

(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2004-164383

(P2004-164383A)

(43) 公開日 平成16年6月10日(2004.6.10)

(51) Int.Cl.⁷

G06F 7/72

G06F 17/10

G09C 1/00

F I

G06F 7/72

G06F 17/10

G09C 1/00

Z

650Z

テーマコード (参考)

5B056

5J104

審査請求 未請求 請求項の数 7 O L (全 14 頁)

(21) 出願番号 特願2002-330569 (P2002-330569)

(22) 出願日 平成14年11月14日 (2002.11.14)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35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

Fターム(参考) 5B056 BB74

5J104 AA18 AA25 NA16 NA39

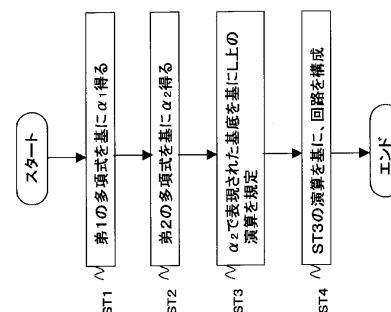
(54) 【発明の名称】 回路構成方法、その方法およびそのプログラム

(57) 【要約】

【課題】有限体上の演算を行う演算回路を従来に比べて少ない回路構成要素で小規模に構成できる回路構成方法を提供する。

【解決手段】第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る(ST1)。第2の有限体から第3の有限体への第2の拡大についての第2の多項式であって、ST1で得られた第1の原始根 α_1 と第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された第2の多項式を基に第2の原始根 α_2 を得る(ST2)。第2の原始根 α_2 を用いて表現された基底を用いて、第3の有限体上の演算を規定して演算回路を構成する(ST3, 4)。

【選択図】 図5



【特許請求の範囲】

【請求項 1】

有限体上の演算を行う演算回路を構成する回路構成方法であって、
 第 1 の有限体から第 2 の有限体への第 1 の拡大についての第 1 の多項式を基に第 1 の原始根 α_1 を得る第 1 の工程と、
 前記第 2 の有限体から前記第 3 の有限体への第 2 の拡大についての第 2 の多項式であって、前記第 1 の工程で得られた前記第 1 の原始根 α_1 と前記第 1 の多項式の 0 次の項の係数とを用いて、0 次の項の係数が規定された前記第 2 の多項式を基に第 2 の原始根 α_2 を得る第 2 の工程と、
 前記第 2 の工程で得られた前記第 2 の原始根 α_2 を用いて表現された基底を用いて、前記第 3 の有限体上の演算を規定する第 3 の工程と、
 前記第 3 の工程で規定された演算を基に、当該演算を行う演算回路を構成する第 4 の工程と
 を有する回路構成方法。

【請求項 2】

前記第 1 の有限体が、有限体 F_q から拡大次数 n の拡大であり、
 前記第 2 の有限体が、前記第 1 の有限体から拡大次数 l_1 の第 1 の拡大であり、
 前記第 3 の有限体が、前記第 2 の有限体から拡大次数 l_2 の第 2 の拡大であり、
 前記第 3 の工程において、下記 (1-1) で示す位数の下記 (1-2) で示す前記第 3 の有限体上の演算を規定する場合に、
 前記第 1 の工程において、前記第 1 の原始根 α_1 を下記 (1-3) を基に得て、
 前記第 2 の工程において、前記第 2 の原始根 α_2 を下記 (1-4) を基に得る
 請求項 1 に記載の回路構成方法。

【数 1】

$$q^{n \cdot l_1 \cdot l_2} (q = p^m, p; \text{素数}, n, l_1, l_2, m; \text{自然数}) \quad \cdots (1-1)$$

【数 2】

$$L := F_{q^{n \cdot l_1 \cdot l_2}} \quad \cdots (1-2)$$

【数 3】

$$\alpha_1: \alpha_1^{l_1} - \alpha_1 + c = 0, \quad X^{l_1} - X + c \in F[X], \text{既約} \quad \cdots (1-3)$$

【数 4】

$$\alpha_2: \alpha_2^{l_2} - \alpha_2 + a = 0, \quad a = c^{-1} \cdot \alpha_1^i \cdot \exists i \in Z, \\ s.t. X^{l_2} - X + a \in K[X], \text{既約} \quad \cdots (1-4)$$

【請求項 3】

前記拡大次数 l_1 と l_2 とが共に q である場合に、
 前記第 1 の工程において、前記第 1 の原始根 α_1 を下記 (1-5), (1-5 a) を基に得て、
 前記第 2 の工程において、前記第 2 の原始根 α_2 を下記 (1-6) を基に得る
 請求項 2 に記載の回路構成方法。

【数 5】

$$\alpha_1: \alpha_1^q - \alpha_1 + c = 0, \quad \exists c \in F \text{ s.t. } Tr_{F_q}^F(c) \neq 0 \quad \cdots (1-5)$$

【数 6】

$$Tr_{F_q}^F(c) := c + c^q + c^{q^2} + \cdots + c^{q^{n-1}} \quad \cdots (1-5a)$$

