Modified Jacobi sequences

D.H.Green and P.R.Green

Abstract: Quadratic residue and twin prime sequences are well known types of binary sequence with ideal periodic autocorrelation functions. These are just special cases of much larger families of sequences referred to here as Legendre sequences and modified Jacobi sequences. Although these more general forms are suboptimal and do not have ideal autocorrelation functions, nevertheless they do exhibit out-of-phase autocorrelation values which are independent of their lengths, and so the longer sequences may be useful. The structure and properties of these sequences are investigated, and a two-dimensional array representation that enables the sequences and their autocorrelation functions to be derived in a simple and compact manner are employed .

1 Introduction

Binary sequences which exhibit good periodic or aperiodic autocorrelation properties are extremely useful in many areas of communication engineering and many sources have been identified over the years [1, 2]. Those sequences which exhibit the ideal two-valued periodic autocorrelation (such as m-sequences, GMW sequences, quadratic residue sequences, twin prime sequences) have been studied extensively. Unfortunately, these ideal types are not available in large numbers or for a wide range of sequence lengths. This makes the search for suboptimal but nevertheless 'good' sequences a worthwhile activity. Legendre sequences, Jacobi sequences and especially modified Jacobi sequences fall into this category. They also possess good aperiodic correlation properties and have high linear equivalence which gives them some cryptographic significance. This paper investigates the construction and properties of these types.

It is customary, when studying binary sequences for their correlation properties, to employ the values $+1$ and -1 to represent the digits of the sequence in place of the usual 0 and 1. This ensures that multiplication on $+1$ and -1 is equivalent to mod-2 addition on 0 and 1, and thereby enables the conventional definitions of correlation to yield meaningful results in the binary case.

Let $\boldsymbol{a} = \{a_0 a_1 a_2 \ldots a_{L-1}\}$ be a binary sequence of length L in which $a_i = 0$ or 1, and let $\hat{\boldsymbol{a}} = \{\hat{a}_0 \hat{a}_1 \hat{a}_2 \ldots \hat{a}_{L-1}\}$ be the same sequence represented in $+1$ and -1 form. Thus, $\hat{a}_i = 1\text{–}2a_i$. The periodic autocorrelation function $r(\tau)$, of $\hat{a}$, can be taken as

$$r(\tau) = \sum_{i=0}^{L-1} \hat{a}_i \cdot \hat{a}_{i+\tau} \quad 0 \le \tau \le L-1 \tag{1}$$

wherein the suffix $i + \tau$ is interpreted mod-L. Alternatively, a simpler definition may be adopted which can be applied to either form of sequence representation and is given by

$$r(\tau) = A_\tau - D_\tau \quad 0 \le \tau \le L-1 \tag{2}$$

where A_τ is the number of agreements and D_τ is the number of disagreements between the sequence and its *cyclic* shift by τ places. Note that $A_\tau + D_\tau = L$, and so

$$r(\tau) = L - 2D_\tau \quad 0 \le \tau \le L-1 \tag{3}$$

Also, $r(0) = L$ and this represents the maximum autocorrelation value.

The definition of the aperiodic autocorrelation of the two-valued sequence $\hat{\mathbf{a}} = \hat{a}_0 \hat{a}_1 \ldots \hat{a}_{L-1}$ of length L, at a relative *linear* shift of τ places, can be written as

$$c(\tau) = \sum_{r=0}^{L-\tau-1} \hat{a}_r \cdot \hat{a}_{r+\tau} \equiv A'_\tau - D'_\tau \tag{4}$$

where A'_τ is the number of agreements and D'_τ is the number of disagreements between the sequence and the overlap of length $L - \tau$ with its shift of τ places.

In this paper, the authors, adopt the agreements-disagreements forms of definition and employ the sequences in their 0 and 1 forms.

The aperiodic autocorrelation merit factor $\mathrm{MF_a}$ introduced by Golay [3] and defined as

$$\mathrm{MF_s} = \frac{L^2}{2\sum_{\tau=1}^{L-1} |c(\tau)|^2} \tag{5}$$

provides a convenient measure of 'goodness' of the aperiodic autocorrelation properties of a binary sequence. It is a simple matter to establish the relationship between the aperiodic and periodic autocorrelation coefficients for the same sequence. This reveals that,

$$r(0) = c(0) = L$$

$$r(\tau) = c(\tau) + c(L - \tau) \text{ for } \tau \ne 0 \tag{6}$$

IEE Proceedings online no. 20000538

DOI: 10.1049/ip-cdt:20000538

Paper first received 9th July 1999 and in revised form 27th January 2000

The authors are with the Department of Electrical Engineering and Electronics, University of Manchester Institute of Science and Technology, P.O. Box 88, Sackville Street, Manchester M60 1QD, UK

0	15	30	10	25	5	20
21	1	16	31	11	26	6
7	22	2	17	32	12	27
28	8	23	3	18	33	13
14	29	9	24	4	19	34

Fig. 1 *Array format for folded sequence of length 35*

Thus, the periodic values can be deduced from the aperiodic values but not *vice-versa*. It is useful to define a periodic version of the merit factor:

$$\mathrm{MF_p} = \frac{L^2}{\sum\limits_{\tau=1}^{L-1} |r(\tau)|^2} \qquad (7)$$

by direct substitution of the equivalent periodic values.

Sequences with a length L which can be factorised into two or more relatively prime factors can be folded into a two-dimensional structure sometimes referred to as a pseudorandom array (PRA) [4]. This can provide a compact form of representation which is useful for manipulating the sequence and which can reveal interesting structural properties of the sequence. One method for performing this folding is to start at the top left-hand corner of the array with the first digit of the sequence and then to place subsequent digits down the diagonal by moving one position in each dimension at each step. When an edge is encountered, the array is re-entered at the opposite edge on the next row or column. In this way, each location in the array will be visited exactly once in one pass through the sequence, provided the dimensions of the array are relatively prime. Fig. 1 illustrates the result of this process when applied to a general sequence of length $L = 35 = 5 \times 7$. Note that, in the general case when $L = pq$, in the first column of the $p \times q$ array $i \equiv 0 \bmod q$ and in the first row $i \equiv 0 \bmod p$. The remainder of the array corresponds to values of i that are relatively prime to L, *i.e.* the highest common factor of i and L is 1. This situation is expressed symbolically as $(i, L) = 1$.

The sequence of L autocorrelation values can also be plotted in this way to give a compact two-dimensional representation of the autocorrelation function. Arrays of this kind are employed in the following investigations.

2 Legendre sequences

Legendre or quadratic residue sequences [1, 2] exist for all lengths L which are prime. They can be constructed using the Legendre symbol

$$\left(\frac{i}{p}\right)$$

which is defined as

$$\left(\frac{i}{p}\right) = \begin{cases} 0 & \text{if } i \text{ is a quadratic residue mod } p \\ 1 & \text{otherwise} \end{cases} \qquad (8)$$

The integer i is a quadratic residue mod p if the equation $x^2 \equiv i \bmod p$ has a solution x which is relatively prime to p.

A Legendre sequence $\boldsymbol{a} = \{a_0 a_1 a_2 \ldots a_{L-1}\}$ is then formed by writing

$$a_i = \left(\frac{i}{L}\right) \quad \text{for } 0 < i < L \qquad (9)$$

and the value of a_0 can be taken either as 0 or 1. As there are exactly $(p-1)/2$ quadratic residues (QR) and $(p-1)/2$ quadratic nonresidues (QNR), Legendre sequences are 'balanced'. If L is an odd prime with $L \equiv m \bmod 4$, then the periodic autocorrelation values $r(\tau)$ are

$$r(\tau) = \begin{cases} L & \text{for} \quad \tau = 0 \\ m-4 & \text{for} \quad \tau = \text{a QR mod } L \\ 2-m & \text{for} \quad \tau = \text{a QNR mod } L \end{cases} \qquad (10)$$

This gives rise to two classes of Legendre sequences.

