भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Stochastic Processes

IID Processes, Examples (Random Walk, Gaussian Process), Binary Pseudo-Random Number Generators

Karthik P. N.
Assistant Professor, Department of AI
Email: pnkarthik@ai.iith.ac.in

21 February 2025

Recap – Mean, Autocorrelation, and Autocovariance

Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$.
Let $\{X_t : t \in \mathcal{T}\}$ be a random process defined w.r.t. $\mathscr{F}$.

Definition (Mean, Autocorrelation, Autocovariance)

- The mean of the process $\{X_t : t \in \mathcal{T}\}$ is a function $M_X : \mathcal{T} \to [-\infty, +\infty]$ defined as

$$M_X(t) = \mathbb{E}[X_t], \qquad t \in \mathcal{T}.$$

- The autocorrelation and autocovariance of the process $\{X_t : t \in \mathcal{T}\}$ are functions $R_X, C_X : \mathcal{T} \times \mathcal{T} \to [-\infty, +\infty]$, defined as

$$R_X(t,s) = \mathbb{E}[X_t X_s], \qquad C_X(t,s) = \mathrm{Cov}(X_t, X_s), \qquad t, s \in \mathcal{T}.$$

Stationary Process

Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$.
Let $\{X_t : t \in \mathbb{R}_+\}$ be a random process defined w.r.t. $\mathscr{F}$.

Definition (Stationary Process)

$\{X_t : t \geq 0\}$ is said to be (strictly) stationary if all FDDs are translation invariant, i.e., for any $n \in \mathbb{N}$, $\mathbf{t} \in \mathbb{R}_+^n$, and $h \in \mathbb{R}_+$,

$$F_{\mathbf{t}} = F_{\mathbf{t}+h}.$$

Here, $\mathbf{t} + h$ is a vector with each coordinate incremented by h with respect to the corresponding coordinate in $\mathbf{t}$.

Weakly Stationary Process

Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$.

Let $\{X_t : t \in \mathbb{R}_+\}$ be a random process defined w.r.t. $\mathscr{F}$.

Definition (Stationary Process)

$\{X_t : t \in \mathbb{R}_+\}$ is said to be weakly stationary (or wide-sense stationary) if for all $t_1, t_2 \in \mathbb{R}_+$ and $h \in \mathbb{R}_+$:

1. $M_X(t_1) = M_X(t_2)$.
2. $C_X(t_1, t_2) = C_X(t_1 + h, t_2 + h)$.

Weakly Stationary Process

Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$.

Let $\{X_t : t \in \mathbb{R}_+\}$ be a random process defined w.r.t. $\mathscr{F}$.

Definition (Stationary Process)

$\{X_t : t \in \mathbb{R}_+\}$ is said to be weakly stationary (or wide-sense stationary) if for all $t_1, t_2 \in \mathbb{R}_+$ and $h \in \mathbb{R}_+$:

1. $M_X(t_1) = M_X(t_2)$.
2. $C_X(t_1, t_2) = C_X(t_1 + h, t_2 + h)$.

Remarks:

- A process is weakly stationary iff it has constant mean, and $C_X(t, t+h) = C_X(0, h)$ for all $t, h \in \mathbb{R}_+$ (proof: exercise!)

Weakly Stationary Process

Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$.
Let $\{X_t : t \in \mathbb{R}_+\}$ be a random process defined w.r.t. $\mathscr{F}$.

Definition (Stationary Process)

$\{X_t : t \in \mathbb{R}_+\}$ is said to be weakly stationary (or wide-sense stationary) if for all $t_1, t_2 \in \mathbb{R}_+$ and $h \in \mathbb{R}_+$:

1. $M_X(t_1) = M_X(t_2)$.
2. $C_X(t_1, t_2) = C_X(t_1 + h, t_2 + h)$.

Remarks:

- A process is weakly stationary iff it has constant mean, and $C_X(t, t+h) = C_X(0, h)$ for all $t, h \in \mathbb{R}_+$ (proof: exercise!)
- Every stationary process with finite variance is wide-sense stationary (proof: exercise!)

IID Process

Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$.
Let $\{X_t : t \in \mathbb{R}_+\}$ be a random process defined w.r.t. $\mathscr{F}$.

