Generation of pseudorandom sequences for use in cross-correlation modulation

D. D. Koleske[a] and S. J. Sibener
The Department of Chemistry and The James Franck Institute, The University of Chicago, 5640 South Ellis Avenue, Chicago, Illinois 60637

(Received on 16 September 1991; accepted for publication 24 March 1992)

In this article we discuss how pseudorandom sequences are generated for use in cross-correlation modulation experiments and present means for generating all pseudorandom sequences (modulo-two) that have a maximum length of $N=2^n-1$, with $n=2$–12. We explain the criteria that the pseudorandom sequences must satisfy, and find the set of recursion coefficients which are used to generate the pseudorandom sequences. These sets of recursion coefficients were calculated for $n=2$–16, with $n=2$–12 being explicitly presented in this article. We also explain how each set of recursion coefficients can be used to generate maximum length pseudorandom sequences of length sufficient for use in cross-correlation chopping.

Despite their usefulness as random number generators, data encryption devices, and white noise sources,[1] maximum-length pseudorandom sequences (MLPRS), or cross-correlation (CC) modulation have been exploited only sparingly in experimental settings. Most notably, they have been used in a variety of time-of-flight (TOF) scattering experiments to gate a flux of particles which are then detected in a time-resolved fashion. In these experiments the incident flux of particles has typically been supplied by either a thermal neutron source,[2–4] or by a molecular beam.[5–7] A cross-correlation (CC) chopping technique is generally favored over single-shot chopping when both chopping procedures produce identical backgrounds due to the significant duty cycle advantages of CC modulation.[6,7] This advantage, the gain factor, may be as high as $N/4$,[6,7] where N is the length of the pattern.

Since the gain in duty cycle may significantly improve the signal-to-noise ratio and decrease the counting times needed to resolve TOF features, we present a table that contains all the base ten values for the *recursion coefficients* (RC) which can be used for the facile generation of MLPRS. Knowing the values of these RC, the MLPRS can be easily generated from the RC and used in CC modulation experiments. Previous papers have provided detailed accounts of both the properties and the usefulness of MLPRS in relation to CC chopping techniques.[2–7] In this article, we focus on the generation of the MLPRS (modulo-two) that have length $N=2^n-1$, where n is an integer. We have calculated all sets of RC for $n=2$–16, with the base ten values of these RC for $n=2$–12 being explicitly presented here. Examples and tables are presented that explain how the RC are used to generate "trial" sequences. These trial sequences are then tested to see if they satisfy three conditions which must be passed if the trial sequence is a MLPRS. Following the discussion and examples, the base ten values for the RC which generate MLPRS are presented. Also included is a discussion of two properties that were discovered in the calculated sets of RC. The purpose of this article is to enable the routine generation of MLPRS using these recursion coefficients for use in a variety of applications having a wide range of resolution requirements.

MLPRS were previously discussed by Peterson[8] and Watson[9] and were derived from polynomials $m(X)$ of degree of n, which are irreducible over the Galois field of integers modulo-two.[8,9] If the coefficients of $m(X)$ are used as the feedback elements in a binary shift register circuit,[1] the output of the shift register generates a MLPRS. [The coefficients of the polynomial $m(X)$ are the same as the recursion coefficients of length n.] Peterson has shown how to generate the coefficients of $m(X)$ algebraically and gives a table of these coefficients in octal form for values of $n=2$–34.[8] Watson generated one set of such polynomial coefficients for $n=2$, 100 using a computer algorithm.[9] Our study differs from these two studies in that all possible sets of recursion coefficients which can be used for generating MLPRS were checked computationally for $n=2$, 16.

There are three conditions that a sequence must satisfy for it to qualify as a MLPRS, and hence be of use in CC modulation. These conditions are: (1) that the sequence recur after $N=2^n-1$ steps, (2) that the autocorrelation of the sequence sum to 2^{n-1}, and (3) that the cross correlation of the sequence sum to 2^{n-2}. If these three conditions are met the sequence is a MLPRS.

