Cross-Correlations of Linearly and Quadratically Related Geometric Sequences and GMW Sequences*

A. Klapper† A. H. Chan‡ M. Goresky§

*Parts of this work have been presented at the Eurocrypt Conference, Århus, Denmark, May 1990, and the Marshall Hall Conference, Burlington, Vt., Sept. 1990

†Northeastern University, Boston, MA 02115 and the University of Manitoba, Winnipeg, Manitoba R3T 2N2. Project sponsored by the National Security Agency under Grant Number MDA904-91-H-0012. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon.

‡Northeastern University, Boston, MA 02115. Project sponsored by the National Security Agency under Grant Number MDA904-91-H-0012. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon.

§Northeastern University, Boston, MA 02115.

Abstract

In this paper we study the cross-correlation function values of geometric sequences obtained from q-ary m-sequences whose underlying m-sequences are linearly or quadratically related. These values are determined by counting the points of intersection of pairs of hypeplanes or of hyperplanes and quadric hypersurfaces of a finite geometry. The results are applied to obtain the cross-correlations of m-sequences and GMW sequences with different primitive polynomials.

1 Introduction

In an earlier paper, Games [4] calculated the cross-correlation values between an m-sequence and a GMW sequence based on the same primitive polynomial. He posed the problem of calculating these cross-correlation values when the m-sequence and the GMW sequence are based on different primitive polynomials. In this paper we partially solve Games' problem, finding three valued cross-correlations, together with a number of similar problems for a wide variety of related pseudorandom binary sequences.

We will be concerned with a binary sequence **S** which is generated from a q-ary m-sequence **U** followed by a nonlinear "feedforward" function $f : GF(q) \rightarrow GF(2)$, where q is a power of a prime p. This is a very general class of binary pseudorandom sequences which includes m-sequences [6], GMW sequences [7], geometric sequences [2], and bent sequences [12], and is closely related to No's sequences [9]. Sequences of this type have many applications in modern communication systems and cryptography ([15], [13]). For example, Chan and Games [2] show that if q is chosen to be a power of an *odd* prime, then the linear complexity of the resulting binary pseudorandom sequence is enormous. These *geometric sequences* are therefore natural choices for stream cipher systems. One of the consequences of our analysis is that the average of the absolute value of the autocorrelation values for the geometric sequences based on a power q of an odd prime is at least q^{n-2}. This may be unacceptably high in applications involving large amounts of data.

For ease of exposition, we shall use the term "geometric sequence" for any binary pseudorandom sequence of the type described above, whether q is even or odd, although the results in the even and odd cases are quite different. Recall that a k-fold decimation of a periodic sequence is obtained by selecting every kth element of the sequence. We will consider (a) the cross-correlation function values of geometric sequences which are obtained from the same underlying q-ary m-sequence (or whose underlying m-sequences are related by a k-fold decimation, k a power of p, i.e. of p-adic weight 1) but different nonlinear feedforward functions and (b) the cross-correlation function values of geometric sequences that are obtained from q-ary m-sequences whose underlying m-sequences are related by a k-fold decimation where k is of the form $q^i + q^j$ (i.e., of q-adic weight 2) and possibly different nonlinear feedforward functions. The m-sequences in case (a) are said to be linearly related, since exponentiation by a power of p is linear over $GF(p)$, while those in case (b) are said to be quadratically related since exponentiation by $q^i + q^j$ is quadratic over $GF(q)$. In case (b), the characteristic must be two – quadratic decimations of m-sequences in odd characteristic are never m-sequences.

The technique in this paper allow us to compute the cross-correlations of a wide variety of types of geometric sequences in terms of cross-correlation functions of shorter sequence based on the feedforward function alone. It is based on counting the points of intersection of hyperplanes and quadric hypersurfaces in a finite geometry, and was inspired by the beautiful exposition of Gold codes in [11] and by the analysis of quadrics related to m-sequences in [5]. (More general correlation problems will involve the counting of points of intersection of hyperplanes and hypersurface of higher degrees. We have some hope that the recent technical advances of Kumar and Moreno [9] may be used to solve these problems.)

In Section 2 we recall the definition and basic properties of geometric sequences, state the main theorem (Theorem 2) on quadratically decimated geometric sequences, together with the analogous but simpler result (Theorem 1) on linearly decimated geometric sequences. In Section 3 we consider several families of geometric sequences and indicate how Theorem 2 may be used to calculate the cross-correlation between any two sequences in the same family. A number of these families have low cross-correlation. Our investigations in Section 3 only scratch the surface of this fascinating topic. We also point out that there is an interesting open problem involving the cross-correlation of families of generalized geometric sequences which are derived from Gold sequences.

Theorems 1 and 2 are proven in similar ways, but Theorem 2 is technically more difficult since it depends on an understanding of the intersection of a quadric with a hyperplane, while Theorem 1 involves only the intersections of hyperplanes. Section 4 contains the proof of Theorem 1, together with the relevant material on hyperplanes in a finite geometry. It is a model for the proof of Theorem 2, which constitutes the bulk of this paper. In Sections 5 and 6, we develop the mathematical tools in number theory and theory of quadratic forms that are needed in the proof of Theorem 2. It turns out that we need to know more than the classification of quadrics ([10]) in a finite geometry: we need to classify and count the number of different configurations involving a quadric and a hyperplane.

Section 7 contains the proof of Theorem 2. In Section 8 we apply our results to obtain the cross-correlation function of an m-sequence and a GMW-sequence with *different* primitive polynomials, such that the exponents defining the GMW sequence have q-adic weight one or two. We find that these cross-correlation functions are three-valued.

2 Geometric Sequences and Correlations

In this section we recall the definition of the geometric sequences and list their basic properties. We summarize our main result on their cross-correlation functions. Throughout this paper, q will denote a fixed power of a fixed prime p, and $GF(q)$ will denote the Galois field of q elements.

Let n be a positive integer and let α and β be primitive elements of $GF(q^n)$ with $\beta = \alpha^k$ (so k is relatively prime to $q^n - 1$). The *q-ary m-sequences* $\mathbf{U}_r = Tr_q^{q^n}(\alpha^r)$ and $\mathbf{V}_r = Tr_q^{q^n}(\beta^r)$ are related by a decimation, $\mathbf{V}_r = \mathbf{U}_{kr}$. Now let f and g be (nonlinear) functions from $GF(q)$ to $GF(2)$. We consider the *geometric sequences* [2]

$$\mathbf{S}_r = f(Tr_q^{q^n}(\alpha^r)) \text{ and } \mathbf{T}_r = g(Tr_q^{q^n}(\beta^r)) = g(Tr_q^{q^n}(\alpha^{kr})). \tag{1}$$

These are $(q^n - 1)$-periodic binary sequences. We say the sequence $\mathbf{T}$ is *related* to the sequence $\mathbf{S}$ with decimation (or *exponent*) k (and a change of feedforward function).

The periodic cross-correlation function of $\mathbf{S}$ and $\mathbf{T}$ is the function whose value at τ is the correlation of the τ-shift of $\mathbf{S}$ with $\mathbf{T}$, represented by

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{r=1}^{q^n-1} (-1)^{\mathbf{S}_{r+\tau}} (-1)^{\mathbf{T}_r}.$$

The object of this paper is to compute the cross-correlation function of $\mathbf{S}$ and $\mathbf{T}$. In this paper we consider two types of values for the decimation k:

1. $k = p^e$ is a power of p: we say that the underlying m-sequences are related by a *linear decimation*.

2. $k = q^i + q^j$ for $0 \le i \le j < n$ (and $i \ne j$ if $q = 2$): we say that k has *q-adic weight* 2, and that $\mathbf{V}_r$ is a *quadratic decimation* of the m-sequence $\mathbf{U}_r$.

