Cross-Correlations of Quadratic Form Sequences in Odd Characteristic

A. Klapper*

Abstract

Cross-correlation functions are determined for a large class of geometric sequences based on m-sequences in odd characteristic. These sequences are shown to have low cross-correlation values in certain cases. They also have significantly higher linear spans than previously studied geometric sequences. These results show that geometric sequences are candidates for use in spread-spectrum communications systems in which cryptographic security is a factor.

1 Introduction

Pseudorandom sequences with low correlation function values and high linear spans are important in several applications of modern communication systems, such as CDMA systems [13]. A number of constructions have been suggested for generating such sequences. Many of these are based on the idea of mapping an m-sequence or modified m-sequence over a finite field into a prime field by a nonlinear function. Specific examples include GMW sequences [5], bent function sequences [12], No sequences [11], and cascaded GMW sequences [1, 8]. Such constructions have also been studied in a general setting by a number of authors where the resulting sequences are known as *geometric sequences* [2, 6, 7].

A geometric sequence **S** is generated from a q-ary m-sequence **U** by applying a nonlinear "feedforward" function $f : GF(q) \rightarrow GF(r)$, where q is a power of a prime number p and r is a prime number (not necessarily distinct from p), to each element of **S**. Completely general results on the cross-correlations of geometric sequences are quite difficult to obtain (and appear inherently connected to deep problems in algebraic geometry). Several cases, however, have been previously considered, such as pairs of geometric sequences that are obtained from the same q-ary m-sequence but different nonlinear feedforward functions [3] and pairs of geometric sequences for which $p = r = 2$ and whose underlying m-sequences are related by a quadratic decimation [7].

Geometric sequences can be generalized by replacing the underlying m-sequence by a function of an m-sequence. For example, No sequences are a special case in which the underlying m-sequence is replaced by the sum of shifts of two sequences quadratically related to the same m-sequence [11]. The case where $p = r = 2$ and the underlying m-sequence is replaced by the sum of a quadratic decimation of an m-sequence and a shift of the same m-sequence was treated by the author [6]. In that paper the cross-correlations of such a *generalized geometric sequence* with an ordinary geometric sequence were computed. In this paper we compute the same sort of cross-correlations in the case where p is odd. The basic technique used is counting the solutions to pairs of equations over finite fields, one quadratic and one linear. (More general correlation problems can be treated by using more general pairs of equations.)

In Section 2 we recall the definition and basic properties of geometric and quadratic form sequences, state the main theorems (Theorems 2.3, 2.4, and 2.5) on cross-correlations of geometric sequences, and recall related

*Department of Computer Science, 763H Anderson Hall, University of Kentucky, Lexington, KY 40506-0046; e-mail: klapper@cs.uky.edu. Research supported by the National Security Agency under Grant Number MDA904-91-H-0012.

results on cross-correlations in characteristic two. In Section 3 we count solutions to pairs of equations. These counts are used in Section 4 to describe the cross-correlations of quadratic form sequences. In Section 5 we determine the ranks of the quadratic forms that appear in geometric sequences, which, combined with the results of Section 4, give us expressions for the cross-correlations of quadratically decimated geometric sequences and prove Theorems 2.3, 2.4, and 2.5.

2 Definitions and Statements of Results

Let q be a fixed power of an odd prime number p, $q = p^e$, and let $GF(q)$ denote the Galois field with q elements. For any $n \geq 1$, we denote the *trace function* from $GF(q^n)$ to $GF(q)$ by $Tr_q^{q^n}$, defined by $Tr_q^{q^n}(x) = \sum_{j=0}^{n-1} x^{q^j}$. Recall that $Tr_q^{q^n}$ is a $GF(q)$-linear function, that every $GF(q)$-linear function h from $GF(q^n)$ to $GF(q)$ can be written in the form $h(x) = Tr_q^{q^n}(Ax)$ for some $A \in GF(q^n)$, and that, for any $m \geq 1$, $Tr_q^{q^{nm}}(x) = Tr_q^{q^n}(Tr_{q^n}^{q^{nm}}(x))$.

For each finite field of odd characteristic, there is a canonical quadratic character, η on $GF(q)^*$: $\eta(x) = 1$ if x is a square, $\eta(x) = -1$ otherwise. We extend η to all of $GF(q)$ by letting $\eta(0) = 0$. We also use the function ν, defined by $\nu(x) = -1$ if $x \neq 0$, $\nu(0) = -1$.

Let α be a primitive element of $GF(q^n)$. The sequence $\mathbf{V}$ whose jth element is $V_j = Tr_q^{q^n}(\alpha^j)$ is a q-ary m-sequence. It is well known that the sequences of this form are precisely the maximal period sequences that can be generated by linear feedback shift registers of length n with entries and coefficients in $GF(q)$ [4, 9]. In particular, they are easy to generate by hardware. Let $k = 1 + q^i$ (that is, k has q-adic weight two) and let γ be any element of $GF(q^n)$. The sequence $\mathbf{V}'$ whose jth element is $Tr_q^{q^n}(\gamma\alpha^{kj})$ is called a *quadratic decimation* of $\mathbf{V}$. This sequence is never an m-sequence when q is odd, but we may have $\gcd(k, q^n - 1) = 2$, in which case the period is half the maximum possible period. More generally, if $\delta \in GF(q^n)$, we consider the sequence $\mathbf{U}$ whose jth term is $U_j = Tr_q^{q^n}(\gamma\alpha^{kj} + \delta\alpha^j)$.

Let r be a prime number, not necessarily distinct from p. Let ζ be a primitive rth root of unity in the field of complex numbers.

