Primitive Polynomials, Linear Feedback Shift Registers

Priyank Kalla

Professor
Electrical and Computer Engineering, University of Utah
kalla@ece.utah.edu
http://www.ece.utah.edu/~kalla

February 5, 2024

Irreducible versus Primitive Polynomials in $\mathbb{F}_{2^k}$

- An irreducible polynomial $P(x) \in \mathbb{F}_2[x]$ is one that cannot be factored into expressions of lower degree. Irreducible polynomial is not divisible by any polynomial other than 1 or itself.
- An irreducible polynomial $P(x) \in \mathbb{F}_2[x]$ is a primitive polynomial if the smallest positive integer n that allows $P(x)$ to divide $x^n + 1$ is $n = 2^k - 1$.
- Recall, $k =$ degree of $P(x)$ and is used to construct $\mathbb{F}_{2^k}$
  - Let $k = 3$, then $n = 2^3 - 1 = 7$.
  - $P(x) = x^3 + x + 1$ is a primitive polynomial because the smallest n for which $P(x) \mid x^n + 1$ is $n = 7$.
  - In other words, $P(x) \mid x^7 + 1$, but $P(x) \nmid x^6 + 1, x^5 + 1, \ldots x + 1$.
  - For $k = 4$, $P_1(x) = x^4 + x^3 + x^2 + x + 1 \mid x^5 + 1$, so $P_1(x)$ is not a primitive polynomial.

Irreducible and Primitive Poly

- Note: Any irreducible poly $P(x) \in \mathbb{F}_2[x]$ of degree k always divides $x^n + 1, n = 2^k - 1$.
- But, an irreducible $P(x)$ may also divide $x^n + 1, n < 2^k - 1$
  - Example: $P_1(x) = x^4 + x^3 + x^2 + x + 1 \mid x^{15} + 1$, but $P_1(x) \mid x^5 + 1$ too. So P_1 is not primitive.
  - $P_2(x) = x^4 + x^3 + 1 \mid x^{15} + 1$, but $P_2(x) \nmid x^n + 1$ for any $n < 15$, so it is primitive.
- A root α of a primitive polynomial is called a primitive root: $P(\alpha) = 0$.
- A primitive root α generates all the non-zero elements of $\mathbb{F}_{2^k} = \{0, 1 = \alpha^{2^k-1}, \alpha, \alpha^2, \ldots, \alpha^{2^k-2}\}$.
- That is, α is a generator of the cyclic group $\mathbb{F}_{2^k}^* = \mathbb{F}_{2^k} - \{0\}$.

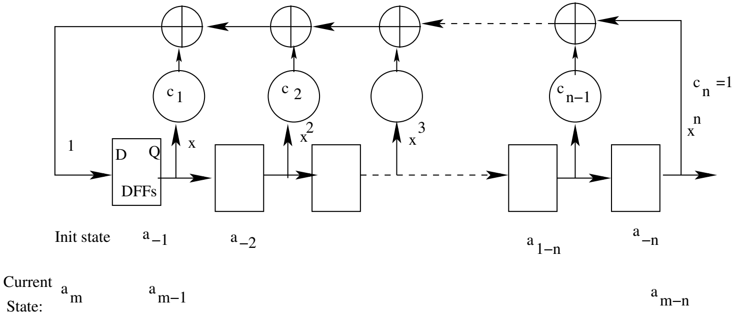
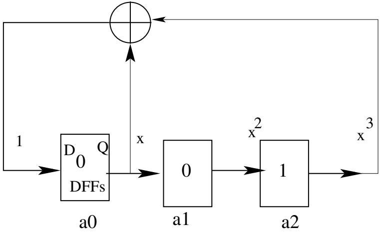


Figure: Type-I LFSR

- Type-I LFSR defined by characteristic polynomial $P(x)$
- $P(x) = 1 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1} + c_nx^n,\ c_i \in \{0, 1\}, c_n = 1,$ gives 1-to-1 mapping between polynomial and LFSR.

