Defence Science Journal, Vol. 66, No. 6, November 2016, pp. 605-611, DOI : 10.14429/dsj.66.10801

On the Number of Integer Recurrence Relations

Yogesh Kumar[#,*], N.R. Pillai[@], and R.K. Sharma[#]

[#]*Indian Institute of Technology Delhi, New Delhi - 110 016, India*
[@]*Scientific Analysis Group, Delhi - 110 054, India*
[*]*E-mail: yogesh_lather@yahoo.co.in*

ABSTRACT

This paper presents the number of k-stage integer recurrence relations (IRR) over the ring $\mathbb{Z}_{2^e}$ which generates sequences of maximum possible period $(2^k-1)2^{e-1}$ for $e \geq 1$. This number corresponds to the primitive polynomials mod 2 which satisfy the condition proposed by Brent and is $2^{(e-2)k+1}(2^{k-1}-1)$ for $e \geq 3$. This number is same as measured by Dai but arrived at with a different condition for maximum period. Our way of counting gives an explicit method for construction of such polynomials. Furthermore, The number of different sequences corresponding to such IRRs of maximum period is also presented.

Keywords: Linear feedback shift register, maximum period, primitive polynomial, LFSR

1. INTRODUCTION

In order to measure the security of sequences generated by any pseudorandom number generator, designers have to count the number of possible seeds and properties of feedback polynomial for the generator. In the case of k-stage linear feedback shift register (LFSR), number of possible seeds and number of feedback polynomials for maximum period 2^k-1 are well known[1,2].

The feedback polynomial of degree k which generates sequences of period 2^k-1 is a primitive polynomial of degree k over the finite field $GF(2)$. We know the number of primitive polynomials of degree k over the finite field $GF(2)$ and given by the formula[2] $\Phi(2^k-1)/k$, where Φ is the Euler's totient function.

Also the number of different sequences of period 2^k-1 generated by k-stage LFSR is equal to the number of primitive polynomials of degree k over the finite field $GF(2)$. For a given sequence over a finite field, the Berlekamp-Massey algorithm[3] finds the shortest linear feedback shift register that can generate the sequence.

Integer recurrence relations (equivalently Lagged Fibonacci Generators (LFG)) have been used as pseudorandom number generators[4] and became popular in recent years. The streams generated by the recurrence relation are integer sequences over the ring $\mathbb{Z}_{2^e}$, $e \geq 1$. In 1933 Ward[5] proposed a condition for maximum period of a sequence and condition for maximum period was nicely presented in 1992 by Dai[6]. Dai[6] also counted the number of feedback polynomials over the ring $\mathbb{Z}_{2^e}[x]$ for a k-stage IRR with the condition proposed by Ward.

Also another but independent condition for maximum period of a sequence over the ring $\mathbb{Z}_{2^e}$, $e \geq 1$ was proposed by Brent[4], in 1994. This condition was on the feedback polynomial $f(x)$ of degree k which generates the sequences modulo 2^e of maximum period $(2^k-1)2^{e-1}$ (polynomial with maximum period is called primitive polynomial over the ring $\mathbb{Z}_{2^e}$. The synthesis algorithm to find the shortest linear (integer) recurrence relation that can generate a given sequence over the finite ring modulo m, (m is an integer) was given by Reeds and Sloane[7].

For LFSR, primitive feedback polynomial of degree k over $GF(2)$ covers all states except zero state i.e. (2^k-1) states. But in case of IRR, this is not the case; that means a primitive polynomial of degree k over the ring $\mathbb{Z}_{2^e}$ can generate $2^{(e-1)(k-1)}$ shift distinct sequences as given in references[6,8].

This paper focuses on the number of polynomials which generate sequences of maximum period with respect to Brent's[4] condition and corresponding number of different sequences of maximum period for a k-stage IRR. Another contribution of the paper is that it explicitly gives a method for construction of primitive polynomials of degree k over the ring $\mathbb{Z}_{2^e}$ which satisfies Brent's condition for maximum period.

2. PRELIMINARIES

In this section, we give some notations and definitions for integer recurrence relations that will be used in the subsequent sections. These notations are basically related to the paper of Brent[4], since our focus is on Brent's condition. We denote a not congruent to b mod n by $a \neq b$ mod n.

The 2-stage integer recurrence relation also called Fibonacci recurrence relation is given as:

$$s_n = s_{n-1} + s_{n-2} \quad for \ n \geq 2$$

Received : 08 April 2016, Revised : 19 May 2016
Accepted : 25 July 2016, Online published : 31 October 2016

The generalisation of integer recurrence relation (also called generalised Fibonacci recurrence relation) as a pseudo-random number generator is defined as:

Definition 1

Let $a_1, a_2, ..., a_k \in \mathbb{Z}_{p^e}$ $e \ge 1$. Given any k-tuple $(s_0, s_1, ..., s_{k-1})$ elements of $\mathbb{Z}_{p^e}$, let $s^\infty = (s_0, s_1, ...)$ denote the infinite sequence of elements of $\mathbb{Z}_{p^e}$, determined by the following linear recurrence relation:

$$s_n \equiv (a_1 s_{n-1} + ... + a_k s_{n-k}) \bmod p^e, k \le n \qquad (1)$$

The system is called k-stage integer recurrence relation (IRR) or Lagged Fibonacci Generator (LFG) over the ring $\mathbb{Z}_{p^e}$, while the sequence s^∞ is referred to as the sequence generated by IRR (1). The k-tuple $(s_0, s_1, ..., s_{k-1})$ is called initial state of the IRR (1).

