ECS455: Chapter 4

Multiple Access

4.4 m-sequence

Dr.Prapun Suksompong prapun.com/ecs455 BKD, 6th floor of Sirindhralai buildingTuesday14:20-15:20Wednesday14:20-15:20Friday9:15-10:15

Office Hours:

Binary Random Sequences

- While DSSS chip sequences must be generated *deterministically*, properties of binary random sequences are useful to gain insight into deterministic sequence design.
- A random binary chip sequences consists of i.i.d. bit values with probability one half for a one or a zero.
 - Also known as Bernoulli sequences/trials, "coin-flipping" sequences
- A random sequence of length *N* can be generated, for example, by flipping a fair coin *N* times and then setting the bit to a one for heads and a zero for tails.

Binary Random Sequence

	X.4	X3	X2	X.1	X.0	\mathbf{X}_1	X_2	X_3	X_4
Coin-flipping sequence	Н	Н	Т	Н	Н	Т	Н	Т	Т
Bernoulli trials/sequence	1	1	0	1	1	0	1	0	0
nary (indp.) random sequence	-1	-1	1	-1	-1	1	-1	1	1
Waveform									
waveform -									

- These names are simply many versions of the same sequence/process.
- You should be able to convert one version to others easily.
- Some properties are conveniently explained when the sequence is expressed in a particular version.

Properties of Binary Random Sequences:

- Consider the sequence $X_1, X_2, X_3, \ldots, X_n, \ldots$
- Disadvantages
 - Can not further "compress" the sequence
 - Difficult to convey the sequence from the Tx to Rx
 - Require large storage at both Tx and Rx
- Advantages
 - Random = unpredictable
 - 1. Balanced property
 - 2. Run length property
 - 3. Shift property

Properties of Binary Random Sequences: Balanced Property

• {0,1} version

$$\frac{1}{N} \sum_{i=1}^{N} X_i \xrightarrow{N \to \infty} \mathbb{E} \left[X_i \right] = 0 \times \frac{1}{2} + 1 \times \frac{1}{2} = \frac{1}{2}$$

• $\{\pm 1\}$ version

$$\frac{1}{N} \sum_{i=1}^{N} X_i \xrightarrow{N \to \infty} \mathbb{E} \left[X_i \right] = \left(-1 \right) \times \frac{1}{2} + 1 \times \frac{1}{2} = 0$$

Runs: An Example

- A run is a subsequence of consecutive identical symbols within the sequence.
- The following sequence contains 16 runs

0001111100110100100001010111011

$\overline{\nabla}$	$\overline{\}$			• Rel. Freq	of Runs
	∖A ru	n of 1s (len	gth = 5)	11111	1/16
\	A run o	f 0s (length	= 3)	0000	1/16
	mon of Du	n I on ctl		111	1/16
Kel. r	req of Ku	n Lengu	115	000	1/16
	Run Length	Rel. Freq.		11	2/16
	4	1/16		00	2/16
	3	2/16		1	4/16
	2	4/16		0	4/16
	1	8/16		0	17 10



FYI: Run-Length Encoding (RLE)

- A very simple form of lossless data compression in which runs of data (that is, sequences in which the same data value occurs in many consecutive data elements) are stored as a single data value and count, rather than as the original run.
- Most useful on data that contains many such runs.
- Example: Consider a screen containing plain black text on a solid white background.

A line, with B representing a black pixel and W representing white, might read as follows:

Properties of Binary Random Sequences: Shift Property

Original sequence: $X_1 \quad X_2 \quad X_3 \quad X_4 \quad \cdots \quad X_N$

Shifted sequence: X_{-1} X_0 X_1 X_2 \cdots X_{N-2} (amount of shift (delay) = 2)

- When the shifted amount = 0, the two sequences are exactly the same.
- When the shifted amount = s, we want to compare X_i and X_{i-s}.
 - What proportion are the same?
 - What proportion are different?
- Recall that the numbers in the sequence are independent results (from several Bernoulli trials)

X_{j-s}	bility
0	1⁄4
1	1⁄4
0	1/4
1	1/4
	X _{j-s} 0 1 0 1

Properties of Binary Random Sequences: Shift Property

- $\{0,1\}$ version: The comparison is done via the XOR (\bigoplus) operation
 - $x \oplus y = 0$ iff they are the same
 - $x \oplus y = 1$ iff they are different
- $\{\pm 1\}$ version: The comparison is done via the multiplication operation
 - $x \times y = 1$ iff they are the same
 - $x \times y = -1$ iff they are different

