(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2019-20966
(P2019-20966A)
(43)公開日　平成31年2月7日(2019.2.7)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 17/17	(2006.01)	G06F	17/17	5B056

審査請求 未請求　請求項の数 5　ＯＬ　（全 15 頁）

(21)出願番号　特願2017-137949 (P2017-137949)
(22)出願日　平成29年7月14日 (2017.7.14)

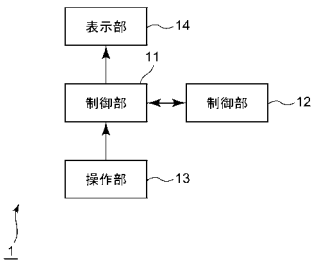
（出願人による申告）平成２７年度、国立研究開発法人科学技術振興機構、戦略的創造研究推進事業「函数論に基づく間接計測の数理基盤構築」委託研究、産業技術力強化法第１９条の適用を受ける特許出願／平成２８年度、国立研究開発法人科学技術振興機構、戦略的創造研究推進事業「蓮尾メタ数理システムデザイン」協働研究、産業技術力強化法第１９条の適用を受ける特許出願／平成２７年度、国立研究開発法人科学技術振興機構、戦略的創造研究推進事業「社会的課題の解決に向けた数学と諸分野の協働」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(71)出願人　504137912
国立大学法人　東京大学
東京都文京区本郷七丁目３番１号
(71)出願人　504132272
国立大学法人京都大学
京都府京都市左京区吉田本町３６番地１
(74)代理人　100122275
弁理士　竹居　信利
(72)発明者　蓮尾　一郎
東京都文京区本郷七丁目３番１号　国立大学法人東京大学内
(72)発明者　奥殿　貴仁
東京都文京区本郷七丁目３番１号　国立大学法人東京大学内

最終頁に続く

(54)【発明の名称】自動証明装置、及びプログラム

(57)【要約】
【課題】得られた補間に対応する現実の証明対象の解釈を容易化できる自動証明装置及びプログラムを提供する。
【解決手段】与えられた証明対象に係るクレイグ補間を表す多項式を生成して出力するソルバーからの入力を受け入れる、当該項式に含まれる係数の比を、整数の比であり、各係数に対応する値がより小さい値となるよう近似した近似係数を求め、当該求められた近似係数のうちから、予め定めた方法で決定された順に、近似係数を選択して、受け入れた多項式の係数を当該選択した近似係数に置き換えた試行多項式を生成し、当該試行多項式が、前記クレイグ補間を表す多項式として成立するかを検証する自動証明装置である。
【選択図】図１



【特許請求の範囲】
【請求項１】
与えられた証明対象に係るクレイグ補間を表す多項式を生成して出力するソルバーからの入力を受け入れる手段と、
前記受け入れた多項式に含まれる係数の比が、整数の比となり、かつ各係数に対応する値がより小さい値となるよう近似した近似係数を、複数求める係数演算手段と、
前記複数求められた近似係数のうちから、予め定めた方法で決定された順に近似係数を選択し、前記受け入れた多項式の係数を当該選択した近似係数に置き換えた試行多項式を生成し、当該試行多項式が、前記クレイグ補間を表す多項式として成立するかを検証する検証手段と、
前記検証により、前記求めたいずれかの近似係数に基づく前記試行多項式が、前記クレイグ補間を表す多項式として成立すると、前記検証手段により判断されたときに、当該近似係数を、解として生成する生成手段と、
を含み、
前記生成手段は、前記求めたいずれかの近似係数に基づく前記試行多項式が、いずれも前記クレイグ補間を表す多項式として成立しないとして前記検証手段により判断されたときには、エラーが発生したものとして所定の処理を実行する、
自動証明装置。
【請求項２】
請求項１記載の自動証明装置であって、
前記ソルバーは、前記証明対象に係る制約が、
任意の変数値に対して
０以上である多項式ｆ、
０より大である多項式ｇ、
０に等しい多項式ｈ
のいずれかを少なくとも一つ含んで設定され、
一対の制約Ｔ，Ｔ′のクレイグ補間を表す多項式を生成して出力するソルバーである自動証明装置。
【請求項３】
請求項１または２に記載の自動証明装置であって、
前記出力される解が、プログラム検証または定理証明の処理に供される自動証明装置。
【請求項４】
請求項１に記載の自動証明装置であって、
前記ソルバーは、前記証明対象に係る制約が、
任意の変数値に対して
０以上である多項式ｆ、
０に等しくない多項式ｇ、
０に等しい多項式ｈ
のいずれかを少なくとも一つ含んで設定され、
一対の制約Ｔ，Ｔ′のクレイグ補間を表す多項式を生成して出力するソルバーである自動証明装置。
【請求項５】
コンピュータを、
与えられた証明対象に係るクレイグ補間を表す多項式を生成して出力するソルバーからの入力を受け入れる手段と、
前記受け入れた多項式に含まれる係数の比が、整数の比となり、かつ各係数に対応する値がより小さい値となるよう近似した近似係数を、複数求める係数演算手段と、
前記複数求められた近似係数のうちから、予め定めた方法で決定された順に近似係数を選択し、前記受け入れた多項式の係数を当該選択した近似係数に置き換えた試行多項式を生成し、当該試行多項式が、前記クレイグ補間を表す多項式として成立するかを検証する

