

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7544274号
(P7544274)

(45)発行日 令和6年9月3日(2024.9.3)

(24)登録日 令和6年8月26日(2024.8.26)

(51)国際特許分類

F I

G 0 9 C 1/00 (2006.01) G 0 9 C 1/00 6 5 0

請求項の数 5 (全11頁)

(21)出願番号	特願2023-528779(P2023-528779)	(73)特許権者	000004226
(86)(22)出願日	令和3年6月14日(2021.6.14)		日本電信電話株式会社
(86)国際出願番号	PCT/JP2021/022586		東京都千代田区大手町一丁目5番1号
(87)国際公開番号	WO2022/264237	(74)代理人	110004381
(87)国際公開日	令和4年12月22日(2022.12.22)		弁理士法人 I T O H
審査請求日	令和5年12月7日(2023.12.7)	(74)代理人	100107766
			弁理士 伊東 忠重
		(74)代理人	100070150
			弁理士 伊東 忠彦
		(74)代理人	100124844
			弁理士 石原 隆治
		(72)発明者	濱田 浩気
			東京都千代田区大手町一丁目5番1号
			日本電信電話株式会社内
		審査官	行田 悦資

最終頁に続く

(54)【発明の名称】 累積計算装置、累積計算方法、及びプログラム

(57)【特許請求の範囲】

【請求項1】

グループに分けられた n 個の値の列 $v = (v_1, \dots, v_n)$ に関して、結合的な二項演算により前記グループごとの累積を計算する累積計算装置であって、

v の各要素 $v_1, \dots, v_n$ のうち、前記グループの先頭の要素には1、前記先頭以外の要素には0を対応させた値の列を $c = (c_1, \dots, c_n)$ として、 v を $v' = (v_1', \dots, v_n')$ (ただし、 $v_i' = (v_i, c_i)$) に変換する値変換部と、

前記二項演算を用いて、2つの対 (w, x) と (y, z) (ただし、 $x, z \in \{0, 1\}$) に対して新しい対 (p, q) を計算する新たな二項演算を作成する二項演算作成部と、
 $i = 1, \dots, n$ について、前記新たな二項演算により累積 s_i' (ただし、 s_i' は前記新たな二項演算による v_1' から v_i' までの累積) を計算する累積計算部と、

各 s_i' ($i = 1, \dots, n$) から前記グループごとの累積を示す値の列 $u = (u_1, \dots, u_n)$ を取り出し、取り出した u を出力する出力部と、
を有し、

前記新たな二項演算は、 $z = 0$ である場合は前記二項演算による w と y の演算結果を p 、 $z = 1$ である場合は y を p とし、 x と z の論理和を q とする、累積計算装置。

【請求項2】

前記二項演算作成部は、

前記二項演算による w と y の演算結果を r 、論理和を表す演算子を OR として、前記新たな二項演算による (w, x) と (y, z) の演算結果を $(zy + (1 - z)r, x OR$

z)と定義することで、前記新たな二項演算を作成する、請求項1に記載の累積計算装置。

【請求項3】

前記出力部は、

$s_i' = (u_i, d_i)$ として、 $u = (u_1, \dots, u_n)$ を取り出し、取り出した u を出力する、請求項1又は2に記載の累積計算装置。

【請求項4】

グループに分けられた n 個の値の列 $v = (v_1, \dots, v_n)$ に関して、結合的な二項演算により前記グループごとの累積を計算する累積計算装置が、

v の各要素 $v_1, \dots, v_n$ のうち、前記グループの先頭の要素には1、前記先頭以外の要素には0を対応させた値の列を $c = (c_1, \dots, c_n)$ として、 v を $v' = (v_1', \dots, v_n')$ (ただし、 $v_i' = (v_i, c_i)$)に変換する値変換手順と、

