

(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
2022年7月28日(28.07.2022)



(10) 国際公開番号

WO 2022/158104 A1

- (51) 国際特許分類:
G06F 7/58 (2006.01) G06N 10/00 (2022.01)
G06F 17/18 (2006.01)
- (21) 国際出願番号: PCT/JP2021/042759
- (22) 国際出願日: 2021年11月22日(22.11.2021)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2021-008663 2021年1月22日(22.01.2021) JP
- (71) 出願人: 日本電気株式会社 (NEC CORPORATION) [JP/JP]; 〒1088001 東京都港区芝五丁目7番1号 Tokyo (JP). NECソリューションイノベータ株式会社(NEC SOLUTION

INNOVATORS, LTD.) [JP/JP]; 〒1368627 東京都江東区新木場一丁目18番7号 Tokyo (JP).

- (72) 発明者: 中村 暢達 (NAKAMURA Nobutatsu); 〒1088001 東京都港区芝五丁目7番1号 日本電気株式会社内 Tokyo (JP). 橋本 慎司 (HASHIMOTO Shinji); 〒1368627 東京都江東区新木場一丁目18番7号 NECソリューションイノベータ株式会社内 Tokyo (JP). 高原 玲央 (TAKAHARA Reo); 〒1368627 東京都江東区新木場一丁目18番7号 NECソリューションイノベータ株式会社内 Tokyo (JP). 柴田 将 (SHIBATA Sho); 〒1368627 東京都江東区新木場一丁目18番7号 NECソリューションイノベータ株式会社内 Tokyo (JP). 森 英憲 (MORI Hidenori); 〒1368627 東京都江東区新

(54) Title: RANDOM NUMBER GENERATOR, RANDOM NUMBER GENERATION METHOD, AND NON-TRANSITORY COMPUTER-READABLE MEDIUM HAVING PROGRAM STORED THEREIN

(54) 発明の名称: 乱数生成器、乱数生成方法、及びプログラムが格納された非一時的なコンピュータ可読媒体

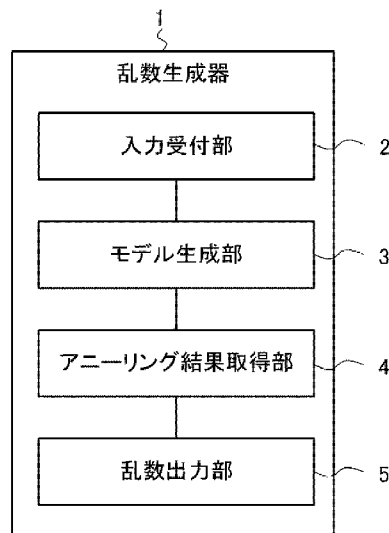


Fig. 1

- 1 Random number generator
2 Input reception unit
3 Model generation unit
4 Annealing result acquisition unit
5 Random number output unit

(57) Abstract: The present invention provides a random number generator, random number generation method, and program capable of high-quality random number generation following a desired distribution. A random number generator (1) according to the present invention has: an input reception unit (2) which receives input designating a probability

木場一丁目 18 番 7 号 NEC ソリュート
ンイノベータ株式会社内 Tokyo (JP).

(74) 代理人: 家入 健 (IEIRI Takeshi); 〒2210835 神
奈川 県 横 浜 市 神 奈 川 区 鶴 屋 町 三 丁 目 3
3 番 8 アサヒビルディング 5 階 響 国 際
特許事務所 Kanagawa (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, BN, BR, BW, BY, BZ, CA, CH,
CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ,
EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY,
MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ,
NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT,
QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL,
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG,
US, UZ, VC, VN, WS, 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, LR, LS,
MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM,
ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ,
TM), ヨーロッパ (AL, 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, RS,
SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM,
GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

一 国際調査報告 (条約第21条(3))

distribution of random numbers; a model generation unit (3) which generates, on the basis of the probability distribution, an Ising model using n (where n is an integer of 2 or more) two-value variables respectively allocated to n partial segments into which a numerical range of the random numbers has been divided; an annealing result acquisition unit (4) which acquires values, of the n two-value variables, which are the execution results of quantum annealing of the Ising model; and a random number output unit (5) which outputs, as random numbers, values included in the partial segments allocated to the two-value variables of which the values obtained as the execution results are prescribed values.

(57) 要約: 所望の分布に従う高品質な乱数を生成することができる乱数生成器、乱数生成方法、及びプログラムを提供する。乱数生成器 (1) は、乱数の確率分布を指定する入力を受付ける入力受付部 (2) と、乱数の数値範囲を分割した n (n は 2 以上の整数) 個の部分区間のそれぞれに割り当てられる n 個の二値変数を用いたイジングモデルを、前記確率分布に基づいて生成するモデル生成部 (3) と、前記イジングモデルについての量子アニーリングの実行結果である n 個の前記二値変数の値を取得するアニーリング結果取得部 (4) と、前記実行結果として得られた値が所定の値である前記二値変数に割り当てられている前記部分区間に含まれる値を乱数として出力する乱数出力部 (5) とを有する。

明 細 書

発明の名称：

乱数生成器、乱数生成方法、及びプログラムが格納された非一時的なコンピュータ可読媒体

技術分野

[0001] 本発明は乱数生成器、乱数生成方法、及びプログラムに関する。

背景技術

[0002] セキュアなデータ通信などにおいて、高品質な乱数を得ることは重要である。しかし、通常の計算機において関数呼び出しで得られる乱数は周期性がある。また、物理的なノイズを利用した乱数生成器により生成された乱数は、物理現象を観察及び再現することで、予測が可能である。したがって、これらの乱数では高いセキュリティを担保できない。

[0003] 近年、量子コンピュータの利用が広まりつつあり、インターネットを介して、一般の利用者でも、量子コンピュータにアクセスし、利用可能となっている。量子コンピュータ技術は発展途上であるが、量子アニーリング方式と呼ばれる量子コンピュータ（以下、量子アニーリングマシンと称す）は利用可能となっている。量子アニーリングマシンは、イジングモデルと呼ばれる定式化された問題を求解することに特化した計算機であり、組合せ最適化問題の求解などに使われている（特許文献1参照）。

[0004] イジングモデルで表現された系における、安定した状態の量子ビット（0，1）の組合せを量子アニーリングマシンにより得ることができる。ただし、量子ゆらぎと呼ばれる特性のため、常に同じ組み合わせが得られるわけではなく、安定した状態近辺の量子ビットの様々な組合せが得られる。量子ビットの様々な組合せの発生確率は、原理的にはボルツマン分布に従う。そのため、量子アニーリングマシンを用いた場合、最適化問題の最適解近辺の解を得ることはできるが、ボルツマン分布以外の利用者が指定する任意の分布に従う解（数値）を得ることはできない。このため、利用者が指定する任意

の分布に従う乱数の生成には量子アニーリングマシンを利用することができなかった。

- [0005] 一方、利用者が指定する分布に従う乱数を得るための技術に関して、特許文献2に開示された技術がある。この文献に記載された技術では、疑似乱数生成器により生成された数値に所定の処理を行うことにより所定の分布に従う乱数を得ている。疑似乱数には周期性があるため、この技術により得られる乱数は、高品質の乱数とならない。

先行技術文献

特許文献

- [0006] 特許文献1：特表2008-525873号公報
特許文献2：特開2019-79523号公報

発明の概要

発明が解決しようとする課題

- [0007] 上述した通り、所望の分布に従う高品質な乱数を生成する技術の提供が求められている。

そこで、本明細書に開示される実施形態が達成しようとする目的の1つは、所望の分布に従う高品質な乱数を生成することができる乱数生成器、乱数生成方法、及びプログラムを提供することである。

課題を解決するための手段

- [0008] 本開示の第1の態様にかかる乱数生成器は、
乱数の確率分布を指定する入力を受付ける入力受付部と、
乱数の数値範囲を分割した n （ n は2以上の整数）個の部分区間のそれぞれに割り当てられる n 個の二値変数を用いたイジングモデルを、前記確率分布に基づいて生成するモデル生成部と、
前記イジングモデルについての量子アニーリングの実行結果である n 個の前記二値変数の値を取得するアニーリング結果取得部と、
前記実行結果として得られた値が所定の値である前記二値変数に割り当て

られている前記部分区間に含まれる値を乱数として出力する乱数出力部とを有する。

- [0009] 本開示の第2の態様にかかる乱数生成方法では、
乱数生成器が、
乱数の確率分布を指定する入力を受け、
乱数の数値範囲を分割した n (n は2以上の整数) 個の部分区間のそれぞれに割り当てられる n 個の二値変数を用いたイジングモデルを、前記確率分布に基づいて生成し、
前記イジングモデルについての量子アニーリングの実行結果である n 個の前記二値変数の値を取得し、
前記実行結果として得られた値が所定の値である前記二値変数に割り当てられている前記部分区間に含まれる値を乱数として出力する。

- [0010] 本開示の第3の態様にかかるプログラムは、
乱数の確率分布を指定する入力を受けける入力受付ステップと、
乱数の数値範囲を分割した n (n は2以上の整数) 個の部分区間のそれぞれに割り当てられる n 個の二値変数を用いたイジングモデルを、前記確率分布に基づいて生成するモデル生成ステップと、
前記イジングモデルについての量子アニーリングの実行結果である n 個の前記二値変数の値を取得するアニーリング結果取得ステップと、
前記実行結果として得られた値が所定の値である前記二値変数に割り当てられている前記部分区間に含まれる値を乱数として出力する乱数出力ステップと
をコンピュータに実行させる。