Class 1: $L \equiv 3 \bmod 4$

$$r(\tau) = \begin{cases} L & \text{for } \tau = 0 \\ -1 & \text{otherwise} \end{cases} \qquad (11)$$

and so this class has the ideal two-valued autocorrelation function. For example, when $L = 11$, the quadratic residues are 1, 3, 4, 5 and 9. The corresponding Legendre sequence is

$$\boldsymbol{a} = \{\mathbf{1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1}\}$$

and its autocorrelation function is

$$\boldsymbol{r} = \{\mathbf{11,\ -1,\ -1,\ -1,\ -1,\ -1,\ -1,\ -1,\ -1,\ -1,\ -1}\}$$

Class 1 Legendre sequences exhibit a mirror-skew symmetry about a_0, and $a_{L-i} = \bar{a}_i$ The sequences conventionally referred as quadratic residue sequences belong to this class.

Class 2: $L \equiv 1 \bmod 4$

$$r(\tau) = \begin{cases} L & \text{for} \quad \tau = 0 \\ -3 & \text{for} \quad \tau = \text{a QR mod } L \\ 1 & \text{for} \quad \tau = \text{a QNR mod } L \end{cases} \qquad (12)$$

and so this class has a three-valued autocorrelation function. For example, when $L = 13$, the quadratic residues are 1, 3, 4, 9, 10, 12. The corresponding Legendre sequence is

$$\boldsymbol{a} = \{\mathbf{1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0}\}$$

and its autocorrelation function is

$$\boldsymbol{r} = \{\mathbf{13,\ -3,\ 1,\ -3,\ -3,\ 1,\ 1,\ 1,\ 1,\ -3,\ -3,\ 1,\ -3}\}$$

Class 2 Legendre sequences exhibit a mirror symmetry about a_0, with $a_{L-i} = a_i$

Using the results of eqns. 11 and 12, it is a simple matter to establish that the periodic merit factors of binary Legendre sequences are given by

$$\mathrm{MF_p} = \begin{cases} \dfrac{L^2}{(L-1)} & \text{for } L \equiv 3 \bmod 4 \\[2ex] \dfrac{L^2}{5(L-1)} & \text{for } L \equiv 1 \bmod 4 \end{cases} \qquad (13)$$

2.1 Proper decimation of Legendre sequences

As Legendre sequences have prime lengths all sampling values give rise to proper decimation and a sequence of samples with the same length as the original. If a Legendre sequence is sampled every s places, the sequence of samples will be identical to the original sequence in both value and phase if s is a quadratic residue mod L. If s is a quadratic nonresidue, the sequences of samples, other than a_0, will be the inverse of the original. Consider the previous class 1 sequence of length 11. If this is sampled with sampling value s, then the sequence of samples will be

$$\mathbf{1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1} \quad \text{if } s = 1, 3, 4, 5, 9$$

$$\mathbf{1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0} \quad \text{if } s = 2, 6, 7, 8, 10$$

For the class 2 sequence of length 13

1 0 1 0 0 1 1 1 1 0 0 1 0 if $s = 1, 3, 4, 9, 10, 12$

1 1 0 1 1 0 0 0 0 1 1 0 1 if $s = 2, 5, 6, 7, 8, 11$

In all cases, the sequences of samples exhibit the same autocorrelation values as the original sequences.

3 Jacobi sequences

Jacobi sequences [5, 6] exist for all lengths of the form $L = pq$, where both p and q are prime. They are constructed using the Jacobi symbol

$$\left[\frac{i}{pq}\right]$$

which is defined as

$$\left[\frac{i}{pq}\right] = \left(\frac{i}{p}\right) \oplus \left(\frac{i}{q}\right) \qquad 0 \leq i < L \tag{14}$$

A Jacobi sequence $\boldsymbol{b} = \{b_0 b_1 b_2 \dots b_{L-1}\}$ can be formed by writing

$$b_i = \left[\frac{i}{pq}\right] = \left(\frac{i}{p}\right) \oplus \left(\frac{i}{q}\right) \qquad 0 \leq i < L \tag{15}$$

Thus, $b_i = 0$ if i, expressed mod p or mod q, is a quadratic residue for both p and q, or is a quadratic nonresidue for both p and q. Otherwise, $b_i = 1$. It follows that Jacobi sequences can be constructed from the modulo-2 sum of two Legendre sequences with lengths p and q, respectively. The periodic autocorrelation function of the Jacobi sequence can also be constructed from a product of the autocorrelation functions of the two Legendre sequences. Consider the case $p = 5$, $q = 7$ so that $L = 35$. The Legendre sequences of lengths 5 and 7 are **1 0 1 1 0** and **1 0 0 1 0 1 1**. Their autocorrelation functions are $\{5, -3, 1, 1, -3\}$ and $\{7, -1, -1, -1, -1, -1, -1\}$. Thus, the Jacobi sequence of length 35 is formed by term-by-term modulo-2 addition as follows:

$$\begin{array}{l}
\mathbf{10110101101011010110101101011010110} \\
\underline{\mathbf{10010111001011100101110010111001011}} \\
\mathbf{00100010100000110011011111100011101}
\end{array}$$

and its autocorrelation function takes the values

```
 5  -3   1   1  -3   5  -3  1   1  -3   5  -3   1   1  -3   5  -3   1
 7  -1  -1  -1  -1  -1  -1  7  -1  -1  -1  -1  -1  -1   7  -1  -1  -1
----------------------------------------------------------------------
35   3  -1  -1   3  -5   3  7  -1   3  -5   3  -1  -1 -21  -5   3  -1

  1  -3   5  -3   1   1  -3   5  -3   1  1  -3   5  -3   1   1  -3
 -1  -1  -1   7  -1  -1  -1  -1  -1  -1  7  -1  -1  -1  -1  -1  -1
-------------------------------------------------------------------
 -1   3  -5 -21  -1  -1   3  -5   3  -1  7   3  -5   3  -1  -1   3
```

In this example, it is found that $r(\tau) \in \{35, 7, 3, -1, -5, -21\}$ and note that this set of values can be related to a 'product' of the values for the two Legendre sequences, *i.e.* $\{5, 1, -3\} \times \{7, -1\}$. In general, there are four cases depending on the interaction of the two types of Legendre sequence. These can be summarised as follows:

$$\begin{array}{cccc}
0\;1\;1\;0\;1\;0\;0 & \quad & 35 & -5 & -5 & -5 & -5 & -5 & -5 \\
1\;0\;0\;1\;0\;1\;1 & & -21 & 3 & 3 & 3 & 3 & 3 & 3 \\
0\;1\;1\;0\;1\;0\;0 & & 7 & -1 & -1 & -1 & -1 & -1 & -1 \\
0\;1\;1\;0\;1\;0\;0 & & 7 & -1 & -1 & -1 & -1 & -1 & -1 \\
1\;0\;0\;1\;0\;1\;1 & & -21 & 3 & 3 & 3 & 3 & 3 & 3 \\
a & & & & & b & & &
\end{array}$$

Fig. 2 *Arrays formed from Jacobi sequence of length 35 and its autocorrelation function*

(i) $p \equiv 3 \bmod 4, q \equiv 3 \bmod 4;$
$r(\tau) \in \{p, -1\} \times \{q, -1\} = \{pq, -p, -q, 1\}$

(ii) $p \equiv 3 \bmod 4, q \equiv 1 \bmod 4;$
$r(\tau) \in \{p, -1\} \times \{q, 1, -3\} = \{pq, p, -3p, -q, -1, 3\}$

(iii) $p \equiv 1 \bmod 4, q \equiv 3 \bmod 4;$
$r(\tau) \in \{p, 1, -3\} \times \{q, -1\} = \{pq, q, -3q, -p, -1, 3\}$

(iv) $p \equiv 1 \bmod 4, q \equiv 1 \bmod 4;$
$r(\tau) \in \{p, 1, -3\} \times \{q, 1, -3\}$
$= \{pq, p, -3p, q, 1, -3, -3q, 9\}$

The previous example is seen to be of type (iii).