Definition 2.1 *If* $\mathbf{S}$ *and* $\mathbf{T}$ *are periodic sequences of elements of* $GF(r)$*, with period* N*, then the cross-correlation of* $\mathbf{S}$ *and* $\mathbf{T}$ *is defined as*

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{i=1}^{N} \zeta^{S_i - T_{i+\tau}}.$$

Equivalently, if χ is an additive character of $GF(r)$ in the complex numbers, and $\bar{\chi}$ is the complex conjugate of χ, then

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{i=1}^{N} \chi(S_i)\bar{\chi}(T_{i+\tau}).$$

Let f and g be (nonlinear) functions from $GF(q)$ to $GF(r)$ and let $\mathbf{U}$ and $\mathbf{V}$ be as above. The sequence $\mathbf{T}$, whose jth elements is $g(V_j)$, is called a *geometric sequence.* The sequence $\mathbf{S}$, whose jth element is $f(U_j)$, is called a *generalized geometric sequence.*

One reason for interest in these sequences is their large linear spans. The following theorem is an easy generalization of the analogous theorem in characteristic two [6]. If α is a primitive element of $GF(q^n)$, then for any k we denote by $\mu(k)$ the number of distinct elements of the form α^{kq^j}, i.e., the size of the Galois coset of α^k. Note that $\mu(k) = n$ if $\gcd(k, q^n - 1) = 1$.

Theorem 2.2 *Let* $f : GF(q) \to GF(p)$, $f(x) = \sum_{i=0}^{q-1} a_i x^i$*. Let* $k < q^n$ *be a sum of at least two distinct powers of* q*, and let* $\gamma \neq 0$, $\delta \neq 0$ *be elements of* $GF(q^n)$*. Then the sequence whose* i*th term is* $f(Tr_q^{q^n}(\gamma\alpha^{ki} + \delta\alpha^i))$ *has linear span*

$$\lambda_q(\mathbf{S}) = \sum_{a_i \neq 0} (n + \mu(k))^{wt(i)},$$

where $wt(i)$ is the number of nonzero coefficients in the base p expansion of i.

For ordinary geometric sequences, the linear span is $\sum_{a_i\neq 0} n^{wt(i)}$, hence much smaller.

It is the objective of this paper to determine the cross-correlations between the sequences $\mathbf{S}$ and $\mathbf{T}$ in terms of properties of f and g. For any such function f, we let the *imbalance* of f be defined by

$$I(f) = \sum_{u\in GF(q)} \zeta^{f(u)}.$$

Then f is balanced if and only if $I(f) = 0$. Also let $F(u) = \zeta^{f(u)}$, and $G(u) = \zeta^{-g(u)}$.

We let $d = \gcd(i, n)$ and $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \Theta_{\mathbf{S},\mathbf{T}}(\tau) - q^{n-2}I(f)I(g) + F(0)G(0)$. If f or g is balanced, then $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \Theta_{\mathbf{S},\mathbf{T}}(\tau) \pm 1$. To each sequence $\mathbf{S}$ there are associated constants $\rho \in GF(q)$ (described in Section 4) and $\epsilon = \pm 1$ (described in Section 3). The parameters s and t and the summation indices u and v in the main theorems take values in $GF(q)$.

Theorem 2.3 *Let $\mathbf{S}$ be a generalized geometric sequence based on primitive element $\alpha \in GF(q^n)$, with exponent $k = q^i + 1$, and coefficients $\gamma = \alpha^\ell$ and δ. Suppose (1) n is even and n/d is odd, or (2) n/d is even, $n/(2d)$ is odd, and $\ell \not\equiv (q^d+1)/2 \pmod{q^d + 1}$, or (3) $n/(2d)$ is even and $\ell \not\equiv 0 \pmod{q^d + 1}$. Then $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ takes the values*

1. $\epsilon q^{n/2-1}(qF(-\rho) - I(f))G(t)$.
2. $\epsilon q^{n/2-1}\sum_{u,v}\eta(v^2 - su)F(u - \rho)G(v - t)$.

The numbers of occurences of these values are given by the table in Theorem 4.2.A, with M replaced by δ, and m replaced by n.

Theorem 2.4 *Let $\mathbf{S}$ be a generalized geometric sequence based on primitive element $\alpha \in GF(q^n)$, with exponent $k = q^i + 1$, and coefficient $\gamma = \alpha^\ell$. Suppose (1) n/d is even, $n/(2d)$ is odd, and $\ell \equiv (q^d + 1)/2 \pmod{q^d + 1}$, or (2) $n/(2d)$ is even and $\ell \equiv 0 \pmod{q^d + 1}$.*

A. If $\gamma^{q^i-1}w^{q^{2i}-1} = -1$ implies that $Tr_q^{q^n}(\delta w) = 0$, then $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ takes the values

1. $\epsilon q^{n/2+d-1}(qF(-\rho) - I(f))G(t)$.
2. $\epsilon q^{n/2+d-1}\sum_{u,v}\eta(v^2 - su)F(u - \rho)G(v - t)$.
3. $\epsilon q^{n/2+d-2}(qF(-\rho) - I(f))I(g)$.

The numbers of occurences of these values are given by the table in Theorem 4.2.A, with M replaced by δ, and m replaced by $n - 2d$.

B. If $\gamma^{q^i-1}w^{q^{2i}-1} = -1$ does not imply that $Tr_q^{q^n}(\delta w) = 0$, then $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ takes the values

1. $\epsilon q^{n/2+d-1}(q\sum_v F(sv - t)G(v) - I(f)I(g))$.
2. 0.

The numbers of occurences of these values are given by the table in Theorem 4.2.B, with M replaced by δ, and m replaced by $n - 2d$.

Theorem 2.5 *Let n be odd. Then $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ takes the values*

1. $\epsilon q^{(n-1)/2}\sum_u \eta(u)F(u - \rho)G(t)$.
2. $\epsilon\eta(s)q^{(n-3)/2}(q\sum_v F(v^2/s - \rho)G(v - t) - I(f)I(g))$.

The numbers of occurences of these values are given by the table in Theorem 4.3.A, with M replaced by δ, and m replaced by n.

Observe that, if we consider $GF(q^n)$ to be an n-dimensional vector space over $GF(q)$, then the function $Tr_q^{q^n}(x^k)$ is a quadratic form in n variables over $GF(q)$. Thus it is logical to consider more general sequences of the form $S_i = f(Q(\alpha^i))$, where Q is an arbitrary quadratic form in n variables over $GF(q)$. We call such sequences *quadratic form* sequences. As a first step, we express the cross-correlations of such sequences with $\mathbf{T}$ in terms of f, g, and properties of the quadratic form Q.