MLPRS are not entirely random, but repeat themselves after N numbers are generated. This is the first condition that the MLPRS sequences must obey, and is the condition of recurrence, which means that the a_{i+N} element should equal the a_i element. This condition is important since the chopping, i.e., beam modulation, pattern is restarted upon the completion of one rotation of the wheel. This is both a necessary and practical constraint when the signal is generated by a mechanical chopper and collected by a multichannel scaler. The sequences are mathematically represented with 1's, which denote an open chopper slot, and 0's, which denote a closed chopper slot.

Since the sequences are not entirely random, we can define the sequence correlation by

[a]Current address: IBM T. J. Watson Research Center, P.O. Box 218, Yorktown Heights, NY 10598.

 0034-6748/92/083852-04$02.00

$$A_j = \sum_{i=0}^{N-1} a_i a_{i+j}. \quad (1)$$

The second condition that must be met for a trial MLPRS, is that when $j=0$, A_0 must equal 2^{n-1}. This operation counts the autocorrelation of the sequence which simply corresponds to summing the number of 1's in the sequence. When $j \neq 0$, A_j counts the cross correlation of the sequence. When a sequence is totally uncorrelated these elements are 0. However, if some correlation exists, A_j is greater than zero. Comsa *et al.*[6] and others,[3,4] have shown that when $j \neq 0$, A_j equals 2^{n-2}. This is the third condition that the trial MLPRS must satisfy. Using these three conditions implies that the total number of 1's in each MLPRS is $N/2$ and the number of 0's is $N/2-1$.[6] Using only these three requirements, i.e., (1) that the sequence be cyclic, (2) that the diagonal elements sum to 2^{n-1}, and (3) that the off-diagonal elements sum to 2^{n-2}, we now proceed to generate the sets of RC which in turn generate MLPRS.

We tested the sets of binary RC spanning the range from of $M=3$ to $M=N-1$, where $N=2^n-1$ and M is the base 10 representation of the RC. Each value of M is translated from its base 10 representation to its base 2 representation. For example, when $n=3$, $N=7$, M spans from 3 to 6 and the possible base 2 representations of the RC $(Q_3Q_2Q_1)$ are $M=3 \rightarrow 011$, $M=4 \rightarrow 100$, $M=5 \rightarrow 101$, and $M \rightarrow 110$. The values of $M=1,2$ are eliminated from testing for all n because a set of RC with only one RC equal to 1 will just repeat the initial values of a_1 through a_n. (Note that this statement is also true for $M=4$, which has only one RC equal to 1. This will also be true for every M which is a power of 2. These values for M can also be eliminated from the search.) The value for $M=N$ is eliminated since for this value of M all the RC are equal to 1, which generates a sequence with all 1's for odd n, or a sequence with alternating 1's and 0's for even n. A trial MLPRS is calculated using the binary values for M, in the following manner: The first n values of a_i, a_{1-3} in our present example, are set equal to 1. (This is not a unique choice and any other initial values can be assigned to the first n values, except choosing them all equal to 0.) The a_{i+1} element is obtained from the binary summation of the products of the n previous a_i's with the set of binary RC, $Q_nQ_{n-1}\cdots Q_3Q_2Q_1$, or more generally:

$$a_{i+1} = Q_n a_i \oplus Q_{n-1} a_{i-1} \oplus Q_{n-2} a_{i-2} \cdots \oplus Q_2 a_{i-n+2} \oplus Q_1 a_{i-n+1}, \quad (2)$$

where the symbol $\oplus$ means that the addition is modulo-two. The a_i's are then shifted by one index ($a_{i-n+1} \rightarrow a_{i-n}$, $a_{i-n+2} \rightarrow a_{i-n+1}$, etc.) and the next a_{i+1} is then calculated using Eq. (2). This procedure is continued until the a_{N+n} element is reached, in order to check that the sequence recurs to the initially assigned a_i's.

