

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4075577号
(P4075577)

(45) 発行日 平成20年4月16日(2008.4.16)

(24) 登録日 平成20年2月8日(2008.2.8)

(51) Int.Cl.

F I

G O 6 F 11/10 (2006.01)

G O 6 F 11/10 3 3 O Z

G O 6 F 17/16 (2006.01)

G O 6 F 17/16 Z

請求項の数 10 (全 22 頁)

(21) 出願番号 特願2002-331677 (P2002-331677)
 (22) 出願日 平成14年11月15日(2002.11.15)
 (65) 公開番号 特開2004-164465 (P2004-164465A)
 (43) 公開日 平成16年6月10日(2004.6.10)
 審査請求日 平成16年4月23日(2004.4.23)

(73) 特許権者 000002185
 ソニー株式会社
 東京都港区港南1丁目7番1号
 (74) 代理人 100094053
 弁理士 佐藤 隆久
 (72) 発明者 菅 真紀子
 東京都品川区北品川6丁目7番35号 ソ
 ニー株式会社内

審査官 久保 正典

(56) 参考文献 特開昭60-133600 (JP, A)
 特開平01-196647 (JP, A)
 特開2001-023394 (JP, A)
)

最終頁に続く

(54) 【発明の名称】 演算回路構成装置および演算回路構成用プログラム

(57) 【特許請求の範囲】

【請求項1】

所定のデータに対してそれぞれ異なる複数の第1の演算を含む複数の第2の演算を施す演算回路を設計する、演算回路設計装置であって、

当該演算回路設計装置は、入力手段と、演算特定手段と、回路構成手段とを有するコンピュータを含み、

前記第1の演算は加算であり、前記第2の演算は線形変換の演算であり、

前記入力手段は、前記複数の第1の演算を含む前記複数の第2の演算の内容を入力し、

前記演算特定手段は、前記入力された前記複数の第2の演算内容について、前記複数の線形変換の演算を行う前記複数の加算のうち、同じデータに対して同じ演算を行う前記加算を特定し、

前記回路構成手段は、前記複数の線形変換の演算で共用され前記特定された前記加算を行う第1の演算回路と、前記複数の線形変換のそれぞれを構成する前記加算のうち前記特定された加算以外の演算を行う第2の演算回路とを有する演算回路を構成する、

演算回路構成装置。

【請求項2】

所定のデータに対してそれぞれ異なる複数の第1の演算を含む複数の第2の演算を施す演算回路を設計する、演算回路設計装置であって、

当該演算回路設計装置は、入力手段と、演算生成手段と、演算特定手段と、回路構成手段とを有するコンピュータを含み、

10

20

前記第 1 の演算が前記所定のデータに対して第 1 の線形変換をそれぞれ異なる所定の回数施す複数の演算であり、前記第 2 の演算が前記複数の第 1 の演算のそれぞれについて前記所定の回数に対応する数の前記第 1 の線形変換を合成した線形変換の演算であり、

前記入力手段が、当該構成すべき演算回路が行う演算の入力および出力、および、当該構成すべき演算回路が行うそれぞれ所定回数に対応する数の第 1 の線形変換をデータに施す複数の内容を規定するデータを入力し、

前記演算生成手段は、前記入力された当該構成すべき演算回路が行う複数の演算のそれぞれについて前記所定の回数に対応する数の第 1 の線形変換を合成して得られる第 2 の線形変換の演算を生成し、

前記演算特定手段は、前記演算生成手段において生成された前記複数の第 2 の線形変換を構成する前記複数の第 2 の演算のうち、同じデータに対して同じ演算を行う前記第 2 の演算を特定し、

前記回路構成手段は、前記複数の第 2 の線形演算で共用され、前記演算特定手段により特定された前記第 2 の演算を行う第 1 の演算回路と、前記複数の第 1 の演算のそれぞれを構成する前記第 2 の演算のうち前記回路特定手段により特定された前記第 2 の演算を除く演算を行う第 2 の演算回路とを有する演算回路を構成する、

演算回路構成装置。

【請求項 3】

前記回路構成手段は、前記演算特定手段で規定された前記第 2 の線形変換を基に、前記所定のデータに対して前記複数の第 1 の演算を並列に行うように前記演算回路を構成する、

請求項 2 に記載の演算回路構成装置。

【請求項 4】

前記所定データは、所定の線形空間上の所定の基底により、ベクトルで表現されたものであり、

前記線形変換は、前記線形空間上で規定された変換である、

請求項 3 に記載の演算回路構成装置。

【請求項 5】

前記所定の線形空間を下記 (1-1) で示し、前記所定の基底として下記 (1-2) に示す基底を用い、下記 (1-2) に示す基底を基に前記所定のデータであるデータ a が下記 (1-3) のように示されるとき、当該データ a を m 次元ベクトルとして下記 (1-4) で示し、前記第 1 の線形変換を下記 (1-1) に示す線形空間上の線形変換 D とし、前記複数の演算の結果であるデータ b を k 次元ベクトルとして下記 (1-5) で示し、下記 (1-5) に示すデータ b を構成する各演算の結果を示すデータ b_i を d_i 次元ベクトルとして下記 (1-6) で示した場合に、

前記演算特定手段 (34) は、 d_i 行 m 列の行列 D で構成され前記第 2 の線形変換を行う下記 (1-7) で示される行列 M を規定し、

前記演算特定手段は、前記記憶手段で規定した下記 (1-7) を基に、前記複数の第 2 の演算のうち、同じデータに対して同じ演算を行う前記第 2 の演算を特定する、

請求項 2 に記載の演算回路構成装置。

ここで、m、 d_i は 2 以上の整数であり、前記複数の演算の少なくとも一つに対応する前記所定の回数が 2 以上であり、k は 2 以上の整数である。

【数 1】

$$\text{線形空間 } F_{g^m} \quad (1-1)$$

【数 2】

$$\{\gamma_1, \gamma_2, \dots, \gamma_m\} \quad (1-2)$$

【数 3】

$$a = a_1 \gamma_1 + a_2 \gamma_2 + \cdots + a_m \gamma_m \quad (1-3)$$

【数 4】

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ \vdots \\ a_m \end{pmatrix} \quad (1-4)$$

10

【数 5】

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ \vdots \\ b_k \end{pmatrix} \quad (1-5)$$

【数 6】

$$b_i = \begin{pmatrix} b_{i,1} \\ b_{i,2} \\ \vdots \\ \vdots \\ b_{i,di} \end{pmatrix} \quad (1-6)$$

20

【数 7】

$$M = \begin{pmatrix} D \\ D^2 \\ \vdots \\ \vdots \\ D^K \end{pmatrix} \quad (1-7)$$

30

【請求項 6】

前記所定の基底として下記（1 - 8）に示す基底を用い、前記データ a が下記（1 - 9）のように示されるとき、前記データ a を m 次元ベクトルとして下記（1 - 10）の示す

40

請求項 5 に記載の演算回路構成装置。

【数 8】

$$\{1, \gamma, \gamma^2, \cdots, \gamma^{m-1}\} \quad (1-8)$$

【数 9】

$$a = a_0 + a_1 \gamma + a_2 \gamma^2 + a_3 \gamma^3 + \cdots + a_{m-1} \gamma^{m-1} \quad (1-9)$$

【数 10】

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ \vdots \\ a_{m-1} \end{pmatrix} \quad (1-10)$$

【請求項 7】

10

前記演算生成手段は、前記線形空間上の元 を基に r 倍の演算を行う前記行列 D で構成された前記行列 M を生成する、

請求項 5 に記載の演算回路構成装置。

【請求項 8】

前記コンピュータは出力手段 (32) をさらに有し、

前記出力手段 (32) は、前記回路構成手段 (34) で構成された前記演算回路を示す情報を出力する、

請求項 1 ~ 7 のいずれかに記載の演算回路構成装置。

【請求項 9】

所定のデータに対してそれぞれ異なる複数の第 1 の演算を含む複数の第 2 の演算を施す演算回路を設計するために、入力手段と、演算特定手段と、回路構成手段とを有するコンピュータで実行される演算回路構成用プログラムであって、