3 Algebraic Tools

In this section we state several results from number theory and the theory of quadratic forms that will be useful in the sequel. The is referred to [9, 10] for the proofs.

We are repeatedly concerned with the divisibility of integers that differ by 1 from powers of odd primes. Suppose b is an odd integer. Let n and i, be non-negative integers, with $n \neq 0$, and let $d = \gcd(n, i)$. Then $\gcd(b^n - 1, b^i - 1) = b^d - 1$; $\gcd(b^n - 1, b^i + 1) = 1 + b^d$ if n/d is even; $\gcd(b^n - 1, b^i + 1) = 2$ otherwise; $\gcd(b^n + 1, b^i + 1) = 1 + b^d$ if n/d; i/d are odd; and $\gcd(b^n + 1, b^i + 1) = 2$ otherwise.

We fix an odd prime p, a power q of p, and a positive integer n. Let $\bar{x}$ denote $(x_1, \ldots, x_n)$ and $B_m(\bar{x}) = x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m$. Under a change of coordinates, $B_m(\bar{x})$ is equivalent to the diagonal form $x_1^2 - x_2^2 + x_3^2 - x_4^2 + - \cdots + x_{m-1}^2 - x_m^2$. Every quadratic form Q can be expressed in terms of some symmetric matrix M as $Q(x_1, \cdots, x_n) = \bar{x}M\bar{x}^t$. The rank of Q is the rank of M. If M (and hence Q) is nonsingular, the determinant of Q, $\det(Q)$, is defined to be the determinant of M. The notion of determinant extends to singular quadratic forms by letting $\det(Q)$ be the determinant of the restriction of Q to a subspace of dimension $\text{rank}(Q)$ on which Q is nonsingular. We can write any quadratic form in one of three standard forms.

Proposition 3.1 *For any quadratic form Q in n variables, if $m = \text{rank}(Q)$, then Q is equivalent under a change of coordinates to precisely one of the following quadratic forms:*

Type I: $B_m(\bar{x})$,
Type II: $B_{m-1}(\bar{x}) + bx_m^2$,
Type III: $B_{m-2}(\bar{x}) + x_{m-1}^2 - ax_m^2$,

where $b \in \{1, a\}$ and a is a fixed nonsquare in $GF(q)$. In the first case, $\det(Q) = (-1)^{m/2}$. In the second case, $\det(Q) = b(-1)^{(m-1)/2}$. In the third case $\det(Q) = a(-1)^{m/2}$. Furthermore, the number of solutions to the equation $Q(\bar{x}) = u$ is $q^{n-1} + \nu(u)\eta((-1)^{m/2}\det(Q))q^{n-m/2-1}$ for a type I or type III quadratic form, and $q^{n-1} + \eta((-1)^{(m-1)/2}u\det(Q))q^{n-(m+1)/2} = q^{n-1} + \eta(ub)q^{n-(m+1)/2}$ for a type II quadratic form.

Any choice of coordinates $e_1, e_2, \ldots, e_n$ for $GF(q^n)$ as a vector space over $GF(q)$ determines an identification $GF(q)^n \to GF(q^n)$ by $\bar{x} = (x_1, x_2, \ldots, x_n) \mapsto \sum_i x_ie_i = x$. We write $\bar{x}$ when an element is to be thought of as a vector in $GF(q)^n$, and we write x when the same vector is to be thought of as an element of $GF(q^n)$ (for a fixed a set of coordinates for $GF(q^n)$).

Consider a system of equations consisting of a quadratic form and linear function. The number of solutions depends on the type and rank of the quadratic form. Let $Q(\overline{x})$ be a quadratic form of rank m in n variables in one of the three standard types, let $M(\overline{x}) = \sum_{i=1}^n a_ix_i = \overline{a} \cdot \overline{x}$, $L(\overline{x}) = \sum_{i=1}^n b_ix_i = \overline{b} \cdot \overline{x}$, and $R(\overline{x}) = Q(\overline{x}) + M(\overline{x})$, with $\{a_i, b_i\} \subseteq GF(q)$. Let $u, v \in GF(q)$. We denote by $N(u, v)$ the number of solutions to the system of equations

$$R(\overline{x}) = u \quad (1)$$
$$L(\overline{x}) = v. \quad (2)$$

We use the following notation.

1. Let $\epsilon = \eta((-1)^{(m-1)/2}\det(Q))$ if m is odd, and $\epsilon = \eta((-1)^{m/2}\det(Q))$ if m is even. So $N_u^Q = q^{n-1} + \epsilon\eta(u)q^{n-(m+1)/2}$ if m is odd, and $N_u^Q = q^{n-1} + \epsilon\nu(u)q^{n-m/2}$ if m is even.

2. $$\hat{Q}(\overline{x}) = \begin{cases} Q(\overline{x}) & \text{if } Q(\overline{x}) = B_m(\overline{x}) \\ B_{m-1}(\overline{x}) + \dfrac{x_m^2}{4b} & \text{if } Q(\overline{x}) = B_{m-1}(\overline{x}) + bx_m^2 \\ B_{m-2}(\overline{x}) + \dfrac{x_{m-1}^2}{4} - \dfrac{x_m^2}{4a} & \text{if } Q(\overline{x}) = B_{m-2}(\overline{x}) + x_{m-1}^2 - ax_m^2. \end{cases}$$

   Note that $\hat{Q}$ is equivalent to Q under a change of coordinates.

3. The bilinear form associated with $Q(\overline{x})$ is $D_m(\overline{x}, \overline{y}) = Q(\overline{x} + \overline{y}) - Q(\overline{x}) - Q(\overline{x})$. We also let $\hat{D}(\overline{x}, \overline{y}) = \hat{Q}(\overline{x} + \overline{y}) - \hat{Q}(\overline{x}) - \hat{Q}(\overline{y})$.

4. If $\overline{x} = (x_1, \cdots, x_n)$ is any vector, then $\overline{x}' = (x_1, \cdots, x_m)$ and $\overline{x}'' = (x_{m+1}, \cdots, x_n)$. Thus $Q(\overline{x}) = Q(\overline{x}')$.