Definition (IID Process)

$\{X_t : t \in \mathbb{R}_+\}$ is said to be an IID process with the common CDF F if for any $n \in \mathbb{N}$ and $\mathbf{t} \in \mathbb{R}_+^n$,

$$F_{\mathbf{t}}(\mathbf{x}) = \prod_{i=1}^{n} F(x_i), \qquad \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n.$$

In simple words, for any $n \in \mathbb{N}$ and $\mathbf{t} = (t_1, \ldots, t_n)$, the random variables $(X_{t_1}, \ldots, X_{t_n})$ are IID.

Some Results on IID Processes

Lemma

Suppose that $\{X_t : t \in \mathbb{R}_+\}$ is an IID process.

1. The FDDs of $\{X_t : t \in \mathbb{R}_+\}$ are consistent.
2. $\{X_t : t \in \mathbb{R}_+\}$ is strictly stationary.
   That is, every IID process is stationary.

Example

- Let $X_1, X_2, \ldots$ be an $\mathbb{N}$-valued IID process.
  Let $S_0 := 0$, and for each $n \in \mathbb{N}$, let

$$S_n = \sum_{i=1}^{n} X_i.$$

  - Determine M_S and C_S for the process $\{S_n\}_{n=0}^{\infty}$.

Example

- Let $X_1, X_2, \ldots$ be an $\mathbb{N}$-valued IID process.
  Let $S_0 := 0$, and for each $n \in \mathbb{N}$, let

$$S_n = \sum_{i=1}^{n} X_i.$$

  - Determine M_S and C_S for the process $\{S_n\}_{n=0}^{\infty}$.
  - Is $\{S_n\}_{n=0}^{\infty}$ wide-sense stationary?

Example

- Let $X_1, X_2, \ldots$ be an $\mathbb{N}$-valued IID process.
  Let $S_0 := 0$, and for each $n \in \mathbb{N}$, let

$$S_n = \sum_{i=1}^{n} X_i.$$

  - Determine M_S and C_S for the process $\{S_n\}_{n=0}^{\infty}$.
  - Is $\{S_n\}_{n=0}^{\infty}$ wide-sense stationary?
  - Determine the joint PMF of $S_1, \ldots, S_n$.

Example

- Let $X_1, X_2, \ldots$ be an $\mathbb{N}$-valued IID process.
  Let $S_0 := 0$, and for each $n \in \mathbb{N}$, let

$$S_n = \sum_{i=1}^{n} X_i.$$

  - Determine M_S and C_S for the process $\{S_n\}_{n=0}^{\infty}$.
  - Is $\{S_n\}_{n=0}^{\infty}$ wide-sense stationary?
  - Determine the joint PMF of $S_1, \ldots, S_n$.
  - If X_i's are IID and $\mathbb{R}$-valued with a common PDF f_X, determine the joint PDF of $S_1, \ldots, S_n$.

Example – Gaussian Process

- Let $\{X_t : t \in \mathbb{R}\}$ be a continuous-time process.
  For any $n \in \mathbb{N}$ and $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, let $(X_{t_1}, \ldots, X_{t_n})$ be jointly continuous, and in particular jointly Gaussian, with the joint PDF

$$f_{\mathbf{t}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n \det(K_{\mathbf{t}})}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})^\top K_{\mathbf{t}}^{-1}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})\right), \qquad \mathbf{x} \in \mathbb{R}^n,$$

  where $\boldsymbol{\mu}_{\mathbf{t}}$ and $K_{\mathbf{t}}$ are given by

Example – Gaussian Process

- Let $\{X_t : t \in \mathbb{R}\}$ be a continuous-time process.
  For any $n \in \mathbb{N}$ and $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, let $(X_{t_1}, \ldots, X_{t_n})$ be jointly continuous, and in particular jointly Gaussian, with the joint PDF

$$f_{\mathbf{t}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n \det(K_{\mathbf{t}})}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})^\top K_{\mathbf{t}}^{-1}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})\right), \qquad \mathbf{x} \in \mathbb{R}^n,$$

  where $\boldsymbol{\mu}_{\mathbf{t}}$ and $K_{\mathbf{t}}$ are given by

$$\boldsymbol{\mu}_{\mathbf{t}} = \begin{bmatrix} \mathbb{E}[X_{t_1}] \\ \vdots \\ \mathbb{E}[X_{t_n}] \end{bmatrix} = \begin{bmatrix} M_X(t_1) \\ \vdots \\ M_X(t_n) \end{bmatrix},$$