Key randomness properties

[Golomb, 1967][Viterbi, 1995, p. 12] Binary random sequences with length *N* asymptotically large have a number of the properties desired in spreading codes

- **Balanced property**: Equal number of ones and zeros.
 - Should have no DC component to avoid a spectral spike at DC or biasing the noise in despreading
- Run length property: The run length is generally short.
 - half of all runs are of length 1
 - a fraction $1/2^n$ of all runs are of length n (Geometric)
 - Long runs reduce the BW spreading and its advantages
- **Shift property**: If they are shifted by any nonzero number of elements, the resulting sequence will have half its elements the same as in the original sequence, and half its elements different from the original sequence.

35

[Goldsmith,2005, p. 387 & Viterbi, p. 12]

Pseudorandom Sequence

- A deterministic sequence that has the balanced, run length, and shift properties as it grows *asymptotically large* is referred to as a **pseudorandom sequence** (noiselike or pseudonoise (PN) signal).
- Ideally, one would prefer a random binary sequence as the spreading sequence.
- However, practical synchronization requirements in the receiver force one to use **periodic** Pseudorandom binary sequences.
- m-sequences

• Quaternary sequences

- Gold codes
- Kasami sequences

• Walsh functions

m-Sequences

• Maximal-length sequences

Longer name: Maximal length linear shift register sequence.

- A type of **cyclic code**
 - Generated and characterized by a generator polynomial
 - Properties can be derived using algebraic coding theory
- Simple to generate with linear feedback shift-register (LFSR) circuits
 - Automated
- Approximate a random binary sequence.
- Disadvantage: Relatively easy to intercept and regenerate by an unintended receiver [Ziemer, 2007, p 11]

GF(2)

- Galois field (finite field) of two elements
- Consist of
 - the symbols 0 and 1 and
 - the (binary) operations of
 - modulo-2 addition (XOR) and
 - modulo-2 multiplication.
- The operations are defined by

+	0	1			0	1
0	0	1	-	0	0	0
1	1	0		1	0	1

4(

Linear Feedback Shift-Register (LFSR)

- Binary sequences drawn from the alphabet $\{0,1\}$ are shifted through the shift register in response to clock pulses.
 - Each clock time, the register shifts all its contents to the right.
- The particular 1s and 0s occupying the shift register stages after a clock pulse are called **states**.



Linear Feedback Shift-Register (LFSR)

- All the values are in GF(2) which means they can only be 0 or 1.
- The value of g_i determines whether the output of the k^{th} FF will be in the sum that produce the feedback bit.
 - 1 signifies closed or a connection and
 - 0 signifies open or no connection.
- Ex. Suppose $g_1 = 0$, $g_2 = 1$, $g_3 = 1$ in our LFSR.



(See Section 13.4.1 in [Lathi, 1998]) **M-Sequence generator (1)** • Start with a "**primitive polynomial**" • $g(x) = g_0 + g_1 x + g_2 x^2 + \dots + g_r x^r$ • r = degree of the polynomial • Use r flip-flops.

- The feedback taps in the feedback shift register are selected to correspond to the coefficients of the primitive polynomial.
- Ex. $g(x) = 1 + x^2 + x^3$ is a primitive polynomial. = $1 + 0x + 1x^2 + 1x^3$

(Degree: $r = 3 \rightarrow$ use 3 flip-flops)



m-sequence generator (2)

- We start with state 100.
 - You may choose different non-zero state.
 - Note that if we start with 000, we won't go anywhere.



- Any polynomial generates periodic sequence.
 - The maximum period is $2^r 1$.
- In this example, the state cycles through all $2^3 1 = 7$ non-zero states.





Primitive Polynomial

- Definition: A LFSR **generates an m-sequence** if and only if (starting with any nonzero state,) it visits all possible nonzero states (in one cycle).
- Technically, one can define primitive polynomial using concepts from finite field theory.
- Fact: A polynomial generates m-sequence if and only if it is a primitive polynomial.
 - Therefore, we use this fact to define primitive polynomial.
- For us, a polynomial is **primitive** if **the corresponding LFSR circuit generates m-sequence**.

Sample Exam Question

Draw the complete **state diagrams** for linear feedback shift registers (LFSRs) using the following polynomials. Does either LFSR generate an m-sequence?

