A Modified Jacobi Sequence Construction Using Multi-Rate Legendre Sequences

Matthew.G.Parker [1]

Inst. for Informatikk, University of Bergen,

5020 Bergen, Norway,

matthew@ii.uib.no

http://www.ii.uib.no/ matthew/MattWeb.html

Abstract

We propose a construction for length $n = pq$ Modified Jacobi sequences using multi-rate length p and length q Legendre sequences, thereby reducing the LFSR complexity of Modified Jacobi sequence generation from $O(pq)$ to $O(p+q)$.

1 Introduction

This paper investigates the generation of a binary Modified Jacobi sequence by means of an additive combination of constituent binary Legendre sequences which are clocked at different rates. These multi-rate combinations demonstrate that sequences of large linear complexity can be generated without resorting to linear feedback shift registers (LFSRs) of large length. Results on the linear complexity of Legendre sequences [3, 5] show that we can generate Legendre sequences of length p using length $O(p)$ LFSRs. Moreover, [2, 7] showed that length pq Modified Jacobi sequences have linear complexity $\simeq pq$ or $\simeq \frac{pq}{2}$. A direct LFSR generation of a Modified Jacobi sequence would therefore require a length pq or $\frac{pq}{2}$ LFSR. Alternatively, in this paper we show that an equivalent multi-rate construction can generate the same sequences, but using a multi-rate parallel combination of Legendre sequences of lengths p and q, thereby only requiring length $O(p)+O(q)$ LFSRs. For reasons of space we omit some proofs.

[1] This work was funded by NFR Project Number 119390/431

2 A Conventional Modified Jacobi Sequence Construction

We define a Modified Jacobi sequence $\{s(t)\}$ of period pq for $t = 0, 1, 2, \ldots, pq-1$, where $p < q$ are distinct odd primes,

$$s(t) = \begin{cases} 0 \text{ if } t \equiv 0(\bmod pq) \\ 0 \text{ if } \left(\frac{t}{p}\right) \cdot \left(\frac{t}{q}\right) = 1 \\ 1 \text{ if } \left(\frac{t}{p}\right) \cdot \left(\frac{t}{q}\right) = -1 \\ 0 \text{ if } t \not\equiv 0(\bmod p) \text{ and } t \equiv 0(\bmod q) \\ 1 \text{ if } t \equiv 0(\bmod p) \text{ and } t \not\equiv 0(\bmod q) \end{cases} \tag{1}$$

where $\left(\frac{t}{p}\right)$ is the Legendre symbol.

We also present here a symmetry of the Modified Jacobi sequence:

Lemma 1 *For p, q prime, define a length pq sequence $f(t)$ such that $f(t) = 0$ for t satisfying $\gcd(t, pq) = 1$, and $f(t) = 1$ otherwise. Then, if $s(t)$ is a length pq Modified Jacobi sequence, then $s(t) + f(t)$ is also a length pq Modified Jacobi sequence, possessing the same periodic and aperiodic correlation properties to within sign change.*

3 A Multi-Rate Example

Before presenting the multi-rate construction, let us set the scene with a small example. Let $p = 3$ and $q = 5$. The length three Legendre sequence is 101. The length five Legendre sequence is 10110. The length 15 'product' binary sequence obtained by summing, mod 2, five repetitions of the length 3 sequence with 3 repetitions of the length 5 sequence as follows,

```
101101101101101 +
101101011010110
---------------
000000110111011
```

5 is a Quadratic Non-Residue, mod 3, so we now add the complement of the length 3 Legendre sequence onto the above 'product' sequence at every 5th position. Thus,

```
000000110111011 +
0    1    0
---------------
000001110111011
```

We also add the length 5 Legendre sequence onto the above sequence at every 3rd position. Thus,

```
000001110111011 +
1  0  1  1  0
---------------
100001010011011
```

This is equivalent to (1) under Lemma 1. In fact, this special example of a Modified Jacobi sequence is simultaneously also a Twin-Prime sequence and an m-sequence.

4 A Trace Representation For Legendre Sequences

Definition 1 *Let* $\mathbf{QR_p}$ *be the set of Quadratic Residues, mod p, i.e. those elements of* Z_p^* *which have square-roots in* Z_p^*.
Let $\mathbf{QNR_p}$ *be the set of Quadratic NonResidues, mod p, i.e. those elements of* Z_p^* *which do not have square-roots in* Z_p^*.

