ISSN 1172-496X (Print)
ISSN 1172-4234 (Online)

TECHNICAL REPORTS FROM THE ELECTRONICS GROUP
AT THE UNIVERSITY OF OTAGO

Table of Linear Feedback Shift Registers

by

Roy Ward, Timothy C.A. Molteno

ELECTRONICS TECHNICAL
REPORT No. 2012-1

UNIVERSITY OF OTAGO
DUNEDIN, NEW ZEALAND

Online version has
URL: `http://www.physics.otago.ac.nz/reports/electronics/ETR2012-1.pdf`
The author has homepage: `http://www.physics.otago.ac.nz/people/molteno`
E-mail: `tim@physics.otago.ac.nz`
Address: Physics Department, University of Otago, P.O. Box 56, Dunedin, New Zealand

Electronics Group at Otago

In 1987 Millman and Grabel discarded the historical definition of 'electronics' as the science and technology of the motion of charges, preferring instead the operational definition that the primary concern of people doing electronics is *information processing*. This makes a distinction from *energy processing* practiced in the rest of electrical engineering. The act of information processing is what gets electronics practicioners invloved in the fours 'C's: communication, computation, control, and components. This practical definition seems to describe well the activities within the Electronics Group in the Physics Department at the University of Otago, and the range of topics covered in this technical report series.

In June 2012, research within the Electronics Group include projects on algorithms for sequential inference, lightweight GPS tags for birds, development of radio telescopes, analysis of networks of random resistors, electrical impedance imaging, calibration of numerical models for geothermal fields using Bayesian inference, modelling and sampling of Gaussian processes, and efficient algorithms for Markov chain Monte Carlo applied to inverse problems.

Table of Linear Feedback Shift Registers

Roy Ward, Timothy C.A. Molteno

Abstract

Tables of maximum-cycle Linear Feedback Shift Register (LFSR) taps currently exist in the literature up to $n = 168$ [2]. In this report, we describe a method for generating maximum-cycle Linear Feedback Shift Register designs. It is used to generate n-stage designs, with minimum number of taps, for all $n \leq 786$ as well as $n = 1024$ and $n = 2048$. These designs are included in this report. This method is computationally efficient, and in addition, can be extended to search for other, non-LFSR, cyclic sequence generators.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

A Linear Feedback Shift Registers (LFSR) is a shift register where either the outputs of several registers are XORed to provide the input bit to be shifted in (Fibonacci) or where the bit shifted out is XORed to the inputs of several registers (Galois) [6]. The two types are equivalent, so we shall only consider Galois shift registers, as they have a smaller depth (one XOR gate).

We specify a Galois LFSR design by the position of the taps. The taps are the positions (the rightmost position is position 1) of the XOR gates. A tap at position i in an n-stage LFSR would indicate that, at each iteration, the shifted output of the first register would be XORed with the output of the ith register and fed into the input of the next register (at position $(i-1)$). An n-stage LFSR with a cycle of length $2^n - 1$ is called a maximum-cycle LFSR. Figure 1.1 shows an 8-stage maximum-cycle LFSR with taps at position 8,6,5 and 4.

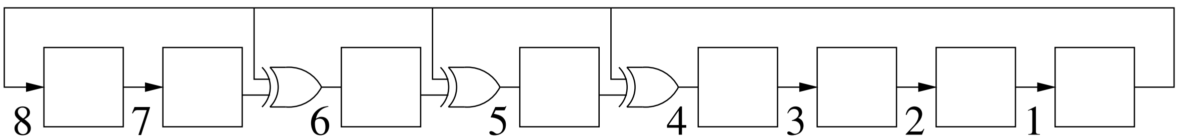

Figure 1.1. An 8-stage Galois LFSR with cycle size 255. This LFSR has taps at positions 8,6,5 and 4.

Alfke [2] presents a table of maximum-cycle n-stage LFSR designs for values of $n \leq 168$. This is the largest table in the literature. Clark and Weng [4] for example, show that a shift register can be constructed from its corresponding polynomial. An LFSR will be a maximum-cycle LFSR if and only if the the polynomial represented by the position of the taps is primitive. For instance, $x^8 + x^6 + x^5 + x^4 + 1$ is a primitive polynomial representing the LFSR 8,6,5,4. Ahmad et. al [1] describe a polynomial-based method to generate maximum-cycle LFSR designs. Their algorithm is designed to find all maximum-cycle LFSR designs and is less efficient than the one presented here for evaluating candidate LFSR designs. It has, to our knowledge, not been applied to values of n greater than 10.

In this paper, we describe a matrix method for generating large n-stage maximum-cycle LFSR designs. This method is efficient, and has been used to generate maximum-cycle LFSR taps for all $n \leq 786$ as well as $n = 1024$ and $n = 2048$ [?]. It is feasible to use this method for all values of n where the prime factors of the corresponding Mersenne number $2^n - 1$ are known. The matrix method we describe can also be extended to search for other, non-LFSR, cyclic sequence generators.

1.1 Representation of LFSRs

The state of an LFSR is a n-vector of 0's and 1's. Motivated by the treatment of Wang et al. [7], an n-stage LFSR can be represented as an $n \times n$ matrix $\mathbf{M}$. Iteration of the LFSR involves multiplication of $\mathbf{M}$ by the current state vector, $\boldsymbol{v}_i$ yielding the next state vector, $\boldsymbol{v}_{i+1}$, i.e.,

$$\boldsymbol{v}_{i+1} = \mathbf{M}\boldsymbol{v}_i.$$

The ith iteration from an initial state $\boldsymbol{v}_0$ can be found by calculating $\mathbf{M}^i$, i.e.,

$$\boldsymbol{v}_i = \mathbf{M}^i \boldsymbol{v}_0.$$

The matrices, $\mathbf{M}$ that represent LFSRs, have the form

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & a_n \\ 1 & 0 & 0 & \dots & 0 & a_{n-1} \\ 0 & 1 & 0 & \dots & 0 & a_{n-2} \\ 0 & 0 & 1 & \dots & 0 & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & a_1 \end{pmatrix}$$

where $a_i = 1$ if a tap is present at the ith position, and $a_i = 0$ otherwise. Note that $a_n = 1$ always.