発明の効果

- [0011] 上述の態様によれば、所望の分布に従う高品質な乱数を生成することができる乱数生成器、乱数生成方法、及びプログラムを提供することができる。

図面の簡単な説明

- [0012] [図1]実施形態の概要にかかる乱数生成器の構成の一例を示すブロック図であ

る。

[図2]実施の形態1にかかる乱数生成システムの構成の一例を示すブロック図である。

[図3]実施の形態1にかかる乱数生成器のハードウェア構成の一例を示すブロック図である。

[図4]実施の形態1にかかる乱数生成器の動作の一例を示すフローチャートである。

[図5]実施の形態2にかかる乱数生成システムの構成の一例を示すブロック図である。

[図6]実施の形態2にかかる乱数生成器の動作の一例を示すフローチャートである。

[図7]実施の形態3にかかる乱数生成システムの構成の一例を示すブロック図である。

[図8]実施の形態3にかかる乱数生成器の動作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

[0013] <実施の形態の概要>

実施形態の詳細を説明する前に、まず、実施形態の概要について説明する。

図1は、実施形態の概要にかかる乱数生成器1の構成の一例を示すブロック図である。乱数生成器1は、量子アニーリングの結果を用いて乱数を生成する装置であり、図1に示すように入力受付部2、モデル生成部3、アニーリング結果取得部4、及び乱数出力部5を有する。

[0014] 入力受付部2は、乱数の確率分布を指定する入力を受付ける。ユーザ等は、所望の確率分布に従う乱数を乱数生成器1に出力させるために、この所望の確率分布を指定する入力を乱数生成器1に与える。

[0015] モデル生成部3は、乱数の数値範囲を分割した n （ n は2以上の整数）個の部分区間のそれぞれに割り当てられる n 個の二値変数を用いたイジングモ

デルを、入力受付部 2 が受付けた確率分布に基づいて生成する。ここで、乱数の数値範囲とは、生成されうる乱数の最小値と最大値により定まる範囲をいう。すなわち、乱数生成器 1 は、この数値範囲に属する乱数を生成する。また、上述した二値変数の値は、この数値範囲に属する部分区間を選択するか否かを表す。換言すると、この二値変数は、当該二値変数が割り当てられた部分区間に含まれる値を乱数として採用するか否かを表す。

[0016] アニーリング結果取得部 4 は、モデル生成部 3 が生成したイジングモデルについての量子アニーリングの実行結果である n 個の二値変数の値を取得する。すなわち、アニーリング結果取得部 4 は、量子アニーリングマシンに、モデル生成部 3 が生成したイジングモデルについての量子アニーリングを実行させ、その実行結果を量子アニーリングマシンから取得する。

[0017] 乱数出力部 5 は、実行結果として得られた値が所定の値（例えば、1）である二値変数に割り当てられている部分区間に含まれる値を乱数として出力する。

[0018] このように、乱数生成器 1 は、指定された確率分布に基づいてイジングモデルを生成し、このイジングモデルについての量子アニーリングの結果にしたがって、乱数を出力する。量子アニーリングの実行結果は、予測が困難であるため、乱数生成器 1 が出力する乱数の予測も困難である。このため、乱数生成器 1 によれば、所望の分布に従う高品質な乱数を生成することができる。

[0019] <実施の形態 1>

次に、実施の形態 1 について説明する。

図 2 は、実施の形態 1 にかかる乱数生成システム 10 の構成の一例を示すブロック図である。図 2 に示すように、乱数生成システム 10 は、乱数生成器 100 と量子アニーリングマシン 200 とを備える。乱数生成器 100 と量子アニーリングマシン 200 とは、例えば、有線又は無線のネットワークを介して、相互に通信可能に接続されている。なお、図 2 に示した構成では、量子アニーリングマシン 200 は、乱数生成器 100 とは別の装置として

図示されているが、乱数生成器 100 に含まれてもよい。

[0020] 乱数生成器 100 は、図 1 に示した乱数生成器 1 に対応している。量子アニーリングマシン 200 は、量子ビットと量子ビット間の結合とを実現する量子チップを備え、イジングモデルについての量子アニーリングを行ない各量子ビットの値を決定する。なお、量子チップは、量子力学における量子状態を用いて動作するチップである。なお、乱数生成システム 10 の量子アニーリングマシン 200 としては、公知のマシンを用いることができるため、その具体的な構成及び処理についての詳細な説明は割愛する。

[0021] 以下、乱数生成器 100 の具体的な構成及び処理について説明する。

乱数生成器 100 は、図 2 に示すように、処理制御部 101、入力受付部 102、モデル生成部 103、アニーリング結果取得部 104、疑似乱数生成部 105、及び乱数出力部 106 を有する。

[0022] 処理制御部 101 は、乱数生成器 100 の上述した構成要素の処理を制御する。本実施の形態では、特に、処理制御部 101 は、生成すべき乱数の個数に応じて、アニーリング結果取得部 104 及び疑似乱数生成部 105 の処理の実行回数を制御する。

[0023] 入力受付部 102 は、図 1 の入力受付部 2 に対応しており、乱数の確率分布を指定する入力を受付ける。入力受付部 102 は、例えば、乱数生成器 100 が備える入力インタフェースを介してユーザが入力した確率分布を受付けてもよいし、乱数生成器 100 が備えるメモリなどの記憶装置から確率分布を読み出すことにより、これを受付けてもよい。また、入力受付部 102 は、他の装置から送信された確率分布を受信することにより、これを受付けてもよい。

[0024] 本実施の形態では、入力受付部 102 は、乱数の確率分布を指定する入力として、部分区間ごとの確率の設定値を受付ける。この部分区間は、確率変数の定義域を区分したものであるが、乱数の数値範囲を分割したものとも言うことができる。例えば、乱数生成器 100 により生成したい乱数の最小値を R_{MIN} 、最大値を R_{MAX} とする。すなわち、乱数生成器 100 により、 R_{MIN}

n 以上、 R_{MAX} 以下の乱数を生成する場合を例に説明する。この場合、乱数生成器100は、 R_{MIN} を下限とし R_{MAX} を上限とする数値範囲を n (n は2以上の整数)等分して得られる n 個の部分区間ごとの確率の設定値を受付ける。つまり、入力受付部102は、部分区間ごとの確率 p_i の指定を受付ける。ここで、添え字 i は、部分区間の識別番号であり、1以上 n 以下の整数である。例えば、ある部分区間に属する数値が最も乱数として出力されやすいようにしたい場合、当該部分区間の確率 p_i の値は、他の部分区間の確率 p_i の値よりも大きい値が設定されることとなる。なお、 p_1 から p_n の総和は1となる。

[0025] 上述した n 、 R_{MIN} 、及び R_{MAX} のそれぞれの値は、予め定められていてもよいし、入力受付部102が受付けてもよい。このように、 n 、 R_{MIN} 、及び R_{MAX} の指定も可能とすることにより、乱数生成器100の運用における利便性を向上することができる。

[0026] なお、本実施の形態では、入力受付部102は、部分区間ごとの確率の設定値を受付けるが、確率分布を指定する入力はこれに限られない。例えば、入力受付部102は、乱数の確率分布を指定する入力として、確率分布の種類(例えば、正規分布など)を指定する情報と、分布のパラメータ(平均及び分散など)とを受付けてもよいし、確率分布を表す数式を受付けてもよい。

なお、入力受付部102は、さらに、生成すべき乱数の個数の指定を受付けてもよい。

[0027] モデル生成部103は、図1のモデル生成部3に対応しており、 n 個の部分区間のそれぞれに割り当てられる n 個の二値変数(量子ビット変数)を用いたイジングモデルを、入力受付部102が受付けた確率分布に基づいて生成する。ここでは、 n 個の二値変数(量子ビット変数)を x_1 、 x_2 、 $\dots$ 、 x_n とする。すなわち、 i 番目の部分区間には、二値変数 x_i が割り当てられる。したがって、 i 番目の部分区間には、確率 p_i と二値変数 x_i が関連づけられる。

[0028] モデル生成部 103 は、具体的には、例えば以下の式（１）で表されるモデル $H(x)$ を生成する。

[0029] <式（１）>

$$H(x) = \sum_{i=1}^n -(\log(p_i))x_i + H_{Onehot}$$

[0030] ここで、上述の通り、 i は、 n 個の部分区間を識別する番号である。 x_i は、 i 番目の部分区間に割り当てられた二値変数であり、 0 または 1 の値をとる。 p_i は、 x_i が割り当てられた部分区間における確率分布の値である。

[0031] 式（１）において、右辺の第一項で表される関数（第一の関数とも称す）は、目的関数である。量子アニーリングマシン 200 によって、関数 H_{Onehot} （第二の関数とも称す）で表される制約を満たしつつこの目的関数の値が最小となるような近似解（すなわち、二値変数 x_1 、 x_2 、 $\dots$ 、 x_n の値の組み合わせ）が探索される。また、右辺の第二項で表される関数 H_{Onehot} は、 n 個の二値変数 x_1 、 x_2 、 $\dots$ 、 x_n のいずれか一つが所定の値（具体的には、 1 ）となり、それ以外の二値変数が当該所定の値以外の値（具体的には、 0 ）となるようにするための制約項である。関数 H_{Onehot} は、具体的には、以下の式（２）で表される。なお、 w は、重みを表す係数であり、モデル生成部 103 は、 w の値として正の所定値を設定する。

[0032] <式（２）>

$$H_{Onehot} = w \left(\sum_{i=1}^n x_i - 1 \right)^2$$

[0033] モデル生成部 103 は、上記数式で表されるモデルの p_i の値を入力受付部 102 が受付けた乱数の確率分布の指定にしたがって決定することにより、

当該確率分布にしたがった乱数を生成するためのイジングモデルを生成する。なお、入力受付部 102 が、部分区間ごとの確率 p_i の設定値ではなく、確率分布を表す数式を受付けた場合及び確率分布の種類及びパラメータを受付けた場合には、モデル生成部 103 は、次のように上記のイジングモデルを生成する。この場合、モデル生成部 103 は、 n 、 R_{MIN} 、及び R_{MAX} を用いて、各部分区間の確率 p_i を特定することにより、上記のイジングモデルを生成する。このとき、部分区間において確率分布の値が一定でない場合には、モデル生成部 103 は、例えば、当該部分区間における確率分布の値の平均値、最小値、又は最大値などを用いて、確率 p_i を決定してもよい。