【数 7】

$$\alpha_2: \alpha_2^q - \alpha_2 + a = 0, \quad \exists a = c^{-1} \cdot \alpha_1^i \in K, \quad 10$$

$$i \in Z \text{ s.t. } Tr_{F_q}^K(\alpha_1^i) \neq 0, \quad \cdots (1-6)$$

【請求項 4】

前記第 3 の工程において、前記第 2 の有限体上の演算を用いて前記第 3 の有限体上の演算を規定し、

前記第 4 の工程において、前記第 3 の工程で用いた前記第 2 の有限体上の演算を行う第 1 の演算回路を構成し、当該第 1 の演算回路を用いて前記第 3 の有限体上の演算を行う第 2 の演算回路を構成する

20

請求項 1 に記載の回路構成方法。

【請求項 5】

前記第 3 の工程において、前記第 2 の多項式の 0 次の項の係数を乗じる前記第 2 の有限体上の演算を用いて、前記第 3 の有限体上の演算を規定する

請求項 4 に記載の回路構成方法。

【請求項 6】

有限体上の演算を行う演算回路を構成する回路構成装置であって、

第 1 の有限体から第 2 の有限体への第 1 の拡大についての第 1 の多項式を基に第 1 の原始根 α_1 を得る第 1 の手段と、

前記第 2 の有限体から前記第 3 の有限体への第 2 の拡大についての第 2 の多項式であって、前記第 1 の手段で得られた前記第 1 の原始根 α_1 と前記第 1 の多項式の 0 次の項の係数とを用いて、0 次の項の係数が規定された前記第 2 の多項式を基に第 2 の原始根 α_2 を得る第 2 の手段と、

30

前記第 2 の手段で得られた前記第 2 の原始根 α_2 を用いて表現された基底を用いて、前記第 3 の有限体上の演算を規定する第 3 の手段と、

前記第 3 の手段で規定された演算を基に、当該演算を行う演算回路を構成する第 4 の手段と

を有する回路構成装置。

【請求項 7】

有限体上の演算を行う演算回路を構成する回路構成装置によって実行されるプログラムであって、

40

第 1 の有限体から第 2 の有限体への第 1 の拡大についての第 1 の多項式を基に第 1 の原始根 α_1 を得る第 1 の手順と、

前記第 2 の有限体から前記第 3 の有限体への第 2 の拡大についての第 2 の多項式であって、前記第 1 の手順で得られた前記第 1 の原始根 α_1 と前記第 1 の多項式の 0 次の項の係数とを用いて、0 次の項の係数が規定された前記第 2 の多項式を基に第 2 の原始根 α_2 を得る第 2 の手順と、

前記第 2 の手順で得られた前記第 2 の原始根 α_2 を用いて表現された基底を用いて、前記第 3 の有限体上の演算を規定する第 3 の手順と、

前記第 3 の手順で規定された演算を基に、当該演算を行う演算回路を構成する第 4 の手順

50

と

を有するプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、有限体上の演算を行う演算回路の回路構成方法、その方法およびそのプログラムに関する。

【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、例えば、有限体上の演算が行われている。 10

このような有限体は、他の有限体からの拡大によって規定される場合がある。

例えば、第1の有限体からの第1の拡大によって第2の有限体が規定され、第2の有限体からの第2の拡大によって第3の有限体が規定される場合に、上記第3の有限体上の演算は、上記第2の有限体上の演算を用いて規定される。

また、上記第2の有限体上の演算は、上記第1の拡大についての第1の多項式によって得られた原始根を基に決定された基底を用いて表現される。また、第2の有限体上の演算は、上記第2の拡大についての第2の多項式によって得られた原始根を基に決定された基底を用いて表現される。

従来の回路構成方法では、上記第2の多項式の0次の項の係数を、上記第1の多項式の0次の項の係数とは無関係に定めている。 20

【0003】

【発明が解決しようとする課題】

しかしながら、上述した従来の回路構成方法では、第3の有限体上の演算を行う演算回路の回路構成要素が多くなり、当該演算回路が大規模化してしまうという問題がある。

【0004】

本発明はかかる事情に鑑みてなされたものであり、有限体上の演算を行う演算回路を従来に比べて少ない回路構成要素で小規模に構成できる回路構成方法、その装置、そのプログラムおよび演算回路を提供することを目的とする。

【0005】

【課題を解決するための手段】

上記の目的を達成するため、第1の発明の回路構成方法は、有限体上の演算を行う演算回路を構成する回路構成方法であって、第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る第1の工程と、前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の工程で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る第2の工程と、前記第2の工程で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する第3の工程と、前記第3の工程で規定された演算を基に、当該演算を行う演算回路を構成する第4の工程とを有する。 40

