LECTURE 10

31/10/2025

COURSE PROGRAM

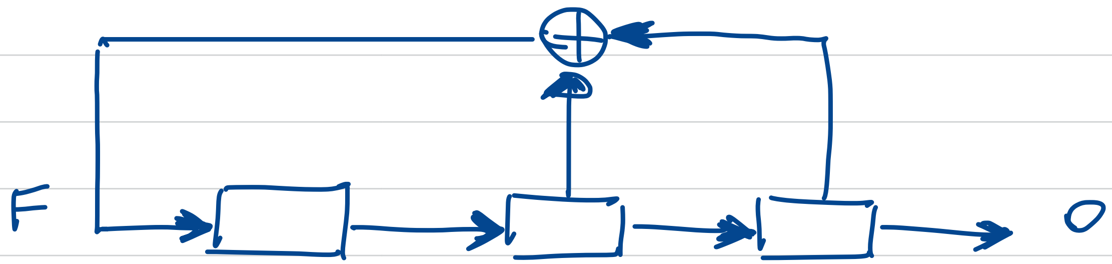
BASEBAND PROCESSING

- ERROR DETECTION
- ERROR CORRECTION
- RANDOMIZER

MODULATIONS

- RECAP ON PSK / QAM
- CHANNEL MODELS
- OFDM

- MAXIMUM PERIOD
- M- SEQUENCES
- PRIMITIVE POLYNOMIAL
- PROPERTIES OF M-SEQUENCES
- N_0 / N_1
- N_T / N_{NT}
- RUNS
- AUTOCORRELATION
- DIFFERENT INITIAL STATE



m

$2^m - 1$

STARTING SEED	F				
	0	1	0	0	
	1	0	1	0	0
	1	1	0	1	0
	1	1	1	0	1
	0	1	1	1	0
	0	0	1	1	1
	1	0	0	1	1
		1	0	0	1

- PERIODIC !
- STARTING SEED MUST BE DIFFERENT FROM 000
- A DIFFERENT STARTING SEED GENERATES A CYCLIC SHIFT OF SAME SEQUENCE

MAXIMUM PERIOD

STATE ≡ CONTENT OF m CELLS

INITIAL STATE (STARTING SEED)

MUST BE DIFFERENT FROM

ALL ZERO STATE

THE MAXIMUM PERIOD IS $2^m - 1$

(WE COVER ALL THE STATES
BUT THE ZERO ONE)