The fact that Jacobi sequences have lengths of the form $L = pq$ ensures that they can be folded into a $p \times q$ array. Fig. 2*a* shows the array formed from the previous sequence of length 35 and Fig. 2*b* gives the array version of its autocorrelation values. Both these arrays are seen to have interesting structures.

Arrays can also be employed in the construction of Jacobi sequences and their autocorrelation functions. If two sequences of length pq are considered, the first made up from q repetitions of the Legendre sequence of length p, and the second made up from p repetitions of the Legendre sequence of length q, which are then plotted on two separate $p \times q$ arrays, the array of the corresponding Jacobi sequence can be found by adding these two arrays in a cell-by-cell mod-2 fashion. In fact, the first array will consist of identical columns containing the Legendre sequence of length p and, consequently, it has rows which are either all 1s or all 0s. Similarly, the second array will have identical rows containing the Legendre sequence of length q and columns which are either all 1s or all 0s. Figs. 3*a* and 3*b* illustrate this for the previous example with $p = 5$, $q = 7$. When these two arrays are added the Jacobi sequence is formed as can be seen from Fig. 3*c*.

The constant nature of the rows of the first array and the columns of the second ensure that the rows of the sum

$$\begin{array}{ccccc}
1\;1\;1\;1\;1\;1\;1 & & 1\;0\;0\;1\;0\;1\;1 & & 0\;1\;1\;0\;1\;0\;0 \\
0\;0\;0\;0\;0\;0\;0 & & 1\;0\;0\;1\;0\;1\;1 & & 1\;0\;0\;1\;0\;1\;1 \\
1\;1\;1\;1\;1\;1\;1 & \oplus & 1\;0\;0\;1\;0\;1\;1 & = & 0\;1\;1\;0\;1\;0\;0 \\
1\;1\;1\;1\;1\;1\;1 & & 1\;0\;0\;1\;0\;1\;1 & & 0\;1\;1\;0\;1\;0\;0 \\
0\;0\;0\;0\;0\;0\;0 & & 1\;0\;0\;1\;0\;1\;1 & & 1\;0\;0\;1\;0\;1\;1 \\
a & & b & & c
\end{array}$$

Fig. 3 *Array of Jacobi sequence of length 35 formed by adding arrays of Legendre sequences*

$$\begin{array}{c|ccccccc}
 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
\hline
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}$$

Fig. 4 *Array construction using row and column labelling*

array are either the Legendre sequence of length q or its inverse (0s and 1s interchanged) and the columns are either the Legendre sequence of length p or its inverse. This enables a more direct method of constructing the final array to be devised. If the rows are labelled with the digits of the sequence of length p and the columns with the sequence of length q, then working down the rows (or along the columns) the row sequence (column sequence) or its inverse is entered according to whether the label on the row (column) is a 0 or a 1, respectively. This process is illustrated for the previous example in Fig. 4. This procedure is similar to that employed by Calabro and Wolf [5] to construct what they termed quadratic residue arrays. Alternatively, the value in each position of the array takes on the mod-2 sum of its co-ordinates. The Jacobi sequence itself can derived from the final array by following the path of the plotting procedure described above and reading off the digits at each step.

A similar technique can be used to derive the autocorrelation function array, but in this case the two factor arrays are multiplied together on a cell-by-cell basis to give the final array. Alternatively, if the row and column labelling is adopted, each cell takes on the value of the product of its co-ordinates. This is illustrated in Fig. 5. The unfolded version of the autocorrelation function can also be read off from its array in a similar manner to that desribed in the preceding test for deriving the sequence.

3.1 Sampling of Jacobi sequences

As Jacobi sequences have composite lengths of the form $L = pq$, with p and q both prime, not all sampling values will lead to proper decimation. This will only arise when the sampling values s is relatively prime to L, and consequently, must not be a multiple of either p or q. There are exactly $(p - 1)(q - 1)$ relatively prime values which fall into four sets of $(p - 1)(q - 1)/4$ equivalent values, each of which produces a distinct sequence of samples.

Jacobi sequences are formed from the sum of two Legendre sequences of lengths p and q, respectively, and so sampling a Jacobi sequence is equivalent to sampling these component sequences. As observed in this paper, when a Legendre sequence is sampled either the original sequence or its inverse (apart from a_0) is obtained. The four sets of sampling values correspond to the four possible cases listed as follows:

$$\begin{array}{c|ccccccc}
 & 7 & -1 & -1 & -1 & -1 & -1 & -1 \\
\hline
5 & 35 & -5 & -5 & -5 & -5 & -5 & -5 \\
-3 & -21 & 3 & 3 & 3 & 3 & 3 & 3 \\
1 & 7 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 7 & -1 & -1 & -1 & -1 & -1 & -1 \\
-3 & -21 & 3 & 3 & 3 & 3 & 3 & 3
\end{array}$$

Fig. 5 *Autocorrelation function array constructed using row and column labelling*

Case (i): s is a QR mod p and a QR mod q. The sampled component sequences are both identical to their original forms, and so they combine to give an identical version of the Jacobi sequence.

Case (ii): s is a QR mod p and a QNR mod q. The component sequence formed from the length p Legendre sequence is unchanged by sampling but that corresponding to the length q Legendre sequence becomes inverted (apart from the positions corresponding to a_0). The combined sequence is therefore distinct from the original Jacobi sequence.

Case (iii): s is a QNR mod p and a QR mod q. Now the component sequence corresponding to the length p Legendre sequence becomes inverted, but that derived from the length q sequence remains unchanged. These combine to form another sequence distinct from the original Jacobi sequence.

Case (iv): s is a QNR mod p and a QNR mod q. Now both component sequences become inverted by sampling and these combine to produce another sequence distinct from the original Jacobi sequence.

All four sequences resulting have the same autocorrelation values as the original Jacobi sequence.

