VLSIのテストパターン生成用のセルオートマトンの構成法

指導教官　伏見 正則　教授

1997年2月14日

篠埜 功

目 次

第1章　序論

1.1　研究の背景

VLSI の状態数は非常に多いので、VLSI のチェックをどのような方法で行うかということは、非常に重要な工学的問題である。出荷前にすべての状態をチェックすることは不可能なので、ある方法でランダムサンプリングをしてテストをする。数年前までは、テストパターン生成器として linear feedback shift register(LFSR) を用いていたが、レジスターの数が大きい時には長い配線が必要となり、不都合が生じることがある。そこで、LFSR のかわりに、セルオートマトン (cellular automata) を用いることに関心が高まってきている。セルオートマトンを用いると、隣接したセル間のみに配線があるようにつくることができ、長い配線が必要なくなるという利点がある。

1.2　研究の目的

最大周期のパターンを生成するセルオートマトンを構成する手法としていくつかのものが提案されているが、そのうちのどの方法がよいかを、計算量を比較することによって決定する。

1.3　セルオートマトンについて

セルオートマトンは、n 個のセルの一次元配列から成っていて、各セルは、0 または 1 を格納する。各セルは、両隣りのセルのみと結合されている (図 1.1)。セルの状態は離散的に変化し、あるセルの次の状態は、そのセルと両隣りのセルの、3 つのセルの現在の状態によって決められる。すなわち、時刻 t における k 番目のセルの状態を $x_k(t)$ とすると、$x_k(t+1)$ は、$x_{k-1}(t), x_k(t), x_{k+1}(t)$ によって決まる。

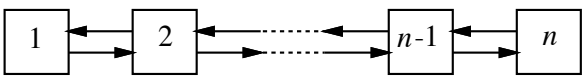

図 1.1: セルオートマトンの結合関係

(左端と右端のセルは、それぞれ、その左隣りと右隣りに、常に状態 0 のセルがあるものとして、次の状態を決めるものとする。すなわち、$x_0(t) = x_{n+1}(t) = 0$ とする。) その決め方として、本論文では、次の 2 つの場合だけを扱う。

- rule 90 : $x_k(t+1) = x_{k-1}(t) + x_{k+1}(t) \pmod 2$
- rule 150 : $x_k(t+1) = x_{k-1}(t) + x_k(t) + x_{k+1}(t) \pmod 2$

(この名前のつけかたは、Wolfram によって決められた [1]。)
k 番目のセルの状態が rule 90 で遷移するとき $c_k = 0$、rule 150 で遷移するとき $c_k = 1$ とすると、状態遷移は、

$$x_k(t+1) = x_{k-1}(t) + c_k x_k(t) + x_{k+1}(t) \pmod 2$$

と表される。行列表示では、

$$X(t) = (x_1(t), \cdots, x_n(t))^{\mathrm{T}},$$

$$A = \begin{bmatrix} c_1 & 1 & & & & \\ 1 & c_2 & 1 & & & \\ & 1 & c_3 & 1 & & \\ & & \ddots & \ddots & \ddots & \\ & & & 1 & c_{n-1} & 1 \\ & & & & 1 & c_n \end{bmatrix}$$

とすると、

$$X(t+1) = AX(t) \tag{1.1}$$

と表される。$X(t)$ は n 次元 0-1 ベクトルで、(1.1) は線形なので、$X(t)$ の周期は $2^n - 1$ を越えることはない。
$X(t)$ の周期について、次のことが成り立つ [2]。

定理 1 $X(t)$ の周期が最大 $(2^n - 1)$ となるための必要十分条件は、A の特性多項式

$$p_n(x) = \det(xI + A) \tag{1.2}$$

が GF(2) 上の原始既約多項式であることである。

1.4 LFSR について

LFSR もセルオートマトンと同じように n 個のセルの一次元配列から成っていて各セルは 0 または 1 を格納するが、結合関係が異なっていて、図 1.2 のようになっている。図 1.2 の中の p_i は 0 または 1 で、$p_k = 1$ のときには、1 番目のセルに $(n-k)$ 番目のセルからのフィードバックがあることを表す。時刻 t における k 番目のセルの状態を $x_k(t)$ とすると、LFSR の状態遷移は、

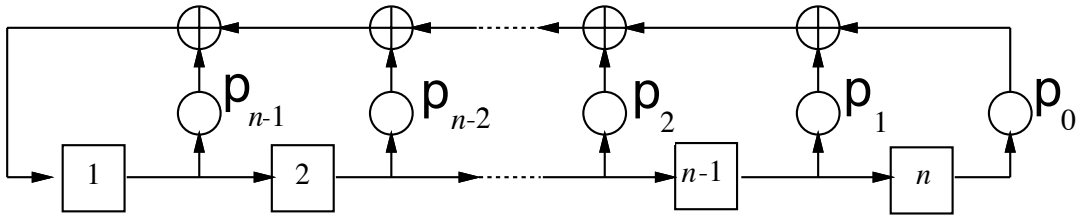

図 1.2: LFSR の結合関係

- $k = 1$ のとき

$$x_1(t+1) = \sum_{i=1}^{n} p_{n-i} x_i(t) \pmod 2,$$

- $2 \leq k \leq n$ のとき

$$x_k(t+1) = x_{k-1}(t)$$

と表される。行列表示では、

$$X(t) = (x_1(t), \cdots, x_n(t))^{\mathrm{T}},$$

$$C = \begin{bmatrix} p_{n-1} & p_{n-2} & p_{n-3} & \cdots & \cdots & p_1 & p_0 \\ 1 & 0 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 1 & 0 & \ddots & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & 0 & 0 \\ 0 & & & \ddots & 1 & 0 & 0 \\ 0 & 0 & \dots & \dots & 0 & 1 & 0 \end{bmatrix} \tag{1.3}$$

とすると、

$$X(t+1) = CX(t) \tag{1.4}$$

と表される。$X(t)$ は n 次元 0-1 ベクトルで、(1.4) は線形なので、$X(t)$ の周期は $2^n - 1$ を越えることはない。
$X(t)$ の周期について、定理 1 と同様なことがなりたつ。すなわち、$X(t)$ の周期が最大 $(2^n - 1)$ となるための必要十分条件は、C の特性多項式

$$p_n(x) = \det(xI + C) \tag{1.5}$$

が GF(2) 上の原始既約多項式であることである [2]。行列式 (1.5) を展開すると、

$$p_n(x) = x^n + p_{n-1}x^{n-1} + p_{n-2}x^{n-2} + \cdots + p_1 x + p_0 \tag{1.6}$$

となる。(1.3) と (1.6) を見比べると、$p_n(x)$ の係数が、行列 C の 1 行とちょうど対応している。よって、最大周期の LFSR を構成したければ、原始既約多項式 $p_n(x)$ を任意に 1 つ選び、それを特性多項式にもつ行列 C を構成すれよい。それが最大周期の LSFR を表す行列となる。

1.5 セルオートマトンとLFSRの関係

(この節の内容は、[3] に書かれている。)

行列の最小多項式は、行列の特性多項式の約数である。したがって、特性多項式が既約であれば、それは最小多項式に等しい。二つの行列が同じ線形写像を表すこと (すなわち相似であること) と、その二つの行列が同じ最小多項式をもつことは同値なので、特性多項式が既約である時には、二つの行列が相似であることと、同じ特性多項式をもつことは、同値である。相似に関して次のことが成り立つ。

定理 2 二つの行列 T, T' が相似であるための必要十分条件は、ある正則行列 P が存在して、

$$PTP^{-1} = T'$$

となることである。

行列 A の特性多項式 $p_n(x)$ が既約であるとすると、$p_n(x)$ の根は、

$$\alpha, \alpha^2, \alpha^4, \cdots, \alpha^{2^{n-1}}$$

と表せる。

$$D = \begin{bmatrix} \alpha & & & & \\ & \alpha^2 & & & \\ & & \ddots & & \\ & & & \alpha^{2^{n-2}} & \\ & & & & \alpha^{2^{n-1}} \end{bmatrix}$$