1.
$$g(x) = 1 + x^2 + x^3$$

2.
$$g(x) = 1 + x + x^2 + x^3$$

46

Solution (1)

Draw the complete **state diagrams** for linear feedback shift registers (LFSRs) using the following polynomials.

Does either LFSR generate an m-sequence?

1. $g(x) = 1 + x^2 + x^3$



The corresponding LFSR generates an msequence because the state diagram contains a cycle that visits all possible nonzero states. We can also conclude that $g(x) = 1 + x^2 + x^3$ is a primitive polynomial.

Solution (2)

 $g(x) = 1 + x + x^2 + x^3$

48

m-Sequences: More properties

- 1. The contents of the shift register will cycle over all possible 2^{*r*}-1 nonzero states before repeating.
- 2. Contain one more 1 than 0 (Slightly unbalanced)
- 3. Shift-and-add property: Sum of two (cyclic-)shifted m-sequences is another (cyclic-)shift of the same m-sequence
- 4. If a window of width *r* is slid along an m-sequence for $N = 2^{r}-1$ shifts, each *r*-tuple except the all-zeros r-tuple will appear exactly once
- 5. For any m-sequence, there are
 - One run of ones of length *r*
 - One run of zeros of length *r*-1
 - One run of ones and one run of zeroes of length r-2
 - Two runs of ones and two runs of zeros of length r-3
 - Four runs of ones and four runs of zeros of length r-4
 - ...
 - + 2^{r-3} runs of ones and 2^{r-3} runs of zeros of length 1



m-Sequences: More Properties

- 3. Shift-and-add property: Sum of two (cyclic-)shifted msequences is another (cyclic-)shift of the same m-sequence
- 4. If a window of width *r* is slid along an m-sequence for $N = 2^r \cdot 1$ shifts, each *r*-tuple except the all-zeros r-tuple will appear exactly once

m-Sequences: Another Example

- $2^{5}-1 = 31$ -chip m-sequence
- The following sequence contains 16 runs

0001111100110100100001010111011

• Rel. Freq of Runs 11111 1/16• Rel. Freq of Run Lengths 0000 1/16Run Length Rel. Freq. 1/16111 5 1/16 000 1/164 1/16 2/162/16 11 3 2 4/16 00 2/168/16 4/164/160 [S.W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, 1967.]

(Time) Autocorrelation Function for Energy Sequence



(Time) Autocorrelation Function for Energy Sequence





MATLAB: xcorr

- r = xcorr(x,y)
 - Return the cross-correlation of two discrete-time sequences, x and y.
 - If x and y have different lengths, the function appends zeros at the end of the shorter vector so it has the same length as the other.
 - The lag (τ) is varied from -(N-1) to (N-1) where N is the longer length of the two sequences.
- [r,lags] = xcorr(____)
 - Also returns vector with the lags (*t*) at which the correlations are computed.



(Time) Autocorrelation Function for Power and Periodic Sequence









m-Sequences: Autocorrelation function



Back to m-Sequences



m-Sequences: Autocorrelation function



Autocorrelation Function for Periodic **Binary Random Sequence**

Consider a periodic sequence whose one period is given by 1 -1 -1 1 -1 1 1 -1 -1] [-1



Autocorrelation Function for Periodic **Binary Random Sequence**

Consider a periodic sequence whose one period is given by 1-2*randi([0 1],1,100000)



Autocorrelation and PSD • (Normalized) autocorrelations of maximal sequence and random binary sequence. - maximal - - - - random binary



References: m-sequences



- Karim and Sarraf, W-CDMA and cdma2000 for 3G Mobile Networks, 2002.
 - Page 84-90
- Viterbi, CDMA: Principles of Spread Spectrum Communication, 1995
 - Chapter 1 and 2
- Goldsmith, Wireless Communications, 2005
 - Chapter 13
- Tse and Viswanath, *Fundamentals of* Wireless Communication, 2005
 - Section 3.4.3



[TK5103.452 K37 2002]



[TK5103.45V57 1995]





Wattph	e Access
4.4 m-se	equence
(Additiona	l Remarks)
	Office Hours: BKD 6th floor of Sirindhralai building
	Tuesday 14:20-15:20
	Wednesday 14:20-15:20
Dr. Prapun Suksompong	





Example: (Time) Autocorrelation Function for Periodic Sequence





Wireless Comm. and Multipath Fading



Wireless Comm. and Multipath Fading