Notice that in case (2), since $\mathbf{V}_r$ is an m-sequence we must have $\gcd(k, q^n - 1) = 1$. This implies that q is even, i.e. the characteristic of the field $GF(q)$ is $p = 2$. We will therefore make this an underlying assumption in our analysis of quadrics and quadratic forms.

The determination of the cross-correlation of geometric sequences is the main result in this paper. For simplicity, we first transform the sequences of zeros and ones into sequences of plus and minus ones by letting $F(u) = (-1)^{f(u)}$, $G(u) = (-1)^{g(u)}$. The answer involves the *imbalance*

$$I(f) = \sum_{u \in GF(q)} F(u)$$

and the *short cross-correlation* function,

$$\Delta_a^e(f,g) = \sum_{u \in GF(q)} F(au)G(u^{p^e})$$

where $a \in GF(q)$.

Theorem 1 *Let* $\mathbf{S}$ *and* $\mathbf{T}$ *denote the geometric sequences defined in Equation (1), with q a power of an arbitrary prime p. Suppose* $\mathbf{T}$ *is linearly related to* $\mathbf{S}$ *with decimation $k = p^e$. Then the values for the periodic cross-correlation are:*

1. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-2}I(f)I(g) - (-1)^{f(0)}(-1)^{g(0)}$ *which occurs for $q^n - q$ values of τ, whenever $\alpha^\tau \notin GF(q)$*

2. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-1}\Delta_a^e(f,g) - (-1)^{f(0)}(-1)^{g(0)}$ *which occurs once for each nonzero value of a, where $a = \alpha^{-\tau} \in GF(q)$*

In particular, the autocorrelation function of the geometric sequence $\mathbf{S}$ *is*

$$\theta_{\mathbf{S},\mathbf{S}}(\tau) = \begin{cases} q^{n-2}I(f)^2 - 1 & \textit{if} \quad \alpha^\tau \notin GF(q) \\ q^{n-1}\Delta_a^e(f,f) - 1 & \textit{if} \quad \alpha^\tau = a \in GF(q) \end{cases}$$

Theorem 2 *Let* $\mathbf{S}$ *and* $\mathbf{T}$ *denote the geometric sequences defined in Equation (1), with q even. Suppose* $\mathbf{T}$ *is quadratically related to* $\mathbf{S}$ *with decimation $k = q^i + q^j$. Let $m = n - \gcd(n, j-i)$. Then m is even and the values for the periodic cross-correlation function $\theta_{\mathbf{S},\mathbf{T}}(\tau)$ are:*

1. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-2}I(f)I(g) - (-1)^{f(0)}(-1)^{g(0)}$ *which occurs for $q^n - q^{m+1} + q^m - 1$ values of τ.*

2. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = (q^{n-2} - q^{n-m/2-2})I(f)I(g) + q^{n-m/2-1}\Delta_a^1(f,g) - (-1)^{f(0)}(-1)^{g(0)}$ *which occurs for $(q^m + q^{m/2})/2$ values of τ for each nonzero $a \in GF(q)$.*

3. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = (q^{n-2} + q^{n-m/2-2})I(f)I(g) - q^{n-m/2-1}\Delta_a^1(f,g) - (-1)^{f(0)}(-1)^{g(0)}$ *which occurs for $(q^m - q^{m/2})/2$ values of τ for each nonzero $a \in GF(q)$.*

Remarks on Theorem 1. Geometric sequences with q odd have important applications to stream cipher systems because of their enormous linear complexity (see [2]). However, in this case the imbalance $I(f)$ cannot be 0. Theorem 1 indicates that the periodic autocorrelation function for these sequences is unacceptably high. On the other hand, if the characteristic p is 2, then by choosing f and g appropriately as above we can guarantee that $I(f) = I(g) = 0$ and that $|\Delta_a^e(f,g)| \leq \sqrt{2q}$. The cross-correlation $\theta_{\mathbf{S},\mathbf{T}}$ consists of periodic pulses of magnitude $q^{n-1}\sqrt{2q}$ occurring once every $(q^n-1)/(q-1)$ clock cycles. Note that Theorem 1 includes the case of two geometric sequences which correspond to the same m-sequence with no decimation at all (i.e. k = 1) but which use different nonlinear feedforward functions.

Remarks on Theorem 2. 1. The same result holds for the slightly more general class of decimations, $k = 2^e(q^i + q^j)$.
2. The underlying primitive elements α and β are related by $\beta = \alpha^k$, or $\alpha = \beta^K$ where $K = k^{-1} \pmod{q^n - 1}$. The q-adic weight of K may be different from 2. Thus by switching the roles of $\mathbf{S}$ and $\mathbf{T}$ we find that *the same cross-correlation values occur if* $\mathbf{T}$ *is related to* $\mathbf{S}$ *through a decimation by* K *(and a change of feedforward function), provided the q-adic weight of* K^{-1} *(mod* $q^n - 1$*) is 2.*
3. By taking $q = 2$ (and f and g to be the identity map $GF(2) \to GF(2)$), the geometric sequences $\mathbf{S}$ and $\mathbf{T}$ become m-sequences and we recover the often calculated cross-correlation values for quadratically decimated m-sequences [5, 8, 11, 14]. In particular, choosing $j-i$ to be relatively prime to n (n odd), and noting that $\Delta_1^1(f,g) = 2$ we obtain

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \begin{cases} -1 & \text{occurring} \quad r/2-1 \quad \text{times} \\ \sqrt{2r}-1 & \text{occurring} \quad r/4+\sqrt{r/8} \quad \text{times} \\ -\sqrt{2r}-1 & \text{occurring} \quad r/4-\sqrt{r/8} \quad \text{times} \end{cases}$$

where $r = 2^n$. Thus we have shown

Corollary 1 *Suppose* i, j, n *are chosen so that* $\gcd(j-i, 2^n-1) = 1$. *Set* $q = 2^n$ *and* $k = 2^i + 2^j$. *Consider the functions* $f, g : GF(q) \to GF(2)$ *defined by* $f(x) = Tr_2^q(x)$ *and* $g(x) = Tr_2^q(x^k)$. *Then* $|\Delta_a^1(f,g)| \leq \sqrt{2q}$ *and in fact,*

$$|\Delta_a^1(f,g)| = \begin{cases} 0 & \textit{for} \quad 2^{n-1} \quad \textit{values of } a \in GF(q) \\ \sqrt{2q} & \textit{for} \quad 2^{n-1} \quad \textit{values of } a \in GF(q) \end{cases}$$

4. Choosing f and g so as to have cross-correlation $|\Delta_a^1(f,g)| \leq \sqrt{2q}$ as above, and choosing $j-i$ to be relatively prime to n (n odd), we find that $|\Theta_{\mathbf{S},\mathbf{T}}(\tau)| \leq \sqrt{2q^n}+1$. Better bounds may be obtained by taking f and g to be appropriately chosen bent functions [12]. Even if f

and g are chosen arbitrarily, the obvious bound $|\Delta_a^1(f,g)| \leq q$ gives $|\Theta_{\mathbf{S},\mathbf{T}}(\tau)| \leq \sqrt{q^{n+1}} + 1$. Thus quadratically related geometric sequences may be easily separated.