1.1.1 Cycles

An LFSR has a cycle of length l from a state $\boldsymbol{v}$ if after l iterations, the LFSR returns to the state $\boldsymbol{v}$, i.e.,

$$\mathbf{M}^l \boldsymbol{v} = \boldsymbol{v} \tag{1.1}$$

This is *not* equivalent to $\mathbf{M}^{l-1} = \mathbf{I}$, where $\mathbf{I}$ is the $n \times n$ identity matrix. This is because an LFSR with an l-cycle, may do so starting only from a subset of the possible LFSR states – other starting states might exhibit l'-cyclic behaviour with length $l' \neq l$ where l and l' are not factors of each other.

An example of this is the 8-stage LFSR with taps at positions 8 and 3. Depending on which starting state is chosen, this design has a cycles of size 217,31,7 and 1 A starting state for the 217-cycle is $\{1, 0, 0, 0, 0, 0, 0, 0\}$, a starting state for the 31-cycle is $\{1, 0, 0, 0, 0, 0, 0, 1\}$, a starting state for the 7-cycle is $\{1, 0, 1, 1, 0, 0, 1, 1\}$ and the starting state for the 1-cycle is $\{0, 0, 0, 0, 0, 0, 0, 0\}$. The existence of the 7-cycle means that $\mathbf{M}^{31-1} \neq \mathbf{I}$.

1.1.2 Maximum-cycle LFSRs

If an n-stage LFSR is a *maximum-cycle* LFSR, then all 2^n-1 non-zero states of that LFSR will be visited as the LFSR is iterated. It follows that the condition for an l-cycle (Equation 1.1) becomes independent of the initial state $\boldsymbol{v}$ when $l = 2^n-1$. Therefore Equation 1.1 becomes

$$\mathbf{M}^{2^n-1} = \mathbf{I}. \tag{1.2}$$

Additionally, an LFSR is a maximum-cycle LFSR if there are no smaller cycles, i.e.,

$$\forall k \in \mathbb{Z} : 1 \leq k < 2^n-1,\ \mathbf{M}^k \neq \mathbf{I} \tag{1.3}$$

1.2 Finding Maximum-Cycle LFSRs

The task of finding a maximum-cycle LFSR can be reduced to the task of finding a LFSR matrix $\mathbf{M}$, such that Equation 1.2 and Equation 1.3 hold. At first glance, it seems that to determine whether Equation 1.3 holds, requires a search over all the possible values of k. The computational complexity of such a brute-force search is order $n^3 2^n$ and becomes prohibitive for large values of n. We show in the next section how this search can be significantly pruned.

1.2.1 Pruning the search tree

The 2^n-2 tests in Equation 1.3, for a 2^n-1-cycle LFSR to have no smaller cycles, can be reduced to only testing factors of 2^n-1.

Consider the set, K, of positive integers that satisfy $\mathbf{M}^k = \mathbf{I}$,

$$K = \{k : 1 \leq k \leq 2^n-1, \mathbf{M}^k = \mathbf{I}\}.$$

Assume that there is a cycle with length less than 2^n-1. The set K will have elements less than 2^n-1. Let the smallest such element be k_0. All multiples if k_0 will also satisfy $matrix M^k = \mathbf{I}$, i.e., for all positive integers $j \in \mathbb{Z}, \mathbf{M}^{jk_0} = \mathbf{I}$.

Assume that there exists $k_x \in K$ where k_x is not a multiple of k_0 and where $\mathbf{M}^{k_x} = \mathbf{I}$ then we can write,

$$k_x = jk_0 + t$$

for some integer $j > 0$ where $0 < t < k_0$. It follows that

$$\mathbf{M}^{k_x} = \mathbf{M}^{jk_0+t} = \mathbf{M}^{jk_0}\mathbf{M}^t = \mathbf{M}^t$$

however by assumption $\mathbf{M}^{k_x} = \mathbf{I}$, so $\mathbf{M}^t = \mathbf{I}$ which violates our assumption that k_0 is the smallest such value. Hence all elements of K must be multiples of k_0.

In a maximal-cycle LFSR Equation 1.2 holds, and $\mathbf{M}^{2^n-1} = \mathbf{I}$ so we know that k_0 must be a factor of 2^n-1. Therefore only values of k that are factors of 2^n-1 need to be checked in order to establish that Equation 1.3 holds.

1.2.2 Prime Factorisation

A further improvement is still possible by considering the prime factorisation of 2^n-1,

$$2^n-1 = \prod_{i=1}^{m} p_i^{k_i},$$

where m is the number of prime factors and the p_i are the prime factors. Any factor of 2^n-1 except 2^n-1 itself is a factor of $\frac{2^n-1}{p_i}$ for some i, so to establish that Equation 1.3 holds, we only need to check that

$$\forall i \in \{1,\ldots,m\},\ \mathbf{M}^{\frac{2^n-1}{p_i}} \neq \mathbf{I}. \tag{1.4}$$

Thus, if a prime factorisation of 2^n-1 is available then we only need to search as many values of k as there are prime factors and Equation 1.2 can be shown to hold with a relatively small amount of computational effort. As there must be fewer than n factors of 2^n-1 this search can be done in polynomial time.