検証手段と、
前記検証により、前記求めたいずれかの近似係数に基づく前記試行多項式が、前記クレイグ補間を表す多項式として成立すると、前記検証手段により判断されたときに、当該近似係数を解として生成し、前記求めたいずれかの近似係数に基づく前記試行多項式が、いずれも前記クレイグ補間を表す多項式として成立しないとして前記検証手段により判断されたときには、エラーが発生したものとして所定の処理を実行する生成手段と、
として機能させるプログラム。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、自動証明装置、及びプログラムに関する。
【背景技術】
【０００２】
近年、大規模集積回路（ＬＳＩ）等の、ハードウェアの設計や検証、ソフトウェアプログラムの検証等において、人為的介入なしに自動で推論を行う自動証明装置の利用が検討されている。例えば、非特許文献２には、ハードウェア設計を、クレイグ補間を用いた方法で検証を行うことで、検証可能な対象を広げることができることが開示されている。
【０００３】
こうした研究を受けて、与えられた証明対象に係るクレイグ補間を表す多項式を生成して出力するソルバーが開発されている（例えば非特許文献１）。このようなソルバーにおいては、多項式の係数が、数値解析により得られているので、一般に簡潔な整数比としては表現されない。また、当該係数には数値誤差を含む。
【先行技術文献】
【非特許文献】
【０００４】
【非特許文献１】Dai, L., et. al., Generating non-linear interpolants by semidefinite programming. In: Sharygina, N., Veith H.(eds.) Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings. Lecture Notes in Computer Science, vol. 8044, pp.364-380, Springer(2013) (http://dx.doi.org/10.1007/978-3-642-39799-8_25)
【非特許文献２】McMillan, K. L., Interpolation and SAT-Based Model Checking, in Proc. of 15th Conf. on Computer Aided Verification (CAV 2003), LNCS, Vol.2725, pp. 1-13, Springer (2003)
【発明の概要】
【発明が解決しようとする課題】
【０００５】
このように従来の技術では、多項式の係数が、一般に簡潔な整数比としては表現されないうえ、数値誤差を含むため、得られた補間に対応する現実のハードウェア設計やプログラムの動作等の証明対象がどのようなものであるか、例えばプログラムの動作検証であれば、どのようなプログラムの動作状態を表すものであるかを解釈することが容易でなく、また、動作検証等の自動化処理の際に障害となり得るという問題点があった。
【０００６】
本発明は上記実情に鑑みて為されたもので、得られた補間に対応する現実の証明対象の解釈を容易化できる自動証明装置及びプログラムを提供することを、その目的の一つとする。
【課題を解決するための手段】
【０００７】
上記従来例の問題点を解決するための本発明は、自動証明装置であって、与えられた証

明対象に係るクレイグ補間を表す多項式を生成して出力するソルバーからの入力を受け入れる手段と、前記受け入れた多項式に含まれる係数の比が、整数の比となり、かつ各係数に対応する値がより小さい値となるよう近似した近似係数を、複数求める係数演算手段と、前記複数求められた近似係数のうちから、予め定めた方法で決定された順に近似係数を選択し、前記受け入れた多項式の係数を当該選択した近似係数に置き換えた試行多項式を生成し、当該試行多項式が、前記クレイグ補間を表す多項式として成立するかを検証する検証手段と、前記検証により、前記求めたいずれかの近似係数に基づく前記試行多項式が、前記クレイグ補間を表す多項式として成立すると、前記検証手段により判断されたときに、当該近似係数を、解として生成する生成手段と、を含み、前記生成手段は、前記求めたいずれかの近似係数に基づく前記試行多項式が、いずれも前記クレイグ補間を表す多項式として成立しないとして前記検証手段により判断されたときには、エラーが発生したものとして所定の処理を実行することとしたものである。

【発明の効果】

【０００８】

本発明によると、得られた補間に対応する現実の証明対象の解釈を容易化できる。

【図面の簡単な説明】

【０００９】

【図１】本発明の実施の形態の一例に係る自動証明装置の構成ブロック図である。

【図２】本発明の実施の形態の一例に係る自動証明装置の機能ブロック図である。

【図３】本発明の実施の形態の一例に係る自動証明装置のソルバー部の動作例を表すフローチャート図である。

【図４】本発明の実施の形態の一例に係る自動証明装置の処理例を表すフローチャート図である。

【図５】本発明の実施の形態の一例に係る自動証明装置が処理する制約の設定例を表す説明図である。

【発明を実施するための形態】

【００１０】

本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係る自動証明装置１は、図１に例示するように、制御部１１と、記憶部１２と、操作部１３と、表示部１４とを含んで構成されている。

