LegTraceRep.tex, 25.8.99, M.G.Parker

Legendre and Twin Prime Sequences: Trace and Multi-Rate Representations

M.G.Parker,

University of Bergen, Department of Informatics, University of Bergen,

N-5020 Bergen, Norway, `matthew@ii.uib.no`

Abstract

Trace representations are presented for all binary Legendre sequences and Twin-Prime sequences, and an alternative multi-rate construction is given for the Twin-Prime sequence.

1 Introduction

Binary sequences with good periodic autocorrelation function (ACF) properties are of theoretical and practical interest, and have application to spread-spectrum communications systems [3]. It is often convenient to find trace representations for these sequences [1], and trace representations have been found for various length $2^n - 1$ sequence families with ideal two-level ACF properties, such as for m-sequences, GMW sequences, Legendre sequences, and Twin-Prime sequences [3]. Results emphasise those sequences of period $2^n - 1$ as these sequences are of maximal length for a given linear feedback shift-register size and are therefore usually preferred for hardware implementations. However, Legendre and Twin-Prime sequences with two-level or three-level ACF also occur for lengths other than $2^n - 1$ and it is of interest to know the trace representations of these sequences aswell. This paper presents such representations, using the trace of non-primitive elements, and can be seen as an extension of the results of [2]. To begin with, the trace representation of all Legendre sequences is derived. This result naturally leads to a trace representation of the Twin-Prime sequence. A final section shows how to alternatively represent the Twin-Prime sequence as a combination of two lower rate Legendre sequences, thereby eliminating conditional construction.

2 A Trace Representation for All 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^**.*

Definition 2 *The Legendre sequence,* $s_p(t)$*, of period* p*,* p *prime, is defined as follows,*

$$s_p(0) = 1, \qquad s_p(t) = 1, \qquad t \in \mathbf{QNR_p}, \qquad s_p(t) = 0, \qquad t \in \mathbf{QR_p}$$

The bipolar form of $s_p(t)$ has an ideal two-valued ACF when it is of prime length $4k + 3$, and a three-valued ACF when it is of prime length $4k + 1$. Moreover, for the three-valued case, the ACF is closely related to the Legendre sequence itself.

Definition 3 *The Trace Function,* $a' = Tr_j^n(a)$*, maps* a *to* a'*, where* $a \in F_{2^n}$*,* $a' \in F_{2^j}$*, and is defined as follows*

$$Tr_j^n(a) = \sum_{i=0}^{n-1} a^{2^i}$$

The following theorem was derived in [2].

Theorem 1 *[2] Let $p = 2^n - 1$ be a prime for some integer $n \geq 3$ and u be a primitive element of Z_p, the set of integers mod p. Let α be a primitive element of F_{2^n} such that,*

$$\sum_{i=0}^{\frac{p-1}{2n}-1} Tr_1^n(\alpha^{u^{2i}}) = 0$$

Then the Legendre Sequence, $s_p(t)$, of period p is given by,

$$s_p(t) = \sum_{i=0}^{\frac{p-1}{2n}-1} Tr_1^n(\alpha^{u^{2i}t})$$

Theorem 1 is restricted to prime periods of length $2^n - 1$. In this section we extend the theorem to all prime periods. The arguments are identical to those given in [2] when the trace is defined over an odd extension of GF(2), but when the trace is defined over an even extension of GF(2) one must generalise the representation to a trace function which maps to an extended field, not the base field. Before we state this generalised theorem we define the Witness Set.

Definition 4 *The Witness Set $\mathbf{WS}(q, n)$ is the set of all factors of $q^n - 1$ which do not occur as factors of $q^t - 1$, $t|n$, $t \neq n$.*

The main theorem of this paper is as follows.

Theorem 2 *The Legendre sequence, $s_p(t)$, of prime period, p, has a minimal trace representation defined by,*

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

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 Theorem 1 is a special case of Theorem 2 when $a = 0$, $p = 2^n - 1$ prime, and α is chosen appropriately.

2.1 Proof of Theorem 2

We first present a series of self-evident lemmas.

Lemma 1 *For p prime, $\mathbf{QR_p} + \mathbf{QNR_p} = Z_p^*$*

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

Let p be an odd prime $\in \mathbf{WS}(2,n)$. Then 2 has order n mod p. Let $n = 2^a v$, where v is odd. Let $A = 2^{a+1}$. Then A has order v, mod p. Let u be a primitive element, mod p, of order $p-1$.