とし、

$$m_i = p_i(\alpha) \ (i = 0, \cdots, n)$$

とし ($m_0 = p_0(\alpha) = 1, m_n = p_n(\alpha) = 0$ である),

$$P = \begin{bmatrix} m_0 & m_0^2 & m_0^4 & \dots & m_0^{2^{n-1}} \\ m_1 & m_1^2 & m_1^4 & \dots & m_1^{2^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ m_{n-2} & m_{n-2}^2 & m_{n-2}^4 & \dots & m_{n-2}^{2^{n-1}} \\ m_{n-1} & m_{n-1}^2 & m_{n-1}^4 & \dots & m_{n-1}^{2^{n-1}} \end{bmatrix}$$

とすると、次のことが成り立つ。

定理 3 P は正則行列であり、$PDP^{-1} = A$ を満たす。

次に、

$$Q = \begin{bmatrix} \alpha^n & (\alpha^n)^2 & (\alpha^n)^4 & \dots & (\alpha^n)^{2^{n-1}} \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha^3 & (\alpha^3)^2 & (\alpha^3)^4 & \dots & (\alpha^3)^{2^{n-1}} \\ \alpha^2 & (\alpha^2)^2 & (\alpha^2)^4 & \dots & (\alpha^2)^{2^{n-1}} \\ \alpha & \alpha^2 & \alpha^4 & \dots & \alpha^{2^{n-1}} \end{bmatrix}$$

とすると、次の定理が成り立つ。

定理 4 Qは正則行列であり、$Q^{-1}CQ = D$を満たす。

よって定理3,4より

$$A = PDP^{-1} = P(Q^{-1}CQ)P^{-1} = (PQ^{-1})C(PQ^{-1})^{-1}$$

となり、定理2より行列AとCは相似となる。すなわち行列AとCは、同じ線形写像の異なる表現である。セルオートマトンとLFSRは行列PQ^{-1}によって関係づけられる。

第2章　セルオートマトンの構成法

この章では、最大周期のセルオートマトンを構成するアルゴリズムを3つ示す。

2.1　セルオートマトンの構成法1

(この方法は、[4] に書かれている方法である。)
行列式 (1.2) を展開することにより、漸化式

$$p_k(x) = (x + c_k)p_{k-1}(x) + p_{k-2}(x), \tag{2.1}$$

$$p_0(x) = 1,\ p_{-1}(x) = 0$$

を得る。

よって、最大周期のセルオートマトンを構成する方法として、次のようなものが考えられる [4]。

[STEP1] ランダムに $c_1, \cdots, c_n$ を選んで漸化式 (2.1) を使って $p_n(x)$ を計算する。

[STEP2] $p_n(x)$ が原始既約多項式かどうか判定する。

[STEP3] $p_n(x)$ が原始既約多項式であればSTEP1で選んだ $c_1, \cdots, c_n$ を採用し、原始既約多項式でなければ、STEP1に戻る。

($c_1, \cdots, c_n$ の組合せの中には、$p_n(x)$ が原始既約多項式になるものが必ず存在することが、次のsectionで示される。)

2.2　セルオートマトンの構成法2

(この構成法は、[5] に書かれている方法である。)

定理 5 任意のGF(2)上の n 次の既約多項式 $p_n(x)$ に対して、

$$p_k(x) = p_{k-2}(x) \pmod{p_{k-1}(x)}\ (k = 1, \cdots, n)$$

を満たす多項式の列 $p_{n-1}(x),\ p_{n-2}(x), \cdots,\ p_0(x)(= 1)$ が存在し、

$$p_{n-1}(x)/p_n(x) = q_1x^{-1} + q_2x^{-2} + \cdots$$

とすると、$q_1, q_2, \cdots, q_n$ を要素とするベクトル $q = (q_1, q_2, \cdots, q_n)^{\mathrm{T}}$ と、

$$\sum_{j=1}^{n} b_{ij} x^{j-1} = x^{i-1} + x^{2i-1} + x^{2i} \pmod{p_n(x)}$$

を満たす b_{ij} を要素に持つ行列 $B = (b_{ij})$ の間には、

$$Bq = (0, 0, \cdots, 0, 1)^{\mathrm{T}}$$

という関係がある [6]。

この定理により、任意の n 次の既約多項式 $p_n(x)$ に対して、それを特性多項式にもつセルオートマトンを表す行列 A を、次のようにして求めることができる [5]。

[STEP1] 行列 B を求める。

[STEP2] $Bq = (0, 0, \cdots, 0, 1)^{\mathrm{T}}$ をガウスの消去法で解いて、$q_1, q_2, \cdots, q_n$ を求める。

[STEP3] $p_n(x)(q_1 x^{-1} + q_2 x^{-2} + \cdots + q_n x^{-n})$ を計算し、次数が負の項を除き、残ったものを $p_{n-1}(x)$ とする。

[STEP4] $p_n(x)$ と $p_{n-1}(x)$ から、漸化式 (2.1) を使って、$c_1, c_2, \cdots, c_n$ を計算する。

なお、行列 B の階数は $n-1$ で、行列 B に列ベクトル $(0, 0, \cdots, 0, 1)^{\mathrm{T}}$ を加えてできる $n \times (n+1)$ 行列の階数も $n-1$ である [6] ので STEP2 で解は必ず存在し、解には任意定数が 1 つ含まれる。ただし、任意定数のとりうる値は 0 または 1 の 2 つなので、解は 2 つとなる。よって、与えられた既約多項式を特性多項式にもつセルオートマトンを表す行列 A は 2 つ存在するが、それは、$c_1, c_2, \cdots, c_n$ が逆に並んだものである [6]。このことは、あるセルオートマトンを左右逆にしても、本質的にはもとのセルオートマトンと同じものであるという事実に対応している。よって、STEP2 では、解を 1 つ求めるだけでよい。

以上により、任意の既約多項式に対して、それを特性多項式にもつセルオートマトンを表す行列 A を構成するアルゴリズムが示されたが、原始既約多項式は既約多項式なので、最大周期のセルオートマトンを構成するには、与える既約多項式を、原始既約多項式にすればよい。

2.3 構成法 2 の例

以下に構成法 2 の例を、

$$p_n(x) = x^6 + x + 1$$

と

$$p_n(x) = x^7 + x + 1$$

の 2 つの場合について示す。

- $p_n(x) = x^6 + x + 1$ のとき、

[STEP1] 行列 B を求めると、

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

となる。

[STEP2] $Bq = (0, \cdots, 0, 1)^{\mathrm{T}}$ を解くと、

$$q_1 = 1,\ q_2 = 0,\ q_3 = 1,\ q_4 = 0,\ q_5 = 0,\ q_6 = 0$$

または、

$$q_1 = 1,\ q_2 = 0,\ q_3 = 1,\ q_4 = 1,\ q_5 = 1,\ q_6 = 0$$

となる。

[STEP3] $p_{n-1}(x)$ を計算すると、

$$(x^6 + x + 1)(x^{-1} + x^{-3}) = x^5 + x^3 + 1 + x^{-1} + x^{-2} + x^{-3}$$

より、

$$p_{n-1}(x) = x^5 + x^3 + 1$$

となる。または、

$$\begin{aligned}(x^6 + x + 1)&(x^{-1} + x^{-3} + x^{-4} + x^{-5}) \\ &= x^5 + x^3 + x^2 + x + 1 + x^{-1} + x^{-2} + x^{-5}\end{aligned}$$