【００１１】

ここで制御部１１はＣＰＵ等のプログラム制御デバイスであり、記憶部１２に格納されたプログラムに従って動作する。本実施の形態の一例では、この制御部１１は、与えられた証明対象に係るクレイグ補間を表す多項式を生成して出力するソルバーからの入力を受け入れ、当該受け入れた多項式に含まれる係数の比が、整数の比となり、かつ、各係数に対応する値がより小さい値となるように、各係数の値を近似した近似係数の組を、複数求める。

【００１２】

なお、ここで補間は、論理式における補間をいい、
ＸかつＹが充足不能な式であるときに、
ＸならばＺが恒真式であり、
ＺかつＹが充足不能な式であり、かつ、
Ｚに現れる変数がＸ，Ｙの双方に現れる、という場合のＺが「ＸならばＹ」のクレイグ補間と呼ばれるものである。

【００１３】

またこの制御部１１は、当該複数求められた近似係数の組のうちから、予め定めた方法で決定された順に近似係数の組を選択する。一例として、当該近似係数の絶対値の和が小さいものから順に選択することとすればよい（１ノルムが最小のものからの順）。また別の例では、各係数の二乗和が最小のものから順（２ノルムが最小のものからの順）、あるいは、係数の絶対値の最大値が最小のものから順（無限大ノルムが最小のものからの順）

に選択することとしてもよい。

【００１４】

制御部１１は、受け入れた多項式の係数のそれぞれを、当該選択した近似係数の組に含まれる対応する値に置き換えた試行多項式を生成し、当該試行多項式が、クレイグ補間を表す多項式として成立するかを検証する。制御部１１は、この検証の処理により、求めたいずれかの近似係数に基づく試行多項式が、クレイグ補間を表す多項式として成立していると判断すると、当該近似係数を、解として所定の処理に供する。

【００１５】

また制御部１１は、上記求めたいずれかの近似係数に基づく試行多項式のいずれもがクレイグ補間を表す多項式として成立しないと判断したときには、エラーが発生したものとして所定の処理を実行する。この制御部１１の詳しい動作については後に述べる。

【００１６】

記憶部１２は、メモリデバイス等であり、制御部１１によって実行されるプログラムを保持する。このプログラムは、コンピュータ可読かつ、非一時的な記憶媒体に格納されて提供され、この記憶部１２に複写されたものであってもよい。本実施の形態において、この記憶部１２は、また、制御部１１のワークメモリとしても動作する。

【００１７】

操作部１３は、キーボードやマウス等であり、ユーザの指示入力を受け入れて、当該指示入力の内容を制御部１１に出力する。表示部１４は、ディスプレイ等であり、制御部１１から入力される指示に従い、情報を表示出力する。

【００１８】

ここで制御部１１の動作について説明する。本実施の形態では、この制御部１１は、記憶部１２に格納されたプログラムを実行することにより、機能的に、図２に例示するように、ソルバー出力受入部２１と、係数演算部２２と、検証処理部２３と、解生成部２４と、出力部２５とを含んで構成される。また本実施の形態では、図２に示すように、この制御部１１が、与えられた証明対象に係るクレイグ補間を表す多項式を生成して出力するソルバーとしても動作し、ソルバー部３１をさらに含んでもよい。もっとも、このソルバー部３１は、他のコンピュータによって実現されてもよく、その場合は、後に説明するソルバー出力受入部２１は、当該ソルバーとして機能する他のコンピュータから、ソルバーの出力を受け入れることとなる。

【００１９】

本実施の形態の一例に係るソルバー部３１は、証明対象として与えられた一対の制約Ｔ，Ｔ′のクレイグ補間を生成する問題を、半正定値計画問題へ変換する。

【００２０】

すなわち、ソルバー部３１は、証明対象に係る制約Ｔ，Ｔ′のそれぞれを、任意の変数値に対して

０以上である少なくとも一つの多項式ｆ、

０より大である少なくとも一つの多項式ｇ、

０に等しい少なくとも一つの多項式ｈ

のいずれかを少なくとも一つ含む表現

【数１】

$$T=\left(\begin{array}{l} f_1(\boldsymbol{X},\boldsymbol{Y})\geq 0,\cdots,f_s(\boldsymbol{X},\boldsymbol{Y})\geq 0,\\ g_1(\boldsymbol{X},\boldsymbol{Y})>0,\cdots,g_t(\boldsymbol{X},\boldsymbol{Y})>0,\\ h_1(\boldsymbol{X},\boldsymbol{Y})=0,\cdots,h_u(\boldsymbol{X},\boldsymbol{Y})=0 \end{array}\right),$$

$$T'=\left(\begin{array}{l} f'_1(\boldsymbol{X},\boldsymbol{Y})\geq 0,\cdots,f'_{s'}(\boldsymbol{X},\boldsymbol{Y})\geq 0,\\ g'_1(\boldsymbol{X},\boldsymbol{Y})>0,\cdots,g'_{t'}(\boldsymbol{X},\boldsymbol{Y})>0,\\ h'_1(\boldsymbol{X},\boldsymbol{Y})=0,\cdots,h'_{u'}(\boldsymbol{X},\boldsymbol{Y})=0 \end{array}\right), \qquad (1)$$

