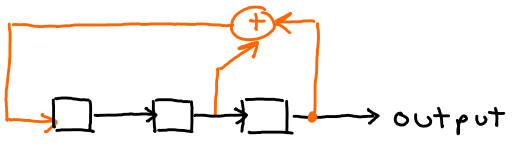
m-Sequence examples

Tuesday, January 11, 2011
12:23 PM

Example 1

$g(\alpha) = \alpha^3 + \alpha^2 + 1$

Degree : $r = 3$ $\Rightarrow$ use 3 FFs



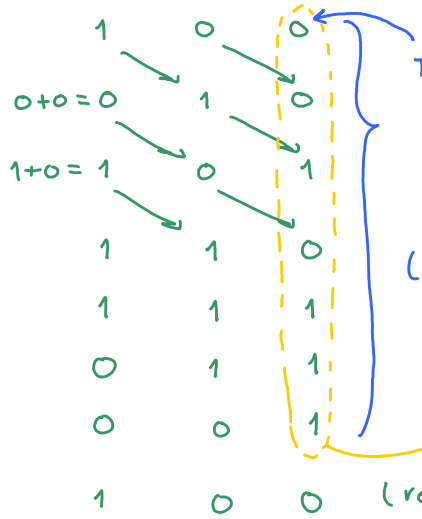
Start with ~~any~~ nonzero states.

I usually start with

1 0 0 ··· 0

if there are more than 3 bits.

$1 + 0\alpha + 1\alpha^2 + 1\alpha^3$ ← coefficient ⇒ connection variable
↳ 1 for connection
↳ 0 for no connection



The state of the whole shift-register can be represented by 3 bits. (r bits)

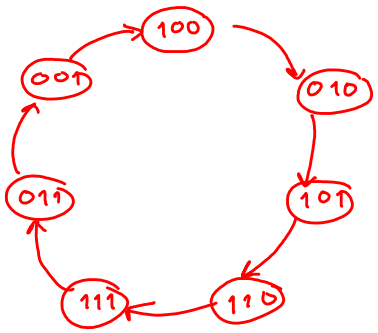
7 possible nonzero state.

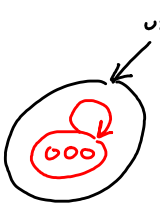
$(2^r - 1)$

m-sequence : 00101110

(periodic with period $2^r - 1 = 7$ when $r = 3$)

state diagram :





This single cycle covers all nonzero states.

So, the LFSR with generator polynomial $g(\alpha) = \alpha^3 + \alpha^2 + 1$ generates m-sequence.

Fact : $g(\alpha)$ generates m-sequence iff $g(\alpha)$ is a primitive polynomial.

We will take this as a definition for primitive polynomial.

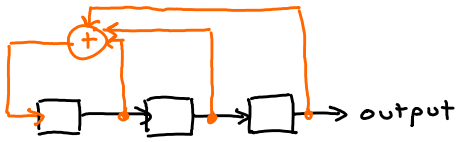
Definition : A polynomial $g(\alpha)$ is a primitive polynomial if the corresponding LFSR circuit generates m-sequence.

For $g(\alpha) = \alpha^3 + \alpha^2 + 1$ is a primitive polynomial

So, $g(\alpha) = \alpha^3 + \alpha^2 + 1$ is a primitive polynomial.

Example 2

$g(\alpha) = \alpha^3 + \alpha^2 + \alpha + 1$



$1 + \alpha + \alpha^2 + \alpha^3$

1 0 0
1 1 0
0 1 1
0 0 1
1 0 0 (repeat)

The cycle does not cover all nonzero states.
Hence, the LFSR with generator polynomial $g(\alpha) = \alpha^3 + \alpha^2 + \alpha + 1$ does not generate m-sequence.

(The polynomial $g(\alpha) = \alpha^3 + \alpha^2 + \alpha + 1$ is not primitive.)

To find the complete state diagram, we need to find out which nonzero states are missing from the cycle above.

We see that 010 is still missing.
So start a new cycle with 010.

0 1 0
1 0 1
0 1 0 (repeat)

Again, we check whether we have all non-zero states.
State 111 is still missing.

So start a new cycle with 111.

1 1 1
1 1 1 (repeat)

Again, we check whether we have all non-zero states.
Turn out that we have all $(4+2+1=7)$ non-zero states.

State diagram :

state diagram :