Some Unexplored State Sequences of Linear Feedback Shift Registers

Sivasankar M.∗ and Prema G.

Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Coimbatore, India.
e-mail: 1m−sivasankar@cb.amrita.edu

Abstract. With the limitation of having only \(\phi(2^n - 1)\) primitive polynomials of degree \(n\) over \(F_2\), any primitive Linear Feedback Shift Register with \(n\) stages can visit the \((2^n - 1)\) non-zero \(n\)-bit states in \(\phi(2^n - 1)\) ways only. In fact it is obvious that there are \((2^n - 1)!\) possible ways of visiting these \((2^n - 1)\) \(n\)-bit strings. In this paper, we attempt to visit all or part of these \((2^n - 1)\) \(n\)-bit strings in some other order using irreducible non-primitive polynomials. The security of the key bit streams hence generated is also analysed.

Keywords: boolean functions, irreducible polynomials, linear feedback shift registers, primitive polynomials, stream ciphers.

1. Introduction

Linear Feedback Shift Registers (shortly LFSRs) play an important role in symmetric key cryptography as they can efficiently generate bit streams for encryption purpose. The demand for new LFSR designs is increasing due to the relative easiness involved in implementing them, both in software and hardware. In general, LFSRs are controlled by primitive polynomials in order to produce maximum period bit sequences. In this paper, we discuss ways of generating bit streams using irreducible non-primitive polynomials.

2. Linear Feedback Shift Registers

We require some basic facts about LFSRs and we refer [1] for the same.

Definition 1. An LFSR of length \(L\) consists of \(L\) stages \(0, 1, \ldots, L - 1\), each capable of storing one bit and having one input and one output; and a clock which controls the movement of data. During each unit of time the following operations are performed: (i) the content of stage 0 is output and forms part of the output sequence; (ii) the content of stage \(i\) is moved to stage \(i - 1\) for each \(i, 1 \leq i \leq L - 1\); (iii) the new content of stage \(L - 1\) is the feedback bit \(s\) which is calculated by adding together modulo 2 the previous contents of a fixed subset of stages \(0, 1, \ldots, L - 1\).

∗Corresponding author

© Elsevier Publications 2013.
Some Unexplored State Sequences of Linear Feedback Shift Registers

Figure 1. An LFSR with $L$ stages.

Starting with an initially loaded state $[s_{L-1}, \ldots, s_1, s_0]$ – called the seed – and with a connection polynomial $C(D) = 1 + c_1 D + c_2 D^2 + \cdots + c_L D^L \in \mathbb{Z}_2(D)$ the LFSR in Figure 1, denoted by $(L, C(D))$, has the feedback $s_j = (c_1 s_{j-1} + c_2 s_{j-2} + \cdots + c_L s_{j-L}) \mod 2$ for $j \geq L$. The generated bit sequence $s_0, s_1, s_2, \ldots$ has a period $p$, if $s_i = s_{i+p}$ for all $i \geq 0$. For encryption purpose, high periodic streams are preferred as the encryption process is XORing the generated bit stream with the flowing bits of the plain text, that is, the message.

3. The Ring of Polynomials Over $\mathbb{F}_2$

We refer [2] for some fundamental concepts. The set of all polynomials $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, of any degree $n \geq 0$ such that $a_i \in \{0, 1\}$, constitutes the polynomial ring $\mathbb{F}_2[x]$, under the usual polynomial addition and multiplication, where the coefficients are added / multiplied in $\mathbb{F}_2$.

Definition 2. Let $f(x) \in \mathbb{F}_2[x]$ be a non zero polynomial. If $f(0) \neq 0$ then the least positive integer $e$ for which $f(x)$ divides $x^e - 1$ is called the order of $f$ denoted by $\text{ord}(f)$. If $f(0) = 0$ then $f(x) = x^h g(x)$ where $g \in \mathbb{F}_2[X]$ with $g(0) \neq 0$. Then $\text{ord}(f) = \text{ord}(g)$.