20

前記第 1 の演算は加算であり、前記第 2 の演算は線形変換の演算であり、

前記入力手段が、前記複数の第 1 の演算を含む前記複数の第 2 の演算の内容を入力する処理を行う第 1 の手順と、

前記演算特定手段が、前記入力された前記複数の第 2 の演算内容について、前記複数の線形変換の演算を行う前記複数の加算のうち、同じデータに対して同じ演算を行う前記加算を特定する処理を行う第 2 の手順と、

前記回路構成手段が、前記複数の線形変換の演算で共用され前記特定された前記加算を行う第 1 の演算回路と、前記複数の線形変換のそれぞれを構成する前記加算のうち前記特定された加算以外の演算を行う第 2 の演算回路とを有する演算回路を構成する処理を行う第 3 の手順と、

30

有する、演算回路構成用プログラム。

【請求項 10】

所定のデータに対してそれぞれ異なる複数の第 1 の演算を含む複数の第 2 の演算を施す演算回路を設計するため、入力手段と、演算生成手段と、演算特定手段と、回路構成手段とを有するコンピュータで実行される演算回路構成用プログラムであって、

前記第 1 の演算が前記所定のデータに対して第 1 の線形変換をそれぞれ異なる所定の回数施す複数の演算であり、前記第 2 の演算が前記複数の第 1 の演算のそれぞれについて前記所定の回数に対応する数の前記第 1 の線形変換を合成した線形変換の演算であり、

40

前記入力手段が、当該構成すべき演算回路が行う演算の入力および出力、および、当該構成すべき演算回路が行うそれぞれ所定回数に対応する数の第 1 の線形変換をデータに施す複数の内容を規定するデータを入力する処理を行う第 1 の手順と、

前記演算生成手段が、前記入力された当該構成すべき演算回路が行う複数の演算のそれぞれについて前記所定の回数に対応する数の第 1 の線形変換を合成して得られる第 2 の線形変換の演算を生成する処理を行う第 2 の手順と、

前記演算特定手段が、前記演算生成手段における処理によって生成された前記複数の第 2 の線形変換を構成する前記複数の第 2 の演算のうち、同じデータに対して同じ演算を行う前記第 2 の演算を特定する処理を行う第 3 の手順と、

前記回路構成手段が、前記複数の第 2 の線形演算で共用され、前記演算特定手段により

50

特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記第2の演算のうち前記回路特定手段における処理により特定された前記第2の演算を除く演算を行う第2の演算回路とを有する演算回路を構成する処理を行う第4の手順と、

を有する、演算回路構成用プログラム。

【発明の詳細な説明】

【0001】

【発明が属する技術分野】

本発明は、例えば、誤り訂正符号や復号などを行う場合に用いられる線形変換などの演算を行う演算回路を構成する演算回路構成装置および演算回路構成用プログラムに関する。

10

【0002】

【従来の技術】

例えば、ハミング符号などの誤り訂正符号や復号では、有限体上で規定された線形空間で種々の線形変換の演算が行われる。

このような線形変換の演算は、例えば、線形空間上の所定の基底により、線形空間上の元をベクトルで表現し、このベクトルに対して線形変換の演算を施して新たなベクトルを得る。

上述した誤り訂正符号や復号では、例えば、複数ビットの所定データに対してそれぞれ異なる線形変換の複数の演算を行なう場合がある。

20

従来では、例えば、上記複数の演算をそれぞれ独立して行なうように演算回路を構成（設計）している。

【0003】

【発明が解決しようとする課題】

しかしながら、上述したように、上記複数の演算をそれぞれ独立して行なうように演算回路を構成すると、演算回路が大規模になるという問題がある。

【0004】

本発明は上述した従来技術の問題点に鑑みてなされ、所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、当該演算回路を小規模に構成できる演算回路構成装置および演算回路構成用プログラムを提供することを目的とする。

30

【0005】

【課題を解決するための手段】

本発明によれば、所定のデータに対してそれぞれ異なる複数の第1の演算を含む複数の第2の演算を施す演算回路を設計する、演算回路設計装置であって、当該演算回路設計装置は、入力手段と、演算特定手段と、回路構成手段とを有するコンピュータを含み、前記第1の演算は加算であり、前記第2の演算は線形変換の演算であり、前記入力手段は、前記複数の第1の演算を含む前記複数の第2の演算の内容を入力し、前記演算特定手段は、前記入力された前記複数の第2の演算内容について、前記複数の線形変換の演算を行う前記複数の加算のうち、同じデータに対して同じ演算を行う前記加算を特定し、前記回路構成手段は、前記複数の線形変換の演算で共用され前記特定された前記加算を行う第1の演算回路と、前記複数の線形変換のそれぞれを構成する前記加算のうち前記特定された加算以外の演算を行う第2の演算回路とを有する演算回路を構成する、演算回路構成装置が提供される。

40

【0006】

上記演算回路構成装置において、演算特定手段が、複数の第1の演算のそれぞれを構成する複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する。

次いで、回路構成手段が、前記複数の第1の演算で共用され前記第1の工程で特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記複数の第2の演算のうち前記第1の工程で特定された前記第2の演算以外の演算を行

50

う第2の演算回路とからなる前記演算回路を構成する。

【0007】

また本発明によれば、所定のデータに対してそれぞれ異なる複数の第1の演算を含む複数の第2の演算を施す演算回路を設計する、演算回路設計装置であって、当該演算回路設計装置は、入力手段と、演算生成手段と、演算特定手段と、回路構成手段とを有するコンピュータを含み、前記第1の演算が前記所定のデータに対して第1の線形変換をそれぞれ異なる所定の回数施す複数の演算であり、前記第2の演算が前記複数の第1の演算のそれぞれについて前記所定の回数に対応する数の前記第1の線形変換を合成した線形変換の演算であり、前記入力手段が、当該構成すべき演算回路が行う演算の入力および出力、および、当該構成すべき演算回路が行うそれぞれ所定回数に対応する数の第1の線形変換をデータに施す複数の内容を規定するデータを入力し、前記演算生成手段は、前記入力された当該構成すべき演算回路が行う複数の演算のそれぞれについて前記所定の回数に対応する数の第1の線形変換を合成して得られる第2の線形変換の演算を生成し、前記演算特定手段は、前記演算生成手段において生成された前記複数の第2の線形変換を構成する前記複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定し、前記回路構成手段は、前記複数の第2の線形演算で共用され、前記演算特定手段により特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記第2の演算のうち前記回路特定手段により特定された前記第2の演算を除く演算を行う第2の演算回路とを有する演算回路を構成する、演算回路構成装置が提供される。

【0008】

本発明によれば、所定のデータに対してそれぞれ異なる複数の第1の演算を含む複数の第2の演算を施す演算回路を設計するために、入力手段と、演算特定手段と、回路構成手段とを有するコンピュータで実行される演算回路構成用プログラムであって、前記第1の演算は加算であり、前記第2の演算は線形変換の演算であり、前記入力手段が、前記複数の第1の演算を含む前記複数の第2の演算の内容を入力する処理を行う第1の手順と、前記演算特定手段が、前記入力された前記複数の第2の演算内容について、前記複数の線形変換の演算を行う前記複数の加算のうち、同じデータに対して同じ演算を行う前記加算を特定する処理を行う第2の手順と、前記回路構成手段が、前記複数の線形変換の演算で共用され前記特定された前記加算を行う第1の演算回路と、前記複数の線形変換のそれぞれを構成する前記加算のうち前記特定された加算以外の演算を行う第2の演算回路とを有する演算回路を構成する処理を行う第3の手順と、有する、演算回路構成用プログラムが提供される。