Example – Gaussian Process

- Let $\{X_t : t \in \mathbb{R}\}$ be a continuous-time process.
  For any $n \in \mathbb{N}$ and $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, let $(X_{t_1}, \ldots, X_{t_n})$ be jointly continuous, and in particular jointly Gaussian, with the joint PDF

$$f_{\mathbf{t}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n \det(K_{\mathbf{t}})}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})^\top K_{\mathbf{t}}^{-1}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})\right), \qquad \mathbf{x} \in \mathbb{R}^n,$$

  where $\boldsymbol{\mu}_{\mathbf{t}}$ and $K_{\mathbf{t}}$ are given by

$$\boldsymbol{\mu}_{\mathbf{t}} = \begin{bmatrix} \mathbb{E}[X_{t_1}] \\ \vdots \\ \mathbb{E}[X_{t_n}] \end{bmatrix} = \begin{bmatrix} M_X(t_1) \\ \vdots \\ M_X(t_n) \end{bmatrix}, \quad K_{\mathbf{t}} = \begin{bmatrix} C_X(t_1, t_1) & C_X(t_1, t_2) & \cdots & C_X(t_1, t_n) \\ C_X(t_2, t_1) & C_X(t_2, t_2) & \cdots & C_X(t_2, t_n) \\ \vdots & \vdots & \vdots & \vdots \\ C_X(t_n, t_1) & C_X(t_n, t_2) & \cdots & C_X(t_n, t_n) \end{bmatrix}$$

Example – Gaussian Process

- Let $\{X_t : t \in \mathbb{R}\}$ be a continuous-time process.
  For any $n \in \mathbb{N}$ and $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, let $(X_{t_1}, \ldots, X_{t_n})$ be jointly continuous, and in particular jointly Gaussian, with the joint PDF

$$f_{\mathbf{t}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n \det(K_{\mathbf{t}})}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})^\top K_{\mathbf{t}}^{-1}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})\right), \qquad \mathbf{x} \in \mathbb{R}^n,$$

where $\boldsymbol{\mu}_{\mathbf{t}}$ and $K_{\mathbf{t}}$ are given by

$$\boldsymbol{\mu}_{\mathbf{t}} = \begin{bmatrix} \mathbb{E}[X_{t_1}] \\ \vdots \\ \mathbb{E}[X_{t_n}] \end{bmatrix} = \begin{bmatrix} M_X(t_1) \\ \vdots \\ M_X(t_n) \end{bmatrix}, \quad K_{\mathbf{t}} = \begin{bmatrix} C_X(t_1,t_1) & C_X(t_1,t_2) & \cdots & C_X(t_1,t_n) \\ C_X(t_2,t_1) & C_X(t_2,t_2) & \cdots & C_X(t_2,t_n) \\ \vdots & \vdots & \vdots & \vdots \\ C_X(t_n,t_1) & C_X(t_n,t_2) & \cdots & C_X(t_n,t_n) \end{bmatrix}$$

Remark

A wide-sense stationary Gaussian process is stationary, i.e.,
for any $n \in \mathbb{N}$, $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, and $h \in \mathbb{R}$,

Example – Gaussian Process

- Let $\{X_t : t \in \mathbb{R}\}$ be a continuous-time process.
  For any $n \in \mathbb{N}$ and $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, let $(X_{t_1}, \ldots, X_{t_n})$ be jointly continuous, and in particular jointly Gaussian, with the joint PDF

$$f_{\mathbf{t}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^n \det(K_{\mathbf{t}})}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})^\top K_{\mathbf{t}}^{-1}(\mathbf{x} - \boldsymbol{\mu}_{\mathbf{t}})\right), \qquad \mathbf{x} \in \mathbb{R}^n,$$

  where $\boldsymbol{\mu}_{\mathbf{t}}$ and $K_{\mathbf{t}}$ are given by

$$\boldsymbol{\mu}_{\mathbf{t}} = \begin{bmatrix} \mathbb{E}[X_{t_1}] \\ \vdots \\ \mathbb{E}[X_{t_n}] \end{bmatrix} = \begin{bmatrix} M_X(t_1) \\ \vdots \\ M_X(t_n) \end{bmatrix}, \quad K_{\mathbf{t}} = \begin{bmatrix} C_X(t_1, t_1) & C_X(t_1, t_2) & \cdots & C_X(t_1, t_n) \\ C_X(t_2, t_1) & C_X(t_2, t_2) & \cdots & C_X(t_2, t_n) \\ \vdots & \vdots & \vdots & \vdots \\ C_X(t_n, t_1) & C_X(t_n, t_2) & \cdots & C_X(t_n, t_n) \end{bmatrix}$$