【0006】

第1の発明の回路構成方法の作用は以下になる。

まず、第1の工程において、第1の有限体から第2の有限体への第1の拡大についての第1の多項式を基に第1の原始根 α_1 を得る。

次に、第2の工程において、前記第2の有限体から前記第3の有限体への第2の拡大についての第2の多項式であって、前記第1の工程で得られた前記第1の原始根 α_1 と前記第1の多項式の0次の項の係数とを用いて、0次の項の係数が規定された前記第2の多項式を基に第2の原始根 α_2 を得る。

次に、第3の工程において、前記第2の工程で得られた前記第2の原始根 α_2 を用いて表現された基底を用いて、前記第3の有限体上の演算を規定する。 50

次に、第 4 の工程において、前記第 3 の工程で規定された演算を基に、当該演算を行う演算回路を構成する。

【0007】

第 2 の発明の回路構成装置は、有限体上の演算を行う演算回路を構成する回路構成装置であって、第 1 の有限体から第 2 の有限体への第 1 の拡大についての第 1 の多項式を基に第 1 の原始根 α_1 を得る第 1 の手段と、前記第 2 の有限体から前記第 3 の有限体への第 2 の拡大についての第 2 の多項式であって、前記第 1 の手段で得られた前記第 1 の原始根 α_1 と前記第 1 の多項式の 0 次の項の係数とを用いて、0 次の項の係数が規定された前記第 2 の多項式を基に第 2 の原始根 α_2 を得る第 2 の手段と、前記第 2 の手段で得られた前記第 2 の原始根 α_2 を用いて表現された基底を用いて、前記第 3 の有限体上の演算を規定する第 3 の手段と、前記第 3 の手段で規定された演算を基に、当該演算を行う演算回路を構成する第 4 の手段とを有する。

10

【0008】

第 2 の発明の回路構成装置の作用は以下のようになる。

まず、第 1 の手段において、第 1 の有限体から第 2 の有限体への第 1 の拡大についての第 1 の多項式を基に第 1 の原始根 α_1 を得る。

次に、第 2 の手段において、前記第 2 の有限体から前記第 3 の有限体への第 2 の拡大についての第 2 の多項式であって、前記第 1 の手段で得られた前記第 1 の原始根 α_1 と前記第 1 の多項式の 0 次の項の係数とを用いて、0 次の項の係数が規定された前記第 2 の多項式を基に第 2 の原始根 α_2 を得る。

20

次に、第 3 の手段において、前記第 2 の手段で得られた前記第 2 の原始根 α_2 を用いて表現された基底を用いて、前記第 3 の有限体上の演算を規定する。

次に、第 4 の手段において、前記第 3 の手段で規定された演算を基に、当該演算を行う演算回路を構成する。

【0009】

第 3 の発明のプログラムは、有限体上の演算を行う演算回路を構成する回路構成装置によって実行されるプログラムであって、第 1 の有限体から第 2 の有限体への第 1 の拡大についての第 1 の多項式を基に第 1 の原始根 α_1 を得る第 1 の手順と、前記第 2 の有限体から前記第 3 の有限体への第 2 の拡大についての第 2 の多項式であって、前記第 1 の手順で得られた前記第 1 の原始根 α_1 と前記第 1 の多項式の 0 次の項の係数とを用いて、0 次の項の係数が規定された前記第 2 の多項式を基に第 2 の原始根 α_2 を得る第 2 の手順と、前記第 2 の手順で得られた前記第 2 の原始根 α_2 を用いて表現された基底を用いて、前記第 3 の有限体上の演算を規定する第 3 の手順と、前記第 3 の手順で規定された演算を基に、当該演算を行う演算回路を構成する第 4 の手順とを有する。

30

【0010】

【発明の実施の形態】

〔本発明の関連技術〕

当該関連技術では、有限体 F が有限体 F_q の n 次拡大であり、有限体 K が有限体 F からの拡大次数 q の拡大であり、有限体 L が有限体 K からの拡大次数 q の拡大である場合に、有限体 K 上の a 倍演算を含む有限体 L 上の演算を行う演算回路を構成する回路構成方法を説明する。

40

ここで、位数が下記 (2-1) で示され、有限体 L が下記 (2-2) のように表現される。本実施形態では、下記 (2-1), (2-2) において、 $l_1 = l_2 = q$ の場合を例示する。

この場合に、上記拡大の関係は、下記 (2-3) で示される。

【0011】

【数 8】

$$q^{n \cdot l_1 \cdot l_2} (q = p^m, p; \text{素数}, n, l_1, l_2, m; \text{自然数}) \quad \cdots (2-1)$$

【 0 0 1 2 】

【数 9】

$$L := F_{q^{n \cdot l_1 \cdot l_2}} \quad \dots (2-2)$$

【 0 0 1 3 】

【数 1 0】

$$(F_q \subset)^{n\text{次}} F \overset{(1)}{\underset{q\text{次拡大}}{\subset}} K \overset{(2)}{\underset{q\text{次拡大}}{\subset}} L \quad \dots (2-3)$$