Type-I LFSR Example



a0a1a2
001
100
110
111
011
101
010
001
100

Figure: Type-I LFSR

- $P(x) = x^3 + x + 1$, put initial state $a_{-n} = 1$, and all else $a_i = 0$

Type-II LFSR

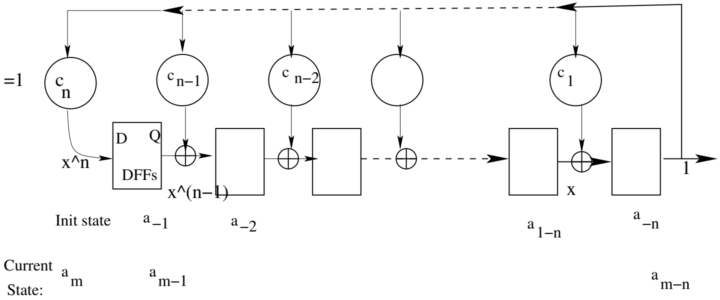


Figure: Type-II LFSR

- Type-II design

Type-II LFSR Example

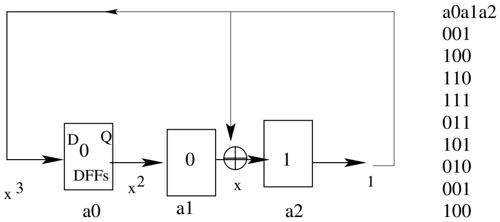


Figure: Type-II LFSR

- $P(x) = x^3 + x + 1$

LFSR Concepts

- $P^*(x) = x^n P(1/x) = x^n + c_1 x^{n-1} + c_2 x^{n-2} + \cdots + c_{n-1}x + 1$ is called the reciprocal polynomial of the LFSR.
- Two polynomials associated with the LFSR: $P(x), P^*(x)$
- LFSR Period: If the initial state of LFSR is $a_{-1} = \cdots = a_{1-n} = 0, a_{-n} = 1$, then LFSR sequence is periodic with a period that is the smallest integer n for which $P(x) \mid (1 - x^n)$.
- When period is $2^k - 1 =$ maximal length sequence, and $P(x) =$ primitive polynomial! [*Remember:* k is the bit-vector word-length of operands in $\mathbb{F}_{2^k}$].
- To generate pseudorandom numbers (k-bit vectors), design an LFSR with the characteristic polynomial $P(x) =$ a primitive polynomial of degree k.

Example of Pseudorandom (Key) Generation

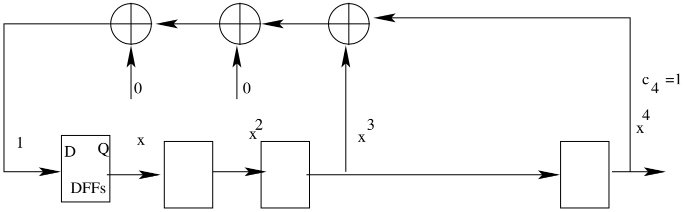


Figure: Type-I LFSR: $P(x) = x^4 + x^3 + 1$

Sequence: $\alpha^3 \rightarrow 1 \rightarrow \alpha \rightarrow \alpha^2 \rightarrow \alpha^4 \ldots \alpha^{14} \rightarrow \ldots$: produces all non-zero entries (15 vectors) and repeats

LFSR Encipherment: Stream Cipher

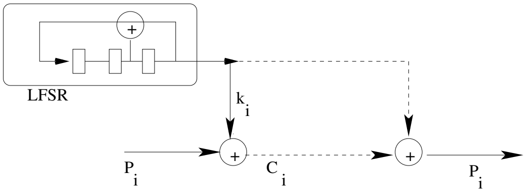


Figure: Encipherment with LFSR

Note: XORs are invertible

$$C_i = P_i \oplus k_i$$
$$P_i = C_i \oplus k_i$$
$$k_i = P_i \oplus C_i$$

Exponentiation in Finite Fields

Lemma

Let $\alpha_1, \ldots, \alpha_t$ *be elements in any finite field* $\mathbb{F}_{p^k}$ *for any prime* p*. Then,* $(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{p^i} = \alpha_1^{p^i} + \alpha_2^{p^i} + \cdots + \alpha_t^{p^i}$*, for all integers* $i \geq 0$*.*