3.1 Irreducible polynomials

A polynomial $p(x) \in \mathbb{F}_2[x]$ is said to be irreducible or prime in $\mathbb{F}_2[x]$, if $p(x)$ has positive degree and $p(x) = b(x)c(x)$ with $b(x), c(x) \in \mathbb{F}_2[x]$ implies that either $b(x)$ or $c(x)$ is a constant polynomial. It is observed that, if a degree $n$ polynomial $f(x)$ is irreducible over $\mathbb{F}_2$ then $\text{ord}(f)$ divides $2^n - 1$. The number of monic irreducible polynomials in $\mathbb{F}_2[x]$ of degree $n$ is given by, $N_2(n) = \frac{1}{2} \sum_{d|n} \mu(d) 2^{\frac{n}{d}}$, where $d$ is a divisor of $n$ and $\mu(d)$ is the Mobius function.

Irreducible polynomials of a particular degree can be constructed efficiently using lower degree irreducible polynomials. The web application available at [3], generates the list of irreducible polynomials of a given degree.

3.2 Primitive polynomials

An interesting subclass of irreducible polynomials is the class of primitive polynomials. A degree $n$ irreducible polynomial $f(x)$, is called primitive if the order of $f(x)$ equals $2^n - 1$. The number of monic primitive polynomials in $\mathbb{F}_2[x]$ of degree $n$ is given by, $\phi(2^n - 1)$, where $\phi$ is the Euler’s totient function. Table 1, gives the number of irreducible and primitive polynomials of given degree $3 \leq n \leq 10$. 

![Diagram of Linear Feedback Shift Register](image-url)
Table 1. Number of irreducible, primitive polynomials of degree $n$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Irreducible</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>18</td>
<td>30</td>
<td>56</td>
<td>99</td>
</tr>
<tr>
<td>Primitive</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>6</td>
<td>18</td>
<td>16</td>
<td>48</td>
<td>60</td>
</tr>
</tbody>
</table>

Figure 2. The Hamilton cycle visited by the LFSR $\langle 3, 1 + D + D^3 \rangle$.

The same application available at [3], picks out the primitive polynomials from the list of irreducible polynomials, for a given degree $n$.

4. Motivation for the Present Work

Considering the possible state space of any $n$-stage LFSR (which is nothing but, the collection of all $2^n - 1$ non zero binary strings of length $n$), we note that only primitive LFSRs – LFSRs whose connection polynomial is a primitive polynomial of degree $n$-visit all these states. The randomness they apply in visiting these states, keep them in a respected position in the design of stream ciphers.

In graph theory point of view, the state sequence of a primitive LFSR (i.e. the order of visiting these $2^n - 1$ binary strings) is actually a Hamilton cycle of the complete graph $K_{2^n - 1}$, whose vertices are the $2^n - 1$ non-zero bit strings of length $n$. The lsb of each state being visited, is considered to produce the key stream. It is obvious that there are $\left(\frac{(2^n - 2)!}{2}\right)$ Hamilton cycles in $K_{2^n - 1}$. Only some of these Hamilton cycles and hence the key stream generated through them are useful to cryptography.

With $n = 3$ the graph $K_{2^3 - 1} = K_7$ is given in Figure 2, and the Hamilton cycle traced by the LFSR with the connection polynomial $1 + D + D^3$ and with the seed (101) is {101, 010, 001, 100, 110, 111, 011, 101}, which is shown in bold directed edges in the figure. The LFSR will continue tracing this Hamilton cycle again and again, producing the bit sequence, ...11001011100101 whose period is 7.

Since we have only $\frac{d(2^n - 1)}{n}$ number of primitive polynomials (which is very less, compared to the number of Hamilton cycles, $\frac{(2^n - 2)!}{2}$, available in $K_{2^n - 1}$), most of the other useful Hamilton
cycles are still unexplored. The proposed algorithm tries to generate some of these unexplored state sequences by using irreducible non-primitive polynomials.

