CIS 628 Part 2 Question(A)

Introduction to Cryptography

Syracuse University

Fall 2022

Homework 2

Part 2, Question(a)

Saket Kiran Thombre

SU ID: 899913802

NetID: sthombre

Email: sthombre@syr.edu

(a) (10 points) Given the algorithm (see the posting on NIST link https://www.itl.nist.gov/div898/handbook/eda/section3/eda35d.htm) determine whether the given sequence of coin tosses is random or not.

HHHHHTTHHHHHTTTTTHHTTHTHTHHHTT

Solution:

We need to find if the given sequence is random or not.

A run is a sum of all increasing or decreasing values in a given set.

Calculating runs in the given coin toss sequence

Heads count: 17 = n1

Heads runs: 6

Tails count: 13 = n2

Tails runs: 6

The expected number of runs

$\bar{R} = \frac{2*n1*n2}{n1+n2} + 1$

Substituting values in the equation we get

$\bar{R} = \frac{2*17*13}{17+13} + 1$

$\bar{R} = \frac{17*13}{15} + 1$

$\bar{R} = 15.733$

To calculate the standard deviation of number of runs

$s^2R = \frac{2n1n2(2n1n2-n1-n2)}{(n1+n2)^2\ (n1+n2-1)}$

Where,

R is observed number of runs.

Substituting values in the equation we get

$s^2R = \frac{2 * 17 * 13\ (2 * 17 * 13 - 17 - 13)}{(17 + 13)^2\ (17 + 13-1)}$

$s^2R = \frac{442(442-30)}{900\ (29)}$

$s^2R = \frac{182104}{26100}$

$s^2R = 6.977$

Now we calculate sR

sR = 2.641

Now we will calculate test statistic

Z = $\frac{R-\overline{R}}{sR}$

Z = $\frac{12-15.733}{2.641}$

Z = -1.413

To find the critical region

|Z| > $Z_{1-a/2}$

Solving further we get,

|Z| = 1.413

We can conclude that

If |Z| > 1.96

If test statistics above critical value, we draw the conclusion that the data are not random; otherwise, the data are random.

Hence, the given sequence is random.