

Anzahl primitiver Polynome berechnen

Anzahl gegeben durch

$$\frac{\varphi(2^n - 1)}{n}, \text{ Grad} = n$$

$$\text{z.B. } \frac{\varphi(2^4 - 1)}{4} = \frac{\varphi(15)}{4} = \frac{\varphi(3) \cdot \varphi(5)}{4} = \frac{2 \cdot 4}{4} = 2$$

$$\begin{aligned}n=9: \quad & \frac{\varphi(2^9-1)}{9} = \frac{\varphi(511)}{9} \\ & = \frac{\varphi(7 \cdot 73)}{9} = \frac{\varphi(7) \cdot \varphi(73)}{9} \\ & = \frac{6 \cdot 72}{9} = 6 \cdot 8 = 48\end{aligned}$$

Bemerkung:

das kleinste $i \in \mathbb{N}$ mit

$$X^i \bmod P(X) = 1$$

heißt *Ordnung* von $X \bmod P(X)$

Schreibweise: $\text{ord}_{P(X)}(X)$

Beispiel :

$$P(x) = x^4 + x^3 + x^2 + x + 1$$

$$\text{ord}_{P(x)} X = 5 \quad \dots$$

weil $X^i \bmod P(x) \neq 1 \quad (1 \leq i \leq 4)$

$$\text{und} \quad X^5 \bmod P(x) = 1$$

$$\text{ord}_{P(x)} X = \underline{\underline{5}}$$

Anzahl möglicher Reste

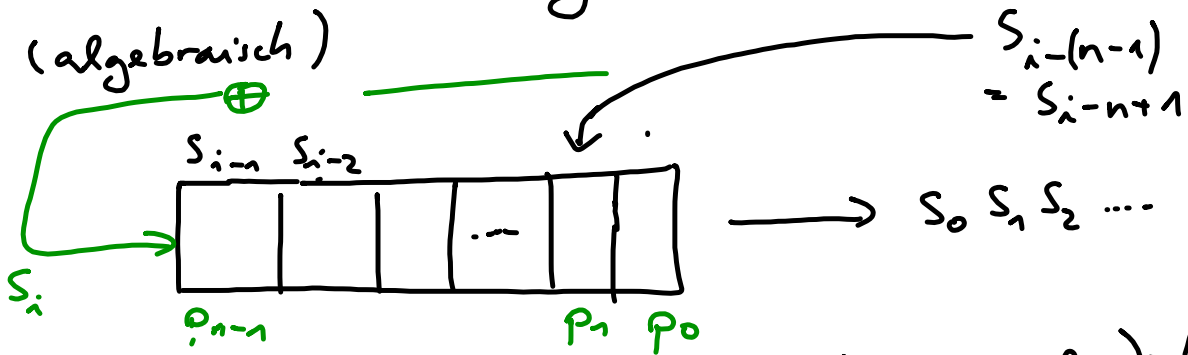
$$2^n - 1 = 2^4 - 1 = \underline{\underline{15}}$$

allgemein:

$$\text{ord}_{P(x)} a(x) \text{ teilt } 2^n - 1,$$

$$\text{wobei } n = \text{Grad von } P(x)$$

Rekursive Darstellung eines LFSR (algebraisch)



Anfangszustand: $\boxed{S_{n-1} \dots S_1 S_0} = (k_{n-1} \dots k_0) = \text{key}$

Rekursion: $S_i = p_0 \cdot S_{i-n} + p_1 \cdot S_{i-n+1} \dots + p_{n-1} \cdot S_{i-1}$

Wie "sicher" ist ein LFSR?

- a). aus s_i die p_i berechnen
bringt es etwas, das Design des
LFSR geheim zu halten?
- b). aus dem s_i den Anfangszustand
berechnen, d.h. kann man den Key
geheim halten?

a) Design aus den s_i berechnen

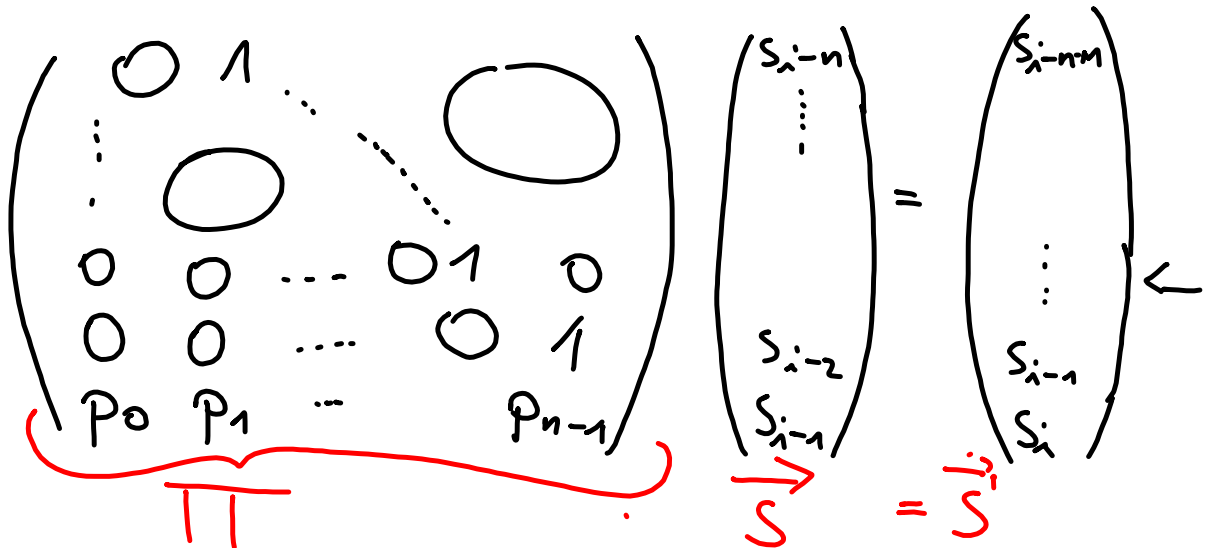
$$\begin{pmatrix} s_{i-n} & s_{i-n+1} & \dots & s_{i-1} \\ s_{i+1-n} & s_{i+2-n} & \dots & s_i \\ \vdots & & & \vdots \\ s_{i-1} & \dots & & s_{i+n-2} \end{pmatrix} \cdot \begin{pmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{n-1} \end{pmatrix} = \begin{pmatrix} s_i \\ s_{i+1} \\ s_{i+2} \\ \vdots \\ s_{i+n-1} \end{pmatrix}$$

$A \quad \cdot \quad \underline{x} \quad = \quad \underline{b}$

\Rightarrow Gauß-Algorithmus

b) Design bekannt, Anfangszustand ausrechnen

$$S_i = p_0 \cdot S_{i-n} + p_1 \cdot S_{i-n+1} + \dots + p_{n-1} \cdot S_{i-1}$$




$\Pi \cdot \vec{s} = \vec{s}'$ LFSR-Operation

j Operationen des LFSR

$$\underbrace{\Pi \cdot \Pi \cdot \Pi \cdots \Pi}_{\Pi^j} \cdot \vec{s}$$

Anfangszustand: 1 Op. rückwärts

$$\Pi \cdot \vec{s} = \vec{s}^1$$


Inverse Matrix benötigt

$\Pi \rightarrow \Pi^{-1}$, falls Π invertierbar

$$k \text{ Op. rückwärts} \Rightarrow (\Pi^{-1})^k \cdot \vec{s}^1 = \begin{pmatrix} k_0 \\ \vdots \\ k_{n-1} \end{pmatrix} \text{ key}$$