Lemma 3 *There is a unique representation for every element of Z_p^* as,*

$$Z_p^* = \{u^j A^k \quad | \quad 0 \le j < \frac{p-1}{v}, 0 \le k < v\}$$

u has even order so the following Lemma is self-evident.

Lemma 4 *The even powers of u, mod p, form the set $\mathbf{QR_p}$. The odd powers of u, mod p, form the set $\mathbf{QNR_p}$.*

A has odd order so we have the following.

Lemma 5 *All powers of A, mod p, are in the set $\mathbf{QR_p}$, mod p.*

It follows from Lemmas 1-5 that,

$$\begin{aligned} \mathbf{QR_p} &= \{u^{2i}A^k | 0 \leq i < \tfrac{p-1}{2v}, 0 \leq k < v\} \\ \mathbf{QNR_p} &= \{u^{2i+1}A^k | 0 \leq i < \tfrac{p-1}{2v}, 0 \leq k < v\} \end{aligned} \tag{1}$$

and therefore that,

$$\begin{aligned} \mathbf{QNR_p} &= \{u^{2i}A^k t | 0 \leq i < \tfrac{p-1}{2v}, 0 \leq k < v, t \in \mathbf{QNR_p}\} \\ \mathbf{QR_p} &= \{u^{2i}A^k t | 0 \leq i < \tfrac{p-1}{2v}, 0 \leq k < v, t \in \mathbf{QR_p}\} \end{aligned} \tag{2}$$

Let $p \in \mathbf{WS}(2,n)$. Then from Definition 4 there is an element α of order p in $\mathrm{GF}(2^n)$. Let $f_{QR_p} = \sum_{r \in \mathbf{QR_p}} \alpha^r$ and $f_{QNR_p} = \sum_{r \in \mathbf{QNR_p}} \alpha^r$. It immediately follows from Lemma 1 that,

$$f_{QR_p} + f_{QNR_p} = \sum_{r=1}^{p-1} \alpha^r = 1 \tag{3}$$

Moreover, from (2),

$$\begin{aligned} f_{QR_p} &= \textstyle\sum_{i=0}^{\frac{p-1}{2v}-1} \sum_{k=0}^{v-1} \alpha^{u^{2i}A^k t}, \qquad t \in \mathbf{QR_p} \\ f_{QNR_p} &= \textstyle\sum_{i=0}^{\frac{p-1}{2v}-1} \sum_{k=0}^{v-1} \alpha^{u^{2i}A^k t}, \qquad t \in \mathbf{QNR_p} \end{aligned} \tag{4}$$

Rewriting in terms of the Trace representation gives,

$$\begin{aligned} f_{QR_p} &= \textstyle\sum_{i=0}^{\frac{p-1}{2v}-1} \ \mathrm{Tr}_{2^a}^n(\alpha^{u^{2i}t}), \qquad t \in \mathbf{QR_p} \\ f_{QNR_p} &= \textstyle\sum_{i=0}^{\frac{p-1}{2v}-1} \ \mathrm{Tr}_{2^a}^n(\alpha^{u^{2i}t}), \qquad t \in \mathbf{QNR_p} \end{aligned} \tag{5}$$

f_{QR_p} and f_{QNR_p} will be elements of $\mathrm{GF}(2^{2^a})$. Define the sequence $s'(t)$ of period p by,

$$s'(t) = \sum_{i=0}^{\frac{p-1}{2v}-1} \ \mathrm{Tr}_{2^a}^n(\alpha^{u^{2i}t})$$

Then $s'(t)$ takes on the values f_{QR_p} and f_{QNR_p} for t in $\mathbf{QR_p}$ and $\mathbf{QNR_p}$ respectively. Define the sequence $s(t)$ by,

$$s(t) = s'(t) + f_{QR_p} \tag{6}$$

Then $s(t)$ takes on the values 0 and $f_{QR_p} + f_{QNR_p} = 1$ for t in $\mathbf{QR_p}$ and $\mathbf{QNR_p}$ respectively. By definition this is the last $p-1$ elements of the Legendre sequence of period p. Setting $s(0) = 1$ and expanding (6) for $t > 0$ leads to Theorem 2. ∎

For $p = 4k+3$ (6) defines a sequence with two-valued periodic ACF. However, this two-valued property holds for $s(0)$ equal to any value when $p = 4k+3$. Theorem 2 fixes $s(0) = 1$ to maintain the binary nature of the sequences. But the above discussion implies that $s(t)$, $s(t)+\delta$, $\overline{s(t)}$, and $\overline{s(t)}+\delta$, all have identical ideal two-valued ACF, where $\delta = (1, 0, 0, \ldots, 0, 0)$. Moreover, for $p = 4k+1$, the sequences $s(t)$, $s(t)+\delta$, $\overline{s(t)}$, and $\overline{s(t)}+\delta$, all have identical three-valued ACF to within a sign change of the ACF. It therefore seems reasonable to refer to all four sequences as the Legendre sequence (this equivalence can alternatively be established by considering sequence decimation). However for the construction of a Twin-Prime sequence, $w(t)$ using two Legendre sequences, the two-valued ACF property is only maintained if $s(t)$ or $\overline{s(t)}+\delta$ are used. Of course, the two-valued property is then further maintained for $\overline{w(t)}$.

