# Golomb's Randomness Postulates

**Definition:**

Let s = $s_0$, $s_1$, $s_2$,….. be an infinite sequence. The subsequence consisting of first n terms of s is denoted by $s^n$ = $s_0$, $s_1$,…., $s_{n-1}$.

**Example**: Let s = 0,1,1,0,1,1,0,1,1,….. be an infinite sequence, then $s^1$ = 0, $s^2$ = 0,1 and so on.

**Definition:**

The sequence s = $s_0$, $s_1$, $s_2$,…… is said to be N-periodic if $s_i$=$s_{i+N}$. The sequence s is periodic if it is N-periodic for some positive integer N.

The period of a periodic sequence s is the smallest positive integer N for which s is N-periodic. If s is a periodic sequence of period N, then the cycle of s is the subsequence $s^N$.

**Example**: Let s = 0,1,1,0,1,1,0,1,1,…. Here $s_i$ = $s_{i+3}$, therefore s is 3-periodic. Therefore s is periodic with period 3, and the cycle of s is the subsequence $s^3$ = 0,1,1.

**Definition:**

Let s be a sequence. A run of s is a subsequence of s consisting of consecutive 0's or consecutive 1's. A run of 0's is called a gap while a run of 1's is called a block.

**Example**: Let s = 0,1,1,0,1,1,… 0 is a run of length 1 called a gap, and 1,1 is a run of length 2 called a block.

**Definition:**

Let s = $s_0$,$s_1$,….. $s_n$ be a periodic sequence of period N. The auto-correlation function of s is the integer valued function C(t) defined as :-

C(t)= (1/N) $\sum_{i=0}^{N-1}(2s_i - 1)(2s_{i+t} - 1)$ for 0 ≤ t ≤ N-1 .

The auto correlation function C(t) measures the amount of similarity between the sequence s and shift of s by t positions.

**Example**: Let s = 0,1,1,0,1,1,… Here N=3

C(0) = (1/3)[(2*0-1)(2*0-1) + (2*1-1)(2*1-1) + (2*1-1)(2*1-1)] = (1/3)[1+1+1) = 1

C(1) = (1/3)[(2*0-1)(2*1-1) + (2*1-1)(2*1-1) + (2*1-1)(2*0-1)] = (1/3)[-1+1-1] = -1/3

Similarly, C(2) = -1/3 and C(3) = 1

If s is a random periodic sequence of period N, then |N.C(t)| can be expected to be quite small for all values of t, $0 \le t \le N$.

**Definition:**

Let s be a periodic sequence of period N. **Golomb's Randomness Postulates** are the following:-

***R1:*** In the cycle $s^N$, the number of 1's differ from the number of 0's by at most 1.

***R2:*** In the cycle $s^N$, at least half the runs have length 1, at least one-fourth have length 2, at least one-eighth have length 3 etc. More over for each of these lengths, there are (almost) equally many gaps and blocks.

***R3:*** The auto-correlation function C(t) is a 2-valued. That is, for some integer k,

$$\text{N.C(t)} = \sum_{i=0}^{N-1}(2s_i - 1)(2s_{i+t} - 1) = \begin{cases} N, & if\ t = 0, N \\ k, & if\ 1 \le t \le N-1 \end{cases}$$

**Example**:

N=15
$S^{15}$ = 0,1,1,0,0,1,0,0,0,1,1,1,1,0,1

Checking R1:

Number of 0's = 7 and Number of 1's = 8

Difference between number of 0's and 1's = 1

Therefore, R1 is satisfied.

Checking R2:

Number of runs of length 1 = 4 ($s_0$, $s_5$, $s_{13}$, $s_{14}$)
Number of gaps = 2 ($s_0$, $s_{14}$) and Number of blocks = 2 ($s_5$, $s_{13}$)

Number of runs of length 2 = 2 ($s_1s_2$, $s_3s_4$)
Number of gaps = 1 ($s_3s_4$) and Number of blocks = 1 ($s_1s_2$)

Number of runs of length 3 = 1 ($s_6s_7s_8$)
Number of gaps = 1 ($s_6s_7s_8$) and Number of blocks = 0

Number of runs of length 4 = 1 ($s_9s_{10}s_{11}s_{12}$)
Number of gaps = 0 and Number of blocks = 1 ($s_9s_{10}s_{11}s_{12}$)

Total number of runs = 4+2+1+1 = 8
Half the runs have length 1, one-fourth have length 2, one-eighth have length 3.

Therefore, R2 is satisfied.

Checking R3:

15.C(t) = $= \begin{cases} 1, & for\ t = 0,15 \\ -1, & for\ 1 \leq t \leq 14 \end{cases}$

That is, C(t) is 2-valued. Therefore, R3 is satisfied.

Therefore, s is a pn-sequence.