より、

$$p_{n-1}(x) = x^5 + x^3 + x^2 + x + 1$$

となる。

[STEP4] $p_n(x), p_{n-1}(x)$ についてユークリッドの互除法を行うことにより、

$$c_1 = 0,\ c_2 = 1,\ c_3 = 1,\ c_4 = 0,\ c_5 = 0,\ c_6 = 0$$

または、

$$c_1 = 0,\ c_2 = 0,\ c_3 = 0,\ c_4 = 1,\ c_5 = 1,\ c_6 = 0$$

を得る。

この 2 つのセルオートマトンは、前に述べた通り、左右対称になっている。

- $p_n(x) = x^7 + x + 1$ のとき、

[STEP1] 行列 B を求めると、

$$B = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

となる。

[STEP2] $Bq = (0, \cdots, 0, 1)^{\mathrm{T}}$ を解くと、

$$q_1 = 1,\ q_2 = 1,\ q_3 = 0,\ q_4 = 1,\ q_5 = 0,\ q_6 = 0,\ q_7 = 0$$

または、

$$q_1 = 1,\ q_2 = 1,\ q_3 = 0,\ q_4 = 1,\ q_5 = 0,\ q_6 = 1,\ q_7 = 1$$

となる。

[STEP3] $p_{n-1}(x)$ を計算すると、

$$\begin{aligned} &(x^7 + x + 1)(x^{-1} + x^{-2} + x^{-4}) \\ &\quad = x^6 + x^5 + x^3 + 1 + x^{-2} + x^{-3} + x^{-4} \end{aligned}$$

より、

$$p_{n-1}(x) = x^6 + x^5 + x^3 + 1$$

となる。または、

$$\begin{aligned} &(x^7 + x + 1)(x^{-1} + x^{-2} + x^{-4} + x^{-6} + x^{-7}) \\ &\quad = x^6 + x^5 + x^3 + x + x^{-2} + x^{-3} + x^{-4} + x^{-5} + x^{-7} \end{aligned}$$

より、

$$p_{n-1}(x) = x^6 + x^5 + x^3 + x$$

となる。

[STEP4] $p_n(x), p_{n-1}(x)$ についてユークリッドの互除法を行うことにより、

$$c_1 = 1,\ c_2 = 0,\ c_3 = 1,\ c_4 = 1,\ c_5 = 0,\ c_6 = 0,\ c_7 = 1$$

または、

$$c_1 = 1,\ c_2 = 0,\ c_3 = 0,\ c_4 = 1,\ c_5 = 1,\ c_6 = 0,\ c_7 = 1$$

を得る。

この 2 つのセルオートマトンは、前に述べた通り、左右対称になっている。

2.4 セルオートマトンの構成法3

(この方法は、[7] に書かれている方法である。)

任意のセルオートマトンを表す行列 A の特性多項式 $p_n(x)$ と $y(x) = p_{n-1}(x)$ の間には、次のような関係がある [7]。

$$\{y(x)\}^2 + (x^2 + x)p_n'(x)y(x) + 1 \equiv 0 \pmod{p_n(x)}. \tag{2.2}$$

$p_n(x)$ が既約多項式の場合は、関係式 (2.2) を満たす $y(x)$ は 2 つ存在し、しかも、その $y(x)$ と $p_n(x)$ についてユークリッドの互除法を行うと、商がすべて 1 次となる [7]。よって、$p_n(x)$ が既約多項式の場合には、関係式 (2.2) を満たす $y(x)$ が求められれば、その $p_n(x)$ を特性多項式にもつセルオートマトンを表す行列 A を構成することができる。

$p_n(x)$ が既約多項式の場合に関係式 (2.2) を満たす $y(x)$ は次のようにして求めることができる [7]。

[STEP1] $p_n(x)$ の形式的導関数 $p_n'(x)$ を計算する。

[STEP2] $(x^2 + x)p_n'(x) \pmod{p_n(x)}$ を計算し、それを $f(x)$ とする。

[STEP3] $f(x)$ の、$\bmod p_n(x)$ に関する逆元 $1/f(x)$ を計算する。

[STEP4] $\{1/f(x)\}^2 \pmod{p_n(x)}$ を計算し、それを $g(x)$ とする。

[STEP5] トレースが 1 となるものを 1 つ見つけ、それを $\theta(x)$ とする。
(トレースとは、

$$\begin{aligned} \mathrm{Tr}(a) &= (a + a^2 + a^4 + \cdots + a^{2^{n-1}}) \pmod{p_n(x)} \\ &= \sum_{i=0}^{n-1} a^{2^i} \pmod{p_n(x)} \end{aligned}$$

と定義されているものである。)

[STEP6] $g(x)\theta^2 + (g(x) + g(x)^2)\theta^4 + \cdots + (g(x) + g(x)^2 + \cdots + g(x)^{2^{n-2}})\theta(x)^{2^{n-1}}$
$\pmod{p_n(x)} = \sum_{i=1}^{n-1}\{\sum_{j=0}^{i-1} g(x)^{2^j}\}\theta(x)^{2^i} \pmod{p_n(x)}$
を計算し、それを $\beta(x)$ とする。

[STEP7] $\beta(x)f(x) \pmod{p_n(x)}$ を計算し、それを $y(x) = p_{n-1}(x)$ とする。
($1/\{\beta(x)f(x)\}$ を $y(x) = p_{n-1}(x)$ としてもよい。)

よって、任意の既約多項式に対して、それを特性多項式にもつセルオートマトンを表す行列 A を構成することができ、それには、次のステップを追加すればよい。

[STEP8] $p_n(x)$ と $p_{n-1}(x)$ から、漸化式 (2.1) を使って、$c_1, c_2, \cdots, c_n$ を計算する。

section2.2 と同様に、最大周期のセルオートマトンを構成するには、与える既約多項式を、原始既約多項式にすればよい。

2.5　構成法3の例

以下に構成法3の例を、

$$p_n(x) = x^6 + x + 1$$

と

$$p_n(x) = x^7 + x + 1$$

の2つの場合について示す。

- $p_n(x) = x^6 + x + 1$ のとき、

[STEP1] $p_n'(x) = 1.$

[STEP2] $f(x) = x^2 + x.$

[STEP3] $1/f(x) = x^4 + x^3 + x^2 + x + 1.$
(STEP3 の詳細は、次の章で示す。)

[STEP4]

$$\begin{aligned} g(x) &= (x^4 + x^3 + x^2 + x + 1)^2 \pmod{x^6 + x + 1} \\ &= x^4 + x^3 + x. \end{aligned}$$

[STEP5] $\theta(x) = x^5 + x^2 + x + 1$ とする。

[STEP6]

$$\begin{aligned} \beta(x) &= \sum_{i=1}^{n-1} \{ \sum_{j=0}^{i-1} (x^4 + x^3 + x)^{2^j} \} (x^5 + x^2 + x + 1)^{2^i} \pmod{x^6 + x + 1} \\ &= x^4 + x + 1. \end{aligned}$$

[STEP7]

$$\begin{aligned} p_{n-1}(x) &= (x^4 + x + 1)(x^2 + x) \pmod{x^6 + x + 1} \\ &= x^5 + x^3 + 1. \end{aligned}$$

(または、

$$\begin{aligned} p_{n-1}(x) &= 1/(x^5 + x^3 + 1) \\ &= x^5 + x^3 + x^2 + x + 1. \ ) \end{aligned}$$

[STEP8] $p_n(x), p_{n-1}(x)$ についてユークリッドの互除法を行うことにより、

$$c_1 = 0,\ c_2 = 1,\ c_3 = 1,\ c_4 = 0,\ c_5 = 0,\ c_6 = 0$$

(または、

$$c_1 = 0,\ c_2 = 0,\ c_3 = 0,\ c_4 = 1,\ c_5 = 1,\ c_6 = 0\ )$$

を得る。

- $p_n(x) = x^7 + x + 1$ のとき、

[STEP1] $p_n'(x) = x^6 + 1.$

[STEP2]

$$\begin{aligned} f(x) &= (x^2 + x)(x^6 + 1) \pmod{x^7 + x + 1} \\ &= x + 1. \end{aligned}$$

[STEP3] $1/f(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x.$

[STEP4]

$$\begin{aligned} g(x) &= (x^6 + x^5 + x^4 + x^3 + x^2 + x)^2 \pmod{x^7 + x + 1} \\ &= x^5 + x^3 + x. \end{aligned}$$

