

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

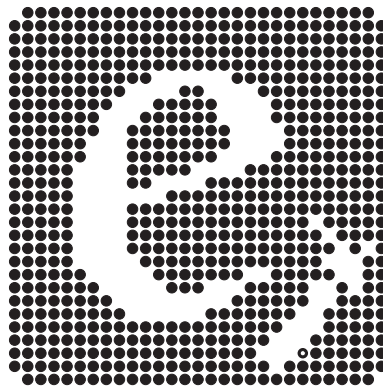
TECHNICAL REPORTS FROM THE ELECTRONICS GROUP
AT THE UNIVERSITY OF OTAGO

Table of Multiple Feedback Shift Registers

by

R. W. Ward, T.C.A. Molteno

ELECTRONICS TECHNICAL
REPORT No. 2009-1



UNIVERSITY OF OTAGO
DUNEDIN, NEW ZEALAND

Online version has

URL: <http://www.physics.otago.ac.nz/reports/electronics/ETR2009-1.pdf>

The author has homepage: <http://elec.otago.ac.nz/w/index.php/TimMolteno>

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 practitioners involved in the four ‘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 September 2008, research within the Electronics Group include projects on lightweight GPS tags for birds, modelling and control of a robotic elbow, design and deployment of an under-sea glider, 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 Multiple Feedback Shift Registers

R. W. Ward, T.C.A. Molteno

Abstract

This report presents a table of maximum-cycle Multiple Feedback Shift Register (MFSR) feedback terms. For all the values of n tested ($n < 787$ and other selected values), there exists a maximum-cycle MFSR with at most three required taps, corresponding to the n where LFSR designs require a minimum of four taps. Our data lends support to the conjecture that there is a two or three-tap maximum-cycle MFSR design for every value of $n \geq 5$.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 5 |
| 1.1 | Notation | 5 |
| 1.2 | Methods | 6 |
| 1.2.1 | Maximum-cycle MFSRs | 6 |
| 1.3 | Efficient searching for maximum-cycle MFSRs | 6 |
| 1.3.1 | Pruning the search tree | 7 |
| 1.3.2 | Prime Factorisation | 7 |
| 1.3.3 | The search algorithm | 8 |
| 2 | Maximum-cycle MFSRs | 11 |

Chapter 1

Introduction

This report contains a table of n -stage maximum-cycle Multiple Feedback Shift Register (MFSR) designs. For all the values of n tested ($n < 787$ and other selected values), there exists a maximum-cycle MFSR with at most three required taps, corresponding to the n where LFSR designs require a minimum of four taps. Our data lends support to the conjecture that there is a two or three-tap maximum-cycle MFSR design for every value of $n \geq 5$.

Multiple Feedback Shift Registers (MFSR). These are a class of feedback shift register that require fewer feedback terms and have a lower fan-out than Linear Feedback Shift Registers (LFSR). They differ from LFSRs in allowing feedback logic to be connected to and from arbitrary bit positions in the shift register. We present a matrix representation of feedback shift registers, and show how MFSRs are a generalisation of LFSRs. For a given characteristic polynomial there are in general many MFSR designs.

1.1 Notation

Each design is presented by describing its feedback terms. In the following tables, entries of the form $i \leftarrow j$, in an n -stage MFSR indicates that the output of bit position j is XORed with the output of $i-1$ and fed into bit position i . The feedback term $1 \leftarrow 8$ is implicit. Figure 1.1 shows an 8-stage maximum-cycle MFSR with feedback terms at $7 \leftarrow 8, 4 \leftarrow 6$.

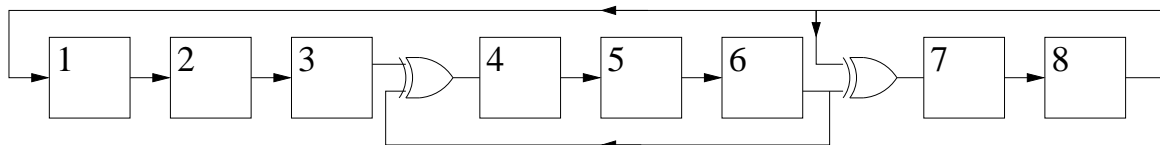


Figure 1.1. An 8-stage maximum cycle MFSR with cycle size $2^8 - 1$

1.2 Methods

An MFSR has a cycle of length l , from a state \mathbf{v}_0 if after l iterations, the MFSR returns to the starting state \mathbf{v}_0 , i.e.,

$$\mathbf{M}^l \mathbf{v}_0 = \mathbf{v}_0 \quad (1.1)$$

Cyclic behaviour can be strongly dependent on the starting state. For example, the zero state $\{0, 0, \dots, 0\}$ is always mapped onto itself under multiplication by any MFSR matrix \mathbf{M} . Thus any MFSR, regardless of the MFSR design, has a cycle of length one starting from the zero state.

Even ignoring the zero state, Equation 1.1 is *not* equivalent to $\mathbf{M}^{l-1} = \mathbf{I}$, where \mathbf{I} is the $n \times n$ identity matrix. This is because an MFSR with an l -cycle, may do so starting only from a subset of the possible MFSR 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 linear feedback shift register 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 $\mathbf{M}^{31-1} \neq \mathbf{I}$.

1.2.1 Maximum-cycle MFSRs

An n -stage MFSR is *maximum-cycle* when all $2^n - 1$ non-zero states occur as the MFSR is iterated. For a maximum-cycle MFSR, the cyclic behaviour must be independent of the initial (non-zero) state. Equation 1.1 then becomes $\mathbf{M}^{2^n - 1} = \mathbf{I}$ or equivalently

$$\mathbf{M}^{2^n} = \mathbf{M}. \quad (1.2)$$

Additionally, a maximum-cycle MFSR can have no smaller cycles, and as a consequence, we get the additional condition:

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

1.3 Efficient searching for maximum-cycle MFSRs

The task of finding a maximum-cycle MFSR can be reduced to the task of finding a MFSR 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 $O(n^3 2^n)$ to check each candidate and this becomes prohibitive for large values of n . We show in the next section how this search can be significantly pruned.

Non-matrix algorithms for maximum-cycle LFSR design have also been described, see for example Cadigal et al. [3] and Ahmad et al. [1] and these could be used by testing the LFSR corresponding with the MFSR.

1.3.1 Pruning the search tree

The $2^n - 2$ tests in Equation 1.3, for a $2^n - 1$ -cycle MFSR 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 of k_0 will also satisfy $\mathbf{M}^k = \mathbf{I}$, 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 MFSR 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.

1.3.2 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

$$\forall i \in \{1, \dots, m\}, \mathbf{M}^{\frac{2^n - 1}{p_i}} \neq \mathbf{I}. \quad (1.4)$$

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 [2]. 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 [4].

1.3.3 The search algorithm

The search for an n -stage maximum-cycle MFSR is performed by considering all potential designs in order of increasing tap number. Clearly zero taps will not lead to a cycle, and one tap will simply be a cyclic register with maximum period n , so our algorithm starts with a search for possible two-tap designs. By definition one of the taps is at $1 \leftarrow n$ for some $0 < i \leq n$, and without loss of generality we place the other tap in the n th column, so that all we need to find is the row i . We call this matrix $\mathbf{M}_{i \leftarrow n}$. We note that this is an LFSR, so using a symmetry property of LFSRs described in [5] we only need to consider $n/2 \leq i \leq n$. For each $\mathbf{M}_{i \leftarrow n}$, Equation 1.2 is checked, and if that holds, Equation 1.4 is tested.

If there are no two-tap designs, a three tap search is conducted, Once again, one of the taps is at $1 \leftarrow n$ and without loss of generality, we put another tap at $i \leftarrow n$ for some $0 < i \leq n$. The third tap put at $j \leftarrow k$ for some $0 < j, k \leq n$. For each candidate matrix $\mathbf{M}_{i \leftarrow n, j \leftarrow k}$ the same tests are done.