に変換する。

【００２１】

なお、個々の多項式ｆ$_1$，ｆ$_2$，…ｆ$_s$，ｇ$_1$，ｇ$_2$…，ｇ$_t$，ｈ$_1$，ｈ$_2$…ｈ$_u$，ｆ'$_1$，ｆ'$_2$…，ｆ'$_{s'}$，ｇ'$_1$，ｇ'$_2$…，ｇ'$_{t'}$，ｈ'$_1$，ｈ'$_2$…ｈ'$_{u'}$は予め、制約Ｔ，Ｔ'に共通に現れる変数Ｘの多項式として任意に定めておく。

【００２２】

このように、証明対象に係る制約Ｔ，Ｔ'のそれぞれを、任意の変数値に対して
０以上である少なくとも一つの多項式ｆ、
０より大である少なくとも一つの多項式ｇ、
０に等しい少なくとも一つの多項式ｈ
のいずれかを少なくとも一つ含む表現で表しておき、ソルバーにて数値解を演算することで、非特許文献１に開示された技術のように、証明対象に係る制約を、０に等しくない多項式を含む多項式の集合で記述する場合に比べ、補間を得やすくなる。

【００２３】

具体的にこのソルバー部３１は、図３に例示するように、不等式を用いた半代数系（ＳＡＳ$_<$：Semialgebraic System with inequalities）にて表現された制約Ｔ，Ｔ'及び、最大次数（degree）を表す自然数ｂを受け入れる（Ｓ１）。

【００２４】

そしてソルバー部３１は、次の数式を満足する、ベクトルα，α'，β，β'，γの数値解を見いだす（Ｓ２）。すなわち、

【数２】

$$\boldsymbol{2}=\{0,1\}$$

とし、ｉ，ｊをそれぞれ

【数３】

$$i\in\boldsymbol{2}^s,j\in\boldsymbol{2}^t,i'\in\boldsymbol{2}^{s'},j'\in\boldsymbol{2}^{t'}$$

（すなわち、ｉをｓビットの２進数値、ｊをｔビットの２進数値…など）として、ベクトルα，α'，β，β'，γが

【数４】

$\alpha_{ij} \in C(0)_{\leq b}$ 及び、

$\alpha'_{i'j'} \in C(0)_{\leq b}$ がＳＯＳである。

$\beta_j (j \in [1,u])$ は、次数ｂ以下の実数係数の多項式、かつ、

$\beta'_{j'} (j' \in [1,u'])$ が、次数ｂ以下の実数係数の多項式、

$\gamma_k (k \in \sigma(b))$ は、非負の実数値

との条件を満足するものとする。

【００２５】

またここで、ベクトルα，α′，β，β′，γ間には、次の制約が規定されているものとする。

【数５】

$$\begin{aligned} & \sum_{i\in\mathbf{2}^s, j\in\mathbf{2}^t} \alpha_{ij} f_1^{i1} \cdots f_s^{is} g_1^{j1} \cdots g_t^{jt} \\ + & \sum_{i'\in\mathbf{2}^{s'}, j'\in\mathbf{2}^{t'}} \alpha_{i'j'} f_1^{'i'1} \cdots f_{s'}^{'i's} g_1^{'j'1} \cdots g_{t'}^{'j't} \\ + & \sum_{k\in\sigma(b)} \gamma_k g_1^{k1} \cdots g_t^{kt} + \sum_{j=1}^{u} \beta_j h_j + \sum_{j'=1}^{u'} \beta'_{j'} h'_{j'} \end{aligned} \qquad (2)$$

$$\sum_{k\in\sigma(b)} \gamma_k \geq 1 \qquad (3)$$

【００２６】

このベクトルα，α′，β，β′，γを得る処理は、記号的解法（例えば量化子除去（quantifier elimination）など）を用いてもよいが、ここでは半正定値計画問題として緩和でき、この場合は広く知られた半正定値計画問題ソルバーを用いることができる。

【００２７】

ここでＣ（０）$_{\leq b}$は、次数ｂ以下のＳＯＳ（Sum of Squares：複数の多項式p_1，$p_2 \cdots p_N$の二乗和、つまり$p_1^2 + p_2^2 + \cdots + p_N^2$）を意味する。また、σ（ｂ）は総和がｂ＋１以下であるような、ｔ個の自然数の組N^tの集合｛（k_1，k_2，…k_t）$\in N^t \mid k_1 + k_2 + \cdots + k_t \leqq b+1$｝を意味する。

【００２８】

ソルバー部３１は、解（数値解）であるベクトルα，α′，β，β′，γが求められたか否かを調べ（Ｓ３）、解が見いだせない場合（Ｓ３：Ｎｏ）は、ソルバー部３１はエラーとして処理を停止する（Ｓ４）。この場合は、後に説明するソルバー出力受入部２１は、何らの入力を受け入れないこととなる。

