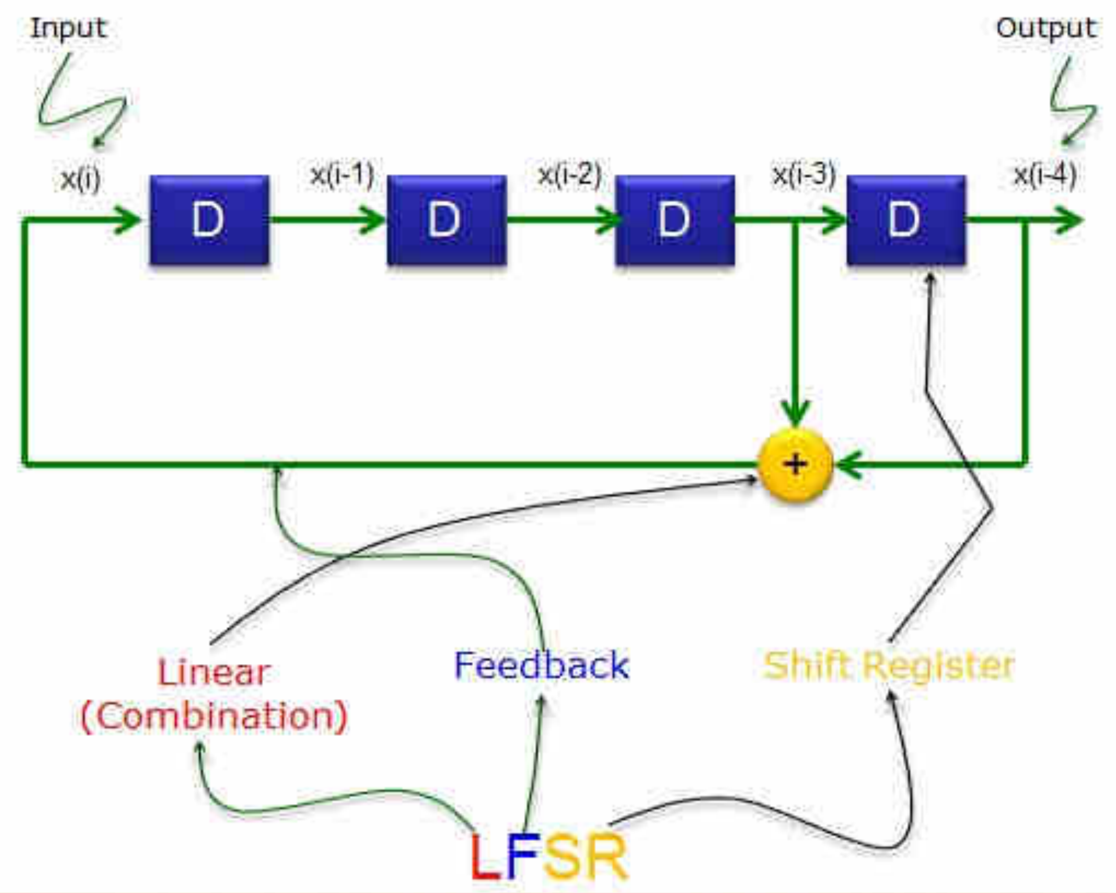
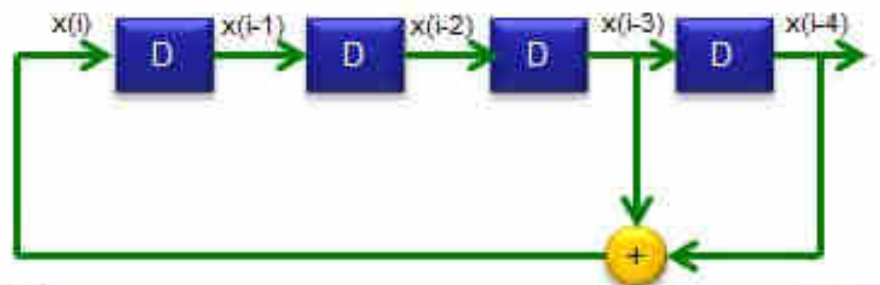
LFSR AND PRIMITIVE POLYNOMIAL

Li Yao

LFSR is a shift register circuit in which two or more outputs from intermediate steps get linearly combined and feedback to inout value.