Remarks on Partial Correlations. Suppose $\mathbf{S}$ and $\mathbf{T}$ are binary sequences of period N. Recall that the partial period cross-correlation of block size K, initial position ℓ, and shift τ is defined to be

$$\Theta_{\mathbf{S},\mathbf{T}}(K,\ell,\tau) = \sum_{j=0}^{K-1} (-1)^{S_{\ell+j+\tau}} (-1)^{T_{\ell+j}},$$

as in [15]. For many applications, it is this partial period correlation which is important, rather than the periodic cross-correlation. These partial period cross-correlations are usually very difficult to compute. A statistical description of the partial period correlation may be obtained by performing a time average:

$$\langle \Theta_{\mathbf{S},\mathbf{T}}(K,\ell,\tau) \rangle = \frac{1}{N} \sum_{\ell=1}^{N} \Theta_{\mathbf{S},\mathbf{T}}(K,\ell,\tau).$$

It is easy to see that this time averaged partial period correlation is related to the periodic cross-correlation $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$ by the following formula:

$$\langle \Theta_{\mathbf{S},\mathbf{T}}(K,\ell,\tau) \rangle = \frac{K}{N} \Theta_{\mathbf{S},\mathbf{T}}(\tau).$$

The proof is straightforward.

3 Families of Geometric Sequences

Using Theorems 1 and 2 it is possible to construct a wide variety of families of geometric sequences having interesting properties. We give a few examples below.

1. Families derived from linear decimations If two geometric sequences $\mathbf{S}$ and $\mathbf{T}$ are related by a linear decimation $k = p^e$ and if $\mathbf{R}$ and $\mathbf{S}$ are related by a linear decimation $k' = p^d$ then $\mathbf{R}$ and $\mathbf{T}$ are related by a linear decimation $k'' = p^{d+e}$. Thus we may construct a family of geometric sequences by varying the feedforward functions f within a family $\{f_1, f_2, \ldots, f_r\}$, and by varying the choice of decimations among various powers of p. The cross-correlations are then all given by Theorem 1.

2. Families derived from quadratic decimations Using the notation of section 2, we fix a quadratic decimation $k = q^i + q^j$ and a family of feedforward functions $\{h_1, h_2, \ldots, h_r\}$ mapping $GF(q) \to GF(2)$, having the property that the cross-correlation

$|\Delta_a^1(h_1, h_2)|$ between any two of them is bounded by $\sqrt{2q}$ (see remarks on Theorem 2). Consider the two families of geometric sequences,

$$\begin{aligned}\mathbf{S}^{(j)}(t) &= h_j(Tr_q^{q^n}(\alpha^t))\\ \mathbf{T}^{(j)}(t) &= h_j(Tr_q^{q^n}(\beta^t))\end{aligned}$$

where $\beta = \alpha^k$. For any two sequences in the first family, the cross-correlations are given by Theorem 1. For any two sequences in the second family the cross-correlation is also given by Theorem 1. Furthermore, the cross-correlation between any sequence in the first family and any sequence in the second family is $\leq \sqrt{2q^n} + 1$ (see remark 4 on Theorem 2).

3. Other families Thusfar, the cross-correlation between generalized geometric sequences of the form

$$S^{A,B}(t) = f(Tr_q^{q^n}(A\alpha^i + B\beta^i))$$

where $\beta = \alpha^k$, remains open. The problem appears to involve counting the number of points on the intersection of two quadric hypersurfaces.

We hope the new techniques introduced by Kumar and Moreno [9] may be used in answering this question.

4 Hyperplanes in $GF(q^n)$

The geometric sequences are based on the geometry of hyperplanes in the finite field $GF(q^n)$. The cross-correlation of these geometric sequences is calculated by counting the number of elements in the intersections of two hyperplanes. The use of intersecting hyperplanes for evaluating cross-correlation of pseudorandom sequences was considered by Games [4] and our method is similar to his. In this section we review some of the basic facts concerning hyperplanes and their intersections, and give the proof for Theorem 1.

Let $Tr_q^{q^n} : GF(q^n) \to GF(q)$ denote the trace function. For any $u \in GF(q)$ we define

$$H_u = \{x \in GF(q^n) | Tr_q^{q^n}(x) = u\}$$

Then H_u is an (affine) hyperplane, i.e. it is a translate of an $n-1$ dimensional vector subspace of $GF(q^n)$. The hyperplanes H_u and H_v are parallel, i.e. they have no points of intersection unless $u = v$, in which case they are equal. Now let $b \neq 0 \in GF(q^n)$, $v \in GF(q)$, and consider the hyperplane

$$\begin{aligned}b^{-1}H_v &= \{b^{-1}y | y \in H_v\}\\ &= \{b^{-1}y | Tr_q^{q^n}(y) = v\}\\ &= \{x | Tr_q^{q^n}(bx) = v\}.\end{aligned}$$

Lemma 1 *The hyperplanes H_u and $b^{-1}H_v$ are parallel if and only if $b \in GF(q)$.*

Proof. If $b \in GF(q)$ then

$$\begin{aligned} b^{-1}H_v &= \{x | Tr_q^{q^n}(bx) = v\} \\ &= \{x | bTr_q^{q^n}(x) = v\} \\ &= H_{b^{-1}v}. \end{aligned}$$

and these hyperplanes are parallel.

On the other hand, if H_u and $b^{-1}H_v$ are parallel, then we must show that $b \in GF(q)$. Since H_u is parallel to H_0, we may assume that $u = 0$. Let us first consider the case when the two parallel hyperplanes H_0 and $b^{-1}H_v$ actually coincide. Thus,

$$x \in H_0 \text{ iff } \; Tr_q^{q^n}(x) = 0 \text{ iff } \; Tr_q^{q^n}(bx) = v.$$

By taking $x = 0$ we see that $v = 0$. Now choose $z \in GF(q^n) - H_0$. Since H_0 is a subspace of dimension $n-1$, the addition of this one more linearly independent element will span all of $GF(q^n)$. Therefore bz may be written as a linear combination involving z and H_0,

$$bz = az + h$$

for some $a \in GF(q)$ and $h \in H_0$. We will show that $b = a \in GF(q)$.

If this were false, we would have $z = h/(b-a)$. But multiplication by a preserves H_0, and multiplication by b also preserves H_0, so multiplication by $(b-a)$ preserves H_0, and so multiplication by $(b-a)^{-1}$ preserves H_0. Therefore $z \in H_0$, and this is a contradiction.

Next we consider the general case, H_0 not necessarily equal to $b^{-1}H_v$. There is a translation $x_0 \in GF(q^n)$ such that

$$H_0 = b^{-1}H_v - x_0.$$

Define $v' = v - Tr_q^{q^n}(bx_0)$. Then

$$\begin{aligned} b^{-1}H_v - x_0 &= \{b^{-1}x - x_0 | Tr_q^{q^n}(x) = v\} \\ &= \{y | Tr_q^{q^n}(by + bx_0) = v\} \\ &= \{y | Tr_q^{q^n}(by) = v'\} \\ &= b^{-1}H_{v'} \end{aligned}$$

Thus $b^{-1}H_{v'} = H_0$ and the preceding special case applies to this situation, from which we conclude that $b \in GF(q)$. □

Lemma 2 *If $b \in GF(q^n) - GF(q)$, then for any u, $v \in GF(q)$, the number of elements in the intersection $H_u \cap b^{-1}H_v$ is precisely q^{n-2}.*

Proof. By Lemma 1, the hyperplanes H_u and $b^{-1}H_v$ are not parallel. If two hyperplanes are not parallel, then their intersection is a hyperplane inside each, i.e. it is an $n-2$ dimensional (affine) subspace of $GF(q^n)$. Therefore it contains q^{n-2} points. □