3 A Trace Representation for the Twin-Prime Sequences

The twin-prime sequence is constructed from the modified mod 2 sum of two Legendre sequences, and is defined as follows.

Definition 5 *The period pp' Twin-Prime sequence, $w(t)$, where p and $p' = p+2$ are prime is defined by,*

$$w(t) =$$

$$s_p(t) + s_{p'}(t), \qquad \gcd(t, pp') = 1$$

$$\begin{cases} 1, & t \in \{0, p', 2p', \ldots, (p-1)p'\} \\ 0, & t \in \{p, 2p, \ldots, (p'-1)p\} \end{cases} \quad or \quad \begin{cases} 0, & t \in \{0, p', 2p', \ldots, (p-1)p'\} \\ 1, & t \in \{p, 2p, \ldots, (p'-1)p\} \end{cases}$$

Theorem 2 naturally leads to a trace expression for Definition 5, as shown in the following Corollary.

Corollary 1 *The period pp' Twin-Prime sequence, $w(t)$, where p and $p' = p+2$ are prime, has a minimal trace representation defined as in Definition 5 where*

$$s_p(t) = \sum_{i=0}^{\frac{p-1}{2v_p}-1} Tr_{2^{a_p}}^{n_p}(\alpha_p^{u_p^{2i}t} + \alpha_p^{u_p^{2i}k_p})$$

$$s_{p'}(t) = \sum_{i=0}^{\frac{p'-1}{2v_{p'}}-1} Tr_{2^{a_{p'}}}^{n_{p'}}(\alpha_{p'}^{u_{p'}^{2i}t} + \alpha_{p'}^{u_{p'}^{2i}k_{p'}})$$

where $k_p \in \mathbf{QR_p}$, $k_{p'} \in \mathbf{QR_{p'}}$, and where $\alpha_p, \alpha_{p'}$ are p and p'^{th} roots of 1, respectively, $p \in \mathbf{WS}(2, n_p)$, $p' \in \mathbf{WS}(2, n_{p'})$, $\alpha_p \in GF(2^{n_p})$, $\alpha_{p'} \in$

$GF(2^{n_{p'}})$, $n_p = 2^{a_p} v_p$, $n_{p'} = 2^{a_{p'}} v_{p'}$, $v_p, v_{p'}$ odd, and $u_p, u_{p'}$ are primitive roots, mod p and mod p', respectively. Without loss of generality k_p and $k_{p'}$ can be chosen as 1.

4 A Multi-Rate Representation for the Twin-Prime Sequence

One can trivially re-specify Corollary 1 to use traces from the extension field $\mathrm{GF}(2^n)$, where $n = \mathrm{lcm}(n_p, n_{p'})$, and where β is a pp'^{th}root of 1 in $\mathrm{GF}(2^n)$, $\alpha_p = \beta^{p'}$, and $\alpha_{p'} = \beta^p$. But perhaps a more useful form uses a combination of 'multi-rate' Legendre sequences, as follows. Firstly we extend Definition 2.

Definition 6 *The Legendre sequence, $s_p(t)$, is as defined in Definition 2 but with the added conditions,*

$$s_p(t) = \overline{s_p(t)} = 0, \ t \text{ non-integer}$$

Then,

Theorem 3 *$w(t)$ is a length pp' twin-prime sequence, given by,*

$$w(t) = s_p(t) + s_{p'}(t) + \overline{s_p(\frac{t}{p'})} + s_{p'}(\frac{t}{p}) + h\delta(t), \qquad h \in \{0, 1\}$$

where $h = 0$ if $2 \in \mathbf{QNR_p}$, $h = 1$ if $2 \in \mathbf{QR_p}$, and $\delta(t) = 1$ for $t = 0$, 0 otherwise.

$$w(t) = s_p(t) + s_{p'}(t) + s_p(\frac{t}{p'}) + \overline{s_{p'}(\frac{t}{p})} + \overline{h}\delta(t), \qquad h \in \{0, 1\}$$

is also a length pp' twin-prime sequence.

