AI 5090: STOCHASTIC PROCESSES

LECTURE 15

SCRIBE: ADHITH T & MADINE KARTHIKEYA VARMA

25 FEBRUARY 2025

Contents

---

1 Recap

1.1 Binary Pseudo Random Number Generator

Pseduo Random Number Generator although seemingly random, is actually produced by a deterministic algorithm (as seen in the previous lecture). Binary PRNG produces pseduo random sequence of usually two values (0,1 generally). In order to obtain a better random sequence we increase the value of the period (N) to a higher value.

2 m-Sequences

Maximal period binary sequences generated by a Linear Feedback Shift Registers (LFSR) are called m-sequences. In m-sequences the number of zeroes and the numbers of ones are approximately equal.

2.1 Example

For $N = 4$, set the tap gains as:

$$(g_0, g_1, g_2, g_3, g_4) = (1, 0, 0, 1, 1) = (23)_8.$$

This setting gives us the maximum possible periodic binary sequence in 4-Stage Binary Linear Feedback Shift Register. Any other tap gain may not give the maximum possible periodic sequence.

2.2 Properties of m-Sequences

- **Period**: They are periodic with period $2^N - 1$.
- **Balanced Distribution**: Contain approximately equal number of ones and zeros in any one period.
- **Autocorrelation Property**: Autocorrelation function is nearly identical to that of IID Ber(0.5) process. Indeed, suppose $X_1, X_2, \cdots$ for $x \in [0, 5]$. Then,

$$M_X(t) = 0.5, \quad R_X(s,t) = E[X_s X_t] = \begin{cases} \frac{1}{2}, & s = t, \\ \frac{1}{4}, & s \neq t. \end{cases}$$

Given a discrete-time signal $\{x[n]\}_{n=0}^{\infty}$ with period N, its autocorrelation is given by

$$R_X[k] = \frac{1}{N} \sum_{n=0}^{N-1} x[n] x[n+k], \quad k \in \{0, 1, 2, \ldots\}.$$

Considering the single period output $(1,1,1,1,0,0,0,1,0,0,1,1,0,1,0)$, we have

$$R_X[k] = \begin{cases} \frac{8}{15}, & k = 0, \\ \frac{4}{15}, & 1 \leq k \leq 14, \end{cases} \qquad R_X[k+15] = R_X[k].$$

3 Generating non-binary m-sequences

3.1 Power Residue Method

Here we are going to discuss about a specific method for this called **power residue method**.
Given numbers (a, x_0, p), let

$$x_n = a \cdot x_{n-1} \mod p$$

where

- p is typically a large prime number. For instance, $p = 2^{31} - 1$ (an instance of a *Mersenne prime* number).
- $x_0 \neq 0$ is called seed value.
  Python and other programs use the computer's internal time to generate this seed value (if seed is not explicitly specified).
- $a \neq 1$ is called multiplicative factor.

Due to mod p, $x_n \in \{1, \ldots, p-1\}$ for all n. Furthermore, x_n will always be periodic, with a maximal period of $p - 1$.
Choice of (a, p) is crucial for obtaining m-sequence.

3.2 Examples

- If $(a, p) = (4, 7)$, then the output sequence (with $x_0 = 1$) is:

$$\begin{aligned} x_1 &= 4 \times 1 \mod 7 = 4, \\ x_2 &= 4 \times 4 \mod 7 = 2, \\ x_3 &= 4 \times 2 \mod 7 = 1, \\ x_4 &= 4 \times 1 \mod 7 = 4, \\ x_5 &= 4 \times 4 \mod 7 = 2. \end{aligned}$$

  Hence, the sequence is $(1, 4, 2, 1, 4, 2, \ldots)$. Notice that the period of this sequence is 3, which is smaller than the maximal possible period of $p - 1 = 6$.

- If $(a, p) = (3, 7)$, then the output sequence (with $x_0 = 1$) is:

$$\begin{aligned}
x_1 &= 3 \times 1 \mod 7 = 3, \\
x_2 &= 3 \times 3 \mod 7 = 2, \\
x_3 &= 3 \times 2 \mod 7 = 6, \\
x_4 &= 3 \times 6 \mod 7 = 4, \\
x_5 &= 3 \times 4 \mod 7 = 5, \\
x_6 &= 3 \times 5 \mod 7 = 1.
\end{aligned}$$

  Hence, the sequence is $(1, 3, 2, 6, 4, 5, 1, 3, 2, \ldots)$. Notice that the period of this sequence is $p - 1 = 6$.

- Most programming languages use $a = 7^5$ and $p = 2^{31} - 1$.

4 σ-Algebra Generated by a Random Variable

In this section, we will review the concept of σ-algebra generated by a random variable. In essence, this σ-algebra is the smallest σ-algebra with respect to which a given random variable will continue to remain a random variable.