【００２９】

また処理Ｓ３において解が見いだせたとき（Ｓ３：Ｙｅｓ）は、ソルバー部３１は、

【数６】

$$f := \Sigma \alpha_{ij} f_1^{i1} \cdots f_s^{is} g_1^{j1} \cdots g_t^{jt}$$
$$g := \Sigma \gamma_k g_1^{k1} \cdots g_t^{kt}$$
$$h := \Sigma \beta_j h_j$$

として、多項式ｆ，ｇ，ｈを定める（Ｓ５）。

【００３０】

そして不等式

【数７】

$$S := (f + g + h > 0)$$

を解として出力する。

【００３１】

またソルバー出力受入部２１は、ソルバー部３１など、ソルバーが出力する解の入力を受け入れる。

【００３２】

係数演算部２２は、ソルバー出力受入部２１が受け入れた解に含まれる変数Ｘの係数の整数比を少なくとも一つ（好適には複数）求める。本実施の形態の一例では、この係数演算部２２は、連分数展開の方法を用いて、この整数比を得る。すなわち係数演算部２２は、ソルバー出力受入部２１が受け入れた解に含まれる変数Ｘのすべての係数が自然数となるよう、受け入れた解を10^n倍する。ここでのｎは、すべての係数が自然数となる最小の正の整数とする。

【００３３】

係数演算部２２は、こうして得られた各係数x_1，$x_2 \cdots x_n$（いずれも自然数であって、少なくとも１つは０でない）について、次の処理（連分数展開（ＣＦＥ）処理と呼ぶ）を実行する。

【００３４】

図４に示すように、まず、係数演算部２２は、深さｄ（ｄは正の整数）の指定を受け入れる（Ｓ１１）。なお、深さｄが指定されていないときはｄ＝１とする。また係数演算部２２は、係数x_1，$x_2 \cdots x_n$のうち最小の係数をx_pとして、係数x_1，$x_2 \cdots x_n$のそれぞれを、このx_pで除した数を超えない最大の整数の組

【数８】

$$a := (\lfloor x_1/x_p \rfloor, \cdots, \lfloor x_n/x_p \rfloor)$$

を求める（Ｓ１２）。

【００３５】

係数演算部２２は、ｄが「１」であるか否かを調べ（Ｓ１３）、ｄが「１」ならば（Ｓ１３：Ｙｅｓ）、上記組ａの最大公約数を求めて、ａの各成分の値をこの最大公約数ｇｃｄ（ａ）で除した値の組を求める（Ｓ１４）：

【数９】

$$y := a / gcd(a)$$

【００３６】

係数演算部２２は、ここで求めたｙ（各成分の値の比が、求める整数比となる）を返り値として記憶部１２に格納して（Ｓ１５）、リターンする（再帰的に呼び出されている場

合は呼び出し元の処理に戻り、最初に呼び出されていた場合は処理を終了する）。
【００３７】
　また、処理Ｓ１３でｄが「１」でなければ、係数を
$x_1 - a_1 x_p$，…，x_{p-1}，$a_{p-1} x_p$，x_p，$x_{p+1} - a_{p+1} x_{p+1}$，…，$x_n - a_n x_p$
とし、深さｄを（ｄ－１）として（Ｓ１６）、ＣＦＥ処理を再帰的に（処理Ｓ１１から）実行し、その返り値をｒ′とする（Ｓ１７）。
【００３８】
　また係数演算部２２は、
【数１０】

$$y := \left(a_1 r'_p + r'_1, \cdots a_{p-1} r'_p + r'_{p-1}, r'_p, a_{p+1} r'_p + r'_{p+1}, \cdots, a_n r'_p + r'_n\right) \qquad (4)$$

にてｙを求め（Ｓ１８）、ｙの各成分を、これらの最大公約数ｇｃｄ（ｙ）で除した結果を返り値として記憶部１２に格納し（Ｓ１９）、リターンする。
【００３９】
　なお、ここまでの例によって得られる近似係数は、各係数に対応する値が整数となるが、当該整数として求められた近似係数を、さらに共通の整数ｄで除した有理数としてもよい。すなわち、近似係数は整数であることに限られない。
【００４０】
　検証処理部２３は、ソルバー出力受入部２１が受け入れた解である多項式の係数を、係数演算部２２が記憶部１２に格納した各整数比の各値を係数（近似係数）で置き換えた試行多項式を生成する。そして検証処理部２３は、生成した試行多項式のうち、クレイグ補間を表す多項式として成立するか否かを検証する。この検証では、Ｔ′に対応する多項式の値域と、試行多項式を、ソルバー出力受入部２１が受け入れた解の多項式で置き換えたときの値域とを比較し、重なり合わない場合に、クレイグ補間を表す多項式として成立していると判断することとなる。
【００４１】
　検証処理部２３は、クレイグ補間を表す多項式として成立している試行多項式であって、係数となっている整数が最も小さいもの（いずれかの変数に着目し、当該変数の係数が最小であるもの、あるいはすべての係数の和が最小である試行多項式）を解生成部２４に出力する。
【００４２】
　なお、この検証処理部２３は、係数演算部２２が記憶部１２に格納した各整数比を用いて生成した試行多項式のいずれもがクレイグ補間を表す多項式として成立していないと判断すると、係数演算部２２が、現在の整数比を得るために利用した深さｄの値をインクリメント（「１」ないしそれ以上の整数値だけインクリメント）して、係数演算部２２に対して、当該インクリメントした後の深さｄを出力し、再度、整数比を生成させることとしてもよい。なお、インクリメント後のｄの値が予め定めたしきい値を超えたとき、またはインクリメントした後のｄの値によっても、ｄのインクリメント前に得られた整数比と同じ整数比が得られた場合（収束してしまった場合）には、エラーが発生したものとして予め定めた処理を実行する。
【００４３】
　一例として検証処理部２３は、上述のようにエラーが発生したと判断したときには、予め定めた処理としてソルバー出力受入部２１が受け入れた解をそのまま出力するよう、出力部２５に指示してもよい。
【００４４】
　解生成部２４は、ソルバー出力受入部２１が受け入れた解である多項式を、検証処理部２３が出力した試行多項式に置き換えて、出力対象となる解を生成する。
【００４５】