The polynomial $x^k - a_1 x^{k-1} - ... - a_k$ is called the polynomial of the IRR (1).

Definition[2] 2

Let $f(x) \in \mathbb{F}_p[x]$ be a non-zero polynomial of degree k. If $f(0) \ne 0$, then the least positive integer $\lambda(p)$ for which $f(x)$ divides $x^{\lambda(p)} - 1$ is called the order of $f(x)$ or period of $f(x)$. In other words $x^{\lambda(p)} \equiv 1 \bmod \big(p, f(x)\big)$.

If $\lambda(p) = p^k - 1$, then $f(x)$ is called a primitive polynomial of degree k over the field $\mathbb{F}_p$.

A congruence relation over modulo an integer m, and a polynomial $f(x)$ is defined as:

Definition[4,9] 3

If $f(x), a(x), b(x)$ are polynomials with integer coefficients. Then $a(x) \equiv b(x) \bmod \big(m, f(x)\big)$ if $a(x) = b(x) + f(x)u(x) + mv(x)$ for some polynomials $u(x)$ and $v(x)$ with integer coefficients.

Since $\mathbb{F}_p$ and $\mathbb{Z}_p$ are equivalent, therefore the definition of order over the finite field $\mathbb{F}_p$ (or $\mathbb{Z}_p$) has been extended over the finite ring $\mathbb{Z}_{p^e}$ as:

Definition[5,6] 4

Let $f(x) \in \mathbb{F}_p[x]$ be a non-zero polynomial of degree k. If $f(0) \ne 0$, then the least positive integer $\lambda(p^e)$ for which $x^{\lambda(p^e)} \equiv 1 \bmod \big(p^e, f(x)\big)$ is called the order of $f(x)$ or period of $f(x) \bmod p^e$. The maximum possible period of $f(x)$ is $p^{e-1}(p^k - 1)$ and such a polynomial is called a primitive polynomial of degree k over $\mathbb{Z}_{p^e}$.

For $p = 2$, the maximum possible period and condition for it is given in the following proposition (we call it Brent's condition).

Proposition[4,9] 1

Let $f(x) = x^k - a_1 x^{k-1} - ... - a_k$ be a primitive polynomial modulo 2, and suppose that $s_0, s_1, ..., s_{k-1}$ are integers not all even.

(a) The period of the recurrence relation (1) $\bmod 2^e$ is $(2^k - 1)2^{e-1}$ for all $e \ge 1$ if and only if

$$\begin{aligned} &f(x)^2 + f(-x)^2 \ne 2f(x^2) \pmod{2^3} \ \mathit{and} \\ &f(x)^2 + f(-x)^2 \ne 2(-1)^k f(-x^2) \pmod{2^3} \end{aligned} \qquad (2)$$

(b) The primitive polynomial $f(x) = x^k + x^l + 1 \bmod 2$, $k > 2$ always has period $(2^k - 1)2^{e-1}$ for all $e \ge 1$.

The following proposition gives the number of different sequences with maximum possible period generated through IRR (1) for $p = 2$.

Proposition[8] 2

There exist $2^{(e-1)(k-1)}$ different sequences of period $(2^k - 1)2^{e-1}$ for all $e \ge 1$ for a primitive polynomial which satisfies the Eqn (2).

3. TRINOMIAL OF DEGREE $k > 2$

In this section, we will find the number of k-stage integer recurrence relations over the ring $\mathbb{Z}_{2^e}$ which generate sequences of maximum possible period $(2^k - 1)2^{e-1}, e \ge 1$ and correspond to a primitive trinomial $\bmod 2$.

Let $g(x) = \sum_{i=0}^{k} a_i x^i$, where $a_k = 1$, be a polynomial of degree k over the ring $\mathbb{Z}_{2^e}$, then for the initial state $(s_0, s_1, ..., s_{k-1})$, the corresponding integer recurrence relation is

$$s_n \equiv -(a_{k-1} s_{n-1} + ... + a_0 s_{n-k}) \bmod 2^e \qquad (3)$$

The relation (1) and relation (3) are equivalent in the sense of polynomial, so for convenience relation (3) is used throughout the paper.

It is enough to enumerate the number of recurrence relations (3) which generate sequences of maximum possible period $(2^k - 1)2^{e-1}$ with the seed $s_0, s_1, ..., s_{k-1}$ and with at least one odd s_i.

