भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Stochastic Processes

PRNGs (contd.), Filtrations, Stopping Time

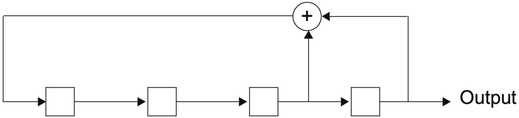
Karthik P. N.
Assistant Professor, Department of AI
Email: pnkarthik@ai.iith.ac.in

25 February 2025

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Pseudo-Random Number Generators (PRNGs)

Binary PRNGs

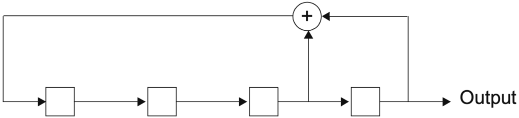


$S_0S_1S_2S_3$	Output
1111	1
0111	1
0011	1
0001	1
1000	0
0100	0
0010	0

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

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

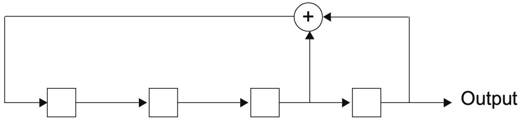
Properties of the Binary PRNG



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)

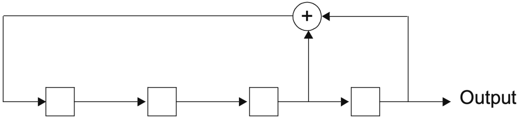
Properties of the Binary PRNG



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)

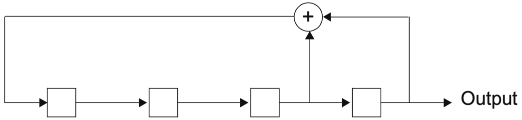
Properties of the Binary PRNG



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)

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

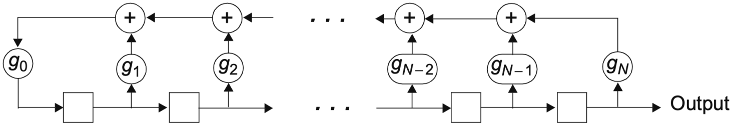


Figure: N-Stage, binary linear feedback shift register.

N-Stage Binary PRNG

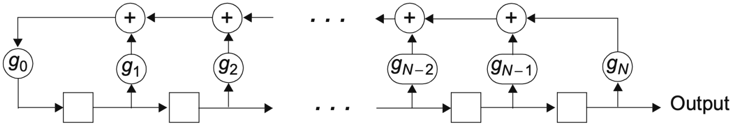


Figure: N-Stage, binary linear feedback shift register.

- $g_0 = g_N = 1$

N-Stage Binary PRNG

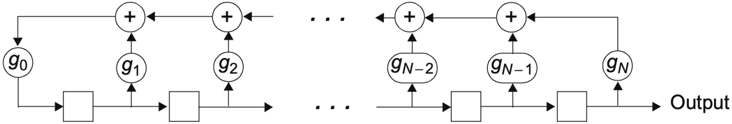


Figure: N-Stage, binary linear feedback shift register.

- $g_0 = g_N = 1$
- Adjust the tap gains $\{g_1, \ldots, g_{N-1}\}$ to achieve highest possible period $(= 2^N - 1)$

N-Stage Binary PRNG

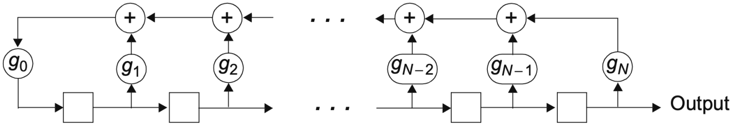


Figure: N-Stage, binary linear feedback shift register.

- $g_0 = g_N = 1$
- Adjust the tap gains $\{g_1, \ldots, g_{N-1}\}$ to achieve highest possible period $(= 2^N - 1)$
- E.g., for $N = 4$, set

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

N-Stage Binary PRNG

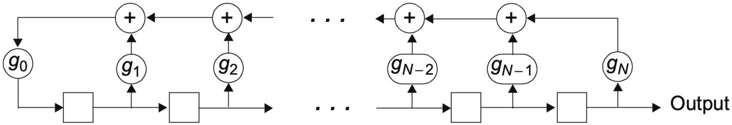


Figure: N-Stage, binary linear feedback shift register.