[0034] 上記数式からわかるように、モデル生成部 103 は、次のようなイジングモデルを生成すると説明することもできる。モデル生成部 103 は、二値変数 x_i についての第一の関数と二値変数 x_i についての第二の関数とを用いて表されるイジングモデルを生成する。ここで、第一の関数は、二値変数 x_i が割り当てられた部分区間における確率分布の値 p_i が大きいほど値が小さくなる関数の値と当該二値変数 x_i の値との積の総和で表される関数である。また、第二の関数は、 n 個の二値変数 x_1 、 x_2 、 $\dots$ 、 x_n のいずれか一つが所定の値である場合に最小値となる関数であり、この条件が満たされない場合、重み w に依存した正の値をとる。

[0035] アニーリング結果取得部 104 は、図 1 のアニーリング結果取得部 4 に対応しており、モデル生成部 103 が生成したイジングモデルについての量子アニーリングの実行結果である n 個の二値変数 x_1 、 x_2 、 $\dots$ 、 x_n のそれぞれの値を取得する。アニーリング結果取得部 104 は、量子アニーリングマシン 200 に処理を実行させるために、モデル生成部 103 が生成したイジングモデルに基づいて、量子アニーリングマシン 200 による量子アニーリングの実行条件を設定する。具体的には、アニーリング結果取得部 104 は、モデル生成部 103 が生成したイジングモデルに基づいて、二値変数に対応する量子ビットと、量子ビット間の相互作用の強さを設定する。そして、アニーリング結果取得部 104 は、量子アニーリングマシン 200 に当該

イジングモデルについての量子アニーリングの実行を指示する。

[0036] これに対し、量子アニーリングマシン200は、量子アニーリングの実行結果、すなわち n 個の二値変数 x_1 、 x_2 、 $\dots$ 、 x_n のそれぞれの値を乱数生成器100に対して出力し、アニーリング結果取得部104がこれを取得する。量子アニーリングマシン200は、式(1)で示した $H(x)$ を最小にする近似解を量子アニーリングの実行結果として出力する。具体的には、アニーリング結果取得部104は、式(1)で表されるイジングモデルに対する量子アニーリングの実行結果として、次のような実行結果を取得する。すなわち、アニーリング結果取得部104は、 n 個の二値変数 x_1 、 x_2 、 $\dots$ 、 x_n のうちの一つの二値変数の値が所定の値（具体的には1）であり、他の二値変数の値が他の値（具体的には0）である実行結果を取得する。

[0037] ここで、二値変数 x_i の値が1となる確率は、 p_i である。したがって、乱数生成器100は、値が所定の値（具体的には1）である二値変数 x_i に対応する部分区間に属する値を乱数として出力することで、指定された確率分布にしたがった乱数を生成することができる。乱数生成器100は、値が所定の値である二値変数 x_i に対応する部分区間内の所定値を乱数として出力してもよいが、本実施の形態では、より様々な値を乱数として出力できるように、乱数生成器100は疑似乱数生成部105を備えている。なお、部分区間内の所定値とは、例えば、当該部分区間の中央の値、最大値、又は最小値などである。

[0038] 疑似乱数生成部105は、量子アニーリングの実行結果として得られた値が所定の値（具体的には1）である二値変数 x_i に割り当てられている部分区間に収まる疑似乱数（一様乱数）を生成する。すなわち、当該部分区間の最小値を疑似乱数の最小値とし、当該部分区間の最大値を疑似乱数の最大値とする疑似乱数を生成する。疑似乱数生成部105は、疑似乱数を生成する公知の関数を用いて疑似乱数を生成する。例えば、疑似乱数生成部105は、乱数値を返す組み込み関数の呼び出しにより、疑似乱数を得てもよい。

[0039] 乱数出力部106は、図1の乱数出力部5に対応しており、量子アニーリ

ングの実行結果にしたがって選択された部分区間に含まれる値を乱数として出力する。本実施の形態では、選択された部分区間に含まれる値として、疑似乱数生成部 105 により生成された疑似乱数を出力する。なお、このように、本実施の形態では、乱数出力部 106 は、量子アニーリングの実行結果にしたがって選択された部分区間における疑似乱数を出力するが、上述の通り、当該部分区間内の所定値を出力してもよい。この場合、乱数生成器 100 は、疑似乱数生成部 105 を有さなくてもよい。乱数出力部 106 は、任意の出力先に乱数を出力する。乱数出力部 106 は、例えば、乱数をディスプレイに出力してもよいし、暗号化処理などの所定の処理を行う装置又は処理部などに乱数を送信してもよい。

[0040] 乱数生成器 100 は、複数の乱数を生成してもよく、この場合、乱数出力部 106 は、生成された複数の乱数を出力する。処理制御部 101 は、生成する乱数の数に応じて、アニーリング結果取得部 104 及び疑似乱数生成部 105 の処理の実行回数を制御する。上述の通り、式 (1) で表されるイジングモデルについて量子アニーリングを実行するたびに、1 つの乱数を生成することができる。したがって、例えば、処理制御部 101 は、 m (m は正整数) 個の乱数を生成する場合、アニーリング結果取得部 104 及び疑似乱数生成部 105 の処理を m 回繰り返すよう処理を制御する。なお、 m の値は、予め定められていてもよいし、入力受付部 102 が受け付けてもよい。このように、乱数生成器 100 は、同一のイジングモデルについての複数回の量子アニーリングの実行結果を取得することにより、複数の乱数を出力する。これにより、任意の個数の乱数を得ることができる。

[0041] 図 3 は、乱数生成器 100 のハードウェア構成の一例を示すブロック図である。図 3 に示すように、乱数生成器 100 は、ネットワークインタフェース 150、メモリ 151、及びプロセッサ 152 を含む。ネットワークインタフェース 150、メモリ 151、及びプロセッサ 152 は、データバスなどを介して相互に接続されている。

[0042] ネットワークインタフェース 150 は、量子アニーリングマシン 200 を

含む他の任意の装置と通信するために使用される。ネットワークインタフェース150は、例えば、ネットワークインタフェースカード（NIC）を含んでもよい。

[0043] メモリ151は、例えば、揮発性メモリ及び不揮発性メモリの組み合わせによって構成される。メモリ151は、プロセッサ152により実行される、1以上の命令を含むソフトウェア（コンピュータプログラム）、及び乱数生成器100の各種処理に用いるデータなどを格納するために使用される。

[0044] プロセッサ152は、メモリ151からソフトウェア（コンピュータプログラム）を読み出して実行することで、図2に示した各構成要素の処理を行う。

[0045] プロセッサ152は、マイクロプロセッサ、MPU（Micro Processor Unit）、又はCPU（Central Processing Unit）などであってもよい。プロセッサ152は、複数のプロセッサを含んでもよい。

このように、乱数生成器100は、コンピュータとして機能する装置であり、情報処理装置とも称される。

[0046] なお、上述したプログラムは、様々なタイプの非一時的なコンピュータ可読媒体（non-transitory computer readable medium）を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体（tangible storage medium）を含む。非一時的なコンピュータ可読媒体の例は、磁気記録媒体（例えばフレキシブルディスク、磁気テープ、ハードディスクドライブ）、光磁気記録媒体（例えば光磁気ディスク）、CD-ROM（Read Only Memory）CD-R、CD-R/W、半導体メモリ（例えば、マスクROM、PROM（Programmable ROM）、EPROM（Erasable PROM）、フラッシュROM、RAM（Random Access Memory））を含む。また、プログラムは、様々なタイプの一時的なコンピュ

ータ可読媒体 (transitory computer readable medium) によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。

[0047] 次に、乱数生成器 100 の動作の流れについて説明する。

図 4 は、乱数生成器 100 の動作の一例を示すフローチャートである。以下、図 4 を参照しつつ、乱数生成器 100 による乱数の生成動作について説明する。

[0048] ステップ S 100 において、入力受付部 102 は、乱数の出力についての設定情報の入力を受付ける。具体的には、入力受付部 102 は、乱数の確率分布を指定する入力を受付ける。また、上述の通り、入力受付部 102 は、さらに、分割数 n 、乱数の最小値 R_{MIN} 、乱数の最大値 R_{MAX} 、及び生成すべき乱数の個数 m のいずれかまたは全てについて指定する入力を受付けてもよい。

[0049] 次に、ステップ S 101 において、モデル生成部 103 は、ステップ S 100 で指定された確率分布に基づいて、イジングモデルを生成する。

[0050] 次に、ステップ S 102 において、アニーリング結果取得部 104 は、ステップ S 101 で生成したイジングモデルについての量子アニーリングの実行結果を量子アニーリングマシン 200 から取得する。すなわち、アニーリング結果取得部 104 は、 n 個の二値変数 x_1 、 x_2 、 $\dots$ 、 x_n のそれぞれの値を取得する。

[0051] 次に、ステップ S 103 において、疑似乱数生成部 105 は、ステップ S 102 で取得した実行結果に基づいて選択される部分区間内で、疑似乱数を生成する。すなわち、疑似乱数生成部 105 は、値が 1 である x_i に対応する部分区間に収まる疑似乱数を生成する。

[0052] 次に、ステップ S 104 において、処理制御部 101 は、指定された個数の乱数が得られたか否かを判定する。指定された個数の乱数が得られていな

い場合には、処理制御部 101 は、ステップ S 102 及びステップ S 103 の処理を再度行うよう制御する。これに対し、指定された個数の乱数が得られた場合には、処理はステップ S 105 へ移行する。

[0053] ステップ S 105 において、乱数出力部 106 は、ステップ S 102 及びステップ S 103 の処理により得られた乱数を入力する。

[0054] 以上、実施の形態 1 について説明した。本実施の形態では、量子アニーリングの結果に基づいて部分区間が選択される。このため、選択される部分区間の予測は困難である。また、各部分区間が選択される確率は、指定された確率分布にしたがう。このため、本実施の形態によれば、所望の分布に従う高品質な乱数を生成することができる。