Remark

A wide-sense stationary Gaussian process is stationary, i.e.,
for any $n \in \mathbb{N}$, $\mathbf{t} = (t_1, \ldots, t_n) \in \mathbb{R}^n$, and $h \in \mathbb{R}$, $\qquad f_{\mathbf{t}+h} = f_{\mathbf{t}}$.

Example – Back to Random Walk

- Let $X_1, X_2, \ldots$ be an $\mathbb{N}$-valued IID process.
  Let $S_0 := 0$, and for each $n \in \mathbb{N}$, let $S_n = \sum_{i=1}^{n} X_i$.

Example – Back to Random Walk

- Let $X_1, X_2, \ldots$ be an $\mathbb{N}$-valued IID process.
  Let $S_0 := 0$, and for each $n \in \mathbb{N}$, let $S_n = \sum_{i=1}^{n} X_i$.
  - Show that $\{S_n\}_{n=0}^{\infty}$ has stationary increments, i.e., for any $n \in \mathbb{N}$ and $0 \leq t_1 < t_2 < \cdots < t_n$,

$$\left(S_{t_2} - S_{t_1}, \ \ldots, S_{t_n} - S_{t_{n-1}}\right) \quad \stackrel{\text{d.}}{=} \quad \left(S_{t_2+h} - S_{t_1+h}, \ \ldots, S_{t_n+h} - S_{t_{n-1}+h}\right) \quad \forall h \in \mathbb{N}.$$

  - Show that $\{S_n\}_{n=0}^{\infty}$ has independent increments, i.e., for any $n \in \mathbb{N}$ and $0 \leq t_1 < t_2 < \cdots < t_n$,

$$S_{t_2} - S_{t_1}, \ \ldots, S_{t_n} - S_{t_{n-1}} \quad \text{are independent.}$$

Example – Back to Random Walk

- Let $X_1, X_2, \ldots$ be an $\mathbb{N}$-valued IID process.
  Let $S_0 := 0$, and for each $n \in \mathbb{N}$, let $S_n = \sum_{i=1}^{n} X_i$.
  - Show that $\{S_n\}_{n=0}^{\infty}$ has stationary increments, i.e.,
    for any $n \in \mathbb{N}$ and $0 \leq t_1 < t_2 < \cdots < t_n$,

$$\left(S_{t_2} - S_{t_1}, \ \ldots, S_{t_n} - S_{t_{n-1}}\right) \quad \stackrel{\text{d.}}{=} \quad \left(S_{t_2+h} - S_{t_1+h}, \ \ldots, S_{t_n+h} - S_{t_{n-1}+h}\right) \quad \forall h \in \mathbb{N}.$$

  - Show that $\{S_n\}_{n=0}^{\infty}$ has independent increments, i.e.,
    for any $n \in \mathbb{N}$ and $0 \leq t_1 < t_2 < \cdots < t_n$,

$$S_{t_2} - S_{t_1}, \ \ldots, S_{t_n} - S_{t_{n-1}} \quad \text{are independent.}$$

Note

Independent + stationary increments property plays an important role in process theory.

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Pseudo-Random Number Generators (PRNGs)

Binary PRNGs

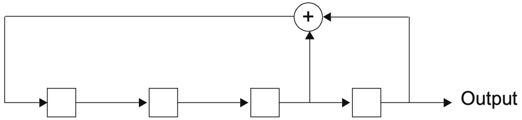
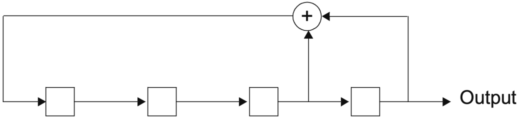
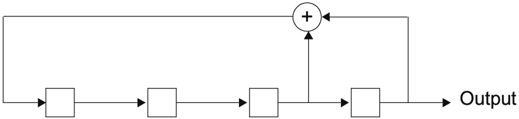


Figure: A four-stage, binary linear feedback shift register.