Let $f(x) = x^k + x^l + 1$ be a primitive polynomial modulo 2, then either k is odd and l is even or k is even and l is odd or both k, l are odd. If we take both k, l even then $f(x)$ becomes reducible polynomial modulo 2 as for $k = 2k'$, $l = 2l'$ for some integer k', l', we have $f(x) = x^{2k'} + x^{2l'} + 1 = (x^{k'} + x^{l'} + 1)^2$ in modulo 2. Therefore, we discuss only three cases of primitive trinomial mod 2.

The condition of equivalence between $f(x)$ and $g(x)$ modulo 2 is given by the following obvious lemma.

Lemma 1

Let $g(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, where $a_k = 1$ and $f(x) = x^k + x^l + 1$, then $g(x) \equiv f(x) \bmod 2$ if and only if $\gcd(a_i, 2) = 2, 1 \le i \, (i \ne l) \le k-1$ and $\gcd(a_l, 2) = 1 = \gcd(a_0, 2)$.

If $g(x) \equiv f(x) \bmod 2$, then it is not necessary that non-trivial sequences generated by $g(x)$ have maximum possible period.

For instance $g(x) = x^5 + 4x^4 + 4x^3 + x^2 + 2x + 13 \in \mathbb{Z}_{2^4}[x]$ is equivalent to a primitive polynomial $f(x) = x^5 + x^2 + 1 \bmod 2$, but $g(x)$ does not generate sequences of maximum possible period.

Next theorem gives the condition on a_i's of $g(x)$ for the maximum possible period.

Theorem 1

Let $f(x)$ be a primitive trinomial $\bmod 2$, where k odd, l even, and $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, where $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$. The period of the sequence corresponding to the recurrence relation (3) given by $g(x)$ is less than $(2^k-1)2^{e-1}$ for all $e\ge 3$ if and only if

i. $a_i = 4r\ for\ 1\le i(\ne l, l/2)\le k-1, r\ge 0$ and

ii. $a_{l/2}=2r$ for odd values of $r\ge 1$ and

iii. $a_i=4r+1\ or\ 4r+3,\ r\ge 0$ for $i=0,l$ that means both a_0 and a_l have value either $4r+1\ or\ 4r+3$.

To prove Theorem 1, we first prove the following lemmas.

Lemma 2

Let $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1$ be a polynomial of degree k. Then

$$g(x)^2+g(-x)^2-2g(x^2)=2\sum_{i=0}^{k-1}a_i(a_i-1)x^{2i}+4\sum_{\substack{0\le i<j\le 2k,\\ i+j=2m}} a_ia_jx^{i+j},$$

where $0<m<k$.

Proof: For given $g(x)$,

$$(g(x))^2=(\sum_{i=0}^{k}a_ix^i)^2=\sum_{i=0}^{k}a_i^2x^{2i}+2\sum_{i=0}^{k-1}\sum_{j>i}^{k}a_ia_jx^{i+j}.$$

Replacing x by $-x$ we get,

$$(g(-x))^2=\sum_{i=0}^{k}a_i^2x^{2i}+2\sum_{0\le i<j\le k}a_ia_j(-1)^{i+j}x^{i+j}.$$

Therefore,

$$(g(x))^2+(g(-x))^2=2\sum_{i=0}^{k}a_i^2x^{2i}+2\sum_{0\le i<j\le k}a_ia_j(1+(-1)^{i+j})x^{i+j}$$

$$=2\sum_{i=0}^{k}a_i^2x^{2i}+4\sum_{\substack{0\le i<j\le k,\\ i+j=2m}}a_ia_jx^{i+j}, 0<m<k.$$

Also,

$$g(x^2)=\sum_{i=0}^{k}a_ix^{2i}.$$

Therefore,

$$(g(x))^2+(g(-x))^2-2g(x^2)=2\sum_{i=0}^{k-1}a_i(a_i-1)x^{2i}+4\sum_{\substack{0\le i<j\le k,\\ i+j=2m}}a_ia_jx^{i+j}, 0<m<k.$$

Lemma 3

Let $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1$ be a polynomial of degree k. Then

$$g(x)^2+g(-x)^2-(-1)^k2g(-x^2)=2\sum_{i=0}^{k-1}a_i(a_i-(-1)^{i+k})x^{2i}+4\sum_{\substack{0\le i<j\le 2k,\\ i+j=2m}}a_ia_jx^{i+j},$$

where $0<m<k$.

Lemma 4

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k odd, l even and $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x],\ a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$. Then

$$g(x)^2+g(-x)^2-2g(x^2)\equiv 0 \bmod 8 \tag{4}$$

if and only if

i. $a_i=4r$ for $1\le i(\ne l, l/2)\le k-1,\ r\ge 0$ and

ii. $a_{l/2}=2r$ for odd values of $r\ge 1$ and

iii. $a_i=4r+1,\ r\ge 0$ for $i=0, l$.