The following three propositions, covering all possibilities for Q, M, and L, are proved by a series of changes of coordinates. We omit the details. For similar analyses, see [9] and [6].

Proposition 3.2 *Suppose that $\overline{b}'' = 0$ and $\overline{a}'' \neq 0$, or that $\overline{b}''$ and $\overline{a}''$ are linearly independent. Then $N(u, v) = q^{n-2}$.*

Proposition 3.3 *Suppose that $\overline{b}'' \neq 0$ and $\overline{a}'' = \lambda\overline{b}''$ for some $\lambda \in GF(q)$.*

1. *If Q has Type I or Type III, then*

   $$N(u, v) = q^{n-2} + \epsilon\nu(u - \lambda v + \hat{Q}(\overline{a}' - \lambda\overline{b}'))q^{n-m/2-2}.$$

2. *If Q has Type II, then*

   $$N(u, v) = q^{n-2} + \epsilon\eta(u - \lambda v + \hat{Q}(\overline{a}' - \lambda\overline{b}'))q^{n-(m+3)/2}.$$

Proposition 3.4 *Let $\overline{a}'' = \overline{b}'' = 0$.*

1. *Suppose Q has type I or type III.*

   (a) *If $\hat{Q}(\overline{b}) = 0$, then*

   $$N(u, v) = \begin{cases} q^{n-2} + \epsilon\nu(u + \hat{Q}(\overline{a}))q^{n-1-m/2} & \textit{if } v = -\hat{D}_n(\overline{a}, \overline{b}) \\ q^{n-2} & \textit{otherwise.} \end{cases}$$

   (b) *If $\hat{Q}(\overline{b}) \neq 0$, then*

   $$N(u, v) = q^{n-2} + \epsilon\eta(4\hat{Q}(\overline{b})(u + \hat{Q}(\overline{a})) - (v + \hat{D}_n(\overline{a}, \overline{b}))^2)q^{n-1-m/2}.$$

2. *Suppose Q has type II.*

   (a) *If $\hat{Q}(\overline{b}) = 0$, then*

   $$N(u, v) = \begin{cases} q^{n-2} + \epsilon\eta(u + \hat{Q}(\overline{a}))q^{n-(m+1)/2} & \textit{if } v = -\hat{D}_n(\overline{a}, \overline{b}) \\ q^{n-2} & \textit{otherwise.} \end{cases}$$

   (b) *If $\hat{Q}(\overline{b}) \neq 0$, then*

   $$N(u, v) = q^{n-2} + \epsilon\nu(4\hat{Q}(\overline{b})(u + \hat{Q}(\overline{a})) - (v + \hat{D}_n(\overline{a}, \overline{b}))^2)\eta(\hat{Q}(\overline{b}))q^{n-(m+3)/2}.$$

4 Cross-Correlations of Quadratic Form Sequences

Let $R(x)$ be the sum of a quadratic form Q and a linear function M on $GF(q^n)$ over $GF(q)$. Let $f, g : GF(q) \to GF(r)$. Let $\mathbf{S}$ be the quadratic form sequence whose jth term is $S_j = f(R(\alpha^j))$ and let $\mathbf{T}$ be the sequence whose jth term is $T_j = g(Tr_q^{q^n}(\alpha^j))$.

Proposition 4.1 *Let $N(u,v) = \{x : R(x) = u$ and $Tr_q^{q^n}(\alpha^\tau x) = v\}$. Then*

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{u,v \in GF(q)} N(u,v)F(u)G(v) - F(0)G(0).$$

Proof: As i ranges from 1 to $q^n - 1$, α^i ranges through all nonzero elements of $GF(q^n)$, since α is primitive. Hence

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{x \in GF(q^n)} F(R(x))G(Tr_q^{q^n}(\alpha^\tau x)) - F(0)G(0). \tag{3}$$

Suppose that elements x, y of $GF(q^n)$ satisfy $Tr_q^{q^n}(\alpha^\tau x) = Tr_q^{q^n}(\alpha^\tau y)$ and $R(x) = R(y)$. Then x and y contribute the same value to the sum in equation (3). Gathering all such terms together we get the expression for $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$ in the statement of the proposition. □

We have reduced the problem of computing cross-correlations of geometric sequences to that of finding solutions to pairs of equations. A similar reduction works if $Q(x)$ and $Tr_q^{q^n}(x)$ are replaced by arbitrary functions from $GF(q^n)$ to $GF(q)$. Note that $N(u,v)$ can be interpreted geometrically as the number of points in the intersection of a quadric hypersurface and a hyperplane.

We can combine the results of Section 3 with Proposition 4.1 to give a complete description of the cross-correlations of $\mathbf{S}$ and $\mathbf{T}$. Throughout we let m be the rank of Q and $\rho = \hat{Q}(\overline{a})$ where $\hat{Q}$ and $\overline{a}$ are as in Section 3 (with respect to coordinates for which Q is in a standard form). To simplify statements, we let

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

We denote by $Ker(M) = \{x : M(x) = 0\}$ the kernel of the linear transformation M, and by $Null(Q) = \{x : \forall y : Q(x+y) = Q(y)\}$ the null space of Q. These are $GF(q)$ vector spaces. The dimension of $Null(Q)$ is $n - \text{rank}(Q)$, and $Null(Q)$ is complementary to the largest subspace on which Q is nonsingular.

The proofs of the values of $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ are a matter of summing over u and v, with appropriate instances of Proposition 3.2, 3.3, or 3.4. There is a one-to-one correspondence between shifts τ and nonzero values of $\overline{b}$. Thus the number of occurrences of each value is found by counting the number of nonzero values of $\overline{b}$ that give the hypotheses of the appropriate proposition. In some cases this in turn leads to an application of Proposition 3.2, 3.3, or 3.4. The details are omitted.

Theorem 4.2 *Let m be even.*

A. If $Null(Q) \subseteq Ker(M)$, then $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ takes the values

1. $\epsilon q^{n-1-m/2}(qF(-\rho) - I(f))G(t)$.
2. $\epsilon q^{n-1-m/2} \sum_{u,v} \eta(su - v^2)F(u-\rho)G(v-t)$.
3. $\epsilon q^{n-2-m/2}(qF(-\rho) - I(f))I(g)$.

