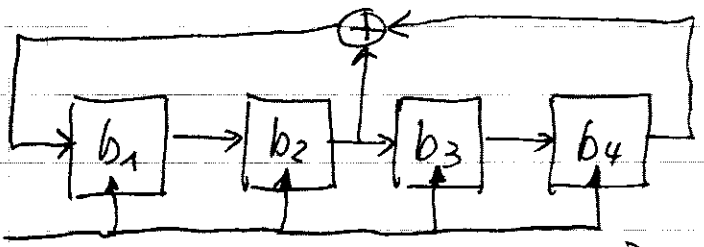
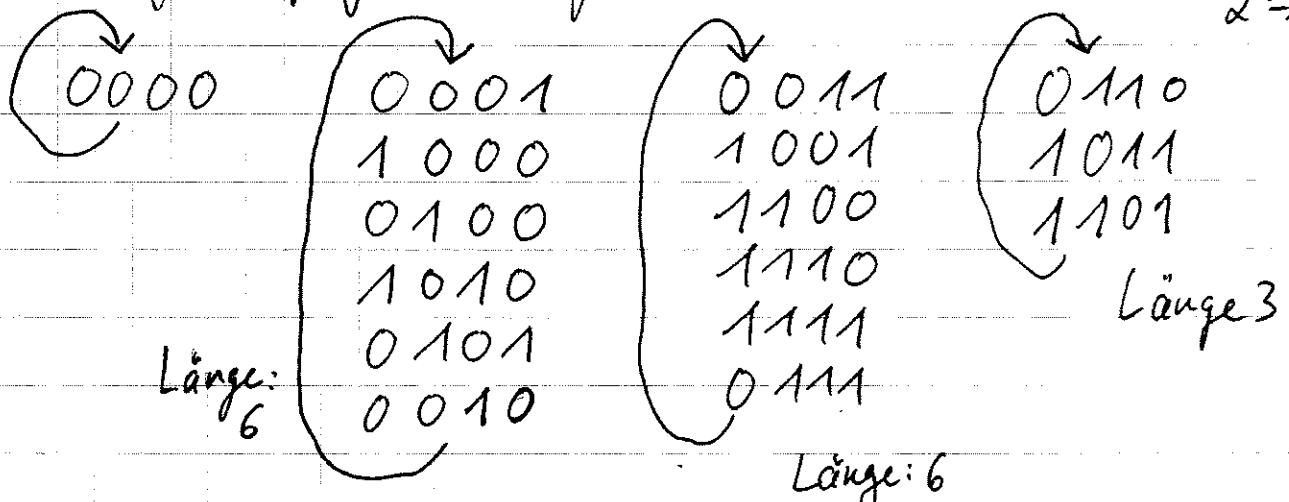
Lösungen der Aufgaben vom 7.5.2018

24.) Schaltplan:

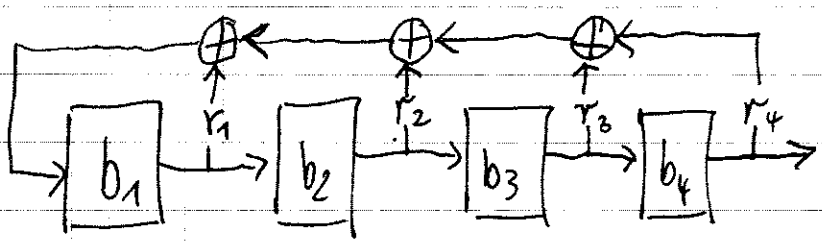


Die längste Periode bei 4 Flip-Flops ist $2^4 - 1 = 15$

Es gibt folgende Zyklen:



25.) Wir drücken die unbekannte Rückkopplungsschaltung mittels r_1, r_2, r_3, r_4 aus:



Hierbei bedeutet $r_i = 1$, dass Leitung vorliegt.