Proof: Using Lemma 2,

$g(x)^2+g(-x)^2-2g(x^2)\equiv 0 \bmod 8$

if and only if

$$2\sum_{i=0}^{k-1}a_i(a_i-1)x^{2i}+4\sum_{\substack{0\le i<j\le k,\\ i+j=2m}}a_ia_jx^{i+j}\equiv 0 \bmod 8$$

if and only if coefficient of each power of x is zero mod 8. That is $2a_0(a_0-1)\equiv 0 \bmod 8$ and

$$2a_m(a_m-1)+4\sum_{\substack{0\le i<j\le k,\\ i+j=2m}}a_ia_j\equiv 0 \bmod 8 \text{ for } 1\le m\le k-1.$$

Since a_0 and a_l are only odd terms, therefore

$$4\sum_{\substack{0\le i<j\le k,\\ i+j=2m}}a_ia_j \bmod 8\equiv\begin{cases}4a_la_0 & if\ \ m=\dfrac{l}{2}\\ 0, & otherwise\end{cases}$$

Thus Eqn. (4) holds if and only if

$$2\sum_{i=0}^{k-1}a_i(a-1)x^{2i}+4a_0a_lx^l\equiv 0 \bmod 8$$

if and only if

$$2a_i(a_i-1)\equiv 0 \bmod 8 \text{ for } 0\le i(\ne \tfrac{l}{2})\le k-1 \text{ and} \tag{5}$$

$$2a_{\frac{l}{2}}(a_{\frac{l}{2}}-1)+4a_0a_l\equiv 0 \bmod 8 \tag{6}$$

Since a_0 and a_l are odd, therefore Eqn. (5) holds if and only if

$a_i=4r$ for $1\le i(\ne l, \frac{l}{2})\le k-1,\ r\ge 0$ and

$a_i=4r+1$ for $i=0, l.$

The Eqn. (6) holds if and only if $a_{l/2}=2r$, where r is an odd integer.

Lemma 5

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k odd, l even and $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x],\ a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$. Then

$$g(x)^2+g(-x)^2-(-1)^k2g(-x^2)\equiv 0 \bmod 8 \tag{7}$$

if and only if

i. $a_i=4r$ for $1\le i(\ne l, l/2)\le k-1,\ r\ge 0$ and

ii. $a_{l/2}=2r$ for odd values of $r\ge 1$ and

iii. $a_i=4r+3,\ r\ge 0$ for $i=0, l.$

Proof of Theorem 1

From Equation (2), the period of sequences corresponding to $g(x)$ is less than the maximum possible for $e\ge 3$ if and only if either Equation (4) holds or Equation (7) hold or both holds.

Using Lemma 4 and 5, conditions hold if and only if

$a_i=4r$ for $1\le i(\ne l, l/2)\le k-1,\ r\ge 0$ and

$a_{l/2}=2r,$ where r is an odd integer, $r\ge 1$ and

both a_0 and a_l have values either $4r+1\ or\ 4r+3.$

Hence the result.

Corollary 1

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k odd, l even. Then the number of $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$ and corresponding sequences have period less than $(2^k-1)2^{e-1}$ for all $e\geq 3$ is $2^{(e-2)k+1}$.

Proof: Using Theorem 1, the number of choices for each a_i's, $1\leq i(\neq l, l/2)\leq k-1$ and $a_{l/2}$ has 2^{e-2} choices for odd values of r. Furthermore, a_l and a_0 has form either $4r+1$ *or* $4r+3$, then their number of choices is $2^{(e-1)+(e-2)}$, because of their dependencies. Hence the number of desired $g(x)$ is $2^{(e-2)(k-3)}2^{e-2}2^{(e-1)+(e-2)}=2^{(e-2)k+1}$.

Corollary 2

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k odd, l even. The number of $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$ and corresponding sequence has maximum period $(2^k-1)2^{e-1}$ is $2^{(e-2)k+1}(2^{k-1}-1)$ for all $e\geq 3$.

Proof: Clearly total choices for $g(x)$ such that $g(x)\equiv f(x) \bmod 2$ is $2^{(e-1)k}$ and choices for those $g(x)$ which generate sequences of lesser period is $2^{(e-2)k+1}$. Therefore, the number of $g(x)$ which generate sequences of maximum period is $2^{(e-2)k+1}(2^{k-1}-1)$.

Example Take $f(x)=x^5+x^2+1$ which is a primitive polynomial modulo 2 of degree 5. Let $g(x)=a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+x^5$ be a polynomial of degree 5 over the ring $\mathbb{Z}_{2^4}$ such that $g(x)\equiv f(x)$ mod 2. The polynomial $g(x)$ satisfies Eqn. (4) if and only if the coefficients a_i's take any value out of the following $a_0\in\{1,5,9,13\}$, $a_1\in\{2,6,10,14\}$, $a_2\in\{1,5,9,13\}$, $a_3\in\{0,4,8,12\}$, and $a_4\in\{0,4,8,12\}$.