[0055] <実施の形態 2>

次に、実施の形態 2 について説明する。

量子アニーリングマシン 200 が備える量子ビットの数を k (k は 2 以上の整数) とする。この場合、実施の形態 1 で示した乱数生成器 100 では、量子の特性を利用した部分区間の選択、すなわち予測が困難な部分区間の選択は、最大でも k 個の部分区間の中から行われることとなる。すなわち、設定可能な部分区間数が量子ビットの数に依存してしまう。本実施の形態では、部分区間の選択を階層的に繰り返すことにより、より多くの部分区間の中から部分区間を選択する。これにより、量子アニーリングマシン 200 の量子ビット数が限られていても、より多くの部分区間の中から選択した乱数を入力することができる。

[0056] 図 5 は、実施の形態 2 にかかる乱数生成システム 10a の構成の一例を示すブロック図である。図 5 に示すように、実施の形態 2 にかかる乱数生成システム 10a は、乱数生成器 100 が乱数生成器 100a に置き換わった点で、実施の形態 1 にかかる乱数生成システム 10 と異なっている。

以下、実施の形態 1 と異なる構成及び処理について説明し、実施の形態 1 と同様な構成及び処理については適宜説明を省略する。

[0057] 図 5 に示されるように、実施の形態 2 にかかる乱数生成器 100a は、主

に、処理制御部 101 が処理制御部 101a に置き換わった点で、実施の形態 1 にかかる乱数生成器 100 と異なっている。また、図 5 に示した構成例では疑似乱数生成部 105 が省略されている。ただし、本実施の形態でも、乱数生成器 100a は、疑似乱数生成部 105 を備えていてもよい。すなわち、本実施の形態において最終的に選択された部分区間に含まれる数値を乱数として出力する際に、この部分区間に含まれる所定値ではなく、疑似乱数生成部 105 により生成した乱数を出力してもよい。

[0058] なお、図 5 に示した構成においても、量子アニーリングマシン 200 は、乱数生成器 100a とは別の装置として図示されているが、乱数生成器 100a に含まれてもよい。

[0059] 処理制御部 101a は、処理制御部 101 と同様、図 5 に示した乱数生成器 100a の各構成要素の処理を制御する。特に、処理制御部 101a は、所定の回数だけ、部分区間の階層的な選択を行うよう、モデル生成部 103 及びアニーリング結果取得部 104 の処理を制御する。ここで、部分区間の階層的な選択とは、 n 個の部分区間の中から量子アニーリング結果にしたがって部分区間を選択し、その後、選択された部分区間に設定された n 個のより細かい部分区間の中から量子アニーリング結果にしたがって部分区間をさらに選択することをいう。処理制御部 101a は、量子アニーリングによる部分区間の階層的な選択を q 回（ q は整数）繰り返すよう制御する。なお、 $q = 0$ の場合、実施の形態 1 と同様、部分区間の階層的な選択、すなわち部分区間の再選択を行わずに乱数を出力することとなる。なお、この q の値は、予め定められていてもよいし、入力受付部 102 が受け付けてもよい。

[0060] 部分区間の階層的な選択を行うために、本実施の形態のモデル生成部 103 は、処理制御部 101a の制御にしたがい、次のような処理を行う。モデル生成部 103 は、モデル生成後にさらに、量子アニーリングの実行により選択された部分区間をさらに分割した n 個の新たな部分区間のそれぞれに割り当てられる n 個の二値変数を用いた新たなイジングモデルを、指定された確率分布に基づいて生成する。具体的には、モデル生成部 103 は、部分区

間の階層的な選択を行うために、式（１）で示したイジングモデルを新たに生成する。ただし、新たなイジングモデルにおいて、 n 個の二値変数 x_i は、選択された部分区間をさらに分割した n 個の新たな部分区間のそれぞれに割り当てられた変数である。また、確率 p_i は、新たな部分区間における確率分布の値である。

[0061] 例えば、入力受付部 102 が、確率分布を表す数式を受付けた場合及び確率分布の種類及びパラメータを受付けた場合には、モデル生成部 103 は、分割数 n 、及び、選択された部分区間の範囲を用いて、新たな部分区間の確率 p_i を特定する。このとき、新たな部分区間において確率分布の値が一定でない場合には、モデル生成部 103 は、例えば、当該部分区間における確率分布の値の平均値、最小値、又は最大値などを用いて、新たな部分区間の確率 p_i を決定してもよい。また、入力受付部 102 は、新たな部分区間の確率 p_i の設定値をそれぞれ指定する入力を受付けてもよい。なお、モデル生成部 103 は、新たな部分区間の確率 p_i の総和が 1 でない場合には、総和が 1 となるように確率 p_i の値を正規化した上で、新たなイジングモデルを生成する。

[0062] 部分区間の階層的な選択を行うために、本実施の形態のアニーリング結果取得部 104 は、処理制御部 101a の制御にしたがい、次のような処理を行う。アニーリング結果取得部 104 は、モデル生成部 103 が、上述した新たなイジングモデルを生成した場合、この新たなイジングモデルについての量子アニーリングの実行結果である n 個の二値変数の値を取得する。取得される n 個の二値変数の値は、細分化された部分区間のうちどの部分区間を選択するべきかを示す。

[0063] 本実施の形態の乱数出力部 106 は、部分区間の階層的な選択が終了すると、最終的に選択された部分区間に含まれる値を乱数として出力する。すなわち、乱数出力部 106 は、新たなイジングモデルについての量子アニーリングの実行結果として得られた値が所定の値（具体的には 1）である二値変数 x_i に割り当てられている新たな部分区間に含まれる値を乱数として出力す

る。なお、本実施の形態では乱数出力部 106 は、選択された部分区間内の所定値（例えば、当該部分区間の中央の値、最大値、又は最小値など）を乱数として出力するが、疑似乱数生成部 105 が生成した値を出力してもよい。

[0064] 次に、乱数生成器 100a の動作の流れについて説明する。

図 6 は、乱数生成器 100a の動作の一例を示すフローチャートである。以下、図 6 を参照しつつ、乱数生成器 100a による乱数の生成動作について説明する。

[0065] ステップ S200 において、図 4 のステップ S100 と同様、入力受付部 102 は、乱数の出力についての設定情報の入力を受付ける。

[0066] 次に、ステップ S201 において、図 4 のステップ S101 と同様、モデル生成部 103 は、ステップ S200 で指定された確率分布に基づいて、イジングモデルを生成する。

[0067] 次に、ステップ S202 において、図 4 のステップ S102 と同様、アニーリング結果取得部 104 は、ステップ S201 で生成したイジングモデルについての量子アニーリングの実行結果を量子アニーリングマシン 200 から取得する。

[0068] 次に、ステップ S203 において、処理制御部 101a は、部分区間の細分化を所定の回数行ったか否かを判定する。すなわち、処理制御部 101a は、部分区間の階層的な選択を q 回行ったか否かを判定する。部分区間の細分化が所定の回数行われていない場合には、処理制御部 101a は、イジングモデルの生成及び量子アニーリングの実行を再度行うよう制御する。すなわち、この場合、処理はステップ S204 へ移行する。これに対し、部分区間の細分化が所定の回数行われた場合には、処理はステップ S205 へ移行する。

[0069] ステップ S204 において、部分区間の階層的な選択を行うために、モデル生成部 103 は、新たな部分区間についてのイジングモデルを生成する。すなわち、モデル生成部 103 は、ステップ S202 において量子アニーリ

ングの実行結果として得られた値が所定の値である二値変数 x_i に割り当てられている部分区間をさらに分割した n 個の新たな部分区間についてのイジングモデルを生成する。ステップS204の処理の後、処理は、ステップS202に戻り、アニーリング結果取得部104は、ステップS204で生成されたイジングモデルについての量子アニーリングの実行結果を量子アニーリングマシン200から取得する。その後、再びステップS203の判定処理が行われる。

[0070] 部分区間の細分化が所定の回数行われると、一つの乱数が得られる。ステップS205では、処理制御部101aは、指定された個数の乱数が得られたか否かを判定する。指定された個数の乱数が得られていない場合には、処理制御部101aは、ステップS202からステップS204の処理を再度行うよう制御する。このとき、ステップS202では、アニーリング結果取得部104は、細分化されていない初期状態の部分区間に割り当てられた二値変数 x_i を用いたイジングモデルについての量子アニーリングの実行結果を取得する。すなわち、以降の処理において、部分区間の階層的な選択が新規に繰り返されることとなる。これに対し、指定された個数の乱数が得られた場合には、処理はステップS206へ移行する。

[0071] ステップS206において、乱数出力部106は、ステップS202からステップS204の処理により得られた乱数を出力する。

[0072] 以上、実施の形態2について説明した。本実施の形態では、部分区間の選択を階層的に繰り返すことにより、より多くの部分区間の中から部分区間が選択される。これにより、量子アニーリングマシン200の量子ビット数が限られていても、より多くの部分区間の中から選択した乱数を出力することができる。

[0073] <実施の形態3>

次に、実施の形態3について説明する。

本実施の形態は、量子アニーリングマシン200が、乱数を生成するための複数のイジングモデルについて同時に量子アニーリングを行う点で、上述

した実施の形態と異なっている。量子アニーリングマシン200が備える量子ビット数に余裕があれば、量子アニーリングマシン200は、複数のイジングモデルについての解を得ることが可能である。そこで、本実施の形態では、複数のイジングモデルに対する1回の量子アニーリングの実行により、効率的に複数の乱数を得ることができる乱数生成器100bについて説明する。

[0074] 図7は、実施の形態3にかかる乱数生成システム10bの構成の一例を示すブロック図である。図7に示すように、実施の形態3にかかる乱数生成システム10bは、乱数生成器100が乱数生成器100bに置き換わった点で、実施の形態1にかかる乱数生成システム10と異なっている。なお、図7に示した構成では、乱数生成器100bは、疑似乱数生成部105を備えるが、乱数生成器100bが部分区間内の所定値を乱数として出力する場合には、疑似乱数生成部105が省略されてもよい。