The algorithm terminates after finding a solution. Within the search for each tap number, we choose the search order to find solutions that avoid two taps in the same row of the matrix, and with non-zero elements clustered near the top-right corner of the matrix. Experience with synthesis of MFSR designs on FPGAs has indicated that these designs will synthesize with short feedback paths and low latency.

In practice, we get good results by searching first on j , choosing k such that $j \leq k < n$ and setting $i = k + 1$ – we have always found a solution in that search space. Pseudocode for this algorithm, showing the candidate search order, is given below.

```

boolean test(M)
  let {p1...pm} = prime factors of 2^n-1;
  if (M^{2^n-1} = I)
    if (forall p_i in {p1...pm}, M^{(2^n-1)/p_i} != I)
      return true;
  return false;

// Two-tap case
for i = {n...n/2}
  if (test(M_{i←n}))
    return i←n;

```

```

// Three-tap case
for j = {n...2}
  for k = {n-1...j}
    i=k+1
    if (test( $M_{i \leftarrow n, j \leftarrow k}$ ))
      return i←n, j←k;

```

The following chapter presents the results of the search for maximum-cycle MFSR designs using the algorithm above.

Chapter 2

Maximum-cycle MFSRs

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

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|--------------------|--------------------------------------|-----|--------------------|--------------------------------------|
| 2 | $2 \leftarrow 2$ | | 36 | $26 \leftarrow 36$ | $36 \leftarrow 36, 29 \leftarrow 35$ |
| 3 | $3 \leftarrow 3$ | $3 \leftarrow 3, 2 \leftarrow 2$ | 37 | | $36 \leftarrow 37, 26 \leftarrow 35$ |
| 4 | $4 \leftarrow 4$ | $4 \leftarrow 4, 3 \leftarrow 3$ | 38 | | $38 \leftarrow 38, 33 \leftarrow 37$ |
| 5 | $4 \leftarrow 5$ | $5 \leftarrow 5, 3 \leftarrow 4$ | 39 | $36 \leftarrow 39$ | $36 \leftarrow 39, 32 \leftarrow 35$ |
| 6 | $6 \leftarrow 6$ | $6 \leftarrow 6, 5 \leftarrow 5$ | 40 | | $39 \leftarrow 40, 20 \leftarrow 38$ |
| 7 | $7 \leftarrow 7$ | $7 \leftarrow 7, 6 \leftarrow 6$ | 41 | $39 \leftarrow 41$ | $41 \leftarrow 41, 39 \leftarrow 40$ |
| 8 | | $7 \leftarrow 8, 4 \leftarrow 6$ | 42 | | $41 \leftarrow 42, 36 \leftarrow 40$ |
| 9 | $6 \leftarrow 9$ | $9 \leftarrow 9, 6 \leftarrow 8$ | 43 | | $43 \leftarrow 43, 38 \leftarrow 42$ |
| 10 | $8 \leftarrow 10$ | $10 \leftarrow 10, 7 \leftarrow 9$ | 44 | | $38 \leftarrow 44, 30 \leftarrow 37$ |
| 11 | $10 \leftarrow 11$ | $10 \leftarrow 11, 8 \leftarrow 9$ | 45 | | $45 \leftarrow 45, 42 \leftarrow 44$ |
| 12 | | $10 \leftarrow 12, 6 \leftarrow 9$ | 46 | | $43 \leftarrow 46, 38 \leftarrow 42$ |
| 13 | | $13 \leftarrow 13, 10 \leftarrow 12$ | 47 | $43 \leftarrow 47$ | $47 \leftarrow 47, 43 \leftarrow 46$ |
| 14 | | $13 \leftarrow 14, 6 \leftarrow 12$ | 48 | | $43 \leftarrow 48, 30 \leftarrow 42$ |
| 15 | $15 \leftarrow 15$ | $15 \leftarrow 15, 14 \leftarrow 14$ | 49 | $41 \leftarrow 49$ | $49 \leftarrow 49, 41 \leftarrow 48$ |
| 16 | | $15 \leftarrow 16, 12 \leftarrow 14$ | 50 | | $48 \leftarrow 50, 39 \leftarrow 47$ |
| 17 | $15 \leftarrow 17$ | $17 \leftarrow 17, 15 \leftarrow 16$ | 51 | | $48 \leftarrow 51, 42 \leftarrow 47$ |
| 18 | $12 \leftarrow 18$ | $16 \leftarrow 18, 9 \leftarrow 15$ | 52 | $50 \leftarrow 52$ | $50 \leftarrow 52, 47 \leftarrow 49$ |
| 19 | | $19 \leftarrow 19, 14 \leftarrow 18$ | 53 | | $52 \leftarrow 53, 46 \leftarrow 51$ |
| 20 | $18 \leftarrow 20$ | $18 \leftarrow 20, 15 \leftarrow 17$ | 54 | | $51 \leftarrow 54, 42 \leftarrow 50$ |
| 21 | $20 \leftarrow 21$ | $20 \leftarrow 21, 18 \leftarrow 19$ | 55 | $32 \leftarrow 55$ | $54 \leftarrow 55, 48 \leftarrow 53$ |
| 22 | $22 \leftarrow 22$ | $22 \leftarrow 22, 21 \leftarrow 21$ | 56 | | $56 \leftarrow 56, 35 \leftarrow 55$ |
| 23 | $19 \leftarrow 23$ | $23 \leftarrow 23, 19 \leftarrow 22$ | 57 | $51 \leftarrow 57$ | $56 \leftarrow 57, 53 \leftarrow 55$ |
| 24 | | $24 \leftarrow 24, 21 \leftarrow 23$ | 58 | $40 \leftarrow 58$ | $58 \leftarrow 58, 53 \leftarrow 57$ |
| 25 | $23 \leftarrow 25$ | $25 \leftarrow 25, 23 \leftarrow 24$ | 59 | | $55 \leftarrow 59, 49 \leftarrow 54$ |
| 26 | | $26 \leftarrow 26, 19 \leftarrow 25$ | 60 | $60 \leftarrow 60$ | $60 \leftarrow 60, 59 \leftarrow 59$ |
| 27 | | $27 \leftarrow 27, 20 \leftarrow 26$ | 61 | | $59 \leftarrow 61, 49 \leftarrow 58$ |
| 28 | $26 \leftarrow 28$ | $26 \leftarrow 28, 23 \leftarrow 25$ | 62 | | $57 \leftarrow 62, 50 \leftarrow 56$ |
| 29 | $28 \leftarrow 29$ | $28 \leftarrow 29, 26 \leftarrow 27$ | 63 | $63 \leftarrow 63$ | $63 \leftarrow 63, 62 \leftarrow 62$ |
| 30 | | $28 \leftarrow 30, 21 \leftarrow 27$ | 64 | | $64 \leftarrow 64, 61 \leftarrow 63$ |
| 31 | $29 \leftarrow 31$ | $31 \leftarrow 31, 29 \leftarrow 30$ | 65 | $48 \leftarrow 65$ | $65 \leftarrow 65, 62 \leftarrow 64$ |
| 32 | | $28 \leftarrow 32, 21 \leftarrow 27$ | 66 | | $66 \leftarrow 66, 57 \leftarrow 65$ |
| 33 | $21 \leftarrow 33$ | $31 \leftarrow 33, 27 \leftarrow 30$ | 67 | | $67 \leftarrow 67, 58 \leftarrow 66$ |
| 34 | | $32 \leftarrow 34, 23 \leftarrow 31$ | 68 | $60 \leftarrow 68$ | $65 \leftarrow 68, 60 \leftarrow 64$ |
| 35 | $34 \leftarrow 35$ | $34 \leftarrow 35, 32 \leftarrow 33$ | 69 | | $67 \leftarrow 69, 60 \leftarrow 66$ |

Continued ...