出力部２５は、解生成部２４が生成した出力対象となる解（または検証処理部２３から入力される指示によりソルバー出力受入部２１が受け入れた解そのもの）を、解として表示部１４に表示出力する。

【００４６】

なお、この出力部２５は、解を表示部１４に表示出力するほか、図示しないプリンタに出力して印刷させてもよいし、他のプログラムの入力となるようデータとして出力して、他のプログラムの処理に供してもよい。

【００４７】

［動作］

本発明の実施の形態は、以上の構成を備えており、次のように動作する。すなわち本実施の形態の一例では、証明対象に係る制約Ｔ，Ｔ′のそれぞれが、任意の変数値に対して
０以上である少なくとも一つの多項式ｆ、
０より大である少なくとも一つの多項式ｇ、
０に等しい少なくとも一つの多項式ｈ
のいずれかを少なくとも一つ含む表現

【数１】

$$T=\left(\begin{array}{l} f_1(\boldsymbol{X},\boldsymbol{Y})\geq 0,\cdots,f_s(\boldsymbol{X},\boldsymbol{Y})\geq 0,\\ g_1(\boldsymbol{X},\boldsymbol{Y})>0,\cdots,g_t(\boldsymbol{X},\boldsymbol{Y})>0,\\ h_1(\boldsymbol{X},\boldsymbol{Y})=0,\cdots,h_u(\boldsymbol{X},\boldsymbol{Y})=0 \end{array}\right),$$

$$T'=\left(\begin{array}{l} f'_1(\boldsymbol{X},\boldsymbol{Y})\geq 0,\cdots,f'_{s'}(\boldsymbol{X},\boldsymbol{Y})\geq 0,\\ g'_1(\boldsymbol{X},\boldsymbol{Y})>0,\cdots,g'_{t'}(\boldsymbol{X},\boldsymbol{Y})>0,\\ h'_1(\boldsymbol{X},\boldsymbol{Y})=0,\cdots,h'_{u'}(\boldsymbol{X},\boldsymbol{Y})=0 \end{array}\right), \qquad (1)$$

に変換されて、その数値解である多項式と、当該多項式が満足する不等式あるいは等式が解として得られる。

【００４８】

一例として、制約Ｔ，Ｔ′が、
Ｔ：＝（ｙ≧ｘ^{2}＋１）
Ｔ′：＝（ｙ≦－ｘ^{2}－１）
であるとする（図５を参照）と、これらの制約Ｔ，Ｔ′は同時には満足されない、つまり、Ｔ∧Ｔ′は矛盾しているから、これらＴ，Ｔ′に共通する変数のみを含む論理式εであって、Ｔならばε、かつε∧Ｔ′が矛盾するεが存在する（クレイグの補間定理）。そしてこのεがクレイグ補間となる。

【００４９】

ソルバーは、この制約Ｔ，Ｔ′からクレイグ補間εを数値解として得る。具体的に、数値解の一つは、
871.465ｙ＋348.560＞０
として得られる。

【００５０】

本実施の形態の自動証明装置１は、この係数871.465，348.560を連分数展開の方法によって丸め処理して近似係数を求める。ここでの例では、この丸め処理の結果として、
５，２
１１，４
…といった係数が整数の比となるような、近似係数の組が得られる。