10

【 0 0 1 4 】

従来の回路構成方法では、図 1 に示すように、有限体 K 上の l_2 次元ベクトル D _ I N を入力し、有限体 K 上の l_2 次元ベクトル D _ O U T を出力し、有限体 K 上の a 倍演算回路 3 0 1 を有し、有限体 L 上の演算を行う演算回路 3 0 0 を構成する。

有限体 K 上の a 倍演算回路 3 0 1 は、有限体 F 上の l_1 次元ベクトル V A を入力し、有限体 F 上の l_1 次元ベクトル V D を出力する。

有限体 F から有限体 K への第 1 の拡大 K/F の原始根 α_1 を下記 (2-4) に示す第 1 の多項式を基に得る。

そして、原始根 α_1 を基に、有限体 K 上の演算の基底を選択する。

【 0 0 1 5 】

20

【数 1 1】

$$\alpha_1: \alpha_1^q - \alpha_1 + c = 0, \quad \exists c \in F \text{ s.t. } Tr_{F_q}^F(c) \neq 0, \quad \dots (2-4)$$

【 0 0 1 6 】

また、有限体 K から有限体 L への第 2 の拡大 L/K の原始根 α_2 を下記 (2-5) に示す第 2 の多項式を基に得る。

そして、原始根 α_2 を基に、有限体 L 上の演算の基底を選択する。

ここで、上記 a 倍演算回路 3 0 1 の a は、下記 (2-5) 内の 0 次の項の係数 a である。

【 0 0 1 7 】

30

【数 1 2】

$$\alpha_2: \alpha_2^q - \alpha_2 + a = 0, \quad \exists a = d \cdot \alpha_1^i \in K,$$

$$i \in Z \text{ s.t. } Tr_{F_q}^K(\alpha_1^i) \neq 0, \quad \dots (2-5)$$

【 0 0 1 8 】

そして、上記原始根 α_1 を基に定められた基底を用いた下記 (2-6) に示す有限体 K 上の任意の元 A を、下記 (2-7) のように有限体 F 上の l_1 (= q) 次元ベクトル V A で示す。 40

【 0 0 1 9 】

【数 1 3】

$$A: A_0 + A_1 \alpha_1 + A_2 \alpha_1^2 + \dots + A_{q-1} \alpha_1^{q-1} \quad \dots (2-6)$$

【 0 0 2 0 】

【数 1 4】

$$VA := (A_0, A_1, A_2, \dots, A_{q-1}) \quad \dots (2-7)$$

【0021】

また、上記原始根 α_1 を基に定められた基底を用いた下記 (2-8) で示す D を、下記 (2-9) のように有限体 F 上の 1_1 ($=q$) 次元ベクトル VD で示す。

【0022】

【数15】

$$D := a \cdot A = D_0 + D_1 \alpha_1 + D_2 \alpha_1^2 + \dots + D_{q-1} \alpha_1^{q-1} \quad \dots (2-8)$$

10

【0023】

【数16】

$$VD := (D_0, D_1, D_2, \dots, D_{q-1}) \quad \dots (2-9)$$

【0024】

この場合に、 $D := a \cdot A$ は、上記 (2-5) で定義される a 、並びに上記 (2-6) で定義される A を用いると、下記 (2-10) のように示され、ベクトル VD は下記 (2-11) のように示される。ここで、下記 (2-12) の左辺の α_1 の q 乗値を右辺の値 ($\alpha_1 - 1$) に置き換えて表現される。 20

【0025】

【数17】

$$\begin{aligned} & -cd \cdot A_{q-i} \cdot \alpha_1^0 + \sum_{k=1}^{i-1} \left\{ (d \cdot A_{k+q-i-1} - cd \cdot A_{k+q-i}) \cdot \alpha_1^k \right\} \\ & + d(A_0 + A_{q-1}) \cdot \alpha_1^i + d \sum_{k=i+1}^{q-1} \left\{ A_{k-i} \cdot \alpha_1^k \right\} \quad \dots (2-10) \end{aligned}$$

30

【0026】

【数18】

$$\begin{aligned} & \left\{ -cdA_{q-i}, dA_{1+q-i-1} - cdA_{1+q-i}, dA_{2+q-i-1} - cdA_{2+q-i}, \dots \right. \\ & \left. \dots, dA_{i-1+q-i-1} - cdA_{i-1+q-i}, d(A_0 + A_{q-1}), dA_{i+1-i}, dA_{i+2-i}, \dots, dA_{q-1-i} \right\} \quad \dots (2-11) \end{aligned}$$