[STEP5] $\theta(x) = 1$ とする。

[STEP6]

$$\begin{aligned} \beta(x) &= \sum_{i=1}^{n-1}\{\sum_{j=0}^{i-1}(x^5 + x^3 + x)\} \pmod{x^7 + x + 1} \\ &= x^5 + x^2 + x. \end{aligned}$$

[STEP7]

$$\begin{aligned} p_{n-1}(x) &= (x^5 + x^2 + x)(x + 1) \pmod{x^7 + x + 1} \\ &= x^6 + x^5 + x^3 + x. \end{aligned}$$

(または、

$$\begin{aligned} p_{n-1}(x) &= 1/(x^6 + x^5 + x^3 + x) \\ &= x^6 + x^5 + x^3 + 1. \ ) \end{aligned}$$

[STEP8] $p_n(x), p_{n-1}(x)$ についてユークリッドの互除法を行うことにより、

$$c_1 = 1,\ c_2 = 0,\ c_3 = 0,\ c_4 = 1,\ c_5 = 1,\ c_6 = 0,\ c_7 = 1$$

(または、

$$c_1 = 1,\ c_2 = 0,\ c_3 = 1,\ c_4 = 1,\ c_5 = 0,\ c_6 = 0,\ c_7 = 1\ )$$

を得る。

第3章　各構成法の計算量

この章では、前章の3つの構成法の計算量を求める。

3.1　構成法1の計算量

GF(2) 上の n 次の原始既約多項式は $\frac{\varphi(2^n-1)}{n}$ 個ある [8]。
(ここで、φ はオイラー関数を表し、$\varphi(m)$ は、m と互いに素な m 以下の自然数 (1 を含む) の総数を表す。m の素因数分解が $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ ならば、

$$\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_r})$$

である。)
$c_1, \cdots, c_n$ の順列は 2^n 個あり、1 つの原始既約多項式に対して 2 組の $c_1, \cdots, c_n$ が対応しているので、ランダムに $c_1, \cdots, c_n$ を選んだ時に $p_n(x)$ が原始既約多項式になる確率は、

$$P(n) = \frac{2\varphi(2^n - 1)}{n \cdot 2^n}$$

である。
($\varphi(2^n - 1) < 2^n - 1$ なので、$P(n) < \frac{2}{n}$ が成り立つ。)

よって、k 回目で初めて $p_n(x)$ が原始既約多項式になる確率は $P(n)\{1-P(n)\}^{k-1}$ なので、初めて $p_n(x)$ が原始既約多項式になるまでの試行回数の平均は、

$$\begin{aligned} \sum_{k=1}^{\infty} kP(n)\{1 - P(n)\}^{k-1} &= \lim_{m\to\infty} \{\frac{1}{P(n)}\{1 - (1 - P(n))^m\} - n(1 - P(n))^m\} \\ &= \frac{1}{P(n)} \end{aligned}$$

回である。$P(n) < \frac{2}{n}$ より、

$$\frac{1}{P(n)} > \frac{n}{2}$$

となる。

平均試行回数が多項式オーダーで抑えられるかどうかは、現段階では不明である。よって、構成法 1 の計算量が多項式オーダーで抑えられるかどうかは不明である。

3.2 構成法2の計算量

3.2.1 STEP1の計算量

各 i について、x^{i-1} で引き算 1 回、x^{2i} でかけ算 1 回、x^{2i-1} で引き算 1 回で、$\lceil \frac{n}{2} \rceil \leq i \leq n$ のときには $\bmod p_n(x)$ の演算が必要となるので、合計では、引き算が $2n$ 回、かけ算が n 回、$\bmod p_n(x)$ が $(n - \lceil \frac{n}{2} \rceil + 1)$ 回となる。$\bmod p_n(x)$ に必要な計算量は各 i について、GF(2) 上の足し算が最大 $(n+1)(2i-n+1)$ 回、シフトが最大 $(n+1)(2i-n)$ 回なので、$\bmod p_n(x)$ に必要な計算量の合計は、

(i) n が偶数のとき、
GF(2) 上の足し算が最大

$$\begin{aligned} \sum_{i=\lceil \frac{n}{2} \rceil}^{n} (n+1)(2i-n+1) &= \sum_{i=\frac{n}{2}}^{n} (n+1)(2i-n+1) \\ &= \frac{1}{4}n^3 + \frac{5}{4}n^2 + 2n + 1 \end{aligned}$$

回、シフトが最大

$$\begin{aligned} \sum_{i=\lceil \frac{n}{2} \rceil}^{n} (n+1)(2i-n) &= \sum_{i=\frac{n}{2}}^{n} (n+1)(2i-n) \\ &= \frac{1}{4}n^3 + \frac{3}{4}n^2 + \frac{1}{2}n \end{aligned}$$

回である。

(ii) n が奇数のとき、
GF(2) 上の足し算が最大

$$\begin{aligned} \sum_{i=\lceil \frac{n}{2} \rceil}^{n} (n+1)(2i-n+1) &= \sum_{i=\frac{n+1}{2}}^{n} (n+1)(2i-n+1) \\ &= \frac{1}{4}n^3 + \frac{5}{4}n^2 + \frac{7}{4}n + \frac{3}{4} \end{aligned}$$

回、シフトが最大

$$\begin{aligned} \sum_{i=\lceil \frac{n}{2} \rceil}^{n} (n+1)(2i-n) &= \sum_{i=\frac{n+1}{2}}^{n} (n+1)(2i-n) \\ &= \frac{1}{4}n^3 + \frac{3}{4}n^2 + \frac{3}{4}n + \frac{1}{4} \end{aligned}$$

回である。

3.2.2 STEP2の計算量

(1) 前進消去の計算量
第 k 段目において、GF(2) 上の足し算が最大 $\sum_{i=k+1}^{n}(n-k+2)$ 回必要である。よって合計では GF(2) 上の足し算が最大

$$\begin{aligned}\sum_{k=1}^{n-1}\sum_{i=k+1}^{n}(n-k-2) &= \sum_{k=1}^{n-1}(n-k)(n-k+2)\\ &= \frac{1}{3}n^3+\frac{1}{2}n^2-\frac{5}{6}n\end{aligned}$$

回必要である。

(2) 後退代入の計算量
GF(2) 上の足し算が最大

$$\sum_{k=1}^{n}(n-k)=\frac{1}{2}n^2-\frac{1}{2}n$$

回必要である。

よって、STEP2 の計算量は、GF(2) 上の足し算が最大

$$(\frac{1}{3}n^3+\frac{1}{2}n^2-\frac{5}{6}n)+(\frac{1}{2}n^2-\frac{1}{2}n)=\frac{1}{3}n^3+n^2-\frac{4}{3}n$$

回である。

3.2.3 STEP3の計算量

GF(2) 上の足し算が最大

$$\sum_{i=1}^{n-1}(n-i)=\frac{1}{2}n^2-\frac{1}{2}n$$

回、シフトが最大

$$\sum_{i=1}^{n-1}(n-i)=\frac{1}{2}n^2-\frac{1}{2}n$$

回必要である。

3.2.4 STEP4 の計算量

STEP4 は、$p_n(x)$ と $p_{n-1}(x)$ について、ユークリッドの互除法を行うことと同じである。しかも、この場合は、次数が必ず 1 次ずつ下がっていく。(k 次の多項式)÷(($k-1$) 次の多項式) の計算量は GF(2) 上の足し算が最大