10

前記二項演算を用いて、2つの対 (w, x) と (y, z) (ただし、 $x, z \in \{0, 1\}$)に対して新しい対 (p, q) を計算する新たな二項演算を作成する二項演算作成手順と、

$i = 1, \dots, n$ について、前記新たな二項演算により累積 s_i' (ただし、 s_i' は前記新たな二項演算による v_1' から v_i' までの累積)を計算する累積計算手順と、

各 s_i' ($i = 1, \dots, n$)から前記グループごとの累積を示す値の列 $u = (u_1, \dots, u_n)$ を取り出し、取り出した u を出力する出力手順と、

を実行し、

前記新たな二項演算は、 $z = 0$ である場合は前記二項演算による w と y の演算結果を p 、 $z = 1$ である場合は y を p とし、 x と z の論理和を q とする、累積計算方法。

20

【請求項5】

コンピュータを、請求項1乃至3の何れか一項に記載の累積計算装置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、累積計算装置、累積計算方法、及びプログラムに関する。

【背景技術】

【0002】

30

暗号化された数値を復元すること無く特定の演算結果を得る方法として、秘密計算と呼ばれる技術が従来から知られている。例えば、非特許文献1には、3パーティの秘密分散技術が記載されている。

【0003】

また、データ処理技術の1つとして、グループ分けされたデータの集計を行う技術が従来から知られている。例えば、非特許文献2には、グループ分けされたデータのグループごとの統計値(平均値、最大値、集計等)を秘密計算により計算する方法が記載されている。なお、これらの統計値は結合的な2項演算の累積により実現される。

【先行技術文献】

【非特許文献】

40

【0004】

【文献】千田浩司, 濱田浩気, 五十嵐大, 高橋克巳. 軽量検証可能3パーティ秘匿関数計算の再考. In CSS, 2010.

【文献】五十嵐大, 千田浩司, 濱田浩気, 高橋克巳. 軽量検証可能3パーティ秘匿関数計算の効率化及びこれを用いたセキュアなデータベース処理. In SCIS, pp. 1-8, 2011.

【発明の概要】

【発明が解決しようとする課題】

【0005】

しかしながら、従来の方法は秘密計算向けにグループを隠しながらグループごとの統計値の計算(つまり、2項演算の累積の計算)を行えるように専用に設計されており、秘密

50

計算ではない通常のデータ処理で使われる累積の計算方法をそのまま秘密計算で用いることができないため効率が悪かった。

【0006】

本発明の一実施形態は、上記の点に鑑みてなされたもので、グループ別の累積計算を効率的に行うことを目的とする。

【課題を解決するための手段】

【0007】

上記目的を達成するため、一実施形態に係る累積計算装置は、グループに分けられた n 個の値の列 $v = (v_1, \dots, v_n)$ に関して、結合的な二項演算により前記グループごとの累積を計算する累積計算装置であって、 v の各要素 $v_1, \dots, v_n$ のうち、前記グループの先頭の要素には 1、前記先頭以外の要素には 0 を対応させた値の列を $c = (c_1, \dots, c_n)$ として、 v を $v' = (v'_1, \dots, v'_n)$ (ただし、 $v'_i = (v_i, c_i)$) に変換する値変換部と、前記二項演算を用いて、2つの対 (w, x) と (y, z) (ただし、 $x, z \in \{0, 1\}$) に対して新しい対 (p, q) を計算する新たな二項演算を作成する二項演算作成部と、 $i = 1, \dots, n$ について、前記新たな二項演算により累積 s'_i (ただし、 s'_i は前記新たな二項演算による v'_1 から v'_i までの累積) を計算する累積計算部と、各 s'_i ($i = 1, \dots, n$) から前記グループごとの累積を示す値の列 $u = (u_1, \dots, u_n)$ を取り出し、取り出した u を出力する出力部と、を有し、前記新たな二項演算は、 $z = 0$ である場合は前記二項演算による w と y の演算結果を p 、 $z = 1$ である場合は y を p とし、 x と z の論理和を q とする。

