Linear Feedback Shift Register Taps

This table lists the appropriate taps for maximum-length LFSR counters of up to 168 bits. The basic description and the table for the first 40 bits was originally published in XCELL and reprinted on page 9-24 of the 1993 and 1994 Xilinx Data Books.

Responding to repeated requests, the list is here extended to 168 bits. This information is based on unpublished research done by Wayne Stahnke while he was at Fairchild Semiconductor in 1970.

Table 3: Taps for Maximum-Length LFSR Counters

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		

LFSR Counters, 3 to 168 Bits

Conventional binary counters use complex or wide fan-in logic to generate high end carry signals. A much simpler structure sacrifices the binary count sequence, but achieves very high speed with very simple logic, easily packing two bits into every CLB. Such Linear Feedback Shift-Register (LFSR) counters are also known as pseudo-random sequence generators.

An n-bit LFSR counter can have a maximum sequence length of 2^n-1. In that case, it goes through all possible code permutations except one, which would be a lock-up state. A maximum length n-bit LFSR counter consists of an n-bit shift register with an XNOR in the feedback path from the last output Qn to the first input D1. The XNOR makes the lock-up state the all-ones state; an XOR would make it the all-zeros state. For normal Xilinx applications, all-ones is more easily avoided, since "by default" the flip-flops wake up in the all-zeros state. Table 3 describes the outputs that must be used as inputs of the XNOR. LFSR outputs are traditionally labeled 1 through n, with 1 being the first stage of the shift register, and n being the last stage. This is different from the conventional 0 to (n-1) notation for binary counters. A multi-input XNOR is also known as an even-parity circuit. Note that the connections described in this table are not necessarily unique; certain other connections may also result in maximum length sequences.

Examples

- A 10-bit shift register counts modulo 1023, if the input D1 is driven by the XNOR of Q10 and the bit three positions to the left (Q7), i.e. a one is shifted into D1 when Q10 and Q7 have even parity, which means they are identical.
- An 8-bit shift register counts modulo 255 if the input D1 is driven by the XNOR of Q8, Q6, Q5, Q4, i.e., a one is shifted into D1 if these four outputs have even parity, (four zeros, or two ones, or four ones).

References:

Wayne Stahnke, *Primitive Polynomials Modulo Two*, private communication in 1970, giving the following references:

E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, 1968

P.H.R. Scholefield, *Shift Registers Generating Maximum-Length Sequences,* Electronic Technology, 10-1960, pp. 389-394

S.W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967

E.J. Watson, *Primitive Polynomials (Mod 2)*, Math. Comp. v.16 pp. 368, 1962

N. Zierler and J. Brillhart, *On Primitive Trinomials*, Information and Control v. 13, pp 541-554, 1968, and v. 14, pp. 566-569, 1969

R.W. Marsh, *Table of Irreducible Polynomials*, Dept. of Commerce, October 1957

H. Riesel, *En Bok om Primtal,* Studentlitteratur, Denmark, 1968

M. Kraitchik, *Théorie dés Nombres*, Gauthier-Villars, Paris, 1922 and 1952

M. Kraitchik, *On the Factorization of* $2^n \pm 1$, Scripta Mathematica, v. 18, pp. 39-52, 1952

J. Brillhart, *Miscellaneous Factorizations*, Math. Comp., v. 17 pp. 447-450, 1963

J. Brillhart and J.L.Selfridge, *Factorizations...*, Math. Comp., v. 21, pp. 87-96, 1967

K.R. Isemonger, *Additional Factorizations...*, Math. Comp., v. 19, pp. 145-146, 1965

R.M. Robinson, *Some Factorizations...*, Math. Comp., v. 11, pp. 265-268, 1957

The Programmable Logic Company℠

Headquarters

Xilinx, Inc.
2100 Logic Drive
San Jose, CA 95124
U.S.A.

Tel: 1 (800) 255-7778
or 1 (408) 559-7778
Fax: 1 (800) 559-7114

Net: hotline@xilinx.com
Web: http://www.xilinx.com