Proof of Theorem 1. Let $S(x) = Tr_q^{q^n}(x)$ and $T(x) = Tr_q^{q^n}(x^k)$ where $k = p^e$ and recall that $F(x) = (-1)^{f(x)}$ and $G(x) = (-1)^{g(x)}$. The cross-correlation function of the sequences **S** and **T** is then given by

$$\begin{aligned} \theta_{\mathbf{S},\mathbf{T}}(\tau) &= \sum_{r=1}^{q^n-1} F(Tr_q^{q^n}(\alpha^{r+\tau}))G(Tr_q^{q^n}(\beta^r)) \\ &= \sum_{x \in GF(q^n)} F(S(\alpha^\tau x))G(T(x)) - F(0)G(0). \end{aligned}$$

since α and β are primitive elements with $\beta = \alpha^k$. Now let $Q_v = \{x : T(x) = v\}$. We have

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{u \in GF(q)} \sum_{v \in GF(q)} |a^{-1}H_u \cap Q_v| F(u)G(v) - F(0)G(0).$$

where $a = \alpha^\tau \in GF(q^n)$. But

$$Q_v = \{x : Tr_q^{q^n}(x^k) = v\} = \{x : (Tr_q^{q^n}(x))^k = v\} = \{x : Tr_q^{q^n}(x) = v^{1/k}\} = H_{v^{1/k}}$$

which is also a hyperplane. The intersection of two hyperplanes is an $(n-2)$-dimensional subspace unless the hyperplanes are parallel. Thus $|a^{-1}H_u \cap Q_v| = q^{n-2}$ unless $a = \alpha^\tau \in GF(q)$ by Lemma 1. If the hyperplanes are parallel, that is, $a \in GF(q)$, then $a^{-1}H_u = H_{au}$ and its intersection with $Q_v = H_{v^{1/k}}$ is empty unless the two hyperplanes actually coincide, i.e. unless $(au)^k = v$. In summary the cross-correlation is

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-2} \sum_{u \in GF(q)} F(u) \sum_{v \in GF(q)} G(v) - F(0)G(0)$$

if $\alpha^\tau \notin GF(q)$, and

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-1} \sum_{u \in GF(q)} F(u)G(a^k u^k) - F(0)G(0)$$

if $\alpha^\tau = a \in GF(q)$. Substituting $v = au$ and $b = a^{-1}$, we can rewrite the last sum as $\sum_{v \in GF(q)} F(bv)G(v^k) = \Delta_b^e(f, g)$. □

5 Number Theoretic Tools

In this section we prove several number theoretic results that will be useful in the proof of Theorem 2.

Lemma 3 *Let b, n and j be non-negative integers and set $d = \gcd(n, j)$. Then* $\gcd(b^n - 1, b^j - 1) = b^d - 1$.

Proof: This is a standard consequence of the division algorithm. $\square$

Lemma 4 *Suppose b is an even integer. Let n, i, and j be non-negative integers, with $i \leq j$ and $n \neq 0$, and let $d = \gcd(n, j - i)$. Then*

$$\gcd(b^n - 1, b^i + b^j) = \begin{cases} 1 & \textit{if} \quad n/d \textit{ is odd} \\ 1 + b^d & \textit{if} \quad n/d \textit{ is even.} \end{cases}$$

Proof: Since b does not divide $b^n - 1$, we have $\gcd(b^n - 1, b^i + b^j) = \gcd(b^n - 1, 1 + b^{j-i})$. Thus we may assume that $i = 0$. Since b is even, $\gcd(b^j + 1, b^j - 1) = \gcd(2, b^j - 1) = 1$. Therefore

$$\begin{aligned} \gcd(b^j + 1, b^n - 1) &= \frac{\gcd(b^{2j} - 1, b^n - 1)}{\gcd(b^j - 1, b^n - 1)} \\ &= \frac{b^{\gcd(2j,n)} - 1}{b^{\gcd(j,n)} - 1} \\ &= \begin{cases} 1 & \text{if } \gcd(2j, n) = \gcd(j, n) \text{, i.e., } n/\gcd(j, n) \text{ is odd} \\ b^{\gcd(j,n)} + 1 & \text{otherwise.} \end{cases} \end{aligned}$$

$\square$

For completeness we note that if b is odd then the same result holds with 2 replacing 1 as the value of the gcd when n/d is odd.

We will need to be able to determine when quadratic polynomials have roots. In odd or zero characteristic this is straightforward – a quadratic polynomial has roots if and only if its discriminant is a square, and the roots are given by the quadratic formula. In characteristic two, however, this fails – the discriminant is always a square (since every element in the field is a square) and the quadratic formula is undefined (it involves division by two). Instead we have the following lemma.

Lemma 5 *Let $c, d, e \in GF(q)$, with q even. Then the quadratic equation $cx^2 + dx + e = 0$ has a nontrivial solution $x \in GF(q)$ iff $d = 0$ or $Tr_2^q(ec/d^2) = 0$.*

Proof: The case $c = 0$ or $e = 0$ is easily handled, so we assume $c \neq 0$ and $e \neq 0$. If $d = 0$ then $x^2 = e/c$ which has a unique solution in $GF(q)$, so we may also assume that $d \neq 0$. The substitution $x' = cx/d$ may be used to convert the quadratic equation to the form $x^2 + x + f = 0$ where $f = ec/d^2$. Since $x^2 + x + f$ is irreducible in $GF(q)$ if and only if $Tr_2^q(f) \neq 0$ [10, Corollary 3.79], the result follows. □

As a consequence of Lemma 5 we can reduce quadratic forms in two variables as follows:

Lemma 6 *Given $c, d, e \in GF(q)$, (with q even), define the quadratic form $g(x, y) = cx^2 + dxy + ey^2$. Then $g(x, y)$ is nonsingular iff $d \neq 0$. In this case, g is equivalent under a linear change of variables to the quadratic form*

$$\begin{cases} xy & \text{if} \quad Tr_2^q(ec/d^2) = 0 \\ x^2 + xy + ay^2 & \text{if} \quad Tr_2^q(ec/d^2) \neq 0. \end{cases}$$

Proof: If $d = 0$ the substitution $x \mapsto \frac{1}{\sqrt{c}}x + \frac{e}{\sqrt{c}}y$ converts the quadratic form $g(x, y)$ into the singular form x^2. Now suppose $d \neq 0$. If $Tr_2^q(ec/d^2) = 0$ then by Lemma 5 there is a nonzero solution λ to the quadratic equation $c\lambda^2 + d\lambda + e = 0$. The change of coordinates $x \mapsto (1 + \lambda c/d)x + (\lambda/d)y$ and $y \mapsto (c/d)x + (1/d)y$ converts the form g into the quadratic form xy. Finally, if $Tr_2^q(ec/d^2) = a \neq 0$, then $Tr_2^q(a + ec/d^2) = 0$ and $x^2 + x + ec/d^2 = a$ has a solution $\lambda \in GF(q)$. Consider the change of variables

1. $x \to \frac{1}{\sqrt{c}}x + \frac{\lambda}{\sqrt{c}}y$,
2. $y \to \frac{\sqrt{c}}{d}y$.

Then $g(x, y)$ becomes $x^2 + xy + ay^2$. □

Throughout the rest of this paper, we fix q a power of 2, and we fix a nonzero element $a \in GF(q)$ such that $Tr_2^q(a) \neq 0$.

6 Quadratic Forms in Characteristic 2

In this section we count the number of solutions to homogeneous quadratic equations. This can be thought of as counting the number of points on a quadric hypersurface. We first must show that under a change of basis every quadratic form in n variables is equivalent to one of several standard forms. We then compute the number of roots of each type of quadratic form. Finally, if $S \neq 0$ is a linear function from $GF(q^n)$ to $GF(q)$, and k is an integer with q-adic weight two which is prime to $q^n - 1$ (so $S(x^k)$ gives rise to an m-sequence), we identify precisely which standard form $S(x^k)$ is equivalent to.