【発明の効果】

【0008】

グループ別の累積計算を効率的に行うことができる。

【図面の簡単な説明】

【0009】

【図1】本実施形態に係る累積計算装置のハードウェア構成の一例を示す図である。

【図2】本実施形態に係る累積計算装置の機能構成の一例を示す図である。

【図3】本実施形態に係る累積計算処理の流れの一例を示すフローチャートである。

【発明を実施するための形態】

【0010】

以下、本発明の一実施形態について説明する。本実施形態では、グループ別の累積計算を効率的に行うことができる累積計算装置 10 について説明する。

【0011】

ここで、 n 個の値の列を $v = (v_1, \dots, v_n)$ とし、 v の各要素 v_i ($i = 1, \dots, n$) はいくつかのグループに分けられており、同一グループ内の要素は連続するインデックス (要素番号) を持つように並べられているものとする。

【0012】

例えば、3つのグループに分けられている場合、或る i', i'' (ただし、 $1 \leq i' < i'' < n$) が存在し、 $v_1 \sim v_{i'}$ が 1 目目のグループ、 $v_{i'+1} \sim v_{i''}$ が 2 目目のグループ、 $v_{i''+1} \sim v_n$ が 3 目目のグループとなる。

【0013】

また、

【0014】

【数1】

を二項演算とする。

【 0 0 1 5 】

このとき、本実施形態に係る累積計算装置 1 0 は、各グループ内で上記の二項演算による累積の計算を行う際に、データ全体（つまり、後述する n 個の値 $v_1', \dots, v_n'$ 全体）に対する累積計算により上記の二項演算によるグループ別の累積を計算できるような新たな二項演算を作成し、この新たな二項演算でデータ全体の累積を計算する。データ全体の累積計算は通常の方法で処理されているものであるため、本実施形態に係る累積計算装置 1 0 は、例えば、秘密計算によりグループ別の累積計算を行う場合であっても、効率的にその計算を行うことが可能となる。

【 0 0 1 6 】

< 累積計算装置 1 0 のハードウェア構成 >

本実施形態に係る累積計算装置 1 0 のハードウェア構成を図 1 に示す。図 1 に示すように、本実施形態に係る累積計算装置 1 0 は一般的なコンピュータ又はコンピュータシステムのハードウェア構成で実現され、入力装置 1 0 1 と、表示装置 1 0 2 と、外部 I / F 1 0 3 と、通信 I / F 1 0 4 と、プロセッサ 1 0 5 と、メモリ装置 1 0 6 とを有する。これらの各ハードウェアは、それぞれがバス 1 0 7 により通信可能に接続される。

【 0 0 1 7 】

入力装置 1 0 1 は、例えば、キーボードやマウス、タッチパネル、各種物理ボタン等である。表示装置 1 0 2 は、例えば、ディスプレイ等である。なお、累積計算装置 1 0 は、例えば、入力装置 1 0 1 及び表示装置 1 0 2 のうちの少なくとも一方を有していなくてもよい。

【 0 0 1 8 】

外部 I / F 1 0 3 は、記録媒体 1 0 3 a 等の外部装置とのインタフェースである。累積計算装置 1 0 は、外部 I / F 1 0 3 を介して、記録媒体 1 0 3 a の読み取りや書き込み等を行うことができる。なお、記録媒体 1 0 3 a としては、例えば、C D (Compact Disc)、D V D (Digital Versatile Disk)、S D メモリカード (Secure Digital memory card)、U S B (Universal Serial Bus) メモリカード等が挙げられる。

【 0 0 1 9 】

通信 I / F 1 0 4 は、累積計算装置 1 0 を通信ネットワークに接続するためのインタフェースである。プロセッサ 1 0 5 は、例えば、C P U (Central Processing Unit) や G P U (Graphics Processing Unit) 等の各種演算装置である。メモリ装置 1 0 6 は、例えば、H D D (Hard Disk Drive) や S S D (Solid State Drive)、フラッシュメモリ、R A M (Random Access Memory)、R O M (Read Only Memory) 等の各種記憶装置である。

