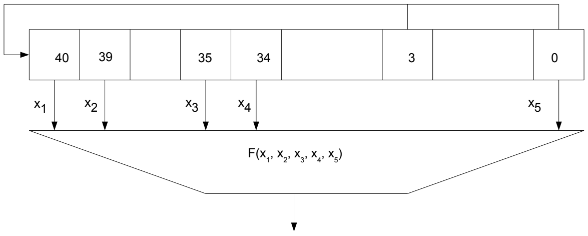
MANDATORY ASSIGNMENT 2



Filter Generator: LFSR of length 41 with characteristic polynomial $X^{41} + X^3 + 1$ and Boolean function $F(x_1, x_2, x_3, x_4, x_5) = x_1 x_2 \oplus x_3 \oplus x_4 \oplus x_5$.

Given key-stream of length $N = 210$, compute the initial state with Fast Correlation attack. Key-stream:

$1,0,0,0,0,0,0,1,1,1,0,0,1,0,1,0,1,1,0,0,0,1,1,1,0,0,0,1,1,0,1,0,1,0,1,1,1,0,1,1,0,$
$1,0,0,0,1,0,1,1,0,0,0,1,1,1,0,0,1,1,1,1,1,1,0,1,1,0,1,1,0,1,1,1,0,1,1,0,0,0,0,1,0,$
$1,1,0,1,0,1,1,1,0,1,1,1,1,0,1,1,0,0,0,0,1,0,1,1,1,1,1,0,1,1,0,0,0,1,1,0,1,0,1,0,1,$
$0,1,0,0,1,1,0,0,0,0,1,0,1,0,1,1,1,1,0,1,0,1,1,1,0,1,1,1,0,1,1,1,0,0,1,1,1,1,1,1,0,$
$0,0,1,0,1,1,0,1,0,1,1,1,1,0,1,1,0,1,1,0,1,0,0,0,1,0,1,1,0,1,1,0,1,1,0,0,0,0,1,1,0,$
$0,1,0,0,0$

Find a good affine approximation for F, compute a posteriori probabilities of zero-relations, choose linear equations with low weight left-hand side, solve them. Provide with a description of the attack, results and your readable (commented) source code, submit as a single pdf file. The deadline is Wednesday, 9 March, 2022, midnight.