- $g_0 = g_N = 1$
- Adjust the tap gains $\{g_1, \ldots, g_{N-1}\}$ to achieve highest possible period $(= 2^N - 1)$
- E.g., for $N = 4$, set

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

- Maximal period sequences are called *m*-sequences

Commonly Used Feedback Connections

SR Length, N	Feedback Connections (in Octal Format)
2	7
3	13
4	23
5	45, 67, 75
6	103, 147, 155
7	203, 211, 217, 235, 277, 313, 325, 345, 367
8	435, 453, 537, 543, 545, 551, 703, 747

Figure: Non-exhaustive list of feedback connections to obtain m-sequences.

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$
- Contain approximately equal number of ones and zeros in any one period

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$
- Contain approximately equal number of ones and zeros in any one period
- Autocorrelation function is nearly identical to that of IID $\mathrm{Ber}(0.5)$ process

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$
- Contain approximately equal number of ones and zeros in any one period
- Autocorrelation function is nearly identical to that of IID $\mathrm{Ber}(0.5)$ process
  - Suppose $X_1, X_2, \cdots \overset{\text{i.i.d.}}{\sim} \mathrm{Ber}(0.5)$

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$
- Contain approximately equal number of ones and zeros in any one period
- Autocorrelation function is nearly identical to that of IID $\mathrm{Ber}(0.5)$ process
  - Suppose $X_1, X_2, \cdots \stackrel{\text{i.i.d.}}{\sim} \mathrm{Ber}(0.5)$
  - Then,

$$M_X(t) = 0.5, \qquad R_X(s,t) =$$

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$
- Contain approximately equal number of ones and zeros in any one period
- Autocorrelation function is nearly identical to that of IID $\mathrm{Ber}(0.5)$ process
  - Suppose $X_1, X_2, \cdots \overset{\text{i.i.d.}}{\sim} \mathrm{Ber}(0.5)$
  - Then,

$$M_X(t) = 0.5, \qquad\qquad R_X(s,t) =$$

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$
- Contain approximately equal number of ones and zeros in any one period
- Autocorrelation function is nearly identical to that of IID $\mathrm{Ber}(0.5)$ process
  - Suppose $X_1, X_2, \cdots \overset{\text{i.i.d.}}{\sim} \mathrm{Ber}(0.5)$
  - Then,

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

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

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

भारतीय प्रौद्योगिकी संस्थान हैदराबाद
Indian Institute of Technology Hyderabad

Properties of m-Sequences

- Are periodic with period $= 2^N - 1$
- Contain approximately equal number of ones and zeros in any one period
- Autocorrelation function is nearly identical to that of IID $\mathrm{Ber}(0.5)$ process
  - Suppose $X_1, X_2, \cdots \overset{\text{i.i.d.}}{\sim} \mathrm{Ber}(0.5)$
  - Then,

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

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

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

  - Considering the single period output $1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0$, we have

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

Non-Binary PRNGs

- How do we generate non-binary m-sequences?

Non-Binary PRNGs

- How do we generate non-binary m-sequences?
- One technique is the power residue method

Non-Binary PRNGs

- How do we generate non-binary m-sequences?
- One technique is the power residue method
- Given numbers (a, x_0, p), let

$$x_n = a x_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

Non-Binary PRNGs

- How do we generate non-binary m-sequences?
- One technique is the power residue method
- Given numbers (a, x_0, p), let

$$x_n = ax_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

  - p is typically a large prime (e.g., $p = 2^{31} - 1 = 2147483647$)

Non-Binary PRNGs

- How do we generate non-binary m-sequences?
- One technique is the power residue method
- Given numbers (a, x_0, p), let

$$x_n = a x_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

  - p is typically a large prime (e.g., $p = 2^{31} - 1 = 2147483647$)
  - $x_0 \neq 0$ is called the seed value (e.g., $x_0 = 12345$)

Non-Binary PRNGs

- How do we generate non-binary m-sequences?
- One technique is the power residue method
- Given numbers (a, x_0, p), let

$$x_n = ax_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

  - p is typically a large prime (e.g., $p = 2^{31} - 1 = 2147483647$)
  - $x_0 \neq 0$ is called the seed value (e.g., $x_0 = 12345$)
  - $a \neq 1$ is the multiplicative factor

Non-Binary PRNGs

- How do we generate non-binary m-sequences?
- One technique is the power residue method
- Given numbers (a, x_0, p), let

$$x_n = a x_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

  - p is typically a large prime (e.g., $p = 2^{31} - 1 = 2147483647$)
  - $x_0 \neq 0$ is called the seed value (e.g., $x_0 = 12345$)
  - $a \neq 1$ is the multiplicative factor
- Due to $(\bmod\ p)$ operation, $x_n \in \{1, \ldots, p-1\}$ for all n