These sequences of samples can also be derived using the array structure described in the preceding text by employing the Legendre sequences or their inverses (apart from a_0) to label the rows and columns. This is illustrated in Fig. 6 using the previous example sequence of length 35. The four arrays corresponding to the four cases listed above yield the following sequences:

(i) **0 0 1 0 0 0 1 0 1 0 0 0 0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 0 0 0 1 1 1 0 1**

for $s \in \{1, 4, 9, 11, 16, 29\}$

(ii) **0 1 0 1 1 0 0 1 0 1 0 1 1 1 0 1 1 1 0 0 0 0 0 0 0 1 0 1 1 1 1 0 0 1 0**

for $s \in \{2, 8, 18, 22, 23, 32\}$

$$\begin{array}{c|ccccccc}
 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
\hline
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}
\qquad
\begin{array}{c|ccccccc}
 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
\hline
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}$$

case(i) *case(ii)*

$$\begin{array}{c|ccccccc}
 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0
\end{array}
\qquad
\begin{array}{c|ccccccc}
 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1
\end{array}$$

case(iii) *case(iv)*

Fig. 6 *Derivation of sampled Jacobi sequences using arrays*

(iii) **0 1 0 1 1 1 0 0 0 1 1 1 1 1 1 0 1 1 0 0 1 1 0 0 0 0 0 1 0 1 0 0 0 1 0**

for $s \in \{6, 19, 24, 26, 31, 34\}$

(iv) **0 0 1 0 0 1 1 1 1 0 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 0 1 0 1 0 0 1 1 0 1**

for $s \in \{3, 12, 13, 17, 27, 33\}$

Note that case (iii) gives the reverse sequence of case (i) and case (iv) gives the reverse sequence of case (ii). The arrays for cases (i) and (iv), and for cases (ii) and (iii), differ only in the forms of the first rows and columns, whereas the main body of the array is the same in each pair.

When the Jacobi sequence is sampled with s equal to a multiple of p or q improper decimation occurs and p sequences of length q or q sequences of length p result. These short sequences are related to cyclic shifts of the component Legendre sequences or their inverses, and appear on the rows and columns of the array form of the Jacobi sequence.

4 Modified Jacobi sequences

The Jacobi sequences described in Section 3 do not exhibit particularly good autocorrelation functions and contain out-of-phase values which are related to the factors p and q. However, a relatively straightforward modification can radically improve this situation so that the out-of-phase autocorrelation values become dependent only on the difference k between p and q. These modified Jacobi sequences of length $L = pq$ can be defined as follows [5, 6]:

$$b_i = \begin{cases} \left(\frac{i}{p}\right) \oplus \left(\frac{i}{q}\right) & \text{for}(i, L) = 1 \quad 0 \leq i < L \\ 0 \quad \text{for } i \equiv 0 \bmod \ q \\ 1 \quad \text{otherwise} \end{cases} \tag{16}$$

This modification is equivalent to forcing b_i of the normal Jacobi sequence to be 0 for all i which are multiples of q and to be 1 for all i, other than $i = 0$, which are multiples of p. These modifications manifest themselves very clearly on the array version of the sequence. Those values of i which are multiples of q (*i.e.* $i \equiv 0 \bmod q$) lie on the first column of the array and those values of i which are multiples of p (*i.e.* $i \equiv 0 \bmod p$) lie on the first row of the array. Thus, to perform the modifications indicated by eqn. 11 it is necessary to make the first column hold all 0s and the first row (apart from the element in the first column) all 1s. This process is illustrated for the example sequence of length 35 in Fig. 7. The resulting sequence in this case is found to be

0 0 1 0 0 1 1 0 1 0 1 0 0 0 0 1 0 0 1 1 1 0 1 1 1 1 1 0 0 0 1 1 1 0 1

0	1	1	0	1	0	0		0	1	1	1	1	1	1
1	0	0	1	0	1	1		0	0	0	1	0	1	1
0	1	1	0	1	0	0		0	1	1	0	1	0	0
0	1	1	0	1	0	0		0	1	1	0	1	0	0
1	0	0	1	0	1	1		0	0	0	1	0	1	1
			unmodified								*modified*			

Fig. 7 *Modification of array version of Jacobi sequence*

These arrays also reveal that some of the values in the first column of the Jacobi sequence are already 0 and some elements on the first row are already 1, and, consequently, it is only necessary to change the remaining elements. This can be seen to be equivalent to adding an extra version of the inverted form of the Legendre sequence of length p to the first column and an extra version of the length q sequence to the first row. If these extra sequences are unfolded from the array, they form two sequences of length pq which are expanded versions of the Legendre sequences. That is, the first is made up from the sequence of length p with $q - 1$ 0s inserted between each digit and the second is the inverted from of the length q sequence with $p - 1$ 0s inserted between each digit. Thus, the modified Jacobi sequence can be thought of as a modulo-2 sum of four component sequences of length pq. The replicated versions of the two Legendre sequences of length p and q form the first two components, and expanded versions of the length p sequence and the inverted form of the length q sequence provide the third and fourth components. For example, in the case of the length 35 sequence:

10110101101011010110101101011010110

10010111001011100101110010111001011

10000000000000100000010000000000000

10000100001000000000100000000000000

00100110101000010011101111100011101

Henceforth, it is assumed, without loss of generality, that $q > p$, so that $k = q - p$ is an even integer. Two distinct classes of modified Jacobi sequences arise depending on the value of k.

Class 1: $k \equiv 2 \bmod 4$. Modified Jacobi sequences in this class have autocorrelation functions of the following form:

$$r(\tau) = \begin{cases} L & \text{for } \tau \equiv 0 \bmod p \text{ and } \tau \equiv 0 \bmod q \\ k - 3 & \text{for } \tau \equiv 0 \bmod p \text{ and } \tau \not\equiv 0 \bmod q \\ 1 - k & \text{for } \tau \not\equiv 0 \bmod p \text{ and } \tau \equiv 0 \bmod q \\ -1 & \text{for } \tau \not\equiv 0 \bmod p \text{ and } \tau \not\equiv 0 \bmod q \end{cases} \tag{17}$$

It follows that this class of modified sequences has a four-valued autocorrelation function except for the case $k = 2$. Then, $k - 3 = 1 - k = -1$, and the sequences have the ideal two-valued autocorrelation function $r(\tau) \in \{L, -1\}$. In this case, $q = p + 2$, and so p and q are consecutive or *twin primes*. The modified Jacobi sequences with $k = 2$ are better known as twin prime sequences [1, 2].

It follows that, in the autocorrelation spectrum,

L	occurs once
$k - 3$	occurs $q - 1$ times
-1	occurs $(p - 1)(q - 1)$ times
$1 - k$	occurs $p - 1$ times

and the periodic merit factor can be shown to take the form

$$\mathrm{MF_p} = \frac{L^2}{L + 2p(k-2)^2 + k(k-4)^2 - 9} \tag{18}$$

Sequences in this class are made up from Legendre sequences belonging to different classes, *i.e.* one from class 1 and one from class 2.

Class 2. $k \equiv 0 \bmod 4$. Modified Jacobi sequences in this class have autocorrelation functions of the following form:

$$r(\tau) = \begin{cases} L & \text{for } \tau \equiv 0 \bmod p, \text{ and } \tau \equiv 0 \bmod q \\ k-3 & \text{for } \tau \equiv 0 \bmod p, \text{ and } \tau \not\equiv 0 \bmod q \\ 1-k & \text{for } \tau \not\equiv 0 \bmod p, \text{ and } \tau \equiv 0 \bmod q \\ 1 & \text{for } \tau \not\equiv 0 \bmod p \text{ and mod } q, \\ & \text{and is a QR both mod } p \\ & \text{and mod } q \text{ or a QNR both mod } p \\ & \text{and mod } q \\ -3 & \text{for } \tau \not\equiv 0 \bmod p \text{ and mod } q, \\ & \text{and is a QR mod } p \\ & \text{and a QNR mod } q \text{ or } \textit{vice versa} \end{cases} \qquad (19)$$

It follows that this class of modified sequences has a five-valued autocorrelation function except for the case $k=4$. Then, $k-3=1$ and $1-k=-3$, and the sequences have three-valued autocorrelation functions with $r(\tau) \in \{L, 1, -3\}$.