$$(k-1+1)\{k-(k-1)+1\} = 2k$$

回、シフトが最大

$$(k-1+1)\{k-(k-1)\} = k$$

回なので、合計では、GF(2) 上の足し算が最大

$$\sum_{k=1}^{n} 2k = n^2 + n$$

回、シフトが最大

$$\sum_{k=1}^{n} k = \frac{1}{2}n^2 + \frac{1}{2}n$$

回である。

3.2.5 構成法 2 の計算量の合計

以上をまとめると、次のようになる。

表 3.1: 構成法 2 の計算量

		GF(2) 上の足し算	シフト
STEP1	(n:偶数)	$\frac{1}{4}n^3 + \frac{5}{4}n^2 + 2n + 1$	$\frac{1}{4}n^3 + \frac{3}{4}n^2 + \frac{1}{2}n$
	(n:奇数)	$\frac{1}{4}n^3 + \frac{5}{4}n^2 + \frac{7}{4}n + \frac{3}{4}$	$\frac{1}{4}n^3 + \frac{3}{4}n^2 + \frac{3}{4}n + \frac{1}{4}$
STEP2		$\frac{1}{3}n^3 + n^2 - \frac{4}{3}n$	0
STEP3		$\frac{1}{2}n^2 - \frac{1}{2}n$	$\frac{1}{2}n^2 - \frac{1}{2}n$
STEP4		$n^2 + n$	$\frac{1}{2}n^2 + \frac{1}{2}n$
合計	(n:偶数)	$\frac{7}{12}n^3 + \frac{15}{4}n^2 + \frac{7}{6}n + 1$	$\frac{1}{4}n^3 + \frac{7}{4}n^2 + \frac{1}{2}n$
	(n:奇数)	$\frac{7}{12}n^3 + \frac{15}{4}n^2 + \frac{11}{12}n + \frac{3}{4}$	$\frac{1}{4}n^3 + \frac{7}{4}n^2 + \frac{3}{4}n + \frac{1}{4}$

(STEP1 の引き算 $2n$ 回とかけ算 n 回は無視できる。)

3.3 構成法3の計算量

3.3.1 STEP1の計算量

偶数次の項は微分すると0になり、奇数次の項は微分すると次数が1次下がる。よって、奇数次の項のみを取り出してシフトすればよい。シフト回数は、$\lceil \frac{n}{2} \rceil$ 回である。

よって、STEP1の計算量は、

(i) n が偶数のときシフトが $\frac{n}{2}$ 回

(ii) n が奇数のときシフトが $\frac{n+1}{2}$ 回

である。

3.3.2 STEP2の計算量

まず、$(x^2+x)p'_n(x)$ の計算量は、GF(2) 上の足し算が n 回、シフトが n 回である。そのあと $\bmod p_n(x)$ をとる計算量は、($(n+1)$ 次の多項式)÷ (n 次の多項式)なので、GF(2) 上の足し算が最大

$$(n+1)(n+1-n+1) = 2n+2$$

回、シフトが最大

$$(n+1)(n+1-n) = n+1$$

回である。よって、STEP2の計算量は、GF(2) 上の足し算が最大

$$n + (2n+2) = 3n+2$$

回、シフトが最大

$$n + (n+1) = 2n+1$$

回である。

3.3.3 STEP3の計算量

$1/f(x)$ は、$p_n(x)$ と $f(x)$ についてユークリッドの互除法を行うことによって得られる。具体的な方法を以下に示す。まず、$p_n(x)$ と $f(x)$ についてユークリッドの互除法を行うことによって $p_n(x)$ と $f(x)$ の最大公約式を求めることができるが、$p_n(x)$ は n 次の既約多項式であり $f(x)$ は $(n-1)$ 次以下の多項式なので $p_n(x)$ と

$f(x)$ の最大公約式は 1 となる。次に、ユークリッドの互除法を行った計算式を逆にたどることによって、1 を $p_n(x)$ と $f(x)$ を使って次のように表わすことができる。

$$s(x)p_n(x) + t(x)f(x) = 1.$$

ここで両辺について $\bmod p_n(x)$ をとると、

$$t(x)f(x) \pmod{p_n(x)} = 1$$

となるので、

$$1/f(x) = t(x)$$

となる。

以下で、$t(x)$ を効率的に求めるための準備をする。

($a(x)$ の次数)$\geq$($b(x)$ の次数) であるような任意の多項式 $a(x), b(x)$ に対してユークリッドの互除法を行う。

$$r_{-1}(x) = a(x),\ r_0(x) = b(x)$$

とおいて、$i \geq 1$ について

$$r_{i-2}(x) = q_i(x)r_{i-1}(x) + r_i(x)$$

という計算を繰り返し行い (ここで ($r_i(x)$ の次数)<($r_{i-1}(x)$ の次数))、$i = m+1$ のときに $r_i(x) = 0$ になったとする。ここで、多項式列 $\{s_i(x)\}, \{t_i(x)\}(i = -1,\ 0,\ 1, \cdots,\ m+1)$ を

$$s_{-1}(x) = 1,\ s_0(x) = 0,$$

$$t_{-1}(x) = 0,\ t_0(x) = 1,$$

$$t_i(x) = t_{i-2}(x) - q_i(x)t_{i-1}(x),$$

$$s_i(x) = s_{i-2}(x) - q_i(x)s_{i-1}(x)$$

と定義すると、次のことが成り立つ [9]。

$$s_i(x)a(x) + t_i(x)b(x) = r_i(x) \tag{3.1}$$

$$(i = -1, 0, 1, \cdots, m+1).$$

(証明)

[I] $i = -1, 0$ のとき、

$$s_{-1}(x)a(x) + t_{-1}(x)b(x) = a(x) = r_{-1}(x),$$

$$s_0(x)a(x) + t_0(x)b(x) = b(x) = r_0(x)$$

となり、(3.1) が成り立つ。

[II] $i = k-2,\ k-1 (1 \leq k \leq m+1)$ のとき (3.1) が成り立つと仮定すると、

$$s_{k-2}(x)a(x) + t_{k-2}b(x) = r_{k-2},$$
$$s_{k-1}(x)a(x) + t_{k-1}b(x) = r_{k-1}$$

であり、

$$\begin{aligned} r_k(x) &= r_{k-2}(x) - q_k(x)r_{k-1}(x) \\ &= s_{k-2}(x)a(x) + t_{k-2}(x)b(x) - q_k(x)\{s_{k-1}(x)a(x) + t_{k-1}(x)b(x)\} \\ &= \{s_{k-2}(x) - q_k(x)s_{k-1}(x)\}a(x) + \{t_{k-2}(x) - q_k(x)t_{k-1}(x)\}b(x) \\ &= s_k(x)a(x) + t_k(x)b(x) \end{aligned}$$

となり、$i = k$ のとき、(3.1) は成り立つ。

よって、数学的帰納法より、$i = -1,\ 0,\ 1, \cdots,\ m+1$ のとき (3.1) は成り立つ。
$a(x) = p_n(x),\ b(x) = f(x)$ とすると、(3.1) より

$$s_m(x)p_n(x) + t_m(x)f(x) = 1$$

となるので、$1/f(x)$ は、漸化式

$$t_i(x) = t_{i-2}(x) - q_i(x)t_{i-1}(x) \tag{3.2}$$

$$(t_{-1}(x) = 0, t_0(x) = 1)$$

によって、効率的に求めることができる。よって、$f(x)$ の逆元 $1/f(x)$ を求めるには、まず、$p_n(x), f(x)$ についてユークリッドの互除法を、商を記憶しながら余りが 1 になるまで繰り返し、漸化式 (3.2) によって $t_m(x)$ を計算すればよい。以下で、$f(x)$ の逆元を求める計算量を、ユークリッドの互除法を行う部分と、そのあとの、漸化式 (3.2) の部分とに分けて求める。

(1) ユークリッドの互除法を行う部分の計算量
ユークリッドの互除法の計算量は、$r_i(x)$ の次数が 1 次ずつ下がっていくとすると、(k 次の多項式)÷(($k-1$) 次の多項式) の計算量は GF(2) 上の足し算が最大 $2k$ 回、シフトが最大 k 回であり、(n 次の多項式)÷(($n-1$) 次の多項式) から (2 次の多項式)÷(1 次の多項式) まで行うので、GF(2) 上の足し算が最大

$$\sum_{k=2}^{n} 2k = n^2 + n - 2$$

回、シフトが最大

$$\sum_{k=2}^{n} k = \frac{1}{2}n^2 + \frac{1}{2}n - 1$$

回である。
実際には、$r_i(x)$ の次数は 1 次ずつ下がるとは限らないが、$r_i(x)$ の次数が 1 次ずつ下がる場合の最悪計算量が最大になるということを以下に示す。

