

Assignment 3 (Topic 4. Pseudo-random Sequence/Number Generators)

1. Design a filtering generator which satisfies the following requirements.
 - (a) Period 31.
 - (b) Balanced.
 - (c) Linear span 15.
2. For a combinatorial function generator, let a boolean function $f(x_0, x_1, x_2) = x_0 + x_1 + x_2$ and three LFSRs have degrees 2, 3 and 5, respectively. Find the prototype of period and linear span of output sequences. How many output sequences are balanced if the initial state of LFSR of degree 5 is loaded to zero?

You may replace one of the above questions by the following problem.

3. Let $\mathbf{a} = \{a_i\}$ and $\mathbf{b} = \{b_i\}$ be two sequences generated by LFSR with a primitive polynomial of degree n , say $f(x)$, as the characteristic polynomial, and $\mathbf{c} = \{c_i\}$ where $c_i = a_i b_i, i = 0, 1, \dots$. Show that the linear span of \mathbf{c} is n^2 . (Hint. Let α be a primitive element in $GF(2^n)$ satisfies that $f(\alpha) = 0$. Then the trace representations of \mathbf{a} and \mathbf{b} are given by $a_i = Tr(\beta\alpha^i)$ and $b_i = Tr(\gamma\alpha^i), \beta$ and $\gamma \in GF(2^n)$. Then

$$c_i = a_i b_i = (\beta\alpha^i + \beta^2\alpha^{2i} + \dots + \beta^{2^{n-1}}\alpha^{2^{n-1}i})(\gamma\alpha^i + \gamma^2\alpha^{2i} + \dots + \gamma^{2^{n-1}}\alpha^{2^{n-1}i}).$$

The linear span of \mathbf{c} is equal to the number of non-zero coefficients of α^i , since we can group these terms into several trace terms and each trace term represents an LFSR.)

4. Let an LFSR with the primitive characteristic polynomial $x^4 + x + 1$.
 - (a) Find a filtering design such that the output sequences have linear span 14.
 - (b) Find a filtering design such that 4-tuples are different with linear span > 4 .