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|------------------|-----|------------|------------------|
| 70 | | 70←70, 55←69 | 117 | | 116←117, 98←115 |
| 71 | 66←71 | 70←71, 66←69 | 118 | 86←118 | 110←118, 95←109 |
| 72 | | 66←72, 51←65 | 119 | 112←119 | 112←119, 104←111 |
| 73 | 49←73 | 72←73, 66←71 | 120 | | 107←120, 86←106 |
| 74 | | 72←74, 68←71 | 121 | 104←121 | 116←121, 106←115 |
| 75 | | 75←75, 65←74 | 122 | | 120←122, 116←119 |
| 76 | | 73←76, 64←72 | 123 | 122←123 | 122←123, 120←121 |
| 77 | | 73←77, 67←72 | 124 | 88←124 | 116←124, 89←115 |
| 78 | | 74←78, 66←73 | 125 | | 117←125, 103←116 |
| 79 | 71←79 | 79←79, 71←78 | 126 | | 115←126, 98←114 |
| 80 | | 76←80, 69←75 | 127 | 127←127 | 127←127, 126←126 |
| 81 | 78←81 | 78←81, 74←77 | 128 | | 119←128, 108←118 |
| 82 | | 75←82, 60←74 | 129 | 125←129 | 129←129, 125←128 |
| 83 | | 78←83, 70←77 | 130 | 128←130 | 128←130, 125←127 |
| 84 | 72←84 | 81←84, 72←80 | 131 | | 126←131, 119←125 |
| 85 | | 83←85, 74←82 | 132 | 104←132 | 128←132, 110←127 |
| 86 | | 86←86, 74←85 | 133 | | 124←133, 113←123 |
| 87 | 75←87 | 80←87, 71←79 | 134 | 78←134 | 129←134, 114←128 |
| 88 | | 86←88, 73←85 | 135 | 125←135 | 134←135, 129←133 |
| 89 | 52←89 | 87←89, 79←86 | 136 | | 134←136, 113←133 |
| 90 | | 89←90, 86←88 | 137 | 117←137 | 134←137, 127←133 |
| 91 | | 87←91, 80←86 | 138 | | 138←138, 131←137 |
| 92 | | 90←92, 82←89 | 139 | | 137←139, 132←136 |
| 93 | 92←93 | 92←93, 90←91 | 140 | 112←140 | 136←140, 115←135 |
| 94 | 74←94 | 94←94, 89←93 | 141 | | 139←141, 129←138 |
| 95 | 85←95 | 94←95, 85←93 | 142 | 122←142 | 136←142, 125←135 |
| 96 | | 90←96, 65←89 | 143 | | 142←143, 139←141 |
| 97 | 92←97 | 96←97, 92←95 | 144 | | 143←144, 116←142 |
| 98 | 88←98 | 98←98, 91←97 | 145 | 94←145 | 145←145, 140←144 |
| 99 | | 93←99, 75←92 | 146 | | 145←146, 142←144 |
| 100 | 64←100 | 94←100, 77←93 | 147 | | 140←147, 126←139 |
| 101 | | 101←101, 95←100 | 148 | 122←148 | 148←148, 131←147 |
| 102 | | 98←102, 80←97 | 149 | | 147←149, 122←146 |
| 103 | 95←103 | 103←103, 95←102 | 150 | 98←150 | 148←150, 138←147 |
| 104 | | 104←104, 94←103 | 151 | 149←151 | 151←151, 149←150 |
| 105 | 90←105 | 105←105, 99←104 | 152 | | 146←152, 136←145 |
| 106 | 92←106 | 106←106, 101←105 | 153 | 153←153 | 153←153, 152←152 |
| 107 | | 102←107, 88←101 | 154 | | 148←154, 130←147 |
| 108 | 78←108 | 101←108, 92←100 | 155 | | 150←155, 143←149 |
| 109 | | 109←109, 103←108 | 156 | | 149←156, 132←148 |
| 110 | | 110←110, 98←109 | 157 | | 153←157, 146←152 |
| 111 | 102←111 | 110←111, 102←109 | 158 | | 154←158, 142←153 |
| 112 | | 110←112, 97←109 | 159 | 129←159 | 158←159, 146←157 |
| 113 | 105←113 | 112←113, 109←111 | 160 | | 159←160, 156←158 |
| 114 | | 107←114, 92←106 | 161 | 144←161 | 161←161, 146←160 |
| 115 | | 114←115, 104←113 | 162 | | 158←162, 152←157 |
| 116 | | 111←116, 96←110 | 163 | | 159←163, 153←158 |

Continued ...

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|----------------------|-----|------------|----------------------|
| 164 | | 164 ← 164, 151 ← 163 | 211 | | 207 ← 211, 193 ← 206 |
| 165 | | 160 ← 165, 146 ← 159 | 212 | 108 ← 212 | 210 ← 212, 206 ← 209 |
| 166 | | 163 ← 166, 142 ← 162 | 213 | | 213 ← 213, 206 ← 212 |
| 167 | 162 ← 167 | 166 ← 167, 162 ← 165 | 214 | | 211 ← 214, 194 ← 210 |
| 168 | | 167 ← 168, 152 ← 166 | 215 | 193 ← 215 | 213 ← 215, 209 ← 212 |
| 169 | 136 ← 169 | 168 ← 169, 159 ← 167 | 216 | | 207 ← 216, 192 ← 206 |
| 170 | 148 ← 170 | 169 ← 170, 162 ← 168 | 217 | 173 ← 217 | 217 ← 217, 206 ← 216 |
| 171 | | 171 ← 171, 153 ← 170 | 218 | 208 ← 218 | 218 ← 218, 211 ← 217 |
| 172 | 166 ← 172 | 166 ← 172, 159 ← 165 | 219 | | 219 ← 219, 201 ← 218 |
| 173 | | 171 ← 173, 161 ← 170 | 220 | | 220 ← 220, 206 ← 219 |
| 174 | 162 ← 174 | 162 ← 174, 149 ← 161 | 221 | | 220 ← 221, 214 ← 219 |
| 175 | 170 ← 175 | 174 ← 175, 170 ← 173 | 222 | | 212 ← 222, 197 ← 211 |
| 176 | | 174 ← 176, 141 ← 173 | 223 | 191 ← 223 | 222 ← 223, 217 ← 221 |
| 177 | 170 ← 177 | 176 ← 177, 173 ← 175 | 224 | | 216 ← 224, 202 ← 215 |
| 178 | 92 ← 178 | 170 ← 178, 159 ← 169 | 225 | 194 ← 225 | 225 ← 225, 201 ← 224 |
| 179 | | 173 ← 179, 156 ← 172 | 226 | | 224 ← 226, 217 ← 223 |
| 180 | | 178 ← 180, 158 ← 177 | 227 | | 214 ← 227, 199 ← 213 |
| 181 | | 181 ← 181, 175 ← 180 | 228 | | 220 ← 228, 206 ← 219 |
| 182 | | 175 ← 182, 162 ← 174 | 229 | | 219 ← 229, 206 ← 218 |
| 183 | 128 ← 183 | 179 ← 183, 156 ← 178 | 230 | | 225 ← 230, 196 ← 224 |
| 184 | | 167 ← 184, 136 ← 166 | 231 | 206 ← 231 | 228 ← 231, 221 ← 227 |
| 185 | 162 ← 185 | 184 ← 185, 175 ← 183 | 232 | | 219 ← 232, 204 ← 218 |
| 186 | | 186 ← 186, 164 ← 185 | 233 | 160 ← 233 | 232 ← 233, 225 ← 231 |
| 187 | | 185 ← 187, 158 ← 184 | 234 | 204 ← 234 | 233 ← 234, 224 ← 232 |
| 188 | | 185 ← 188, 180 ← 184 | 235 | | 235 ← 235, 226 ← 234 |
| 189 | | 181 ← 189, 170 ← 180 | 236 | 232 ← 236 | 232 ← 236, 227 ← 231 |
| 190 | | 190 ← 190, 173 ← 189 | 237 | | 235 ← 237, 230 ← 234 |
| 191 | 183 ← 191 | 191 ← 191, 183 ← 190 | 238 | | 226 ← 238, 209 ← 225 |
| 192 | | 192 ← 192, 165 ← 191 | 239 | 204 ← 239 | 239 ← 239, 226 ← 238 |
| 193 | 179 ← 193 | 188 ← 193, 180 ← 187 | 240 | | 238 ← 240, 233 ← 237 |
| 194 | 108 ← 194 | 193 ← 194, 178 ← 192 | 241 | 172 ← 241 | 238 ← 241, 226 ← 237 |
| 195 | | 195 ← 195, 186 ← 194 | 242 | | 234 ← 242, 221 ← 233 |
| 196 | | 195 ← 196, 186 ← 194 | 243 | | 238 ← 243, 222 ← 237 |
| 197 | | 193 ← 197, 171 ← 192 | 244 | | 235 ← 244, 218 ← 234 |
| 198 | 134 ← 198 | 184 ← 198, 165 ← 183 | 245 | | 243 ← 245, 233 ← 242 |
| 199 | 166 ← 199 | 198 ← 199, 189 ← 197 | 246 | | 246 ← 246, 212 ← 245 |
| 200 | | 199 ← 200, 196 ← 198 | 247 | 166 ← 247 | 246 ← 247, 229 ← 245 |
| 201 | 188 ← 201 | 201 ← 201, 185 ← 200 | 248 | | 234 ← 248, 217 ← 233 |
| 202 | 148 ← 202 | 198 ← 202, 181 ← 197 | 249 | 164 ← 249 | 246 ← 249, 234 ← 245 |
| 203 | | 203 ← 203, 196 ← 202 | 250 | 148 ← 250 | 249 ← 250, 234 ← 248 |
| 204 | | 200 ← 204, 168 ← 199 | 251 | | 249 ← 251, 239 ← 248 |
| 205 | | 205 ← 205, 176 ← 204 | 252 | 186 ← 252 | 244 ← 252, 222 ← 243 |
| 206 | | 206 ← 206, 178 ← 205 | 253 | | 253 ← 253, 247 ← 252 |
| 207 | 165 ← 207 | 199 ← 207, 183 ← 198 | 254 | | 254 ← 254, 236 ← 253 |
| 208 | | 203 ← 208, 194 ← 202 | 255 | 204 ← 255 | 254 ← 255, 251 ← 253 |
| 209 | 204 ← 209 | 208 ← 209, 205 ← 207 | 256 | | 254 ← 256, 233 ← 253 |
| 210 | | 208 ← 210, 176 ← 207 | 257 | 246 ← 257 | 254 ← 257, 246 ← 253 |