【0009】

また本発明によれば、所定のデータに対してそれぞれ異なる複数の第1の演算を含む複数の第2の演算を施す演算回路を設計するため、入力手段と、演算生成手段と、演算特定手段と、回路構成手段とを有するコンピュータで実行される演算回路構成用プログラムであって、前記第1の演算が前記所定のデータに対して第1の線形変換をそれぞれ異なる所定の回数施す複数の演算であり、前記第2の演算が前記複数の第1の演算のそれぞれについて前記所定の回数に対応する数の前記第1の線形変換を合成した線形変換の演算であり、前記入力手段が、当該構成すべき演算回路が行う演算の入力および出力、および、当該構成すべき演算回路が行うそれぞれ所定回数に対応する数の第1の線形変換をデータに施す複数の内容を規定するデータを入力する処理を行う第1の手順と、前記演算生成手段が、前記入力された当該構成すべき演算回路が行う複数の演算のそれぞれについて前記所定の回数に対応する数の第1の線形変換を合成して得られる第2の線形変換の演算を生成する処理を行う第2の手順と、前記演算特定手段が、前記演算生成手段における処理によって生成された前記複数の第2の線形変換を構成する前記複数の第2の演算のうち、同じデータに対して同じ演算を行う前記第2の演算を特定する処理を行う第3の手順と、前記回路構成手段が、前記複数の第2の線形演算で共用され、前記演算特定手段により特定された前記第2の演算を行う第1の演算回路と、前記複数の第1の演算のそれぞれを構成する前記第2の演算のうち前記回路特定手段における処理により特定された前記第2の演算を除

く演算を行う第2の演算回路とを有する演算回路を構成する処理を行う第4の手順と、を有する、演算回路構成用プログラムが提供される。

【0010】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

〔本発明の関連技術〕

図1は、本発明の関連技術に係わる演算回路101の構成図である。

演算回路101は、データaを入力として、データ $b_1 \sim b_k$ を出力する。

演算回路101は、 i を $1 \sim k$ を満たす2以上の自然数、 l_i を自然数とした場合に、各系統で行列 $M_{i,1} \sim M_{i,l_i}$ によって規定された演算 $C_{i,1} \sim C_{i,l_i}$ を順に行う複数系統の演算回路モジュールを有し、これらの演算回路モジュールで並列に演算を行う。

10

各演算モジュールは、演算 $C_{i,1} \sim C_{i,l_i}$ をそれぞれ行う複数の演算回路 $2i1_j$ を直接に接続して構成される。

演算回路101は、線形空間上の基底によりベクトル表現されたデータaを入力し、演算回路 $2i1_1 \sim 2i1_{l_i}$ でデータaに線形演算を施し、演算回路 $2i1_1 \sim 2i1_{l_i}$ からそれぞれ $b_1 \sim b_k$ を出力する。

【0011】

図1に示す演算回路1は、各演算回路モジュール内の演算 $C_{i,1} \sim C_{i,l_i}$ を図2に示すように合成した演算回路モジュール $i1_j$ (j は2以上の整数)を用いた演算回路201のように構成することで、小規模化および高速化が図れる。

20

この場合に、図2および下記(2-1)に示すように規定された線形変換列が、下記(2-2)に示すように合成される。

【0012】

【数11】

$$\begin{aligned} &\{C_{1,1}, C_{1,2}, \dots, C_{1,l_1}\}, \\ &\{C_{2,1}, C_{2,2}, \dots, C_{2,l_2}\}, \\ &\dots \dots \dots \dots \dots \dots \\ &\{C_{k,1}, C_{k,2}, \dots, C_{k,l_k}\}, \end{aligned} \quad (2-1)$$

30

$$\{C_{i,j-1} \text{の値域}\} \subset \{C_{i,j} \text{の定義域}\}$$

【0013】

【数12】

$$\begin{aligned} &C_{1,l_1} \circ \dots \circ C_{1,2} \circ C_{1,1} : a \mapsto b_1 \\ &C_{2,l_2} \circ \dots \circ C_{2,2} \circ C_{2,1} : a \mapsto b_2 \\ &\dots \dots \dots \dots \dots \dots \\ &C_{k,l_k} \circ \dots \circ C_{k,2} \circ C_{k,1} : a \mapsto b_k \end{aligned} \quad (2-2)$$

40

【0014】

このとき、上記(2-1)に示す演算 $C_{i,1} \sim C_{i,l_i}$ を線形変換を行う行列 $M_{i,1} \sim M_{i,l_i}$ とすると、上記(2-1)、(2-2)は、それぞれ下記(2-3)、(2-4)のように示される。

【0015】

【数13】

$$\begin{aligned}
&\{M_{1,1}, M_{1,2}, \dots, M_{1,l}\}, \\
&\{M_{2,1}, M_{2,2}, \dots, M_{2,l}\}, \\
&\dots \dots \dots \dots \dots \dots \\
&\{M_{k,1}, M_{k,2}, \dots, M_{k,k}\},
\end{aligned}
\tag{2-3}$$

【 0 0 1 6 】

【 数 1 4 】

$$\begin{aligned}
M_1 &:= M_{1,l}, \dots, M_{1,2}M_{1,1} : a \mapsto b_1 \\
M_2 &:= M_{2,l}, \dots, M_{2,2}M_{2,1} : a \mapsto b_2 \\
&\dots \\
M_k &:= M_{k,l}, \dots, M_{k,2}M_{k,1} : a \mapsto b_k
\end{aligned}
\tag{2-4}$$

10

【 0 0 1 7 】

これにより、演算回路 2 0 1 を、下記 (2 - 5) に示す行列を行う回路として構成できる。

【 0 0 1 8 】

【 数 1 5 】

$$M := \begin{pmatrix} M_1 \\ M_2 \\ \dots \\ M_k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_k \end{pmatrix}
\tag{2-5}$$

20

【 0 0 1 9 】

次に、入力したデータ F S 0 に対して、第 1 の線形変換 D をそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータ $b_1 \sim b_k$ を出力する演算回路の構成方法について説明する。

図 3 は、このような演算回路 3 0 1、並びにその周辺回路を説明するための図である。

30

【 0 0 2 0 】

図 3 に示すように、セレクタ 3 1 2 において選択信号 S E L を基に、入力データ a とデータ M L S とのうち一方のデータが選択され、当該選択されたデータ F S 0 がレジスタ 3 1 3₀ および演算回路 3 0 1 に出力される。

演算回路 3 0 1 は、セレクタ 1 2 から入力したデータ F S 0 に対して、第 1 の線形変換 D をそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータ $b_1 \sim b_k$ をそれぞれレジスタ 3 1 3₁ ~ 3 1 3_k に出力する。

レジスタ 3 1 3₀ ~ 3 1 3_k は、入力したデータ F S 0 , $b_1 \sim b_k$ を保持し、所定のタイミングで、これらをデータ O U T₀ ~ O U T_k として出力する。

演算回路 3 1 4 は、データ O U T_k を入力し、これに第 1 の線形演算 D を施して、その結果であるデータ M S L をセレクタ 3 1 2 に出力する。

40

【 0 0 2 1 】

演算回路 3 0 1 は、例えば、図 3 に示すように、それぞれ線形変換 D を行う複数の演算回路 3 2 1₁ ~ 3 2 1_k を直列に接続し、データ a を初段の回路 3 2 1₁ に入力し、個々の演算回路 3 2 1₁ ~ 3 2 1_k で生成されたデータ $b_1 \sim b_k$ をレジスタ 3 1 3₁ ~ 3 1 3_k に出力するように構成 (設計) される。

【 0 0 2 2 】

ここで、図 3 に示す演算回路 3 0 1 は、有限体 $F(2^4)$ の元、 $x^2 + x + 1 = 0$ に対して 2 倍演算を行なうものである場合、図 4 に示すように構成される。

この場合に、図 3 に示すように、あるタイミングで入力されたデータ a に対して、デー

50

タ OUT_0 , OUT_1 , OUT_2 は、以下ようになる。

【 0 0 2 3 】

【 表 1 】

OUT_0 :	a ,	$a x^{k+1}$,	$a x^{2k+2}$,	\dots ,
OUT_1 :	$a x$,	$a x^{k+2}$,	$a x^{2k+3}$,	\dots ,
OUT_2 :	$a x^2$,	$a x^{k+3}$,	$a x^{2k+4}$,	\dots ,

