PRÁCTICA Nº 3: POSTULADOS DE GOLOMB

Objetivo: Análisis de secuencias cifrantes binarias aptas para cifrado en flujo.

Desarrollo:

1. Verificación del primer postulado de Golomb.
   Unos y ceros deben aparecer con idéntica frecuencia pudiendo diferir como máximo en una unidad. La salida de este procedimiento debe ser el número de ceros y unos que hay en la secuencia de entrada.

2. Verificación del segundo postulado de Golomb
   En cada periodo, la mitad de las rachas son de longitud 1, la cuarta parte de longitud 2, la octava de 3, etc. Las rachas de ceros y de unos deben aparecer con idéntica frecuencia para cada longitud. Pudiendo en este caso diferir también en una unidad.

   Lo primero que se debe hacer es contar las rachas totales existentes en la secuencia. No debes olvidar examinar el final y comienzo de la secuencia con especial cuidado.
   Una vez hecho esto lo siguiente es determinar cuántas rachas de cada longitud existen.
   Por último, se comprueba que las proporciones se verifican para cada longitud teniendo en cuenta el redondeo y que para cada longitud el número de gaps y blocks no difieren en más de una unidad.
   Mostrar como salida para este postulado la tabla con la siguiente información: Rachas totales: 15

Longitud	Nº gaps	Nº blocks	Nº de rachas	Proporción teórica
1	4	4	8	15 / 2 = 7.5
2	2	2	4	15 / 4 = 3.750
3	1	1	2	15 / 8 = 1.875
4	1	0	1	15 / 16 = 0.937
5	0	1	1	15 / 32 = 0.468

   El ejemplo que se presenta aquí es para la tercera secuencia que aparece al final de este enunciado.

3. Verificación del tercer postulado de Golomb.
   Se debe calcular la autocorrelación (Autocorrelación AC(k) = (NºCoinc - NºDif) / T) existente entre la secuencia original y la desplazada k posiciones, para todo valor de k comprendido entre 1 y la longitud de la secuencia comprobando cada vez que dicho valor permanece constante.
   Se debe mostrar como salida el valor de autocorrelación obtenido para cada desplazamiento (k) hasta k = T- 1 o hasta encontrar un valor que sea diferente del obtenido para el desplazamiento anterior.

4. Si se verifican todos los postulados diremos que la secuencia es una pn-secuencia

Ejemplos:
La secuencia 1000111101011001 00 no cumple el tercer postulado de Golomb

La secuencia 1011001010000111 no cumple el segundo y tampoco el tercer postulado de Golomb

La secuencia 1000 0110 0100 1111 1011 1000 1010 110 cumple los tres postulados de Golomb