Consequently,

$$\begin{array}{ll} L & \text{occurs once} \\ k-3 & \text{occurs } q-1 \text{ times} \\ 1 & \text{occurs } (p-1)(q-1)/2 \text{ times} \\ -3 & \text{occurs } (p-1)(q-1)/2 \text{ times} \\ 1-k & \text{occurs } p-1 \text{ times} \end{array}$$

and the periodic merit factor is given by

$$\mathrm{MF_p} = \frac{L^2}{5L + 2pk(k-4) + k[(k-4)^2 - 4] - 5} \qquad (20)$$

Sequences in this class are made up from Legendre sequences of the same class, *i.e.* both class 1 or both class 2.

Thus, for both classes of modified Jacobi sequences, the out-of-phase autocorrelation values are independent of the sequence length and depend only on the difference k between the two prime factors. For example, when

$$\begin{array}{ll} k=2 & r(\tau) \in \{L, -1\} \\ & \mathrm{MF_p} = L^2/(L-1) \\ k=4 & r(\tau) \in \{L, 1, -3\} \\ & \mathrm{MF_p} = L^2/(5L-21) \\ k=6 & r(\tau) \in \{L, 3, -1, -5\} \\ & \mathrm{MF_p} = L^2/(L+32p+15) \\ k=8 & r(\tau) \in \{L, 5, 1, -3, -7\} \\ & \mathrm{MF_p} = L^2/(5L+64p+91) \\ k=10 & r(\tau) \in \{L, 7, -1, -9\} \\ & \mathrm{MF_p} = L^2/(L+128p+351) \\ k=12 & r(\tau) \in \{L, 9, 1, -3, -11\} \\ & \mathrm{MF_p} = L^2/(5L+192p+715) \\ k=14 & r(\tau) \in \{L, 11, -1, -13\} \\ & \mathrm{MF_p} = L^2/(L+288p+1391) \\ k=16 & r(\tau) \in \{L, 13, 1, -3, -15\} \\ & \mathrm{MF_p} = L^2/(5L+384p+2235) \end{array}$$

etc.

When these autocorrelation functions are folded into their array formats regular structures emerge as can be observed in Fig. 8. For both classes, the maximum value L is placed in the first element of the array and the remainders of the first row and column take the value $k-3$ and $1-k$, respectively. For class 1 sequences, the remainder of the array holds -1, whereas for class 2 sequences the remainder of the array is equally shared between the values 1 and -3. The autocorrelation value 1 occurs in the positions corresponding to the 0s in the sequence array and the value -3 occurs in the positions of the 1s. Fig. 9 shows the variation of the periodic merit factor with sequence length for various values of k.

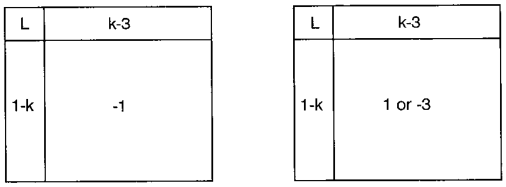


Fig. 8 *Structure of autocorrelation function of modified Jacobi sequences: Class 1 and Class 2*

4.1 Sampling modified Jacobi sequences

It has been observed that modified Jacobi sequences can be regarded as being composed of the mod-2 sum of four component sequences: a replicated form and an expanded form of two Legendre sequences. The expanded forms ensure that the first column on the array version of the sequence holds all 0s and the first row holds all 1s. The four cases of proper decimation identified for the unmodified sequences still apply, but now, when s is equivalent to

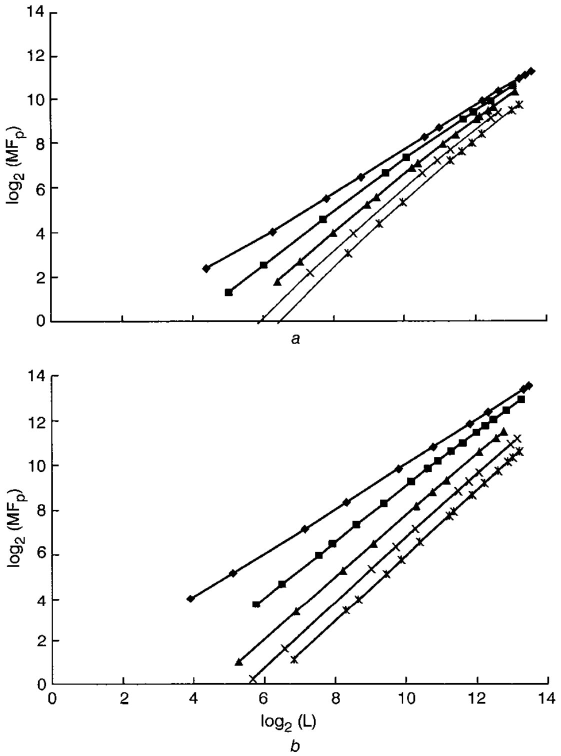


Fig. 9 *Periodic merit factor of modified Jacobi sequences for $k \leq 20$*

a $k=0 \bmod 4$	*b* $k=2 \bmod 4$
-◆- $k=4$	-◆- $k=2$
-■- $k=8$	-■- $k=6$
-▲- $k=12$	-▲- $k=10$
-×- $k=16$	-×- $k=14$
-×- $k=20$	-×- $k=18$

a QR mod p or mod q, both forms of each Legendre sequence remain unchanged, and when s is equivalent to a QNR both forms become inverted. This ensures that the arrays of the sampled modified Jacobi sequences still have an all 0s first column and an all 1s first row. As a result, only two distinct forms result and case (i) and case (iv) combine to yield the original sequence, and case (ii) and case (iii) combine to produce a new sequence. Thus, in the case of the length 35 sequence, the following holds:

00100110101000010011101111100011101

if $s \in \{1, 3, 4, 9, 11, 12, 13, 16, 17, 27, 29, 33\}$

01011100011111011100100001010110010

if $s \in \{2, 6, 8, 18, 19, 22, 23, 24, 26, 31, 32, 34\}$

Table 1: All available modified Jacobi sequences with $L < 5000$ and $k \leq 20$

k	p	q	L	$r(\tau)$
2	3	5	15	{15, −1}
	5	7	35	{35, −1}
	11	13	143	{143, −1}
	17	19	323	{323, −1}
	29	31	899	{899, −1}
	41	43	1763	{1763, −1}
	59	61	3599	{3599, −1}
4	3	7	21	{21, 1, −3}
	7	11	77	{77, 1, −3}
	13	17	221	{221, 1, −3}
	19	23	437	{437, 1, −3}
	37	41	1517	{1517, 1, −3}
	43	47	2021	{2021, 1, −3}
	67	71	4757	{4757, 1, −3}
6	5	11	55	{55, 3, −1, −5}
	7	13	91	{91, 3, −1, −5}
	11	17	187	{187, 3, −1, −5}
	13	19	247	{247, 3, −1, −5}
	17	23	391	{391, 3, −1, −5}
	23	29	667	{667, 3, −1, −5}
	31	37	1147	{1147, 3, −1, −5}
	37	43	1591	{1591, 3, −1, −5}
	41	47	1927	{1927, 3, −1, −5}
	47	53	2491	{2491, 3, −1, −5}
	53	59	3127	{3127, 3, −1, −5}
	61	67	4087	{4087, 3, −1, −5}
	67	73	4891	{4891, 3, −1, −5}
8	3	11	33	{33, 5, 1, −3, −7}
	5	13	65	{65, 5, 1, −3, −7}
	11	19	209	{209, 5, 1, −3, −7}
	23	31	713	{713, 5, 1, −3, −7}
	29	37	1073	{1073, 5, 1, −3, −7}
	53	61	3233	{3233, 5, 1, −3, −7}
	59	67	3953	{3953, 5, 1, −3, −7}
10	3	13	39	{39, 7, −1, −9}
	7	17	119	{119, 7, −1, −9}
	13	23	299	{299, 7, −1, −9}
	19	29	551	{551, 7, −1, −9}
	31	41	1271	{1271, 7, −1, −9}
	43	53	2279	{2279, 7, −1, −9}
	61	71	4331	{4331, 7, −1, −9}
12	5	17	85	{85, 9, 1, −3, −11}
	7	19	133	{133, 9, 1, −3, −11}
	11	23	253	{253, 9, 1, −3, −11}
	17	29	493	{493, 9, 1, −3, −11}
	19	31	589	{589, 9, 1, −3, −11}
	29	41	1189	{1189, 9, 1, −3, −11}
	31	43	1333	{1333, 9, 1, −3, −11}
	41	53	2173	{2173, 9, 1, −3, −11}
	47	59	2773	{2773, 9, 1, −3, −11}
	59	71	4189	{4189, 9, 1, −3, −11}
	61	73	4453	{4453, 9, 1, −3, −11}
14	3	17	51	{51, 11, −1, −13}
	5	19	95	{95, 11, −1, −13}
	17	31	527	{527, 11, −1, −13}
	23	37	851	{851, 11, −1, −13}
	29	43	1247	{1247, 11, −1, −13}
	47	61	2867	{2867, 11, −1, −13}
	53	67	3551	{3551, 11, −1, −13}
	59	73	4307	{4307, 11, −1, −13}
16	3	19	57	{57, 13, 1, −3, −15}
	7	23	161	{161, 13, 1, −3, −15}
	13	29	377	{377, 13, 1, −3, −15}
	31	47	1457	{1457, 13, 1, −3, −15}
	37	53	1961	{1961, 13, 1, −3, −15}
	43	59	2537	{2537, 13, 1, −3, −15}
18	5	23	115	{115, 15, −1, −17}
	11	29	319	{319, 15, −1, −17}
	13	31	403	{403, 15, −1, −17}
	19	37	703	{703, 15, −1, −17}
	23	41	943	{943, 15, −1, −17}
	29	47	1363	{1363, 15, −1, −17}
	41	59	2419	{2419, 15, −1, −17}
	43	61	2623	{2623, 15, −1, −17}
	53	71	3763	{3763, 15, −1, −17}
	61	79	4819	{4819, 15, −1, −17}
20	3	23	69	{69, 17, 1, −3, −19}
	11	31	341	{341, 17, 1, −3, −19}
	17	37	629	{629, 17, 1, −3, −19}
	23	43	989	{989, 17, 1, −3, −19}
	41	61	2501	{2501, 17, 1, −3, −19}
	47	67	3149	{3149, 17, 1, −3, −19}
	53	73	3869	{3869, 17, 1, −3, −19}
	59	79	4661	{4661, 17, 1, −3, −19}

Table 2: Legendre sequences for $L < 80$

Class	L	Legendre sequence
1	3	101
2	5	10110
1	7	1001011
1	11	10100011101
2	13	1010011110010
2	17	10010111001110100
1	19	1011000010101111001
1	23	10000101001100110101111
2	29	10110000101110110111010000110
1	31	1001001000011101010001111011011
2	37	1010011010000111011110111000010110010
2	41	10010011000111110101001010111110001100100
1	43	1011010110001000001110100011111011100101001
1	47	10000100001101010001101100100111010100111101111
2	53	10110100100010100011111100110011111100010100010010110
1	59	10100010101101100010000110000011111001111011100100101011101
2	61	1010001110110000011001011010111111010110100110000011011100010
1	67	1011010110011100001010000001101110100010011111101011110001100101001
1	71	10000001000101100100011100101001011100010110101100011101100101110111111
2	73	1000010100110111010011100010111101100001011110100011100101110110010100000
1	79	1001001100001011010000001001111001110101010100011000011011111101001011110011011

This new sequence of samples has the same autocorrelation values as the original and is observed to be the reverse of the original.

5 Imbalance of sequences

The imbalance of a binary sequence is defined as the difference between the number of 1s and the number of 0s. A Legendre sequence of length p (with $a_0 = 1$) contains $(p+1)/2$ 1s and $(p-1)/2$ 0s and, therefore, has an imbalance I given by

$$I = \frac{(p+1)}{2} - \frac{(p-1)}{2} = 1 \tag{21}$$

A Jacobi sequence of length $L = pq$, formed from the sum of two Legendre sequences can be shown to have $(pq-1)/2$ 1s and $(pq+1)/2$ 0s, and so its imbalance is given by

$$I = \frac{(pq-1)}{2} - \frac{(pq+1)}{2} = -1 \tag{22}$$

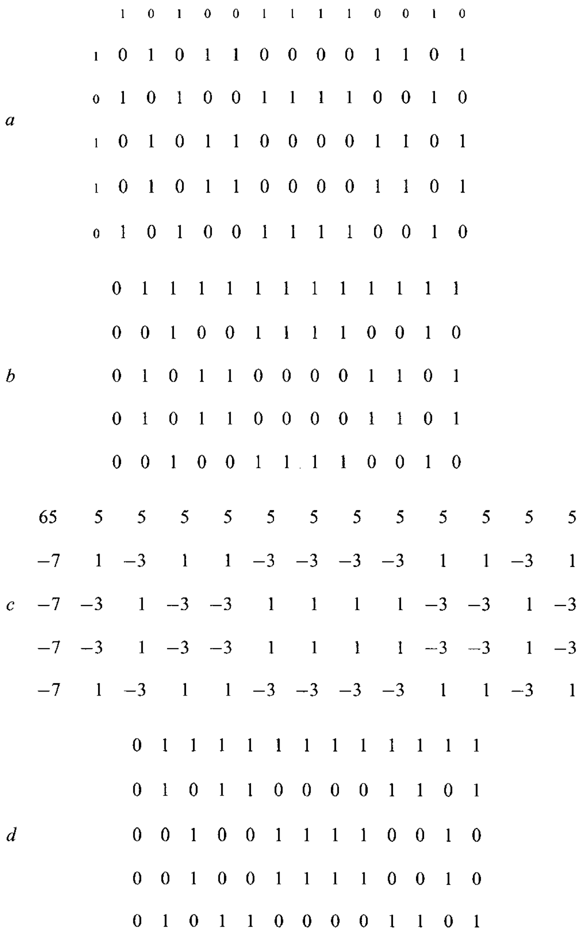
The modification described above changes $(p-1)/2$ 1s to 0s and $(q-1)/2$ 0s to 1s so the net change in the number of 1s is $(q-1)/2 - (p-1)/2 = (q-p)/2$. It follows that the imbalance changes to

$$\begin{aligned} I &= \frac{(pq-1)}{2} + \frac{(q-p)}{2} - \left\{\frac{(pq+1)}{2} - \frac{(q-p)}{2}\right\} \\ &= q - p - 1 = k - 1 \end{aligned} \tag{23}$$

for the modified Jacobi sequences.