【 0 0 2 4 】

ここで、 $FS0 = A0 + A1$ とすると、以下ようになる。

$$FS0 \cdot = A1 + (A0 + A1)$$

$$FS0 \cdot^2 = (A0 + A1) + A0$$

10

【 0 0 2 5 】

従って、図 4 に示す演算回路 321_1 , 321_2 は、図 5 に示すように、それぞれ 1 個の加算回路 351_1 , 351_2 によって構成される。

【 0 0 2 6 】

しかしながら、上述したように、演算回路 301 を設計すると、回路規模が大きくなるという問題がある。

また、演算回路 301 において、データ a を初段の回路 321_1 に入力してから最終段の回路 321_k からデータ b_k が出力されるまでの時間が長くなり、高性能な演算回路 301 を設計できないという問題がある。

【 0 0 2 7 】

20

以下、上述した関連技術の問題点を解決する本発明の実施形態を説明する。

〔 第 1 実施形態 〕

図 6 は、本実施形態の回路構成方法で構成（設計）される演算回路 11 の周辺回路を説明するための図である。

図 6 に示すように、セレクト 12 において選択信号 SEL を基に、入力データ a とデータ $M L S$ とのうち一方のデータが選択され、当該選択されたデータ $FS0$ がレジスタ 13_0 および演算回路 11 に出力される。

演算回路 11 は、セレクト 12 から入力したデータ $FS0$ に対して、第 1 の線形変換 D をそれぞれ異なる所定の回数施す複数の演算を行い、当該演算の結果であるデータ $b_1 \sim b_k$ をそれぞれレジスタ $13_1 \sim 13_k$ に出力する。

30

レジスタ $13_0 \sim 13_k$ は、入力したデータ $FS0$, $b_1 \sim b_k$ を保持し、所定のタイミングで、これらをデータ $OUT_0 \sim OUT_k$ として出力する。

演算回路 14 は、データ OUT_k を入力し、これに第 1 の線形演算 D を施して、その結果であるデータ $M S L$ をセレクト 12 に出力する。

【 0 0 2 8 】

本実施形態の回路構成方法は、図 6 に示す演算回路 11 を構成（設計）するものである。

【 0 0 2 9 】

本実施形態では、所定の線形空間が、 q を素数とした場合に有限体 F_q の m 次拡大であり、その元が F_q 上の m 次ベクトルで表現された場合に、当該所定の線形空間を下記（3 - 1）、あるいは $F(q^m)$ で示す。

40

【 0 0 3 0 】

【 数 1 6 】

線形空間 F_{q^m}

(3-1)

【 0 0 3 1 】

また、所定の基底として下記（3 - 2）に示す基底を用い、下記（3 - 2）に示す基底を基に前記所定のデータであるデータ a を下記（3 - 3）のように示す。

【 0 0 3 2 】

【 数 1 7 】

50

$$\{\gamma_1, \gamma_2, \dots, \gamma_m\} \quad (3-2)$$

【 0 0 3 3 】

【 数 1 8 】

$$a = a_1 \gamma_1 + a_2 \gamma_2 + \dots + a_m \gamma_m \quad (3-3)$$

【 0 0 3 4 】

また、上記データ a を m 次元ベクトルとして下記 (3 - 4) のように示す。

【 0 0 3 5 】

【 数 1 9 】

10

$$a = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix} \quad (3-4)$$

また、上記第 1 の線形変換 D を上記 (3 - 1) に示す線形空間上の線形変換 D とする。

【 0 0 3 6 】

また、上記複数の演算の結果であるデータ b を k 次元ベクトルとして下記 (3 - 5) で示し、下記 (3 - 5) に示すデータ b を構成する各演算の結果を示すデータ b_i を d_i 次元ベクトルとして下記 (3 - 6) で示す。

20

ここで、m, d_i は 2 以上の整数であり、前記複数の演算の少なくとも一つに対応する前記所定の回数が 2 以上であり、k は 2 以上の整数である。

【 0 0 3 7 】

【 数 2 0 】

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} \quad (3-5)$$

30

【 0 0 3 8 】

【 数 2 1 】

$$b_i = \begin{pmatrix} b_{i,1} \\ b_{i,2} \\ \vdots \\ b_{i,d_i} \end{pmatrix} \quad (3-6)$$

40

【 0 0 3 9 】

ここで、上記複数の演算を、それぞれ O P₁ ~ O P_k とすると、これらは下記 (3 - 7) で示される。

【 0 0 4 0 】

【 数 2 2 】

$$\begin{array}{lll}
OP_1: \{D\}, & D: & a \mapsto b_1 \\
OP_2: \{D, D\}, & D^2 := D \circ D: & a \mapsto b_2 \\
OP_3: \{D, D, D\}, & D^3 := D \circ D \circ D: & a \mapsto b_2 \\
\cdots \cdots \cdots \cdots \cdots & \cdots & \\
OP_k: \{D, D, D, \cdots, D\}, & D^k := D \circ D \circ D \circ \cdots \circ D: & a \mapsto b_k
\end{array}$$

(3-7)

10

【 0 0 4 1 】

そして、第 1 の線形変換 D を表す d 行 m 列の行列を M_d とすると、上記 (3-7) は、下記 (3-8) で示される。

【 0 0 4 2 】

【 数 2 3 】

$$\begin{array}{ll}
\{M_d\}, & M_d: a \mapsto b_1 \\
\{M_d, M_d\}, & M_d^2: a \mapsto b_2 \\
\{M_d, M_d, M_d\}, & M_d^3: a \mapsto b_3 \\
\cdots \cdots \cdots & \cdots \\
\{M_d, M_d, M_d, \cdots, M_d\}, & M_d^k: a \mapsto b_k
\end{array} \quad (3-8)$$

20

【 0 0 4 3 】

上記 $OP_1 \sim OP_k$ によって規定される変換列の合成を表した d 行 m 列の行列 $M_d \sim M_d^k$ を縦に並べた $k \cdot d$ 行 m 列の行列 M は、下記 (3-9) で示される。

【 0 0 4 4 】

【 数 2 4 】

$$M := \begin{pmatrix} M_d \\ M_d^2 \\ \cdots \\ M_d^k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \cdots \\ b_k \end{pmatrix} = \begin{pmatrix} D \cdot a \\ D^2 \cdot a \\ \cdots \\ D^k \cdot a \end{pmatrix} \quad (3-9)$$

30

【 0 0 4 5 】

上記 (3-9) に示すように、行列 M が、データ a に対して第 1 の線形変換と、第 2 の変換 $D^2 \sim D^k$ をそれぞれ行う k 個の演算を規定している。

【 0 0 4 6 】

図 7 は、本実施形態の回路構成方法を実行するコンピュータ 29 を説明するための図である。

40

図 7 に示すように、コンピュータ 29 は、例えば、操作部 31、ディスプレイ 32、メモリ 33 および CPU 34 を有し、これらがバス 30 を介して接続されている。

操作部 31 は、キーボードやマウスなどの操作手段であり、CPU 34 にプログラムの実行指示、データ選択指示、並びにデータ入力を行うために用いられる。

ディスプレイ 32 は、CPU 34 の処理結果を表示する。

メモリ 33 は、CPU 34 によって実行されるプログラム 41 と、プログラム 41 の実行に用いられるデータ 42 とを記憶する。

【 0 0 4 7 】

CPU 34 は、プログラム 41 を実行して以下に示す処理を行い、プログラム 41 の実行過程でデータ 42 を用いて、演算回路 11 の回路を構成 (設計) する処理を行う。

50

プログラム 4 1 は、本発明のプログラムに対応し、以下に示す各ステップの内容を示す手順を記述している。

また、CPU 3 4 がプログラム 4 1 を実行することで、本発明の回路構成装置が構成され、CPU 3 4 がステップ S T 1 2 を実行して本発明の第 1 の手段を構成し、CPU 3 4 がステップ S T 1 3 を実行して本発明の第 2 の手段を構成する。

【0048】

以下、本実施形態の回路構成方法の動作例を、CPU 3 4 の処理と関連付けて説明する。

図 8 は、本実施形態の回路構成方法の動作例を説明するためのフローチャートである。

ステップ S T 1 1 :

