17 m-sequene

Tuesday, January 18, 2011
11:29 AM

Lecture 17 (DSSS and m-sequence)

Review : Spread Spectrum (SS)
- → Freq. Hopping (FH)
- → Direct Sequence (DS) ← *

Need spreading codes/sequences $c(t)$ ← how can we construct this??

(A) Random spreading sequence $c(t)$

These names are simply many versions of the same sequence/process.

- coin-flipping sequence: $\cdots\; X_{-4}\; X_{-3}\; X_{-2}\; X_{-1}\; X_0\; X_1\; X_2\; X_3\; X_4\; X_5 \cdots$ — - - - H H T H H T T T H T - - -
- Bernoulli trials/sequence: - - - 1 1 0 1 1 0 0 0 1 0 - - -
- Binary independent random sequence. → −1 −1 1 −1 −1 1 1 1 −1 1 ← This is what we will really use in DSSS

Note that we map $0 \to 1$, $1 \to -1$ } will discuss more about the reason behind this mapping.

- You should be able to convert one version to others easily.
- Some properties are conveniently explained via a particular version

Disadvantages : Random → Require large storage at both T_x & R_x

Advantages : (0) Random → unpredictable

(1) Balanced property

Consider $X_1, X_2, \ldots, X_N$

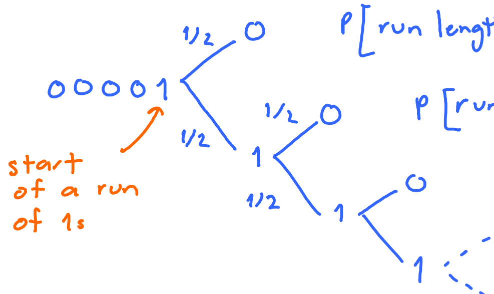
use $\{0, 1\}$ version

Fraction of 1s: $$\frac{1}{N}\sum_{i=1}^{N} X_i \xrightarrow[\text{LLN}]{N\to\infty} \mathbb{E}X_i = \frac{1}{2}$$

(2) Run length property

Run: consecutive 1s (or 0s)

Recall that long runs are undesirable



$P[\text{run length} = 1] = \frac{1}{2}$

$P[\text{run length} = 2] = \frac{1}{4}$

$$P[\text{run length} = n] = \frac{1}{2^n}$$

As n increases, $P \downarrow$

$\Rightarrow$ small probability of having long runs.

③ Shift property

Use $\{-1, 1\}$ version

$$X_1 \quad X_2 \quad X_3 \quad X_4 \quad \cdots \quad X_N$$

$\times$ multiply

shifted : $$X_{-1} \quad X_0 \quad X_1 \quad X_2 \quad \cdots \quad X_{N-2}$$

(normalized) auto correlation $$\frac{1}{N} \sum_{i=1}^{N} \underbrace{X_i X_{i-2}}_{Y_i} \xrightarrow[\text{LLN}]{N \to \infty} \mathbb{E} Y_i = 0$$

(i.i.d)

$$\therefore \sum_{i=1}^{N} X_i X_{i-2} \approx \text{small} \times N \quad (\text{"small"})$$

auto correlation when there is no shift

$$\frac{1}{N} \sum_{i=1}^{N} X_i X_{i-0} = \frac{1}{N} \sum_{i=1}^{N} X_i^2 = \frac{1}{N} \sum_{i=1}^{N} 1 = 1$$

$$\sum_{i=1}^{N} X_i X_{i-0} = N \quad (\text{"large"})$$

Ⓑ Pseudo random sequence

- $\hookrightarrow$ not random
- $\hookrightarrow$ mimick some important properties of Bernoulli trial above

$\Rightarrow$ m- sequence

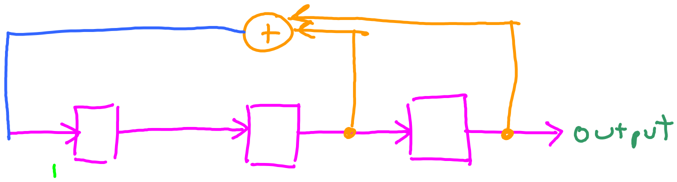
m - Sequence generator

$$q(x) = x^3 + x^2 + 1 \quad (\text{Degree} = 3)$$

r

$= 1 + 0x + 1x^2 + 1x^3$

coefficients → 1 for connection
→ 0 for no connection



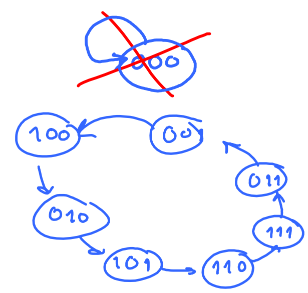
$1 + 0x + 1x^2 + 1x^3$

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

m-sequence

$\cdots 0010111 \cdots$

Complete state diagram.



Periodic with period $2^r - 1$ $\quad (2^3 - 1 = 7)$

Theorem

The three statements below are equivalent

1) Polynomial $g(x)$ generates m-sequence
2) $g(x)$ is a primitive polynomial.
3) The state diagram of the LFSR circuit generated by $g(x)$ visits all non-zero states in one cycle.

Implication

We can use ③ to test whether a polynomial $g(x)$ is primitive.

For this class, we use ③ as a definition of a primitive polynomial.

Lecture 18 (Jan 21)

Properties of m-sequence.

(5) Run length.

n = Run Length	#	fraction	
r	1	$1/2^{r-1}$	$\frac{1}{2^{n-1}},\ n=r$
$r-1$	$1 = 2^0$	$1/2^{r-1}$	
$r-2$	$1+1=2=2^1$	$2/2^{r-1} = 1/2^{r-2}$	$\frac{1}{2^n},\ n<r$
$r-3$	$2+2=4=2^2$	$2^2/2^{r-1} = 1/2^{r-3}$	
$r-4$	2^3		
$\vdots$		$\vdots$	
$r-i$	2^{i-1}		
$\vdots$	$\vdots$		
1	2^{r-2}	$2^{r-2}/2^{r-1} = 1/2$	

Total # runs $= 1 + \underbrace{2^0 + 2^1 + 2^2 + \cdots + 2^{r-2}}_{A} = 2^{r-1}$ runs.

$$A = 2^0 + 2^1 + 2^2 + \cdots + 2^{r-2}$$

$$2A = 2 + 2^2 + \cdots + 2^{r-2} + 2^{r-1}$$

$$A = 2^{r-1} - 2^0 = 2^{r-1} - 1$$

Ex $0010111 \leftarrow g(x) = x^3 + x^2 + 1$ $\leftarrow r=3$

$\underline{\underline{4}}$ runs

runs $2^{r-1} = 2^{3-1} = 2^2 = 4$ ✓