Conditions on M, Q	*Case*	*Parameters*	*Number of Occurrences*
$M = 0$	*1*	$t = 0$	$q^{m-1} + \epsilon(q-1)q^{m/2-1} - 1$
	2	$s \neq 0$, $t = 0$	$q^{m-1} - \epsilon q^{m/2-1}$
	3	–	$q^n - q^m$
$M \neq 0$, $\rho = 0$	*1*	$t = 0$	$q^{m-2} + \epsilon(q-1)q^{m/2-1} - 1$
	1	$t \neq 0$	q^{m-2}
	2	$s, t \neq 0$	q^{m-2}
	2	$s \neq 0$, $t = 0$	$q^{m-2} - \epsilon q^{m/2-1}$
	3	–	$q^n - q^m$
$\rho \neq 0$	*1*	$t = 0$	$q^{m-2} - 1$
	1	$t \neq 0$	$q^{m-2} + \epsilon q^{m/2-1}$
	2	$s \neq 0$	$q^{m-2} + \epsilon\eta(4\rho s - t^2)q^{m/2-1}$
	3	–	$q^n - q^m$

B. If $Null(Q) \not\subseteq Ker(M)$, *then* $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ *takes the values*

1. $\epsilon q^{n-1-m/2}(q\sum_v F(sv-t)G(v) - I(f)I(g))$.
2. 0.

Case	*Parameters*	*Number of Occurrences*
1	$s \neq 0$	$q^{m-1} + \epsilon\nu(t)q^{m/2-1}$
2	–	$q^n - q^{m+1} + q^m - 1$

Theorem 4.3 *Let* m *be odd.*

A. If $Null(Q) \subseteq Ker(M)$, *then* $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ *takes the values*

1. $\epsilon q^{n-(m+1)/2}\sum_u \eta(u)F(u-\rho)G(t)$.
2. $\epsilon\eta(s)q^{n-(m+3)/2}(q\sum_v F(v^2/s-\rho)G(v-t) - I(f)I(g))$.
3. $q^{n-(m+3)/2}\sum_u \eta(u)F(u-\rho)I(g)$.

Conditions on M, Q	*Case*	*Parameters*	*Number of Occurrences*
$M = 0$	*1*	$t = 0$	$q^{m-1} - 1$
	2	$s \neq 0$, $t = 0$	$q^{m-1} + \epsilon q^{(m-1)/2}$
	3	–	$q^n - q^m$
$M \neq 0$, $\rho = 0$	*1*	$t = 0$	$q^{m-2} - 1$
	1	$t \neq 0$	q^{m-2}
	2	$s, t \neq 0$	q^{m-2}
	2	$s \neq 0$, $t = 0$	$q^{m-2} + \epsilon\eta(s)q^{(m-1)/2}$
	3	–	$q^n - q^m$
$\rho \neq 0$	*1*	$t = 0$	$q^{m-2} + \epsilon(q-1)q^{(m-3)/2}$
	1	$t \neq 0$	$q^{m-2} + \epsilon q^{(m-3)/2}$
	2	$s \neq 0$	$q^{m-2} + \epsilon\nu(4\rho s - t^2)\eta(\rho)q^{(m-3)/2}$
	3	–	$q^n - q^m$

B. If $Null(Q) \not\subseteq Ker(M)$, *then* $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ *takes the values*

1. $\epsilon q^{n-(m+3)/2}\sum_{u,v} \eta(u+sv+t)F(u)G(v)$.
2. 0.

Case	*Parameters*	*Number of Occurrences*
1	$s \neq 0$	$q^{m-1} + \epsilon\eta(t)q^{(m-1)/2}$
2	–	$q^n - q^{m+1} + q^m - 1$

It is interesting to determine the minimal cross-correlations achievable in the preceding two theorems. The dominant term in $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$ is $q^{n-2}I(f)I(g)$. Sequences have small cross-correlations only if the feedforward functions are balanced. This is only possible if $r = p$, that is, the range of f and g is $GF(p)$. We assume this. The remaining terms are minimized by making the rank m as large as possible. That is, by making $m = n$. In the next section we see cases where this occurs.

Theorem 4.4 *Suppose f and g are balanced, and $m = n$. In Theorem 4.2.A: in case 1, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = q^{n/2}$; in case 2, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = |q^{n/2-1}\sum_{u,v}\eta(v^2 - su)F(u-\rho)G(v-t)| \leq q^{n/2+1}$; in case 3, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = 0$.*

In Theorem 4.2.B: in case 1, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = |q^{n/2}\sum_{v} F(sv - t)G(v)| \leq q^{n/2+1}$; in case 2, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = 0$.

In Theorem 4.3.A: in case 1, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = |q^{(n-1)/2}\sum_{u}\eta(u)F(u-\rho)| \leq q^{(n+1)/2}$; in case 2, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = |q^{(n-1)/2}\sum_{v} F(v^2/s - \rho)G(v-t)| \leq q^{(n+1)/2}$; in case 3, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = 0$.

In Theorem 4.3.B: in case 1, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = |q^{(n-3)/2}\sum_{u,v}\eta(u + sv + t)F(u)G(v)| \leq q^{(n+1)/2}$; in case 2, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + F(0)G(0)| = 0$.

In all cases the cross-correlations are close to the square root of the period with no additional restrictions on f and g. With additional restrictions, these values can be made smaller. Taking f to be as balanced as possible on $\{u - \rho : u \text{ is a square }\}$, the bound in case A.1 of Theorem 4.3 can be made less than $(p-1)q^{(n-1)/2}$. Also, the sums in case A.2 of Theorem 4.3 are essentially cross-correlations. If we choose f and g so these cross-correlations are small, then we can further bound $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$. Similar considerations apply in other cases.