The numbers 2^n-1 are known as Mersenne numbers [3]. Implementation of the algorithm described in Equation 1.4 requires a table of the prime factors of Mersenne numbers. A table of all prime factors of the Mersenne numbers $M(n)$ for values of n up to $n = 786$ was generated and is available in machine readable form from Reference [5].

1.2.3 The search algorithm

The search for an n-stage maximum-cycle LFSR is performed by considering all potential designs in order of increasing tap number. Ahmad et. al [1] show in their Theorem 4, that an n-stage LFSR design must have an even number of taps in order to be maximum-cycle. Therefore, our algorithm starts with a search for possible two-tap designs. Each two-tap design with taps at positions i and j is represented by a matrix $\mathbf{M}_{i,j}$. The first tap is always at position $i = n$ and represents the feedback from bit 1 to bit n.The two-tap search must check LFSRs with the second tap at positions $n/2 \leq j < n$ (since, if $\mathbf{M}_{n,i_1,\ldots,i_k}$ is an LFSR, then $\mathbf{M}_{n,n-i_k,\ldots,n-i_1}$ is an LFSR with the same cyclic properties; reflected bit-order and reversed in time). For each pair of tap positions, i, j, Equation 1.2 is checked, and if this test is satisfied, the candidate LFSR design is checked against Equation 1.4 using the prime factors of 2^n-1.

If no two-tap designs are found a four-tap design search is conducted. Once again, the first tap position is n, and a search over the remaining three tap positions is carried out. For each candidate design $\mathbf{M}_{i,j,k,l}$, the same tests are done.

The pseudocode for this algorithm, showing the order in which the candidate designs are searched, is shown below.

```
boolean test(M)
    let {p1...pm} = prime factors of 2^n-1;
    if (M^(2^n-1) = I)
```

```
        if (∀p_i ∈ {p_1...p_m}, M^((2^n−1)/p_i) ≠ I)
            return true;
    return false;

// Two-tap case
for j = {n−1 ... n/2}
    if (test(M_{n,j}))
        return (n,j);

// Four-tap case
for l = {n−1 ... n/2}
    for j = {n−1 ... l+1}
        for k = {l−1 ... j+1}
            if (test(M_{n,j,k,l}))
                return (n,j,k,l);
```

Chapter 2

Table of LFSR Taps

Table 2.1: Shift Registers with Cycle Size $2^n - 1$

n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4
2	2, 1		24		24, 23, 21, 20	46		46, 40, 39, 38
3	3, 2		25	25, 22	25, 24, 23, 22	47	47, 42	47, 46, 43, 42
4	4, 3		26		26, 25, 24, 20	48		48, 44, 41, 39
5	5, 3	5, 4, 3, 2	27		27, 26, 25, 22	49	49, 40	49, 45, 44, 43
6	6, 5	6, 5, 3, 2	28	28, 25	28, 27, 24, 22	50		50, 48, 47, 46
7	7, 6	7, 6, 5, 4	29	29, 27	29, 28, 27, 25	51		51, 50, 48, 45
8		8, 6, 5, 4	30		30, 29, 26, 24	52	52, 49	52, 51, 49, 46
9	9, 5	9, 8, 6, 5	31	31, 28	31, 30, 29, 28	53		53, 52, 51, 47
10	10, 7	10, 9, 7, 6	32		32, 30, 26, 25	54		54, 51, 48, 46
11	11, 9	11, 10, 9, 7	33	33, 20	33, 32, 29, 27	55	55, 31	55, 54, 53, 49
12		12, 11, 8, 6	34		34, 31, 30, 26	56		56, 54, 52, 49
13		13, 12, 10, 9	35	35, 33	35, 34, 28, 27	57	57, 50	57, 55, 54, 52
14		14, 13, 11, 9	36	36, 25	36, 35, 29, 28	58	58, 39	58, 57, 53, 52
15	15, 14	15, 14, 13, 11	37		37, 36, 33, 31	59		59, 57, 55, 52
16		16, 14, 13, 11	38		38, 37, 33, 32	60	60, 59	60, 58, 56, 55
17	17, 14	17, 16, 15, 14	39	39, 35	39, 38, 35, 32	61		61, 60, 59, 56
18	18, 11	18, 17, 16, 13	40		40, 37, 36, 35	62		62, 59, 57, 56
19		19, 18, 17, 14	41	41, 38	41, 40, 39, 38	63	63, 62	63, 62, 59, 58
20	20, 17	20, 19, 16, 14	42		42, 40, 37, 35	64		64, 63, 61, 60
21	21, 19	21, 20, 19, 16	43		43, 42, 38, 37	65	65, 47	65, 64, 62, 61
22	22, 21	22, 19, 18, 17	44		44, 42, 39, 38	66		66, 60, 58, 57
23	23, 18	23, 22, 20, 18	45		45, 44, 42, 41	67		67, 66, 65, 62
68	68, 59	68, 67, 63, 61	120		120, 118, 114, 111	172	172, 165	172, 169, 165, 161
69		69, 67, 64, 63	121	121, 103	121, 120, 116, 113	173		173, 171, 168, 165
70		70, 69, 67, 65	122		122, 121, 120, 116	174	174, 161	174, 169, 166, 165
71	71, 65	71, 70, 68, 66	123	123, 121	123, 122, 119, 115	175	175, 169	175, 173, 171, 169
72		72, 69, 63, 62	124	124, 87	124, 119, 118, 117	176		176, 167, 165, 164
73	73, 48	73, 71, 70, 69	125		125, 120, 119, 118	177	177, 169	177, 175, 174, 172
74		74, 71, 70, 67	126		126, 124, 122, 119	178	178, 91	178, 176, 171, 170
75		75, 74, 72, 69	127	127, 126	127, 126, 124, 120	179		179, 178, 177, 175
76		76, 74, 72, 71	128		128, 127, 126, 121	180		180, 173, 170, 168
77		77, 75, 72, 71	129	129, 124	129, 128, 125, 124	181		181, 180, 175, 174
78		78, 77, 76, 71	130	130, 127	130, 129, 128, 125	182		182, 181, 176, 174
79	79, 70	79, 77, 76, 75	131		131, 129, 128, 123	183	183, 127	183, 179, 176, 175