In general we let $\bar{x}$ denote $(x_1, \ldots, x_n)$ and $B_m(\bar{x}) = x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m$. A quadratic form in n variables, $Q(\bar{x}) = \sum_i \sum_j a_{ij}x_ix_j$, *represents zero* if it has a nonzero root. The quadratic form Q has *rank* m if there is a linear change of variables so that Q may be expressed as a function of m variables (and no fewer). The quadratic form Q is *nonsingular* if $\mathrm{rank}(Q) = n$.

Quadratic forms $Q(\bar{x})$ in n variables over $GF(q)$ (with q even) have been classified [10, Theorem 6.30] and are given as follows:

Type I: $B_m(\bar{x})$,
Type II: $B_m(\bar{x}) + x_{m+1}^2$,
Type III: $B_m(\bar{x}) + x_{m+1}^2 + x_{m+1}x_{m+2} + ax_{m+2}^2$.
where $m = \mathrm{rank}(Q)$.

Proposition 1 *For any quadratic form Q in n variables, the number of solutions to the equation $Q(\bar{x}) = v$ is:*

Type I: $\begin{cases} q^{n-1} + q^{n-m/2} - q^{n-m/2-1} & \textit{if} \quad v = 0 \\ q^{n-1} - q^{n-m/2-1} & \textit{if} \quad v \neq 0, \end{cases}$

Type II: q^{n-1},

Type III: $\begin{cases} q^{n-1} - q^{n-m/2-1} + q^{n-m/2-2} & \textit{if} \quad v = 0 \\ q^{n-1} + q^{n-m/2-2} & \textit{if} \quad v \neq 0. \end{cases}$

Proof: Any solution $(x_1, x_2, \ldots, x_m)$ to the equation

$$Q(x_1, x_2, \ldots, x_m) = v. \tag{2}$$

gives rise to q^{n-m} solutions $\bar{x} = (x_1, x_2, \ldots, x_n)$ of the equation $Q(\bar{x}) = v$ by allowing the last $n - m$ coordinates to have arbitrary values. This reduces the problem to the case where Q is nonsingular. The number of solutions to $Q(\bar{x}) = v$ for nonsingular quadratic forms have been calculated [10, Theorem 6.32] and our results follow. □

Any choice of basis $e_1, e_2, \ldots, e_n$ for $GF(q^n)$ as a vectorspace over $GF(q)$ determines an identification $GF(q)^n \to GF(q^n)$ by $\bar{x} = (x_1, x_2, \ldots, x_n) \mapsto \sum_i x_ie_i = x$. When such a basis has been chosen, we shall write $\bar{x}$ if the element x is to be thought of as a vector in $GF(q)^n$, and we shall write x when the same vector is to be thought of as an element of the field $GF(q^n)$. Fix $c \in GF(q^n)$ $c \neq 0$ and define the function $T : GF(q)^n \to GF(q)$ by $T(\bar{x}) = Tr_q^{q^n}(cx^k)$.

Theorem 3 *Suppose $k = q^i + q^j$ (so k has q-adic weight 2). Then $T(\bar{x})$ is a quadratic form. Moreover, if $n/\gcd(n, j-i)$ is odd, then it is a type II quadratic form, with*

$$m = \begin{cases} n - \gcd(n, j-i) & \text{if} \quad i \neq j \\ 0 & \text{if} \quad i = j \end{cases}$$

and m is even.

Proof: Let $e_1, e_2, \ldots, e_n$ denote the chosen basis, then

$$\begin{aligned} T(\bar{x}) &= Tr_q^{q^n}(c(\sum_{h=1}^{n} x_h e_h)^{q^i+q^j}) \\ &= Tr_q^{q^n}(c(\sum_{h=1}^{n} x_h e_h^{q^i})(\sum_{l=1}^{n}(x_l e_l^{q^j})) \\ &= \sum_{h=1}^{n}\sum_{l=1}^{n} a_{hl} x_h x_l \end{aligned}$$

where $a_{hl} = Tr_q^{q^n}(ce_h^{q^i} e_l^{q^j})$, and $T(\bar{x})$ is a quadratic form.

If $n/\gcd(n, j-i)$ is odd, then by Lemma 4, k is relativelly prime to $q^n - 1$ and the function $x \mapsto x^k$ is invertible. It follows that $Tr_q^{q^n}(cx^k)$ takes on every value in $GF(q)$ the same number of times. This rules out types I and III quadratic forms. Thus T is a type II quadratic form.

It only remains to determine m, which in this case is equal to $\text{rank}(T) - 1$. In the determination of the rank of T, we may assume that $i = 0$ because $x^k = (x^{q^i})^{(1+q^{j-i})}$ and the map $x \mapsto x^{q^i}$ is invertible.

Suppose first that $j = 0$ and let $c = d^2$. Then $T(\bar{x}) = Tr_q^{q^n}(cx^2) = (Tr_q^{q^n}(dx))^2 = x_1^2$, where $x_1 = Tr_q^{q^n}(dx)$. This is the the desired form.

Now suppose $j > 0$. The type II quadratic form $B_m(\bar{x}) + x_{m+1}^2$ has rank $m+1$. Consider the set

$$W = \{w \in GF(q^n) : T(w) = 0 \text{ and } \forall y \in GF(q^n), T(w+y) = T(y)\}.$$

W is a $GF(q)$-vector subspace in $GF(q^n)$, and the dimension of W is the co-rank of T. We must show that W has dimension $\gcd(n, j) - 1$.

Let $w \in GF(q^n)$. Expanding out the expression $(w + y)^{1+q^j}$, we see that $w \in W$ if and only if $Tr_q^{q^n}(cw^k) = 0$ and for every $y \in GF(q^n)$, $Tr_q^{q^n}(cwy^{q^j}) = Tr_q^{q^n}(cw^{q^j}y)$. Since

$Tr_q^{q^n}(x) = Tr_q^{q^n}(x^q)$, the right hand side of this equation is unchanged if we raise its argument to the power q^j, which gives

$$Tr_q^{q^n}(cwy^{q^j}) = Tr_q^{q^n}(c^{q^j} w^{q^{2j}} y^{q^j})$$

or

$$Tr_q^{q^n}((cw + c^{q^j} w^{q^{2j}})y^{q^j}) = 0$$

for all $y \in GF(q^n)$. This implies that $cw = c^{q^j} w^{q^{2j}}$, or, if $w \neq 0$, that $(dw)^{q^{2j}-1} = 1$, where $c = d^{q^j+1}$. Such a d exists, by Lemma 4. Thus $dw \in GF(q^{2j})$ and since $dw \in GF(q^n)$, we conclude that $dw \in GF(q^{\gcd(n,2j)}) = GF(q^{\gcd(n,j)})$ by our assumption that $n/gcd(n,j)$ is odd. In summary,