5 Cross-Correlations of Geometric Sequences

We apply the results of Section 4 to the case of generalized geometric sequences. Specifically, we let $Q(x) = Tr_q^{q^n}(\gamma x^{1+q^i})$. For purposes of implementation, we can represent $M(x)$ and $L(x)$ by $Tr_q^{q^n}(\delta x)$ and $Tr_q^{q^n}(\beta x)$, respectively. Thus we are considering the cross-correlations between the sequence $\mathbf{S}$ whose jth term is $f(Tr_q^{q^n}(\gamma\alpha^{j(1+q^i)} + \delta\alpha^j))$ and the sequence $\mathbf{T}$ whose jth term is $g(Tr_q^{q^n}(\beta\alpha^j))$, for some primitive element α of $GF(q^n)$. We can assume $\beta = 1$, since the various nonzero values of B correspond to different shifts τ.

Proposition 5.1 *The function $Q(x) = Tr_q^{q^n}(x^{1+q^i})$ is a quadratic form on $GF(q^n)$ over $GF(q)$.*

The proof is a matter of choosing coordinates to represent x and expanding x^{1+q^i} with respect to the coordinates. Thus in order to determine the specific values of the cross-correlations of $\mathbf{S}$ and $\mathbf{T}$, it suffices to determine $\text{rank}(Q)$ and $\eta(\det(Q))$. Of these, the rank is the most important since, as we have seen, the determinant of Q only affects the sign of $\Gamma_{\mathbf{S},\mathbf{T}}$.

Theorem 5.2 *Let $\gamma = \alpha^\ell$ and $d = \gcd(n, i)$. The rank of $Q(x) = Tr_q^{q^n}(\gamma x^{1+q^i})$ is*

1. *n if n/d is odd;*
2. *$n - 2d$ if n/d is even, $n/2d$ is odd, and $\ell \equiv (q^d + 1)/2 \pmod{q^d + 1}$;*
3. *n if n/d is even, $n/2d$ is odd and $\ell \not\equiv (q^d + 1)/2 \pmod{q^d + 1}$;*
4. *$n - 2d$ if $n/2d$ is even and $\ell \equiv 0 \pmod{q^d + 1}$;*
5. *n if $n/2d$ is even and $\ell \not\equiv 0 \pmod{q^d + 1}$.*

Proof: Consider the null space, W, of Q, defined by

$$\begin{aligned} W &= \{w \in GF(q^n) : Q(w) = 0 \text{ and } \forall y \in GF(q^n) : Q(w+y) = Q(y)\} \\ &= \{w \in GF(q^n) : \forall y \in GF(q^n)^* : Q(w+y) = Q(y)\}. \end{aligned}$$

The set W is a $GF(q)$-vector subspace in $GF(q^n)$, and the dimension of W is the co-rank of Q. We compute the dimension of W.

Let $w \in GF(q^n)^*$. Expanding the expression $(w+y)^{1+q^i}$, we see that $w \in W$ if and only if for every $y \in GF(q^n)$,

$$Tr_q^{q^n}(\gamma w y^{q^i}) = -Tr_q^{q^n}(\gamma w^{q^i} y). \tag{4}$$

Since $Tr_q^{q^n}(x) = Tr_q^{q^n}(x^q)$, the right hand side of equation (4) is unchanged if we raise its argument to the power q^i, which gives

$$Tr_q^{q^n}(w y^{q^i}) = -Tr_q^{q^n}(\gamma^{q^i} w^{q^{2i}} y^{q^i}).$$

for all $y \in GF(q^n)$. This implies that $\gamma w = -\gamma^{q^i} w^{q^{2i}}$, or, if $w \neq 0$, that $\gamma^{q^i - 1} w^{q^{2i}-1} = -1$.

Let $z = \gamma w^{q^i+1}$. Then $w \in W$ if and only if $z^{q^i-1} = -1$. On the other hand, $z \in GF(q^n)$, so $z^{q^n-1} = 1$. It follows that

$$z^{\gcd(q^n-1, 2(q^i-1))} = 1.$$

The remainder of the computation of the rank of W breaks into two cases.
1. n/d **is odd:** In this case $\gcd(q^n-1, 2(q^i-1)) = q^d - 1$, so $z^{q^d-1} = 1$. This implies $z^{q^i-1} = 1$, a contradiction. Thus $W = \{0\}$ and the rank is n.
2. n/d **is even:** In this case $\gcd(q^n-1, 2(q^i-1)) = 2(q^d-1)$, and $\gcd(q^n-1, q^{2i}-1) = q^{2d}-1$. Suppose v is a second element of W. Then $(v/w)^{q^{2i}-1} = 1$, so $(v/w)^{q^{2d}-1} = 1$. That is, $v/w \in GF(q^{2d})$. Conversely, if $a \in GF(q^{2d})$, then $aw \in W$. Thus either $|W| = q^{2d}$ and the rank is $n - 2d$, or $|W| = 1$ and the rank is n.

It thus suffices to determine when there is at least one nonzero element of W. We have $z^{2(q^d-1)} = 1$ and $z^{q^d-1} = -1 = \alpha^{(q^n-1)/2}$. Then

$$\begin{aligned} \exists w : \left(\alpha^\ell w^{1+q^i}\right)^{q^d-1} &= \alpha^{(q^n-1)/2} && \text{if and only if} \\ \exists w : \alpha^\ell w^{1+q^i} &= \alpha^{(q^n-1)/(2(q^d-1))} && \text{if and only if} \\ \exists w : w^{1+q^i} &= \alpha^{(q^n-1)/(2(q^d-1))-\ell} && \text{if and only if} \\ \exists r : \alpha^{r(1+q^i)} &= \alpha^{(q^n-1)/(2(q^d-1))-\ell} && \text{if and only if} \\ \exists r,s : r(1+q^i) &= \frac{q^n-1}{2(q^d-1)} - \ell + s(q^n-1) && \text{if and only if} \\ \ell &\equiv \frac{q^n-1}{2(q^d-1)} \pmod{q^d+1}, \end{aligned}$$

since $\gcd(q^i+1, q^n-1) = q^d+1$ in this case.

Furthermore, if $n/(2d)$ is even, then q^d+1 divides $(q^n-1)/(2(q^d-1))$. Thus W is nontrivial if and only if $\ell \equiv 0 \pmod{q^d+1}$. On the other hand, if $n/(2d)$ is odd, then $(q^n-1)/(2(q^d-1)) \equiv (q^d+1)/2 \pmod{q^d+1}$, so W is nontrivial if and only if $\ell \equiv (q^d+1)/2 \pmod{q^d+1}$. □

In case n/d is even, we can further determine the type of Q.