The polynomial $g(x)$ satisfies Eqn. (7) if and only if the coefficients a_i's take any value out of the following $a_0\in\{3,7,11,15\}$, $a_1\in\{2,6,10,14\}$, $a_2\in\{3,7,11,15\}$, $a_3\in\{0,4,8,12\}$, and $a_4\in\{0,4,8,12\}$. Then the number of choices for polynomial $g(x)$ to satisfy Eqns. (4) and (7) simultaneously is $2(2^2 2^2).(2^2).(2^2).(2^2)=2^{11}$, which is equal to the formula, given in Corollary 1. Therefore, the number of primitive polynomials $g(x)\in\mathbb{Z}_{2^4}[x]$ corresponding to $f(x)$ is $2^{11}(2^4-1)$.

Lemma 6

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k even, l odd, and $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$. Then

$$g(x)^2+g(-x)^2-2g(x^2)\equiv 0 \text{ mod } 8$$

if and only if

i. $a_i=4r$ for $1\leq i(\neq l, k/2)\leq k-1,\ r\geq 0$ and

ii. $a_{k/2}=2r$ for odd values of $r\geq 1$ and

iii. $a_i=4r+1,\ r\geq 0$ for $i=0,\ l$.

Lemma 7

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k even, l odd, and $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$. Then

$$g(x)^2+g(-x)^2-2(-1)^k g(-x^2)\equiv 0 \text{ mod } 8$$

if and only if

i. $a_i=4r$ for $1\leq i(\neq l, k/2)\leq k-1,\ r\geq 0$ and

ii. $a_{k/2}=2r$ for odd values of $r\geq 1$ and

iii. $a_l=4r+3,\ r\geq 0$ and

iv. $a_0=4r+1,\ r\geq 0$.

Theorem 2

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k even, l odd, and $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$. The period of the sequence corresponding to the recurrence relation (3) given by $g(x)$ is less than $(2^k-1)2^{e-1}$ for all $e\geq 3$ if and only if

i. $a_i=4r$ for $1\leq i(\neq l, k/2)\leq k-1,\ r\geq 0$ and

ii. $a_{k/2}=2r$ for odd values of $r\geq 1$ and

iii. $a_l=2r+1,\ r\geq 0$ and

iv. $a_0=4r+1,\ r\geq 0$.

Proof: Using Lemma 6 and 7, result holds.

Corollary 3

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k even, l odd. The number of $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$ and corresponding sequences have period

i. less than $(2^k-1)2^{e-1}$ is $2^{(e-2)k+1}$ for all $e\geq 3$.

ii. $(2^k-1)2^{e-1}$ is $2^{(e-2)k+1}(2^{k-1}-1)$ for all $e\geq 3$.

Theorem 3

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k odd, l odd, and $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, $a_k=1,\ k>2$ such that $g(x)\equiv f(x) \bmod 2$. The period of the sequence corresponding to the recurrence relation (3) given by $g(x)$ is less than $(2^k-1)2^{e-1}$ for all $e\geq 3$ if and only if

i. $a_i=4r$ for $1\leq i(\neq l, (k+l)/2)\leq k-1,\ r\geq 0$ and

ii. $a_{(k+l)/2}=2r$ for odd values of $r\geq 1$ and

iii. $a_l=4r+1,\ r\geq 0$ and

iv. $a_0=2r+1,\ r\geq 0$.

Corollary 4

Let $f(x)$ be a primitive trinomial mod 2 of degree k, for k odd, l odd. The number of $g(x)=\sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$,

$a_k = 1, k > 2$ such that $g(x) \equiv f(x) \bmod 2$ and corresponding sequences have period

i. less than $(2^k - 1)2^{e-1}$ is $2^{(e-2)k+1}$ for all $e \geq 3$.

ii. $(2^k - 1)2^{e-1}$ is $2^{(e-2)k+1}(2^{k-1} - 1)$ for all $e \geq 3$.

Therefore, from Corollary 2, 3 and 4, the number of $g(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x],\ a_k = 1,\ k > 2$ such that $g(x) \equiv f(x) \bmod 2$ and corresponding sequences have period maximum period is $2^{(e-2)k+1}(2^{k-1} - 1)$ for all $e \geq 3$.

Corollary 5

Let $f(x)$ be a primitive trinomial mod 2 of degree k, the number of different sequences of IRRs of period $(2^k - 1)2^{e-1}$, $e \geq 3$ corresponds to a unique $f(x)$ is $2^{(k-1)(2e-3)+(e-1)}(2^{k-1} - 1)$.

Proof: According to Proposition 2, each primitive trinomial mod 2 generate $2^{(k-1)(e-1)}$ different sequences of maximum possible period. The number of different polynomials which generate sequences of maximum possible period is $2^{(e-2)k+1}(2^{k-1} - 1)$. Therefore, the number of different sequences with maximum possible period which correspond to $f(x)$ is $2^{(k-1)(2e-3)+(e-1)}(2^{k-1} - 1)$.