This procedure for generating the trial MLPRS using a set of binary RC is shown in more detail in Table I, again using $M=3$ $(n=3)$ as an example. The RC are shown on top of the second thru fourth columns as $Q_3=0$, $Q_2=1$, and $Q_1=1$. The first row shows an initial set of a_{1-3} all chosen equal to 1 and entered in the second through fourth columns in Table I. The sum of Eq. (2), $Q_1a_1 \oplus Q_2a_2 \oplus Q_3a_3 = 2$, and is shown in the fifth column with the modulo-two sum shown in sixth column. This modulo-two term, equal to 0 for this first row, is the value assigned to a_4. Stepping to the next index, $i+1=5$, the a_{2-4} values shown in columns 2–4 generate a modulo-two value of 1 for a_5. This generation process is continued until $i+1=10$ which is when a MLPRS will repeat the initial starting sequence (i.e., $a_{1-3}=111$). The MLPRS for this example is 1110010, and is shown in Table I.

TABLE I. Generation of the trial MLPRS: 1110010, for $n=3$, $N=7$, and $M=3$. The set of recursion coefficients is $Q_3=0$, $Q_2=1$, and $Q_1=1$. The first column contains the value of $i+1$, a_{i+1}, where i is the sequence index [Eq. (2)]. The second through fourth columns contain the curent values of a_{i-2} through a_i. The sum of Eq. (2) is shown in the fifth column and the modulo-2 sum is shown in the sixth column. The calculated MLPRS is read from top to bottom starting at $i+1=8=1$ down $i+1=10=3$; then it is read from $i+1=4$ to $i+1=7$.

$M=3$	$Q_3=0$	$Q_2=1$	$Q_1=1$		
$i+1$	a_i	a_{i-1}	a_{i-2}	sum	modulo-2 sum
4	1	1	1	2	0
5	0	1	1	2	0
6	0	0	1	1	1
7	1	0	0	0	0
8=1	0	1	0	1	1
9=2	1	0	1	1	1
10=3	1	1	0	1	1

This trial MLPRS for $M=3$ is then tested to see if it meets the three previously discussed conditions. For the above example, with $M=3$, the recurrence condition is met, as the values repeat: $a_1=a_8$, $a_2=a_9$, and $a_3=a_{10}$. The sum of the diagonal elements for this sequence equals 4, which satisfies the second condition. The third condition is also satisfied, and can be checked using Eq. (1) with $j \neq 0$; here for example, when $j=1$ we have

$$A_1 = 1*0+1*1+1*1+0*1+0*0+1*0+0*1=2. \quad (3)$$

Since this trial MLPRS meets all three conditions, the sequence 1110010 is a true MLPRS.

One property of MLPRS is that if the MLPRS is read in reverse (from right to left), the reverse sequence is also a MLPRS. This is demonstrated in Table II by producing the MLPRS for $M=5$ ($n=3$ and the Q_i's become $Q_3=1$,

TABLE II. Same as Table I except $M=5$ and the set of recursion coefficients: $Q_3=1$, $Q_2=0$, and $Q_1=1$. The resulting MLPRS is 1110100 which upon reversal is 1110010. This reversed sequence, 1110010, is identical to the MLPRS generated and shown in Table I.

$M=5$	$Q_3=1$	$Q_2=0$	$Q_1=1$		
$i+1$	a_i	a_{i-1}	a_{i-2}	sum	modulo-2 sum
4	1	1	1	2	0
5	0	1	1	1	1
6	1	0	1	2	0
7	0	1	0	0	0
8=1	0	0	1	1	1
9=2	1	0	0	1	1
10=3	1	1	0	1	1

TABLE III. Base 10 values for the recursion coefficients which produce MLPRS for $n=2$–12. For each value of n the value of $N=2^n-1$, M are shown.