Theorem 5.3 *Suppose n/d is even. Then*

1. *If $n/(2d)$ is even and $\ell \equiv 0 \pmod{q^d+1}$, then Q has type III.*

2. *If $n/(2d)$ is even and $\ell \not\equiv 0 \pmod{q^d+1}$, then Q has type I.*

3. *If $n/(2d)$ is odd and $\ell \equiv (q^d+1)/2 \pmod{q^d+1}$, then Q has type I.*

4. *If $n/(2d)$ is odd and $\ell \not\equiv (q^d+1)/2 \pmod{q^d+1}$, then Q has type III.*

Proof: The number of nonzero roots Z of Q is given by

$$N_0^Q = q^{n-1} + (q-1)\eta((-1)^{m/2}\Delta)q^{n-m/2-1} - 1 = q^{n-1} + (q-1)\epsilon q^{n-m/2-1} - 1,$$

where m is the rank of Q and Δ is the determinant of Q. The group $G = \{c : c^{1+q^i} \in GF(q)\} = \{c : c^{(q-1)(1+q^i)} = 1\}$ acts faithfully on Z. Therefore N_0^Q is divisible by $|G|$. If n/d is even, then $|G| = (q-1)(q^d+1)$, which must divide $q^{n-1} + (q-1)\epsilon q^{n-m/2-1} - 1$. In other words

$$q^d + 1 \left| \frac{q^{n-1}-1}{q-1} + \epsilon q^{n-m/2-1} \right. .$$

Suppose $n/(2d)$ is even. Then q^d+1 divides $(q^n-1)/(q-1)$, so it also divides $q^{n-1} + \epsilon q^{n-m/2-1}$, and so also divides $q^{m/2} + \epsilon$. When $m = n$, this implies $\epsilon = 1$, whereas when $m = n-2d$, this implies $\epsilon = -1$.

Suppose $n/(2d)$ is odd. Then q^d+1 does not divide $(q^n-1)/(q-1)$, so it does not divide $q^{n-1} + \epsilon q^{n-m/2-1}$, nor does it divide $q^{m/2} + \epsilon$. When $m = n$, this implies $\epsilon = -1$, whereas when $m = n-2d$, this implies $\epsilon = 1$.
□

6 Example: Generalized GMW Sequences

Let $c = 1 + p^\ell$ and consider the feedforward functions $f(x) = Tr_p^q(x^{c/2})$ and $g(x) = Tr_p^q(x^c)$, with $\gcd(c/2, q-1) = 1$. Then $\mathbf{S}$ is the sequence whose jth term is

$$S_j = Tr_p^q((Tr_q^{q^n}(\gamma\alpha^{j(1+q^i)} + \delta\alpha^j))^{c/2}),$$

while $\mathbf{T}$ is the sequence whose jth term is

$$S_j = Tr_p^q((Tr_q^{q^n}(\alpha^j))^c).$$

Assume further that $\delta \neq 0$ is chosen so that $\rho = 0$, and that n is odd. Let $q = p^e$.

The feedforward function f is balanced, so, as shown in the comments following Theorem 4.3, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau)+1|$ is bounded by the maximum of

1. $|q^{(n-1)/2}\sum_u \eta(u)F(u)| \leq q^{(n+1)/2}$ and
2. $|q^{(n-1)/2}\sum_v F(v^2/s)G(v-t)| \leq q^{(n+1)/2}$.

Since $\gcd(c/2, q-1) = 1$, we have that $x^{c/2}$ is a square if and only if x is a square. Hence

$$\begin{aligned} \sum_u \eta(u)F(u) &= \sum_u \eta(u)\zeta^{Tr_p^q(u)} && (5) \\ &= 2\Big(\sum_{\substack{u\neq 0 \\ \text{a square}}} \zeta^{Tr_p^q(u)}\Big) + 1 && (6) \\ &= \sum_u \zeta^{Tr_p^q(u^2)}. && (7) \end{aligned}$$

We have $2 = 1 + p^0$, $\gcd(e, 0) = e$, and $e/e = 1$, odd, so the rank of the $GF(p)$ quadratic form $Tr_p^q(u^2)$ is e. Using Proposition 3.1, we see that the absolute value of the sum in equation (7) is $p^{e/2}$ if e is even. If e is odd, we have

$$\sum_{u\in GF(q)} \zeta^{Tr_p^q(u^2)} = p^{(e-1)/2} \sum_{v\in GF(p)} \zeta^{v^2} = p^{(e-1)/2}p^{1/2} = p^{e/2}.$$

Thus for any e, the bound for this case is $q^{n/2}$.

In the second case, for $s' = s^{-c/2}$,

$$\begin{aligned}\sum_v F(v^2/s)G(v-t) &= \sum_v \zeta^{Tr_p^q(s'v^{1+p^\ell})-Tr_p^q((v-t)^{1+p^\ell})} &(8)\\ &= \sum_v \zeta^{Tr_p^q((s'-1)v^{1+p^\ell}+(t^{p^\ell}+t^{p^{e-\ell}})v-t^{1+p^\ell})}. &(9)\end{aligned}$$

This is just the imbalance of a $GF(p)$ quadratic form on $GF(q)$ if $s \neq 1$, or, of a linear function if $s = 1$. If $s \neq 1$, the rank is e for all s' if $e/\gcd(e,\ell)$ is odd. Again using Proposition 3.1, we see that the absolute value of the sum in equation (9) is $p^{e/2}$. Thus the bound for this case is $q^{n/2}$. If $s = 1$, the function $(t^{p^\ell}+t^{p^{e-\ell}})v-t^{1+p^\ell}$ is balanced unless $t^{p^{2\ell}} + t = 0$. It can be shown that when $e/\gcd(e,\ell)$ is odd, this is only possible if $t = 0$. Thus the bound is zero if $s = 1$ and $t \neq 0$, and is $q^{(n+1)/2}$ for the $q^{n-2} + \epsilon q^{(n-1)/2}$ shifts that correspond to $s = 1$, $t = 0$ when n is odd. In summary, we have the following.