【0027】

【数19】

$$\alpha_1^q = \alpha_1 - c \quad \dots (2-12)$$

40

【0028】

上記回路構成方法では、上記 (2-10), (2-11) を基に、図2に示すように、図1に示す有限体 K 上の a 倍演算回路 301 を構成する。

図2に示す a 倍演算回路 301 には、上記 (2-7) で示す q 次元ベクトル VA が入力される。

図2に示す $A[0] \sim A[q-1]$ が、上記 (2-7) に示す $A_0 \sim A_{q-1}$ にそれぞれ対応している。

a 倍演算回路 301 は、上記 (2-4) より得られる下記 (2-12) を基に α_1 の q 50

次の項を1次および0次の項で置き換えて上記(2-10)に示す演算を行うように構成される。

これにより、a倍演算回路301は、 α_1 のq次未満の項の係数についての演算を行うように構成される。

【0029】

図2に示すように、上記回路構成方法は、データA[0]～A[q-1]のそれぞれが、係数dを乗算するq-1個の乗算回路31_1～31_q-1、係数cdを乗算するi-1個の乗算回路32_1～32_i-1、加算回路33のうち、対応する回路に入力されるようにa倍演算回路301を構成する。

また、上記回路構成方法は、乗算回路32_0～32_i-1の出力が、インバータ35_0～35_i-1にそれぞれ入力されるようにa倍演算回路301を構成する。

また、上記回路構成方法は、乗算回路31_1～31_i-1の出力が、それぞれ加算回路34_1～34_i-1に入力されるようにa倍演算回路301を構成する。

また、上記回路構成方法は、インバータ35_1～35_i-1の出力が、それぞれ加算回路34_1～34_i-1に入力されるようにa倍演算回路301を構成する。

また、上記回路構成方法は、乗算回路33の出力が、係数dを乗算する乗算回路32に入力されるようにa倍演算回路301を構成する。

そして、インバータ35_0、加算回路34_1～34_i-1、乗算回路32、並びに乗算回路31_i～31_q-1の出力が、それぞれデータD[0]～[q-1]となる。

図2に示すD[0]～D[q-1]が、上記(2-9)，(2-11)に示すD_0～D_{q-1}にそれぞれ対応している。

【0030】

〔発明の実施の形態〕

本実施形態では、上述した関連技術と同様に、有限体F（本発明の第1の有限体）が有限体F_qのn次拡大であり、有限体K（本発明の第2の有限体）が有限体Fからの拡大次数qの拡大であり、有限体L（本発明の第3の有限体）が有限体Kからの拡大次数qの拡大である場合に、有限体K上のa倍演算を含む有限体L上の演算を行う演算回路を構成する回路構成方法を説明する。

ここで、位数が下記(3-1)で示され、有限体Lが下記(3-2)のように表現される。本実施形態では、下記(3-1)，(3-2)において、 $l_1 = l_2 = q$ の場合を例示する。例えば、qは2、nは4である。

この場合に、上記拡大の関係は、下記(3-3)で示される。

【0031】

【数20】

$$q^{n \cdot l_1 \cdot l_2} (q = p^m, p; \text{素数}, n, l_1, l_2, m; \text{自然数}) \quad \dots (3-1)$$

【0032】

【数21】

$$L := F_{q^{n \cdot l_1 \cdot l_2}} \quad \dots (3-2)$$

【0033】

【数22】

$$\begin{matrix} n\text{次} & \overset{(1)}{q\text{次拡大}} & \overset{(2)}{q\text{次拡大}} \\ (F_q \subset) & F \subset & K \subset L \end{matrix} \quad \dots (3-3)$$

【0034】

20

30

40

50

本実施形態の回路構成方法では、図 3 に示すように、有限体 K 上の l_2 ($=q$) 次元ベクトル D_IN を入力し、有限体 K 上の l_2 次元ベクトル D_OUT を出力し、有限体 K 上の a 倍演算回路 101 を有し、有限体 L 上の演算を行う演算回路 100 を構成する。有限体 K 上の a 倍演算回路 101 は、有限体 F 上の l_1 ($=q$) 次元ベクトル VA を入力し、有限体 F 上の l_1 次元ベクトル VD を出力する。

有限体 F から有限体 K への第 1 の拡大 K/F (本発明の第 1 の拡大) の第 1 の原始根 α_1 (本発明の第 1 の原始根) を下記 (3-4) に示す第 1 の多項式を基に得る。

そして、原始根 α_1 を基に、有限体 K 上の演算の基底を選択する。

【0035】

【数 23】

$$\alpha_1: \alpha_1^q - \alpha_1 + c = 0, \quad \exists c \in F \text{ s.t. } Tr_{F_q}^F(c) \neq 0, \quad \dots (3-4)$$

10

【0036】

上記 (3-4) において、トレース Tr は、下記 (3-4a) のように定義される。

【0037】

【数 24】

$$Tr_{F_q}^F(c) := c + c^q + c^{q^2} + \dots + c^{q^{n-1}} \quad \dots (3-4a)$$

20

【0038】

また、有限体 K から有限体 L への第 2 の拡大 L/K (本発明の第 2 の拡大) の第 2 の原始根 α_2 (本発明の第 2 の原始根) を下記 (3-5) に示す第 2 の多項式 (本発明の第 2 の多項式) を基に得る。

ここで、下記 (3-5) に示す第 2 の多項式は、上記 (3-4) に示す第 1 の多項式の第 1 の原始根 α_1 と当該第 1 の多項式の 0 次の項の係数 c とを用いて、0 次の項の係数 a が規定されている。

