

【公報種別】特許法第 17 条の 2 の規定による補正の掲載  
 【部門区分】第 6 部門第 3 区分  
 【発行日】令和 2 年 8 月 27 日 (2020.8.27)

【公表番号】特表 2019-523492 (P2019-523492A)  
 【公表日】令和 1 年 8 月 22 日 (2019.8.22)  
 【年通号数】公開・登録公報 2019-034  
 【出願番号】特願 2019-502642 (P2019-502642)  
 【国際特許分類】

**G 0 6 F 21/14 (2013.01)**

【F I】

G 0 6 F 21/14

【手続補正書】

【提出日】令和 2 年 7 月 14 日 (2020.7.14)

【手続補正 1】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

体の元に計算を実行する計算デバイスであって、体加算及び体乗算が前記体に定義される計算デバイスにおいて、

符号化体元を格納するオペランドストアであって、符号化体元が、前記体の元を符号化形態で表し、符号化体元が、少なくとも 2 つの異なる符号化、すなわち、

前記少なくとも 2 つの異なる符号化のうちの第 1 の符号化であって、前記符号化体元が表され、前記第 1 の符号化における前記符号化体元が、2 つの元のリストとして表され、前記符号化体元が、前記 2 つの元の間の差である、第 1 の符号化と、

前記少なくとも 2 つの異なる符号化のうちの第 2 の符号化であって、前記符号化体元が指数を表す 2 つの元のリストとして表され、前記符号化体元が、前記体の生成元を前記 2 つの元の間の差で累乗したものであり、前記体の前記元に実行されている計算を隠すために、前記オペランドストア内の少なくともいくつかの体元が前記第 1 の符号化によって符号化され、前記オペランドストア内の少なくともいくつかの体元が前記第 2 の符号化によって符号化される、第 2 の符号化と、

のうちの一方によって符号化される、オペランドストアと、

複数の演算子ユニットを含む演算子モジュールであって、前記複数の演算子ユニットが

、  
 前記第 1 の符号化によって符号化された体元を受け取り、前記第 2 の符号化によって再符号化された同じ体元を生成する第 1 の変換演算子ユニット、

前記第 2 の符号化によって符号化された体元を受け取り、前記第 1 の符号化によって再符号化された同じ体元を生成する第 2 の変換演算子ユニット、

加算演算子ユニットの集合であって、前記第 1 の符号化によって符号化された 2 つの体元を加算する、加算演算子ユニットの集合、及び

乗算演算子ユニットの集合であって、前記乗算演算子ユニットの集合が、前記指数を加算することによって、前記第 2 の符号化によって符号化された前記 2 つの体元を乗算する、乗算演算子ユニットの集合を含む、演算子モジュールと、

前記第 1 の符号化又は前記第 2 の符号化によって両方とも符号化された第 1 の符号化体元及び第 2 の符号化体元をオペランドストアから受け取り、

前記第 1 の符号化体元及び前記第 2 の符号化体元を、

加算では、前記第 2 の符号化によって符号化された任意の符号化体元に前記第 2 の変換演算子ユニットを適用し、前記加算演算子ユニットの集合を適用し、

乗算では、前記第 1 の符号化によって符号化された任意の符号化体元に前記第 1 の変換演算子ユニットを適用し、前記乗算演算子ユニットの集合を適用することによって選択的に加算するか又は乗算する、計算マネージャとを含む、計算デバイス。

【請求項 2】

前記加算演算子ユニットの集合及び前記乗算演算子ユニットの集合が、符号化体元及びパラメータを受け取り、

前記符号化体元及び前記パラメータに固定計算を実行し、それにより、新しい符号化体元を生成する

少なくとも 1 つの 2 項演算子ユニットを含む、請求項 1 に記載の計算デバイス。

【請求項 3】

前記第 1 の変換演算子ユニット及び前記第 2 の変換演算子ユニットが単項であり、並びに／又は

前記加算演算子ユニットの集合及び前記乗算演算子ユニットの集合のうちの少なくとも 1 つの演算子ユニットが単項であり、

単項演算子ユニットが、符号化体元を受け取り、

前記符号化体元に固定計算を実行し、それにより、新しい符号化体元を生成する、請求項 1 又は 2 に記載の計算デバイス。

【請求項 4】

第 1 の 1 対 1 マッピングが、前記加算演算子ユニットの集合と前記乗算演算子ユニットの集合との間で定義され、加算に適用される前記加算演算子ユニットの集合内の演算ユニットのシーケンスが、乗算に適用される前記乗算演算子ユニットの集合内の演算ユニットのシーケンスへの前記第 1 の 1 対 1 マッピングによって 1 対 1 でマップされる、請求項 1 から 3 のいずれか一項に記載の計算デバイス。

【請求項 5】

第 2 の 1 対 1 マッピングが、入力元と、前記加算演算子ユニットの集合内の 2 項演算子の出力元及びパラメータ並びに前記入力元と、前記乗算演算子ユニットの集合内の 2 項演算子の出力元及びパラメータとの間で定義される、請求項 1 から 4 のいずれか一項に記載の計算デバイス。