Definition 1 (σ-Algebra Generated by a Random Variable)**.** *Fix a measurable space $(\Omega, \mathscr{F})$.*
Let $X : \Omega \to \mathbb{R}$ be a random variable with respect to $\mathscr{F}$.
The σ-algebra generated by X, denoted $\sigma(X)$, is defined as:

$$\sigma(X) := \left\{ A \in \mathscr{F} : A = X^{-1}(B) \text{ for some } B \in \mathscr{B}(\mathbb{R}) \right\}.$$

- The σ-algebra $\sigma(X)$ is the smallest σ-algebra on Ω that makes X measurable.
- The structure of $\sigma(X)$ is closely related to the Borel σ-algebra $\mathscr{B}(\mathbb{R})$ on $\mathbb{R}$.

Example

Consider the following example:

$$\Omega = \{1, \ldots, 6\}, \qquad \mathscr{F} = 2^{\Omega} = \text{power set of } \Omega.$$

Define a function $X : \Omega \to \mathbb{R}$ as follows:

$$X(\omega) = \begin{cases} 0, & \omega = 1, 2, \\ 4, & \omega = 5, 6, \\ 6, & \omega = 3, 4. \end{cases}$$

We then readily observe that

$$X^{-1}(-\infty, x] = \begin{cases} \emptyset, & x < 0, \\ \{1, 2\}, & 0 \le x < 4, \\ \{1, 2, 5, 6\}, & 4 \le x < 6, \\ \Omega, & x \ge 6. \end{cases}$$

Furthermore, we note that

$$X^{-1}(\{x\}) = \begin{cases} \{1, 2\}, & x = 0, \\ \{3, 4\}, & x = 6, \\ \{5, 6\}, & x = 4, \\ \emptyset, & x \notin \{0, 4, 6\}. \end{cases}$$

Combining the above observations, we have

$$\sigma(X) = \Big\{ \emptyset, \Omega, \{1, 2\}, \{3, 4\}, \{5, 6\}, \{1, 2, 3, 4\}, \{3, 4, 5, 6\}, \{1, 2, 5, 6\} \Big\}.$$

4.1 σ-Algebra Generated by a Random Vector

The above definition for the σ-algebra generated by a random variable may be extended naturally to random vectors as follows.

Definition 2 (σ-Algebra Generated by a Random Vector)**.** *Fix a measurable space $(\Omega, \mathscr{F})$ and $n \in \mathbb{N}$.*
Let $(X_1, \ldots, X_n) : \Omega \to \mathbb{R}^n$ be a random vector with respect to $\mathscr{F}$.
The σ-algebra generated by $(X_1, \ldots, X_n)$, denoted $\sigma(X_1, \ldots, X_n)$, is defined as:

$$\sigma(X_1, \ldots, X_n) := \left\{A \in \mathscr{F} : A = (X_1, \ldots, X_n)^{-1}(B) \text{ for some } B \in \mathscr{B}(\mathbb{R}^n)\right\}.$$

5 Filtrations

The idea of filtrations plays a crucial role in the study of stochastic processes. Formally, a filtration is a non-decreasing collection of σ-algebras, and is defined below.

Definition 3 (Filtration)**.** *Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$. Let $\mathcal{T}$ be an ordered index set.*
A collection of σ-algebras $\mathcal{G}_\bullet = \{\mathcal{G}_t : t \in \mathcal{T}\}$ such that $\mathcal{G}_t \subseteq \mathscr{F}$ for all $t \in \mathcal{T}$ is called a **filtration** *if*

$$\mathcal{G}_s \subseteq \mathcal{G}_t, \quad \forall s \leq t.$$

Suppose that $\{X_t : t \in \mathcal{T}\}$ is a stochastic process defined with respect to $\mathscr{F}$. Then, the **natural filtration** associated with the process $\{X_t\}_{t \in \mathcal{T}}$ is given by

$$\mathcal{G}_t = \sigma(X_s : s \leq t), \qquad t \in \mathcal{T}.$$

The concept of filtrations is closely associated with that of *stopping times*, defined next.

6 Stopping Times

Definition 4 (Stopping Time)**.** *Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$. Let $\mathcal{T}$ be an ordered index set. Fix a filtration $\mathcal{G}_\bullet = \{\mathcal{G}_t : t \in \mathcal{T}\}$. A random variable $\tau : \Omega \to \mathcal{T} \cup \{+\infty\}$ is called a* **stopping time** *with respect to the filtration $\mathcal{G}_\bullet$ if*

$$P(\tau < \infty) = 1,$$

and for each $t \in \mathcal{T}$, the event

$$\{\tau \leq t\} \in \mathcal{G}_t.$$

Simply put, the latter condition above dictates that the answer to the question "Is the value of τ lesser than or equal to t?" may be determined by simply looking at the process up to (and including) time t.

Example 1. *Let $\{X_t\}_{t \in \mathcal{T}}$ be a stochastic process. Define τ as the first time X_t exceeds a threshold a, i.e.,*

$$\tau := \inf\{t \in \mathcal{T} : X_t \geq a\}.$$

Then, we observe that for every $t \in \mathcal{T}$,

$$\{\tau \leq t\} = \{\exists s \leq t, X_s \geq a\} \in \mathcal{G}_t.$$

Therefore, under the additional condition that $\mathbb{P}(\tau < +\infty) = 1$, it follows that τ as defined above is a stopping time with respect to the natural filtration of the process $\{X_t\}_{t \in \mathcal{T}}$.