【００５１】

自動証明装置１は、これらの得られた近似係数の組のうち、最小の近似係数（含まれる各係数の絶対値の総和が最小のもの、すなわち１ノルムが最小のもの）から順に、もとの

多項式における対応する係数に置き換えた試行多項式が、制約Ｔ，Ｔ′のクレイグ補間εとなっているか否かを調べる。

【００５２】

ここでは、自動証明装置１は、係数871.465を、対応する整数の値５に置き換え、係数348.560を、対応する整数の値２に置き換えた、試行多項式を用いた不等式

５ｙ＋２＞０

が制約Ｔ，Ｔ′

Ｔ：＝（ｙ≧ｘ^{2}＋１）

Ｔ′：＝（ｙ≦－ｘ^{2}－１）

に対するクレイグ補間εとなっているか否かを調べる。

【００５３】

ここでの例では、制約Ｔの表す値域ｙ≧ｘ^{2}＋１が、試行多項式を用いた不等式５ｙ＋２＞０の値域に含まれるので、

「制約Ｔであれば、εである」

が成立する。

【００５４】

また、試行多項式を用いた不等式５ｙ＋２＞０の値域は、制約Ｔ′の表す値域ｙ≦－ｘ^{2}－１と重なり合わないので、

「εと、制約Ｔ′とは矛盾する」

も成立する。

【００５５】

すなわち、この試行多項式を用いた不等式５ｙ＋２＞０は、上記制約Ｔ，Ｔ′のクレイグ補間となっていると判断できる。

【００５６】

自動証明装置１は、このように、各不等式（または等式）の値域を比較することで、試行多項式がクレイグ補間となっているか否かを調べて判断する。ここでの例では、上述のように、最初に調べた試行多項式を用いた不等式５ｙ＋２＞０が与えられた制約Ｔ，Ｔ′のクレイグ補間となっていると判断できるので、自動証明装置１は、この試行多項式を用いた不等式５ｙ＋２＞０を解として表示部１４に表示出力する。

【００５７】

この自動証明装置１によると、数値的に得られた解に比べ、簡略にされた不等式により解が示されるので、対応する現実の条件として解釈しやすい解が得られることとなる。

【００５８】

またこの自動証明装置１が出力した解を、プログラム検証または定理証明の処理システムに入力することで、プログラム検証または定理証明の処理に対して、本実施の形態の自動証明装置１の出力を供することができる。

【００５９】

［変形例（Daiの方法を採用する例）］

本実施の形態の以上の例では、ソルバー（ソルバー部３１等）が、証明対象に係る制約として、任意の変数値に対して

０以上である多項式ｆ、

０より大である多項式ｇ、

０に等しい多項式ｈ

のいずれかを少なくとも一つ含んで設定されるものとしたが、クレイグ補間を表す、多項式を用いた不等式あるいは等式が数値解として得られるのであれば、本実施の形態の自動証明装置１は、このソルバーを用いる例に限られず、他のソルバーを用いてもよい。

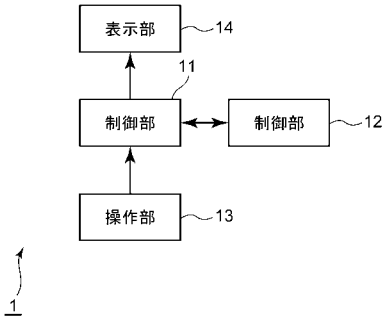
【００６０】

例えば本実施の形態において、数値解を求めるためのソルバーは、非特許文献１に示された方法を採用してもよい。この場合は、証明対象に係る制約が、任意の変数値に対して

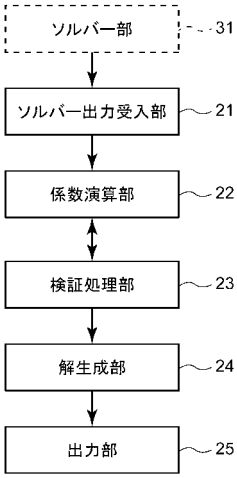
０以上である多項式ｆ、

０に等しくない多項式ｇ、
０に等しい多項式ｈ
のいずれかを少なくとも一つ含んで設定されることとなる。
【００６１】
［実施形態の効果］
本実施の形態によると、数値解析された多項式を、比較的簡潔な整数比の係数で表現しなおす。これにより数値解として得られた補間に対応する現実のプログラムの動作等の証明対象への対応付けを簡易にさせることができ、利用者にとっての理解が容易になるだけでなく、自動検証にも有用となる。
【００６２】
さらに、この処理に用いるソルバーとして、「０に等しくない」との制約の記述を、「０より大である」に置き換えたソルバーを用いることで、比較的多くの制約について補間を得ることができる。
【産業上の利用可能性】
【００６３】
本発明では、種々の証明問題に対して比較的簡潔なクレイグ補間の多項式表現を出力できるので、大規模集積回路（ＬＳＩ）等の、ハードウェアの設計や検証、ソフトウェアプログラムの検証等に、クレイグ補間を用いた方法を採用し、これを自動化する場合に有用である。
【符号の説明】
【００６４】
１　自動証明装置、１１　制御部、１２　記憶部、１３　操作部、１４　表示部、２１　ソルバー出力受入部、２２　係数演算部、２３　検証処理部、２４　解生成部、２５　出力部、３１　ソルバー部。