Binary PRNGs

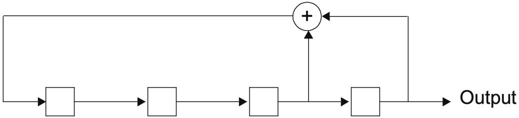


Binary PRNGs



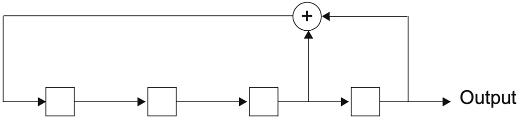
$S_0S_1S_2S_3$	Output
1111	1

Binary PRNGs



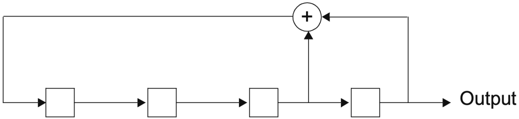
$S_0S_1S_2S_3$	Output
1111	1
0111	1

Binary PRNGs



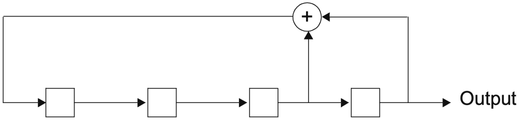
$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1

Binary PRNGs



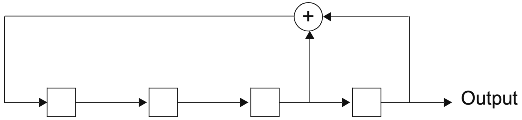
$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1
0001	1

Binary PRNGs



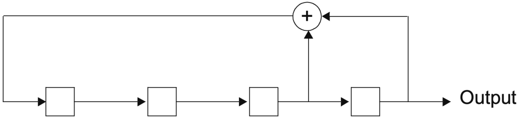
$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1
0001	1
1000	0

Binary PRNGs



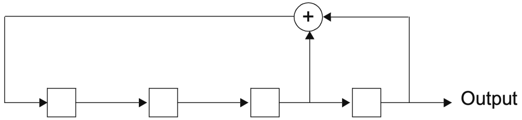
$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1
0001	1
1000	0
0100	0

Binary PRNGs



$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1
0001	1
1000	0
0100	0
0010	0

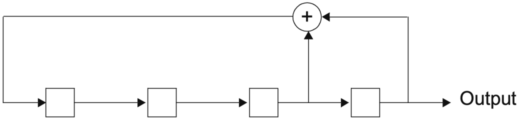
Binary PRNGs



$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1
0001	1
1000	0
0100	0
0010	0

$S_0S_1S_2S_3$	Output
1001	1
1100	0
0110	0
1011	1
0101	1
1010	0
1101	1
1110	0

Binary PRNGs



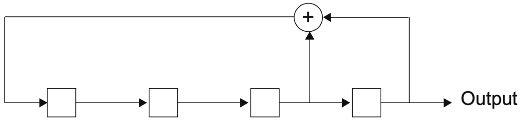
$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1
0001	1
1000	0
0100	0
0010	0

$S_0S_1S_2S_3$	Output
1001	1
1100	0
0110	0
1011	1
0101	1
1010	0
1101	1
1110	0

Output (one period): 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

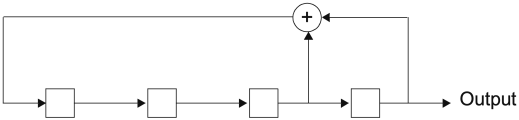
Properties of the Binary PRNG



Output (one period): $1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0$

- Number of zeros in one period $\approx$ number of ones in one period (desirable of uniform binary random number generator)
- Period = 15 (not desirable of uniform binary random number generator)

Properties of the Binary PRNG



Output (one period): $1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0$

- Number of zeros in one period $\approx$ number of ones in one period (desirable of uniform binary random number generator)
- Period = 15 (not desirable of uniform binary random number generator)

Possible Workaround for Periodicity in Output

Increase the number of stages N.

N-Stage Binary PRNG

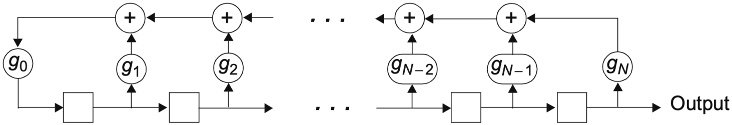


Figure: N-Stage, binary linear feedback shift register.