Corollary

Let $\alpha_1, \ldots, \alpha_t$ *be elements in any finite field* $\mathbb{F}_{2^k}$*. Then,* $(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^2 = \alpha_1^2 + \alpha_2^2 + \cdots + \alpha_t^2$*, for all integers* $i \geq 0$*.*

Many Linear Functions over finite fields have natural invertibility. Here's an example: Consider $\mathbb{F}_{2^3}$ with $P(x) = x^3 + x + 1, P(\alpha) = 0$:

$$\begin{aligned}
A &= a_0 + a_1\alpha + a_2\alpha^2 \\
A^2 &= a_0^2 + a_1^2\alpha^2 + a_2^2\alpha^4 \quad (\text{as } (a+b)^2 = a^2 + b^2) \\
A^2 &= a_0 + a_1\alpha^2 + a_2\alpha^4 \quad (\text{as } a_i \in \{0, 1\}) \\
A^4 &= a_0 + a_1\alpha^4 + a_2\alpha^8 \quad (\text{as } a_i \in \{0, 1\})
\end{aligned}$$

$$\begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \\ 1 & \alpha^4 & \alpha^8 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} A \\ A^2 \\ A^4 \end{bmatrix}$$

$$C \cdot a = A$$

Treat C as a matrix of constants, A as a vector of constants, and a as the vector or indeterminates. Then C is a $k \times k$ square matrix, with a special structure!

Vandermonde Matrices and their Determinants

Definition (Vandermonde Matrix)

A Vandermonde matrix $V(x_1, \ldots, x_m) = \begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \ldots & x_3^{n-1} \\ \vdots & \vdots & \ldots & \vdots & \\ 1 & x_m & x_m^2 & \ldots & x_m^{n-1} \end{bmatrix}$ is a matrix where terms in every row form a geometric progression.

Vandermonde Matrices and their Determinants

Definition (Square Vandermonde Matrix & Determinants)

Let $\mathbf{V}(x_1, \ldots, x_n)$ *denote a square* $n \times n$ *matrix of the form*

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & . & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{bmatrix} \tag{1}$$

Then $\mathbf{V}(x_1, \ldots, x_n)$ *is a* **square Vandermonde Matrix**, *the determinant of which can be computed as:*

$$|\mathbf{V}(x_1, \ldots, x_n)| = \prod_{1 \leq i < j \leq n} (x_j - x_i) \tag{2}$$

This determinant is non-zero if each $x_i \in \{x_1, \ldots, x_n\}$ *is a distinct element.*

Back to our example ...

Consider $\mathbb{F}_{2^3}$ with $P(x) = x^3 + x + 1, P(\alpha) = 0$:

$$\begin{bmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \\ 1 & \alpha^4 & \alpha^8 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} A \\ A^2 \\ A^4 \end{bmatrix}$$

$$C \cdot a = A$$

Note: $C=$ Vandermond Matrix $V(\alpha, \alpha^2, \alpha^4)$: Prove that $|C| = 1$.

$$\begin{aligned} |\mathbf{C}| &= (\alpha^4 - \alpha^2) \cdot (\alpha^4 - \alpha) \cdot (\alpha^2 - \alpha) \\ &= (\alpha^4 + \alpha^2) \cdot (\alpha^4 + \alpha) \cdot (\alpha^2 + \alpha) \\ &= 1 \pmod{\alpha^3 + \alpha + 1} \end{aligned} \tag{3}$$

In other words, $|C| \neq 0$, C is invertible, and moreover, $|C| = 1$. So, you can find $a_i = F_i(A)$ in $\mathbb{F}_{2^3}$.