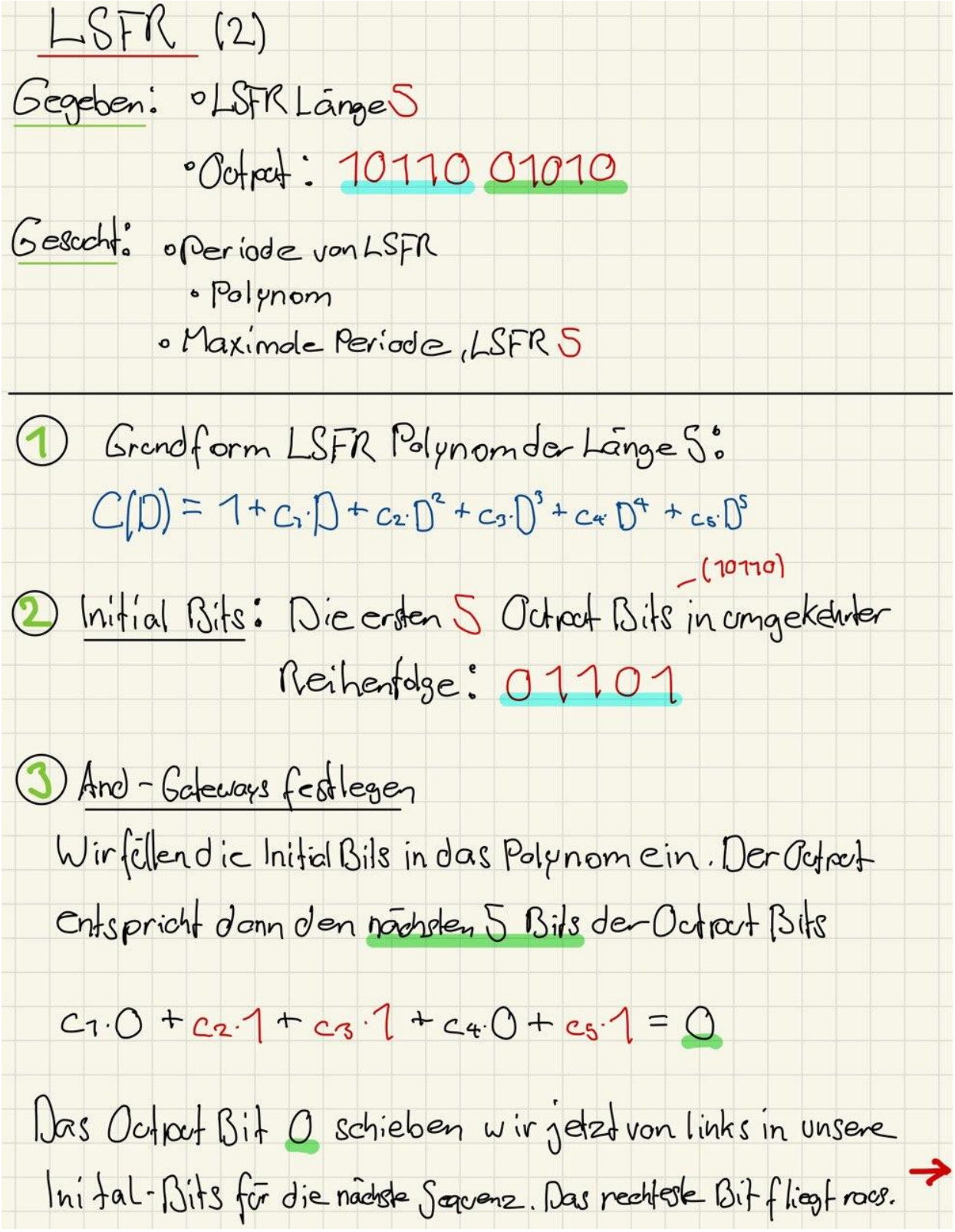
LSFR

Paper Way 2 (mathematischer):

Dieser Weg sollte besser verständlich sein und beinhaltet alle wesentlichen Schritte.



