値とも表記する。)は、これまでに行われた全ての結果解釈を経て累積された、要素(不具合設定素子)ごとの除外履歴値である。

これに対し、「検査式単位」の欄に記録される除外履歴値(以下、検査式単位除外履歴値とも表記する。)は、検査式A、B、C・・・別に累積された要素ごとの除外履歴値である。

[0042] また、「図面単位」の欄に記録される除外履歴値(以下、図面単位除外履歴値とも表記する。)は、設計図面単位で算出される除外履歴値である。具体的には、一つの設計図面に含まれる要素それぞれの素子個別除外履歴値の平均値(即ち、素子個別除外履歴値の合計を、その設計図面に含まれる要素数で割った値)である。図面単位除外履歴値は、その設計図面に含まれてい

る素子が総じてどの程度除外されやすいかを図面単位で表したものである。

[0043] (検証処理装置の処理フロー)

図7～図10は、第1の実施形態に係る検証処理装置の処理フローを示す図である。

以下、図7～図10を参照しながら、検証処理装置1による主要因の絞り込み処理の流れについて詳しく説明する。

[0044] 本実施形態に係る検証処理装置1は、反例出力(図4のステップS2)から結果解釈(図4のステップS3)の過程で主要因を絞り込むにあたり、図7、図8および図9に示す処理フローを順に行う。

[0045] 具体的には、図7に示す処理フローは、図面単位除外履歴値を用いた除外処理の流れを示している。また、図8に示す処理フローは、検査式単位除外履歴値を用いた除外処理の流れを示している。また、図9に示す処理フローは、素子個別除外履歴値を用いた除外処理の流れを示している。

[0046] (図面単位除外履歴値を用いた除外処理)

まず、図7を参照しながら、図面単位除外履歴値を用いた除外処理について説明する。

図7に示すように、検証処理装置1の選択部101は、図面単位除外履歴値が所定の閾値を上回っている設計図面(DWG1、DWG2、...)のうちの一つを選択する(ステップS01)。ここで、図面単位除外履歴値が所定の閾値を上回っている設計図面が一つもない場合は、この除外処理はスキップされる。

[0047] 次に、検証処理装置1の検査部100は、ステップS01で選択された一つの設計図面に含まれる全ての要素を検査対象モデルMODから除外し(ステップS02)、再度のモデル検査を実施する(ステップS03)。

[0048] 再度のモデル検査の検査結果がTRUEにならなかった(再度、反例が出力された)場合(ステップS04; NO)、ステップS02において図面単位で除外した要素は全て主要因ではなかったと判断できるので、検証処理装置1は、除外した要素を検査対象モデルMODに戻すことはせず、更なる絞

り込みを続ける。

一方、再度のモデル検査にて検査結果がTRUEに転じた（反例が出力されなくなった）場合（ステップS04；YES）、ステップS02において図面単位で除外した要素の中に主要因が含まれていたと判断できるので、検証処理装置1は、一旦、除外した要素を検査対象モデルMODに戻す（ステップS05）。

[0049] ステップS01の条件を満たす全ての設計図面を選択していない場合（ステップS06；NO）、選択部101は、当該条件を満たしている次の設計図面を選択する（ステップS07）。そして、検証処理装置1は、ステップS02からステップS05までの処理を繰り返し、主要因となる要素の絞り込みを続ける。

[0050] ステップS01の条件を満たす全ての設計図面を選択していた場合（ステップS06；YES）、検証処理装置1は、図面単位除外履歴値を用いた除外処理を終了する。

[0051] （検査式単位除外履歴値を用いた除外処理）

次に、図8を参照しながら、検査式単位除外履歴値を用いた除外処理について説明する。

図8に示すように、検証処理装置1の選択部101は、検査式単位除外履歴値が所定の閾値を上回っている要素（X1、X2、・・・）の全てを選択する（ステップS11）。ここで、検査式単位除外履歴値が所定の閾値を上回っている要素が一つもない場合は、この除外処理はスキップされる。

[0052] 次に、検証処理装置1の検査部100は、ステップS11で選択された全ての要素を検査対象モデルMODから除外し（ステップS12）、再度のモデル検査を実施する（ステップS13）。