M - SEQUENCE

WHEN PERIOD N IS MAXIMUM

$$N = 2^m - 1$$

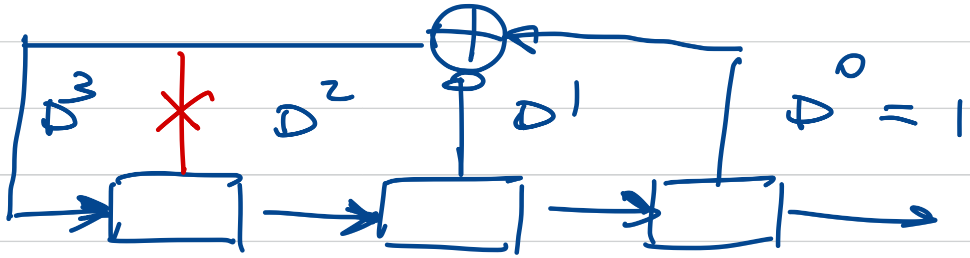
$\rightarrow$ M - SEQUENCE

$\downarrow$

MAXIMUM PERIOD

MAXIMUM LENGTH

PRIMITIVE POLYNOMIAL



$$p(D) = D^3 + D + 1$$

THE PERIOD IS MAXIMUM (M-SEQUENCE)
IFF $p(D)$ PRIMITIVE

M-SEQUENCE PROPERTIES

PERIOD $\quad N = 2^m - 1$

$N_0 / N_1 \quad N_1 = N_0 + 1$

$N_T / N_{NT} \quad N_T = N_{NT} + 1$

RUNS $\quad N_i = N_R / 2^i \quad 1 \le i \le m-1$

AUTOCORRELATION $\quad R(\tau \neq 0) = -1$

0010111

$x_0 = 3$

$x_1 = 4$

$x_1 = x_0 + 1$

$\boxed{N_0 / N_1}$

FOR ANY m - SEQUENCE

$$N_1 = N_0 + 1$$

PROOF : ASSIGNMENT 2

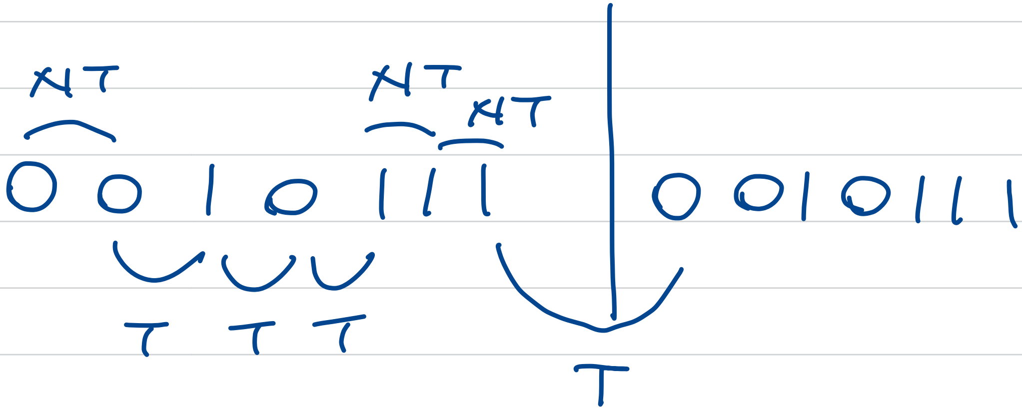
IDEAL RANDOM SEQUENCE $N_1 = N_0$

$m = 10$ $N = 2^m - 1 = 1023$

$N_1 = 512$ $N_0 = 511$

WELL BALANCED !!

$$\boxed{N_T / N_{NT}}$$



$$N_T = N_{NT} + 1$$

$\boxed{\text{RUNS}}$

IDEAL $\qquad N_i = \dfrac{N_R}{2^i}$

$$\overbrace{00}^{2}\underbrace{1}_{1}\overbrace{0}^{1}\underbrace{111}_{3} \quad \Big| \quad 0010111$$

$N_R = 4$

$N_1 = 2 \qquad\qquad N_1(0) = N_1(1) = 1$

$N_2 = 1$

$N_3 = 1$

THE PROPERTY $N_i = \frac{N_R}{2^i}$

IS VERIFIED ONLY

FOR $i = 1, 2, \ldots, m-1$

THEN THERE IS A RUN (OF ONES)

OF LENGTH m

$\longrightarrow$ ASSIGNMENT 2

NO LONGER RUNS

GOOD PROPERTY!

NO LONG RUNS → GOOD FOR PRACTICAL APPLICATIONS

AUTO · CORRELATION

$$R(\tau) = \sum_{i=1}^{N} v'(i)\, v'(i-\tau)$$

$\underline{v}$ 0010111

$\underline{v}'$ $-1 \quad -1 \quad +1 \quad -1 \quad +1 \quad +1 \quad +1$

$\tau = 1$ $+1 \quad -1 \quad -1 \quad +1 \quad -1 \quad +1 \quad +1$

$-1 \quad +1 \quad -1 \quad -1 \quad -1 \quad +1 \quad +1 \quad = \quad -1$

FOR ANY M. SEQUENCE

$$R(z=0) = N$$

$$R(z \neq 0) = -1$$

(IT'S IMPOSSIBLE TO OBTAIN 0 BECAUSE N IS ODD)

ASSIGNMENT 2 : PROOF

HINT 1 LINEARITY

HINT 2 R d_H

IMPORTANT

$\boxed{\text{DIFFERENT INITIAL STATE}}$

NOTE: IF WE CHANGE THE INITIAL STATE WE OBTAIN A CYCLIC SHIFT OF SAME M. SEQUENCE

→ ALL M. SEQ. PROPERTIES DO NOT DEPEND ON THE INITIAL STATE

SUMMARY

M. SEQUENCES HAVE VERY GOOD PROPERTIES IN TERMS OF RANDOMNESS

- N_0 / N_1
- N_T / N_{NT}
- RUNS
- AUTOCORRELATION

FOR THIS REASON →

USED BY MOST COMMUNICATION SYSTEMS

PROBLEM:

ALL THIS GOOD PROPERTIES

ARE VERYFIED IFF

WE USE ENTIRE M. SEQUENCE

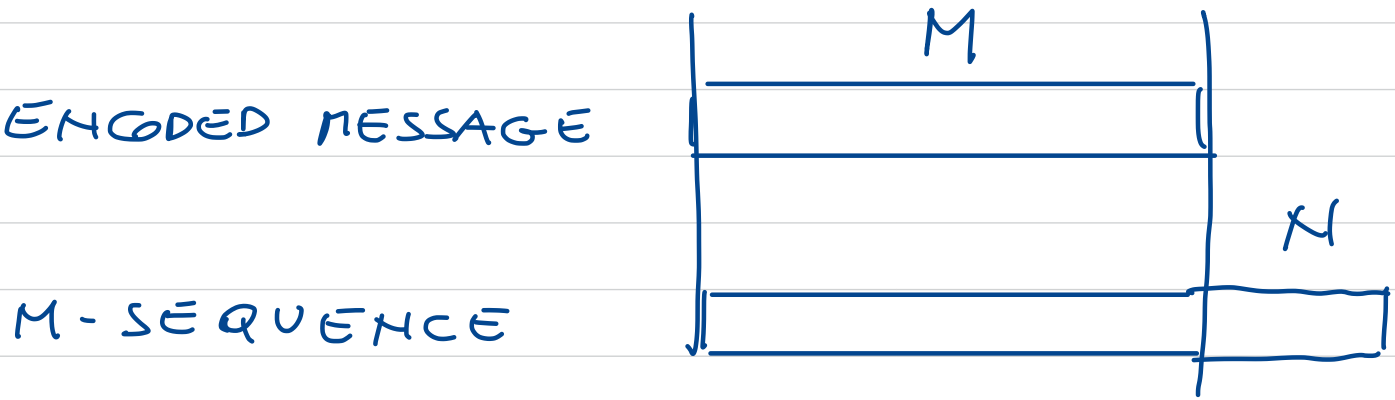
WITH LENGTH N

WE (BINARY SUM)

THE ENCODED MESSAGE

TO BE TRANSMITTED

AND THE RANDOMIZER SEQUENCE



IF $M < N$ WE ONLY USE A PORTION

OF THE M-SEQUENCE

"TRUNCATION"

TRUNCATION

UNFORTUNATELY TRUNCATED M-SEQUENCES LOSE MOST OF THE GOOD PROPERTIES OF ENTIRE M-SEQUENCES

→ ASSIGNMENT 2

CROSS - CORRELATION

WE COMPARE TWO DIFFERENT

BINARY SEQUENCES

$\underline{v} \rightarrow \underline{v}'$

$\underline{w} \rightarrow \underline{w}'$

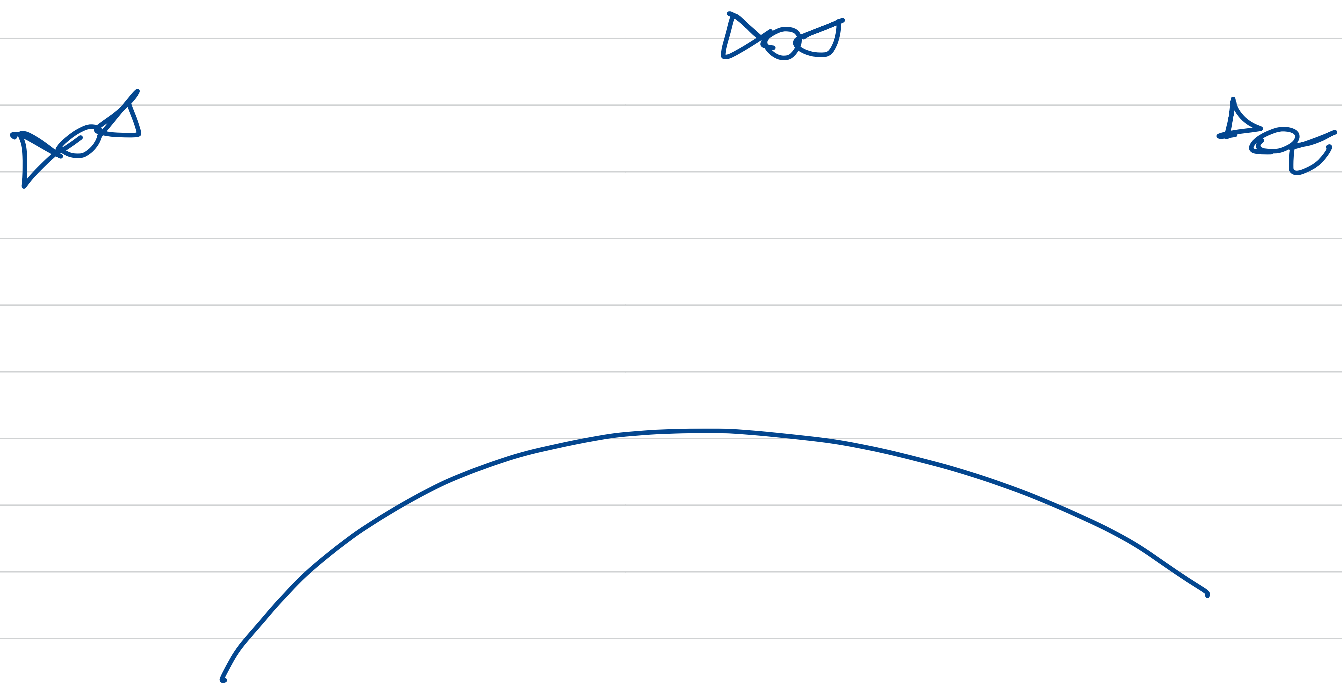
$$R(\tau) = \sum_{i=1}^{N} v'(i)\, w'(i-\tau)$$