An example of 4-bit LFSR



Initial State

State	X(i-1)	X(i-2)	X(i-3)	X(i-4)	X(i)
0	1	1	1	1	0
1	0	1	1	1	0
2	0	0	1	1	0
3	0	0	0	1	1
4	1	0	0	0	0
5	0	1	0	0	0
6	0	0	1	0	1
7	1	0	0	1	1
8	1	1	0	0	0
9	0	1	1	0	1
10	1	0	1	1	0
11	0	1	0	1	1
12	1	0	1	0	1
13	1	1	0	1	1
14	1	1	1	0	1
15	1	1	1	1	0

Same State As Initial State

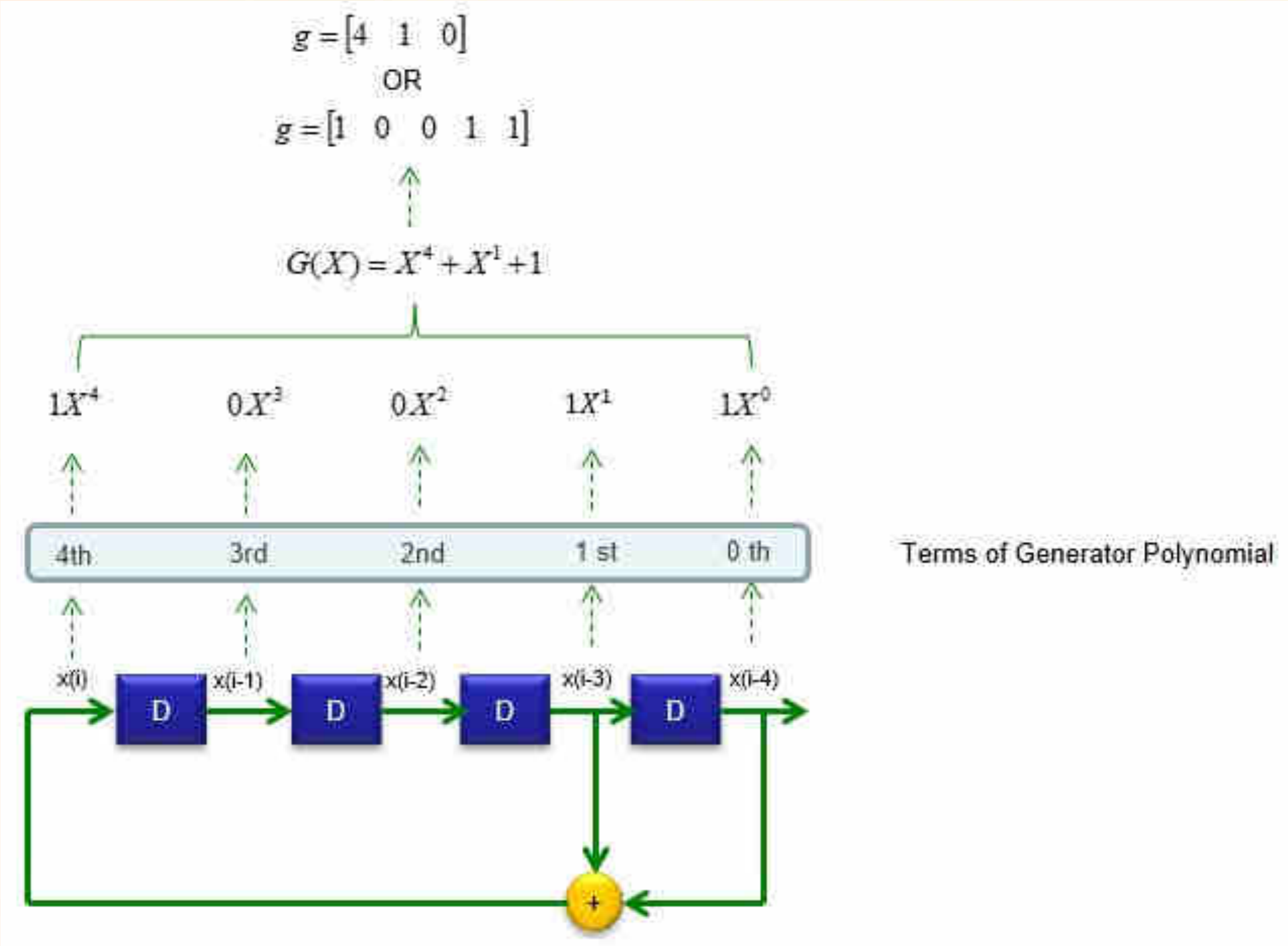
Deterministic

Pseudorandom

$2^n - 1$ states

m-sequence :
MaxiMum length
sequence

How to denote a LFSR



Generally, any n-bit LFSR can be denoted by a generator polynomial of degree n.