Continued ...

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|----------------------|-----|------------|----------------------|
| 258 | 176 ← 258 | 253 ← 258, 224 ← 252 | 305 | 204 ← 305 | 305 ← 305, 293 ← 304 |
| 259 | | 259 ← 259, 245 ← 258 | 306 | | 303 ← 306, 296 ← 302 |
| 260 | | 260 ← 260, 240 ← 259 | 307 | | 305 ← 307, 291 ← 304 |
| 261 | | 252 ← 261, 239 ← 251 | 308 | | 296 ← 308, 268 ← 295 |
| 262 | | 258 ← 262, 244 ← 257 | 309 | | 306 ← 309, 300 ← 305 |
| 263 | 171 ← 263 | 263 ← 263, 251 ← 262 | 310 | | 310 ← 310, 295 ← 309 |
| 264 | | 264 ← 264, 255 ← 263 | 311 | | 303 ← 311, 288 ← 302 |
| 265 | 224 ← 265 | 264 ← 265, 261 ← 263 | 312 | | 306 ← 312, 267 ← 305 |
| 266 | 220 ← 266 | 266 ← 266, 260 ← 265 | 313 | 235 ← 313 | 311 ← 313, 307 ← 310 |
| 267 | | 263 ← 267, 245 ← 262 | 314 | 300 ← 314 | 312 ← 314, 300 ← 311 |
| 268 | 244 ← 268 | 268 ← 268, 253 ← 267 | 315 | | 315 ← 315, 306 ← 314 |
| 269 | | 269 ← 269, 263 ← 268 | 316 | 182 ← 316 | 312 ← 316, 275 ← 311 |
| 270 | 218 ← 270 | 268 ← 270, 261 ← 267 | 317 | | 309 ← 317, 292 ← 308 |
| 271 | 214 ← 271 | 270 ← 271, 252 ← 269 | 318 | | 312 ← 318, 299 ← 311 |
| 272 | | 260 ← 272, 223 ← 259 | 319 | 284 ← 319 | 318 ← 319, 309 ← 317 |
| 273 | 251 ← 273 | 273 ← 273, 267 ← 272 | 320 | | 320 ← 320, 317 ← 319 |
| 274 | 208 ← 274 | 273 ← 274, 266 ← 272 | 321 | 291 ← 321 | 320 ← 321, 315 ← 319 |
| 275 | | 269 ← 275, 258 ← 268 | 322 | 256 ← 322 | 321 ← 322, 300 ← 320 |
| 276 | | 263 ← 276, 248 ← 262 | 323 | | 321 ← 323, 311 ← 320 |
| 277 | | 272 ← 277, 256 ← 271 | 324 | | 322 ← 324, 314 ← 321 |
| 278 | 274 ← 278 | 278 ← 278, 274 ← 277 | 325 | | 323 ← 325, 301 ← 322 |
| 279 | 275 ← 279 | 279 ← 279, 275 ← 278 | 326 | | 311 ← 326, 294 ← 310 |
| 280 | | 279 ← 280, 268 ← 278 | 327 | 294 ← 327 | 323 ← 327, 311 ← 322 |
| 281 | 189 ← 281 | 278 ← 281, 269 ← 277 | 328 | | 320 ← 328, 289 ← 319 |
| 282 | 248 ← 282 | 279 ← 282, 272 ← 278 | 329 | 280 ← 329 | 322 ← 329, 309 ← 321 |
| 283 | | 279 ← 283, 272 ← 278 | 330 | | 330 ← 330, 315 ← 329 |
| 284 | 166 ← 284 | 282 ← 284, 273 ← 281 | 331 | | 326 ← 331, 319 ← 325 |
| 285 | | 269 ← 285, 251 ← 268 | 332 | 210 ← 332 | 332 ← 332, 320 ← 331 |
| 286 | 218 ← 286 | 276 ← 286, 263 ← 275 | 333 | 332 ← 333 | 332 ← 333, 330 ← 331 |
| 287 | 217 ← 287 | 284 ← 287, 277 ← 283 | 334 | | 330 ← 334, 314 ← 329 |
| 288 | | 288 ← 288, 278 ← 287 | 335 | | 327 ← 335, 315 ← 326 |
| 289 | 269 ← 289 | 282 ← 289, 272 ← 281 | 336 | | 332 ← 336, 326 ← 331 |
| 290 | | 289 ← 290, 286 ← 288 | 337 | 283 ← 337 | 333 ← 337, 325 ← 332 |
| 291 | | 286 ← 291, 278 ← 285 | 338 | | 335 ← 338, 324 ← 334 |
| 292 | 196 ← 292 | 288 ← 292, 276 ← 287 | 339 | | 334 ← 339, 314 ← 333 |
| 293 | | 284 ← 293, 256 ← 283 | 340 | | 337 ← 340, 316 ← 336 |
| 294 | 234 ← 294 | 291 ← 294, 270 ← 290 | 341 | | 341 ← 341, 318 ← 340 |
| 295 | 248 ← 295 | 295 ← 295, 283 ← 294 | 342 | 218 ← 342 | 329 ← 342, 314 ← 328 |
| 296 | | 296 ← 296, 263 ← 295 | 343 | 269 ← 343 | 343 ← 343, 323 ← 342 |
| 297 | 293 ← 297 | 297 ← 297, 293 ← 296 | 344 | | 339 ← 344, 318 ← 338 |
| 298 | | 293 ← 298, 276 ← 292 | 345 | 324 ← 345 | 345 ← 345, 330 ← 344 |
| 299 | | 279 ← 299, 254 ← 278 | 346 | | 337 ← 346, 320 ← 336 |
| 300 | 294 ← 300 | 294 ← 300, 287 ← 293 | 347 | | 339 ← 347, 325 ← 338 |
| 301 | | 297 ← 301, 290 ← 296 | 348 | | 344 ← 348, 326 ← 343 |
| 302 | 262 ← 302 | 294 ← 302, 268 ← 293 | 349 | | 349 ← 349, 338 ← 348 |
| 303 | | 296 ← 303, 284 ← 295 | 350 | 298 ← 350 | 345 ← 350, 330 ← 344 |
| 304 | | 299 ← 304, 278 ← 298 | 351 | 318 ← 351 | 344 ← 351, 327 ← 343 |