$r_i(x)$ が k 次、$r_{i+1}(x)$ が $(k-d)$ 次 $(d \geq 2)$ だったとすると、$r_i(x) \div r_{i-1}(x)$ の計算量は、GF(2) 上の足し算が最大

$$(k-d+1)\{k-(k-d)+1\} = (d+1)k - d^2 + 1$$

回、シフトが最大

$$(k-d+1)\{k-(k-d)\} = dk - d^2 + d$$

回である。
その部分の次数が 1 次ずつ下がっていたとすると (すなわち $r_i(x)$ が k 次、$r_{i+1}(x)$ が $(k-1)$ 次、$\cdots$、$r_{i+d}(x)$ が $(k-d)$ 次だったとすると)、$r_i(x) \div r_{i+1}(x),\ r_{i+1}(x) \div r_{i+2}(x),\ \cdots,\ r_{i+(d-1)}(x) \div r_{i+d}(x)$ の計算量は、GF(2) 上の足し算が最大

$$\sum_{j=k-d+1}^{k} 2j = 2dk - d^2 + d$$

回、シフトが最大

$$\sum_{j=k-d+1}^{k} j = dk - \frac{1}{2}d^2 + \frac{1}{2}d$$

回である。この部分の計算量の差をとると、GF(2) 上の足し算については、

$$\begin{aligned}(2dk - d^2 + d) - \{(d+1)k - d^2 + 1\} &= (d-1)k + d - 1 \\ &= (d-1)(k+1) \\ &> 0\end{aligned}$$

となり、シフトについては、

$$\begin{aligned}(dk - \frac{1}{2}d^2 + \frac{1}{2}d) - (dk - d^2 + d) &= \frac{1}{2}d^2 - \frac{1}{2}d \\ &= \frac{1}{2}d(d-1) \\ &> 0\end{aligned}$$

となる。よって、$r_i(x)$ の次数が 1 次ずつ下がる場合の最悪計算量が最大であるので、ユークリッドの互除法を行う部分の計算量は、GF(2) 上の足し算が最大 (n^2+n-2) 回、シフトが最大 $(\frac{1}{2}n^2 + \frac{1}{2}n - 1)$ 回である。

(2) 漸化式 (3.2) の部分の計算量
まず、$q_i(x)$ がすべて 1 次の場合の計算量を求める。この場合は $t_i(x)$ の次数

は 1 次ずつ上がっていき、$m = n - 1$ となっている。
多項式のかけ算 $(q_i(x)t_{i-1}(x))$ については、$t_1(x)$ を求めるときには $t_1(x) = q_1(x)$ なので多項式のかけ算は不要で、$t_2(x)$ を求めるとき 1 次 $\times$ 1 次、$t_3(x)$ を求めるとき 1 次 $\times$ 2 次、$\cdots$、$t_m(x)$ を求めるとき 1 次 $\times$ $(n-2)$ 次である。
(i 次の多項式)$\times$ (j 次の多項式) の計算量が GF(2) 上の足し算が最大 $\{ij + \min(i, j)\}$ 回、シフトが最大 $\{ij + \min(i, j)\}$ 回なので、多項式のかけ算の部分の計算量は、GF(2) 上の足し算が最大

$$\sum_{k=1}^{n-2}(k+1) = \frac{1}{2}n^2 - \frac{1}{2}n - 1$$

回、シフトが最大

$$\sum_{k=1}^{n-2}(k+1) = \frac{1}{2}n^2 - \frac{1}{2}n - 1$$

回である。
次に多項式の足し算の部分の計算量を求める。$t_1(x)$ を求めるときには $t_1(x) = q_1(x)$ なので多項式の足し算は不要で、$t_2(x)$ を求めるとき 0 次 + 2 次、$t_3(x)$ を求めるとき 1 次 + 3 次、$\cdots$、$t_m(x)$ を求めるとき $(n-3)$ 次 + $(n-1)$ 次である。
(i 次の多項式)+ (j 次の多項式) の計算量は GF(2) 上の足し算が $\{\min(i, j)+1\}$ 回なので、多項式の足し算の部分の計算量は、GF(2) 上の足し算が

$$\sum_{k=0}^{n-3}(k+1) = \frac{1}{2}n^2 - \frac{3}{2}n + 1$$

回である。よって、漸化式 (3.2) の部分の $q_i(x)$ がすべて 1 次の場合の計算量は、GF(2) 上の足し算が最大

$$(\frac{1}{2}n^2 - \frac{1}{2}n - 1) + (\frac{1}{2}n^2 - \frac{3}{2}n + 1) = n^2 - 2n$$

回、シフトが最大 $(\frac{1}{2}n^2 - \frac{1}{2}n - 1)$ 回である。
実際には、$q_i(x)$ は 1 次式とは限らないが、$q_i(x)$ がすべて 1 次式の場合の最悪計算量が最大になるということを以下に示す。
$q_k(x)$ が d 次 $(d \geq 2)$ だったとすると、漸化式 (3.2) の部分の計算量は、多項式 $f(x)$ の次数を $|f(x)|$ で表すことにすると、多項式のかけ算 $(q_k(x)t_{k-1}(x))$ の部分で GF(2) 上の足し算が

$$d|t_{k-1}(x)| + \min(d,\ |t_{k-1}(x)|)$$

回、シフトが最大

$$d|t_{k-1}(x)| + \min(d,\ |t_{k-1}(x)|)$$

回であり、多項式の足し算の部分で GF(2) 上の足し算が $\{|t_{k-2}(x)|+1\}$ 回なので、合計で GF(2) 上の足し算が最大

$$d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)+|t_{k-2}(x)|+1$$

回、シフトが最大

$$d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)$$

回である。
その部分の商の次数がすべて 1 次だったとすると (すなわち $q_k(x),\ q_{k+1}(x),\cdots,\ q_{k+d-1}(x)$ が 1 次だったとすると)、その部分の計算量は、多項式のかけ算の部分で GF(2) 上の足し算が最大

$$\sum_{i=1}^{d}\{|t_{k+i-2}(x)|+1\}$$

回、シフトが最大

$$\sum_{i=1}^{d}\{|t_{k+i-2}(x)|+1\}$$

回であり、多項式の足し算の部分で GF(2) 上の足し算が

$$\sum_{i=1}^{d}\{|t_{k+i-3}(x)|+1\}$$

回なので、合計で、GF(2) 上の足し算が最大

$$\sum_{i=1}^{d}\{|t_{k+i-2}(x)|+1\}+\sum_{i=1}^{d}\{|t_{k+i-3}(x)|+1\}$$

回、シフトが最大

$$\sum_{i=1}^{d}\{|t_{k+i-2}(x)|+1\}$$

回である。この部分の計算量の差をとると、GF(2) 上の足し算については、

$$\begin{aligned}
&\{\sum_{i=1}^{d}(|t_{k+i-2}(x)|+1)+\sum_{i=1}^{d}(|t_{k+i-3}(x)|+1)\}\\
&\qquad-\{d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)+|t_{k-2}(x)|+1\}\\
&\geq\ \{\sum_{i=1}^{d}(|t_{k-1}(x)|+1)+|t_{k-2}(x)|+|t_{k-1}(x)+d\}\\
&\qquad-\{d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)+|t_{k-2}(x)|+1\}\\
&=\ (d|t_{k-1}(x)|+d+|t_{k-2}(x)|+|t_{k-1}(x)|+d)\\
&\qquad-\{d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)+|t_{k-2}(x)|+1\}\\
&=\ 2d+|t_{k-1}(x)|-\min(d,\ |t_{k-1}(x)|)-1\\
&=\ d+|t_{k-1}(x)|-\min(d,\ |t_{k-1}(x)|)+d-1\\
&>\ 0
\end{aligned}$$