4.1 Proof of Theorem 3

We prove only the first of the two constructions in Theorem 3. The second construction follows a similar proof. It is easy to see that Theorem 3 is satisfied for positions t where $\gcd(t, pp') = 1$. Now consider non-zero positions $t = kp'$, k integer, of $w(t)$. At such positions Theorem 3 states that,

$$w(kp') = s_p(kp') + s_{p'}(kp') + \overline{s_p(k)} + s_{p'}(\frac{kp'}{p}) \tag{7}$$

From Definitions 2 and 6 $s_{p'}(\frac{kp'}{p}) = 0$ and $s_{p'}(kp') = 1$. Substituting into (7) implies that Theorem 3 is correct iff,

$$w(kp') = s_p(kp') + \overline{s_p(k)} + 1$$

From Lemma 2 if $p' \in \mathbf{QR_p}$ then $s_p(kp') = s_p(k)\ \forall k$. In this case $w(kp') = 0$. Conversely, if $p' \in \mathbf{QNR_p}$ then $s_p(kp') = \overline{s_p(k)}\ \forall k$. In this case $w(kp') = 1$.

Now consider non-zero positions $t = jp$, j integer, of $w(t)$. At such positions Theorem 3 states that,

$$w(jp) = s_p(jp) + s_{p'}(jp) + \overline{s_p(\frac{jp}{p'})} + s_{p'}(j) \tag{8}$$

From Definition 6 $\overline{s_p(\frac{jp}{p'})} = 0$ and $s_p(jp) = 1$. Substituting into (8) implies that Theorem 3 is correct iff,

$$w(jp) = s_{p'}(jp) + s_{p'}(j) + 1$$

If $p \in \mathbf{QR_{p'}}$ then $s_{p'}(jp) = s_{p'}(j)\ \forall k$. In this case $w(jp) = 1$. Conversely, if $p \in \mathbf{QNR_{p'}}$ then $s_{p'}(jp) = \overline{s_{p'}(j)}\ \forall k$. In this case $w(jp) = 0$.

Now consider position $t = 0$. In this case Theorem 3 simplifies to,

$$w(0) = h + 1$$

From the definition of the Twin-Prime sequence, as described in Definition 5, if $w(kp') = 1$ then $w(jp) = 0$ and $w(0) = 1$. From the above considerations this is only possible when

$$p' \in \mathbf{QNR_p}, \qquad p \in \mathbf{QNR_{p'}}, \qquad h = 0$$

Similarly, from Definition 5, if $w(kp') = 0$ then $w(jp) = 1$ and $w(0) = 0$. From the above considerations this is only possible when

$$p' \in \mathbf{QR_p}, \qquad p \in \mathbf{QR_{p'}}, \qquad h = 1$$

Theorem 3 follows by observing that $p' \bmod p = 2$. ∎

(As a side observation, we note from the above proof that when $p \in \mathbf{QNR_{p'}}$, then $p' \in \mathbf{QNR_p}$. Similarly, when $p \in \mathbf{QR_{p'}}$, then $p' \in \mathbf{QR_p}$.)

The following Lemma shows the symmetry operation which maps between the two constructions of Theorem 3.

Lemma 6 *For p, p' prime, define a length pp' sequence $r(t)$ such that $r(t) = 0$ for t satisfying $\gcd(t, pp') = 1$, and $r(t) = 1$ otherwise. Then, if $w(t)$ is a length pp' Twin-Prime sequence, then $w(t) + r(t)$ is also a length pp' Twin-Prime sequence.*

5 Conclusion

This paper has derived a Trace representation for all Legendre sequences, thereby generalising the result of [2]. This representation naturally leads to a Trace representation for the Twin-Prime sequence. Finally a multi-rate construction for the Twin-Prime sequence has been presented. This construction eliminates the need for 'mid-sequence' conditional instructions and may lead to simpler hardware using a combination of multi-rate linear feedback shift registers. The multi-rate idea also suggests that other sequences with optimal ACF properties may be constructed similarly, and this should be an area for further research.

References

[1] T.Helleseth,P.V.Kumar, "Sequences with Low Correlation", in *Handbook of Coding Theory*, R.Brualdi,C.Huffman,V.Pless, Eds.

[2] 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 '96

[3] M.K.Simon,J.K.Omura,R.A.Scholtz,B.K.Levitt, *Spread Spectrum Communications, Vol 1*, Rockville, MD: Computer Science Press, '85