Continued ...

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|----------------------|-----|------------|----------------------|
| 352 | | 340 ← 352, 317 ← 339 | 399 | 314 ← 399 | 398 ← 399, 389 ← 397 |
| 353 | 285 ← 353 | 347 ← 353, 331 ← 346 | 400 | | 399 ← 400, 396 ← 398 |
| 354 | | 352 ← 354, 336 ← 351 | 401 | 250 ← 401 | 398 ← 401, 376 ← 397 |
| 355 | | 355 ← 355, 350 ← 354 | 402 | | 394 ← 402, 380 ← 393 |
| 356 | | 354 ← 356, 337 ← 353 | 403 | | 398 ← 403, 391 ← 397 |
| 357 | | 345 ← 357, 330 ← 344 | 404 | 216 ← 404 | 401 ← 404, 384 ← 400 |
| 358 | | 356 ← 358, 330 ← 355 | 405 | | 396 ← 405, 384 ← 395 |
| 359 | 292 ← 359 | 356 ← 359, 349 ← 355 | 406 | 250 ← 406 | 403 ← 406, 394 ← 402 |
| 360 | | 360 ← 360, 335 ← 359 | 407 | 337 ← 407 | 398 ← 407, 376 ← 397 |
| 361 | | 360 ← 361, 354 ← 359 | 408 | | 404 ← 408, 363 ← 403 |
| 362 | 300 ← 362 | 358 ← 362, 337 ← 357 | 409 | 323 ← 409 | 408 ← 409, 399 ← 407 |
| 363 | | 363 ← 363, 356 ← 362 | 410 | | 396 ← 410, 370 ← 395 |
| 364 | 298 ← 364 | 355 ← 364, 338 ← 354 | 411 | | 406 ← 411, 360 ← 405 |
| 365 | | 363 ← 365, 354 ← 362 | 412 | 266 ← 412 | 410 ← 412, 402 ← 409 |
| 366 | 338 ← 366 | 366 ← 366, 342 ← 365 | 413 | | 411 ← 413, 384 ← 410 |
| 367 | 347 ← 367 | 367 ← 367, 356 ← 366 | 414 | | 410 ← 414, 372 ← 409 |
| 368 | | 354 ← 368, 321 ← 353 | 415 | 314 ← 415 | 414 ← 415, 397 ← 413 |
| 369 | 279 ← 369 | 368 ← 369, 353 ← 367 | 416 | | 403 ← 416, 378 ← 402 |
| 370 | 232 ← 370 | 369 ← 370, 366 ← 368 | 417 | 311 ← 417 | 416 ← 417, 389 ← 415 |
| 371 | | 366 ← 371, 358 ← 365 | 418 | | 418 ← 418, 401 ← 417 |
| 372 | | 365 ← 372, 336 ← 364 | 419 | | 402 ← 419, 377 ← 401 |
| 373 | | 363 ← 373, 346 ← 362 | 420 | | 414 ← 420, 383 ← 413 |
| 374 | | 364 ← 374, 343 ← 363 | 421 | | 416 ← 421, 405 ← 415 |
| 375 | 360 ← 375 | 375 ← 375, 368 ← 374 | 422 | 274 ← 422 | 416 ← 422, 394 ← 415 |
| 376 | | 375 ← 376, 356 ← 374 | 423 | 399 ← 423 | 419 ← 423, 399 ← 418 |
| 377 | 337 ← 377 | 375 ← 377, 367 ← 374 | 424 | | 423 ← 424, 416 ← 422 |
| 378 | 336 ← 378 | 364 ← 378, 336 ← 363 | 425 | 414 ← 425 | 423 ← 425, 419 ← 422 |
| 379 | | 375 ← 379, 361 ← 374 | 426 | | 420 ← 426, 390 ← 419 |
| 380 | 334 ← 380 | 380 ← 380, 363 ← 379 | 427 | | 423 ← 427, 417 ← 422 |
| 381 | | 361 ← 381, 330 ← 360 | 428 | 324 ← 428 | 421 ← 428, 402 ← 420 |
| 382 | 302 ← 382 | 376 ← 382, 358 ← 375 | 429 | | 421 ← 429, 404 ← 420 |
| 383 | 294 ← 383 | 379 ← 383, 370 ← 378 | 430 | | 426 ← 430, 414 ← 425 |
| 384 | | 346 ← 384, 305 ← 345 | 431 | 312 ← 431 | 420 ← 431, 405 ← 419 |
| 385 | 380 ← 385 | 384 ← 385, 380 ← 383 | 432 | | 424 ← 432, 405 ← 423 |
| 386 | 304 ← 386 | 380 ← 386, 349 ← 379 | 433 | 401 ← 433 | 430 ← 433, 416 ← 429 |
| 387 | | 381 ← 387, 371 ← 380 | 434 | | 427 ← 434, 400 ← 426 |
| 388 | | 380 ← 388, 356 ← 379 | 435 | | 415 ← 435, 386 ← 414 |
| 389 | | 384 ← 389, 353 ← 383 | 436 | 272 ← 436 | 421 ← 436, 394 ← 420 |
| 390 | 302 ← 390 | 380 ← 390, 345 ← 379 | 437 | | 433 ← 437, 427 ← 432 |
| 391 | 364 ← 391 | 387 ← 391, 371 ← 386 | 438 | 374 ← 438 | 434 ← 438, 399 ← 433 |
| 392 | | 380 ← 392, 365 ← 379 | 439 | 391 ← 439 | 429 ← 439, 403 ← 428 |
| 393 | 387 ← 393 | 387 ← 393, 380 ← 386 | 440 | | 440 ← 440, 437 ← 439 |
| 394 | 260 ← 394 | 388 ← 394, 376 ← 387 | 441 | 411 ← 441 | 438 ← 441, 429 ← 437 |
| 395 | | 391 ← 395, 385 ← 390 | 442 | | 441 ← 442, 436 ← 440 |
| 396 | 372 ← 396 | 394 ← 396, 348 ← 393 | 443 | | 443 ← 443, 428 ← 442 |
| 397 | | 387 ← 397, 373 ← 386 | 444 | | 442 ← 444, 410 ← 441 |
| 398 | | 396 ← 398, 381 ← 395 | 445 | | 441 ← 445, 434 ← 440 |

Continued ...