CPU 3 4 は、例えば、ユーザによる操作部 3 1 の操作に応じて、上記 (3 - 4) , (3 - 5) , (3 - 6) に示すように演算回路 1 1 が行う演算の入力および出力の形式、並びに上記 (3 - 7) に示すように演算回路 1 1 が行うそれぞれ所定の回数に対応する数の第 1 の線形変換 D をデータ a に施す複数の演算の内容を規定するデータを入力する。

【0049】

ステップ S T 1 2 :

CPU 3 4 が、ステップ S T 1 1 で入力した上記 (3 - 7) に示す演算回路 1 1 が行う複数の演算のそれぞれについて、上記所定の回数に対応する数の第 1 の線形変換 D を合成して得られる第 2 の線形変換 (第 1 の演算) を行う上記 (3 - 9) に示す行列 M を生成する (規定する) 処理を行う。

【0050】

ステップ S T 1 3 :

CPU 3 4 が、上記ステップ S T 1 2 で規定された複数の第 2 の線形変換 (第 1 の演算) を構成する複数の第 2 の演算のうち、同じデータに対して同じ演算を行う前記第 2 の演算を特定する。

【0051】

ステップ S T 1 4 :

CPU 3 4 が、複数の第 2 の線形演算 (第 1 の演算) で共用されステップ S T 1 3 で特定された上記第 2 の演算を行う第 1 の演算回路と、上記複数の第 1 の演算のそれぞれを構成する上記複数の第 2 の演算のうちステップ S T 1 3 で特定された上記第 2 の演算以外の演算を行う第 2 の演算回路とからなる図 9 に示す演算回路 1 1 を構成する。

このとき、CPU 3 4 が、上記 (3 - 9) に示すステップ S T 1 2 で生成された (規定された) 行列 M を基に、データ F S 0 に対して第 1 の線形変換 $D \sim D^k$ をそれぞれ行う k 個の演算を並列に行うように演算回路 1 1 の構成 (設計) データを生成する。

具体的には、CPU 3 4 が、図 9 に示すように、データ F S 0 に対して第 1 の線形変換 $D \sim D^k$ をそれぞれ行う演算回路 $21_1 \sim 21_k$ を並列に配置した演算回路 1 1 の構成を示す構成データを生成する。

【0052】

これにより、CPU 3 4 は、入力したデータ F S 0 に上記 (3 - 9) に示す行列 M で規定された線形変換を施し、データ $b_1 \sim b_k$ を出力するように構成された演算回路 1 1 の構成データを生成する。

【0053】

図 9 に示すように演算回路 1 1 を構成することで、レジスタ $13_0 \sim 13_k$ からの出力は、横方向を時間として、図 10 に示すようになる。

すなわち、演算回路 1 から、データ $b_1 \sim b_k$ が略同じタイミングで出力されるため、データ $OUT_0 \sim OUT_k$ も略同じタイミングで出力される。

このとき、演算回路 1 1 が行う行列 M の演算と、演算回路 1 1 に入力されるデータ F S 0 と、データ $OUT_0 \sim OUT_k$ との関係は、下記 (3 - 10) で示される。

【0054】

【数 2 5】

10

20

30

40

50

$$M \cdot FSO = \begin{pmatrix} D \cdot FSO \\ D^2 \cdot FSO \\ D^3 \cdot FSO \\ \vdots \\ D^K \cdot FSO \end{pmatrix} = \begin{pmatrix} OUT_0 \\ OUT_1 \\ OUT_2 \\ \vdots \\ OUT_k \end{pmatrix} \quad (3-10)$$

【 0 0 5 5 】

ここで、上記行列 M は上記 (3 - 1) で規定された線形空間の元によって構成されるため、データ $OUT_1 \sim OUT_K$ (データ $b_1 \sim b_k$) は、上記線形空間の元とデータ FSO の各要素との積、並びにそれらの和として規定される (生成される)。そのため、それらの組み合わせは、高々有限となり、例えば、値 k が値 m に対して大きい場合に、図 8 に示すように、演算回路 1 1 から出力されたデータ b_k を演算回路 1 4 およびセレクタ 1 2 を介して演算回路 1 1 にフィードバックすることで、多様な演算に対応可能な演算回路 1 1 を小規模な構成で構築できる。

10

【 0 0 5 6 】

以下、ここで、図 9 に示す演算回路 1 1 の演算回路 2 1₁ , 2 1_k は、有限体 $F(2^4)$ の元、 $x^2 + x + 1 = 0$ に対して 2 倍演算を行なうものである場合、図 1 1 に示す演算回路 2 2 1 のように構成される。

20

この場合に、図 3 に示すように、あるタイミングで入力されたデータ a に対して、データ OUT_0 , OUT_1 , OUT_2 は、以下のようになる。

【 0 0 5 7 】

$OUT_0 : a, a \times x^{k+1}, a \times x^{2k+2}, \dots,$
 $OUT_1 : a \times x^k, a \times x^{k+2}, a \times x^{2k+3}, \dots,$
 $OUT_2 : a \times x^2, a \times x^{k+3}, a \times x^{2k+4}, \dots,$

すなわち、 $FSO = A_0 + A_1$ とすると、次のクロックサイクルにおけるデータ OUT_0 , OUT_1 , OUT_2 は、以下のようになる。

【 0 0 5 8 】

$OUT_0 : FSO = A_0 + A_1$
 $OUT_1 : FSO \cdot x = A_1 + (A_0 + A_1)$
 $OUT_2 : FSO \cdot x^2 = (A_0 + A_1) + A_0$

30

【 0 0 5 9 】

この場合に、前述した図 8 に示すステップ $ST13$ において、CPU 3 4 が、上記 2 倍演算を構成する複数の第 2 の演算のうち、同じデータに対して同じ演算を行う上記第 2 の演算、すなわち、演算「 $A_0 + A_1$ 」を特定する。

そして、図 8 に示すステップ $ST14$ において、CPU 3 4 が、複数の 2 倍演算 (すなわち、2 倍演算と、 x^2 倍演算) で共用されステップ $ST13$ で特定された演算「 $A_0 + A_1$ 」を行う図 1 1 に示す第 1 の演算回路 1 1 5 (図 1 1 では加算回路) と、複数の 2 倍演算のそれぞれを構成する上記複数の第 2 の演算のうちステップ $ST13$ で特定された上記第 2 の演算以外の演算を行う第 2 の演算回路 (図 1 1 に示す例では無し) とからなる図 1 1 に示す演算回路 1 1 a を構成する。

40

【 0 0 6 0 】

なお、上述した実施形態において、上記第 1 の線形変換が、上記 (3 - 1) で規定した線形空間の元に対して「2 倍演算 ($\times x$)」を行うものである場合には、上記複数の演算を、それぞれ $OP_1 \sim OP_K$ とすると、これらは下記 (3 - 1 1) で示される。

【 0 0 6 1 】

【 数 2 6 】

$$\begin{array}{lll}
OP_1: \{(\times \gamma^1)\}, & (\times \gamma^1): & a \mapsto b_1 \\
OP_2: \{(\times \gamma^1), (\times \gamma^1)\}, & (\times \gamma^1) \circ (\times \gamma^1): & a \mapsto b_2 \\
OP_3: \{(\times \gamma^1), (\times \gamma^1), (\times \gamma^1)\}, & (\times \gamma^1) \circ (\times \gamma^1) \circ (\times \gamma^1): & a \mapsto b_3 \\
\vdots & \vdots & \vdots \\
OP_k: \{(\times \gamma^1), (\times \gamma^1), (\times \gamma^1), \dots, (\times \gamma^1)\}, & (\times \gamma^1) \circ (\times \gamma^1) \circ (\times \gamma^1) \circ \dots \circ (\times \gamma^1): & a \mapsto b_k
\end{array}$$

(3-11)