5. Proposed Bitstream Generator

It is known that the period of the binary stream generated by an $n$-bit LFSR, is a divisor of $2^n - 1$. If a primitive connection polynomial is used in the LFSR, then an $m$-sequence is generated. If an irreducible non-primitive connection polynomial is used, the period of the stream generated is a proper divisor of $2^n - 1$. For example a 6-stage LFSR with an irreducible non-primitive connection will either cycle through 21 states or through 9 states. This is so, as $2^6 - 1 = 63 = 3^2 \times 7$. So the 63 non-zero states are either divided into three 21 state cycles or seven 9 state cycles [2].

After a keen analysis of the factorisation of $2^n - 1$ for various values of $n \geq 3$ we select an $n$ with less prime factors. This actually enhances the chance of divisors being large numbers and hence the chance of large period streams being generated. Few such values of $n$ and the factorisation of $2^n - 1$ are: $n = 23, 2^{23} - 1 = 47 \times 178481; n = 26, 2^{26} - 1 = 3 \times 2731 \times 8191; n = 27, 2^{27} - 1 = 7 \times 73 \times 262657$ and $n = 34, 2^{34} - 1 = 3 \times 43691 \times 131071$. For algorithms for factorising $2^n - 1$, [4] can be referred.

The project, The Great Internet Mersenne Prime Search (GIMPS) [5], searches for Mersenne Primes; but as a byproduct it gives the factorisation of Mersenne composite numbers and helps us to select a suitable $n$ as the degree of the irreducible non-primitive connection polynomial.

5.1 The algorithm

**Step 1.** Select a Mersenne composite Number, $2^n - 1$ with less number of prime factors.

**Step 2.** Select an irreducible non-primitive polynomial of degree $n$.

**Step 3.** Use the polynomial selected in Step 2 as the connection polynomial to generate the bit stream.

We notice that with a non primitive irreducible connection polynomial, the randomness of the LFSR in visiting the states is less, when compared with a primitive polynomial connection. This slight drawback can be rectified by using $m$ LFSRs ($m \geq 2$) with different irreducible non-primitive polynomials and mixing the $m$ parallel output bits using a cryptographically secure Boolean function. The theory of designing immune Boolean functions is well studied and improved designs are also being developed periodically [6].

5.2 The improved algorithm

**Step 1.** Select a Mersenne composite Number, $2^n - 1$, with less number of prime factors.

**Step 2.** Select $m \geq 2$ number of $n$-stage LFSRs and select an equal number irreducible non-primitive polynomials of degree $n$.

**Step 3.** Select a cryptographically secure Boolean function $f(x_1, x_2, \ldots, x_m)$.

**Step 4.** Use the Boolean value $f(b_1, b_2, \ldots, b_m)$, where $b_i$ is the bit output of the $i^{th}$ LFSR, $1 \leq i \leq m$, as the next key bit.
6. Security Analysis of the Generated Key Stream

For analysis purpose we have generated three bitstreams, using three 9-stage LFSRs having the irreducible non-primitive connection polynomials, $1 + x^5 + x^7 + x^8 + x^9$, $1 + x^3 + x^4 + x^7 + x^9$ and $1 + x + x^2 + x^4 + x^9$, with seeds $(100101111)$, $(111111111)$ and $(111111111)$ respectively.

As $2^9 - 1 = 511 = 7 \times 73$, first 73 bits of each stream (expecting a state cycle of length 73) is separately analysed for balancedness and number of runs. Later these three streams are mixed using the Boolean function $1 \oplus x_1 \oplus x_2 x_3$, and the resulting stream is also analysed for the above stated properties. The results are shown in Figure 3 (values of the bits are plotted against their position in the stream) and it is observed that the sequences posses expected randomness properties.

7. Concluding Remarks

Deviating away from the conventional way of bit stream generation, a new way of generation using irreducible non-primitive polynomials is discussed. By analysing more about the dominant factors of $2^n - 1$ and the equivalence class of irreducible polynomials generating the same states, more insight in this direction is expected in near future.

References