Continued ...

n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4
80		80, 78, 76, 71	132	132, 103	132, 130, 127, 123	184		184, 177, 176, 175
81	81, 77	81, 79, 78, 75	133		133, 131, 125, 124	185	185, 161	185, 184, 182, 177
82		82, 78, 76, 73	134	134, 77	134, 133, 129, 127	186		186, 180, 178, 177
83		83, 81, 79, 76	135	135, 124	135, 132, 131, 129	187		187, 182, 181, 180
84	84, 71	84, 83, 77, 75	136		136, 134, 133, 128	188		188, 186, 183, 182
85		85, 84, 83, 77	137	137, 116	137, 136, 133, 126	189		189, 187, 184, 183
86		86, 84, 81, 80	138		138, 137, 131, 130	190		190, 188, 184, 177
87	87, 74	87, 86, 82, 80	139		139, 136, 134, 131	191	191, 182	191, 187, 185, 184
88		88, 80, 79, 77	140	140, 111	140, 139, 136, 132	192		192, 190, 178, 177
89	89, 51	89, 86, 84, 83	141		141, 140, 135, 128	193	193, 178	193, 189, 186, 184
90		90, 88, 87, 85	142	142, 121	142, 141, 139, 132	194	194, 107	194, 192, 191, 190
91		91, 90, 86, 83	143		143, 141, 140, 138	195		195, 193, 192, 187
92		92, 90, 87, 86	144		144, 142, 140, 137	196		196, 194, 187, 185
93	93, 91	93, 91, 90, 87	145	145, 93	145, 144, 140, 139	197		197, 195, 193, 188
94	94, 73	94, 93, 89, 88	146		146, 144, 143, 141	198	198, 133	198, 193, 190, 183
95	95, 84	95, 94, 90, 88	147		147, 145, 143, 136	199	199, 165	199, 198, 195, 190
96		96, 90, 87, 86	148	148, 121	148, 145, 143, 141	200		200, 198, 197, 195
97	97, 91	97, 95, 93, 91	149		149, 142, 140, 139	201	201, 187	201, 199, 198, 195
98	98, 87	98, 97, 91, 90	150	150, 97	150, 148, 147, 142	202	202, 147	202, 198, 196, 195
99		99, 95, 94, 92	151	151, 148	151, 150, 149, 148	203		203, 202, 196, 195
100	100, 63	100, 98, 93, 92	152		152, 150, 149, 146	204		204, 201, 200, 194
101		101, 100, 95, 94	153	153, 152	153, 149, 148, 145	205		205, 203, 200, 196
102		102, 99, 97, 96	154		154, 153, 149, 145	206		206, 201, 197, 196
103	103, 94	103, 102, 99, 94	155		155, 151, 150, 148	207	207, 164	207, 206, 201, 198
104		104, 103, 94, 93	156		156, 153, 151, 147	208		208, 207, 205, 199
105	105, 89	105, 104, 99, 98	157		157, 155, 152, 151	209	209, 203	209, 207, 206, 204
106	106, 91	106, 105, 101, 100	158		158, 153, 152, 150	210		210, 207, 206, 198
107		107, 105, 99, 98	159	159, 128	159, 156, 153, 148	211		211, 203, 201, 200
108	108, 77	108, 103, 97, 96	160		160, 158, 157, 155	212	212, 107	212, 209, 208, 205
109		109, 107, 105, 104	161	161, 143	161, 159, 158, 155	213		213, 211, 208, 207
110		110, 109, 106, 104	162		162, 158, 155, 154	214		214, 213, 211, 209
111	111, 101	111, 109, 107, 104	163		163, 160, 157, 156	215	215, 192	215, 212, 210, 209
112		112, 108, 106, 101	164		164, 159, 158, 152	216		216, 215, 213, 209
113	113, 104	113, 111, 110, 108	165		165, 162, 157, 156	217	217, 172	217, 213, 212, 211
114		114, 113, 112, 103	166		166, 164, 163, 156	218	218, 207	218, 217, 211, 210
115		115, 110, 108, 107	167	167, 161	167, 165, 163, 161	219		219, 218, 215, 211
116		116, 114, 111, 110	168		168, 162, 159, 152	220		220, 211, 210, 208
117		117, 116, 115, 112	169	169, 135	169, 164, 163, 161	221		221, 219, 215, 213
118	118, 85	118, 116, 113, 112	170	170, 147	170, 169, 166, 161	222		222, 220, 217, 214
119	119, 111	119, 116, 111, 110	171		171, 169, 166, 165	223	223, 190	223, 221, 219, 218
224		224, 222, 217, 212	276		276, 275, 273, 270	328		328, 323, 321, 319
225	225, 193	225, 224, 220, 215	277		277, 274, 271, 265	329	329, 279	329, 326, 323, 321
226		226, 223, 219, 216	278	278, 273	278, 277, 274, 273	330		330, 328, 323, 322
227		227, 223, 218, 217	279	279, 274	279, 278, 275, 274	331		331, 329, 325, 321
228		228, 226, 217, 216	280		280, 278, 275, 271	332	332, 209	332, 325, 321, 320
229		229, 228, 225, 219	281	281, 188	281, 280, 277, 272	333	333, 331	333, 331, 329, 325
230		230, 224, 223, 222	282	282, 247	282, 278, 277, 272	334		334, 333, 330, 327