【0039】

【数 25】

$$\alpha_2: \alpha_2^q - \alpha_2 + a = 0, \quad \exists a = c^{-1} \cdot \alpha_1^i \in K,$$

30

$$i \in Z \text{ s.t. } Tr_{F_q}^K(\alpha_1^i) \neq 0, \quad \dots (3-5)$$

【0040】

そして、上記第 1 の原始根 α_1 を基に定められた基底を用いた下記 (3-6) に示す有限体 K 上の任意の元 A を、下記 (3-7) のように有限体 F 上の l_1 次元ベクトル VA で示す。

【0041】

【数 26】

$$A: A_0 + A_1 \alpha_1 + A_2 \alpha_1^2 + \dots, A_{q-1} \alpha_1^{q-1} \quad \dots (3-6)$$

40

【0042】

【数 27】

$$VA := (A_0, A_1, A_2, \dots, A_{q-1}) \quad \dots (3-7)$$

【0043】

また、上記第 1 の原始根 α_1 を基に定められた基底を用いた下記 (3-8) で示す D を

50

、下記（３－９）のように有限体 F 上の l_1 次元ベクトル VD で示す。

【００４４】

【数２８】

$$D := a \cdot A = D_0 + D_1 \alpha_1 + D_2 \alpha_1^2 + \cdots + D_{q-1} \alpha_1^{q-1} \quad \cdots (3-8)$$

【００４５】

【数２９】

$$VD := (D_0, D_1, D_2, \cdots, D_{q-1}) \quad \cdots (3-9)$$

10

【００４６】

この場合に、 $D := a \cdot A$ は、上記（３－５）で定義される a 、並びに上記（３－６）で定義される A を用いると、下記（３－１０）のように示され、ベクトル $D _ V$ は下記（３－１１）で示される。ここで、上記（３－４）から得られる下記（３－１２）の左辺の α_1 の q 乗値を右辺の値（ $\alpha_1 - 1$ ）に置き換えて表現される。

【００４７】

【数３０】

$$D := a \cdot A$$

20

$$\begin{aligned} &= -A_{l_1-i} \cdot \alpha_1^0 + \sum_{k=1}^{i-1} \left\{ (c^{-1} \cdot A_{k+l_1-i-1} - A_{k+l_1-i}) \cdot \alpha_1^k \right\} \\ &+ c^{-1} (A_0 + A_{l_1-1}) \cdot \alpha_1^i + c^{-1} \sum_{k=i+1}^{l_1-1} \left\{ A_{k-i} \cdot \alpha_1^k \right\} \quad \cdots (3-10) \end{aligned}$$

【００４８】

【数３１】

30

$$\begin{aligned} &(-A_{l_1-i}, c^{-1} A_{1+l_1-i-1} - A_{1+l_1-i}, c^{-1} A_{2+l_1-i-1} - A_{2+l_1-i}, \cdots \\ &\cdots, c^{-1} A_{i-1+l_1-i-1} - A_{i-1+l_1-i}, c^{-1} (A_0 + A_{l_1-1}), \quad \cdots (3-11) \\ &c^{-1} A_{i+1-i}, c^{-1} A_{i+2-i}, \cdots, c^{-1} A_{l_1-1-i}) \end{aligned}$$

【００４９】

【数３２】

$$\alpha_1^q = \alpha_1 - c \quad \cdots (3-12)$$

40

【００５０】

上記回路構成方法では、上記（３－１０）、（３－１１）を基に、図１に示すように、有限体 K 上の a 倍演算回路 １０１ を構成する。

ここで、 a 倍演算回路 １０１ の a は、上記（３－５）内の a である。

【００５１】

図４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（本発明の回路構成装置）の構成図である。

図４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 50

リ 3 3 および C P U 3 4 を有し、これらがバス 3 0 を介して接続されている。
 操作部 3 1 は、キーボードやマウスなどの操作手段であり、ユーザの操作に応じた操作信号を C P U 3 4 に出力する。
 ディスプレイ 3 2 は、C P U 3 4 による回路構成の処理に応じた画面を表示する。
 メモリ 3 3 は、C P U 3 4 の処理に用いられるプログラム 4 1 (本発明のプログラム) およびデータ 4 2 を記憶する。

【0052】

C P U 3 4 は、プログラム 4 1 を実行し、データ 4 2 を用いて、以下に示すように上記有限体 L 上の演算回路における上記有限体 K 上の a 倍演算回路を構成 (設計) する。
 C P U 3 4 が、本発明の回路構成装置の第 1 ~ 第 4 の手段に対応している。

10

【0053】

図 5 は、C P U 3 4 が演算回路 2 内の各乗算回路を構成する場合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 :

C P U 3 4 が、有限体 F から有限体 K への第 1 の拡大についての上記 (3-4) に示す第 1 の多項式を基に第 1 の原始根 α_1 を得る。

【0054】

ステップ S T 2 :