【 0 0 2 0 】

本実施形態に係る累積計算装置 1 0 は、図 1 に示すハードウェア構成を有することにより、後述する各種処理を実現することができる。なお、図 1 に示すハードウェア構成は一例であって、累積計算装置 1 0 は、例えば、複数のプロセッサ 1 0 5 を有していてもよいし、複数のメモリ装置 1 0 6 を有していてもよい。また、累積計算装置 1 0 は、図示したハードウェア以外にも様々なハードウェアを有していてもよい。

【 0 0 2 1 】

< 累積計算装置 1 0 の機能構成 >

本実施形態に係る累積計算装置 1 0 の機能構成を図 2 に示す。図 2 に示すように、本実施形態に係る累積計算装置 1 0 は、値変換部 2 0 1 と、二項演算作成部 2 0 2 と、累積計算部 2 0 3 と、出力部 2 0 4 と、記憶部 2 0 5 とを有する。値変換部 2 0 1、二項演算作成部 2 0 2、累積計算部 2 0 3、及び出力部 2 0 4 は、例えば、累積計算装置 1 0 にインストールされた 1 以上のプログラムがプロセッサ 1 0 5 に実行させる処理により実現される。また、記憶部 2 0 5 は、例えば、メモリ装置 1 0 6 により実現される。なお、記憶部 2 0 5 は、例えば、累積計算装置 1 0 と通信ネットワークを介して接続される記憶装置等により実現されていてもよい。

10

20

30

40

50

【 0 0 2 2 】

値変換部 2 0 1 は、 v の各要素のうちグループ内での先頭の要素には 1、それ以外の要素には 0 を対応させた値の列を $c = (c_1, \dots, c_n)$ として、 v を $v' = (v_1', \dots, v_n')$ (ただし、 $v_i' = (v_i, c_i)$) に変換する。

【 0 0 2 3 】

二項演算作成部 2 0 2 は、データ全体に対する累積計算によって元の二項演算によるグループ別の累積を計算できるような新たな二項演算を作成する。

【 0 0 2 4 】

累積計算部 2 0 3 は、 $v' = (v_1', \dots, v_n')$ 全体に対して新たな二項演算による累積計算を行う。

10

【 0 0 2 5 】

出力部 2 0 4 は、新たな二項演算による累積計算の結果から、元の二項演算によるグループ別の累積計算の結果を取り出し、その取り出した結果を出力する。

【 0 0 2 6 】

記憶部 2 0 5 は、累積計算の対象である n 個の値の列 $v = (v_1, \dots, v_n)$ や累積計算の途中結果、累積計算結果等を記憶する。

【 0 0 2 7 】

< 累積計算処理の流れ >

本実施形態に係る累積計算処理の流れについて図 3 を参照しながら説明する。

【 0 0 2 8 】

20

まず、値変換部 2 0 1 は、 v の各要素のうちグループ内での先頭の要素には 1、それ以外の要素には 0 を対応させた値の列を $c = (c_1, \dots, c_n)$ として、 v を $v' = (v_1', \dots, v_n')$ (ただし、 $v_i' = (v_i, c_i)$) に変換する (ステップ S 1 0 1)。

【 0 0 2 9 】

次に、二項演算作成部 2 0 2 は、データ全体 (つまり、 n 個の値 $v_1', \dots, v_n'$ 全体) に対する累積計算によって元の二項演算によるグループ別の累積を計算できるような新たな二項演算