$$G(X) = X^4 + X + 1$$

…	1	0	1	0	1	1	0	0	1	0	0	0	1	1	1	1
…	X^{15}	X^{14}	X^{13}	X^{12}	X^{11}	X^{10}	X^9	X^8	X^7	X^6	X^5	X^4	X^3	X^2	X^1	X^0

$$X^{15} + X^{12} + X^{11} = 0 \qquad X^{11}G(X) = 0$$
$$X^{14} + X^{11} + X^{10} = 0 \qquad X^{10}G(X) = 0$$
$$X^{13} + X^{10} + X^{9} = 0 \qquad X^{9}G(X) = 0$$
$$X^{12} + X^{9} + X^{8} = 0 \qquad X^{8}G(X) = 0$$
$$X^{11} + X^{8} + X^{7} = 0 \qquad X^{7}G(X) = 0$$
$$X^{10} + X^{7} + X^{6} = 0 \qquad X^{6}G(X) = 0$$
$$X^{9} + X^{6} + X^{5} = 0 \qquad X^{5}G(X) = 0$$
$$X^{8} + X^{5} + X^{4} = 0 \qquad X^{4}G(X) = 0$$
$$X^{7} + X^{4} + X^{3} = 0 \qquad X^{3}G(X) = 0$$
$$X^{6} + X^{3} + X^{2} = 0 \qquad X^{2}G(X) = 0$$
$$X^{5} + X^{2} + X = 0 \qquad XG(X) = 0$$
$$X^{4} + X + 1 = 0 \qquad G(X) = 0$$