C P U 3 4 が、ステップ S T 1 で得られた第 1 の原始根 α_1 および第 1 の多項式の 0 次の項の係数とを用いてその 0 次の項の係数 a が規定された上記 (3-5) に示す第 2 の多項式を基に上記第 2 の原始根 α_2 を得る。

20

【0055】

ステップ S T 3 :

C P U 3 4 が、ステップ S T 2 で得られた上記原始根 α_2 を用いて表現された基底を用いて、有限体 L 上の演算を規定する。

そして、上記有限体 L 上の演算内に、上有限体 K 上の a 倍演算がある場合に、上記 (3-10), (3-11) を基に、a 倍演算を規定する。このとき、上記 (3-12) を基に、上記 (3-10) における α_1 の q 次の項を 1 次および 0 次の項の係数 c で置き換えて、当該 a 倍演算を規定する。これにより、上記 a 倍演算は、 α_1 の q 次未満の項の係数についての演算によって規定される。

30

【0056】

ステップ S T 4 ;

C P U 3 4 が、ステップ S T 3 で規定された演算を基に、上記有限体 K 上の a 倍演算回路を含む、有限体 L 上の上記演算を行う演算回路を構成する。

【0057】

本実施形態では、例えば、図 3 に示す有限体 K 上の a 倍演算回路 1 0 1 が、図 6 に示すように構成される。

すなわち、C P U 3 4 が、上記 (3-7) で示す q 次元ベクトル V A を入力するように a 倍演算回路 1 0 1 を構成する。

図 6 に示す A [0] ~ A [q-1] が、上記 (3-7) に示す $A_0 \sim A_{q-1}$ にそれぞれ対応している。

40

また、C P U 3 4 が、図 6 に示すように、データ A [0] ~ A [q-1] のそれぞれが、インバータ 1 3 __ 0 ~ 1 3 __ i-1、 c^{-1} 倍演算を行う c^{-1} 倍演算回路 1 1 __ 1 ~ 1 1 __ i-1、 c^{-1} 倍演算回路 1 1 __ i+1 ~ 1 1 __ q-1 および、加算回路 1 2 のうち対応する回路に入力されるように a 倍演算回路 1 0 1 を構成する。

【0058】

また、C P U 3 4 が、 c^{-1} 倍演算回路 1 1 __ 1 ~ 1 1 __ i-1 の出力が加算回路 1 4 __ 1 ~ 1 4 __ i-1 に入力されるように a 倍演算回路 1 0 1 を構成する。また、C P U 3 4 が、インバータ 1 3 __ 1 ~ 1 3 __ i-1 の出力が加算回路 1 4 __ 1 ~ 1 4 __ i-1 に入力されるように a 倍演算回路 1 0 1 を構成する。

50

【0059】

また、CPU334が、加算回路12の出力が c^{-1} 倍演算回路11__iに入力されるようにa倍演算回路101を構成する。

そして、CPU34が、インバータ13__0、加算回路14__1～14__i-1、 c^{-1} 倍演算回路11__i～11__q-1の出力が、それぞれデータD〔0〕～〔q-1〕となるように、a倍演算回路101を構成する。

図6に示すD〔0〕～D〔q-1〕が、上記(3-9)、(3-11)に示す $D_0 \sim D_{q-1}$ にそれぞれ対応している。

【0060】

以上説明したように、本実施形態の回路構成方法によれば、上記(3-5)に示すように、第2の多項式の0次の項の係数aを、上記(3-4)に示す第1の多項式の第1の原始根 α_1 と当該第1の多項式の0次の項の係数cとを用いて規定することで、図2に示すa倍演算回路301に比べて、回路数が削減され、小規模化された図6に示すa倍演算回路101を構成できる。図2に示す従来のa倍演算回路301では、X倍演算回路として上記(2-4)に示す係数cと上記(2-5)に示す係数dとに係わる乗算を行う回路が必要だったが、a倍演算回路101では、X倍演算回路は係数cに係わる回路のみとなる。

【0061】

本発明は上述した実施形態には、限定されない。

例えば、上記(3-4)、(3-5)において、 $q=2$ 、 $n=4$ とすると、第1の有限体Fは下記(4-1)で示され、上記(3-4)、(3-5)はそれぞれ下記(4-2)、(4-3)で示される。

【0062】

【数33】

$$F = F_2(\gamma), \gamma^4 + \gamma + 1 = 0 \quad \cdots(4-1)$$

【0063】

【数34】

$$\alpha_1: \alpha_1^2 + \alpha_1 + c = 0, \quad c = \gamma^3 \quad \cdots(4-2)$$

【0064】

【数35】

$$\alpha_2: \alpha_2^2 + \alpha_2 + a = 0, \quad a = \gamma^{-3} \cdot \alpha_1 \quad \cdots(4-3)$$

【0065】

また、上述した実施形態では、K上のa倍演算回路を含むL上の演算回路を構成する場合を例示したが、本発明は、その他、K上の乗算回路または逆元生成回路を含むL上の演算回路を構成してもよい。