以下、実施の形態1と異なる構成及び処理について説明し、実施の形態1と同様な構成及び処理については適宜説明を省略する。

[0075] 図7に示されるように、実施の形態3にかかる乱数生成器100bは、主に、モデル生成部103がモデル生成部103bに置き換わり、アニーリング結果取得部104がアニーリング結果取得部104bに置き換わった点で、実施の形態1にかかる乱数生成器100と異なっている。なお、図7に示した構成においても、量子アニーリングマシン200は、乱数生成器100bとは別の装置として図示されているが、乱数生成器100bに含まれてもよい。

[0076] モデル生成部103bは、モデル生成部103と同様、入力受付部102が受付けた確率分布に基づいてイジングモデルを生成する。本実施の形態においても、モデル生成部103bは、式(1)で表されるモデル $H(x)$ を生成する。ただし、モデル生成部103bは、同時に量子アニーリングが実行される複数のイジングモデルを生成する。ここでは、同時に量子アニーリングが実行されるイジングモデルの数を s (s は2以上の整数)とする。つ

まり、モデル生成部 103b は、 s 個のイジングモデルを生成する。ここで、 s 個のイジングモデルは同一であってもよいし、異なってもよい。このため、各イジングモデルは、二値変数 x_i の数（つまり、 n の値）が異なってもよいし、確率値 p_i の値（つまり、確率分布）が異なってもよいし、二値変数 x_i に割り当てられる部分区間が異なってもよい。説明のため、 s 個のイジングモデルにおける二値変数 x_i の総数を t とする。なお、それぞれのイジングモデルにおける二値変数の数 x_i を n_1 、 n_2 、 $\dots$ 、 n_s とすると、 $t = n_1 + n_2 + \dots + n_s$ となる。ここで、 n_1 、 n_2 、 $\dots$ 、 n_s がいずれも 2 以上の整数であるとする、 s が 2 以上の整数であることを考慮すると、 t は 4 以上の整数である。

[0077] モデル生成部 103b が生成した s 個のイジングモデルの合計 t 個の二値変数 x_i のそれぞれは、異なる量子ビットに対応付けられることとなる。このため、量子アニーリングマシン 200 が備える量子ビットの数を k とすると、 t の値は k 以下である。

[0078] アニーリング結果取得部 104b は、 s 個のイジングモデルにおける二値変数 x_i の集合である t 個の二値変数 x_i を同一の量子アニーリングマシン 200 の t 個の量子ビットに対応させる。量子アニーリングマシン 200 は、 s 個のイジングモデルについての量子アニーリングを同時に実行し、 s 個のイジングモデルの解を得る。これにより、アニーリング結果取得部 104b は、 s 個のイジングモデルについての量子アニーリングの実行結果である t 個の二値変数 x_i の値を取得する。

[0079] 次に、乱数生成器 100b の動作の流れについて説明する。

図 8 は、乱数生成器 100b の動作の一例を示すフローチャートである。以下、図 8 を参照しつつ、乱数生成器 100b による乱数の生成動作について説明する。

[0080] ステップ S300 において、図 4 のステップ S100 と同様、入力受付部 102 は、乱数の出力についての設定情報の入力を受付ける。本ステップにおいて、入力受付部 102 は、複数のイジングモデルそれぞれを生成するた

めに必要な情報を受付ける。

[0081] 次に、ステップS 3 0 1において、モデル生成部1 0 3 bは、ステップS 3 0 0で指定された確率分布に基づいて、複数のイジングモデルを生成する。

[0082] 次に、ステップS 3 0 2において、アニーリング結果取得部1 0 4 bは、ステップS 3 0 1で生成した複数のイジングモデルについての同時に実行された量子アニーリングの結果を量子アニーリングマシン2 0 0から取得する。すなわち、アニーリング結果取得部1 0 4 bは、各イジングモデルの二値変数 x_i の値を取得する。これにより、各イジングモデルにおいて、部分区間の選択が可能となる。

[0083] 次に、ステップS 3 0 3において、疑似乱数生成部1 0 5は、ステップS 3 0 2で取得した実行結果に基づいて選択される部分区間内で、疑似乱数を生成する。疑似乱数生成部1 0 5は、生成したイジングモデル毎に疑似乱数を生成する。

[0084] 次に、ステップS 3 0 4において、処理制御部1 0 1は、指定された個数の乱数が得られたか否かを判定する。本実施の形態では、複数のイジングモデルについての量子アニーリングを同時に行っているため、ステップS 3 0 2及びステップS 3 0 3の処理を1回行うだけで、複数の乱数を得ることができる。しかしながら、それでも得られた乱数の数が指定された個数に達していない場合には、再度、量子アニーリングを行う。このため、指定された個数の乱数が得られていない場合には、処理制御部1 0 1は、ステップS 3 0 2及びステップS 3 0 3の処理を再度行うよう制御する。これに対し、指定された個数の乱数が得られた場合には、処理はステップS 3 0 5へ移行する。

[0085] ステップS 3 0 5において、乱数出力部1 0 6は、ステップS 3 0 2及びステップS 3 0 3の処理により得られた乱数を出力する。

[0086] 以上、実施の形態3について説明した。本実施の形態では、複数のイジングモデルについて同時に実行された量子アニーリングの結果を用いて乱数が

生成される。このため、量子アニーリングマシン 200 を用いた効率的な乱数の生成が可能となる。

[0087] なお、本実施の形態は、実施の形態 2 と組み合わせることができる。すなわち、本実施の形態において、実施の形態 2 と同様に、部分区間の選択を階層的に繰り返してもよい。この場合、モデル生成部 103b は、部分区間を細分化した新たな部分区間に割り当てられる二値変数を用いた新たなイジングモデルを、s 個の既存のイジングモデル毎に 1 つずつ生成する。そして、アニーリング結果取得部 104b は、さらに s 個の新たなイジングモデルについての量子アニーリングの実行結果である t 個の二値変数の値を取得する。

[0088] なお、本発明は上記実施の形態に限られたものではなく、趣旨を逸脱しない範囲で適宜変更することが可能である。例えば、上述した乱数生成器を含む情報処理装置は、生成した乱数を用いた所定の処理を行う処理部を有してもよい。例えば、処理部は、乱数を用いる公知の所定の暗号化処理を行ってもよいし、モンテカルロシミュレーションなどの乱数を用いるシミュレーション処理を行ってもよい。なお、この処理部も、例えば、プロセッサがメモリに格納されたプログラムを実行することにより実現されてもよい。

[0089] なお、上述した実施の形態では、イジングモデルに対する量子アニーリングの実行結果を用いて乱数の生成を行ったが、量子アニーリングの代わりにシミュレーティッドアニーリングの実行結果が用いられてもよい。

[0090] 以上、実施の形態を参照して本願発明を説明したが、本願発明は上記によって限定されるものではない。本願発明の構成や詳細には、発明のScope内で当業者が理解し得る様々な変更をすることができる。

[0091] この出願は、2021年1月22日に出願された日本出願特願2021-008663を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0092] 1 乱数生成器

- 2 入力受付部
- 3 モデル生成部
- 4 アニーリング結果取得部
- 5 乱数出力部
- 10 乱数生成システム
 - 10a 乱数生成システム
 - 10b 乱数生成システム
 - 100 乱数生成器
 - 100a 乱数生成器
 - 100b 乱数生成器
 - 101 処理制御部
 - 101a 処理制御部
 - 102 入力受付部
 - 103 モデル生成部
 - 103b モデル生成部
 - 104 アニーリング結果取得部
 - 104b アニーリング結果取得部
 - 105 疑似乱数生成部
 - 106 乱数出力部
- 150 ネットワークインタフェース
 - 151 メモリ
 - 152 プロセッサ
- 200 量子アニーリングマシン

請求の範囲

- [請求項1] 乱数の確率分布を指定する入力を受付ける入力受付手段と、
乱数の数値範囲を分割した n (n は 2 以上の整数) 個の部分区間のそれぞれに割り当てられる n 個の二値変数を用いたイジングモデルを、前記確率分布に基づいて生成するモデル生成手段と、
前記イジングモデルについての量子アニーリングの実行結果である n 個の前記二値変数の値を取得するアニーリング結果取得手段と、
前記実行結果として得られた値が所定の値である前記二値変数に割り当てられている前記部分区間に含まれる値を乱数として出力する乱数出力手段と
を有する乱数生成器。
- [請求項2] 前記イジングモデルは、前記二値変数についての第一の関数と前記二値変数についての第二の関数とを用いて表されるモデルであり、
前記第一の関数は、前記二値変数が割り当てられた前記部分区間における前記確率分布の値が大きいほど値が小さくなる関数の値と当該二値変数の値との積の総和で表される関数であり、
前記第二の関数は、 n 個の前記二値変数のいずれか一つが前記所定の値である場合に最小値となる関数である
請求項 1 に記載の乱数生成器。
- [請求項3] 前記モデル生成手段は、さらに、前記実行結果として得られた値が前記所定の値である前記二値変数に割り当てられている前記部分区間をさらに分割した n 個の新たな部分区間のそれぞれに割り当てられる n 個の二値変数を用いた新たなイジングモデルを、前記確率分布に基づいて生成し、
前記アニーリング結果取得手段は、さらに前記新たなイジングモデルについての量子アニーリングの実行結果である n 個の前記二値変数の値を取得し、
前記乱数出力手段は、前記新たなイジングモデルについての量子ア