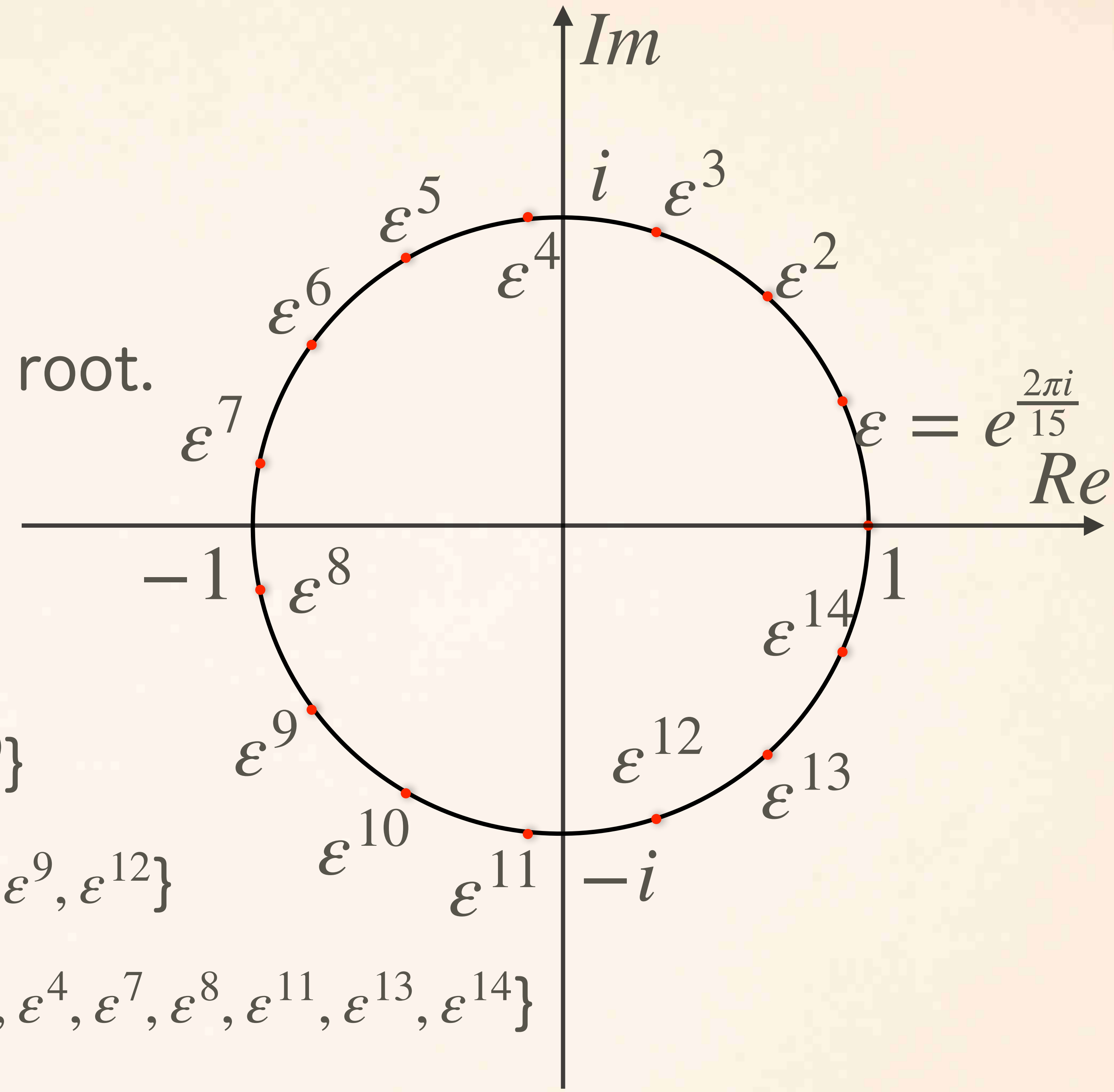
$$\Rightarrow \quad X^{15} = 1$$

$$G(X) \mid (X^{15} - 1) \quad \mathit{in} \quad \mathbb{F}_2[x]$$

$$\mathbb{F}_2[x] : \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_0, a_1, a_2, \ldots a_n \in \mathbb{F}_2\}$$

Generally, the generator polynomial of any n-bit LFSR which achieves m-sequence is a factor of $X^{2^n-1} - 1$ in $\mathbb{F}_2[x]$.

Factor $2^{2^n-1}-1$ in $\mathbb{Z}[x]$



If $\zeta^d = 1$ and $\zeta^k \neq 1 (0 < k < d)$,

ζ is called a dth primitive unit root.

1st primitive unit root:$\{1\}$

3rd primitive unit root:$\{\varepsilon^5, \varepsilon^{10}\}$

5th primitive unit root:$\{\varepsilon^3, \varepsilon^6, \varepsilon^9, \varepsilon^{12}\}$

15th primitive unit root:$\{\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^7, \varepsilon^8, \varepsilon^{11}, \varepsilon^{13}, \varepsilon^{14}\}$

nth primitive unit root:$\{e^{2\pi i \frac{k}{n}} \mid 0 < k \leqslant n, gcd(k, n) = 1\}$

$$\sum_{d|n} \varphi(d) = n$$

Cyclotomic Polynomial

$\Phi_n(x) = \prod_{1 \leqslant k \leqslant n, gcd(k,n)=1} (x - e^{2\pi i \frac{k}{n}})$, $e^{2\pi i \frac{k}{n}}$ is a nth primitive unit root.

$\Phi_n(x)$ is called a nth Cyclotomic Polynomial.

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

$$x^n - 1 = f(x)\Phi_n(x) = f(x)g(x) + r(x)$$
$$f(x)(\Phi_n(x) - g(x)) = r(x)$$

$$X^{15} - 1 = (x-1)(x-\varepsilon^5)(x-\varepsilon^{10})(x-\varepsilon^3)(x-\varepsilon^6)(x-\varepsilon^9)(x-\varepsilon^{12})$$
$$(x-\varepsilon)(x-\varepsilon^2)(x-\varepsilon^4)(x-\varepsilon^7)(x-\varepsilon^8)(x-\varepsilon^{11})(x-\varepsilon^{13})(x-\varepsilon^{14})$$

$$\Phi_1(x) = x - 1$$

$$\Phi_3(x) = \frac{x^3 - 1}{\Phi_1(x)} = x^2 + x + 1$$

$$\Phi_5(x) = \frac{x^5 - 1}{\Phi_1(x)} = x^4 + x^3 + x^2 + x + 1$$

$$\Phi_{15}(x) = \frac{x^{15} - 1}{\Phi_1(x)\Phi_3(x)\Phi_5(x)} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