$$dW = \left\{ w' \in GF(q^{\gcd(n,j)}) : Tr_q^{q^n}(cw'/d) = 0 \right\}.$$

This is a vectorspace over $GF(q)$ of dimension $\gcd(n,j) - 1$. □

7 Proof of Theorem 2

We return to the situation of Theorem 2: q is a power of 2, α and β are primitive elements of $GF(q)$, $\beta = \alpha^k$ where $k = q^i + q^j$ is relatively prime to $q^n - 1$, f and g are nonlinear feedforward functions from $GF(q)$ to $GF(2)$. Let $S(x) = Tr_q^{q^n}(x)$, and $T(x) = Tr_q^{q^n}(x^k)$. Then the geometric sequences $\mathbf{S}$ and $\mathbf{T}$ are given by $\mathbf{S} = f(S(1)), f(S(\alpha)), f(S(\alpha^2)), \ldots$ and $\mathbf{T} = g(S(1)), g(S(\beta)), g(S(\beta^2)), \ldots = g(T(1)), g(T(\alpha)), g(T(\alpha^2)), \ldots$. We will write $F(x) = (-1)^{f(x)}$ and $G(x) = (-1)^{g(x)}$, where we consider $GF(2)$ to be $\{0, 1\}$ as a subset of the integers. The cross-correlation function of $\mathbf{S}$ and $\mathbf{T}$ is the function whose value at τ is the periodic correlation of the τ-shift of $\mathbf{S}$ with $\mathbf{T}$,

$$\begin{aligned} \theta_{\mathbf{S},\mathbf{T}}(\tau) &= \sum_{r=1}^{q^n-1} F(Tr_q^{q^n}(\alpha^{\tau+r}))G(Tr_q^{q^n}(\beta^r)) \\ &= \sum_{r=1}^{q^n-1} F(S(\alpha^{\tau+r}))G(T(\alpha^r)) \\ &= \sum_{x \in GF(q^n)} F(S(\alpha^\tau x))G(T(x)) - F(0)G(0). \end{aligned}$$

Now let $H_u = \{x : S(\alpha^\tau x) = u\}$, and $Q_v = \{x : T(x) = v\}$. By Theorem 3, T is a quadratic form of type II with $m = n - \gcd(n, j - i)$ so Q_v is a quadric hypersurface and H_u is a hyperplane in $GF(q^n)$. We have

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{u,v \in GF(q)} |H_u \cap Q_v| F(u)G(v) - F(0)G(0).$$

Thus in order to compute the cross-correlation of $\mathbf{S}$ and $\mathbf{T}$, we must compute the cardinalities of the intersections of various hyperplanes and quadric hypersurfaces in affine n-space over $GF(q)$.

By Proposition 1, the quadratic form $T(x)$ can be represented in some basis as $B_m(\bar{x}) + x_{m+1}^2$, where $m = n - \gcd(n, j-i)$. We fix such a basis from here on and write $S(\alpha^\tau x) = \sum_{r=1}^{n} c_r x_r$ for some $\{c_r\} \subseteq GF(q)$. There is a one-to-one correspondence between the shift τ and the coefficients $\{c_r\}$. This correspondence can only be computed by determining the basis that puts $T(x)$ in standard form. We will express the cross-correlation value $\theta_{\mathbf{S},\mathbf{T}}(\tau)$ as a function of $\{c_r\}$, rather than as a function of τ and will count the number of occurrences of each value.

We now proceed with a case by case analysis, depending upon the $\{c_r\}$.

Proposition 2 *Suppose that $c_r \neq 0$ for some $r \geq m+2$. Then*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-2} I(f) I(g) - F(0)G(0)$$

which contributes to case 1 of Theorem 2.

Proof: If we fix a solution $(x_1, x_2, \ldots x_{m+1})$ to the equation $Q(\bar{x}) = v$, then we can always find exactly q^{n-m-2} values of $x_{m+2}, \ldots, x_n$ that make $S(\bar{x}) = u$. By Proposition 1 there are q^m solutions to $Q(\bar{x}) = v$. Thus,

$$\sum_{u,v \in GF(q)} |H_u \cap Q_v| F(u) G(v) = q^{n-m-2} q^m \sum_{u \in GF(q)} F(u) \sum_{v \in GF(q)} G(v) = q^{n-2} I(f) I(g).$$

$\square$

From now on we assume $c_{m+2} = \cdots = c_n = 0$. The number of simultaneous solutions $(x_1, \ldots, x_n)$ to the equations $S(\bar{x}) = u$ and $Q(\bar{x}) = v$ is thus q^{n-m-1} times the number of simultaneous solutions $(x_1, \ldots, x_{m+1})$ to the equations $S(x_1, \ldots, x_{m+1}) = u$ and $Q(x_1, \ldots, x_{m+1}) = v$, since $x_{m+2}, \ldots, x_n$ may be chosen arbitrarily.

Proposition 3 *Suppose that $c_1 = \cdots = c_m = c_{m+2} = \cdots = c_n = 0$, $c_{m+1} \neq 0$. Then*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = (q^{n-2} - q^{n-m/2-2}) I(f) I(g) + q^{n-m/2-1} \Delta^1_{c_{m+1}}(f, g) - F(0)G(0)$$

which contributes to case 2 of Theorem 2.

Proof: In this case the equation $S(\bar{x}) = u$ uniquely determines $x_{m+1} = u/c_{m+1}$. Thus the second equation becomes

$$B_m(\bar{x}) = v + u^2/c_{m+1}^2.$$

By Proposition 1, this equation has $q^{m-1} + q^{m/2} - q^{m/2-1}$ solutions if $v + u^2/c_{m+1}^2 = 0$, and has $q^{m-1} - q^{m/2-1}$ solutions otherwise. Thus

$$|H_u \cap Q_v| = \begin{cases} q^{n-2} - q^{n-m/2-2} + q^{n-m/2-1} & \text{if} \quad v + u^2/c_{m+1}^2 = 0 \\ q^{n-2} - q^{n-m/2-2} & \text{otherwise.} \end{cases}$$

and

$$\begin{aligned} \sum_{u \in GF(q)} \sum_{v \in GF(q)} |H_u \cap Q_v| F(u) G(v) &= (q^{n-2} - q^{n-m/2-2}) \sum_{u \in GF(q)} \sum_{v \in GF(q)} F(u) G(v) \\ &\quad - q^{n-m/2-1} \sum_{u \in GF(q)} F(u) G(u^2/c_{m+1}^2). \end{aligned}$$

The proposition follows. □

Proposition 4 *Suppose $c_{m+2} = \cdots = c_n = 0$ and $c_i \neq 0$ for some $i \leq m$.*

1. *If $c_{m+1} \neq 0$ and $Tr_2^q(B_m(\bar{c})/c_{m+1}^2) \neq 0$, then*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = (q^{n-2} + q^{n-m/2-2}) I(f) I(g) - q^{n-m/2-1} \Delta^1_{c_{m+1}}(f,g) - F(0)G(0)$$

which contributes to case 3 of Theorem 2.

2. *If $c_{m+1} \neq 0$ and $Tr_2^q(B_m(\bar{c})/c_{m+1}^2) = 0$, then*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = (q^{n-2} - q^{n-m/2-2}) I(f) I(g) + q^{n-m/2-1} \Delta^1_{c_{m+1}}(f,g) - F(0)G(0)$$

which contributes to case 2 of Theorem 2.

3. *If $c_{m+1} = 0$, then*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-2} I(f) I(g) - F(0)G(0)$$

which contributes to case 1 of Theorem 2.

