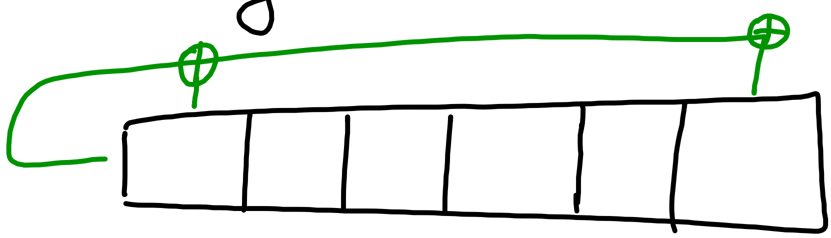
Beobachtung:



2 Bits verknüpft $\Rightarrow$ Länge $2^6 - 1$ möglich

3 Bits $\rightarrow$ nie $2^6 - 1$

4 Bits $\rightarrow$ möglich

5

letztes Bit nicht berücksichtigen

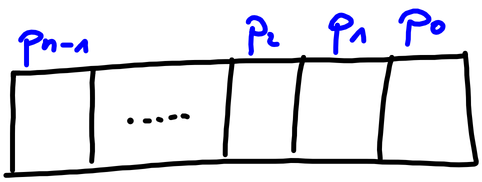
$\longrightarrow$ nie max. Periodenlänge

Modell für LFSR:

Polynome über der Menge $\overbrace{\underbrace{\{0,1\}}_{GF(2)}}^{\mathbb{F}_2}$

galois field mit 2 Elementen

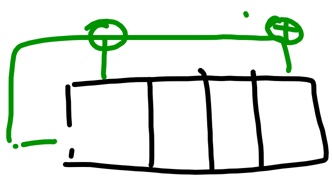
"Galois Körper"



Schieberegister mit n Bit

$\rightsquigarrow$ Polynom $X^n + p_{n-1}X^{n-1} + \dots + p_2X^2 + p_1X + p_0$

Beispiel:



$\rightsquigarrow X^4 + X^3 + 1$

Einschub: Rechnen mit Polynomen über $\mathbb{F}_2$

$\oplus = +$

$$(X+1)\cdot(X+1) = X^2 + \underbrace{X + X}_{(\underbrace{1+1}_{0})\cdot X} + 1$$

$$= X^2 + 1$$

"+" ist in $\mathbb{F}_2$ dasselbe wie "–"

Satz: Die Periodenlänge ist maximal 2^{n-1}, wenn das zugehörige Polynom primitiv ist.

irreduzibel

nicht zerlegbar

max. Ordnung von X

Irreduzibilität von Polynomen

$$x^2 + 1 = (x+1) \cdot (x+1)$$

Polynom vom Grad 2 zerlegt in Polynome vom Grad 1

$$x^3 + x^2 + x = x \cdot (x^2 + x + 1)$$ auch reduzibel

Analogie:

Primfaktorzerlegung

$$30 = 2 \cdot \underbrace{15}_{\text{zerlegbar}} = 2 \cdot 3 \cdot 5$$

Untersuchung von Nullstellen funktioniert bis zum Grad 3

$$(\text{Grad } 3) = (\text{Grad } 1) \cdot (\text{Grad } 2)$$

Nullstelle sichtbar

$$(\text{Grad } 4) = (\quad) \cdot (\quad)$$

evtl. (Grad 1)·(Grad 2)

Übung: suche irreduzible Polynome vom Grad 3

$P(X) := X^3 + p_2 \cdot X^2 + p_1 \cdot X + p_0$

$p_0 = 1$ notwendig, sonst $P(X) = X \cdot (\dots)$

$P(1) = 1 + p_2 + p_1 + 1 \overset{?}{=} 0$

$p_1 \neq p_2$ notwendig

übrig bleiben

$$\left.\begin{array}{l} X^3 + X^2 + 1 \\ X^3 + X + 1 \end{array}\right\}$$ sind irreduzibel, weil $P(0) = P(1) = 1$

Übung: alle irred. Polynome vom Grad 4 finden max Periodenlänge bei

irreduzibel $\boxed{\text{und}}$ primitiv

$i = 0$

multipliziere mit X mod $P(X)$

$i = i + 1$

solange Ergebnis $\neq 1$

wenn $i = 2^n - 1$, dann $P(X)$ primitiv

Übung:

welche der oben gefundenen $P(X)$

vom Grad 4 sind primitiv

Beispiel: $P(X) = X^3 + X + 1$

starte mit 1, mult. mit X, danach mod $P(X)$

i	$X^i \bmod P(X)$
1	X
2	X^2
3	$X+1$
4	X^2+X
5	X^2+X+1
6	X^2+1
7	$\boxed{1}$

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

$X^3+X+1 \pmod{P(X)} = 0$

$X^3 = +X+1$