8. Lecture
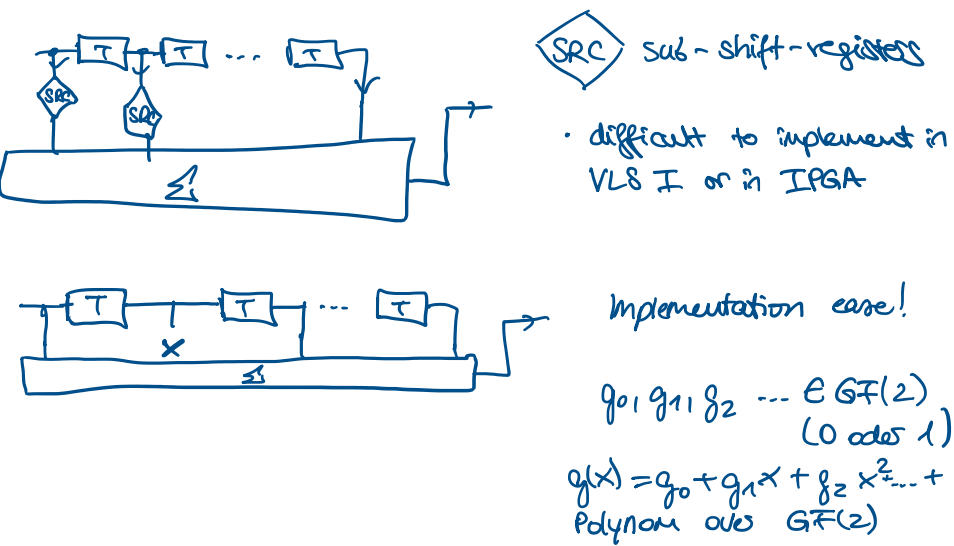
zykl. Reed- Salomon codes over $GF(2^M)$

↓ Real-Time (fast)   ↓ optimal performance   ↓ binary transmission

---
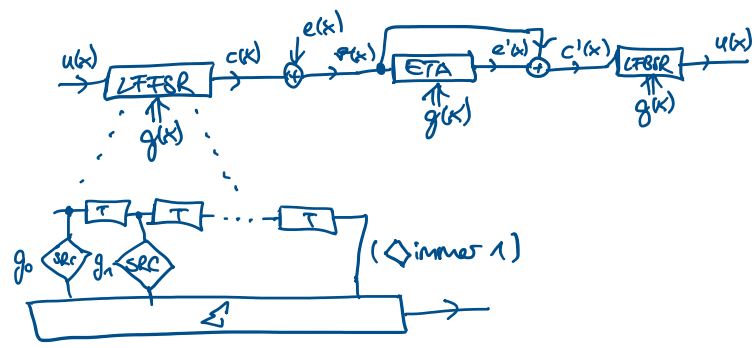
↗ Folien
   SNR - signal to noise ratio | Bit error probability should be kleiner als $2*10^{-4}$ |

d_{min} ⟷ SNR relationship (can look up)

↑SNR → prob. ↓

algorithmen domain → nicht unter (10^{-4})
   ⟹ aber kann error-correcting codes benutzen

C_{etr} (read-Salomon code)

BCH (Bose - Chaudhuri - Hocquenghian) codes

SRC sub-shift-registers

· difficult to implement in VLSI or in IPGA

Implementation ease!

$g_0, g_1, g_2 \cdots \in GF(2)$
   (0 oder 1)
$g(x) = g_0 + g_1 x + g_2 x^2 \cdots +$
Polynom over $GF(2)$

"t" number of errors to be corrected then $g(x)$ roots $\geq 2t$

$g(x) \longrightarrow$ "poor" coefficients $\in GF(2)$
        $\longrightarrow$ "rich" roots

Properties of polynoms over $GF(2)$ $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_n x^n$

$f_0, f_1, \cdots, f_n \in GF(2) \rightarrow f(\beta) = \emptyset \rightarrow f(\beta^{2^e}) = \emptyset$
$\beta^e, e \rightarrow 2, \cdots,$ conjugate roots
$f^{2^e}(x) = f(x^{2^e}) \implies f^{2^e}(\beta) = f(\beta^{2^e}) = \emptyset$

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

$= f_0^2 + f_1^2 x^2 + f_1 x(\cancel{f_2 x^2 + \cdots + f_n x^n}) + f_1 x(f_2 x^2 + \cdots + f_n x^n) + (f_2 x^2 + \cdots + f_n x^n)^2$ $GF(2)$

$= f_0^2 + f_1^2 x^2 + f_2^2 x^4 + \cdots + f_n^2 x^{2n}$

$= f_0 + f_1 x^2 + f_2 x^4 + \cdots + f_n x^{2n}$

$= f(x^2)$

Minimal polynom: $\beta, \beta^2 \cdots \beta^{2^e}$ $\Phi(x) = \prod_e (x + \beta^{2^e})$

→ Minimal polynoms over $GF(8)$

(y, y^2, y^4) $(y^8 = y)$
$(y^3, y^6, y^{12} = y^5)$ ⟹ 3 different roots

power table

y^0	1
y^1	y
y^2	y^2
y^3	$y+1$
y^4	y^2+y
y^5	y^2+y+1
y^6	y^2+1

$\Phi_1(x) = (x+y)(x+y^2)(x+y^4)$
$= (x^2 + y^4 x + y^3)(x+y^4)$
$= x^3 + y^4 x^2 + y^3 x + y^4 x^2 + \cancel{} + y x + y^7$
$= x^3 + (y+1+y)x + 1$
$= x^3 + x + 1$

$\Phi_3(x) = (x+y^3) + (x+y^5) + (x+y^6)$
$= (x^2 + y^2 x + y)(x+y^6)$
$= x^3 + y^2 x^2 + y x + x^2 y^6 + y x + 1$
$= x^3 + x^2 + 0 \cdot x + 1$ $y^6 = (y^2 + 1)$
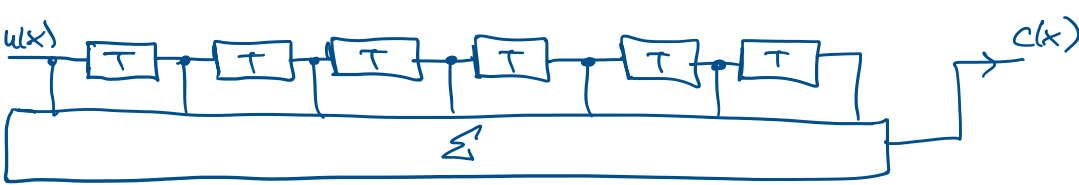
BCH codes: "t" # of errors to be corrected

$g(x) = \Phi_1(x) \cdots \Phi_{2t-1}(x)$

EXAMPLE

$t = 2$ $g(x) = \Phi_1(x) \Phi_3(x)$

$= (x^3 + x + 1)(x^3 + x^2 + 1)$
$= x^6 + x^4 + x^3 + x^5 + x^3 + x^2 + x^3 + x + 1$
$= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

Notieren: $C(7, 1)$ $\xrightarrow{n=8-1}$ no longer a MDS code !!!