Thus for a unique primitive trinomial modulo 2, there are huge number of different sequences of maximum possible period. Furthermore, for a primitive trinomial modulo 2, all of the forms can be determined explicitly using Theorem 1, 2, and 3.

4. OTHER THAN TRINOMIAL OF DEGREE *K*>2

In this section, we will enumerate the number of polynomials over $\mathbb{Z}_{2^e}$ corresponding to a primitive polynomial (other than trinomial) over mod 2 satisfying the Eqn. (2).

The structure of primitive polynomial f(x) mod 2 is unknown in terms of their weight; therefore assume the general polynomial as:

Let $f(x) = \sum_{i \in A} x^i$, where $A = \{l_0, l_1, l_2, ..., l_{s+1}\}$ and $k = l_0 > l_1 > ... > l_s > l_{s+1} = 0,\ s > 1$ be a primitive polynomial mod 2 of degree k, which satisfies the Eqn. (2) and let $g(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, where $a_k = 1$ be a polynomial of degree k. We assume this throughout the section.

Lemma 8

Let $g(x) \in \mathbb{Z}_{2^e}[x]$ and $f(x)$ be two polynomials as considered above, then $g(x) \equiv f(x) \bmod 2$ if and only if $\gcd(a_i, 2) = 1,\ i \in A$, otherwise $\gcd(a_i, 2) = 2$.

Lemma 9

Let $f(x)$ be a primitive polynomial mod 2 of degree k and $g(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, where $a_k = 1,\ k > 2$ such that $g(x) \equiv f(x) \bmod 2$. Then

$$g(x)^2 + g(-x)^2 - 2g(x^2) \equiv 0 \bmod 8 \qquad (8)$$

if and only if

i. $a_i = 4r + 3,\ r \geq 0$, for some $i \in A$ and

ii. $a_i = 4r + 1,\ r \geq 0$, for some $i \in A$ and

iii. $a_i = 4r,\ r \geq 0$, for some $i \notin A$ and

iv. $a_i = 2r,\ r$ odd, for other $i \notin A$.

Proof: Using Lemma 2,

$$g(x)^2 + g(-x)^2 - 2g(x^2) \equiv 0 \bmod 8$$

if and only if

$$2\sum_{i=0}^{k-1} a_i(a_i - 1)x^{2i} + 4\sum_{\substack{0 \leq i < j \leq k, \\ i+j=2m}} a_i a_j x^{i+j} \equiv 0 \bmod 8,\ 0 < m < k$$

if and only if coefficient of each power of x is zero mod 8. That is

$$2a_0(a_0 - 1) \equiv 0 \bmod 8 \ \textit{and}$$

$$2a_m(a_m - 1) + 4\sum_{\substack{0 \leq i < j \leq k, \\ i+j=2m}} a_i a_j \equiv 0 \bmod 8 \ \textit{for}\ 1 \leq m \leq k-1.$$

Since $a_i,\ i \in A$ is odd and $a_i,\ i \notin A$ is even, therefore

$$4\sum_{\substack{0 \leq i < j \leq k, \\ i+j=2m}} a_i a_j \bmod 8 \equiv \begin{cases} 4a_i a_j & \textit{for some } i, j \in A \\ 0, & \textit{otherwise} \end{cases}$$

Thus Eqn (8) holds if and only if

$$2a_m(a_m - 1) + 4a_i a_j \equiv 0 \bmod 8 \text{ for some } m \qquad (9)$$

and corresponding to some $i, j \in A$ and

$$2a_m(a_m - 1) \equiv 0 \bmod 8 \text{ for other } m's \qquad (10)$$

The Eqn (9) holds if and only if

$a_m = 2r,\ r$ odd for some even value of a_m and

$a_m = 4r + 3,\ r \geq 0$, for some odd value of a_m.

Also the Eqn (10) holds if and only if

$a_m = 4r,\ r \geq 0$, for some even value of a_m and

$a_m = 4r + 1,\ r \geq 0$, for some odd value of a_m.

Therefore, Eqn (8) holds if and only if

$a_m = 4r + 3,\ r \geq 0$, for some $m \in A$ and

$a_m = 4r + 1,\ r \geq 0$, for other $m \in A$ and

$a_m = 4r,\ r \geq 0$, for some $m \notin A$ and

$a_m = 2r,\ r$ odd, for other $m \notin A$.

Lemma 10

Let $f(x)$ be a primitive polynomial mod 2 of degree k and $g(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, where $a_k = 1,\ k > 2$ such that $g(x) \equiv f(x) \bmod 2$. Then

$$g(x)^2 + g(-x)^2 - 2(-1)^k g(-x^2) \equiv 0 \bmod 8 \qquad (11)$$

if and only if

i. $a_i = 4r + 3,\ r \geq 0$, for some $i \in A$ and

ii. $a_i = 4r + 1,\ r \geq 0$, for some $i \in A$ and

iii. $a_i = 4r,\ r \geq 0$, for some $i \notin A$ and

iv. $a_i = 2r,\ r$ odd, for other $i \notin A$.