Die unbekannten initialen Werte seien b_1, b_2, b_3, b_4
Wir beobachten $2n$ Bits des Ausgabestroms und erhalten:

Schieberegister → $a_1\ a_2\ a_3\ a_4\ b_1\ b_2\ b_3\ b_4$

$a_1\ a_2\ a_3\ a_4$: mit diesen 4 Bits lässt sich die Rückkopplung ermitteln:

$b_1\ b_2\ b_3\ b_4$: dies sind die initialen Werte

Es gilt: $a_4 = b_1 r_1 \oplus b_2 r_2 \oplus b_3 r_3 \oplus b_4 r_4$

$a_3 = a_4 r_1 \oplus b_1 r_2 \oplus b_2 r_3 \oplus b_3 r_4$

$a_2 = a_3 r_1 \oplus a_4 r_2 \oplus b_1 r_3 \oplus b_2 r_4$

$a_1 = a_2 r_1 \oplus a_3 r_2 \oplus a_4 r_3 \oplus b_1 r_4$

Aus diesen 4 Gleichungen (über $\mathbb{Z}_2$) lassen sich die 4 Unbekannten r_1, r_2, r_3, r_4 ermitteln.

32.) Schlüssellänge $m=1$: A B C B A B B B A C

$$\widetilde{IC} = \frac{3}{10}\cdot\frac{2}{9} + \frac{5}{10}\cdot\frac{4}{9} + \frac{2}{10}\cdot\frac{1}{9} = \frac{28}{90} \approx 31\,\%$$

Schlüssellänge $m=2$:

A	C	A	B	A
B	B	B	B	C

$$\widetilde{IC}_1 = \frac{3}{5}\cdot\frac{2}{4} = \frac{6}{20} \approx 30\%$$
$$\widetilde{IC}_2 = \frac{4}{5}\cdot\frac{3}{4} = \frac{12}{20} \approx 60\%$$
} im Mittel: 45 %

Schlüssellänge $m=3$:

A	B	B
B	A	B
C	B	A

$\widetilde{IC}_1 = \frac{2}{4}\cdot\frac{1}{3} = \frac{2}{12} \approx 16.7\%$ $\widetilde{IC}_2 = \frac{2}{3}\cdot\frac{1}{2} = \frac{2}{6} \approx 33{,}3\%$

$\widetilde{IC}_3 = 0\%$, im Mittel: 16,7 %

Der größte Wert liegt bei $m=2$ vor.

1. Zeile: A C A B A

		parallel. Koinz index
shift = 0	A C A B A	$0{,}7\cdot 0{,}6 + 0{,}2\cdot 0{,}2 + 0{,}1\cdot 0{,}2 = 0{,}48$
shift = 1	B A B C B	$0{,}7\cdot 0{,}2 + 0{,}2\cdot 0{,}6 + 0{,}1\cdot 0{,}2 = 0{,}28$
shift = 2	C B C A C	$0{,}7\cdot 0{,}2 + 0{,}2\cdot 0{,}2 + 0{,}1\cdot 0{,}6 = 0{,}24$

2. Zeile: BBBBC

- Shift=0: BBBBC — $0{,}7 \cdot 0 + 0{,}2 \cdot 0{,}8 + 0{,}1 \cdot 0{,}2 = 0{,}18$
- Shift=1: CCCCA — $0{,}7 \cdot 0{,}2 + 0{,}2 \cdot 0 + 0{,}1 \cdot 0{,}8 = 0{,}22$
- Shift=2: AAAAB — $0{,}7 \cdot 0{,}8 + 0{,}2 \cdot 0{,}2 = 0{,}6$

Am plausibelsten: Shift=0 bei 1. Zeile; Shift=2 bei 2. Zeile.
D.h. Schlüsselwort ist AB.
Klartext ist daher: AACAAABAAB (7 A's, 2 B's, 1 C)

33.) In diesem Fall gilt $L_i = R_{i-1}$, $R_i = L_{i-1}$
Da eindeutig die Umkehrabbildung $(L_i, R_i) \mapsto (L_{i-1}, R_{i-1})$ berechnet werden kann, ist die Abbildung injektiv.
Da Wertebereich = Definitionsbereich (nämlich $\{0,1\}^{64}$) ist die Abbildung sogar bijektiv.