【 0 0 3 0 】

【 数 2 】

30

$$\circ'$$

として、以下により定義される二項演算を作成する (ステップ S 1 0 2)。

【 0 0 3 1 】

【 数 3 】

40

$$(w, x) \circ' (y, z) = (zy + (1 - z)(w \circ y), x \text{OR} z)$$

ここで、 w, y は任意の値を取り得る変数、 x, z は 0 又は 1 を取り得る変数、 OR は x と z の少なくとも一方が 1 のときに 1、それ以外のときに 0 となる演算子 (つまり、論理和を表す演算子) である。

【 0 0 3 2 】

次に、累積計算部 2 0 3 は、 $v' = (v_1', \dots, v_n')$ 全体に対して新たな二項演

50

算により累積を計算する（ステップ S 1 0 3）。すなわち、累積計算部 2 0 3 は、新たな二項演算により v' の累積 $s' = (s'_1, \dots, s'_n)$ を計算する。ここで、各 $i = 1, \dots, n$ に対して、

【 0 0 3 3 】

【数 4】

$$s'_i = v'_1 \circ' v'_2 \circ' \dots \circ' v'_i$$

10

である。

【 0 0 3 4 】

そして、出力部 2 0 4 は、各 s'_i を $s'_i = (u_i, d_i)$ とするとき、値の列 $u = (u_1, \dots, u_n)$ を取り出し、元の二項演算の累積結果として出力する（ステップ S 1 0 4）。このとき、各 u_i が、元の二項演算による $v_1, \dots, v_i$ の累積計算の結果となる。また、各 $i = 1, \dots, n$ について、 $d_i = 1$ である。

【 0 0 3 5 】

なお、出力部 2 0 4 による出力先は任意としてよいが、例えば、記憶部 2 0 5 に保存する、他の装置又は機器に送信する、等とすることが考えられる。

20

【 0 0 3 6 】

< 実施例 >

以下では、上記の累積計算処理の実施例について説明する。

【 0 0 3 7 】

実施例 1

本実施例では、先頭から 4、2、1、3 個ずつの 4 つのグループに分けられた値の列 $v = (3, 5, 1, 2, 4, 6, 1, 3, 2, 8)$ が与えられ、二項演算 $\max(x, y)$ によるグループごとの累積計算を行う場合について説明する。なお、 $\max(x, y)$ は x と y の最大値を出力する二項演算である。

【 0 0 3 8 】

まず、上記のステップ S 1 0 1 では、グループの先頭の要素には 1、それ以外の要素には 0 を対応させた値の列 $c = (1, 0, 0, 0, 1, 0, 1, 1, 0, 0)$ が作成され、 v が以下の v' に変換される。

【 0 0 3 9 】

$$v' = ((v_1, c_1), \dots, (v_{10}, c_{10})) = ((3, 1), (5, 0), (1, 0), (2, 0), (4, 1), (6, 0), (1, 1), (3, 1), (2, 0), (8, 0))$$

上記のステップ S 1 0 2 では、上記の数 3 で定義される新たな二項演算が作成され、上記のステップ S 1 0 3 で、 $v' = ((v_1, c_1), \dots, (v_{10}, c_{10}))$ 全体に対して新たな二項演算により累積が計算される。