The condition in following theorem is the combination of conditions in Theorem 1, 2 and 3.

Theorem 4

Let $f(x)$ be a primitive polynomial mod 2 of degree k and $g(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, where $a_k = 1,\ k > 2$ such that

$g(x) \equiv f(x) \bmod 2$. The period of the sequence corresponds to the recurrence relation (3) is less than $(2^k-1)2^{e-1}$ for all $e \geq 3$ if and only if

i. $a_i = 4r,\ r \geq 0,$ for some $i \notin A$ and

ii. $a_i = 2r,\ r$ odd, for some $i \notin A$ and

iii. $a_i = 4r+1,\ r \geq 0,$ for some $i \in A$ and

iv. $a_i = 4r+3,\ r \geq 0,$ for some $i \in A$ and

v. $a_i = 4r+3$ *or* $4r+1,\ r \geq 0,$ for some $i \in A$ and (if occurs for more than one a_i as in Theorem 1 because of dependency).

Corollary 6

Let $f(x)$ be a primitive polynomial mod 2 of degree k. The number of $g(x) = \sum_{i=0}^{k} a_i x^i \in \mathbb{Z}_{2^e}[x]$, where $a_k = 1,\ k > 2$ such that $g(x) \equiv f(x) \bmod 2$ and corresponding sequences have period

i. Less than $(2^k-1)2^{e-1}$ is $2^{(e-2)k+1}$ for all $e \geq 3$.

ii. $(2^k-1)2^{e-1}$ is $(2^{k-1}-1)2^{(e-2)k+1}$ for all $e \geq 3$.

Corollary 7

Let $f(x)$ be a primitive polynomial mod 2 of degree k, the number of different sequences of IRRs of period $(2^k-1)2^{e-1},\ e \geq 3$ corresponding to a unique $f(x)$ is $2^{(k-1)(2e-3)+(e-1)}(2^{k-1}-1)$.

Thus the number of different sequences is same as in Corollary 5.

5. TRINOMIAL OF DEGREE $k = 2$

In this section, we will enumerate $g(x) = x^2 + a_1x + a_0 \in \mathbb{Z}_{2^e}[x],\quad e \geq 3$ for maximum possible period $(2^2-1)2^{e-1}$ with a_1 and a_0 as an odd integers.

If $a_1 = 1$ and $a_0 = 1$, then the only primitive trinomial $f(x) = x^2 + x + 1$ modulo 2 does not satisfies the condition of maximum possible period as given in Proposition 1. Therefore, the condition given in Proposition 1 is for $k > 2$. Instead of this, a degree 2 trinomial can generate sequences of maximum possible period for other odd values of a_1 and a_0 and these values can be determined from the following theorem.

Theorem 5

Let $g(x) = x^2 + a_1x + a_0 \in \mathbb{Z}_{2^e}[x],\quad e \geq 3$ be a polynomial, then

$$g(x)^2 + g(-x)^2 - 2g(x^2) \neq 0 \bmod 8 \text{ and} \tag{12}$$

$$g(x)^2 + g(-x)^2 - 2(-1)^2 g(-x^2) \neq 0 \bmod 8 \tag{13}$$

if and only if $a_0 = 4r+3,\ r \geq 0$.

Proof: Using Lemma 2 and 3,

$$g(x)^2 + g(-x)^2 - 2g(x^2) = [2a_1(a_1-1) + 4a_0]x^2 + 2a_0(a_0-1)$$

and

$$g(x)^2 + g(-x)^2 - 2(-1)^2 g(-x^2) = [2a_1(a_1+1) + 4a_0]x^2 + 2a_0(a_0-1).$$

Since a_0 and a_1 are odd, then $2a_1(a_1-1) + 4a_0 \equiv 0 \bmod 8$ for $a_1 \geq 3$ always. Thus Eqns (12) and (13) depends only on a_0.

Therefore Eqns. (12) and (13) holds if and only if $2a_0(a_0-1) \neq 0 \bmod 8$.

Since a_0 is odd, then $2a_0(a_0-1) \neq 0 \bmod 8$ if and only if $a_0 \neq 4r+1,\ r \geq 0$.

Thus Eqns. (12) and (13) holds if and only if $a_0 = 4r+3,\ r \geq 0.$

Corollary 8

For odd a_0 and a_1, the number of different $g(x) = x^2 + a_1x + a_0 \in \mathbb{Z}_{2^e}[x],\ e \geq 3$ which generate sequences of maximum period is 2^{2e-3}.

Proof: Since a_1 is an odd integer, therefore a_1 has 2^{e-1} choices. Also a_0 is odd and has the form $4r+3,\ r \geq 0,$ therefore a_0 has 2^{e-2} choices. Thus number of different polynomials which generate sequences of maximum period is 2^{2e-3}.