再度のモデル検査の検査結果がTRUEにならなかった（再度、反例が出力された）場合（ステップS14；NO）、ステップS12で除外した要素は全て主要因ではなかったと判断できるので、検証処理装置1は、除外した要素を検査対象モデルMODに戻すことはせず、更なる絞り込みを続ける。

一方、再度のモデル検査にて検査結果がTRUEに転じた（反例が出力されなくなった）場合（ステップS14；YES）、ステップS12で除外した要素の中に主要因が含まれていたと判断できるので、検証処理装置1は、一旦、除外した要素を検査対象モデルMODに戻す（ステップS15）。この場合、検証処理装置1は、ステップS15で検査モデルMODに戻した要素を対象に、二分岐探索で更なる絞り込みをかけ（ステップS16）、効率的に除外処理を進めていく。ステップS16で行う二分岐探索については後述する。

[0053] （素子個別除外履歴値を用いた除外処理）

次に、図9を参照しながら、素子個別除外履歴値を用いた除外処理について説明する。

図9に示すように、検証処理装置1の選択部101は、素子個別除外履歴値が所定の閾値を上回っている要素（X1、X2、・・・）の全てを選択する（ステップS21）。ここで、素子個別除外履歴値が所定の閾値を上回っている要素が一つもない場合は、この除外処理はスキップされる。

[0054] 次に、検証処理装置1の検査部100は、ステップS21で選択された全ての要素を検査対象モデルMODから除外し（ステップS22）、再度のモデル検査を実施する（ステップS23）。

再度のモデル検査の検査結果がTRUEにならなかった（再度、反例が出力された）場合（ステップS24；NO）、ステップS22で除外した要素は全て主要因ではなかったと判断できるので、検証処理装置1は、除外した要素を検査対象モデルMODに戻すことはせず、更なる絞り込みを続ける。

一方、再度のモデル検査にて検査結果がTRUEに転じた（反例が出力されなくなった）場合（ステップS24；YES）、ステップS22で除外した要素の中に主要因が含まれていたと判断できるので、検証処理装置1は、一旦、除外した要素を検査対象モデルMODに戻す（ステップS25）。この場合、検証処理装置1は、ステップS25で検査モデルMODに戻した要素を対象に、二分岐探索で更なる絞り込みをかけ（ステップS26）、効率的に除外処理を進めていく。

的に除外処理を進めていく。ステップS 2 6で行う二分岐探索については後述する。

[0055] 上述したステップS 1 6 (図8) およびステップS 2 6 (図9) の二分岐探索について、図10を参照しながら説明する。

ステップS 1 5又はステップS 2 5で検査対象モデルMODに戻された要素が、要素X 1～X 8の8個であったとする。このとき、検証処理装置1の選択部101は、これらの要素X 1～X 8を二つのグループG 1 1 (X 1、X 2、X 3、X 4)、G 1 2 (X 5、X 6、X 7、X 8)に分ける(ステップS 3 0)。

[0056] 選択部101は、グループG 1 1、G 1 2のいずれか一方(グループG 1 1)を選択する。検査部100は、選択されたグループG 1 1に含まれる全ての要素X 1～X 4を検査対象モデルMODから除外し、再度のモデル検査を行う。ここで、検査結果=TRUE(反例が出力されない)となったとする。この場合、選択部101は、要素X 1～X 4を、一旦、検査対象モデルMODに戻し、これらの要素X 1～X 4を更に二つのグループG 2 1 (X 1、X 2)、G 2 2 (X 3、X 4)に分ける(ステップS 3 1)。

[0057] 選択部101は、グループG 2 1、G 2 2のいずれか一方(グループG 2 1)を選択する。検査部100は、選択されたグループG 2 1に含まれる全ての要素X 1、X 2を検査対象モデルMODから除外し、再度のモデル検査を行う。ここで、検査結果=TRUE(反例が出力されない)となったとしても、グループG 2 1を構成する要素はX 1、X 2の2つのみなので、これ以上の絞り込みは行わない。検証処理装置1は、別のグループについての絞り込みを行う。