Continued . . .

n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4
231	231, 205	231, 229, 227, 224	283		283, 278, 276, 271	335		335, 333, 328, 325
232		232, 228, 223, 221	284	284, 165	284, 279, 278, 276	336		336, 335, 332, 329
233	233, 159	233, 232, 229, 224	285		285, 280, 278, 275	337	337, 282	337, 336, 331, 327
234	234, 203	234, 232, 225, 223	286	286, 217	286, 285, 276, 271	338		338, 336, 335, 332
235		235, 234, 229, 226	287	287, 216	287, 285, 282, 281	339		339, 332, 329, 323
236	236, 231	236, 229, 228, 226	288		288, 287, 278, 277	340		340, 337, 336, 329
237		237, 236, 233, 230	289	289, 268	289, 286, 285, 277	341		341, 336, 330, 327
238		238, 237, 236, 233	290		290, 288, 287, 285	342	342, 217	342, 341, 340, 331
239	239, 203	239, 238, 232, 227	291		291, 286, 280, 279	343	343, 268	343, 338, 335, 333
240		240, 237, 235, 232	292	292, 195	292, 291, 289, 285	344		344, 338, 334, 333
241	241, 171	241, 237, 233, 232	293		293, 292, 287, 282	345	345, 323	345, 343, 341, 337
242		242, 241, 236, 231	294	294, 233	294, 292, 291, 285	346		346, 344, 339, 335
243		243, 242, 238, 235	295	295, 247	295, 293, 291, 290	347		347, 344, 337, 336
244		244, 243, 240, 235	296		296, 292, 287, 285	348		348, 344, 341, 340
245		245, 244, 241, 239	297	297, 292	297, 296, 293, 292	349		349, 347, 344, 343
246		246, 245, 244, 235	298		298, 294, 290, 287	350	350, 297	350, 340, 337, 336
247	247, 165	247, 245, 243, 238	299		299, 295, 293, 288	351	351, 317	351, 348, 345, 343
248		248, 238, 234, 233	300	300, 293	300, 290, 288, 287	352		352, 346, 341, 339
249	249, 163	249, 248, 245, 242	301		301, 299, 296, 292	353	353, 284	353, 349, 346, 344
250	250, 147	250, 247, 245, 240	302	302, 261	302, 297, 293, 290	354		354, 349, 341, 340
251		251, 249, 247, 244	303		303, 297, 291, 290	355		355, 354, 350, 349
252	252, 185	252, 251, 247, 241	304		304, 303, 302, 293	356		356, 349, 347, 346
253		253, 252, 247, 246	305	305, 203	305, 303, 299, 298	357		357, 355, 347, 346
254		254, 253, 252, 247	306		306, 305, 303, 299	358		358, 351, 350, 344
255	255, 203	255, 253, 252, 250	307		307, 305, 303, 299	359	359, 291	359, 358, 352, 350
256		256, 254, 251, 246	308		308, 306, 299, 293	360		360, 359, 335, 334
257	257, 245	257, 255, 251, 250	309		309, 307, 302, 299	361		361, 360, 357, 354
258	258, 175	258, 254, 252, 249	310		310, 309, 305, 302	362	362, 299	362, 360, 351, 344
259		259, 257, 253, 249	311		311, 308, 306, 304	363		363, 362, 356, 355
260		260, 253, 252, 250	312		312, 307, 302, 301	364	364, 297	364, 363, 359, 352
261		261, 257, 255, 254	313	313, 234	313, 312, 310, 306	365		365, 360, 359, 356
262		262, 258, 254, 253	314	314, 299	314, 311, 305, 300	366	366, 337	366, 362, 359, 352
263	263, 170	263, 261, 258, 252	315		315, 314, 306, 305	367	367, 346	367, 365, 363, 358
264		264, 263, 255, 254	316	316, 181	316, 309, 305, 304	368		368, 361, 359, 351
265	265, 223	265, 263, 262, 260	317		317, 315, 313, 310	369	369, 278	369, 367, 359, 358
266	266, 219	266, 265, 260, 259	318		318, 313, 312, 310	370	370, 231	370, 368, 367, 365
267		267, 264, 261, 259	319	319, 283	319, 318, 317, 308	371		371, 369, 368, 363
268	268, 243	268, 267, 264, 258	320		320, 319, 317, 316	372		372, 369, 365, 357
269		269, 268, 263, 262	321	321, 290	321, 319, 316, 314	373		373, 371, 366, 365
270	270, 217	270, 267, 263, 260	322	322, 255	322, 321, 320, 305	374		374, 369, 368, 366
271	271, 213	271, 265, 264, 260	323		323, 322, 320, 313	375	375, 359	375, 374, 368, 367
272		272, 270, 266, 263	324		324, 321, 320, 318	376		376, 371, 369, 368
273	273, 250	273, 272, 271, 266	325		325, 323, 320, 315	377	377, 336	377, 376, 374, 369
274	274, 207	274, 272, 267, 265	326		326, 325, 323, 316	378	378, 335	378, 374, 365, 363
275		275, 266, 265, 264	327	327, 293	327, 325, 322, 319	379		379, 375, 370, 369
380	380, 333	380, 377, 374, 366	432		432, 429, 428, 419	484	484, 379	484, 483, 482, 470
381		381, 380, 379, 376	433	433, 400	433, 430, 428, 422	485		485, 479, 469, 468