ニーリングの前記実行結果として得られた値が前記所定の値である前記二値変数に割り当てられている前記新たな部分区間に含まれる値を乱数として出力する

請求項 1 又は 2 に記載の乱数生成器。

[請求項4] 同一の前記イジングモデルについての複数回の量子アニーリングの実行結果を取得することにより、複数の乱数を出力する

請求項 1 乃至 3 のいずれか一項に記載の乱数生成器。

[請求項5] 前記モデル生成手段は、 s 個（ s は 2 以上の整数）の前記イジングモデルを生成し、

前記アニーリング結果取得手段は、 s 個の前記イジングモデルにおける前記二値変数の集合である t 個（ t は 4 以上の整数）の前記二値変数を同一の量子アニーリングマシンの t 個の量子ビットに対応させることにより、 s 個の前記イジングモデルについての量子アニーリングの実行結果である t 個の前記二値変数の値を取得する

請求項 1 乃至 4 のいずれか一項に記載の乱数生成器。

[請求項6] 前記実行結果として得られた値が前記所定の値である前記二値変数に割り当てられている前記部分区間に収まる疑似乱数を生成する疑似乱数生成手段をさらに有し、

前記乱数出力手段は、前記実行結果にしたがって選択された前記部分区間における前記疑似乱数を出力する

請求項 1 乃至 5 のいずれか一項に記載の乱数生成器。

[請求項7] 前記部分区間を指定する入力を受付ける

請求項 1 乃至 6 のいずれか一項に記載の乱数生成器。

[請求項8] 乱数生成器が、

乱数の確率分布を指定する入力を受け、

乱数の数値範囲を分割した n （ n は 2 以上の整数）個の部分区間のそれぞれに割り当てられる n 個の二値変数を用いたイジングモデルを、前記確率分布に基づいて生成し、

前記イジングモデルについての量子アニーリングの実行結果である
n 個の前記二値変数の値を取得し、

前記実行結果として得られた値が所定の値である前記二値変数に割
り当てられている前記部分区間に含まれる値を乱数として出力する
乱数生成方法。

[請求項9]

乱数の確率分布を指定する入力を受付ける入力受付ステップと、

乱数の数値範囲を分割した n (n は 2 以上の整数) 個の部分区間の
それぞれに割り当てられる n 個の二値変数を用いたイジングモデルを
、前記確率分布に基づいて生成するモデル生成ステップと、

前記イジングモデルについての量子アニーリングの実行結果である
n 個の前記二値変数の値を取得するアニーリング結果取得ステップと
、

前記実行結果として得られた値が所定の値である前記二値変数に割
り当てられている前記部分区間に含まれる値を乱数として出力する乱
数出力ステップと

をコンピュータに実行させるプログラムが格納された非一時的なコ
ンピュータ可読媒体。

[図1]

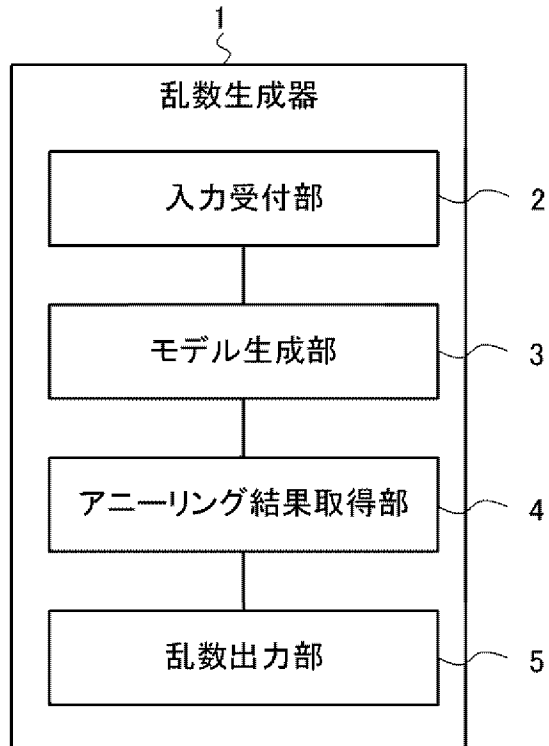


Fig. 1

[図2]

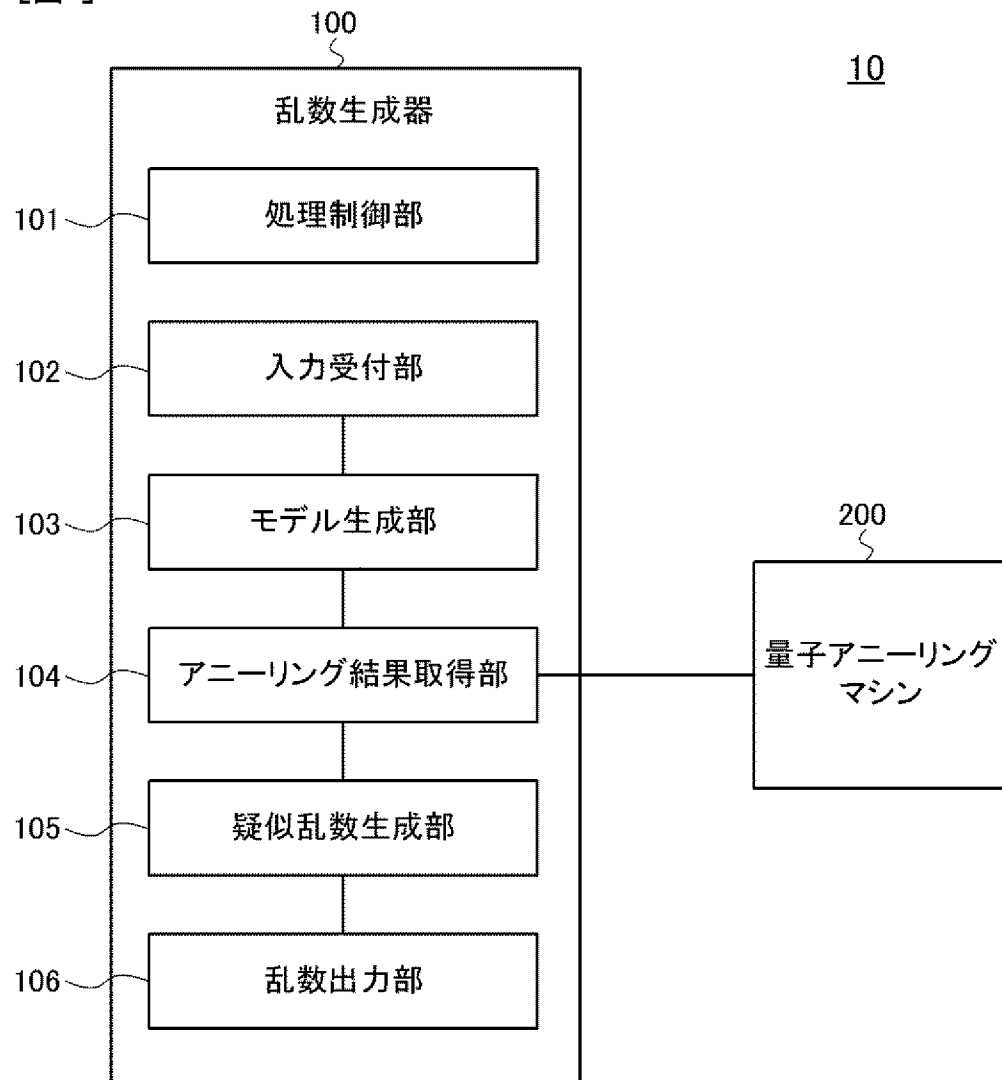


Fig. 2

[図3]

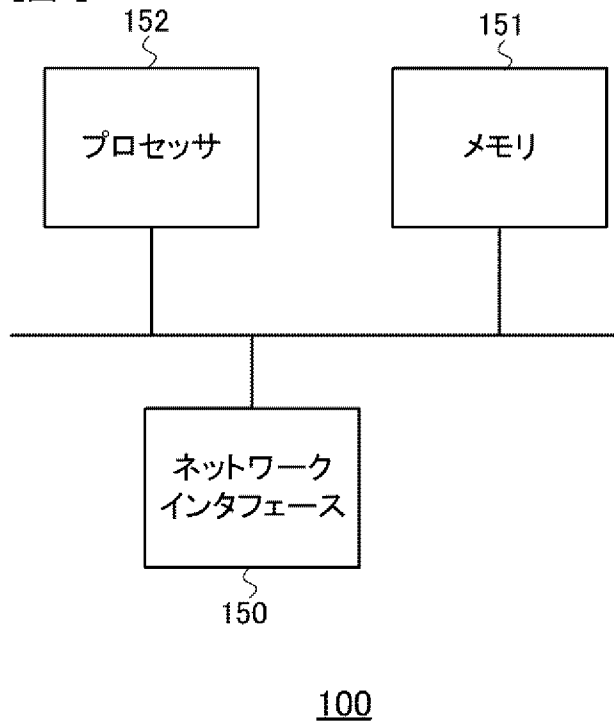


Fig. 3

[図4]