Proof: By symmetry, we may assume that $c_m \neq 0$. We count the number of simultaneous solutions $(x_1, \ldots, x_{m+1})$ to the equations $S(\alpha^\tau x) = u$ and $T(x) = v$. The equation $S(\alpha^\tau x) = u$ implies that

$$x_m = \sum_{r=1}^{m-1} \frac{c_r}{c_m} x_r + \frac{u}{c_m} + \frac{c_{m+1}}{c_m} x_{m+1}.$$

Substituting for x_m in $T(x)$, it remains to count the number of solutions to

$$B_{m-2}(\bar{x}) + \sum_{r=1}^{m-1} \frac{c_r}{c_m} x_r x_{m-1} + \frac{u}{c_m} x_{m-1} + \frac{c_{m+1}}{c_m} x_{m-1} x_{m+1} + x_{m+1}^2 = v \tag{3}$$

among the variables $x_1, \ldots, x_{m-1}, x_{m+1}$. We can nearly put this in standard form by the change of basis that replaces x_r by $x_r + (c_{\phi(r)}/c_m) x_{m-1}$ for $r = 1, \ldots, m-2$, where $\phi(r) = r-1$ if r is even, and $\phi(r) = r+1$ if r is odd (i.e., ϕ interchanges the indices 1 with 2, 3 with 4, etc.). Equation (3) becomes

$$B_{m-2}(\bar{x}) + \frac{B_m(\bar{c})}{c_m^2} x_{m-1}^2 + \frac{u}{c_m} x_{m-1} + \frac{c_{m+1}}{c_m} x_{m-1} x_{m+1} + x_{m+1}^2 = v. \tag{4}$$

Unfortunately this is an *inhomogeneous* quadratic equation and it is necessary to eliminate the linear term before we can count the number of solutions.

Case 1. Suppose $c_{m+1} \neq 0$. Then, without changing the count on the number of solutions, we can perform an affine change of coordinates by replacing x_{m+1} by $x_{m+1} + u/c_{m+1}$. Equation (4) becomes

$$B_{m-2}(\bar{x}) + \frac{B_m(\bar{c})}{c_m^2} x_{m-1}^2 + \frac{c_{m+1}}{c_m} x_{m-1} x_{m+1} + x_{m+1}^2 = v + \frac{u^2}{c_{m+1}^2}. \tag{5}$$

Suppose further that $Tr_2^q(B_m(\bar{c})/c_{m+1}^2) \neq 0$. Then the part of Equation (5) involving the variables x_{m-1} and x_{m+1} is a quadratic form that does not represent zero, and by Lemma 6 there is a change of basis which puts the equation in the standard form

$$B_{m-2}(\bar{x}) + x_{m-1}^2 + x_{m-1} x_{m+1} + \frac{B_m(\bar{c})}{c_{m+1}^2} x_{m+1}^2 = v + \frac{u^2}{c_{m+1}^2}.$$

This is a type III homogeneous equation so it has $q^{m-1} - q^{m/2} + q^{m/2-1}$ solutions if $v = u/c_{m+1}^2$, and it has $q^{m-1} + q^{m/2-1}$ solutions otherwise. The asserted value for the cross-correlation follows.

Case 2. Suppose that $c_{m+1} \neq 0$ and $Tr_2^q(B_m(\bar{c})/c_{m+1}^2) = 0$. Then the part of Equation (5) involving x_{m-1} and x_{m+1} represents zero and is not a square. By Lemma 6 there is a change of basis which puts the equation in the form

$$B_{m-2}(\bar{x}) + x_{m-1}x_{m+1} = v + \frac{u^2}{c_{m+1}^2}.$$

This is a type I homogeneous equation so it has $q^{m-1} + q^{m/2} - q^{m/2-1}$ solutions if $v = u/c_{m+1}^2$, and $q^{m-1} - q^{m/2-1}$ solutions otherwise. The asserted value for the cross-correlation follows.

Case 3 Suppose $c_{m+1} = 0$ and let $d^2 = B_m(\bar{c})/c_m^2$. Then the change of basis that replaces x_{m+1} by $x_{m+1} + dx_{m-1}$ puts Equation (4) in the form

$$B_{m-2}(\bar{x}) + ux_{m-1} + x_{m+1}^2 = v.$$

If we choose values for $x_1, \ldots, x_{m-1}$ then we can always find a unique x_{m+1} that gives a solution to the equation, so this equation always has q^{m-1} solutions. The asserted value for the cross-correlation follows. □

It is straightforward to count the number of occurences of each of the values (letting the coefficients c_r vary). We summarize these preceding cases and their appearance in Theorem 2:

Theorem 2 *The cross-correlation with shift τ of the geometric sequences* **S** *and* **T** *of equation 1 is:*

1. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-2}I(f)I(g) - F(0)G(0)$ *if* $c_r \neq 0$ *for some* $r \geq m+2$, *or* $c_{m+1} = \cdots = c_n = 0$. *This occurs for* $q^n - q^{m+1} + q^m - 1$ *values of* τ.

2. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = (q^{n-2} - q^{n-m/2-2})I(f)I(g) + q^{n-m/2-1}\Delta_a^1(f,g) - F(0)G(0)$ *if* $c_{m+2} = \cdots = c_n = 0$, $c_{m+1} \neq 0$, *and* $Tr_2^q(B_m(\bar{c})/c_{m+1}^2) = 0$. *This occurs for* $(q^m + q^{m/2})/2$ *values of* τ *for each nonzero* $a \in GF(q)$.

3. $\theta_{\mathbf{S},\mathbf{T}}(\tau) = (q^{n-2} + q^{n-m/2-2})I(f)I(g) - q^{n-m/2-1}\Delta_a^1(f,g) - F(0)G(0)$ *if* $c_{m+2} = \cdots = c_n = 0$, $c_{m+1} \neq 0$, *and* $Tr_2^q(B_m(\bar{c})/c_{m+1}^2) \neq 0$. *This occurs for* $(q^m - q^{m/2})/2$ *values of* τ *for each nonzero* $a \in GF(q)$.

8 Application: GMW Sequences

In this section we apply the previous results to the calculation of the cross-correlation functions of GMW sequences [7, 15]. They exhibit the same autocorrelation statistics as m-sequences, but have greater linear complexity.

Definition 1 *Let q be a power of 2, ℓ and n be positive integers with $\gcd(\ell, q-1) = 1$. Let β be a primitive element of $GF(q^n)$. The sequence $\mathbf{T}$ whose ith element is $Tr_2^q([Tr_q^{q^n}(\beta^i)]^\ell)$ is called a GMW sequence.*

Recently Games [4] calculated the cross-correlation function of the GMW sequence $\mathbf{T}$ and an m-sequence $\mathbf{S}_i = Tr_2^{q^n}(\alpha^i)$ based on the same primitive element $\alpha = \beta$. We will find the cross-correlation function in the case that the primitive elements α and β are linearly or quadratically related, $\beta = \alpha^k$ (where k has q-adic weight 1 or 2). Note that the GMW sequence $\mathbf{T}$ is a special case of a geometric sequence, with feedforward function $g(x) = Tr_2^q(x^\ell)$, and the m-sequence $\mathbf{S}$ is a geometric sequence with feedforward function $f(x) = Tr_2^q(x)$. In order to apply Theorem 2, we will consider the case in which ℓ has dyadic weight 1 or 2. This gives rise to four possibilities:

1. (quadratic-quadratic) $k = q^i + q^j$ and $\ell = 2^s + 2^t$
2. (linear-quadratic) $k = 2^i$ and $\ell = 2^s + 2^t$
3. (quadratic-linear) $k = q^i + q^j$ and $\ell = 2^s$
4. (linear-linear) $k = 2^i$ and $\ell = 2^s$.

Of these possibilities, cases (2), (3), and (4) have already been covered previously: by observing $Tr_q^{q^n}(x^2) = (Tr_q^{q^n}(x))^2$ and $Tr_2^q(x^2) = Tr_2^q(x)$, we see that the GMW sequence $\mathbf{T}$ in case (4) is precisely the m-sequence $\mathbf{S}$, the GMW sequence $\mathbf{T}$ in case (3) is a quadratic decimation of $\mathbf{S}$, and the GMW sequence $\mathbf{T}$ in case (2) is based on the same primitive element as the m-sequence $\mathbf{S}$. For completeness, we will again summarize the results at the end of this section.

