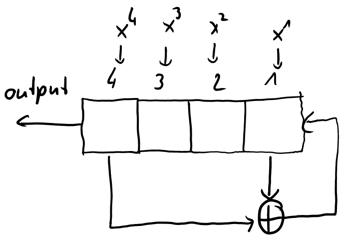
Linear Feedback Shift Register (LFSR)

06 May 2014 09:58

m-Sequenz

primitives Polynom: $(4,1,0) \rightarrow$ Feedback-Polynom: $x^4 + x^1 + 1$

zugehörige Schaltung:



Vorgehen: 1. und 4. Stelle XOR-en, links shiften und das XOR-te rechts einschieben

seed: 1111

output	$x^4\ x^3\ x^2\ x^1$	Vorher. x^4 ⊕ Vorher. x^1 = neues x^1
1	1110	$1 \oplus 1 = 0$
1	1101	$1 \oplus 0 = 1$
1	1010	$1 \oplus 1 = 0$
1	0101	$1 \oplus 0 = 1$
0	1011	$0 \oplus 1 = 1$
1	0110	$1 \oplus 1 = 0$
0	1100	$0 \oplus 0 = 0$
1	1001	$1 \oplus 0 = 1$

output	$x^4\ x^3\ x^2\ x^1$	Vorher. x^4 ⊕ Vorher. x^1 = neues x^1
1	0010	$1 \oplus 1 = 0$
0	0100	$0 \oplus 0 = 0$
0	1000	$0 \oplus 0 = 0$
1	0001	$1 \oplus 0 = 1$
0	0011	$0 \oplus 1 = 1$
0	0111	$0 \oplus 1 = 1$
0	1111	$0 \oplus 1 = 1$

$\Rightarrow$ Periode von 15

$\Rightarrow$ Output: 111101011001000

Überprüfen der Zufallseigenschaften (des Outputs):

1. 0-er im Output : 7
   1-er imOutput : 8 → ausgeglichen ✓

2. Runlänge: k
   Anzahl Runs der Länge k: #
   Formel: $P = \left(\frac{1}{2}\right)^k$ für $k \leq (n-1)$ und $P = \left(\frac{1}{2}\right)^{k-1}$ für $k = n$
   Test: $\sum \# = 4 + 2 + 1 + 1 = 8$; muss gelten: $P * 8 = \#$

Test: $\sum \# = 4 + 2 + 1 + 1 = 8$; muss gelten: $P * 8 = \#$

k	$\#$	P	Test
1	4	$(1/2)^1 = 1/2$	$8 \cdot 1/2 = 4$ ✓
2	2	$(1/2)^2 = 1/4$	$8 \cdot 1/4 = 2$ ✓
3	1	$(1/2)^3 = 1/8$	$8 \cdot 1/8 = 1$ ✓
4	1	$(1/2)^{4-1} = 1/8$	$8 \cdot 1/8 = 1$ ✓

3.

Output	111101011001000
Output um 1 nach rechts geshiftet	011110101100100
XOR der zwei Sequenzen soll die gleiche Sequenz wieder ergeben aber geshiftet	100011110101100

✓