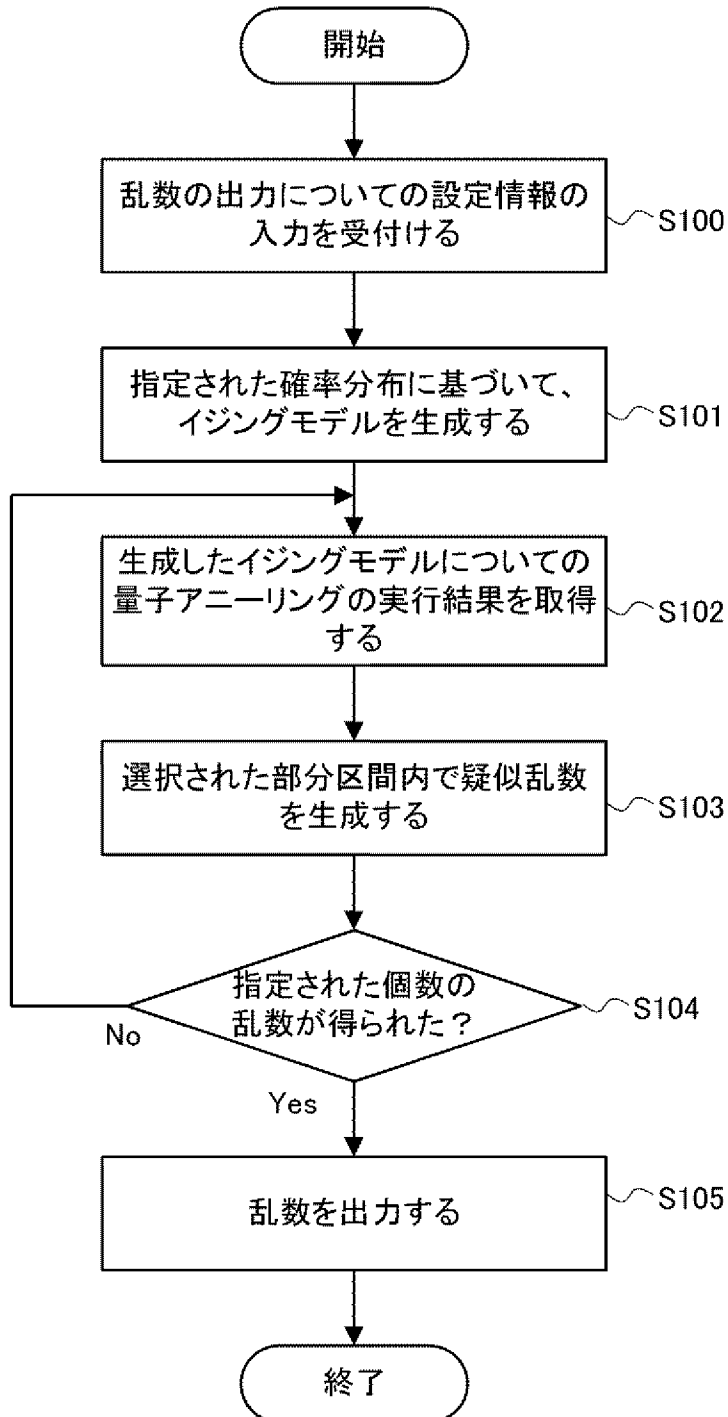


Fig. 4

[図5]

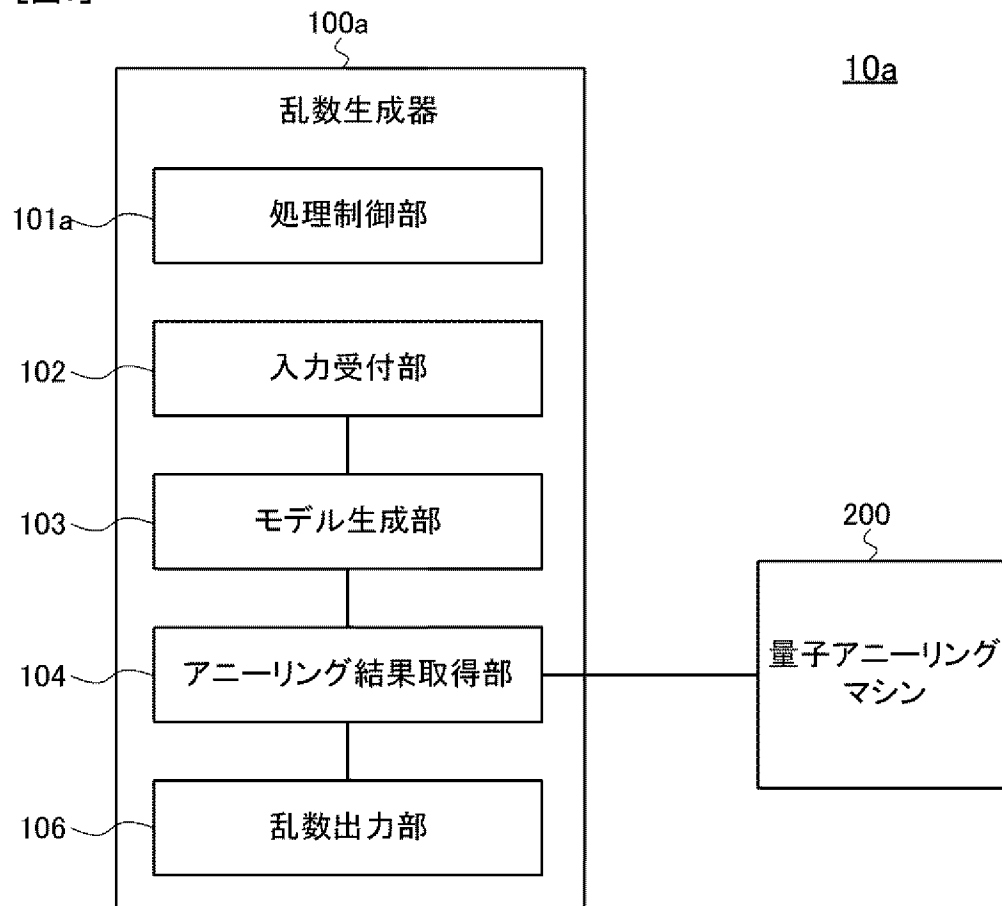


Fig. 5

[図6]

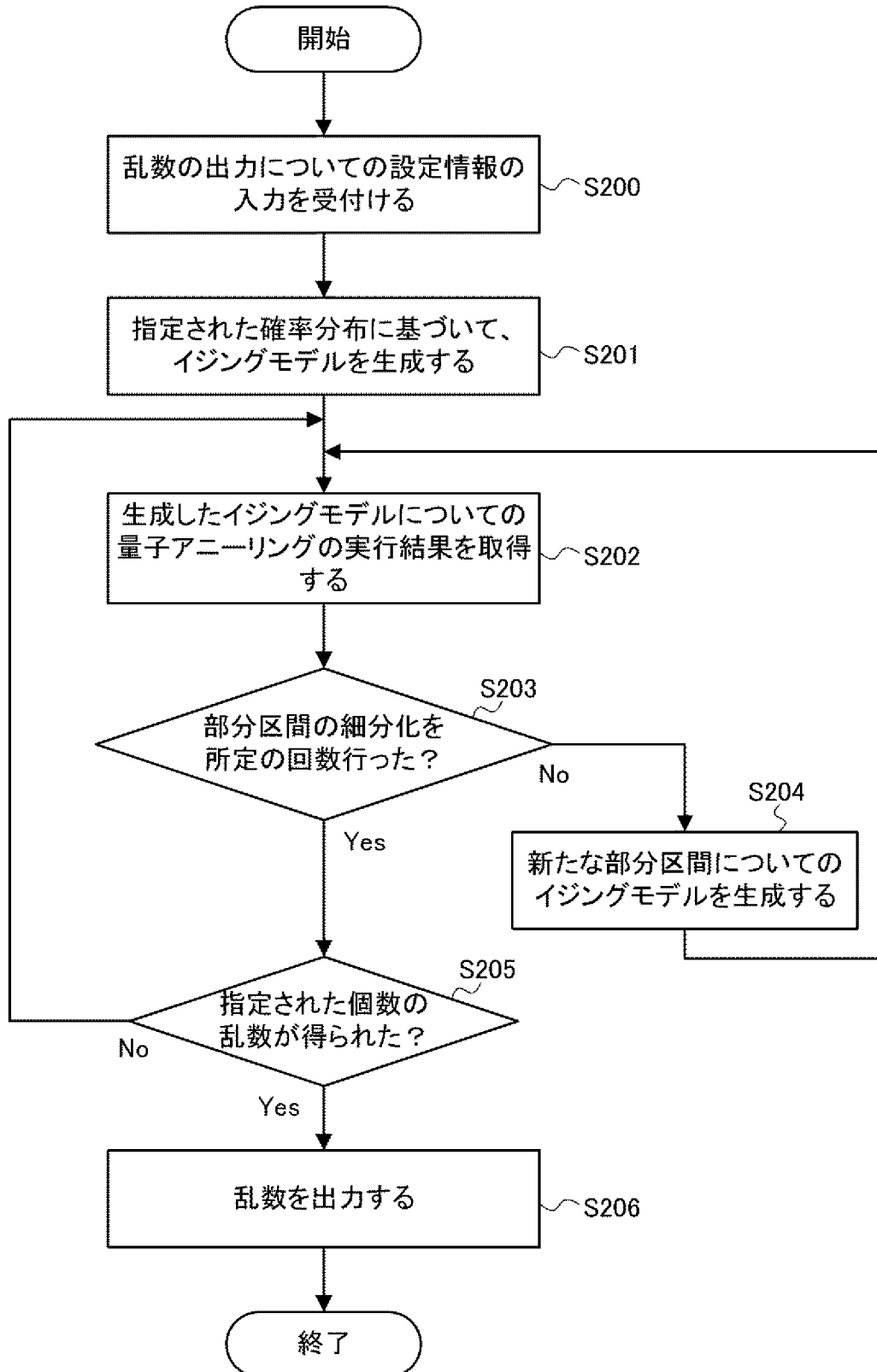


Fig. 6

[図7]