[0058] 選択部101は、グループG 2 1、G 2 2の他方側(グループG 2 2)を選択する。検査部100は、選択されたグループG 2 2に含まれる全ての要素X 3、X 4を検査対象モデルMODから除外し、再度のモデル検査を行う。ここで、検査結果=FALSE(反例が出力された)となったとする。この場合、要素X 3、X 4は、主要因ではないと判断できるので、検証処理装

置 1 は、検査対象モデルMODからの除外を確定する（ステップS 3 3）。

[0059] 続いて、選択部 1 0 1 は、グループG 1 1、G 1 2の他方側（グループG 1 2）を選択する。検査部 1 0 0 は、選択されたグループG 1 2に含まれる全ての要素X 5～X 8を検査対象モデルMODから除外し、再度のモデル検査を行う。ここで、検査結果=F A L S E（反例が出力された）となったとする。この場合、選択部 1 0 1 は、要素X 5～X 8は、主要因ではないと判断できるので、検証処理装置 1 は、検査対象モデルMODからの除外を確定する（ステップS 3 4）

[0060] 検証処理装置 1 は、以上のような二分岐探索により、効率的に主要因を絞り込むことができる。

[0061] 図 7～図 9 の処理フローが終了した後、検証処理装置 1 は、残った要素について一つずつ絞り込みを行い、結果解釈の処理を完了する。

[0062] （作用、効果）

以上の通り、第 1 の実施形態に係る検証処理装置 1 は、複数の要素ごとの除外頻度（除外履歴値）を示す除外履歴情報を生成する除外履歴生成部 1 0 2 を備える。この除外履歴生成部 1 0 2 は、再度のモデル検査の結果として再度の反例が出力された場合に、選択された要素の除外履歴値を増加させて除外履歴情報を更新する。そして、選択部 1 0 1 は、次の結果解釈の過程において、除外履歴生成部 1 0 2 が生成した除外履歴情報に基づき、除外履歴値が相対的に高い要素を選択する。

[0063] このようにすることで、過去の結果解釈で除外されやすい要素を優先的に選択し、検査対象モデルMODから除外することとなる。そうすると、検査結果=T R U Eとなったために、除外した要素を再び検査対象モデルMODに戻してやり直すという工程が発生する頻度を低減させることができる。

したがって、検査結果から結果解釈を得るために要する工程を大幅に低減することができる。

[0064] また、第 1 の実施形態に係る除外履歴生成部 1 0 2 は、一つの設計図面に含まれる要素ごとの除外履歴値に基づいて当該設計図面単位の除外頻度（図

面単位除外履歴値)を示す除外履歴情報を生成する。そして、選択部101は、当該除外履歴情報に基づき、図面単位除外履歴値が高い設計図面に含まれる記要素の全てを選択する。

[0065] このようにすることで、不安全事故の発生との関わりが少ない機能(設計図面)の単位で、一度の再検査で多数の要素を除外できる可能性が高くなる。したがって、結果解釈(主要因の絞り込み)に要する工程をより低減することができる。

例えば、空調機能(設計図面)の不具合は、不安全事故(ブレーキが作動しない、走行中にドアが開く等)の発生にかかわる要素を含まない場合が多い。このような場合、本実施形態によれば、空調機能の設計図面に含まれる複数の要素が一度に除外されることとなり、主要因の特定までに至る工程が短縮される。

[0066] また、第1の実施形態に係る除外履歴生成部102は、複数の要素それぞれの、検査式単位の除外頻度(検査式単位除外履歴値)を示す除外履歴情報を生成する。そして、選択部101は、当該除外履歴情報に基づき、次のモデル検査で用いる検査式に対応する検査式単位除外履歴値が高い要素を選択する。

[0067] このようにすることで、同一検査式内での結果解釈数が増えた場合に、検査中の検査式に関わりが少ない多数の要素を一度に除外できる可能性が高くなる。したがって、結果解釈に要する工程をより低減することができる。

[0068] また、第1の実施形態に係る選択部101は、再度のモデル検査の結果として反例が出力されなくなった場合に、前回選択した複数の要素を二つのグループに分けたうちの一方を選択する。