THERE IS AN APPLICATION

WHERE CROSS-CORRELATION

IS FUNDAMENTAL

C	D	M	A
O	I	U	C
D	V	L	C
E	I	T	E
	S	I	S
	I	P	S
	O	L	
	N	E	



GPS: TO EACH SATELLITE WE ASSIGN
A BINARY SEQUENCE (CODE)
IF THEIR CROSS-CORRELATION IS
SMALL → LOW INTERFERENCE
THEY CAN TRANSMIT AT THE SAME TIME
ON THE SAME BAND → CDMA

M. SEQUENCES

HAVE GOOD PROPERTIES IN TERMS OF AUTO. CORRELATION

BUT POOR PROPERTIES IN TERMS OF CROSS. CORRELATION

→ ASSIGNMENT 2

GOLD CODES

GOLD SEQUENCES ARE
OBTAINED BY SUMMING
TWO M · SEQUENCES
WITH SAME LENGTH N
GENERATED BY DIFFERENT
PRIMITIVE POLYNOMIALS

GOLD CODES HAVE
VERY GOOD PROPERTIES
FOR CROSS-CORRELATION
(VERY CLOSE TO IDEAL BOUNDS)

→ VERY POPULAR FOR CDMA

→ IN PARTICULAR

GNSS → E.G. GPS

G	N	S	S
C	A	A	Y
O	V	T	S
B	I	E	T
A	G	L	E
L	A	L	M
	T	I	S
	I	T	
	O	E	
	N		

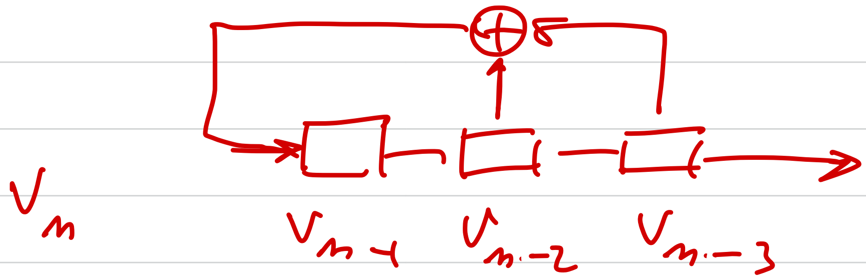
ASSIGNMENT 2

PROVE THAT THE FOR AN
M-SEQUENCE THE POLYNOMIAL MUST BE
PRIMITIVE

NOT FOR FINAL EXAM

DO NOT TRANSLATE THESE
RED SLIDES INTO BEAMER

1. LFSR AND LINEAR RECURRENCE SEQUENCES



$$V_n = V_{n-2} \oplus V_{n-3}$$

LINEAR RECURRENCE SEQUENCE

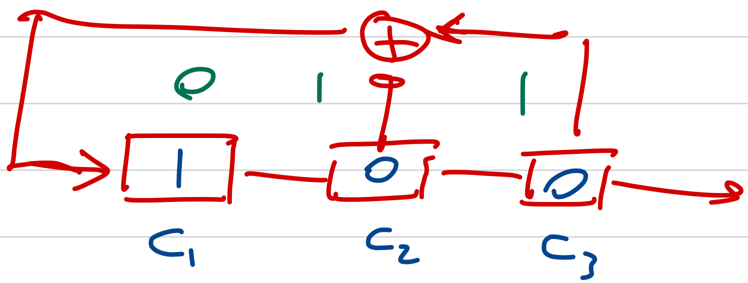
BINARY SUM

INTEGER SUM

$$U_n = U_{n-1} + U_{n-2}$$

→ FIBONACCI SEQUENCE

2. LFSR AND MATRIX DESCRIPTION



$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} c_2 + c_3 \\ c_1 \\ c_2 \end{bmatrix}$$