We define the Legendre sequence as follows:

Definition 2 *Let* $r_p(t)$ *be the binary Legendre sequence of length p, p prime, such that*

$$r_p(t) = \begin{cases} 1 \text{ if } t \equiv 0(\ mod\ p) \\ 0 \text{ if } t \in \mathbf{QR_p} \\ 1 \text{ if } t \in \mathbf{QNR_p} \\ \overline{r_p(t)} = 0 \text{ if } t \text{ non-integer} \end{cases}$$

Definition 3 *The Witness Set* $\mathbf{WS}(x, n)$ *is the set of all factors of* $x^n - 1$ *which do not occur as factors of* $x^t - 1$, $t|n$, $t \neq n$.

We now present a trace representation for all Legendre sequences. This is similar to that given in [5]. However, [5] achieves a trace right down to the base field, GF(2), whereas the representation presented here only traces down to GF(2^a), (a is defined below). A proof for Theorem 1 can be found in [8].

Theorem 1 *[8] The Legendre sequence, $r_p(t)$, of prime period, p, has a minimal trace representation defined by,*

$$r_p(0) = 1, r_p(t) = \sum_{i=0}^{\frac{p-1}{2v}-1} Tr_{2^a}^n(\alpha^{u^{2i}t} + \alpha^{u^{2i}k}), \qquad k \in \mathbf{QR}, t > 0$$

where α is a p^{th}root of 1, $p \in \mathbf{WS}(2, n)$, $\alpha \in$ GF(2^n), $n = 2^a v$, v odd, and u is a primitive element of Z_p. Without loss of generality k can be chosen as 1.

It is evident that, when $a = 0$, $p = 2^n - 1$ prime, and the Legendre sequence is of Mersenne prime length [6]. The combined results of [3, 5, 8] all give a linear complexity for a Legendre sequence of length p to be $O(p)$.

The following section formally describes the Multi-Rate Modified Jacobi construction.

5 A Multi-Rate Modified Jacobi Sequence Construction

Definition 4 *Define $C_x(r(t)) = r(t)$ if $x = 0$ and $\overline{r(t)}$ if $x = 1$, where $\overline{*}$ means 'complement' each element of $*$.*

We now define a Modified Jacobi sequence $\{s(t)\}$ of period pq for $t = 0, 1, 2, \ldots, pq - 1$, where $p < q$ are distinct odd primes, as follows.

Theorem 2 *If p or q is of the form $4k + 1$, k a positive integer,*

$$s(t) = r_p(t) + r_q(t) + C_{q \in \mathbf{QNR_p}}(r_p(\frac{t}{q})) + C_{q \in \mathbf{QR_p}}(r_q(\frac{t}{p}))$$

Alternatively, if p and q are both of the form $4k + 3$, k a positive integer,

$$s(t) = r_p(t) + r_q(t) + C_{q \in \mathbf{QR_p}}(r_p(\frac{t}{q})) + C_{q \in \mathbf{QR_p}}(r_q(\frac{t}{p}))$$

The Twin-Prime sequence is a special case of Theorem 2 where $q = p+2$. In this case, either p or q is of the form $4k + 1$, so the first of the two expressions in Theorem 2 is used.

6 Proof of Theorem 2

Our aim is to prove that Theorem 2 gives a sequence construction identical, up to symmetry, to the conventional Modified Jacobi construction of (1). For our proof we need the following well-known Theorem and Lemma.

Theorem 3 *[1] The Law of Quadratic Reciprocity states: If p and q are distinct primes, then,*

$$p \in \mathbf{QR_q} \Rightarrow q \in \mathbf{QR_p}, \qquad p \in \mathbf{QNR_q} \Rightarrow q \in \mathbf{QNR_p}$$

iff p and/or q are of the form $4k + 1$, k a positive integer

Similarly,

$$p \in \mathbf{QR_q} \Rightarrow q \in \mathbf{QNR_p}, \qquad p \in \mathbf{QNR_q} \Rightarrow q \in \mathbf{QR_p}$$

iff neither p or q are of the form $4k + 1$, k a positive integer

Lemma 2 *Let $x_0, x_1 \in \mathbf{QR_p}$, $y_0, y_1 \in \mathbf{QNR_p}$. Then $x_0y_0 \in \mathbf{QNR_p}$, $x_0x_1, y_0y_1 \in \mathbf{QR_p}$.*

We prove only the first of the two constructions in Theorem 2, that is where p or q are of the form $4k+1$. The second construction follows a similar proof. Likewise we only prove for the case $q \in \mathbf{QNR_p}$, the case $q \in \mathbf{QR_p}$ being similarly proved.