Corollary 9

The number of different sequences corresponding to 2-degree IRR of maximum possible period for $e \geq 3$ is 2^{3e-4}.

Proof: Since each polynomial generates $2^{(e-1)(k-1)}$ different sequences (using Proposition 2), therefore the number of different sequences of period $3 * 2^{e-1}$ is 2^{3e-4}.

If $k = 2$, then the number of different sequences in Corollary 5 is equal to the number of different sequences in Corollary 9.

For each case, the number of different polynomials of maximum period is $2^{(k-1)(2e-3)+(e-1)}(2^{k-1}-1)$ for $e \geq 3$ and the number of different polynomials of period less than maximum is $2^{(e-2)k+1}$ for all $e \geq 3$.

If $e = 1$, then the number of different polynomials of maximum period is $\frac{\Phi(2^k-1)}{k}$, since primitive polynomial mod 2 has maximum period.

If $e = 2$, then polynomial $f(x)$ given in Proposition (1a) needs to satisfy only the second part of the Eqn. (2) for maximum period as given in references[4,9]. Therefore Lemma 5 holds only for one choice of $g(x)$, out of total 2^k choices of $g(x)$ in $\mathbb{Z}_{2^2}[x]$. Thus the number of different polynomials giving maximum period in $\mathbb{Z}_{2^2}[x]$ is 2^k-1. Similarly for other cases, we get the same result.

Remark: The number of primitive polynomials of degree k in modulo 2 satisfying the condition of Proposition 1 is $\frac{\Phi(2^k-1)}{k}2^{(e-2)+1}(2^{k-1}-1)$ for $e \geq 3$. For general p, we refer the readers to the article[10] and the references cited there. The way of counting (as explained in previous part of this paper) the number of desired polynomials also describes an explicit method for the construction of polynomials for maximum period.

6. CONCLUSION

Integer recurrence relations are being used in cryptographic applications as pseudo random number sequence generators. For a given primitive polynomial modulo 2 satisfying the condition of maximum period given by Brent, there exist many different polynomials in the ring $\mathbb{Z}_{2^e}[x]$ with same period and this number is huge. It will be difficult for a cryptanalyst to find out the exact one used in the designed system. We have counted the number of such polynomials and also given an explicit method for construction of such polynomials.

REFERENCES

1. Golomb, S.W. Shift register sequences. Holden-Day, San Francisco, 1967.
2. Lidl, R. & Niederreiter, H. Finite fields and their applications. Cambridge University Press, 2000.
3. Massey, J.L. Shift-register synthesis and BCH decoding, *IEEE Trans. Info. Theory, IT*-15, 1969, 122-127. doi: 10.1109/TIT.1969.1054260
4. Brent, R.P. On the periods of generalised fibonacci recurrences. *Math. Comput.*, 1994, **63**, 389-401. doi: 10.1090/S0025-5718-1994-1216256-7
5. Ward, D. The Arithmetical theory of linear recurring series. *Trans Amer. Math. Soc.,* 1933*,* **35**, 600-628. doi: 10.1090/S0002-9947-1933-1501705-4
6. Dai, Z.D. Binary sequences derived from ML-sequences over rings I: Period and minimal polynomials. *J. Cryptology,* 1992, **5**, 193-207. doi: 10.1007/BF02451115
7. Reeds, J.A. & Sloane, N.J.A. Shift-Register Synthesis (Modulo m). *SIAM J. Comput*., 1985, **14**, 505-513. doi: 10.1137/0214038
8. Mascagni M.; Cuccaro S, Pryor D. and Robinson M. A fast, high quality, reproducible, parallel, lagged-Fibonacci pseudorandom number generator. Supercomputing Research Center, 17100 Science Drive, Bowie, MD 20715, 1994. Report No. SRC-TR-94-115.
9. Knuth, D.E. The art of computer programming, semi-numerical algorithms. Edition 3rd. Low Price Edition, Pearson Education, Inc., Boston, USA, 2007.
10. Goltvanitsa, M.A.; Zaitsev, S.N. & Nechaev, A.A. Skew linear recurring sequences of maximal period over Galois rings. *J. Math. Sci.*, 2012, **2**(187), 115-128. doi: 10.1007/s10958-012-1054-2

CONTRIBUTORS

Mr Yogesh Kumar is a research scholar in the department of mathematics, IIT Delhi, India. He received a MSc in mathematics from Kurukshetra University. His research interests include algebra, finite fields and cryptography.

Dr N.R. Pillai is a senior scientist in Scientific Analysis Group, DRDO, Delhi, India. He did his PhD in computer science from IISc, Bangalore, India. His main research interests are cryptography, coding theory and modules of computations.

Dr R.K. Sharma is a professor in the department of mathematics, IIT Delhi, India. He received his PhD in mathematics from IIT Delhi. His main research interests are algebra and cryptography.