n	N	M's
2	3	3
3	7	3
4	15	9
5	31	5, 15, 23
6	63	3, 27, 39
7	127	3, 9, 15, 29, 39, 43, 63, 75, 111
8	255	29, 43, 45, 77, 95, 99, 135, 207
9	511	17, 27, 45, 51, 89, 95, 111, 119, 125, 135, 149, 163, 175, 183, 189, 207, 219, 275, 287, 315, 335, 347, 383, 399
10	1023	9, 27, 39, 45, 101, 111, 139, 197, 215, 231, 243, 255, 269, 291, 317, 323, 343, 363, 399, 407, 455, 503, 567, 591, 603, 639, 735, 765, 791
11	2023	5, 23, 43, 45, 71, 99, 101, 113, 123, 141, 149, 159, 169, 177, 207, 231, 235, 245, 269, 275, 293, 297, 315, 317, 325, 347, 371, 373, 383, 387, 399, 427, 429, 441, 455, 485, 503, 519, 531, 533, 621, 639, 669, 679, 683,735, 751, 763, 771, 819, 831, 843, 863, 879, 893, 903, 907, 915, 943, 951, 957, 987, 999, 1035, 1055, 1111, 1131, 1139, 1175, 1179, 1203, 1215, 1223, 1271, 1295, 1319, 1351, 1391, 1439, 1467, 1495, 1511, 1575, 1631, 1695, 1743
12	4095	83, 105, 123, 125, 153, 209, 235, 263, 287, 291, 315, 335, 343, 363, 389, 435, 473, 473, 479, 525, 567, 573, 615, 627, 639, 697, 715, 783, 797, 825, 831, 845, 931, 1031, 1079, 1103, 1117, 1127, 1141, 1191, 1197, 1235, 1295, 1309, 1357, 1427, 1495, 1501, 1515, 1607, 1725, 1859, 1971, 1983, 2135, 2199, 2287, 2331, 2427, 2443, 2511, 2535, 2587, 2603, 2847, 2903, 2983, 3007, 3095, 3111, 3231, 3279, 3631

$Q_2=0$, and $Q_1=1$). This set of RC shown in Table II also produces a MLPRS, 1110100, which if reversed is 0010111. Because the sequence is cyclic it can be read (from left to right) starting at any point in the sequence, and the previously reversed sequence becomes 11100110. This sequence, 1110010, is the same as the sequence shown in Table I.

The sets of RC have another interesting property. After all of the possible sets of RC which generated MLPRS were found, a relationship was discovered between pairs of sets of RC with the same n. Paired sets of RC were found that were related to each other by shifting the least significant binary RC digit to the most significant binary digit position: for half of the RC sets, $Q_nQ_{n-1}\cdots Q_3Q_2Q_1$, a "shifted" set of RC was also found, $Q_1Q_nQ_{n-1}\cdots Q_3Q_2$, which also generated MLPRS. The property was taken into account when compiling the list of RC reported in Table III, and for listing the total number of RC in Table IV. For the sets of RC listed in Table III, the lowest RC, Q_1, is always equal to 1 so that M is always odd. Therefore the "shifted" set of RC obtained by moving Q_1 to the Q_n position always results in a set of "shifted" RC that have larger numerical value than the "initial" RC (shifted M is greater than initial M). For each set of RC shown in Table III, shifting the least significant binary digit to the most significant binary digit position can only be applied once. Shifting the RC listed in Table III more than once will not generate MLPRS.

TABLE IV. The total number of sets of recursion coefficients (excluding the shifted set of recursion coefficients) as a function n.

n	No. of MLPRS
2	1
3	1
4	1
5	3
6	3
7	9
8	8
9	24
10	30
11	88
12	72
13	315
14	378
15	900
16	1024

The sets of RC reported in Table III were screened in the following manner. Once a set of RC passed the tests to prove it generated a MLPRS, its shifted complement was calculated and stored in an array. Subsequent sets of RC which also generated MLPRS were then screened to see if they were previously listed in the shifted complement array. If the subsequent set of RC was listed in the shifted complement array, the set was not stored. If the set was not found listed in the shifted complement array, its M value was stored and the RC elements were added to the shifted complement array. For example, shifting the set of RC (011) in Table I, gives the set of RC (101) which are identical to the set of RC shown in Table II. The set of RC was screened in this manner to cut down on the number of M's reported in Table III.