となり、シフトについては、

$$\begin{aligned}
&\sum_{i=1}^{d}(|t_{k+i-2}(x)|+1)-\{d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)\}\\
&\quad\geq\ \sum_{i=1}^{d}(|t_{k-1}(x)|+1)-\{d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)\}\\
&\quad=\ d|t_{k-1}(x)|+d-\{d|t_{k-1}(x)|+\min(d,\ |t_{k-1}(x)|)\}\\
&\quad=\ d-\min(d,\ |t_{k-1}(x)|)\\
&\quad\geq\ 0
\end{aligned}$$

となる。よって、$q_i(x)$ がすべて 1 次の場合の最悪計算量が最大であるので、漸化式 (3.2) の部分の計算量は、GF(2) 上の足し算が最大 (n^2-2n) 回、シフトが最大 $(\frac{1}{2}n^2-\frac{1}{2}n-1)$ 回である。

(1), (2) より、STEP3 の計算量は、GF(2) 上の足し算が最大

$$(n^2+n-2)+(n^2-2n)=2n^2-n-2$$

回、シフトが最大

$$(\frac{1}{2}n^2+\frac{1}{2}n-1)+(\frac{1}{2}n^2-\frac{1}{2}n-1)=n^2-2$$

回である。

3.3.4 STEP4 の計算量

GF(2) 上の多項式の 2 乗は、各項の 2 乗の和なので、$\{1/f(x)\}^2$ の計算量は、シフトが n 回以下である。次に、$\bmod p_n(x)$ の計算量は、$\{1/f(x)\}^2$ の次数は最大で $2n-2$ なので、GF(2) 上の足し算が最大

$$(n+1)(2n-2-n+1)=n^2-1$$

回、シフトが最大

$$(n+1)(2n-2-n)=n^2-n-2$$

回である。

よって、STEP4 の計算量は、GF(2) 上の足し算が最大 (n^2-1) 回、シフトが最大

$$n+(n^2-n-2)=n^2-2$$

回である。

3.3.5 STEP5の計算量

(i) n が奇数のとき
n が奇数のときは、1 のトレースがつねに 1 となるので、$\theta(x) = 1$ とすればよい。

(ii) n が偶数のとき
GF(2^n) の 2^n 個の元のうち、トレースが 1 の元が 2^{n-1} 個、トレースが 0 の元が 2^{n-1} 個あるので、ランダムに元を選んでトレースを計算するということをトレースが 1 になるまで繰り返すという方法をとると、各回の試行でトレースが 1 になる確率は $\frac{1}{2}$ なので、k 回目で初めてトレースが 1 になる確率は $(\frac{1}{2})^k$ である。よって、初めてトレースが 1 となるまでの試行回数の平均は、

$$\begin{aligned}\sum_{k=1}^{\infty} k(\frac{1}{2})^k &= \lim_{n\to\infty}\{2 - (\frac{1}{2})^{n-1} - \frac{n}{2^n}\} \\ &= 2\end{aligned}$$

回である。

トレースを求めるには、

$$\begin{aligned}a^2 &= a \cdot a \pmod{p_n(x)} \\ a^4 &= a^2 \cdot a^2 \pmod{p_n(x)} \\ a^8 &= a^4 \cdot a^4 \pmod{p_n(x)} \\ &\vdots \\ a^{2^{n-1}} &= a^{2^{n-2}} \cdot a^{2^{n-2}} \pmod{p_n(x)}\end{aligned}$$

のように、2 乗して $\bmod p_n(x)$ をとるということを繰り返してから、$a^1, a^2, \cdots, a^{2^{n-1}}$ の和をとればよい。トレースの値は、必ず 0 か 1 になるので、$a^1, a^2, \cdots, a^{2^{n-1}}$ の和をとるときには、0 次の項のみの和をとればよい。

STEP4 と同様にして、1 回多項式を 2 乗して $\bmod p_n(x)$ をとる計算量は GF(2) 上の足し算が最大 (n^2-1) 回、シフトが最大 (n^2-2) 回である。それを $(n-1)$ 回行うと、GF(2) 上の足し算が最大

$$(n^2-1)(n-1) = n^3 - n^2 - n + 1$$

回、シフトが最大

$$(n^2-2)(n-1) = n^3 - n^2 - 2n + 2$$

回必要である。

$a^1, a^2, \cdots, a^{2^{n-1}}$ の 0 次の項の和をとる計算量は、GF(2) 上の足し算が $(n-2)$ 回である。

よってトレースの計算量は、GF(2) 上の足し算が最大

$$n^3 - n^2 - n + 1 + n - 2 = n^3 - n^2 - 1$$

回、シフトが最大 $(n^3 - n^2 - 2n + 2)$ 回となる。

よって、n が偶数のときの STEP5 の平均計算量は、GF(2) 上の足し算が

$$2(n^3 - n^2 - 1) = 2n^3 - 2n^2 - 2$$

回以下、シフトが

$$2(n^3 - n^2 - 2n + 2) = 2n^3 - 2n^2 - 4n + 4$$

回以下である。

この方法では最悪計算量が無限大になるので、最悪計算量を有限にするには、同じ多項式のトレースは計算しないようにすればよい。しかし、そうしたとしても、トレースの計算を最大 2^{n-1} 回行う (2^{n-1} 回行ってすべてトレースが 0 になった場合は、それ以外のすべての元はトレースが 1 なので、それ以上トレースの計算はする必要がない。) ので、最悪計算量は指数関数的になる。よって現段階では、STEP5 の、n が偶数の場合の最悪計算量を多項式オーダーに抑えることはできない。

3.3.6 STEP6 の計算量

(i) n が奇数のとき

n が奇数のときは $\theta(x) = 1$ とするので、

$$\begin{aligned}
\beta(x) &= g(x) + (g(x) + g(x)^2) + \cdots + (g(x) + g(x)^2 + \cdots + g(x)^{2^{n-1}}) \\
&= g(x)^2 + g(x)^8 + g(x)^3 2 + \cdots + g(x)^{2^{n-1}} \\
&= \sum_{i=1}^{\frac{n-1}{2}} g(x)^{2^{2i-1}}
\end{aligned}$$

を計算すればよい。これを求めるときには、多項式を 2 乗して $\bmod p_n(x)$ をとるという計算を $(n-2)$ 回行い、多項式の足し算を $(\frac{n-1}{2} - 1)$ 回行う。STEP4 と同様にして、1 回多項式を 2 乗して $\bmod p_n(x)$ をとる計算量は GF(2) 上の足し算が最大 $(n^2 - 1)$ 回、シフトが最大 $(n^2 - 2)$ 回である。それを $(n - 2)$ 回行うと、GF(2) 上の足し算が最大

$$(n^2 - 1)(n - 2) = n^3 - 2n^2 - n + 2$$

回、シフトが最大

$$(n^2 - 2)(n - 2) = n^3 - 2n^2 - 2n + 4$$

回必要である。多項式の足し算は、最大次数が $n-1$ なので 1 回につき GF(2) 上の足し算を最大

$$n-1+1=n$$

回行うので、$(\frac{n-1}{2}-1)$ 回では最大

$$n(\frac{n-1}{2}-1)=\frac{1}{2}n^2-\frac{3}{2}n$$

回である。よって、n が奇数のときの STEP6 の計算量は、GF(2) 上の足し算が最大

$$(n^3-2n^2-n+2)+(\frac{1}{2}n^2-\frac{3}{2}n)=n^3-\frac{3}{2}n^2-\frac{5}{2}n+2$$