34.)
$$H(X,Y) = -\sum_{x,y} P(X=x, Y=y) \cdot \log_2 P(X=x, Y=y)$$
$$\overset{\text{(Unabh.)}}{=} -\sum_{x,y} P(X=x) \cdot P(Y=y) \cdot \log_2 \left(P(X=x) \cdot P(Y=y) \right)$$
$$= -\sum_{x,y} P(X=x) \cdot P(Y=y) \cdot \left(\log_2 P(X=x) + \log_2 P(Y=y) \right)$$
$$= -\sum_{x} P(X=x) \log_2 P(X=x) \underbrace{\sum_{y} P(Y=y)}_{=1}$$
$$- \sum_{y} P(Y=y) \cdot \log_2 P(Y=y) \cdot \underbrace{\sum_{x} P(X=x)}_{=1}$$
$$= H(X) + H(Y).$$

35.) $H(Y|X) = \sum_x P(X=x) \cdot H(Y|X=x)$

$= \sum_x P(X=x) \cdot \sum_y \underbrace{P(Y=y|X=x)}_{= \begin{cases} 1, & y=f(x) \\ 0, & \text{sonst} \end{cases}} \cdot \log_2 \underbrace{P(Y=y|X=x)}_{\text{elito.}}$

$= \sum_x P(X=x) \cdot 0 = 0$

36.) $1 + x^2 + x^4 = (1 + x + x^2) \cdot (1 - x + x^2)$

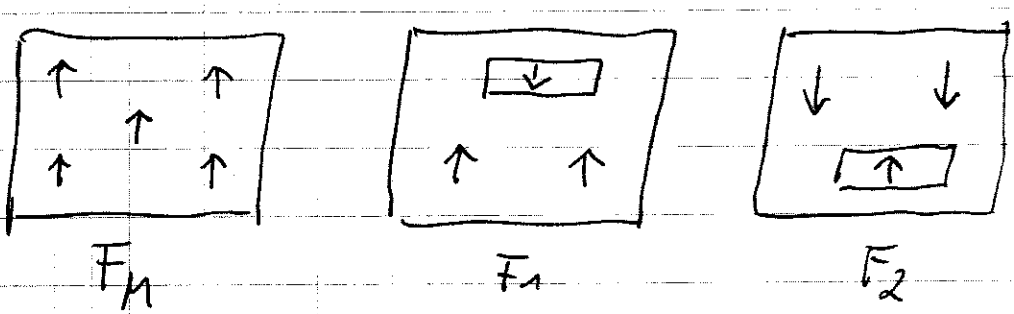
37.) a.) Abgesehen von der 0 besitzt jede der $n-1$ zu n teilerfremden Zahlen genau 2 verschiedene Quadratwurzeln (w und $-w$). Es gibt $\frac{n-1}{2}$ Quadrat-zahlen (sofern Quadratzahl). Größer kann die Periode nicht sein

b.) In $\mathbb{Z}_n^*$ (wobei $|\mathbb{Z}_n^*| = \varphi(n) = (p-1)(q-1)$) gibt es $\frac{p-1}{2} \cdot \frac{q-1}{2} \leq \frac{n}{4}$ Quadratzahlen. Länger kann eine Periode nicht sein.

38.) Die 4 leeren Kästchen erhalten folgende Werte:

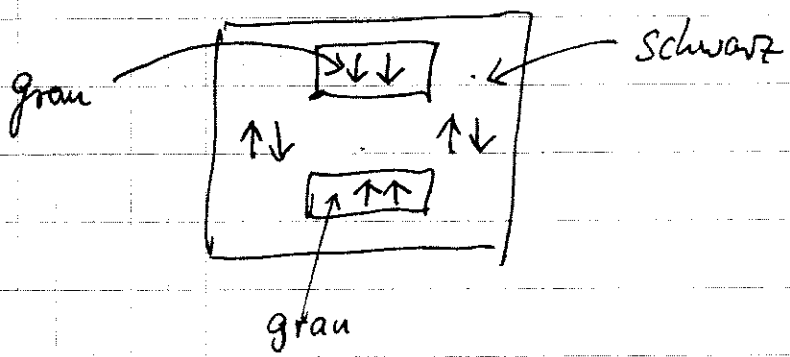
1110	0110
0110	0010

39.) Wir beschreiben die Folien F_M, F_1, F_2 kompakt wie folgt:



F_M F_1 F_2

Die rechteckigen Kästchen stellen die Schriften „Hallo" und „Welt" dar.
Legt man F_1, F_2 übereinander, erhält man:



Die richtige Antwort ist also:

Hallo ist lesbar (grau auf schwarz)

Welt ist lesbar (grau auf schwarz)