

Sistemas de Tiempo Real: FPGAs 2013/14

Práctica 5: Secuencias de Números Binarios Pseudo-Aleatorios

Objetivo

En esta práctica se pretende repasar parte de los conceptos vistos en las prácticas anteriores y lo mostrado en el tutorial de VHDL en las clases de teoría.

Enunciado

En numerosas aplicaciones es preciso generar números aleatorios para acelerar procesos que simulados en PCs suelen tardar una cantidad de tiempo considerable. Esta aleatoriedad deseada se suele asociar al término *ruido blanco*, el cual es un tipo de ruido impredecible muy habitual en telecomunicaciones (por ejemplo, es el sonido que produce una radio analógica entre emisoras).

Dado que no es habitual que exista de manera nativa una fuente de ruido blanco que permita obtener números puramente aleatorios, en una FPGA se suele recurrir a un registro generador de secuencias binarias pseudo-aleatorias (PRBS, *Pseudo-Random Binary Sequence*). Al contrario que el ruido blanco, una PRBS es predecible, dado que se repite cada m bits, pero si se trocea en varias partes más pequeñas, parecerá que la sucesión de subsecuencias es realmente aleatoria (obviamente cuanto más grande sea m , más aleatoria parecerá).

Una forma fácil de crear una PRBS consiste en hacer uso de un registro de desplazamiento en el que algunos bits realimentan (tras pasar por una XOR o una XNOR) al bit más significativo. La Figura 1 ilustra esta idea, en donde los elementos X_i son bits inicializados con un valor denominado *semilla*. La salida del sistema es una secuencia denominada PN (*Pseudo-Noise*) o PRN (*Pseudo-Random Noise*) que está constituida por el vector de bits X_i .

Atención: el registro mostrado en la Figura 1 genera números aleatorios pero no tiene período máximo (sólo para el caso de 4 bits). Para obtener un período máximo, habría que crear el registro utilizando puertas XNOR siguiendo las indicaciones de la tabla incluida al final de esta práctica.

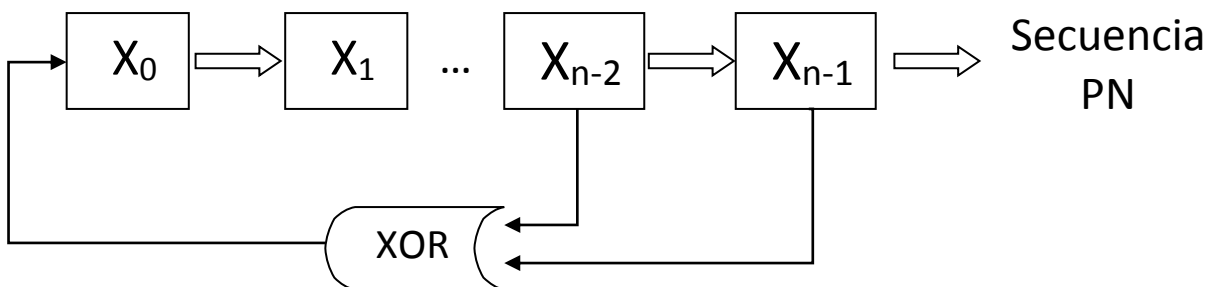


Figura 1: ejemplo de registro PRBS.

Si en lugar de coger el vector de bits se utiliza directamente la secuencia PN bit a bit (usando como salida X_{n-1}), se puede determinar si ésta es pseudo-aleatoria a través de la autocorrelación:

Dada una secuencia de N bits X_i (con i entre 0 y $N-1$), la cual posee m unos y $N-m$ ceros, se dirá que es pseudo-aleatoria cuando su función de autocorrelación

$$AC(v) = \sum_{i=0}^{N-1} X_i X_{i+v}$$

tome únicamente dos valores:

$$AC(v) = \begin{cases} m, & \text{si } v \equiv 0 \pmod{N} \\ \frac{m * (m - 1)}{N - 1}, & \text{en otro caso} \end{cases}$$

Teniendo en cuenta esta información, se pide:

- 1) Crear un nuevo proyecto en ISE (**p5a**) con un módulo VHDL que implementará las funciones requeridas en los apartados 2 y 3.
- 2) Diseñar e implementar la estructura del registro PRBS teniendo en cuenta que se deberá actualizar en cada ciclo de reloj.
- 3) Diseñar e implementar el comportamiento del PRBS, el cual debe seguir el esquema mostrado en la Figura 1 y debe tener una longitud configurable en tiempo de síntesis a través de una constante.
- 4) Crear un **Test Bench** que permita verificar el correcto comportamiento del generador. Con este fin, suponer que se utiliza un reloj a 10 MHz e introducir los estímulos oportunos. Debe de tenerse en cuenta que la semilla será una entrada de tipo BIT_VECTOR, que la secuencia PN se volcará a la salida en una señal que también es de tipo BIT_VECTOR y que se deberán mostrar capturas del funcionamiento del sistema para al menos dos registros PRBS (por ejemplo, de 4 y 32 bits).
- 5) Crear un segundo proyecto en ISE (**p5b**) con un módulo VHDL que implementará únicamente las funcionalidades de los apartados 6 y 7.
- 6) Diseñar e implementar un registro PRBS optimizado para tener ciclo máximo para secuencias de 40 bits.
- 7) Añadir una función que calcule el valor de la autocorrelación para subsecuencias de 4 bits (luego en la fórmula de la autocorrelación, v es igual a 4) sobre la secuencia global de 40 bits. No