Factor $\Phi_{2^n-1}(x)$ in $\mathbb{F}_2[x]$

A field $(\mathbb{F}, +, *)$ is a set $\mathbb{F}$ together with two binary operations on $\mathbb{F}$ called addition(+) and multiplication(*).A binary operation is a mapping $\mathbb{F} \times \mathbb{F} \to \mathbb{F}$.These operations are required to satisfy the following properties.

- $(\mathbb{F}, +)$ is an Abel group.
- $(\mathbb{F} \backslash \{0\}, *)$ is an Abel group.
- Distributivity of * over +.

Finite fields(also called Galois fields) are fields with finitely many elements. The field with p^n elements(p being prime) is usually denoted by $\mathbb{F}_{p^n}$. In $\mathbb{F}_{p^n}$, $\underbrace{1 + 1 + 1 + \cdots + 1}_{p} = 0$. p is called characteristic.

A subfield of a field $\mathbb{L}$ is a subset $\mathbb{K}$ of $\mathbb{L}$ that is a field with respect to the field operations inherited from $\mathbb{L}$.

If $\mathbb{K}$ is a subfield of $\mathbb{L}$, then $\mathbb{L}$ is an extension field of $\mathbb{K}$,and this pair of fields is a field extension. Such a field extension is denoted $\mathbb{L}/\mathbb{K}$.

Given a field extension $\mathbb{L}/\mathbb{K}$, the larger field $\mathbb{L}$ is a $\mathbb{K}$-vector space. The dimension of this vector space is called the degree of the extension and is denoted by $[\mathbb{L}:\mathbb{K}]$.

Let $\mathbb{L}/\mathbb{K}$ be a field extension, $\alpha \in \mathbb{L}$. Then the minimum polynomial of α is defined as the monic polynomial of least degree among all polynomials in $\mathbb{K}[x]$ having α as a root.

Some examples about field extension

1. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ $\quad f(x) = x^2 - 2 \quad [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

2. $\mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}$ $\quad f(x) = x^2 + 1 \quad [\mathbb{C} : \mathbb{R}] = 2$

3. $$\begin{aligned}\mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \mathbb{Q}(\sqrt{2})(\sqrt{3}) \\ &= \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}(\sqrt{2})\} \\ &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}\end{aligned}$$

   $f_1(x) = x^2 - 3 \quad [\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$

   $f_2(x) = x^2 - 2 \quad [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \quad [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$

4. $\mathbb{F}_p(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbb{F}_p\}$

   $f(x) = x^n + \cdots \quad [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$

Lemma 1. For any field $\mathbb{F}$ of characteristic p and any $f(x) \in \mathbb{F}[x]$, $f^p(x) = f(x^p)$ if and only if $f(x) \in \mathbb{F}_p[x]$; i.e., if and only if all coefficients f_i are in the prime subfield $\mathbb{F}_p \subseteq \mathbb{F}$.

Proof.

$$f(x) = f_0 + f_1 x^+ f_2 x^2 + \cdots + f_n x^n$$

$$\forall a, b \in \mathbb{F}, (a+b)^p = a^p + C_p^1 a^{p-1} b + \cdots + b^p$$

$$\forall k \in \{1,2,3,\cdots,p-1\}, \quad C_p^k = \frac{p!}{k!(p-k)!}, \quad p \mid C_p^k$$

$$C_p^k a^{p-k} b^k = 0, \quad (a+b)^p = a^p + b^p$$

$$f^p(x) = (f_0 + f_1 x^+ f_2 x^2 + \cdots + f_n x^n)^p = f_0^p + f_1^p x^p + f_2^p x^{2p} + \cdots + f_n^p x^{np}$$

$$f(x^p) = f_0 + f_1 x^p + f_2 x^{2p} + \cdots + f_n x^{np}$$

$$\forall i \in \{0,1,2,\cdots,n\}, \quad f_i \in \mathbb{F}_p \Leftrightarrow f_i^p = f_i$$

