Testing Random number generator

HERNÁNDEZ MARTINEZ JORGE IVÁN

Departamento de Física, CUCEI, Universidad de Guadalajara.

jorgeivanhdzmtz@gmail.com

I. INTRODUCTION

So far, we've seen that there are many different applications requiring random numbers, and that there are many different ways of acquiring them. We've mentioned above that not all sources of random numbers behave in the same way, and that some are better than others, at least for different applications. This begs the question: how can we tell if a random number generator is 'good' (or 'good enough')?. Certainly, this is not the only requirement we would demand of a RNG. For example, it would be important for a RNG designed to produce a long sequence of zeros and ones to produce them in roughly equal quantities. It would be nice for there to be independence between elements or sub sequences of a sequence produced by a RNG. In addition, a RNG should be fairly efficient in order to be of any real use. Not surprisingly, there are a lot of different tests for RNG's and the sequences they produce.

II. THE CHI-SQUARE TEST

This statistical test allows to consider how good is the hypothesis of uniform distribution over the interval (0, 1) for a sequence of n random numbers. The procedure is like follow. Divide the interval (0, 1) into r sub intervals of equal length and count the number n_k of random numbers that fall within each sub interval $k = 1, ..., r$ calculate

$$\chi^2 = \sum \frac{(n_k - n/r)^2}{n/r} \tag{1}$$

consider $\alpha = 0{,}1$ then we have to get

$$\chi^2 < \chi^2_{1-\alpha} \tag{2}$$

and in that case the RGN pass the test.

I. ordered pair test

A first test can be performed visually graphing in the plane the ordered pairs $(x_1, x_2), (x_3, x_4), ..., (x_{n-1}, x_n)$ of a sequence $(xi)_i^n$ of n random numbers. If the same are evenly distributed randomly in the interval (0,1) the points should fill the square (0,1)x(0,1) without any discernible pattern.

II. sample mean test and sample variance

A random variable x evenly distributed in the interval (0,1) has a function of distribution density $f(x) = 1$, $0 < x < 1$, whereupon your average is

$$\mu = \int_0^1 xf(x) = \frac{1}{2} \tag{3}$$

and the variance is

$$\sigma^2 = \int_0^1 (x-\mu)^2 f(x)dx = \frac{1}{12} \tag{4}$$

Consequently, a random sample of x, xi_i^n of size n, will have a sample mean

$$\mu = \frac{1}{n} \sum x_i \tag{5}$$

whose expected value is $\mu = 0{,}5$ and a variance sample

$$s^2 = \frac{1}{n-1} \sum (x_i - \mu)^2 \tag{6}$$

whose expected value is $s^2 = \frac{1}{12}$

III. Testing

I. Chi squared

The first test is the chi-squared test. I have to open 2 cicles to be able to evaluate in the corresponding equation

```
        !------------test para rng---
        !test of chi^2
        chi=0

        div=10       !number of divisions
        E=100              !expected frequency
        do j=1,div
        oi=0
         max=j*0.1
        min=(j-1)*0.1

               do q=1,n
                  if (max>c(q) .and. c(q)>=min) then
                  oi=oi+1      !how many numbers fall in that interval
                  end if
               end do
        chi=((oi-E)**2)/E    !calculate aech chi
        tchi=tchi+chi         !sum all chi
        write(400,*)oi,tchi

        enddo
        print*, 'el valor de chi al cuadrado es', tchi
!el valor chi total y el que buscamos
        !pause
```

at the end we get for 1000 random number $\chi = 4{,}40$ and is less than $\chi^2_{\alpha=0{,}05{,}9} = 16{,}9$. this would indicate that our rng passed the chi squared test

II. Ordered pair test

this test is simple, we only have to sabe the data in ordered pairs of odd and even.

```
!test de aleatoriedad de pares ordenados———
do q=1,n,2
  w=q+1
   write(500,*)c(q),c(w)
end do
```

then using next code of matlab for plot:

```
datos= textread('C:\Users\omarc\Desktop\test_pares.dat');
x = datos(:,1);
y= datos(:,2);
plot(x,y,'.')
ylabel('even␣pairs')
xlabel('Odd␣pairs')
```

we get the next plot

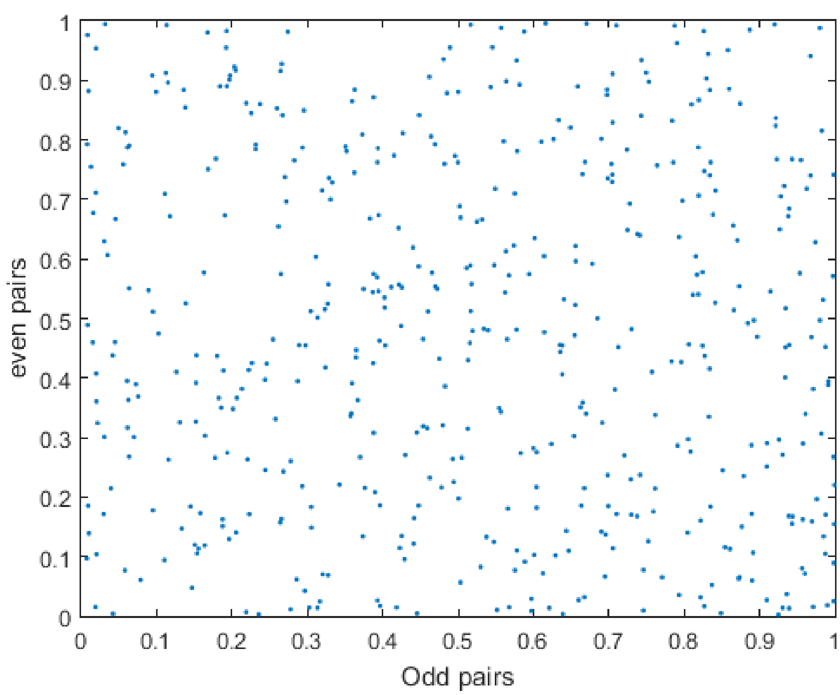

Figura 1

and we can see there is no pattern there, so then the RNG also passes this test

III. Sample mean test and sample variance

For the last test, i do a cicle to use the random number and evaluate to get the variance and the average.

```
        !test de media muestral y varianza muestral---
        stot=0  !start condition of variance
        prom=1/n
         do q=1,n
         s=((c(q)-(1/n))**2)/(n-1)
!calculate the variance
         stot=stot+s
         enddo
        write(600,*)prom, stot
```

When we run the program we get 2 values, the first is the mean and has a value of $\mu = 0{,}49720258$ and the second is the variance and has a value $s^2 = 8{,}63106549E - 02$.
As we can see, according to the theory. we should have obtained a value close to 0.5 for the average and 0.083 for the variance. And our values are too close, so it can be said that our RNG also passes this test

Referencias

[1] S. Teukolsky *Numerical Recipes in FORTRAN* chapter7. Get from $http : //nuclear.fis.ucm.es/wordpress/wp - content/uploads/2011/09/RandomNumbers.pdf$

[2] David G. Carta *Two Fast Implementations of the "Minimal Standard" Random Number Generator*.Volume 33 P. 87-88

[3] Herbert Hoeger *GENERACION DE NUMEROS ALEATORIOS* .Get from $hhttp : //webdelprofesor.ula.ve/ingenieria/hhoeger/simulacion/PARTE4.pdf$

[4] Dan Biebighauser *Testing Random Number Generators* .Get from $http : //www - users.math.umn.edu/ garrett/students/reu/pRNGs.pdf$