(31) Neue Bit Reihenfolge: 00110 X

Neue Sequenz ins Polynom: (01010 1) (1 2 3 4 5)

$c_1 \cdot 0 + c_2 \cdot 0 + c_3 \cdot 1 + c_4 \cdot 1 + c_5 \cdot 0 = 1$

Das machen wir jetzt 5 mal (solange wir Output Bits haben):

$c_1 \cdot 0 + c_2 \cdot 1 + c_3 \cdot 1 + c_4 \cdot 0 + c_5 \cdot 1 = 0$

$c_1 \cdot 0 + c_2 \cdot 0 + c_3 \cdot 1 + c_4 \cdot 1 + c_5 \cdot 0 = 1$

$c_1 \cdot 1 + c_2 \cdot 0 + c_3 \cdot 0 + c_4 \cdot 1 + c_5 \cdot 1 = 0$

$c_1 \cdot 0 + c_2 \cdot 1 + c_3 \cdot 0 + c_4 \cdot 0 + c_5 \cdot 1 = 1$

$c_1 \cdot 1 + c_2 \cdot 0 + c_3 \cdot 1 + c_4 \cdot 0 + c_5 \cdot 0 = 0$

Mit dieser Gleichung kann man jetzt 'erraten', welches die Gateways sind → c_1, c_3, c_5

Je nach LSFR ist das aber fast unmöglich. Ander MEP wird ein einfacheres LSFR kommen → siehe nächste Seite

(12) LSFR Länge 4: 0001 1110

$$c_1 \cdot 1 + c_2 \cdot 0 + c_3 \cdot 0 + c_4 \cdot 0 = 1$$

$$c_2 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 0 + c_4 \cdot 0 = 1$$

$$c_1 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 1 + c_4 \cdot 0 = 1$$

$$c_1 \cdot 1 + c_2 \cdot 1 + c_3 \cdot 1 + c_4 \cdot 1 = 0$$

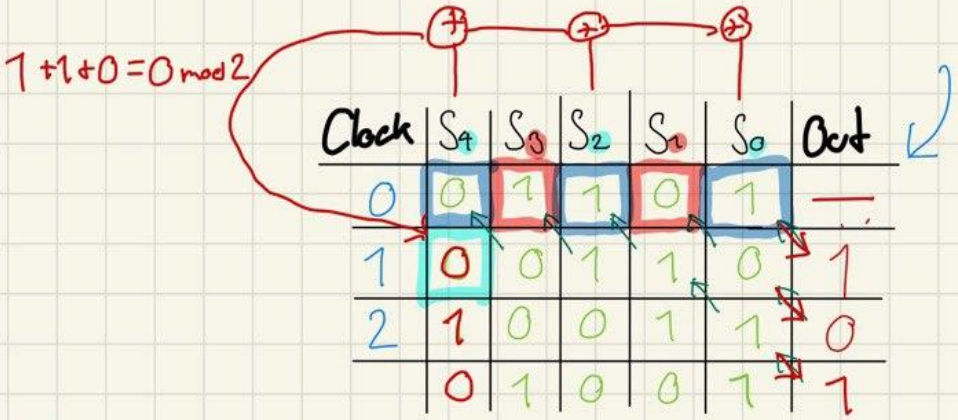
Hier sehen wir sehr schnell das c_1 ein Gateway ist.

c_2 und c_3 können keine Gateways sein und c_4 ist wieder eins.

(4) Mit den Gateways könnte man jetzt die Periode des LSFR suchen.

Dafür müsste man die Tabelle erstellen und schauen, wann sich die

Innet Bits wiederholen (Dauert lange...)



Nach wievielen Clocks wiederholt sich '01101' = Periode

⑤ Maximale Periode: Die maximale Periode ist nur mit "primitive Polynoms" möglich ⇒ Siehe Tabelle!

Für LSFR-5 wäre das (0, 2, 5) 5 = lange LSFR

Also wenn c2 und c5 Gateways sind

Die Formel lautet dann: $2^L - 1 \Rightarrow 2^5 - 1 = 31$

⑥ Mit den Gateways c1, c3, c5 können wir das effektive Polynom aufschreiben.

Aus: $C(D) = 1 + c_1 \cdot D + c_2 \cdot D^2 + c_3 \cdot D^3 + c_4 \cdot D^4 + c_5 \cdot D^5$

Wird: $C(D) = 1 + D^1 + D^3 + D^5$