LFSR - Polynome

LFSR = linear feedback shift reg.

LFSR mit max. Periode

→ Polynom, irreduzibel und primitiv

Beispiel: für Grad $n = 2$

ist $P(X) = X^2 + X + 1$

geeignet

$P(X) \equiv X^2 + X + 1 \pmod 2$

Grad 2: ✓

$X^2 + X + 1$

ist das einzige irreduzible Polynom

Grad 3:

$X^3 + 1$ hat Nullstelle $X=1$

$X^3 + X + 1$ irreduzibel

$X^3 + X^2 + 1$ irreduzibel

$X^3 + X^2 + X + 1$ hat Nullstelle

.....

Frage: ist $P(X) = X^3 + X + 1$ primitiv

$\Leftrightarrow$ $X^j \bmod P(X) = 1$ erst für $j = 2^3 - 1$

[X^j wird aus $X^{j-1} \cdot X$ berechnet]

j	$X^j \bmod P(X)$
1	X
2	X^2
3	$X + 1$
4	$X^2 + X$
5	$X^2 + X + 1$
6	$X^2 + 1$
7	1

✓ Ordnung maximal $\rightarrow P(X)$ primitiv

$X^3 \bmod X^3 + X + 1$:

$X^3 + X + 1 \bmod X^3 + X + 1 = 0$

$\Rightarrow X^3 = X + 1 \bmod X^3 + X + 1$

$P(X) = X^3 + X^2 + 1$ ebenfalls primitiv (Übung)

allgemein: die Anzahl primitiver Polynome vom Grad n ist

$$\frac{\varphi(2^n - 1)}{n}$$

Grad 4:

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

↑ primitive Polynome

Polynomliste

$X^4 + X + 1$ irred.

$X^4 + X^2 + 1$

$X^4 + X^3 + 1$ irred.

$X^4 + X^3 + X^2 + X + 1$ irred.

$(X^2+X+1)\cdot(X^2+X+1)$

Frage: $P(X) = X^4 + X + 1$ primitiv?

Ordnung von X ist Teiler von $2^n - 1$,

d.h. von $2^4 - 1 = 15$

$\rightsquigarrow$ teste $j = 3$, $j = 5$

$X^3 \bmod P(X) \neq 1$ ✓

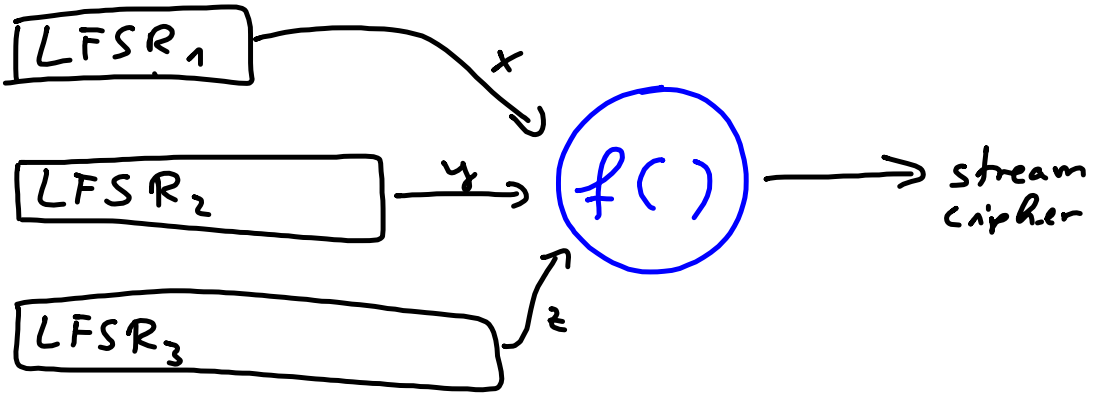
$X^5 = X^4 \cdot X = (X+1)\cdot X = X^2 + X \neq 1$

$\Rightarrow P(X)$ primitiv

Ebenso: $X^4 + X^3 + 1$ primitiv

$X^4 + X^3 + X^2 + X + 1$ irreduzibel aber nicht primitiv

Verwendung in Stromchiffren



f() heißt Combiner und muss nicht-linear sein

nicht-linear:

a) $x_i = x + \underbrace{y \cdot z}_{\text{Grad 2}}$

$x_i = x_{i-1} + x_{i-4} + x_{i-5}$ LFSR

bzw.
f durch Wertetabelle darstellen (z.B. Stromchiffre E_0, Bluetooth)

b) nicht-lineare Schieberegister benutzen (NFSR)

(z.B. Trivium, Grain siehe ESTREAM-Projekt)