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|----------------------|-----|------------|----------------------|
| 446 | 342 ← 446 | 441 ← 446, 410 ← 440 | 493 | | 489 ← 493, 468 ← 488 |
| 447 | 375 ← 447 | 446 ← 447, 431 ← 445 | 494 | 358 ← 494 | 492 ← 494, 478 ← 491 |
| 448 | | 443 ← 448, 422 ← 442 | 495 | 420 ← 495 | 495 ← 495, 470 ← 494 |
| 449 | 316 ← 449 | 441 ← 449, 427 ← 440 | 496 | | 494 ← 496, 451 ← 493 |
| 450 | 372 ← 450 | 447 ← 450, 392 ← 446 | 497 | 420 ← 497 | 490 ← 497, 481 ← 489 |
| 451 | | 441 ← 451, 426 ← 440 | 498 | | 496 ← 498, 456 ← 495 |
| 452 | | 449 ← 452, 436 ← 448 | 499 | | 495 ← 499, 489 ← 494 |
| 453 | | 445 ← 453, 434 ← 444 | 500 | | 494 ← 500, 470 ← 493 |
| 454 | | 445 ← 454, 428 ← 444 | 501 | | 491 ← 501, 477 ← 490 |
| 455 | 418 ← 455 | 455 ← 455, 440 ← 454 | 502 | | 498 ← 502, 490 ← 497 |
| 456 | | 447 ← 456, 386 ← 446 | 503 | 501 ← 503 | 503 ← 503, 501 ← 502 |
| 457 | 442 ← 457 | 455 ← 457, 447 ← 454 | 504 | | 498 ← 504, 461 ← 497 |
| 458 | 256 ← 458 | 448 ← 458, 433 ← 447 | 505 | 350 ← 505 | 504 ← 505, 485 ← 503 |
| 459 | | 456 ← 459, 446 ← 455 | 506 | 412 ← 506 | 496 ← 506, 472 ← 495 |
| 460 | 400 ← 460 | 458 ← 460, 445 ← 457 | 507 | | 501 ← 507, 488 ← 500 |
| 461 | | 461 ← 461, 455 ← 460 | 508 | 400 ← 508 | 501 ← 508, 486 ← 500 |
| 462 | 390 ← 462 | 455 ← 462, 426 ← 454 | 509 | | 496 ← 509, 474 ← 495 |
| 463 | 371 ← 463 | 463 ← 463, 446 ← 462 | 510 | | 510 ← 510, 462 ← 509 |
| 464 | | 452 ← 464, 425 ← 451 | 511 | 502 ← 511 | 510 ← 511, 502 ← 509 |
| 465 | 407 ← 465 | 464 ← 465, 453 ← 463 | 512 | | 506 ← 512, 479 ← 505 |
| 466 | | 466 ← 466, 451 ← 465 | 513 | 429 ← 513 | 513 ← 513, 482 ← 512 |
| 467 | | 462 ← 467, 448 ← 461 | 514 | | 514 ← 514, 493 ← 513 |
| 468 | | 460 ← 468, 429 ← 459 | 515 | | 506 ← 515, 487 ← 505 |
| 469 | | 461 ← 469, 440 ← 460 | 516 | | 515 ← 516, 510 ← 514 |
| 470 | 322 ← 470 | 462 ← 470, 401 ← 461 | 517 | | 516 ← 517, 506 ← 515 |
| 471 | 471 ← 471 | 471 ← 471, 470 ← 470 | 518 | 486 ← 518 | 508 ← 518, 493 ← 507 |
| 472 | | 471 ← 472, 448 ← 470 | 519 | 441 ← 519 | 518 ← 519, 483 ← 517 |
| 473 | | 470 ← 473, 459 ← 469 | 520 | | 516 ← 520, 433 ← 515 |
| 474 | 284 ← 474 | 471 ← 474, 456 ← 470 | 521 | 490 ← 521 | 520 ← 521, 513 ← 519 |
| 475 | | 472 ← 475, 466 ← 471 | 522 | | 520 ← 522, 476 ← 519 |
| 476 | 462 ← 476 | 462 ← 476, 447 ← 461 | 523 | | 518 ← 523, 501 ← 517 |
| 477 | | 472 ← 477, 458 ← 471 | 524 | 358 ← 524 | 518 ← 524, 501 ← 517 |
| 478 | 358 ← 478 | 465 ← 478, 440 ← 464 | 525 | | 520 ← 525, 494 ← 519 |
| 479 | 376 ← 479 | 470 ← 479, 455 ← 469 | 526 | | 517 ← 526, 484 ← 516 |
| 480 | | 471 ← 480, 438 ← 470 | 527 | 481 ← 527 | 518 ← 527, 503 ← 517 |
| 481 | 344 ← 481 | 481 ← 481, 472 ← 480 | 528 | | 514 ← 528, 497 ← 513 |
| 482 | | 472 ← 482, 436 ← 471 | 529 | 488 ← 529 | 526 ← 529, 502 ← 525 |
| 483 | | 479 ← 483, 446 ← 478 | 530 | | 528 ← 530, 521 ← 527 |
| 484 | 380 ← 484 | 480 ← 484, 422 ← 479 | 531 | | 531 ← 531, 513 ← 530 |
| 485 | | 476 ← 485, 463 ← 475 | 532 | 532 ← 532 | 532 ← 532, 531 ← 531 |
| 486 | | 480 ← 486, 467 ← 479 | 533 | | 519 ← 533, 493 ← 518 |
| 487 | 394 ← 487 | 486 ← 487, 473 ← 485 | 534 | | 518 ← 534, 461 ← 517 |
| 488 | | 488 ← 488, 485 ← 487 | 535 | | 534 ← 535, 528 ← 533 |
| 489 | 407 ← 489 | 488 ← 489, 476 ← 487 | 536 | | 536 ← 536, 485 ← 535 |
| 490 | 272 ← 490 | 480 ← 490, 450 ← 479 | 537 | 444 ← 537 | 523 ← 537, 507 ← 522 |
| 491 | | 491 ← 491, 477 ← 490 | 538 | | 534 ← 538, 527 ← 533 |
| 492 | | 492 ← 492, 485 ← 491 | 539 | | 531 ← 539, 517 ← 530 |

Continued ...