【 0 0 6 2 】

10

そして、第 1 の線形変換 D を表す d i 行 m 列の行列を M r とすると、上記 (3 - 1 1) は、下記 (3 - 1 2) で示される。

【 0 0 6 3 】

【数 2 7 】

$$\begin{array}{ll}
\{M_r\}, & M_r: a \mapsto b_1 \\
\{M_r, M_r\}, & M_r^2: a \mapsto b_2 \\
\{M_r, M_r, M_r\}, & M_r^3: a \mapsto b_3 \\
\vdots & \vdots \\
\{M_r, M_r, M_r, \dots, M_r\}, & M_r^k: a \mapsto b_k
\end{array} \quad (3-12)$$

20

【 0 0 6 4 】

上記 O P ₁ ~ O P _k によって規定される変換列の合成を表した d i 行 m 列の行列 M r ~ M r ^k を縦に並べた k · d i × m の行列 M r は、下記 (3 - 1 3) で示される。

ここで、M r ^x (x は 1 ~ k を満たす整数) は、x 個の M r を合成した行列である。

【 0 0 6 5 】

【数 2 8 】

$$M := \begin{pmatrix} M_r \\ M_r^2 \\ \vdots \\ M_r^k \end{pmatrix} : a \mapsto \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_k \end{pmatrix} = \begin{pmatrix} \gamma^1 \cdot a \\ \gamma^{2r} \cdot a \\ \vdots \\ \gamma^{kr} \cdot a \end{pmatrix} \quad (3-13)$$

30

【 0 0 6 6 】

上記 (3 - 1 3) に示すように、行列 M が、データ a に対して $\gamma^1 \sim \gamma^{kr}$ 倍演算 ($\times \gamma^r$) をそれぞれ行う k 個の演算を規定している。

【 0 0 6 7 】

この場合には、図 1 2 に示すように、C P U 3 4 が、データ F S 0 に対して $\gamma^1 \sim \gamma^{kr}$ 倍演算 ($\times \gamma^r$) をそれぞれ行う演算回路 2 1 ₁ ~ 2 1 _k を有する演算回路 1 1 の構成を示す構成データを生成する (規定する) 。

40

【 0 0 6 8 】

以上説明したように、本実施形態の回路構成方法では、上述したように図 8 に示すステップ S T 1 3 において、複数の第 1 の演算 (D 倍演算、 γ^r 倍演算) を構成する複数の第 2 の演算のうち、同じデータに対して同じ演算を行う上記第 2 の演算を特定する。

そして、ステップ S T 1 4 において、上記複数の第 1 の演算で共用された上記特定された上記第 2 の演算を行う第 1 の演算回路と、上記複数の第 1 の演算のそれぞれを構成する上記複数の第 2 の演算のうち上記特定された上記第 2 の演算以外の演算を行う第 2 の演算回路とからなる演算回路 1 1 , 1 1 a を構成する。

50

そのため、本実施形態の回路構成方法によれば、演算回路 1 1 , 1 1 a を小規模に構成できる。

【 0 0 6 9 】

また、本実施形態の回路構成方法では、図 8 に示すステップ S T 1 2 で、ステップ S T 1 1 で入力した上記 (3 - 7) に示す演算回路 1 1 が行う複数の演算のそれぞれについて、上記所定の回数に対応する数の第 1 の線形変換 D を合成して得られる第 2 の線形変換 (第 1 の演算) を行う上記 (3 - 9) に示す行列 M を生成し (規定し)、これに対して上述したステップ S T 1 3 , S T 1 4 の処理を行う。

そのため、本実施形態の回路構成方法によれば、演算回路 1 1 , 1 1 a を小規模に構成できると共に、演算時間を短縮できる。

10

また、本実施形態の回路構成方法では、図 9 および図 1 1 に示すように、演算回路 1 1 が、データ F S 0 に対して、第 1 の演算を並列に行うため、演算時間をさらに短縮できる。

すなわち、演算回路 2 1 ₁ ~ 2 1 _k においてデータ F S 0 (データ a) を並列に処理するため、データ b ₁ ~ b _k (データ O U T ₁ ~ O U T _k) の全てを略同じタイミングで得ることができる。

そのため、データ F S 0 を入力してからデータ b ₂ ~ b _k を得るまでの時間を図 3 に示す構成に比べて短縮した演算回路 1 1 を構成 (設計) できる。

【 0 0 7 0 】

〔 第 2 実施形態 〕

20

本実施形態では、有限体 F (2 ⁴) 上の元として扱われる 4 ビットのデータ D (= D [3] , D [2] , D [1] , D [0]) を縦ベクトルと見なし、当該データ D に対して下記 (3 - 1 4) , (3 - 1 5) で示す行列 M 1 , M 2 で示される 2 つの線形変換を施す回路を構成する場合を例示する。

【 0 0 7 1 】

【 数 2 9 】

$$M1 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \quad (3-14)$$

30

【 0 0 7 2 】

【 数 3 0 】

$$M2 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (3-15)$$

【 0 0 7 3 】

従来では、出力値 E 1 = M 1 ・ D、E 2 = M 2 ・ D は、それぞれ縦ベクトルとして表現され、下記 (3 - 1 6) , (3 - 1 7) で示される。

40

【 0 0 7 4 】

【 数 3 1 】

$$\begin{aligned} E1 &= (E1[3], E1[2], E1[1], E1[0]) \\ &= (D[1] + D[2], D[3], D[0] + D[2], D[0] + D[1] + D[3]) \end{aligned} \quad (3-16)$$

【 0 0 7 5 】

【 数 3 2 】

$$\begin{aligned} E2 &= (E2[3], E2[2], E2[1], E2[0]) \\ &= (D[1], D[0], D[0] + D[2] + D[3], D[1] + D[2]) \end{aligned} \quad (3-17)$$

【 0 0 7 6 】

従来の回路構成方法では、図 1 3 に示すように、上記 (3 - 1 6) に示す演算を行う演算回路 4 0 2 と、上記 (3 - 1 7) に示す演算を行う演算回路 4 0 3 とを有する演算回路 4 0 1 が構成される。

演算回路 4 0 2 は、加算回路 4 1 1 , 4 1 2 , 4 1 3 , 4 1 4 で構成される。

また、演算回路 4 0 3 は、加算回路 4 2 1 , 4 2 2 , 4 2 3 で構成される。

【 0 0 7 7 】

本実施形態の回路構成方法は、上記 (3 - 1 4) , (3 - 1 5) に示す行列 M 1 , M 2 によって表現される線形変換を、有限体 $F(2^4)$ 上の元として扱われる 4 ビットのデータ $D(=D[3], D[2], D[1], D[0])$ に施すことは同じである。

本実施形態では、2つの 4×4 行列を用いる代わりに、行列 M 1 と M 2 とを連結した下記 (3 - 1 8) に示される行列 M を用いる。

【 0 0 7 8 】

【数 3 3 】

$$M = \begin{pmatrix} M1 \\ M2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad (3-18)$$

【 0 0 7 9 】

本実施形態の回路構成方法では、上記行列 M の演算を行い、上記 (3 - 1 6) , (3 - 1 7) 内の演算において、行列 M 1 に相当する第 1 の演算と行列 M 2 に相当する第 1 の演算とを構成する複数の第 2 の演算のうち、共通する第 2 の演算である「 $D[0] + D[2]$ 」、並びに「 $D[1] + D[2]$ 」を特定する。

そして、図 1 4 に示すように、第 2 の演算「 $D[0] + D[2]$ 」を行う図 1 3 に示す加算回路 4 1 2 と 4 2 1 と、第 2 の演算「 $D[1] + D[2]$ 」を行う図 1 3 に示す加算回路 4 1 3 と 4 2 2 が共用化され、加算回路 4 1 2 , 4 1 3 が削減され、図 1 3 に示す演算回路 4 0 1 に比べて、回路規模が縮小された演算回路 4 0 3 が構成される。

これにより、図 1 3 に示す演算回路 4 0 1 と同じ演算を行う図 1 4 に示す演算回路 4 0 3 を、演算回路 4 0 1 に比べて小規模に構成できる。

【 0 0 8 0 】

本発明は上述した実施形態には限定されない。

その他の実施形態として、上記所定の基底として下記 (3 - 1 9) に示す基底を用い、上記データ a を下記 (3 - 2 0) のように示し、前記データ a を m 次元ベクトルとして下記 (3 - 2 1) のように示してもよい。