6 Sequence and autocorrelation function construction using arrays

The discussions from Section 5 will enable any Jacobi or modified Jacobi sequence and its autocorrelation function to be constructed very easily using the array format. Table 1



```
     1  0  1  0  0  1  1  1  1  0  0  1  0
  1  0  1  0  1  1  0  0  0  0  1  1  0  1
  0  1  0  1  0  0  1  1  1  1  0  0  1  0
a 1  0  1  0  1  1  0  0  0  0  1  1  0  1
  1  0  1  0  1  1  0  0  0  0  1  1  0  1
  0  1  0  1  0  0  1  1  1  1  0  0  1  0

     0  1  1  1  1  1  1  1  1  1  1  1  1
     0  0  1  0  0  1  1  1  1  0  0  1  0
b    0  1  0  1  1  0  0  0  0  1  1  0  1
     0  1  0  1  1  0  0  0  0  1  1  0  1
     0  0  1  0  0  1  1  1  1  0  0  1  0

   65   5   5   5   5   5   5   5   5   5   5   5   5
   −7   1  −3   1   1  −3  −3  −3  −3   1   1  −3   1
c  −7  −3   1  −3  −3   1   1   1   1  −3  −3   1  −3
   −7  −3   1  −3  −3   1   1   1   1  −3  −3   1  −3
   −7   1  −3   1   1  −3  −3  −3  −3   1   1  −3   1

     0  1  1  1  1  1  1  1  1  1  1  1  1
     0  1  0  1  1  0  0  0  0  1  1  0  1
d    0  0  1  0  0  1  1  1  1  0  0  1  0
     0  0  1  0  0  1  1  1  1  0  0  1  0
     0  1  0  1  1  0  0  0  0  1  1  0  1
```

Fig. 10 *Array construction of sequences and autocorrelation function*

lists all the available modified Jacobi sequences with length $L < 5000$ and with $k \leq 20$. Table 2 lists all the Legendre sequences required for the construction of the sequences in Table 1.

As an example of this process, the case $L = 65 = 5 \times 13$ is considered, so $k = 8$ and $r(\tau) \in \{65, 5, -1, -7\}$. The Legendre sequence of length 5 is **10110** and of length 13 is **1010011110010** and these are used to label the rows and columns of a 5 × 13 array. The entries in the array are made equal to the mod-2 sum of their co-ordinates as shown in Fig. 10*a*. This produces the Jacobi sequence of length 65. This array is modified by setting all elements in the first column to 0 and all elements, except the first, in the first row to 1. This produces the array of Fig. 10*b*, which can be unfolded to produce the modified Jacobi sequence of length 65. This takes the form

0001011000111001010111111101001100
11001011111111010100111000110100

In this case, $k = 8 \equiv 0$ mod-4, and so the autocorrelation array conforms to the general structure of eqn, 19. This has the maximum value of 65 placed in the leading element of the first row and column. The remaining positions in the first row take the value $k - 3 = 5$ and the remaining values in the first column take the value $1 - k = -7$. Elements in the main body of the array take the value of 1 or -3 and these occupy the respective positions of the 0s and 1s in the sequence array. This gives the array of Fig. 10*c*. The distinct sampled version of this sequence can be derived by inverting the sequence array in all positions except on the first row or column as depicted in Fig. 10*d*. Its autocorrelation array will be similar to Fig. 10*c*, but with the 1s and -3s interchanged.

7 Aperiodic autocorrelation

Quadratic residue sequences and twin prime sequences also exhibit high merit factors when their *aperiodic* autocorrelation functions are investigated, especially when employed in a cyclically shifted form [6]. The situation is illustrated in Fig. 11*a*, which shows the variation of aperiodic merit factor with the initial cyclic shift for a class 1 Legendre sequence of length $L = 1019$. It can be observed that the maximum merit factor appears at a shift of approximately 25% of the sequence length in either direction. Class 2 Legendre sequences and the other forms of modified Jacobi sequences also retain this property. Fig. 11*b* shows the plot for a class 2 Legendre sequence of length 1013, Fig. 12*a* corresponds to a modified Jacobi sequence of length $L = 1763 = 41 \times 43$, for which $k = 2$, *i.e.* a twin prime sequence, and Fig. 12*b* results from a modified Jacobi sequence of length $L = 1517 = 37 \times 41$, for which $k = 4$. Fig. 13 shows variation of the maximum merit factor for optimally shifted Legendre sequences with length. They are observed to approach an asymptotic level of about 6. Other large classes of sequences such as *m*-sequences and GMW sequences have an asymptotic aperiodic merit factor of only 3. Fig. 14 demonstrates that modified Jacobi sequences with $k = 4$ have a similar behaviour to the Legendre sequences. The data in Table 3 confirm that this is also the case for other values of *k*.

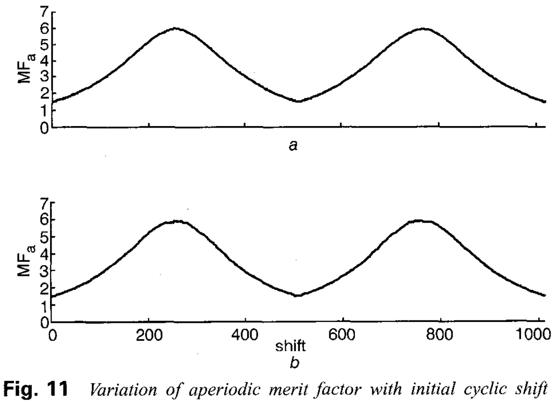


Fig. 11 *Variation of aperiodic merit factor with initial cyclic shift of sequence*

a Legendre sequence, $L = 1019$ (class 1)
b Legendre sequence, $L = 1013$ (class 2)

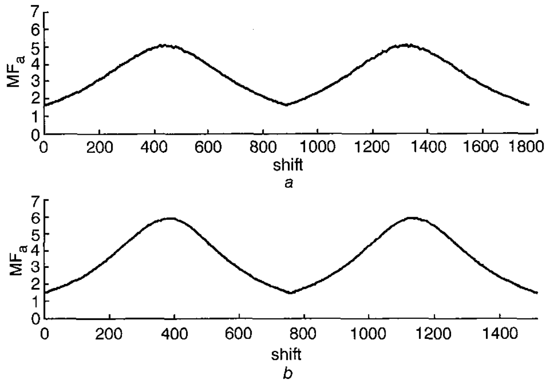


Fig. 12 *Variation of aperiodic merit factor with initial cyclic shift of sequence*

a MJ sequence, $L = 1763$, $k = 2$ (twin prime)
b MJ sequence, $L = 1517$, $k = 4$

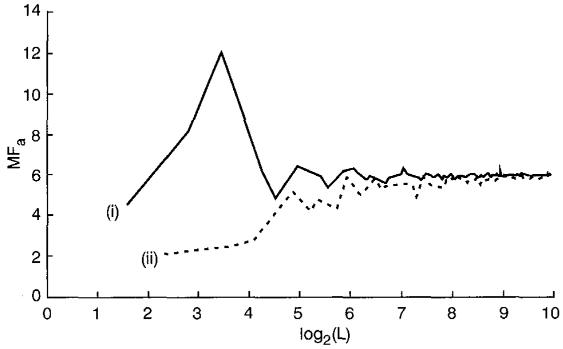


Fig. 13 *Maximum aperiodic merit factor of Legendre sequences in their optimal shift pposition*

(i) class 1
(ii) class 2

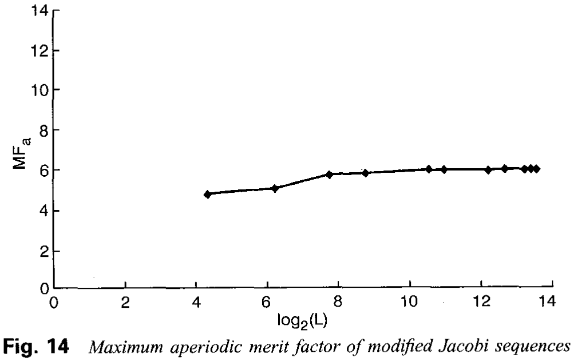


Fig. 14 *Maximum aperiodic merit factor of modified Jacobi sequences with $k = 4$, in their optimal cyclic shift position*