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|----------------------|-----|------------|----------------------|
| 540 | 362 ← 540 | 520 ← 540, 494 ← 519 | 587 | | 581 ← 587, 568 ← 580 |
| 541 | | 533 ← 541, 512 ← 532 | 588 | 438 ← 588 | 577 ← 588, 560 ← 576 |
| 542 | | 542 ← 542, 525 ← 541 | 589 | | 583 ← 589, 556 ← 582 |
| 543 | 528 ← 543 | 539 ← 543, 527 ← 538 | 590 | 498 ← 590 | 584 ← 590, 573 ← 583 |
| 544 | | 532 ← 544, 487 ← 531 | 591 | | 583 ← 591, 566 ← 582 |
| 545 | 424 ← 545 | 544 ← 545, 516 ← 543 | 592 | | 591 ← 592, 560 ← 590 |
| 546 | | 542 ← 546, 501 ← 541 | 593 | 508 ← 593 | 591 ← 593, 577 ← 590 |
| 547 | | 541 ← 547, 515 ← 540 | 594 | 576 ← 594 | 588 ← 594, 560 ← 587 |
| 548 | | 537 ← 548, 514 ← 536 | 595 | | 595 ← 595, 586 ← 594 |
| 549 | | 523 ← 549, 480 ← 522 | 596 | | 588 ← 596, 548 ← 587 |
| 550 | 358 ← 550 | 547 ← 550, 530 ← 546 | 597 | | 597 ← 597, 540 ← 596 |
| 551 | 417 ← 551 | 548 ← 551, 536 ← 547 | 598 | | 598 ← 598, 592 ← 597 |
| 552 | | 543 ← 552, 506 ← 542 | 599 | 570 ← 599 | 596 ← 599, 585 ← 595 |
| 553 | 515 ← 553 | 552 ← 553, 541 ← 551 | 600 | | 600 ← 600, 590 ← 599 |
| 554 | | 552 ← 554, 544 ← 551 | 601 | 401 ← 601 | 600 ← 601, 590 ← 599 |
| 555 | | 550 ← 555, 524 ← 549 | 602 | | 600 ← 602, 583 ← 599 |
| 556 | 404 ← 556 | 556 ← 556, 518 ← 555 | 603 | | 603 ← 603, 584 ← 602 |
| 557 | | 552 ← 557, 541 ← 551 | 604 | | 602 ← 604, 584 ← 601 |
| 558 | | 554 ← 558, 545 ← 553 | 605 | | 602 ← 605, 592 ← 601 |
| 559 | 526 ← 559 | 558 ← 559, 551 ← 557 | 606 | | 586 ← 606, 558 ← 585 |
| 560 | | 547 ← 560, 510 ← 546 | 607 | 503 ← 607 | 600 ← 607, 585 ← 599 |
| 561 | 491 ← 561 | 558 ← 561, 551 ← 557 | 608 | | 608 ← 608, 501 ← 607 |
| 562 | | 558 ← 562, 516 ← 557 | 609 | 579 ← 609 | 598 ← 609, 581 ← 597 |
| 563 | | 553 ← 563, 538 ← 552 | 610 | 484 ← 610 | 601 ← 610, 572 ← 600 |
| 564 | 402 ← 564 | 550 ← 564, 524 ← 549 | 611 | | 601 ← 611, 576 ← 600 |
| 565 | | 559 ← 565, 542 ← 558 | 612 | | 598 ← 612, 570 ← 597 |
| 566 | 414 ← 566 | 564 ← 566, 549 ← 563 | 613 | | 605 ← 613, 595 ← 604 |
| 567 | 425 ← 567 | 562 ← 567, 555 ← 561 | 614 | | 612 ← 614, 563 ← 611 |
| 568 | | 562 ← 568, 529 ← 561 | 615 | 405 ← 615 | 615 ← 615, 609 ← 614 |
| 569 | 493 ← 569 | 560 ← 569, 548 ← 559 | 616 | | 615 ← 616, 596 ← 614 |
| 570 | 504 ← 570 | 561 ← 570, 512 ← 560 | 617 | 418 ← 617 | 611 ← 617, 602 ← 610 |
| 571 | | 561 ← 571, 542 ← 560 | 618 | | 617 ← 618, 584 ← 616 |
| 572 | | 566 ← 572, 528 ← 565 | 619 | | 605 ← 619, 582 ← 604 |
| 573 | | 570 ← 573, 564 ← 569 | 620 | | 613 ← 620, 600 ← 612 |
| 574 | 562 ← 574 | 570 ← 574, 561 ← 569 | 621 | | 617 ← 621, 570 ← 616 |
| 575 | 430 ← 575 | 573 ← 575, 554 ← 572 | 622 | 326 ← 622 | 616 ← 622, 605 ← 615 |
| 576 | | 564 ← 576, 546 ← 563 | 623 | 556 ← 623 | 617 ← 623, 591 ← 616 |
| 577 | 553 ← 577 | 572 ← 577, 563 ← 571 | 624 | | 624 ← 624, 609 ← 623 |
| 578 | | 572 ← 578, 540 ← 571 | 625 | 493 ← 625 | 619 ← 625, 611 ← 618 |
| 579 | | 573 ← 579, 518 ← 572 | 626 | | 621 ← 626, 608 ← 620 |
| 580 | | 574 ← 580, 553 ← 573 | 627 | | 615 ← 627, 582 ← 614 |
| 581 | | 576 ← 581, 569 ← 575 | 628 | 406 ← 628 | 626 ← 628, 598 ← 625 |
| 582 | 498 ← 582 | 564 ← 582, 521 ← 563 | 629 | | 614 ← 629, 580 ← 613 |
| 583 | 454 ← 583 | 582 ← 583, 576 ← 581 | 630 | | 622 ← 630, 582 ← 621 |
| 584 | | 584 ← 584, 511 ← 583 | 631 | 325 ← 631 | 626 ← 631, 618 ← 625 |
| 585 | 465 ← 585 | 572 ← 585, 557 ← 571 | 632 | | 616 ← 632, 525 ← 615 |
| 586 | | 585 ← 586, 580 ← 584 | 633 | 533 ← 633 | 633 ← 633, 609 ← 632 |

Continued ...

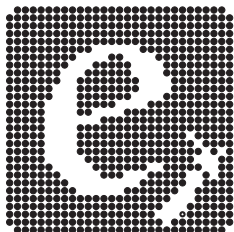
| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|----------------------|-----|------------|----------------------|
| 634 | 320 ← 634 | 616 ← 634, 596 ← 615 | 681 | | 676 ← 681, 663 ← 675 |
| 635 | | 632 ← 635, 622 ← 631 | 682 | | 670 ← 682, 655 ← 669 |
| 636 | | 634 ← 636, 608 ← 633 | 683 | | 678 ← 683, 661 ← 677 |
| 637 | | 632 ← 637, 613 ← 631 | 684 | | 662 ← 684, 614 ← 661 |
| 638 | | 638 ← 638, 633 ← 637 | 685 | | 685 ← 685, 682 ← 684 |
| 639 | 624 ← 639 | 627 ← 639, 611 ← 626 | 686 | 490 ← 686 | 678 ← 686, 663 ← 677 |
| 640 | | 639 ← 640, 624 ← 638 | 687 | 675 ← 687 | 680 ← 687, 663 ← 679 |
| 641 | 631 ← 641 | 631 ← 641, 620 ← 630 | 688 | | 682 ← 688, 649 ← 681 |
| 642 | 524 ← 642 | 640 ← 642, 612 ← 639 | 689 | 676 ← 689 | 688 ← 689, 673 ← 687 |
| 643 | | 641 ← 643, 631 ← 640 | 690 | | 688 ← 690, 681 ← 687 |
| 644 | | 633 ← 644, 620 ← 632 | 691 | | 681 ← 691, 662 ← 680 |
| 645 | | 640 ← 645, 614 ← 639 | 692 | 394 ← 692 | 692 ← 692, 661 ← 691 |
| 646 | 398 ← 646 | 644 ← 646, 629 ← 643 | 693 | | 693 ← 693, 671 ← 692 |
| 647 | 643 ← 647 | 647 ← 647, 643 ← 646 | 694 | | 689 ← 694, 644 ← 688 |
| 648 | | 648 ← 648, 626 ← 647 | 695 | 484 ← 695 | 692 ← 695, 681 ← 691 |
| 649 | 613 ← 649 | 639 ← 649, 620 ← 638 | 696 | | 684 ← 696, 651 ← 683 |
| 650 | 648 ← 650 | 648 ← 650, 645 ← 647 | 697 | 431 ← 697 | 688 ← 697, 674 ← 687 |
| 651 | | 626 ← 651, 599 ← 625 | 698 | 484 ← 698 | 684 ← 698, 668 ← 683 |
| 652 | 560 ← 652 | 652 ← 652, 626 ← 651 | 699 | | 669 ← 699, 624 ← 668 |
| 653 | | 651 ← 653, 642 ← 650 | 700 | | 695 ← 700, 680 ← 694 |
| 654 | | 634 ← 654, 594 ← 633 | 701 | | 691 ← 701, 678 ← 690 |
| 655 | 568 ← 655 | 647 ← 655, 631 ← 646 | 702 | 666 ← 702 | 666 ← 702, 629 ← 665 |
| 656 | | 650 ← 656, 631 ← 649 | 703 | | 698 ← 703, 690 ← 697 |
| 657 | 620 ← 657 | 657 ← 657, 650 ← 656 | 704 | | 695 ← 704, 614 ← 694 |
| 658 | 604 ← 658 | 652 ← 658, 644 ← 651 | 705 | 687 ← 705 | 705 ← 705, 698 ← 704 |
| 659 | | 647 ← 659, 614 ← 646 | 706 | | 684 ← 706, 622 ← 683 |
| 660 | | 647 ← 660, 612 ← 646 | 707 | | 694 ← 707, 679 ← 693 |
| 661 | | 659 ← 661, 624 ← 658 | 708 | 422 ← 708 | 702 ← 708, 672 ← 701 |
| 662 | 366 ← 662 | 659 ← 662, 646 ← 658 | 709 | | 709 ← 709, 706 ← 708 |
| 663 | 407 ← 663 | 657 ← 663, 627 ← 656 | 710 | | 710 ← 710, 696 ← 709 |
| 664 | | 664 ← 664, 625 ← 663 | 711 | 620 ← 711 | 709 ← 711, 698 ← 708 |
| 665 | 633 ← 665 | 661 ← 665, 642 ← 660 | 712 | | 704 ← 712, 683 ← 703 |
| 666 | | 664 ← 666, 633 ← 663 | 713 | 673 ← 713 | 707 ← 713, 697 ← 706 |
| 667 | | 658 ← 667, 647 ← 657 | 714 | 692 ← 714 | 708 ← 714, 683 ← 707 |
| 668 | | 663 ← 668, 640 ← 662 | 715 | | 715 ← 715, 709 ← 714 |
| 669 | | 649 ← 669, 611 ← 648 | 716 | 534 ← 716 | 704 ← 716, 684 ← 703 |
| 670 | 518 ← 670 | 670 ← 670, 665 ← 669 | 717 | | 708 ← 717, 687 ← 707 |
| 671 | 657 ← 671 | 669 ← 671, 657 ← 668 | 718 | | 718 ← 718, 689 ← 717 |
| 672 | | 668 ← 672, 662 ← 667 | 719 | 570 ← 719 | 713 ← 719, 705 ← 712 |
| 673 | 646 ← 673 | 673 ← 673, 653 ← 672 | 720 | | 692 ← 720, 662 ← 691 |
| 674 | | 672 ← 674, 658 ← 671 | 721 | 713 ← 721 | 721 ← 721, 713 ← 720 |
| 675 | | 671 ← 675, 608 ← 670 | 722 | 492 ← 722 | 719 ← 722, 680 ← 718 |
| 676 | 436 ← 676 | 668 ← 676, 648 ← 667 | 723 | | 723 ← 723, 692 ← 722 |
| 677 | | 677 ← 677, 647 ← 676 | 724 | | 720 ← 724, 712 ← 719 |
| 678 | | 674 ← 678, 648 ← 673 | 725 | | 719 ← 725, 701 ← 718 |
| 679 | 614 ← 679 | 674 ← 679, 653 ← 673 | 726 | 722 ← 726 | 726 ← 726, 722 ← 725 |
| 680 | | 667 ← 680, 636 ← 666 | 727 | 548 ← 727 | 721 ← 727, 710 ← 720 |