【 0 0 8 1 】

【数 3 4 】

$$\{1, \gamma, \gamma^2, \dots, \gamma^{m-1}\} \quad (3-19)$$

【 0 0 8 2 】

【数 3 5 】

$$a = a_0 + a_1 \gamma + a_2 \gamma^2 + a_3 \gamma^3 + \dots + a_{m-1} \gamma^{m-1} \quad (3-20)$$

10

20

30

40

50

【 0 0 8 3 】

【 数 3 6 】

$$a = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{m-1} \end{pmatrix} \quad (3-21)$$

10

【 0 0 8 4 】

【 発 明 の 効 果 】

以上説明したように、本発明によれば、所定データに対してそれぞれ異なる複数の演算を行なう演算回路を構成する場合に、同じデータについて同じ演算を行う回路を特定して、それを共通回路化することにより、当該演算回路を小規模に構成できる演算回路構成装置および演算回路構成用プログラムを提供することができる。

【 図 面 の 簡 単 な 説 明 】

【 図 1 】 図 1 は、本発明の関連技術を説明するための図である。

【 図 2 】 図 2 は、本発明の関連技術を説明するための図である。

20

【 図 3 】 図 3 は、本発明の関連技術を説明するための図である。

【 図 4 】 図 4 は、本発明の関連技術を説明するための図である。

【 図 5 】 図 5 は、本発明の関連技術を説明するための図である。

【 図 6 】 図 6 は、本発明の第 1 実施形態の回路構成方法で構成（設計）される演算回路の周辺回路を説明するための図である。

【 図 7 】 図 7 は、本発明の第 1 実施形態の回路構成方法を実行するコンピュータを説明するための図である。

【 図 8 】 図 8 は、本発明の第 1 実施形態の回路構成方法の手順によって演算回路を構成する場合を説明するためのフローチャートである。

【 図 9 】 図 9 は、本発明の第 1 実施形態の回路構成方法で構成（設計）される演算回路を説明するための図である。

30

【 図 1 0 】 図 1 0 は、図 9 に示す演算回路のデータ出力タイミングを説明するための図である。

【 図 1 1 】 図 1 1 は、図 9 に示す演算回路の具体例を説明するための図である。

【 図 1 2 】 図 1 2 は、本発明の第 1 実施形態の回路構成方法によって構成される「 $r \sim r^k$ 」倍演算（ \times 「 r 」）を行う演算回路を説明するための図である。

【 図 1 3 】 図 1 3 は、本発明の第 2 実施形態の回路構成方法の関連技術を説明するための図である。

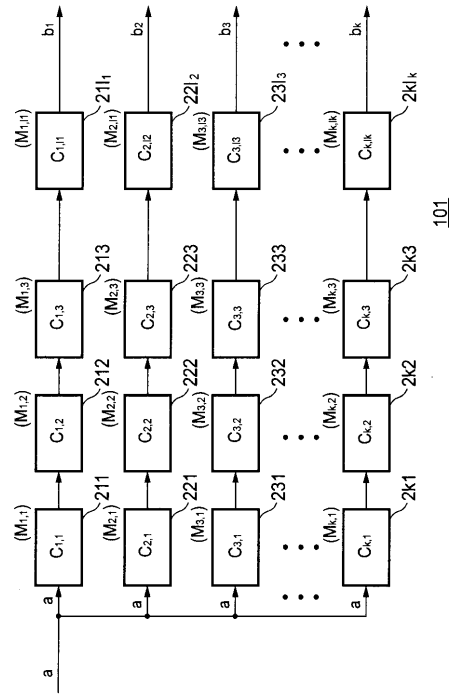
【 図 1 4 】 図 1 4 は、本発明の第 2 実施形態の回路構成方法を説明するための図である。

40

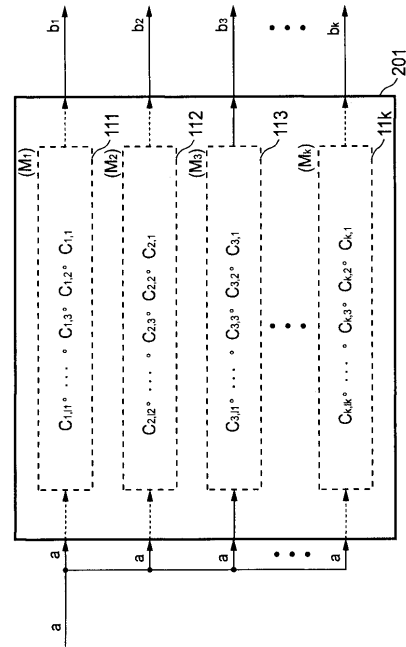
【 符 号 の 説 明 】

1 1 ... 演算回路、1 2 ... セレクタ、1 3₀ ~ 1 3_k ... レジスタ、1 4 ... 演算回路、2 1₁ ~ 2 1_k ... 演算回路、3 0 ... バス、3 1 ... 操作部、3 2 ... ディスプレイ、3 3 ... メモリ、4 1 ... プログラム、4 2 ... データ