回、シフトが最大 (n^3-2n^2-2n+4) 回である。

(ii) n が偶数のとき
多項式を 2 乗して $\bmod p_n(x)$ をとるという計算を、$g(x)$ の方で $(n-2)$ 回行い、$\theta(x)$ の方で $(n-1)$ 回行うので、合計で

$$n-2+n-1=2n-3$$

回行う。STEP4 と同様にして、1 回多項式を 2 乗して $\bmod p_n(x)$ をとる計算量は GF(2) 上の足し算が最大 (n^2-1) 回、シフトが最大 (n^2-2) 回である。それを $(2n-3)$ 回おこなうと、GF(2) 上の足し算が最大

$$(n^2-1)(2n-3)=2n^3-3n^2-2n+3$$

回、シフトが最大

$$(n^2-2)(2n-3)=2n^3-3n^2-4n+6$$

回必要である。

多項式の足し算は合計で $(2n-4)$ 回行う。多項式の足し算は 1 回につき GF(2) 上の足し算を最大 n 回行うので、$(2n-4)$ 回では最大

$$n(2n-4)=2n^2-4n$$

回である。

多項式のかけ算をして $\bmod p_n(x)$ をとるという計算を $(n-1)$ 回行う。多項式のかけ算 1 回の計算量は、GF(2) 上の足し算が最大

$$n(n-1)=n^2-n$$

回、シフトが最大

$$n(n-1) = n^2 - n$$

回である。そのあと mod $p_n(x)$ をとる計算量は、かけ算をした結果の最大次数が $2n-2$ なので、GF(2) 上の足し算が最大

$$(n+1)(2n-2-n+1) = n^2 - 1$$

回、シフトが最大

$$(n+1)(2n-2-n) = n^2 - n - 2$$

回である。よって、1 回多項式のかけ算をして mod $p_n(x)$ をとる計算量は、GF(2) 上の足し算が最大

$$n^2 - n + n^2 - 1 = 2n^2 - n - 1$$

回、シフトが最大

$$n^2 - n + n^2 - n - 2 = 2n^2 - 2n - 2$$

回である。それを $(n-1)$ 回行うと、GF(2) 上の足し算が最大

$$(2n^2 - n - 1)(n-1) = 2n^3 - 3n^2 + 1$$

回、シフトが最大

$$(2n^2 - 2n - 2)(n-1) = 2n^3 - 4n^2 + 2$$

回必要である。よって、n が偶数のときの STEP6 の計算量は、GF(2) 上の足し算が最大

$$(2n^3 - 3n^2 - 2n + 3) + (2n^2 - 4n) + (2n^3 - 3n^2 + 1) = 4n^3 - 8n^2 - 6n + 4$$

回、シフトが最大

$$(2n^3 - 3n^2 - 4n + 6) + (2n^3 - 4n^2 + 2) = 4n^3 - 7n^2 - 4n + 8$$

回である。

3.3.7 STEP7 の計算量

かけ算をして mod $p_n(x)$ をとるという計算を 1 回おこなうので、STEP6 と同様にして、GF(2) 上の足し算が最大 $(2n^2 - n - 1)$ 回、シフトが最大 $(2n^2 - 2n - 2)$ 回である。

3.3.8 STEP8 の計算量

これは、構成法 2 の STEP4 と全く同じなので、計算量は、GF(2) 上の足し算が最大 (n^2+n) 回、シフトが最大 $(\frac{1}{2}n^2+\frac{1}{2}n)$ 回である。

3.3.9 構成法 3 の計算量の合計

以上をまとめると、次のようになる。

表 3.2: 構成法 3 の計算量

		GF(2) 上の足し算	シフト
STEP1	(n:偶数)	0	$\frac{n}{2}$
	(n:奇数)	0	$\frac{n+1}{2}$
STEP2		$3n+2$	$2n+1$
STEP3		$2n^2-n-2$	n^2-2
STEP4		n^2-1	n^2-2
STEP5	(n:偶数)	$2n^3-2n^2-2$	$2n^3-2n^2-4n+4$
	(n:奇数)	0	0
STEP6	(n:偶数)	$4n^3-8n^2-6n+4$	$4n^3-7n^2-4n+8$
	(n:奇数)	$n^3-\frac{3}{2}n^2-\frac{5}{2}n+2$	n^3-2n^2-2n+4
STEP7		$2n^2-n-1$	$2n^2-2n-2$
STEP8		n^2+n	$\frac{1}{2}n^2+\frac{1}{2}n$
合計	(n:偶数)	$6n^3-4n^2-4n$	$6n^3-\frac{9}{2}n^2-8n+7$
	(n:奇数)	$n^3+\frac{9}{2}n^2-\frac{1}{2}n$	$n^3+\frac{5}{2}n^2-n-\frac{1}{2}$

(STEP5 は、平均計算量である。)

第4章　各構成法の実行時間

以下に、いくつかの GF(2) 上の原始既約多項式に対する実行時間を示す。(CPU 時間は SPARCstation 20 での値である。)

表 4.1: 実行例

原始既約多項式	CPU 時間 [秒]		セルオートマトン
	構成法 2	構成法 3	
x^6+x+1	0.140	0.030	011000
x^7+x+1	0.140	0.020	1011001
$x^{20}+x^3+1$	0.150	0.050	01101011100001010110
$x^{40}+x^{21}+x^{19}+x^2+1$	0.150	0.150	1100110000011000000100010100000100110011
$x^{60}+x+1$	0.180	0.340	1110011110100101110100001011110011010000101110100101111001
$x^{80}+x^{38}+x^{37}+x+1$	0.220	0.730	0101011001000010000010100011001111011110111101010110111011100000100001001101010
$x^{99}+x^{47}+x^{45}+x^2+1$	0.290	0.220	略
$x^{100}+x^{37}+1$	0.270	1.310	略
$x^{199}+x^{34}+1$	0.800	1.580	略
$x^{200}+x^{163}+x^2+x+1$	1.210	15.710	略
$x^{299}+x^{21}+x^2+x+1$	1.510	4.270	略
$x^{300}+x^7+1$	1.540	32.220	略

第5章　結論

5.1　計算量、実行時間の比較

- 計算量について構成法2と構成法3を比較すると、どちらも n^3 のオーダーだが、構成法2のほうが係数が小さい。
- 実行時間について構成法2と構成法3を比較すると、次数が低いときには構成法3の方がCPU時間が短いが、次数が高くなると、構成法3の方がCPU時間が長くなる。n が偶数でかつ次数が高いときに、構成法3のCPU時間が特に長くなっている。

よって、構成法2と構成法3とでは、構成法2の方が優れていると結論付けることができる。

5.2　今後の課題

- 構成法1の平均計算量を求める。
- 最大周期のセルオートマトンの新たな構成法を探す。

謝辞

本研究は様々な人の助力の上に成立しました。
指導教官の伏見正則先生は、研究の指針を与えて下さって、途中で問題が生じた時には、有効な助言をして下さいました。
助手の諸星穂積氏は、いろいろと質問に答えて下さいました。
数理第二研究室の松井知己先生、大学院生、卒論生の皆さんにもいろいろとお世話になりました。
以上の方々に心から感謝します。

参考文献

[1] S. Wolfram. Statistical mechanics of cellular automata. *Reviews of Modern Physics*, 55:601–644, 1983.

[2] Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, 1986.

[3] Kevin Cattel and Jon C. Muzio. An explicit similarity transform between cellular automata and LFSR matrices. *Manuscript*, University of Victoria, 1996.

[4] P. H. Bardell. Analysis of celllular automata used as pseudorandom pattern generators. *Proc. 1990 International Test Conference*, 762-768, 1990.

[5] Shu Tezuka and Masanori Fushimi. A method of designing cellular automata as pseudorandom number generators for built-in self-test for VLSI. *Contemporary Mathematics*, 168:363–367, 1994.

[6] J. P. Mesirov and M. M. Sweet. Continued fraction expansions of rational expressions with irreducible denominators in characteristic 2. *Journal of Number Theory*, 27:144–148, 1987.

[7] Kevin Cattel and Jon C. Muzio. Synthesis of one-dimensional linear hybrid cellular automata. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 15:325–335, 1996.

[8] 高橋 磐郎. **組合せ理論とその応用**. 岩波書店, 1979.

[9] R. J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer, 1987.