es necesario implementar la verificación de si son pseudo-aleatorias. La salida de la autocorrelación debe enlazarse con una señal para poder mostrar el resultado al simular.

8) Crear un **Test Bench** análogo al de (4) que permita observar las secuencias de 40 bits generadas y las salidas de su autocorrelación para subsecuencias de 4 bits.

9) Enviar por correo electrónico (a tiago.fernandez@udc.es) una memoria explicativa breve indicando cómo se ha realizado el diseño (entradas, salidas...) y las pruebas (incluir capturas de las simulaciones que demuestren el buen funcionamiento del sistema). Acompañar la memoria del directorio del proyecto comprimido.

Tabla para creación de registros PRBS de n bits con período máximo.

n	XNOR from	n	XNOR from	n	XNOR from	n	XNOR from
3	3,2	45	45,44,42,41	87	87,74	129	129,124
4	4,3	46	46,45,26,25	88	88,87,17,16	130	130,127
5	5,3	47	47,42	89	89,51	131	131,130,84,83
6	6,5	48	48,47,21,20	90	90,89,72,71	132	132,103
7	7,6	49	49,40	91	91,90,8,7	133	133,132,82,81
8	8,6,5,4	50	50,49,24,23	92	92,91,80,79	134	134,77
9	9,5	51	51,50,36,35	93	93,91	135	135,124
10	10,7	52	52,49	94	94,73	136	136,135,11,10
11	11,9	53	53,52,38,37	95	95,84	137	137,116
12	12,6,4,1	54	54,53,18,17	96	96,94,49,47	138	138,137,131,130
13	13,4,3,1	55	55,31	97	97,91	139	139,136,134,131
14	14,5,3,1	56	56,55,35,34	98	98,87	140	140,111
15	15,14	57	57,50	99	99,97,54,52	141	141,140,110,109
16	16,15,13,4	58	58,39	100	100,63	142	142,121
17	17,14	59	59,58,38,37	101	101,100,95,94	143	143,142,123,122
18	18,11	60	60,59	102	102,101,36,35	144	144,143,75,74
19	19,6,2,1	61	61,60,46,45	103	103,94	145	145,93
20	20,17	62	62,61,6,5	104	104,103,94,93	146	146,145,87,86
21	21,19	63	63,62	105	105,89	147	147,146,110,109
22	22,21	64	64,63,61,60	106	106,91	148	148,121
23	23,18	65	65,47	107	107,105,44,42	149	149,148,40,39
24	24,23,22,17	66	66,65,57,56	108	108,77	150	150,97
25	25,22	67	67,66,58,57	109	109,108,103,102	151	151,148
26	26,6,2,1	68	68,59	110	110,109,98,97	152	152,151,87,86
27	27,5,2,1	69	69,67,42,40	111	111,101	153	153,152
28	28,25	70	70,69,55,54	112	112,110,69,67	154	154,152,27,25
29	29,27	71	71,65	113	113,104	155	155,154,124,123
30	30,6,4,1	72	72,66,25,19	114	114,113,33,32	156	156,155,41,40
31	31,28	73	73,48	115	115,114,101,100	157	157,156,131,130
32	32,22,2,1	74	74,73,59,58	116	116,115,46,45	158	158,157,132,131
33	33,20	75	75,74,65,64	117	117,115,99,97	159	159,128
34	34,27,2,1	76	76,75,41,40	118	118,85	160	160,159,142,141
35	35,33	77	77,76,47,46	119	119,111	161	161,143
36	36,25	78	78,77,59,58	120	120,113,9,2	162	162,161,75,74
37	37,5,4,3,2,1	79	79,70	121	121,103	163	163,162,104,103
38	38,6,5,1	80	80,79,43,42	122	122,121,63,62	164	164,163,151,150
39	39,35	81	81,77	123	123,121	165	165,164,135,134
40	40,38,21,19	82	82,79,47,44	124	124,87	166	166,165,128,127
41	41,38	83	83,82,38,37	125	125,124,18,17	167	167,161
42	42,41,20,19	84	84,71	126	126,125,90,89	168	168,166,153,151
43	43,42,38,37	85	85,84,58,57	127	127,126		
44	44,43,18,17	86	86,85,74,73	128	128,126,101,99		