Lecture Two

Randomness

5. Golomb's Concept of Randomness

Golomb's randomness postulates are presented here for historical reasons they were one of the first attempts to establish some necessary conditions for a periodic pseudorandom sequence to look random. It is emphasized that these conditions are far from being sufficient for such sequences to be considered random.

Definition(5.1): Let $S=s_0,s_1,s_2\ldots$ be an infinite sequence. The subsequence consisting of the first n terms of S is denoted by $S^n=s_0,s_1,s_2,\ldots,s_{n-1}$.

Definition(5.2): The sequence $S=s_0,s_1,s_2$ . . . is said to be **n-periodic** if $s_i=s_{i+n}$ for all $i\geq 0$. 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.

Definition(5.3): Let S be a sequence. A **run** of S is a subsequence of S consisting of consecutive 0′s or consecutive 1′s which is neither preceded nor succeeded by the same symbol.

A run of 0′s is called a **gap**, while a run of 1′s is called a **block**.

Definition(5.4): Let $S= s_0,s_1,s_2\ldots$ be a periodic sequence of period n. The **autocorrelation function** of S is the integer-valued function C(t) defined as:

$$n.C(\tau)=\sum_{i=0}^{n-1}(2s_i-1)\cdot(2s_{i+t}-1),\ 0\le\tau\le n-1.$$

The autocorrelation function $C(\tau)$ measures the amount of similarity between the sequence S and a shift of S by τ positions. If S is a random periodic sequence of period n, then $n.C(\tau)$ can be expected to be quite small for all values of τ, $0<\tau<n$.

Definition(5.5): Let S be a periodic sequence of period n. Golomb′s randomness postulates are the following:

R1: In the cycle S^n of S, the number of 1′s differs 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., as long as the number of runs so indicated exceeds 1. Moreover, for each of these lengths, there are (almost) equally many gaps and blocks.

R3: The autocorrelation function $C(\tau)$ is two-valued. That is for some integer K:

$$n.C(\tau)=\sum_{i=0}^{n-1}(2s_i-1)\cdot(2s_{i+t}-1)=\begin{cases}n & ,t=0\\ K & ,1\le t\le n-1\end{cases}$$

Definition(5.6): A binary sequence which satisfies Golomb′s randomness postulates is called a **pseudo-noise sequence** or a **pn-sequence**.

Pseudo-noise sequences arise in practice as output sequences of maximum-length linear feedback shift registers.

Example (5.1): (pn-sequence) Consider the periodic sequence S of period n=15 with cycle S^{15}=011001000111101

The following shows that the sequence S satisfies Golomb′s randomness postulates.

R1: The number of 0′s in s^{15} is 7, while the number of 1′s is 8.

R2: S^{15} has 8 runs. There are 4 runs of length 1 (2 gaps and 2 blocks), 2 runs of length 2 (1 gap and 1 block), 1 run of length 3 (1 gap), and 1 run of length 4 (1 block).

R3: The autocorrelation function $C(\tau)$ takes on two values :$C(0)=1$ and $C(\tau)=1/15$ for $1\leq\tau\leq14$. Hence, S is a pn-sequence.