Continued ...

n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4
382	382, 301	382, 379, 375, 364	434		434, 429, 423, 422	486		486, 481, 478, 472
383	383, 293	383, 382, 378, 374	435		435, 430, 426, 423	487	487, 393	487, 485, 483, 478
384		384, 378, 369, 368	436	436, 271	436, 432, 431, 430	488		488, 487, 485, 484
385	385, 379	385, 383, 381, 379	437		437, 436, 435, 431	489	489, 406	489, 484, 483, 480
386	386, 303	386, 381, 380, 376	438	438, 373	438, 436, 432, 421	490	490, 271	490, 485, 483, 481
387		387, 385, 379, 378	439	439, 390	439, 437, 436, 431	491		491, 488, 485, 480
388		388, 387, 385, 374	440		440, 439, 437, 436	492		492, 491, 485, 484
389		389, 384, 380, 379	441	441, 410	441, 440, 433, 430	493		493, 490, 488, 483
390	390, 301	390, 388, 380, 377	442		442, 440, 437, 435	494	494, 357	494, 493, 489, 481
391	391, 363	391, 390, 389, 385	443		443, 442, 437, 433	495	495, 419	495, 494, 486, 480
392		392, 386, 382, 379	444		444, 435, 432, 431	496		496, 494, 491, 480
393	393, 386	393, 392, 391, 386	445		445, 441, 439, 438	497	497, 419	497, 493, 488, 486
394	394, 259	394, 392, 387, 386	446	446, 341	446, 442, 439, 431	498		498, 495, 489, 487
395		395, 390, 389, 384	447	447, 374	447, 446, 441, 438	499		499, 494, 493, 488
396	396, 371	396, 392, 390, 389	448		448, 444, 442, 437	500		500, 499, 494, 490
397		397, 392, 387, 385	449	449, 315	449, 446, 440, 438	501		501, 499, 497, 496
398		398, 393, 392, 384	450	450, 371	450, 443, 438, 434	502		502, 498, 497, 494
399	399, 313	399, 397, 390, 388	451		451, 450, 441, 435	503	503, 500	503, 502, 501, 500
400		400, 398, 397, 395	452		452, 448, 447, 446	504		504, 502, 490, 483
401	401, 249	401, 399, 392, 389	453		453, 449, 447, 438	505	505, 349	505, 500, 497, 493
402		402, 399, 398, 393	454		454, 449, 445, 444	506	506, 411	506, 501, 494, 491
403		403, 398, 395, 394	455	455, 417	455, 453, 449, 444	507		507, 504, 501, 494
404	404, 215	404, 400, 398, 397	456		456, 454, 445, 433	508	508, 399	508, 505, 500, 495
405		405, 398, 397, 388	457	457, 441	457, 454, 449, 446	509		509, 506, 502, 501
406	406, 249	406, 402, 397, 393	458	458, 255	458, 453, 448, 445	510		510, 501, 500, 498
407	407, 336	407, 402, 400, 398	459		459, 457, 454, 447	511	511, 501	511, 509, 503, 501
408		408, 407, 403, 401	460	460, 399	460, 459, 455, 451	512		512, 510, 507, 504
409	409, 322	409, 406, 404, 402	461		461, 460, 455, 454	513	513, 428	513, 505, 503, 500
410		410, 407, 406, 400	462	462, 389	462, 457, 451, 450	514		514, 511, 509, 507
411		411, 408, 401, 399	463	463, 370	463, 456, 455, 452	515		515, 511, 508, 501
412	412, 265	412, 409, 404, 401	464		464, 460, 455, 441	516		516, 514, 511, 509
413		413, 407, 406, 403	465	465, 406	465, 463, 462, 457	517		517, 515, 507, 505
414		414, 405, 401, 398	466		466, 460, 455, 452	518	518, 485	518, 516, 515, 507
415	415, 313	415, 413, 411, 406	467		467, 466, 461, 456	519	519, 440	519, 517, 511, 507
416		416, 414, 411, 407	468		468, 464, 459, 453	520		520, 509, 507, 503
417	417, 310	417, 416, 414, 407	469		469, 467, 464, 460	521	521, 489	521, 519, 514, 512
418		418, 417, 415, 403	470	470, 321	470, 468, 462, 461	522		522, 518, 509, 507
419		419, 415, 414, 404	471	471, 470	471, 469, 468, 465	523		523, 521, 517, 510
420		420, 412, 410, 407	472		472, 470, 469, 461	524	524, 357	524, 523, 519, 515
421		421, 419, 417, 416	473		473, 470, 467, 465	525		525, 524, 521, 519
422	422, 273	422, 421, 416, 412	474	474, 283	474, 465, 463, 456	526		526, 525, 521, 517
423	423, 398	423, 420, 418, 414	475		475, 471, 467, 466	527	527, 480	527, 526, 520, 518
424		424, 422, 417, 415	476	476, 461	476, 475, 468, 466	528		528, 526, 522, 517
425	425, 413	425, 422, 421, 418	477		477, 470, 462, 461	529	529, 487	529, 528, 525, 522
426		426, 415, 414, 412	478	478, 357	478, 477, 474, 472	530		530, 527, 523, 520
427		427, 422, 421, 416	479	479, 375	479, 475, 472, 470	531		531, 529, 525, 519
428	428, 323	428, 426, 425, 417	480		480, 473, 467, 464	532	532, 531	532, 529, 528, 522

Continued ...