【請求項 6】

前記加算演算子ユニットの集合及び前記乗算演算子ユニットの集合が、2 項上昇演算子ユニットを含み、前記上昇演算子ユニットが、

前記第 1 の符号化又は前記第 2 の符号化によって符号化された体元を受け取ることであって、前記符号化が、第 1 の体元及び第 2 の体元の表現を含む、受け取ること、及びパラメータ体元を受け取ることと、

第 1 の体元体とパラメータの逆数との乗算を計算し、第 2 の体元体と前記パラメータの前記逆数との乗算を計算することであって、前記新しい符号化体元が、前記 2 つの計算の結果によって表される、計算することとを行い、並びに／又は

前記加算演算子ユニットの集合及び前記乗算演算子ユニットの集合が、2 項下降演算子ユニットを含み、前記下降演算子ユニットが、

前記第 1 の符号化又は前記第 2 の符号化によって符号化された体元を受け取ることであって、前記符号化が、第 1 の体元及び第 2 の体元の表現を含む、受け取ること、及びパラメータ体元を受け取ることと、

前記第 1 の体元体と前記パラメータとの乗算を計算し、前記第 2 の体元体と前記パラメータとの乗算を計算することであって、前記新しい符号化体元が、前記 2 つの計算の結果によって表される、計算することと  
を行う、請求項 1 に記載の計算デバイス。

【請求項 7】

前記加算演算子ユニットの集合及び前記乗算演算子ユニットの集合が、単項ボックス演算子ユニットを含み、前記ボックス演算子ユニットが、

前記第 1 の符号化又は前記第 2 の符号化によって符号化された体元を受け取ることであって、前記符号化が、第 1 の体元及び第 2 の体元の表現を含む、受け取ること、及びパラメータ体元を受け取ることと、

前記符号化体元に固定増分を加えたものの符号反転を符号化形態で得ることと  
を行う、請求項 1 又は 6 に記載の計算デバイス。

【請求項 8】

第 1 の符号化体元が、変換の後に必要ならば、1 番目の第 1 の体元及び 1 番目の第 2 の体元の表現を含み、前記第 2 の符号化体元が、変換の後に必要ならば、2 番目の第 1 の体元及び 2 番目の第 2 の体元の表現を含み、前記加算演算子ユニットの集合の適用及び前記乗算演算子ユニットの集合の適用が、

パラメータの前記 2 番目の第 1 の体元をもつ前記上昇演算子ユニット、  
ボックス演算子ユニット、

パラメータの前記 2 番目の第 1 の体元をもつ前記下降演算子ユニット、  
パラメータの前記 2 番目の第 2 の体元をもつ前記上昇演算子ユニット、  
ボックス演算子ユニット、

パラメータの前記 2 番目の第 2 の体元をもつ前記下降演算子ユニット  
を含む、請求項 6 に従属する請求項 7 に記載の計算デバイス。

【請求項 9】

前記演算子モジュールが、複数の前記演算子ユニットを実施するルックアップテーブルを格納する記憶装置を含む、請求項 1 から 8 のいずれか一項に記載の計算デバイス。

【請求項 10】

第 1 の符号化の前記 2 つの体元のリストが、指数として表され、前記 2 つの体元が、指数によって示された体の共通基底元の累乗の前記指数である、請求項 1 から 9 のいずれか一項に記載の計算デバイス。

【請求項 11】

前記第 2 の符号化によって符号化された符号化体元は、対応する前記指数が特別な元に等しい場合、数 0 を表す、請求項 1 から 10 のいずれか一項に記載の計算デバイス。

【請求項 12】

前記第 2 の符号化における前記符号化体元が、2 つの元のリストとして表され、符号化体元が、前記体の生成元を前記 2 つの元の間の差で累乗したものであり、

第 2 のタイプの符号化体元における元が、 $n$  を前記体の元の数として、

【数 26】

$$\mathbb{Z}_{n-1}$$

のうちの 1 つ又は複数と、前記特別な元とからなる第 2 の符号化集合に制限され、  
オプションとして、

第 1 のタイプの符号化体元における元が、第 1 の符号化集合に制限され、前記第 1 の符号化集合が前記体の差集合であり、前記第 1 の符号化集合及び前記第 2 の符号化集合が同じサイズを有する、請求項 11 に記載の計算デバイス。

【請求項 13】

前記演算子モジュールが、

前記第 1 の符号化によって符号化された体元を受け取り、前記第 1 の符号化によって再符号化された同じ体元を生成する第 1 のダミー変換演算ユニット、及び／又は

前記第 2 の符号化によって符号化された体元を受け取り、前記第 2 の符号化によって再符号化された同じ体元を生成する第 2 のダミー変換演算ユニットを含む、請求項 1 から 12 のいずれか一項に記載の計算デバイス。