Non-Binary PRNGs

- How do we generate non-binary m-sequences?
- One technique is the power residue method
- Given numbers (a, x_0, p), let

$$x_n = a x_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

  - p is typically a large prime (e.g., $p = 2^{31} - 1 = 2147483647$)
  - $x_0 \neq 0$ is called the seed value (e.g., $x_0 = 12345$)
  - $a \neq 1$ is the multiplicative factor
- Due to $(\bmod\ p)$ operation, $x_n \in \{1, \ldots, p-1\}$ for all n
- The choice of (a, p) is crucial to obtain an m-sequence

Non-Binary PRNGs

Recursion

$$x_n = ax_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

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

Non-Binary PRNGs

Recursion

$$x_n = ax_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

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

$$(1, 4, 2, 1, 4, 2, \cdots)$$

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

Non-Binary PRNGs

Recursion

$$x_n = ax_{n-1} \bmod p, \qquad n \in \mathbb{N}.$$

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

$$(1, 4, 2, 1, 4, 2, \cdots)$$

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

$$(1, 3, 2, 6, 4, 5, 1, 3, 2, 6, 4, 5, \cdots)$$

- In most programming languages:
  - $a = 7^5, \quad p = 2^{31} - 1.$
  - Output normalised to take values in $\left\{\frac{1}{p}, \frac{2}{p}, \ldots, \frac{p-1}{p}\right\}$

Stopping Times

σ-Algebra Generated by a Random Variable

Fix a measurable space $(\Omega, \mathscr{F})$.
Let $X : \Omega \to \mathbb{R}$ be a random variable w.r.t. $\mathscr{F}$.

Definition (σ-Algebra Generated by a Random Variable)

The σ-algebra generated by X, denoted $\sigma(X)$, is defined as

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

σ-Algebra Generated by a Random Variable

Fix a measurable space $(\Omega, \mathscr{F})$.
Let $X : \Omega \to \mathbb{R}$ be a random variable w.r.t. $\mathscr{F}$.

Definition (σ-Algebra Generated by a Random Variable)

The σ-algebra generated by X, denoted $\sigma(X)$, is defined as

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

Remark: $\sigma(X)$ is the smallest σ-algebra w.r.t. which X is a RV.

σ-Algebra Generated by a Random Vector

Fix a measurable space $(\Omega, \mathscr{F})$.
Let $(X_1, \ldots, X_n) : \Omega \to \mathbb{R}^n$ be a random vector w.r.t. $\mathscr{F}$.

Definition (σ-Algebra Generated by a Random Vector)

The σ-algebra generated by $(X_1, \ldots, X_n)$, denoted $\sigma(X_1, \ldots, X_n)$, is defined as

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

Filtrations

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

Let $\mathcal{T}$ be an ordered index set.

Filtrations

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

Let $\mathcal{T}$ be an ordered index set.

Definition (Filtration)

Consider a collection of σ-algebras $\mathscr{G}_\bullet = \{\mathscr{G}_t : t \in \mathcal{T}\}$ such that $\mathscr{G}_t \subseteq \mathscr{F}$ for all t.

The above collection is called a filtration if

$$\mathscr{G}_s \subseteq \mathscr{G}_t \qquad \forall s \leq t.$$

Filtrations

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

Let $\mathcal{T}$ be an ordered index set.

Definition (Filtration)

Consider a collection of σ-algebras $\mathscr{G}_\bullet = \{\mathscr{G}_t : t \in \mathcal{T}\}$ such that $\mathscr{G}_t \subseteq \mathscr{F}$ for all t.

The above collection is called a filtration if

$$\mathscr{G}_s \subseteq \mathscr{G}_t \qquad \forall s \leq t.$$

Example:

Let $\{X_t : t \in \mathcal{T}\}$ be a stochastic process defined w.r.t. $\mathscr{F}$. Then,

$$\mathscr{G}_t = \sigma(X_s : s \leq t)$$

is called the natural filtration associated with the process $\{X_t : t \in \mathcal{T}\}$.

Stopping Time

Fix a probability space $(\Omega, \mathscr{F}, \mathbb{P})$.
Let $\mathcal{T}$ be an ordered index set.
Fix a filtration $\mathscr{G}_\bullet = \{\mathscr{G}_t : t \in \mathcal{T}\}$.

Definition (Stopping Time)

A random variable $\tau : \Omega \to \mathbb{R} \cup \{\pm\infty\}$ is called a stopping time w.r.t. the filtration $\mathscr{G}_\bullet$ if:

- $\mathbb{P}(\tau < +\infty) = 1$.
- For each $t \in \mathcal{T}$,
$$\{\tau \leq t\} \in \mathscr{G}_t.$$

That is, the answer to the question "is $\tau \leq t$?" can be decided by simply looking at the process up to (including) time t.