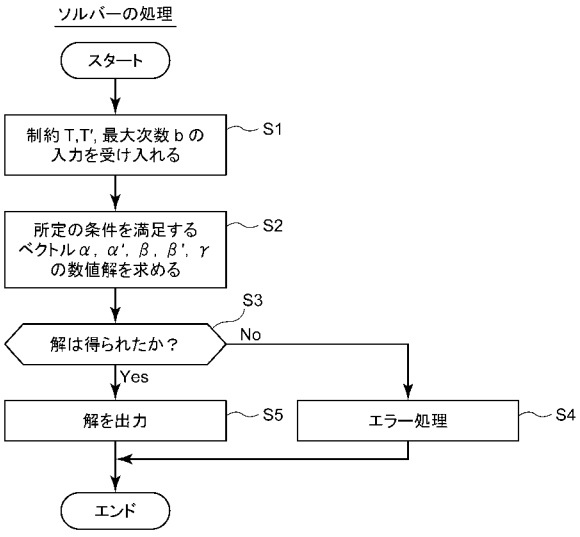
【図１】


表示部
14
11
制御部
制御部
12
操作部
13
1

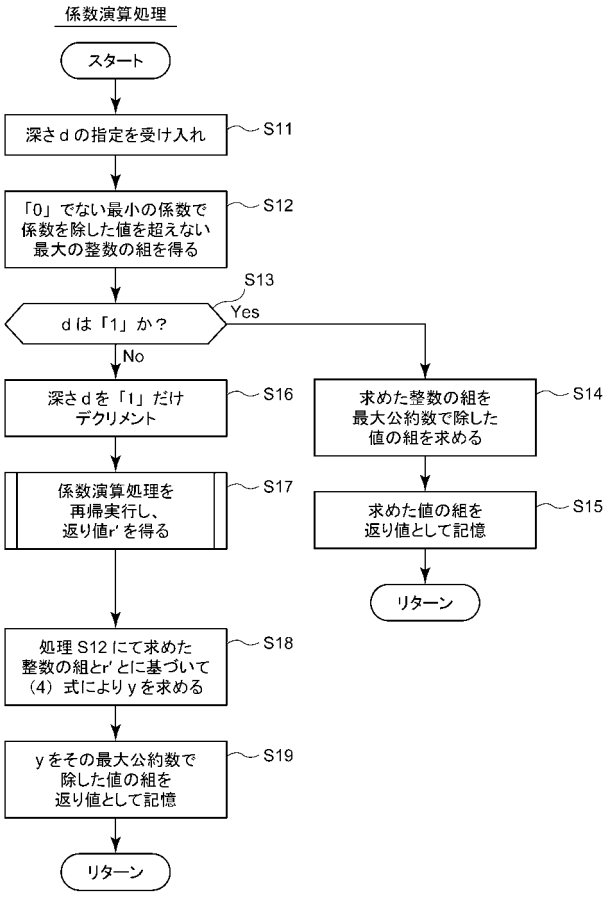
【図２】


ソルバー部
31
ソルバー出力受入部
21
係数演算部
22
検証処理部
23
解生成部
24
出力部
25

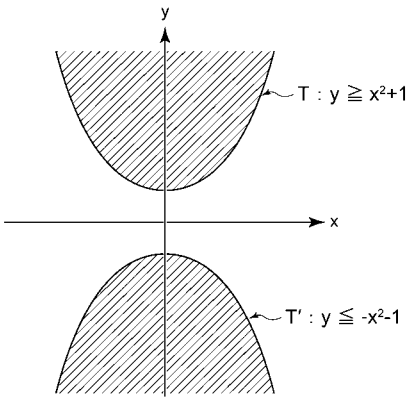
【図３】


ソルバーの処理
スタート
制約 T,T', 最大次数 b の
入力を受け入れる
S1
所定の条件を満足する
ベクトル α , α', β , β', γ
の数値解を求める
S2
S3
解は得られたか？
No
Yes
解を出力
S5
エラー処理
S4
エンド

【図４】


係数演算処理
スタート
深さ d の指定を受け入れ
S11
「0」でない最小の係数で
係数を除した値を超えない
最大の整数の組を得る
S12
S13
d は「1」か？
Yes
No
深さ d を「1」だけ
デクリメント
S16
係数演算処理を
再帰実行し、
返り値r' を得る
S17
処理 S12 にて求めた
整数の組とr' とに基づいて
(4) 式により y を求める
S18
y をその最大公約数で
除した値の組を
返り値として記憶
S19
リターン
求めた整数の組を
最大公約数で除した
値の組を求める
S14
求めた値の組を
返り値として記憶
S15
リターン

【図５】



フロントページの続き

(72)発明者　木戸　肩吾
東京都文京区本郷七丁目３番１号　国立大学法人東京大学内
(72)発明者　末永　幸平
京都府京都市左京区吉田本町３６番地１　国立大学法人京都大学内
(72)発明者　小島　健介
京都府京都市左京区吉田本町３６番地１　国立大学法人京都大学内
(72)発明者　西田　雄気
京都府京都市左京区吉田本町３６番地１　国立大学法人京都大学内

Ｆターム(参考) 5B056 BB52