Continued ...

| n | 2-tap MFSR | 3-tap MFSR | n | 2-tap MFSR | 3-tap MFSR |
|-----|------------|----------------------|------|------------|--------------------------|
| 728 | | 694 ← 728, 651 ← 693 | 759 | 662 ← 759 | 753 ← 759, 701 ← 752 |
| 729 | 672 ← 729 | 722 ← 729, 705 ← 721 | 760 | | 758 ← 760, 719 ← 757 |
| 730 | 584 ← 730 | 727 ← 730, 712 ← 726 | 761 | 759 ← 761 | 761 ← 761, 759 ← 760 |
| 731 | | 730 ← 731, 724 ← 729 | 762 | 680 ← 762 | 715 ← 762, 648 ← 714 |
| 732 | | 730 ← 732, 726 ← 729 | 763 | | 748 ← 763, 730 ← 747 |
| 733 | | 729 ← 733, 722 ← 728 | 764 | | 753 ← 764, 738 ← 752 |
| 734 | | 728 ← 734, 695 ← 727 | 765 | | 756 ← 765, 737 ← 755 |
| 735 | 692 ← 735 | 730 ← 735, 713 ← 729 | 766 | | 744 ← 766, 713 ← 743 |
| 736 | | 732 ← 736, 703 ← 731 | 767 | 600 ← 767 | 757 ← 767, 733 ← 756 |
| 737 | 733 ← 737 | 737 ← 737, 733 ← 736 | 768 | | 738 ← 768, 689 ← 737 |
| 738 | 392 ← 738 | 728 ← 738, 692 ← 727 | 769 | 650 ← 769 | 759 ← 769, 740 ← 758 |
| 739 | | 739 ← 739, 716 ← 738 | 770 | | 760 ← 770, 745 ← 759 |
| 740 | 588 ← 740 | 730 ← 740, 697 ← 729 | 771 | | 763 ← 771, 738 ← 762 |
| 741 | | 721 ← 741, 683 ← 720 | 772 | 766 ← 772 | 766 ← 772, 759 ← 765 |
| 742 | | 728 ← 742, 671 ← 727 | 773 | | 757 ← 773, 715 ← 756 |
| 743 | 654 ← 743 | 743 ← 743, 731 ← 742 | 774 | 590 ← 774 | 766 ← 774, 750 ← 765 |
| 744 | | 736 ← 744, 699 ← 735 | 775 | 409 ← 775 | 772 ← 775, 757 ← 771 |
| 745 | 488 ← 745 | 742 ← 745, 718 ← 741 | 776 | | 760 ← 776, 717 ← 759 |
| 746 | 396 ← 746 | 726 ← 746, 697 ← 725 | 777 | 749 ← 777 | 762 ← 777, 732 ← 761 |
| 747 | | 744 ← 747, 738 ← 743 | 778 | 404 ← 778 | 776 ← 778, 760 ← 775 |
| 748 | | 742 ← 748, 722 ← 741 | 779 | | 774 ← 779, 760 ← 773 |
| 749 | | 749 ← 749, 743 ← 748 | 780 | | 774 ← 780, 710 ← 773 |
| 750 | | 742 ← 750, 668 ← 741 | 781 | | 773 ← 781, 759 ← 772 |
| 751 | 734 ← 751 | 750 ← 751, 734 ← 749 | 782 | 454 ← 782 | 762 ← 782, 722 ← 761 |
| 752 | | 746 ← 752, 619 ← 745 | 783 | 716 ← 783 | 773 ← 783, 747 ← 772 |
| 753 | 596 ← 753 | 749 ← 753, 741 ← 748 | 784 | | 771 ← 784, 726 ← 770 |
| 754 | 736 ← 754 | 746 ← 754, 733 ← 745 | 785 | 694 ← 785 | 783 ← 785, 775 ← 782 |
| 755 | | 746 ← 755, 734 ← 745 | 786 | | 781 ← 786, 756 ← 780 |
| 756 | 408 ← 756 | 747 ← 756, 684 ← 746 | 1024 | | 991 ← 1024, 940 ← 990 |
| 757 | | 757 ← 757, 751 ← 756 | 2048 | | 2030 ← 2048, 1925 ← 2029 |
| 758 | | 751 ← 758, 706 ← 750 | 4096 | | 4079 ← 4096, 3944 ← 4078 |

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] 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.
- [3] N.P. Cagigal and S. Bracho. Algorithmic determination of linear-feedback in a shift register for pseudorandom binary sequence generation. *IEE Proceedings G. Electronic Circuits and Systems*, 133:191–4, 1986.
- [4] 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.
- [5] R.W. Ward and T.C.A. Molteno. Generation of Large Maximum-cycle Linear Feedback Shift Registers. *Submitted to IEEE Transactions on Computers*, 2007.



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