$\square$

$\eta \in \{\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^7, \varepsilon^8, \varepsilon^{11}, \varepsilon^{13}, \varepsilon^{14}\}, \eta^{2^4} = \eta$

$\exists f(x) \in \mathbb{F}_2[x], f(\eta) = 0 \Rightarrow f(\eta^2) = f(\eta^{2^2}) = f(\eta^{2^3}) = f(\eta) = 0$

let $\quad \mathbb{F} = \mathbb{F}_2(\eta) \quad h(x) = (x-\eta)(x-\eta^2)(x-\eta^{2^2})(x-\eta^{2^3}) \quad h(x) \in \mathbb{F}[x]$

$$\begin{aligned} h^2(x) &= (x-\eta)^2(x-\eta^2)^2(x-\eta^{2^2})^2(x-\eta^{2^3})^2 \\ &= (x^2-\eta^2)(x^2-\eta^{2^2})(x^2-\eta^{2^3})(x^2-\eta^{2^4}) \\ &= (x^2-\eta)(x^2-\eta^2)(x^2-\eta^{2^2})(x^2-\eta^{2^3}) \\ &= h(x^2) \end{aligned}$$

$h(x) \in \mathbb{F}_2[x]$

$$\Phi_{15}(x) = \underbrace{(x-\varepsilon)(x-\varepsilon^2)(x-\varepsilon^4)(x-\varepsilon^8)}_{h_1(x)}\underbrace{(x-\varepsilon^7)(x-\varepsilon^{14})(x-\varepsilon^{13})(x-\varepsilon^{11})}_{h_2(x)}$$

$\Phi_{15}(x) = (x^4+x+1)(x^4+x^3+1)$

Search primitive polynomials in $\mathbb{F}_2[x]$

Generally, $\Phi_{2^n-1}(x)$ can be divided into $\dfrac{\varphi(2^n-1)}{n}$ different n-degree polynomials(called primitive polynomials) in $\mathbb{F}_2[x]$.

$$r_n = \frac{\varphi(2^n-1)}{n2^n} = \frac{\prod(1-\frac{1}{p_i})}{n}$$

$n =$	5	6	9	14	18
$r_n =$	0.186	0.095	0.094	0.046	0.030
$1/n =$	0.200	0.167	0.111	0.071	0.056
$n =$	26	29	30	33	41
$r_n =$	0.026	0.034	0.017	0.025	0.024
$1/n =$	0.038	0.034	0.033	0.030	0.024
$n =$	50	53	65	69	74
$r_n =$	0.012	0.019	0.015	0.012	0.009
$1/n =$	0.020	0.019	0.015	0.014	0.013
$n =$	81	86	90	98	
$r_n =$	0.010	0.008	0.005	0.007	
$1/n =$	0.012	0.012	0.011	0.010	

Lemma 2.If $f(x) \in \mathbb{F}_2[x]$ is a nth irreducible polynomial, then $f(x) \,|\, (x^{2^n-1} - 1)$.

Proof. $\mathbb{F} = \{f_0 + f_1 x + \cdots + f_{n-1}x^{n-1} \,|\, f_0, f_1, \ldots f_{n-1} \in \mathbb{F}_2\}$

$$f_0(x), f_1(x), \ldots, f_{2^n-1}(x) \in \mathbb{F}\backslash\{0\} \quad (\forall 0 \leqslant i < j \leqslant 2^n - 1, f_i(x) \neq f_j(x))$$

$$\forall 0 \leqslant i < j \leqslant 2^n - 1, xf_i(x) \not\equiv xf_j(x) \pmod{f(x)}$$