【0066】

【発明の効果】

本発明によれば、有限体上の演算を行う演算回路を従来に比べて少ない回路構成要素で小規模に構成できる回路構成方法、その装置、そのプログラムおよび演算回路を提供することができる。

【図面の簡単な説明】

【図1】図1は、本発明の関連技術の回路構成方法によって構成される有限体L上の演算を行う演算回路を説明するための図である。

【図2】図2は、図1に示す有限体K上のa倍演算回路の構成図である。

【図 3】図 3 は、本発明の実施形態の回路構成方法によって構成される有限体 L 上の演算を行う演算回路を説明するための図である。

【図 4】図 4 は、本発明の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。

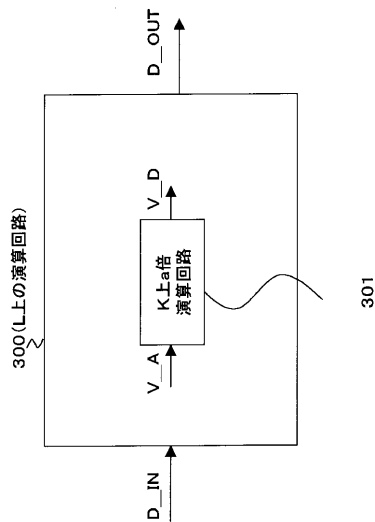
【図 5】図 5 は、図 4 に示すコンピュータの処理を説明するための図である。

【図 6】図 6 は、図 3 に示す有限体 K 上の a 倍演算回路の構成図である。

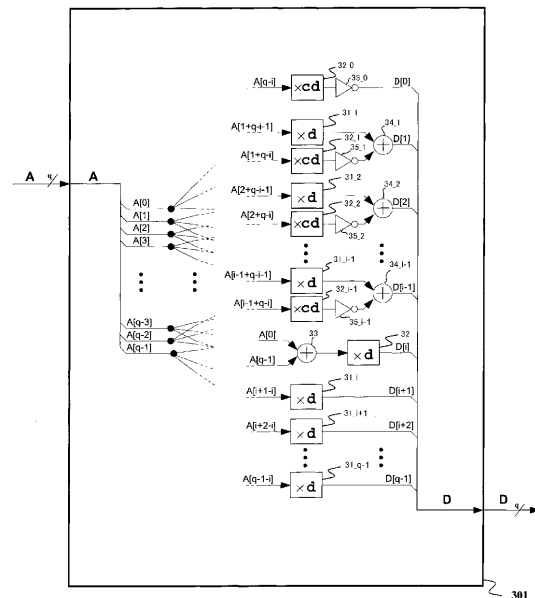
【符号の説明】

30…バス、31…操作部、32…ディスプレイ、33…メモリ、34…CPU、100、300…有限体 L 上の演算回路、101、301…有限体 K 上の a 倍演算回路

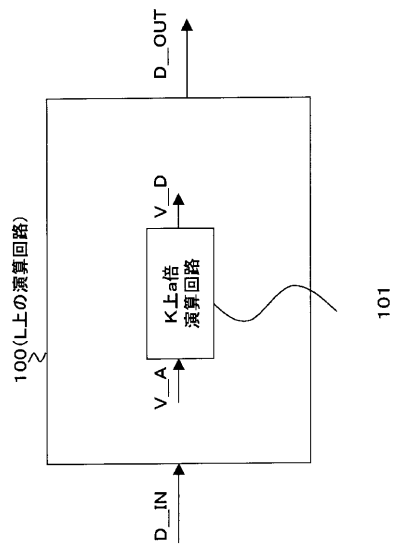
【図 1】



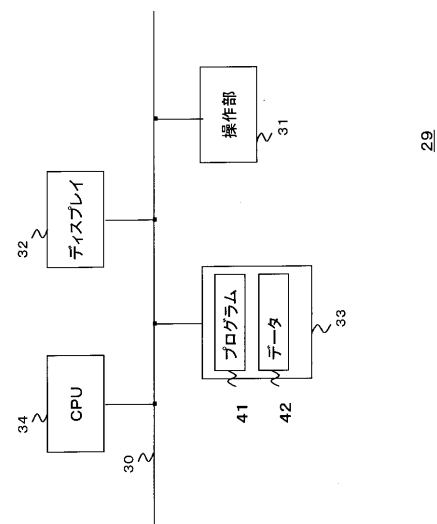
【図 2】



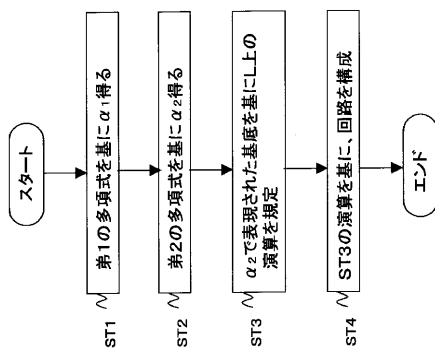
【図 3】



【図 4】



【図 5】



【図 6】