このようにすることで、二分岐探索を用いて主要因を効率的に絞り込むことができる。

[0069] 以上の通り、第1の実施形態に係る検証処理装置1によれば、モデル検査の反例解釈の作業に要する負担を軽減できる。

[0070] <第2の実施形態>

次に、第2の実施形態に係る検証処理装置1について、図11及び図12を参照しながら説明する。

[0071] (最適閾値の決定処理)

図11は、第2の実施形態に係る検証処理装置のCPUの機能構成を示す図である。

図11に示すように、第2の実施形態に係る検証処理装置1は、CPU10の機能として、新たに閾値決定部103を有することを特徴とする。

ここで、第1の実施形態に係る検証処理装置1において、図7のステップS01、図8のステップS11、及び、図9のステップS12に用いる閾値は固定値であった。しかし、第2の実施形態に係る検証処理装置1は、閾値決定部103の機能により、最適な閾値が決定される。

[0072] 閾値決定部103は、除外頻度（除外履歴値）に基づいて各要素を検査対象モデルMODから除外するか否かの判定に用いる閾値を決定する。特に、閾値決定部103は、過去の解釈結果より主要因ではないと判断された要素の除外履歴値と、主要因であると判断された要素除外履歴値とに基づいて最適な閾値を決定する。以下、閾値決定部103の処理について図12を参照しながら詳しく説明する。

[0073] (閾値決定部の処理)

図12は、第2の実施形態に係る閾値決定部の処理の内容を示す図である。

まず、閾値決定部103は、複数の閾値候補T1（例えば、“0.7”、“0.8”、“0.9”）を有している。閾値決定部103は、過去のモデル検査における解釈結果より、これら複数の閾値候補T1（0.7、0.8、0.9）の中から最適な閾値を決定する。

[0074] 例えば、図12右側の表のように、あるモデル検査による解釈結果がY1 & X1 & X3となり、その結果、除外履歴生成部102によって更新された各要素X1～X4の除外履歴値がそれぞれX1=0.7、X2=0.9、X3=0.5、X4=0.8であったとする。この場合、反例からこの解釈結

果（Y 1 & X 1 & X 3）を得る工程では、選択部 1 0 1 によって主要因ではない要素 X 2、X 4 のみが一度に選択されることが最も望ましかったといえる。

[0075] そこで、閾値決定部 1 0 3 は、要素 X 2、X 4 のみが選択され得るような閾値を決定する。具体的には、図 1 2 左側の表のように、複数の閾値候補 T 1 の各値について点数付けを行う。点数付けのルールは、以下の（A）～（D）のとおりである。

（A）閾値判定の結果、除外されてほしい要素（主要因ではない要素）が除外される場合：+ 1 点

（B）閾値判定の結果、除外されてほしい要素が除外されない場合：0 点

（C）閾値判定の結果、除外されてはいけない要素（主要因となる要素）が除外される場合：- 1 点

（D）閾値判定の結果、除外されてはいけない要素が除外されない場合：0 点

[0076] 閾値決定部 1 0 3 は、複数の要素 X 1 ～X 4 のそれぞれについて（A）～（D）のルールより得られる点数の総計が最も高い閾値候補を、次の結果解釈の際に採用する閾値に決定する。

（A）～（D）のルールに基づいて、図 1 2 に示す例では“0. 8”の閾値候補が最も高得点となる。したがって、閾値決定部 1 0 3 は、閾値を“0. 8”に決定する。

[0077] （作用、効果）

以上の通り、第 2 の実施形態に係る検証処理装置 1 によれば、結果解釈が行われる度に、その結果から、主要因ではない要素のみが適切に選択されるような閾値に決定される。これにより、主容易ではない要素のみが検査対象モデル MOD から除外されやすくなるので、結果解釈に要する工程を一層軽減することができる。

[0078] 上述の実施形態においては、検証処理装置 1 の各種処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、この

プログラムをコンピュータが読み出して実行することによって上記各種処理が行われる。また、コンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、CD-ROM、DVD-ROM、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータが当該プログラムを実行するようにしてもよい。

[0079] 上記プログラムは、上述した機能の一部を実現するためのものであってもよい。更に、上述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