40

【 0 0 4 0 】

例えば、

【 0 0 4 1 】

【数 5】

$$s'_1 \circ' s'_2 \circ' \dots \circ' s'_{10}$$

50

を左から順に計算していく累積計算方法を用いると、 $s' = (s_1', \dots, s_{10}')$ は以下のように計算できる。

【 0 0 4 2 】

【 数 6 】

$$s'_1 = (3, 1)$$

$$s'_2 = s'_1 \circ' (5, 0) = (5, 1)$$

$$s'_3 = s'_2 \circ' (1, 0) = (5, 1)$$

$$s'_4 = s'_3 \circ' (2, 0) = (5, 1)$$

$$s'_5 = s'_4 \circ' (4, 1) = (4, 1)$$

$$s'_6 = s'_5 \circ' (6, 0) = (6, 1)$$

$$s'_7 = s'_6 \circ' (1, 1) = (1, 1)$$

$$s'_8 = s'_7 \circ' (3, 1) = (3, 1)$$

$$s'_9 = s'_8 \circ' (2, 0) = (3, 1)$$

$$s'_{10} = s'_9 \circ' (8, 0) = (8, 1)$$

10

20

したがって、上記のステップ S 1 0 4 では $u = (3, 5, 5, 5, 4, 6, 1, 3, 3, 8)$ が取り出され、それが出力される。この u により、元の二項演算 $\max(x, y)$ によるグループごとの累積計算（つまり、グループ内の各要素までの累積の最大値の計算）ができていることがわかる。

【 0 0 4 3 】

30

実施例 2

上記の実施例 1 では、ステップ S 1 0 3 で新たな二項演算により $s_1', \dots, s_{10}'$ を左から順に計算したが、その代わりに、本実施例では $s_1', \dots, s_{10}'$ を並列に計算する。これにより、実施例 1 よりも効率的に累積の計算を行うことが可能となる。なお、結合的な二項演算が並列に計算可能であることは既知である。

【 0 0 4 4 】

< まとめ >

以上のように、本実施形態に係る累積計算装置 1 0 は、各グループ内で二項演算による累積の計算を行う際に、累積対象の各値に対してグループの先頭の要素には 1、それ以外には 0 となるフラグを付与すると共に新たな二項演算を定義し、この新たな二項演算によりデータ全体（つまり、値とフラグの組の全体）に対して累積計算を行う。この新たな二項演算は、グループの先頭の要素は累積の値が計算済みであることを利用して、当該フラグを計算済みであるか否かを表すものと見做することで、元の二項演算を、値とフラグの組に対する二項演算に拡張したものである。

40

【 0 0 4 5 】

これにより、本実施形態に係る累積計算装置 1 0 は、例えば、秘密計算（秘密分散も含む。）によりグループ別の累積計算を行う場合であっても、効率的にその計算を行うことが可能となる。これは、累積の計算を行いたい二項演算を決められた順序で適用する任意の方法を使って、同じ順序で秘密計算によりグループ別の累積の計算が可能となるためである。このため、例えば、二項演算として $\max$ 又は $\min$ を用いることで、秘密計算で

50

の `group by max` 又は `group by min` 操作等を効率的に実現することが可能となる。

【0046】

したがって、本実施形態に係る累積計算装置10は、通常のデータ処理に用いられるだけでなく、例えば、データ内容を秘匿化したままデータ処理やデータ分析を行う場合に適用することが可能である。具体例を挙げれば、本実施形態に係る累積計算装置10は、データ内容を秘匿化したまま所定のタスク（例えば、何等かの予測、分類等）を実現する機械学習モデルの学習用データを作成することが可能である。また、それに加えて、本実施形態に係る累積計算装置10は、その学習用データで学習された機械学習モデルにより種々の予測や分類、それら予測又は分類結果に基づく他の機器、装置、システム等の制御等

10

【0047】

本発明は、具体的に開示された上記の実施形態に限定されるものではなく、請求の範囲の記載から逸脱することなく、種々の変形や変更、既知の技術との組み合わせ等が可能である。

【符号の説明】

【0048】

10	累積計算装置
101	入力装置
102	表示装置
103	外部I/F
103a	記録媒体
104	通信I/F
105	プロセッサ
106	メモリ装置
107	バス
201	値変換部
202	二項演算作成部
203	累積計算部
204	出力部
205	記憶部