FEEDBACK CONNECTIONS →

$$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{array}{c} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \end{array} \begin{array}{l} c_1 \\ c_2 \\ c_3 \end{array} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$$

IDENTITY | CURRENT STATE | NEXT STATE

COLUMN MULTIPLICATION $\equiv$ LFSR STATE EVOLUTION

$$\begin{bmatrix}1\\0\\0\end{bmatrix} \to \begin{bmatrix}0\\1\\0\end{bmatrix} \to \begin{bmatrix}1\\0\\1\end{bmatrix} \to \begin{bmatrix}1\\1\\0\end{bmatrix} \to \begin{bmatrix}1\\1\\1\end{bmatrix} \to \begin{bmatrix}0\\1\\1\end{bmatrix} \to \begin{bmatrix}0\\0\\1\end{bmatrix} \to \begin{bmatrix}1\\0\\0\end{bmatrix}$$

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

WE HAVE $G^N = I$

FOR $N = 2^m - 1$

3. LFSR AND POLYNOMIAL MULTIPLICATION

WE TAKE THE SAME MATRIX

$$G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

AND WE CONSIDER ROW MULTIPLICATION

$$(0\,0\,1) \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = (0\,1\,0)$$

ROW MULTIPLICATION CORRESPONDS TO THIS POLYNOMIAL MULTIPLICATION:

$$\boxed{p(D) \cdot D \mod g(D)}$$

$\leftarrow$ LFSR POLYNOMIAL

$$p(D) = p_2 D^2 + p_1 D^1 + p_0 \equiv (p_2\ p_1\ p_0)$$

$$g(D) = D^3 + D + 1 \qquad G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$[1] \cdot D \mod g(D) = D$

$[D] \cdot D \mod g(D) = D^2$

$[D^2] \cdot D \mod g(D) = D+1$

$[D+1] \cdot D \mod g(D) = D^2+D$

$[D^2+D] \cdot D \mod g(D) = D^2+D+1$

$[D^2+D+1] \cdot D \mod g(D) = D^2+1$

$[D^2+1] \cdot D \mod g(D) = 1$

WE HAVE

$$p(D) \cdot D^N = p(D) \mod g(D) \text{ FOR } N = 2^m - 1$$

$(001) \cdot G = (010)$

$(010) \cdot G = (100)$

$(100) \cdot G = (011)$

$(011) \cdot G = (110)$

$(110) \cdot G = (111)$

$(111) \cdot G = (101)$

$(101) \cdot G = (001)$

THIS CONFIRMS THAT

$$G^N = I \text{ FOR } N = 2^m - 1$$

SINCE WE HAVE

$$p(D)\cdot D^N = p(D) \mod g(D)$$

$$p(D)\cdot(D^N+1) = 0 \mod g(D)$$

$g(D)$ DIVIDES D^N+1

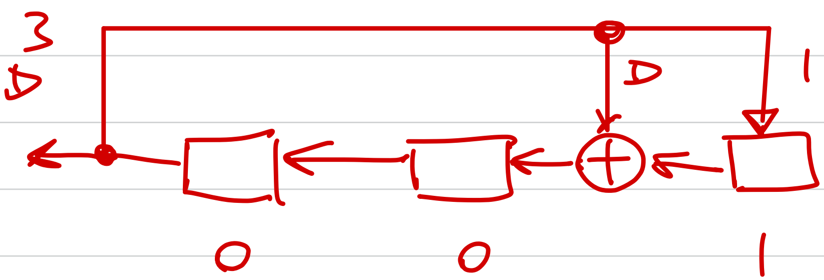
FOR $N = 2^m - 1$

(AND NOT LESS)

$\rightarrow$ $g(D)$ MUST BE A $\boxed{\text{PRIMITIVE POLYNOMIAL}}$

4. LFSR AND GALOIS IMPLEMENTATION

IT IS INTERESTING TO NOTE THAT THE ROW MULTIPLICATION CAN BE OBTAINED WITH THIS LFSR STRUCTURE CALLED GALOIS IMPLEMENTATION (THE USUAL ONE IS CALLED FIBONACCI IMPLEMENTATION)



0 0 1
0 1 0
1 0 0
0 1 1
1 1 0
1 1 1
1 0 1
0 0 1