The sets of RC we have found (excluding the shifted RC) are shown in Table III, for $n=2$–12 and the number of unique MLPRS (excluding the shifted RC) are shown in Table IV for $n=2$–16. These coefficients can be easily used to generate MLPRS for any value of n. The MLPRS can then be machined or lithographically etched onto a mechanical wheel, or applied as voltage pulses, to gate experiments.

The MLPRS generated from the sets of RC in Table III can be compared to previously published CC wheel patterns.[4-6] We transcribed the CC pattern in a clockwise fashion from the picture of each wheel shown in each of the following references.[4-6] Nowikow and Grice designed a CC wheel with four identical patterns of 31 sequence elements[4] which corresponds to the first set of RC, Q_i's=00101 in the $n=5$ section of Table III, $M=5$. Hirschy and Aldridge designed a CC wheel with one pattern of 255 sequence elements[5] which corresponds to the sixth set of Q_i's =01100011 in the $n=8$ section, $M=99$. Finally, the CC wheel designed by Comsa *et al.* has two identical patterns with 255 sequence elements[6] and corresponds to the reverse MLPRS generated from the first set of Q_i's =00011101 in the $n=8$ section, $M=29$. In addition, we find that the two element RC for $n=2$, 12 in Horowitz and Hill are found in Table III.[1] We note that the RC pre-

sented in Table III can be used to generate a large selection of MLPRS for use in CC modulation experiments, many of which have been not previously used for such purposes.

In conclusion, we have presented the sets of recursion coefficients in Table III for $n=2$–12 and demonstrated how these recursion coefficients can be used to generate maximum length pseudorandom sequences. These sequences can be exploited for cross-correlation modulation measurements. The signal-to-noise enhancement resulting from such CC chopping will depend primarily on how the increase in duty cycle influences the background counting rate. Providing a list of sequences having differing lengths is useful, as one can now conveniently select the appropriate MLPRS length which achieves the desired time resolution for a given application. For a mechanical chopper spinning near 400 Hz the time resolution on any time-of-flight (TOF) feature is ≈ 5 μs for $n=9$, but decreases to ≈ 2.5 μs for $n=10$. When changing from lower time resolution to higher, the lithographic precision of the etched chopper wheel will decrease. However this is not a problem since imperfections in the etched wheel can generally be corrected for during the deconvolution.[6] The actual choice of pattern can therefore depend on the desired time resolution.

We thank D. F. Padowitz, S. F. King, and T. J. Curtiss. This work was supported, in part, by the Air Force Office of Scientific Research and the National Science Foundation Materials Research Laboratory at The University of Chicago.

[1] P. Horowitz and W. Hill, *The Art of Electronics* (Cambridge, London, 1982).
[2] K. Sköld, Nucl. Instrum. Methods **63**, 114 (1968).
[3] G. Wilhelmi and F. Gompf, Nucl. Instrum. Methods **81**, 36 (1970).
[4] C. V. Nowikow and R. Grice, J. Phys. E **12**, 515 (1979).
[5] W. L. Hirschy and J. P. Aldridge, Rev. Sci. Instrum. **42**, 381 (1971).
[6] G. Comsa, R. David, and B. J. Schumacher, Rev. Sci. Instrum. **52**, 789 (1981).
[7] R. David, K. Kern, P. Zeppenfeld, and G. Comsa, Rev. Sci. Instrum. **57**, 2771 (1986).
[8] W. W. Peterson, *Error-Correcting Codes* (Wiley, New York, 1961).
[9] E. J. Watson, Math. Comp. **16**, 368 (1962).