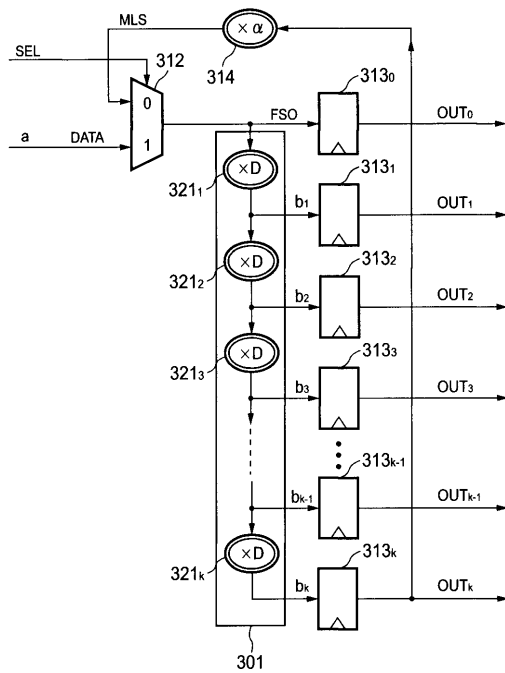
【図 1】



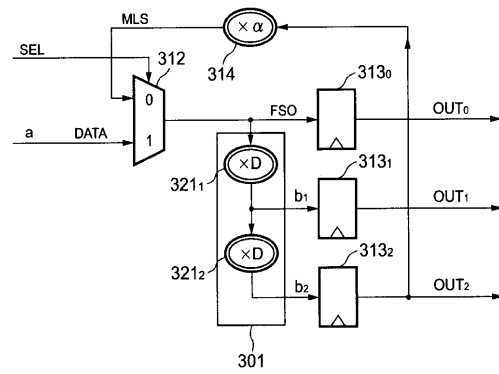
【図 2】



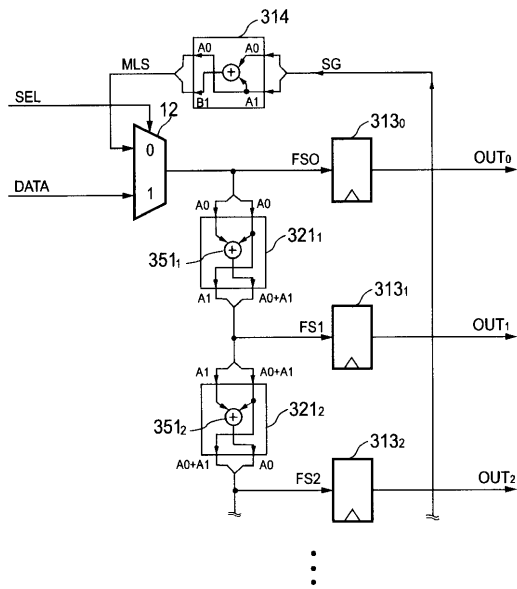
【図 3】



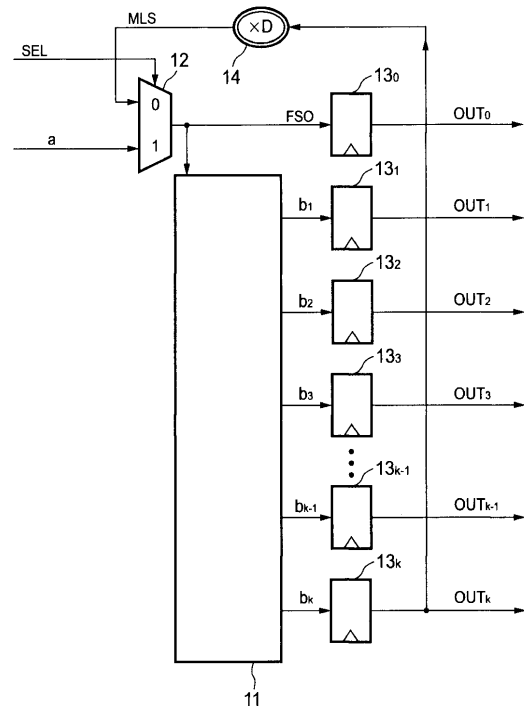
【図 4】



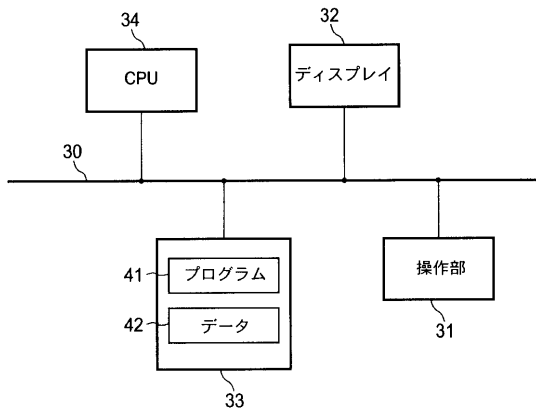
【図 5】



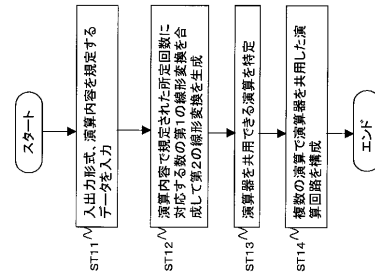
【図 6】



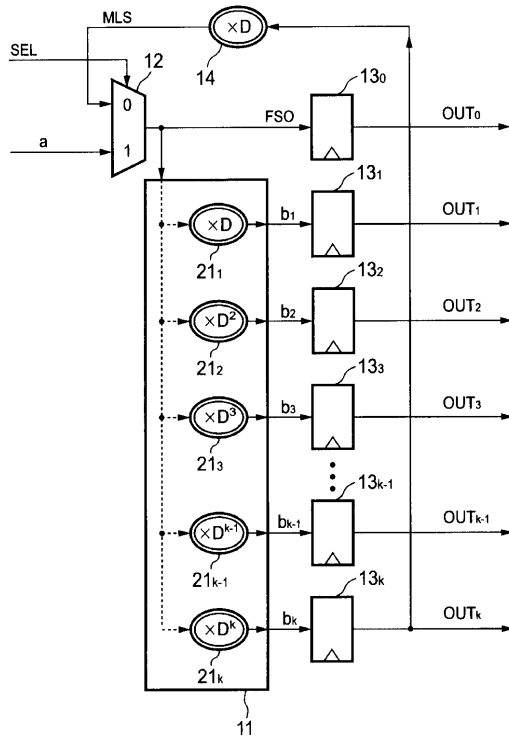
【図 7】



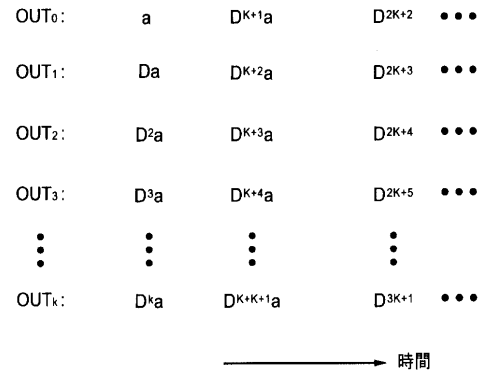
【図 8】



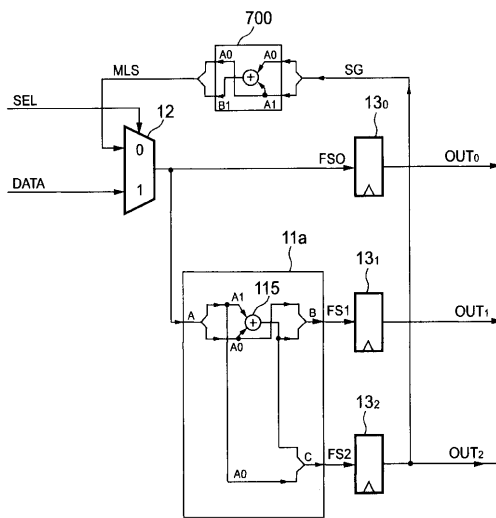
【図 9】



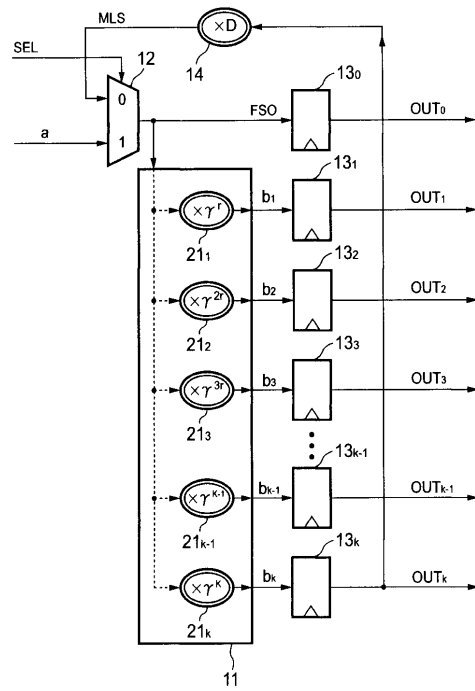
【図 10】



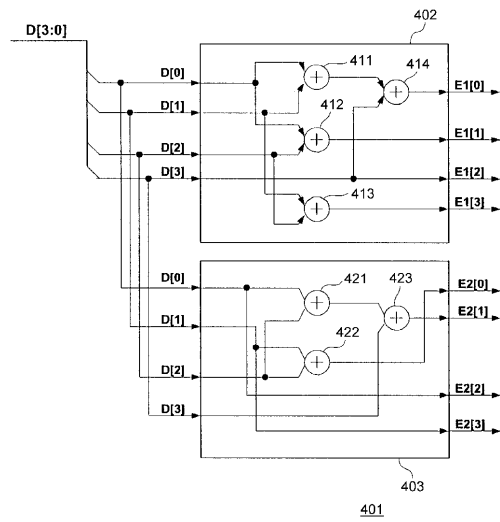
【図 11】



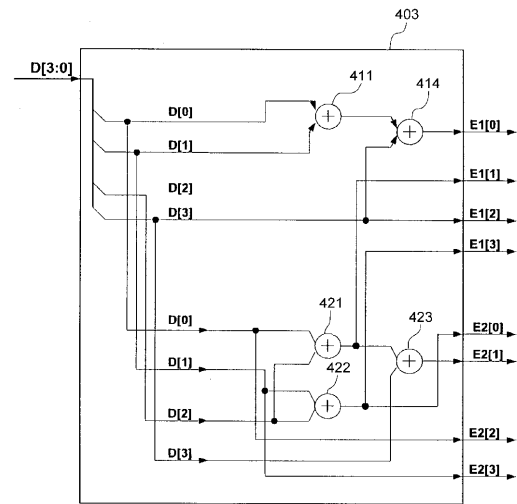
【図 12】



【図 13】



【図 14】



フロントページの続き

(58)調査した分野(Int.Cl. , D B 名)

G06F11/08-11/10

G06F12/16

G06F17/00-17/18