We now concentrate on case 1. The imbalances of f and g are 0 since $\gcd(k, q^n - 1) = 1$ and $\gcd(\ell, q-1) = 1$. To simplify the answer, let us assume that $\gcd(n, j-i) = 1$ and $\gcd(n_1, t-s) = 1$ where $q = 2^{n_1}$.

The short correlation $\Delta_a^1(f, g)$ may be calculated by applying Theorem 2 to the short sequences $\mathbf{S}'_i = Tr_2^q(\gamma^i)$ and $\mathbf{T}'_i = Tr_2^q(\gamma^{i\ell})$, where γ is a primitive element of $GF(q)$. We find that

$$\Delta_a^1(f,g) = \begin{cases} 0 & \text{occurring} \quad q/2 - 1 \quad \text{times} \\ \sqrt{2q} & \text{occurring} \quad q/4 + \sqrt{q/8} \quad \text{times} \\ -\sqrt{2q} & \text{occurring} \quad q/4 - \sqrt{q/8} \quad \text{times.} \end{cases}$$

Applying Theorem 2 to $\mathbf{S}$ and $\mathbf{T}$ we obtain the following result.

Theorem 4 (Part 1) *The cross-correlation function of the m-sequence* $\mathbf{S}_i = Tr_2^{q^n}(\alpha^i)$ *with the GMW sequence* $\mathbf{T}_i = Tr_2^q([Tr_q^{q^n}(\beta^i)]^\ell)$ *in case (1) above is three valued, given by*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \begin{cases} -1 & \textit{occurring} \quad q^n/2 - 1 \quad \textit{times} \\ \sqrt{2q^n} - 1 & \textit{occurring} \quad q^n/4 + \sqrt{q^n/8} \quad \textit{times} \\ -\sqrt{2q^n} - 1 & \textit{occurring} \quad q^n/4 - \sqrt{q^n/8} \quad \textit{times.} \end{cases}$$

For case (2) we apply Theorem 2 under the simplifying assumption that $\gcd(n_1, t-s) = 1$ and obtain $\Delta_a^s(f,g) = \Delta_a^1(f,g)$ which was tabulated above. Applying Theorem 1 to $\mathbf{S}$ and $\mathbf{T}$ we obtain the following result.

Theorem 4 (Part 2) *The cross-correlation in case (2) is three-valued,*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \begin{cases} -1 & \textit{occurring} \quad q^n - q/2 - 1 \quad \textit{times} \\ q^{n-1}\sqrt{2q} - 1 & \textit{occurring} \quad q/4 + \sqrt{q/8} \quad \textit{times} \\ -q^{n-1}\sqrt{2q} - 1 & \textit{occurring} \quad q/4 - \sqrt{q/8} \quad \textit{times.} \end{cases}$$

For cases (3) and (4) we find that

$$\Delta_a^1(f,g) = \Delta_a^s(f,g) = \begin{cases} 0 & \text{for } q-2 \text{ nonzero values of } a \in GF(q) \\ q & \text{when } a = 1. \end{cases}$$

Applying Theorems 2 and 1, and assuming that $\gcd(n, j-i) = 1$ we obtain

Theorem 4 (Parts 3 and 4) *The cross-correlation in case (3) is three-valued,*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \begin{cases} -1 & \textit{occurring} \quad q^n - q^{n-1} - 1 \quad \textit{times} \\ \sqrt{q^{n+1}} - 1 & \textit{occurring} \quad \frac{1}{2}(q^{n-1} + \sqrt{q^{n-1}}) \quad \textit{times} \\ -\sqrt{q^{n+1}} - 1 & \textit{occurring} \quad \frac{1}{2}(q^{n-1} - \sqrt{q^{n-1}}) \quad \textit{times} \end{cases}$$

while in case (4) the GMW sequence $\mathbf{T}$ *is a decimation of the m-sequence* $\mathbf{S}$ *and the cross-correlation is*

$$\theta_{\mathbf{S},\mathbf{T}}(\tau) = \begin{cases} -1 & \textit{occurring} \quad q^n - 1 \quad \textit{times} \\ q^n - 1 & \textit{occurring} \quad 1 \quad \textit{time.} \end{cases}$$

Remarks. For any $(q-1)$-periodic pseudorandom sequence $\mathbf{T}$ we may write $\mathbf{T}_i = F(\alpha^i)$ for some (nonlinear) function $F : GF(q) \rightarrow GF(2)$, where α denotes a primitive element of $GF(q)$. Since the cross-correlation function $\theta_{\mathbf{S},\mathbf{T}}(\tau)$ with an m-sequence $\mathbf{S}_i = Tr_2^q(\alpha^i)$ is simply the discrete Fourier transform of $(-1)^F$, Parseval's equality gives the usual lower bounds on the possible values of the cross-correlation [16]:

Proposition 5 *For any $(q-1)$-periodic pseudorandom sequence of bits $\mathbf{T}$, and for any m-sequence $\mathbf{S}$, we have*

$$\sum_{\tau=0}^{q-2} |\theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|^2 = q^2 - I^2$$

where I denotes the imbalance of the sequence T', obtained from T by adding a 0.

We conclude that for balanced sequences, the smallest uniform bound on the cross-correlations occurs when they are all equal, in which case $\theta_{\mathbf{S},\mathbf{T}}(\tau) = \sqrt{q} - 1$ (and F is a bent function [12]).

9 Acknowledgements

We would like to thank an anonymous referee for several useful suggestions that improved this paper.

References

[1] L. Brynielsson, On the linear complexity of combined shift registers, in Proceedings of Eurocrypt (1984) 156-160.

[2] A. H. Chan and R. Games, On the linear span of binary sequences from finite geometries, q odd, IEEE Trans. Inf. Thy. 36 (1990) 548-552.

[3] L. E. Dickson, Linear Groups (Teubner, Leipzig, 1901, reprinted by Dover Publications, N. Y., 1958).

[4] R. Games, Cross-correlation of m-sequences and GMW-sequences with the same primitive polynomial, Discrete Applied Mathematics 12 (1985) 139-146.

[5] R. Games, The Geometry of m-sequences: three-valued cross-correlations and quadrics in finite projective geometry, SIAM J. Alg. Disc. Meth. 7 (1986) 43-52.

[6] S. Golomb, Shift Register Sequences, (Aegean Park Press, Laguna Hills, CA, 1982).

[7] B. Gordon, W. H. Mills, and L. R. Welch, Some new difference sets, Canad. J. Math 14 (1962) 614-625.

[8] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math 16 (1976) 209-232.

[9] V. Kumar and O. Moreno, Prime-phase sequences with periodic correlation properties better than binary sequences, IEEE Trans Inf Thy 36 (1991) 603-616.

[10] R. Lidl and H. Niederreiter, Finite fields, in: Encyclopedia of Mathematics vol. 20 (Cambridge University Press, Cambridge, 1983).

[11] R. McEliece Finite Fields for Computer Scientists and Engineers (Kluwer Academic Publishers, Boston, 1987).

[12] O. Rothaus. On bent functions, Journal of Combinatorial Theory Series A 20 (1976) 300-305.

[13] R. Rueppel, Analysis and Design of Stream Ciphers, (Springer Verlag, N. Y., 1986).

[14] D. Sarwate and M. Pursley. Cross-correlation properties of pseudorandom and related sequences, in: IEEE Proceedings 1968 (1980) 593-619.

[15] M. Simon, J. Omura, R. Scholtz, and B. Levitt, Spread-Spectrum Communications, Vol. 1 (Computer Science Press, 1985).

[16] L. R. Welch, Lower bounds on the maximum correlation of signals, IEEE Trans. Inform. Theory 20 (1974) 397-399.