n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4
429		429, 422, 421, 419	481	481, 343	481, 480, 472, 471	533		533, 531, 530, 529
430		430, 419, 417, 415	482		482, 477, 476, 473	534		534, 533, 529, 527
431	431, 311	431, 430, 428, 426	483		483, 479, 477, 474	535		535, 533, 529, 527
536		536, 533, 531, 529	588	588, 437	588, 577, 572, 571	640		640, 638, 637, 626
537	537, 443	537, 536, 535, 527	589		589, 586, 585, 579	641	641, 630	641, 640, 636, 622
538		538, 537, 536, 533	590	590, 497	590, 588, 587, 578	642	642, 523	642, 636, 633, 632
539		539, 535, 534, 529	591		591, 587, 585, 582	643		643, 641, 640, 632
540	540, 361	540, 537, 534, 529	592		592, 591, 573, 568	644		644, 634, 633, 632
541		541, 537, 531, 528	593	593, 507	593, 588, 585, 584	645		645, 641, 637, 634
542		542, 540, 539, 533	594	594, 575	594, 586, 584, 583	646	646, 397	646, 635, 634, 633
543	543, 527	543, 538, 536, 532	595		595, 594, 593, 586	647	647, 642	647, 646, 643, 642
544		544, 538, 535, 531	596		596, 592, 591, 590	648		648, 647, 626, 625
545	545, 423	545, 539, 537, 532	597		597, 588, 585, 583	649	649, 612	649, 648, 644, 638
546		546, 545, 544, 538	598		598, 597, 592, 591	650	650, 647	650, 644, 635, 632
547		547, 543, 540, 534	599	599, 569	599, 593, 591, 590	651		651, 646, 638, 637
548		548, 545, 543, 538	600		600, 599, 590, 589	652	652, 559	652, 647, 643, 641
549		549, 546, 545, 533	601	601, 400	601, 600, 597, 589	653		653, 646, 645, 643
550	550, 357	550, 546, 533, 529	602		602, 596, 594, 591	654		654, 649, 643, 640
551	551, 416	551, 550, 547, 542	603		603, 600, 599, 597	655	655, 567	655, 653, 639, 638
552		552, 550, 547, 532	604		604, 600, 598, 589	656		656, 646, 638, 637
553	553, 514	553, 550, 549, 542	605		605, 600, 598, 595	657	657, 619	657, 656, 650, 649
554		554, 551, 546, 543	606		606, 602, 599, 591	658	658, 603	658, 651, 648, 646
555		555, 551, 546, 545	607	607, 502	607, 600, 598, 595	659		659, 657, 655, 644
556	556, 403	556, 549, 546, 540	608		608, 606, 602, 585	660		660, 657, 656, 648
557		557, 552, 551, 550	609	609, 578	609, 601, 600, 597	661		661, 657, 650, 649
558		558, 553, 549, 544	610	610, 483	610, 602, 600, 599	662	662, 365	662, 659, 656, 650
559	559, 525	559, 557, 552, 550	611		611, 609, 607, 601	663	663, 406	663, 655, 652, 649
560		560, 554, 551, 549	612		612, 607, 602, 598	664		664, 662, 660, 649
561	561, 490	561, 558, 552, 550	613		613, 609, 603, 594	665	665, 632	665, 661, 659, 654
562		562, 560, 558, 551	614		614, 613, 612, 607	666		666, 664, 659, 656
563		563, 561, 554, 549	615	615, 404	615, 614, 609, 608	667		667, 664, 660, 649
564	564, 401	564, 563, 561, 558	616		616, 614, 602, 597	668		668, 658, 656, 651
565		565, 564, 559, 554	617	617, 417	617, 612, 608, 607	669		669, 667, 665, 664
566	566, 413	566, 564, 561, 560	618		618, 615, 604, 598	670	670, 517	670, 669, 665, 664
567	567, 424	567, 563, 557, 556	619		619, 614, 611, 610	671	671, 656	671, 669, 665, 662
568		568, 558, 557, 551	620		620, 619, 618, 611	672		672, 667, 666, 661
569	569, 492	569, 568, 559, 557	621		621, 616, 615, 609	673	673, 645	673, 666, 664, 663
570	570, 503	570, 563, 558, 552	622	622, 325	622, 612, 610, 605	674		674, 671, 665, 660
571		571, 569, 566, 561	623	623, 555	623, 614, 613, 612	675		675, 674, 672, 669
572		572, 571, 564, 560	624		624, 617, 615, 612	676	676, 435	676, 675, 671, 664
573		573, 569, 567, 563	625	625, 492	625, 620, 617, 613	677		677, 674, 673, 669
574	574, 561	574, 569, 565, 560	626		626, 623, 621, 613	678		678, 675, 673, 663
575	575, 429	575, 572, 570, 569	627		627, 622, 617, 613	679	679, 613	679, 676, 667, 661
576		576, 573, 572, 563	628	628, 405	628, 626, 617, 616	680		680, 679, 650, 645
577	577, 552	577, 575, 574, 569	629		629, 627, 624, 623	681		681, 678, 672, 670
578		578, 562, 556, 555	630		630, 628, 626, 623	682		682, 681, 679, 675
579		579, 572, 570, 567	631	631, 324	631, 625, 623, 617	683		683, 682, 677, 672

Continued ...