【請求項 14】

体の元に計算を実行する計算デバイスであって、体加算及び体乗算が前記体に定義される計算デバイスにおいて、

符号化体元を格納するオペランドストアであって、符号化体元が、前記体の元を符号化形態で表し、符号化体元が、少なくとも 2 つの異なる符号化、すなわち、

前記少なくとも 2 つの異なる符号化のうちの第 1 の符号化であって、前記符号化体元が表され、前記第 1 の符号化における前記符号化体元が、2 つの元のリストとして表され、前記符号化体元が、前記 2 つの元の間の差である、第 1 の符号化と、

前記少なくとも 2 つの異なる符号化のうちの第 2 の符号化であって、前記符号化体元が指数を表す 2 つの元のリストとして表され、前記符号化体元が、前記体の生成元を前記 2 つの元の間の差で累乗したものであり、前記体の前記元に行われている計算を隠すために、前記オペランドストア内の少なくともいくつかの体元が前記第 1 の符号化によって符号化され、前記オペランドストア内の少なくともいくつかの体元が前記第 2 の符号化によって符号化される、第 2 の符号化と、

のうちの一方によって符号化される、オペランドストアと、

前記第 1 の符号化又は前記第 2 の符号化によって両方とも符号化された第 1 の符号化体元及び第 2 の符号化体元を受け取る入力インタフェースと、

プロセッサ回路とを含み、

前記プロセッサ回路が、

前記第 1 の符号化によって符号化された体元を受け取り、前記第 2 の符号化によって再符号化された同じ体元を生成する第 1 の変換演算子、

前記第 2 の符号化によって符号化された体元を受け取り、前記第 1 の符号化によって再符号化された同じ体元を生成する第 2 の変換演算子、

加算演算子の集合であって、前記第 1 の符号化によって符号化された 2 つの体元を加算する、加算演算子の集合、及び

乗算演算子の集合であって、前記指数を加算することによって、前記第 2 の符号化によって符号化された前記 2 つの体元を乗算する、乗算演算子ユニットの集合を含む複数の演算子と、

前記第 1 の符号化又は前記第 2 の符号化によって両方とも符号化された第 1 の符号化体元及び第 2 の符号化体元を前記オペランドストアから受け取り、

前記第 1 の符号化体元及び前記第 2 の符号化体元を、

加算では、前記第 2 の符号化によって符号化された任意の符号化体元に第 2 の変換演算子ユニットを適用し、加算演算子ユニットの集合を適用し、

乗算では、前記第 1 の符号化によって符号化された任意の符号化体元に第 1 の変換演算子ユニットを適用し、乗算演算子ユニットの集合を適用することによって選択的に加算すること又は乗算することを含む、計算デバイス。

【請求項 15】

体の元に計算を実行する計算方法であって、体加算及び体乗算が体に定義される計算方法において、

符号化体元を格納するステップであって、符号化体元が、前記体の元を符号化形態で表し、符号化体元が、少なくとも 2 つの異なる符号化、すなわち、

前記少なくとも 2 つの異なる符号化のうちの第 1 の符号化であって、前記符号化体元が表され、前記第 1 の符号化における前記符号化体元が、2 つの元のリストとして表され、前記符号化体元が、前記 2 つの元の間の差である、第 1 の符号化と、

前記少なくとも 2 つの異なる符号化のうちの第 2 の符号化であって、前記符号化体元が指数を表す 2 つの元のリストとして表され、前記符号化体元が、前記体の生成元を前記

2つの元の間の差で累乗したものであり、前記体の前記元に行われている計算を隠すために、少なくともいくつかの体元が前記第1の符号化によって符号化されて格納され、少なくともいくつかの体元が前記第2の符号化によって符号化されて格納される、第2の符号化と、

のうちの一方によって符号化される、格納するステップと、

第1の符号化又は第2の符号化によって両方とも符号化されて格納される第1の符号化体元及び第2の符号化体元を受け取るステップと、

前記第1の符号化体元及び前記第2の符号化体元を、

加算では、前記第2の符号化によって符号化された任意の符号化体元に第2の変換演算子ユニットを適用し、加算演算子ユニットの集合を適用することであって、前記第2の変換演算子ユニットが、前記第2の符号化によって符号化された体元を受け取り、前記第1の符号化によって再符号化された同じ体元を生成し、前記加算演算子ユニットの集合が、前記第1の符号化によって符号化された2つの体元を加算する、適用することと、

乗算では、前記第1の符号化によって符号化された任意の符号化体元に第1の変換演算子ユニットを適用し、乗算演算子ユニットの集合を適用することであって、前記第1の変換演算子ユニットが、前記第1の符号化によって符号化された体元を受け取り、前記第2の符号化によって再符号化された同じ体元を生成し、前記乗算演算子ユニットの集合が、前記指数を加算することによって、前記第2の符号化によって符号化された前記2つの体元を乗算する、適用することと

によって選択的に加算するか又は乗算するステップと  
を有する、計算方法。

【請求項16】

請求項15に記載の方法をプロセッサシステムに実行させる命令を表す一時的又は非一時的データを含む、コンピュータ可読媒体。