[0080] 以上のとおり、本開示に係るいくつかの実施形態を説明したが、これら全ての実施形態は、例として提示したものであり、発明の範囲を限定することを意図していない。これらの実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で種々の省略、置き換え、変更を行うことができる。これらの実施形態及びその変形は、発明の範囲や要旨に含まれると同様に、特許請求の範囲に記載された発明とその均等の範囲に含まれる。

[0081] <付記>

各実施形態に記載の検証装置、検証処理方法およびプログラムは、例えば以下のように把握される。

[0082] (1) 第1の態様に係る検証処理装置1は、複数の要素(X1、X2、・・・)を含む検査対象モデルMODに対してモデル検査を実施する検査部100と、前記モデル検査の結果として出力された反例に含まれる複数の要素のうちの一つ以上を選択する選択部101と、複数の要素ごとの除外頻度(除外履歴値)を示す除外履歴情報を生成する除外履歴生成部102と、を備える。検査部100は、更に、前記選択された要素を除外してなる検査対象モデルMODに対して再度のモデル検査を実施し、除外履歴生成部102は、前記再度のモデル検査の結果として再度の反例が出力された場合に、前記選択

された要素の前記除外頻度を増加させて前記除外履歴情報を更新し、選択部 101 は、前記除外履歴情報に基づき、前記除外頻度が高い要素を選択する。

[0083] (2) 第2の態様に係る検証処理装置1において、除外履歴生成部102は、一つの設計図面に含まれる前記要素ごとの除外頻度に基づいて当該設計図面単位の除外頻度を示す除外履歴情報を生成する。選択部101は、当該除外履歴情報に基づき、前記設計図面単位の除外頻度が高い設計図面に含まれる前記要素の全てを選択する。

[0084] (3) 第3の態様に係る検証処理装置1において、除外履歴生成部102は、前記複数の要素それぞれの、検査式単位の除外頻度を示す除外履歴情報を生成する。選択部101は、当該除外履歴情報に基づき、次の前記モデル検査で用いる検査式に対応する前記検査式単位の除外頻度が高い要素を選択する。

[0085] (4) 第4の態様に係る検証処理装置1において、選択部101は、前記再度のモデル検査の結果として反例が出力されなくなった場合に、前回選択した複数の要素を二つのグループに分けたうちの一方を選択する。

[0086] (5) 第5の態様に係る検証処理装置1において、前記除外頻度との対比により各要素を前記検査対象モデルから除外するか否かの判定に用いる閾値を決定する閾値決定部103をさらに備える。

[0087] (6) 第6の態様に係る検証処理方法は、複数の要素を含む検査対象モデルに対してモデル検査を実施するステップと、前記モデル検査の結果として出力された反例に含まれる複数の要素のうちの一つ以上を選択するステップと、複数の要素ごとの除外頻度を示す除外履歴情報を生成するステップと、前記選択された要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、前記再度のモデル検査の結果として再度の反例が出力された場合に、前記選択された要素の前記除外頻度を増加させて前記除外履歴情報を更新するステップと、を有し、前記選択するステップでは、前記除外履歴情報に基づき、前記除外頻度が高い要素を選択する。

[0088] (7) 第7の態様に係るプログラムは、コンピュータに、複数の要素を含む検査対象モデルに対してモデル検査を実施するステップと、前記モデル検査の結果として出力された反例に含まれる複数の要素のうちの一つ以上を選択するステップと、複数の要素ごとの除外頻度を示す除外履歴情報を生成するステップと、前記選択された要素を除外してなる検査対象モデルに対して再度のモデル検査を実施するステップと、前記再度のモデル検査の結果として再度の反例が出力された場合に、前記選択された要素の前記除外頻度を増加させて前記除外履歴情報を更新するステップと、を実行させ、前記選択するステップでは、前記除外履歴情報に基づき、前記除外頻度が高い要素を選択する。

産業上の利用可能性

[0089] 上述の情報処理装置、情報処理方法およびプログラムによれば、マハラノビス距離に係る処理をより適切に行うことができる。

符号の説明

[0090] 1 検証処理装置
10 CPU
100 検査部
101 選択部
102 除外履歴生成部
103 閾値決定部
11 メモリ
12 ディスプレイ
13 入力デバイス
14 ストレージ
MOD 検査対象モデル