n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4	n	LFSR-2	LFSR-4
580		580, 579, 576, 574	632		632, 629, 619, 613	684		684, 681, 671, 666
581		581, 575, 574, 568	633	633, 532	633, 632, 631, 626	685		685, 684, 682, 681
582	582, 497	582, 579, 576, 571	634	634, 319	634, 631, 629, 627	686	686, 489	686, 684, 674, 673
583	583, 453	583, 581, 577, 575	635		635, 631, 625, 621	687	687, 674	687, 682, 675, 673
584		584, 581, 571, 570	636		636, 632, 628, 623	688		688, 682, 674, 669
585	585, 464	585, 583, 582, 577	637		637, 636, 628, 623	689	689, 675	689, 686, 683, 681
586		586, 584, 581, 579	638		638, 637, 633, 632	690		690, 687, 683, 680
587		587, 586, 581, 576	639	639, 623	639, 636, 635, 629	691		691, 689, 685, 678
692	692, 393	692, 687, 686, 678	725		725, 720, 719, 716	758		758, 757, 746, 741
693		693, 691, 685, 678	726	726, 721	726, 725, 722, 721	759	759, 661	759, 757, 756, 750
694		694, 691, 681, 677	727	727, 547	727, 721, 719, 716	760		760, 757, 747, 734
695	695, 483	695, 694, 691, 686	728		728, 726, 725, 724	761	761, 758	761, 760, 759, 758
696		696, 694, 686, 673	729	729, 671	729, 726, 724, 718	762	762, 679	762, 761, 755, 745
697	697, 430	697, 689, 685, 681	730	730, 583	730, 726, 715, 711	763		763, 754, 749, 747
698	698, 483	698, 690, 689, 688	731		731, 729, 725, 723	764		764, 761, 759, 758
699		699, 698, 689, 684	732		732, 729, 728, 725	765		765, 760, 755, 754
700		700, 698, 695, 694	733		733, 731, 726, 725	766		766, 757, 747, 744
701		701, 699, 697, 685	734		734, 724, 721, 720	767	767, 599	767, 763, 760, 759
702	702, 665	702, 701, 699, 695	735	735, 691	735, 733, 728, 727	768		768, 764, 751, 749
703		703, 702, 696, 691	736		736, 730, 728, 723	769	769, 649	769, 763, 762, 760
704		704, 701, 699, 692	737	737, 732	737, 736, 733, 732	770		770, 768, 765, 756
705	705, 686	705, 704, 698, 697	738	738, 391	738, 730, 729, 727	771		771, 765, 756, 754
706		706, 697, 695, 692	739		739, 731, 723, 721	772	772, 765	772, 767, 766, 764
707		707, 702, 699, 692	740	740, 587	740, 737, 728, 716	773		773, 767, 765, 763
708	708, 421	708, 706, 704, 703	741		741, 738, 733, 732	774	774, 589	774, 767, 760, 758
709		709, 708, 706, 705	742		742, 741, 738, 730	775	775, 408	775, 771, 769, 768
710		710, 709, 696, 695	743	743, 653	743, 742, 731, 730	776		776, 773, 764, 759
711	711, 619	711, 704, 703, 700	744		744, 743, 733, 731	777	777, 748	777, 776, 767, 761
712		712, 709, 708, 707	745	745, 487	745, 740, 738, 737	778	778, 403	778, 775, 762, 759
713	713, 672	713, 706, 703, 696	746	746, 395	746, 738, 733, 728	779		779, 776, 771, 769
714	714, 691	714, 709, 707, 701	747		747, 743, 741, 737	780		780, 775, 772, 764
715		715, 714, 711, 708	748		748, 744, 743, 733	781		781, 779, 765, 764
716	716, 533	716, 706, 705, 704	749		749, 748, 743, 742	782	782, 453	782, 780, 779, 773
717		717, 716, 710, 701	750		750, 746, 741, 734	783	783, 715	783, 782, 776, 773
718		718, 717, 716, 713	751	751, 733	751, 750, 748, 740	784		784, 778, 775, 771
719	719, 569	719, 711, 710, 707	752		752, 749, 732, 731	785	785, 693	785, 780, 776, 775
720		720, 718, 712, 709	753	753, 595	753, 748, 745, 740	786		786, 782, 780, 771
721	721, 712	721, 720, 713, 712	754	754, 735	754, 742, 740, 735	1024		1024, 1015, 1002, 1001
722	722, 491	722, 721, 718, 707	755		755, 754, 745, 743	2048		2048, 2035, 2034, 2029
723		723, 717, 710, 707	756	756, 407	756, 755, 747, 740	4096		4096, 4095, 4081, 4069
724		724, 719, 716, 711	757		757, 756, 751, 750			

References

[1] A. Ahmad and A.M. Elabdalla. An efficient method to determine linear feedback connections in shift registers that generate maximal length pseudo-random up and down binary sequences. *Computers and Electrical Engineering*, 23(1):33–39, 1997.

[2] Peter Alfke. Application Note: Efficient Shift Registers, LFSR Counters, and Long Pseudo- Random Sequence Generators. Technical report, Xilinx Inc., San Jose, CA, 1996. App. note XApp052.

[3] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S.S. Wagstaff Jr. Factorizations of $b^n \pm 1$, b= 2, 3, 5, 6, 7, 10, 11, 12 up to High Powers. *Contemporary Mathematics*, 22, 2002.

[4] D.W. Clark and L.J. Weng. Maximal and near-maximal shift register sequences: efficient event-counters and easy discrete logarithms. *Computers, IEEE Transactions on*, 43(5):560–568, 1994.

[5] T.C.A. Molteno and R. W. Ward. Table of prime factors of Mersenne numbers. Technical report, University of Otago, Dunedin, New Zealand, 2007. http://www.physics.otago.ac.nz/px/research/electronics/papers/technical-reports/mersenne_factor_table.pdf.

[6] M.J.B. Robshaw. Stream Ciphers. *RSA Labratories*, 25, 1995.

[7] L.T. Wang and E.J. McCluskey. Hybrid designs generating maximum-length sequences. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, 7(1):91–99, 1988.

Electronics Group
Department of Physics
University of Otago
elec.otago.ac.nz