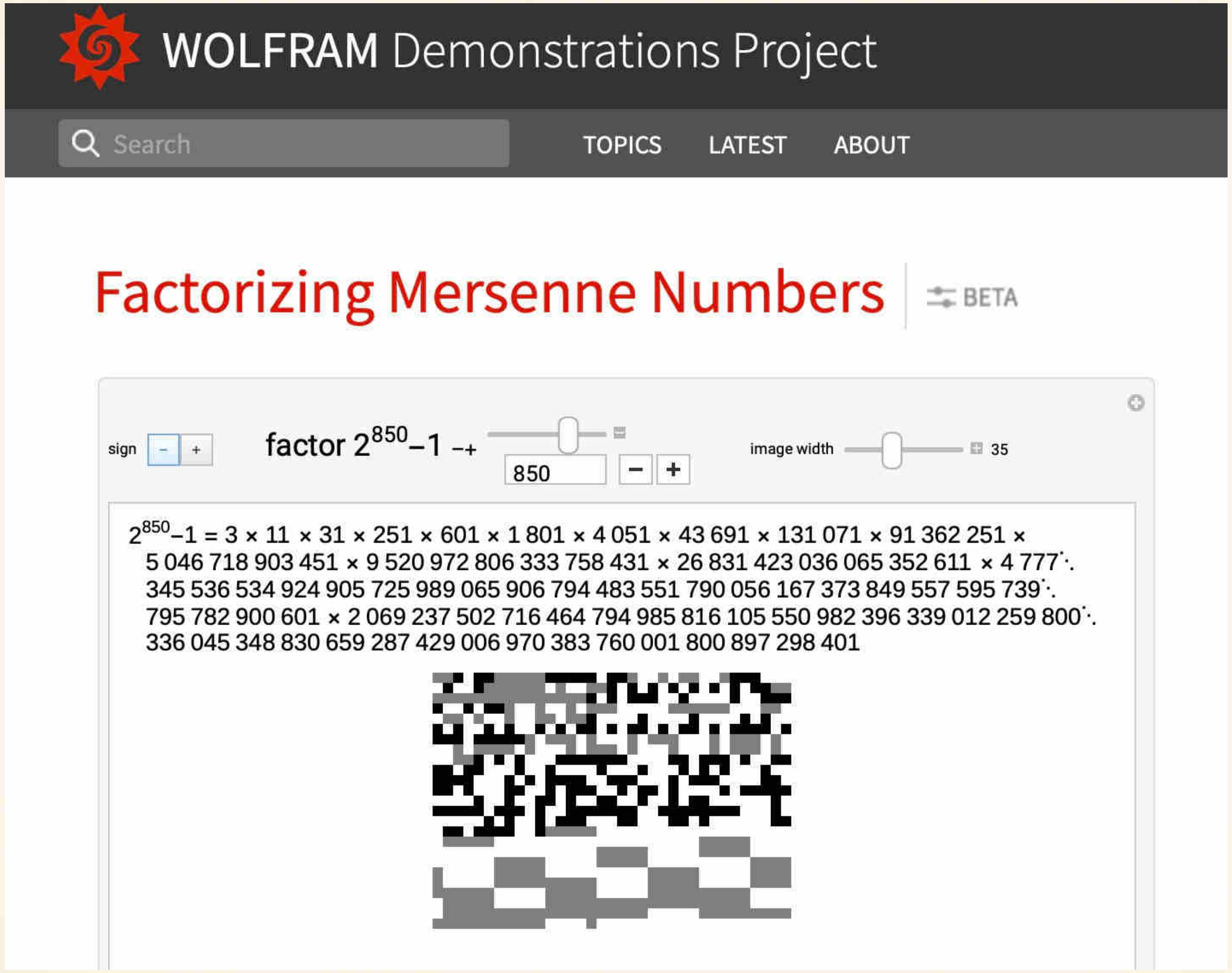
$$\prod_0^{2^n-1} f_i(x) \equiv \prod_0^{2^n-1} xf_i(x) \pmod{f(x)}$$

$$x^{2^n-1} \equiv 1 \pmod{f(x)} \quad f(x) \,|\, (x^{2^n-1} - 1) \qquad \square$$

Lemma 3. $f(x) \in \mathbb{F}_2[x]$ is a nth primitive polynomial if and only if

- $f(x) \,|\, (x^{2^n-1} - 1)$
- $\forall 1 \leqslant k < n, gcd(f(x), x^{2^k-1} - 1) = 1$
- $\forall t \,|\, 2^n - 1, f(x) \nmid (x^t - 1)$

https://demonstrations.wolfram.com/FactorizingMersenneNumbers/



The largest known Mersenne Prime $2^{82,589,933} - 1$

Thank you!