Table 3: Merit factors of all available modified Jacobi sequences with $L < 5000$ and $k \leq 20$

k	L	MF_p	MF_a	τ	k	L	MF_p	MF_a	τ
2	15	16.07	4.17	1	12	85	3.44	3.34	18
	35	36.03	4.75	24		133	6.49	4.17	38
	143	144.01	4.01	108		253	15.64	4.90	58
	323	324.00	4.65	89		493	37.72	5.58	118
	899	900.00	4.87	225		589	47.47	5.62	152
	1763	1764.00	5.13	441		1189	115.61	5.97	302
	3599	3600.00	5.32	2695		1333	133.28	5.88	334
4	21	5.25	4.79	5		2173	242.75	5.85	544
	77	16.29	5.09	17		2773	325.77	5.92	702
	221	45.06	5.72	58		4189	531.94	5.95	1054
	437	88.25	5.83	112		4453	571.58	5.95	1122
	1517	304.24	5.97	381	14	51	1.13	1.50	18
	2021	405.04	5.99	508		95	3.08	2.46	29
	4757	952.24	5.97	1199		527	40.76	4.42	136
6	55	13.15	3.99	14		851	81.68	4.64	639
	91	25.09	3.64	13		1247	141.49	4.93	314
	187	63.12	4.44	136		2867	461.94	5.25	2151
	247	89.98	4.09	62		3551	624.05	5.32	888
	391	160.93	4.40	96		4307	817.55	5.36	1082
	667	313.74	4.82	507	16	57	0.88	1.27	12
	1147	610.77	4.89	859		161	4.53	3.54	39
	1591	907.27	5.09	1185		377	15.60	4.88	88
	1927	1141.16	5.17	484		1457	99.09	5.80	367
	2491	1547.40	5.21	629		1961	146.51	5.85	479
	3127	2021.11	5.28	773		2537	204.77	5.90	645
	4087	2759.10	5.37	3059	18	115	2.14	2.02	34
	4891	3393.17	5.40	1215		319	10.75	3.75	238
8	33	2.43	2.62	9		403	15.35	3.81	103
	65	5.74	4.00	18		703	35.43	4.38	178
	209	23.74	5.23	48		943	54.76	4.72	245
	713	99.14	5.78	181		1363	94.16	4.91	346
	1073	157.46	5.89	271		2419	217.29	5.17	596
	3233	531.98	5.96	790		2623	244.34	5.16	672
	3953	661.23	5.97	1008		3763	411.42	5.31	954
10	39	1.97	2.35	15		4819	586.88	5.37	1244
	119	10.37	3.66	26	20	69	0.65	0.95	16
	299	38.63	4.07	75		341	8.44	4.32	85
	551	91.06	4.64	418		629	20.76	5.16	160
	1271	288.99	5.00	313		989	39.60	5.48	253
	1739	443.03	5.06	453		2501	142.87	5.89	636
	2279	638.53	5.17	1701		3149	194.97	5.90	799
	4331	1501.81	5.36	1091		3869	256.76	5.93	969
						4661	328.67	5.94	1179

8 Conclusions

Quadratic residue sequences and twin prime sequences are well known types of binary sequences with ideal periodic autocorrelation. In this paper, the authors have indicated that these sequences correspond to special cases of the much larger classes of Legendre sequences and modified Jacobi sequences, respectively. Legendre sequences exist for all lengths $L=p$, a prime, and Jacobi and modified Jacobi sequences exist for all lengths $L=pq$, with p and q both prime. It has been demonstrated that both classes of Legendre sequences and modified Jacobi sequences exhibit out-of-phase periodic autocorrelation values which are independent of the sequence length. Consequently, the 'peak-to-sidelobe' ratio and the periodic merit factor improve for the longer versions of these sequences.

When a Legendre sequence of length L is sampled with a sampling value s which is equivalent to a QR mod-L the sequence of samples is identical to the original sequence and always has the same phase, *i.e.* it is self-similar. When s is equivalent to a non QR, a distinct sequence is produced which is equivalent to the original sequence with all its digits except a_0 inverted. Similarly, proper decimation of a modified Jacobi sequence either reproduces the original sequence in identical phase or gives a distinct sequence which is the reverse (except for b_0) of the original. Sequences of samples have the same correlation values as the original.

Quadratic residue sequences also possess high linear complexity [7, 8] and therefore have cryptographic significance. They have also been employed in the acoustic design of concert halls [9] and twin prime sequences have been used in their two-dimensional array versions as partially opaque filters for X-ray image processing [10–12]. It is anticipated that these properties and applications are shared by the general forms of Legendre and modified Jacobi sequences, due to their common forms of origin.

It has been shown that the array representations are simple to generate and provide a convenient and compact two-dimensional format for constructing these sequences and deriving their autocorrelation functions, and also highlight their inner structure.

Design data have been included to enable any Jacobi or modified Jacobi sequence with length $L < 5000$ and with $k \leq 20$ to be constructed and its autocorrelation function to be derived using the procedures described in this paper.

9 References

1 EVERETT, D.: 'Periodic digital sequences with pseudorandom properties', *GEC J.*, 1966, **33**, pp. 115–126

2 FAN, P., and DARNELL, M.: 'Sequence design for communications applications' (John Wiley, Research Studies Press, Taunton, 1996)

3 GOLAY, M.J.E.: 'Sieves for low autocorrelation of binary sequences', *IEEE Trans. Inf. Theory*, 1977, **IT-23**, (1), pp. 43–51

4 GREEN, D.H.: 'Structural properties of pseudorandom arrays and volumes and their related sequences', *IEE Proc. E, Comput Digit. Tech*, 1985, **132**, (3), pp. 133–145

5 CALABRO, D., and WOLF, J.K.: 'On the synthesis of two-dimensional arrays with desirable correlation properties', *Inf. Control*, 1968, **11**, pp. 537–560

6 JENSEN, J.M., JENSEN, H.E., and HØHOLDT, T.: 'The merit factor of binary sequences related to difference sets', *IEEE Trans. Inf. Theory*, 1991, **IT-37**, (3), pp. 617–626

7 NO, J.-S., LEE, H.-K., CHUNG, H., SONG, H.-Y., and YANG, K.: 'Trace representation of Legendre sequences of Mersenne prime period', *IEEE Trans. Inf. Theory*, 1996, **IT-42**, (6), pp. 2254–2255

8 DING, C., HELLESETH, T., and SHAN, W.: 'On the linear complexity of Legendre sequences', *IEEE Trans. Inf. Theory*, 1998, **IT-44**, (3), pp. 1276–1282

9 SCHROEDER, M.R.: 'Toward better acoustics for concert halls', *Phys. Today*, 1980, **33**, (10), pp. 24–30

10 FENIMORE, E.E., and CANNON, T.M.: 'Coded aperture imaging with uniformly redundant arrays', *Appl. Opt.*, 1978, **17**, (3), pp. 337–347

11 TRUSSELL, H.J.: 'Processing of X-ray images', *Proc. IEEE*, 1981, **69**, (5), pp. 615–627

12 SCHROEDER, M.R.: 'Number theory in science and communication (Springer Series in Information Sciences, Berlin, 1997, 3rd edn.)