It is easy to see that Theorem 2 is equivalent to (1) for positions t where $\gcd(t, pq) = 1$.

For the other positions we have two different possibilities, depending on whether $q \in \mathbf{QNR_p}$ or $q \in \mathbf{QR_p}$. For $q \in \mathbf{QNR_p}$ we have the following:

Consider the non-zero positions $t = kq$, k integer, of $s(t)$. At such positions Theorem 2 states that,

$$s(kq) = r_p(kq) + r_q(kq) + \overline{r_p(k)} + r_q(\frac{kq}{p}) \tag{2}$$

From Definition 2 $r_q(\frac{kq}{p}) = 0$ and $r_q(kq) = 1$. Substituting into (2),

$$s(kq) = r_p(kq) + \overline{r_p(k)} + 1$$

Using Lemma 2 and the fact that $q \in \mathbf{QNR_p}$ gives $r_p(kq) = \overline{r_p(k)}\ \forall k$. In this case $s(kq) = 1$.

Now consider non-zero positions $t = jp$, j integer, of $s(t)$. At such positions Theorem 2 states that,

$$s(jp) = r_p(jp) + r_q(jp) + \overline{r_p(\frac{jp}{q})} + r_q(j) \tag{3}$$

From Definition 2 $\overline{r_p(\frac{jp}{q})} = 0$ and $r_p(jp) = 1$. Substituting into (3),

$$s(jp) = r_q(jp) + r_q(j) + 1$$

Using Lemma 2, $q \in \mathbf{QNR_p}$, and applying Theorem 3, then $p \in \mathbf{QNR_q}$ and $r_q(jp) = \overline{r_q(j)}\ \forall k$. In this case $s(jp) = 0$.

Now consider position $t = 0$. In this case Theorem 2 simplifies to,

$$s(0) = 1$$

So, in summary, for the case where either p or q is of the from $4k + 1$, and where $q \in \mathbf{QNR_p}$ we have,

$$s(t) = \begin{cases} 1 \text{ if } t \equiv 0(\bmod pq) \\ 0 \text{ if } \left(\frac{t}{p}\right) \cdot \left(\frac{t}{q}\right) = 1 \\ 1 \text{ if } \left(\frac{t}{p}\right) \cdot \left(\frac{t}{q}\right) = -1 \\ 1 \text{ if } t \not\equiv 0(\bmod p) \text{ and } t \equiv 0(\bmod q) \\ 0 \text{ if } t \equiv 0(\bmod p) \text{ and } t \not\equiv 0(\bmod q) \end{cases}$$

This is equivalent to (1) under Lemma 1. The other case where $q \in \mathbf{QR_p}$ is similarly proved, as are the cases where neither p or q are of the form $4k+1$.

∎

7 Final Note

Upon completion of this paper, the author became aware of a recent publication [4] which also proposes the same Modified Jacobi construction using multi-rate Legendre sequences. Hence this paper remains unpublished!

References

[1] L.Childs, "Quadratic Residues", **A Concrete Introduction to Higher Algebra**, Springer-Verlag, pp 293-298, 1988

[2] C.Ding, "Linear Complexity of Some Generalized Cyclotomic Sequences", *International Journal of Algebra and Computation*, Vol 44, No 4, pp 1693-1698, 1998

[3] C.Ding,T.Helleseth,W.Shan, "On the Linear Complexity of Legendre Sequences", *IEEE Trans. Inf. Theory*, Vol 44, No 3, pp 1276-1278, May 1998

[4] D.H.Green,P.R.Green, "Modified Jacobi Sequences", *IEE Proc. Comp. and Dig. Tech.*, Vol 147, No 4,pp 241-251, July 2000

[5] J-H.Kim,M.Shin,H-Y.Song, "Trace Representation of Legendre Sequences", Preprint, Nov 3, 1999

[6] J-S.No,H-K.Lee,H.Chung,H-Y.Song,K.Yang, "Trace Representation of Legendre Sequences of Mersenne Prime Period", *IEEE Trans. Inf. Theory*, Vol 42, No 6, pp 2254-2255, Nov 1996

[7] J-H.Kim,M.Shin,H-Y.Song, "On the Linear Complexity of Binary Jacobi Sequences of Period pq", Preprint, Nov 3, 1999

[8] M.G.Parker, "Legendre and Twin-Prime Sequences: Trace and Multi-Rate Representations", (unpublished), available at http://www.ii.uib.no/ matthew/MattWeb.html, 1999