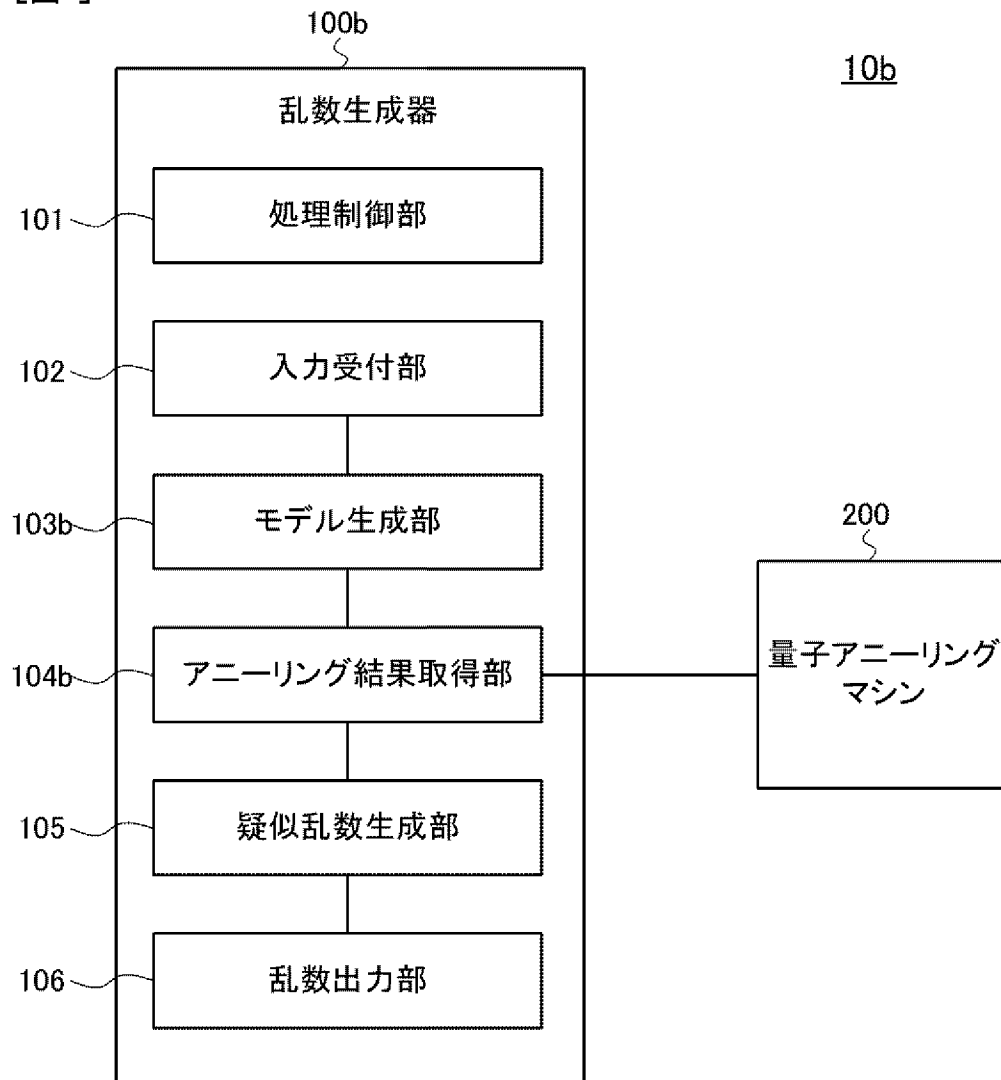


Fig. 7

[図8]

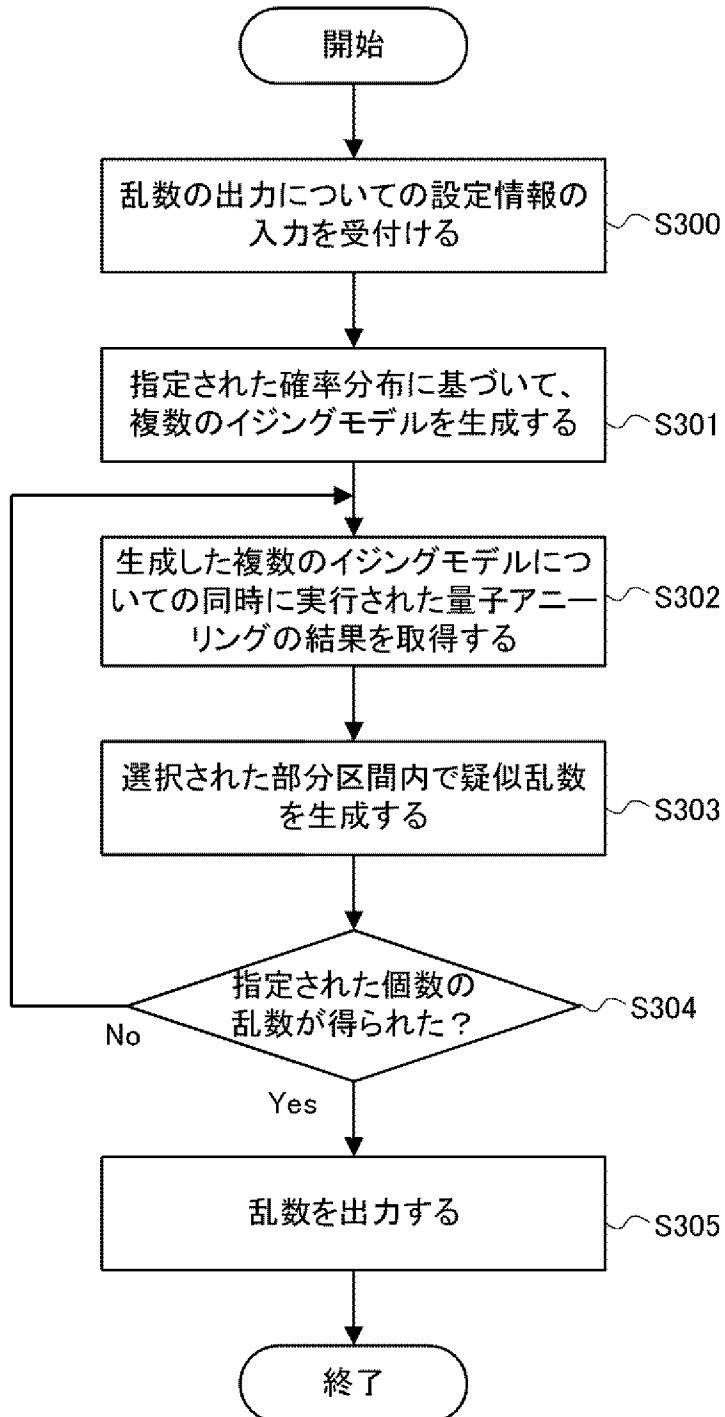


Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2021/042759

A. CLASSIFICATION OF SUBJECT MATTER**G06F 7/58**(2006.01)i; **G06F 17/18**(2006.01)i; **G06N 10/00**(2022.01)i

FI: G06F7/58 680; G06N10/00; G06F17/18 Z

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)

G06F7/58; G06N10/00; G06F17/18

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

Published examined utility model applications of Japan 1922-1996

Published unexamined utility model applications of Japan 1971-2022

Registered utility model specifications of Japan 1996-2022

Published registered utility model applications of Japan 1994-2021

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	WO 2020/170410 A1 (TOSHIBA KK) 27 August 2020 (2020-08-27) entire text, all drawings	1-9
A	JP 2003-323292 A (NTT DOCOMO INC.) 14 November 2003 (2003-11-14) entire text, all drawings	1-9

☐ 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

14 January 2022

Date of mailing of the international search report

25 January 2022

Name and mailing address of the ISA/JP

Japan Patent Office (ISA/JP)
3-4-3 Kasumigaseki, Chiyoda-ku, Tokyo 100-8915
Japan

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/JP2021/042759

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO	2020/170410	A1	27 August 2020	US 2021/0383266 A1 entire text, all drawings CA 3130883 A1	
JP	2003-323292	A	14 November 2003	(Family: none)	

A. 発明の属する分野の分類（国際特許分類（IPC）） G06F 7/58(2006.01)i; G06F 17/18(2006.01)i; G06N 10/00(2022.01)i FI: G06F7/58 680; G06N10/00; G06F17/18 Z														
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（IPC）） G06F7/58; G06N10/00; G06F17/18 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 <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922 - 1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971 - 2022年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996 - 2022年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994 - 2022年</td> </tr> </table> 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）			日本国実用新案公報	1922 - 1996年	日本国公開実用新案公報	1971 - 2022年	日本国実用新案登録公報	1996 - 2022年	日本国登録実用新案公報	1994 - 2022年				
日本国実用新案公報	1922 - 1996年													
日本国公開実用新案公報	1971 - 2022年													
日本国実用新案登録公報	1996 - 2022年													
日本国登録実用新案公報	1994 - 2022年													
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	WO 2020/170410 A1 (株式会社 東芝) 27.08.2020 (2020 - 08 - 27) 全文, 全図	1-9												
A	JP 2003-323292 A (株式会社エヌ・ティ・ティ・ドコモ) 14.11.2003 (2003 - 11 - 14) 全文, 全図	1-9												
☐ 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。														
<table border="0"> <tr> <td>* 引用文献のカテゴリー</td> <td>“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの</td> </tr> <tr> <td>“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの</td> <td>“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</td> </tr> <tr> <td>“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</td> <td>“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</td> </tr> <tr> <td>“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）</td> <td>“&” 同一パテントファミリー文献</td> </tr> <tr> <td>“O” 口頭による開示、使用、展示等に言及する文献</td> <td></td> </tr> <tr> <td>“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</td> <td></td> </tr> </table>			* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの	“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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	“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	“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	“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）	“&” 同一パテントファミリー文献	“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	
* 引用文献のカテゴリー	“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抵触するものではなく、発明の原理又は理論の理解のために引用するもの													
“A” 特に関連のある文献ではなく、一般的な技術水準を示すもの	“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													
“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	“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													
“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）	“&” 同一パテントファミリー文献													
“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														
国際調査を完了した日	国際調査報告の発送日													
14.01.2022	25.01.2022													
名称及びあて先 日本国特許庁(ISA/JP) 〒100-8915 日本国 東京都千代田区霞が関三丁目4番3号	権限のある職員（特許庁審査官） 豊田 真弓 5E 8386 電話番号 03-3581-1101 内線 3521													

国際調査報告
パテントファミリーに関する情報

国際出願番号

PCT/JP2021/042759

引用文献			公表日	パテントファミリー文献			公表日
WO	2020/170410	A1	27.08.2020	US	2021/0383266	A1	
				全文, 全図			
				CA	3130883	A1	
				(ファミリーなし)			
JP	2003-323292	A	14.11.2003				