Homework 3

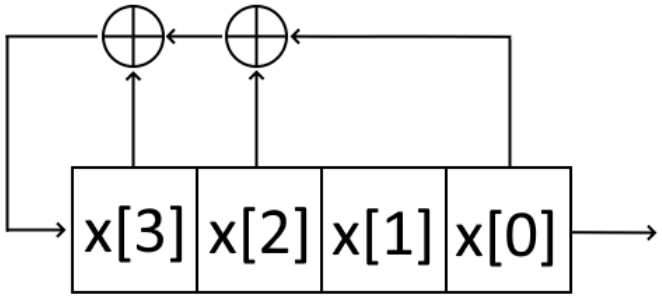
Ασημάκης Κύδρος
ΑΕΜ: 3881
asimakis@csd.auth.gr

Μάρτιος 2023

Έστω LFSR μήκους 4 με πολυώνυμο ανάδρασης $f(x) = x^4+x^2+x+1$ και seed $(x[3], x[2], x[1], x[0])$:

1 Βρείτε τα outputs $y[0] - y[8]$ συναρτήσει των $x[0], x[1], x[2], x[3]$.

Από το πολυώνυμο ανάδρασης προκύπτει ο παρακάτω καταχωρητής:



Γνωρίζοντας τα taps, καταλήγουμε στον παρακάτω πίνακα καταστάσεων του καταχωρητή:

0	$x[3]$	$x[2]$	$x[1]$	$\underline{x[0]}$
1	$x[3] \oplus x[2] \oplus x[0]$	$x[3]$	$x[2]$	$\underline{x[1]}$
2	$x[2] \oplus x[1] \oplus x[0]$	$x[3] \oplus x[2] \oplus x[0]$	$x[3]$	$\underline{x[2]}$
3	$x[3] \oplus x[2] \oplus x[1]$	$x[2] \oplus x[1] \oplus x[0]$	$x[3] \oplus x[2] \oplus x[0]$	$\underline{x[3]}$
4	$x[0]$	$x[3] \oplus x[2] \oplus x[1]$	$x[2] \oplus x[1] \oplus x[0]$	$\underline{x[3] \oplus x[2] \oplus x[0]}$
5	$x[1]$	$x[0]$	$x[3] \oplus x[2] \oplus x[1]$	$\underline{x[2] \oplus x[1] \oplus x[0]}$
6	$x[2]$	$x[1]$	$x[0]$	$\underline{x[3] \oplus x[2] \oplus x[1]}$
7	$x[3]$	$x[2]$	$x[1]$	$\underline{x[0]}$
8	$x[3] \oplus x[2] \oplus x[0]$	$x[3]$	$x[2]$	$\underline{x[1]}$

Βλέπουμε πως ο καταχωρητής έχει περίοδο 7, άρα μετά το $y[6]$ ξαναγυρίζουμε στην αρχή.

Η τελευταία στήλη πάντα δηλώνει τα outputs των δεδομένων καταστάσεων. Επομένως οι τύποι των y είναι:

$$
\begin{aligned}
y[0] &= y[7] = x[0] \\
y[1] &= y[8] = x[1] \\
y[2] &= x[2] \\
y[3] &= x[3] \\
y[4] &= x[3] \oplus x[2] \oplus x[0] \\
y[5] &= x[2] \oplus x[1] \oplus x[0] \\
y[6] &= x[3] \oplus x[2] \oplus x[1]
\end{aligned}
$$

2 Βρείτε το αρχικό seed αν $y[5] = y[8] = 1$, $y[6] = y[7] = 0$, χωρίς brute force.

Από τα παραπάνω έχουμε

$$x[0] = y[7] = 0$$
$$x[1] = y[8] = 1$$
$$x[2] = y[5] \oplus x[1] \oplus x[0] = 1 \oplus 1 \oplus 0 = 0$$
$$x[3] = y[6] \oplus x[2] \oplus x[1] = 0 \oplus 0 \oplus 1 = 1$$

επομένως το αρχικό seed είναι

1010