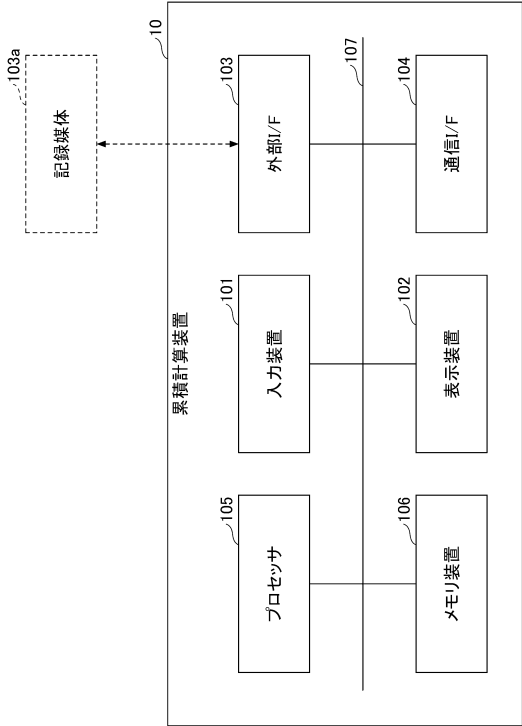
20

30

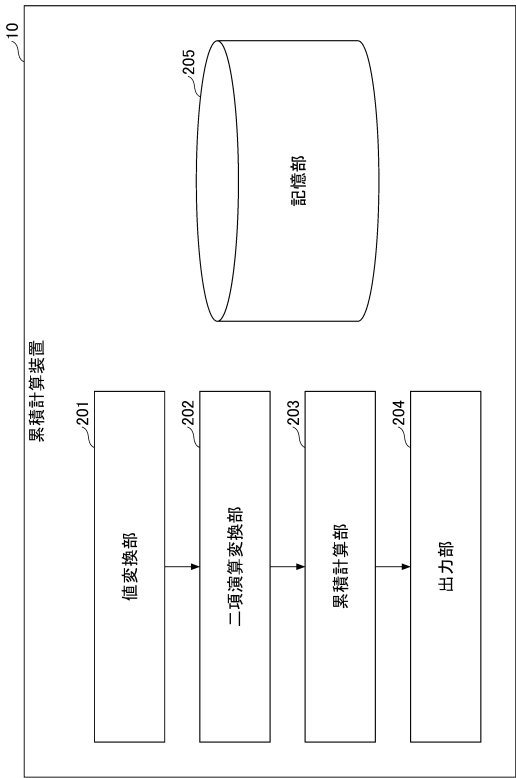
40

50

【図面】
【図 1】



【図 2】



10

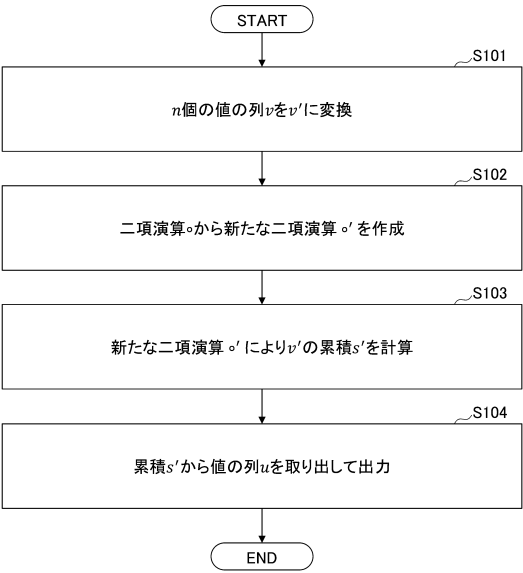
20

30

40

50

【図 3】



10

20

30

40

50

フロントページの続き

- (56)参考文献 特開 2 0 1 4 - 0 8 1 4 7 5 (J P , A)
国際公開第 2 0 1 9 / 2 0 8 4 8 4 (W O , A 1)
国際公開第 2 0 1 9 / 2 0 8 4 8 5 (W O , A 1)
国際公開第 2 0 1 9 / 2 0 8 4 8 6 (W O , A 1)
国際公開第 2 0 1 9 / 2 2 5 4 0 1 (W O , A 1)
- (58)調査した分野 (Int.Cl. , D B 名)
G 0 9 C 1 / 0 0