Números Pseudoaleatorios

Dr. Misael Erikson Maguiña Palma

Números pseudoaleatorios

Que son los numeros pseudoaleatorios:

Un **número pseudo-aleatorio** es un número generado en un proceso que parece producir números al azar, pero no lo hace realmente. De ahi se le da el prefijo *Pseudo* que quiere decir falso ya que su generación parte de algoritmos determinísticos, lo cual nos quiere decir que obtendremos siempre el mismo resultado bajo las mismas condiciones iniciales.

Un número aleatorio es aquél que es generado a partir de la distribución Uniforme U(0,1).

Para que sirven los números pseudoaleatorios:

La funcion de los numeros pseudoaleatorios es que apartir de ellos podemos generar variables aleatorias las cuales estan sujetas en el mayor de los casos, a distribuciones estadisticas que son las que se usan para establecer el comportamiento de los materiales, sucesos, personas, etc., en todo proceso de simulacion.

Que es un algoritmo

Es una posible solución a un problema. Es una método o proceso sistemático para resolver el problema (siempre que cumpla ciertas condiciones)

Numero aleatorios y pseudoaleatorios

- Dado que la simulación sin un equipo de computo es impactico la generación deberá ser realizada desde herramienta. Se menciona algunas consideraciones al respecto:
- Rapidez,
- Portabilidad,
- Periodo largo,
- Reproductible,
- Imprescindible: uniformidad e independencia

Métodos de Generación de números Pseudoaleatorios

- Algoritmo de cuadrado medios
- Algoritmo de productos medios
- Algoritmo de multiplicación constante
- Algoritmo lineal
- Algoritmo congruencias multiplicativo
- Algoritmo congruencia aditivo
- Algoritmo congruencia no lineal

Algoritmo de cuadrado medios

Un primer método es la generación de números pseudoaleatorios es el de los cuadrados Medios siguiendo los pasos:

- Generar una Semilla Xo
- Obtener el cuadrado de dicho numero.
- Extraer n dígitos de la parte central obtenida en el paso.

P1: Obtener semilla (valores iniciales 445)
P2: Aplicación de Algoritmos recursivos (elevar al cuadrado)
P3: Validación del conjunto de datos generados

Ejemplo: Consideremos la semilla 445

	X	X2	N° Aleatorio
445	1| 9802 | 5	0,9802	
9802	96| 0792 | 04	0,0792	
792	6 | 2726 | 4	0,2726	
2726	.....	.....	

Algoritmo productos medios

- Inicio
- Introducir el numero de iteraciones a realizar (n)
- Introducir una semilla (Xo) con D dígitos (d>3).
- Introducir una semilla(X1) con D dígitos (d>3).
- Verificar que el numero de Dígitos Xo sea igual al numero de dígitos de X1
- Xo>99, X1>999.
- Realizar al multiplicación (Xo*X1), para obtener Yo.
- Sean X2 los D dígitos del centro de resultado de l multiplicación .
- Sea Ri=0.D dígitos del centro.
- Multiplicar Xi por X2 para obtener Y1
- Sea X3=D dígitos del centro de Y1.
- R3=0.D dígitos del centro.
- Terminamos cuanto completamos el numero de iteraciones

Algoritmo de multiplicación constante

Multiplicar a*x

Sea Yo=a*Xo; sean X1=D dígitos del centro y sea ri=0.D dígitos del centro para todos desde i=1,2,...,n

Y0=(6965)(9803)=68277895

Donde X1=2778

r1=0.2778

Y1=(6965)(2778)=19348770

Donde X2=3487

r2=0.3487

Algoritmo lineal

- Conocido también como congruencia fue propuesto por D. H. Lehmer en 1951 ha sido el mas usado.
- Genera una secuencia de números enteros por medio de la siguiente ecuación recursiva:
- Xi+1=(aXi+C) mod (m) i=0,1,2,3,..,n (10^g)----
- Donde: X0=Semilla > a=cte Multiplicativa > c=cte Aditiva > m=modulo
- La operación "mod m" significa multiplicar Xi*a sumar c y dividir el resultado entre m para obtener el residuo Xi+1.
- El algoritmo genera números enteros S={0,1,2,3,...,m-1}, y para obtener numero pesudo aleatorio en (0,1) se requiere la siguiente ecuación:

$$r_i = \frac{x_i}{m-1} \quad i - 1,2,3,\ldots,n$$

Condiciones

- m=10^g
- a=1+4k k debe ser entero
- c=Relativamente primo a m
- g=entero
- Se obtiene el periodo de vida máximo
- N=m=10^g

Algoritmo congruencias multiplicativo

- Surge del algoritmo congruencia lineal cuando C=0; entonces la ecuación es:

  $X_{i+1}=(aX_i) \bmod (m) \qquad i=0,1,2,3,\ldots,n$

- La ventaja de este método es que en comparación con el algoritmo lineal es que este implica una operación menos. Los parámetros de arranque de este algoritmo son X0, a y m, todos los cuales deben ser números enteros y mayores que cero. Para transformar los números Xi en el intervalo (0,1) sean la ecuación: $r_i=x_i/(m-1)$.

- De acuerdo con Banks, Carson, Nelson y Nicol, las condiciones que deben cumplir los parámetros para que el algoritmo congruencial multiplicativo alcance su máximo periodo son:

  $m=2^g$

  $a=3+8k$ o $a=5+8k$ $k=0,1,2,3,\ldots\ldots$

Xo debe ser un numero impar g debe ser entero. a partir de estas condiciones se logra un periodo de vida máximo $N=(k/4)=2^{(g-2)}$

Algoritmo congruencia aditivo

Este algoritmo requiere una secuencia previa de n números enteros $X_1, X_2, X_3, X_4, \ldots, X_n$ para generar una nueva secuencia de números enteros que empiezan en $X_{n+1}, X_{n+2}, X_{n+3}, X_{n+4} \cdots$

Su ecuación recursiva es:

$$X_i = (X_{i-1} + X_{i-n}) \bmod (m) \qquad i = n+1, n+2, n+3 \ldots, N$$

Los números r_i, pueden ser generados mediante la ecuación:

$$r_i = X_i / (m-1)$$

Pruebas de aleatoridad

- Prueba de aleatoriedad y de independencia:

1. Prueba de media(1/2)
2. Prueba de varianza (1/2)
3. Prueba de frecuencias
4. Prueba de Kolmogorov-Smirnov

Uniformidad

5. Prueba de corridas arriba y abajo
6. Pruebas de corridas arriba y debajo de la media

Independencia