Proposition 6.1 *Suppose $f(x) = Tr_p^q(x^{c/2})$ and $g(x) = Tr_p^q(x^c)$ with $c = 1+p^\ell$, $e/\gcd(e,\ell)$ odd, and n odd. Then $|\Theta_{\mathbf{S},\mathbf{T}}(\tau)+1|$ is $q^{(n+1)/2}$ for $q^{n-2} + \epsilon q^{(n-1)/2}$ values of τ. For the remaining shifts, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau)+1|$ is bounded by $q^{n/2}$.*

On the other hand, if we let $e/\gcd(e,\ell)$ be even, and take $g(x) = Tr_p^q(\sigma x^c - \pi x)$, then the sum in case two is

$$\sum_v F(v^2/s)G(v-t) = \sum_v \zeta^{Tr_p^q((s'-\sigma)v^{1+p^\ell}+(\sigma t^{p^\ell}+(\sigma t)^{p^{e-\ell}}-\pi)v+(\pi-t^{1+p^\ell}))}.$$

By observing that we can choose σ so the $GF(p)$-linear transformation on $GF(q)$ taking t to $\sigma t^{p^\ell} + (\sigma t)^{p^{e-\ell}}$ is singular, we see that π can be chosen so that when $s' = 1$, the resulting linear function is not identically zero for any fixed t. We lose a little – the quadratic form now has rank $e - 2\gcd(e,\ell)$ for $(p^e-1)/(p^{\gcd(e,\ell)}+1)$ values of s. This rank is maximized at $e-2$ by taking e even and $\gcd(e,\ell) = 1$. Similar considerations as above lead to the following.

Proposition 6.2 *Suppose $f(x) = Tr_p^q(x^{c/2})$ and $g(x) = Tr_p^q(\sigma x^c - \pi x)$ with $c = 1+p^\ell$, e even, $\gcd(e,\ell) = 1$, n odd, and σ and π chosen so $\sigma t^{p^\ell} + (\sigma t)^{p^{e-\ell}} - \pi$ is never zero. Then $|\Theta_{\mathbf{S},\mathbf{T}}(\tau)+1|$ is at most $pq^{n/2}$.*

7 Example: Cascaded GMW Sequences

The idea of iterating the type of function used as a feedforward function for GMW sequences has been studied by several authors [1, 8] in the case where the characteristic of the underlying fields is two. The sequences that arise tend to have very large linear spans (due to all the exponentiation) and sometimes have computable, and small, cross-correlations. In this section we use our results on cross-correlations of geometric sequences recursively to compute the cross-correlations of certain cascaded GMW sequences in odd characteristic. We first recall the definitions. Cascaded GMW sequences can be defined for more general exponents, but the conditions we impose are necessary to be able to apply the results of this paper.

Let p be an odd prime, let $n_1, \cdots, n_t$ be odd positive integers, and define inductively: $q_1 = p$, and $q_{j+1} = q_j^{n_j}$. Thus we have a tower of Galois fields

$$GF(q_1) \subseteq GF(q_2) \subseteq \cdots \subseteq GF(q_t) \subseteq GF(q_{t+1}).$$

Let $\ell_1, \cdots, \ell_t$ and $i_1, \cdots, i_t$ be positive integers satisfying

$$\gcd\left(\ell_j \frac{q_j^{i_j}+1}{2}, q_{j+1}-1\right) = 1 \quad \text{for } j = 1, \cdots, t.$$

We define functions $h_j(u)$ and $h'_j(u)$ from $GF(q_j)$ to $GF(p)$ inductively as follows. Let $h_1(u) = h'_1(u) = u$, and

$$\begin{aligned} h_{j+1}(u) &= h_j(Tr_{q_j}^{q_{j+1}}(u^{\ell_j(q_j^{i_j}+1)/2})) \\ h'_{j+1}(u) &= h'_j(Tr_{q_j}^{q_{j+1}}(u^{\ell_j})). \end{aligned}$$

for $j = 1, \cdots, t-1$. Observe that by the hyptotheses on the ℓ_j and i_j, the functions h_j and h'_j are balanced. Finally, we let

$$\begin{aligned} f_{j+1}(u) &= h_j(Tr_{q_j}^{q_{j+1}}(u^{q_j^{i_j}+1})) \\ g_{j+1}(u) &= h'_j(Tr_{q_j}^{q_{j+1}}(u)), \end{aligned}$$

for $j = 1, \cdots, t$. Let $\mathbf{S}^j$ and $\mathbf{T}^j$ be geometric sequences whose ith elements are $f_j(\alpha^i)$ and $g_j(\alpha^i)$, respectively, for some fixed primitive element $\alpha \in GF(q_j)$ $(j = 2, \cdots, t+1)$. To find the cross-correlations of $\mathbf{S}^j$ and $\mathbf{T}^j$ we first need a lemma. For simplicity we let $H_j(u) = \zeta^{h_j(u)}$ and $H'_j(u) = \zeta^{h'_j(u)}$. Also let $k_j = q_j^{i_j} + 1$.

Lemma 7.1 *For any j, we have $\sum_u \eta(u)H_j(u) = \pm q_j^{1/2}$.*

Proof: The proof is by induction on j. In general we have

$$\sum_u \eta(u)H_j(u) = \sum_u H_j(u^2).$$

For $j = 1$, this is $\sum_u \zeta^{u^2}$ which can be seen to be $p^{1/2}$ by using addition formulas for trigonometric functions. For $j > 1$, we have

$$\begin{aligned} \sum_{u \in GF(q_j)} H_j(u^2) &= \sum_{u \in GF(q_j)} H_{j-1}(Tr_{q_{j-1}}^{q_j}(x^{\ell_{j-1}k_{j-1}})) \\ &= \sum_{u \in GF(q_j)} H_{j-1}(Tr_{q_{j-1}}^{q_j}(x^{k_{j-1}})) \\ &= \sum_{v \in GF(q_{j-1})} |\{u : Tr_{q_{j-1}}^{q_j}(x^{k_{j-1}}) = v\}| H_{j-1}(v) \\ &= \pm q_{j-1}^{(n_{j-1}-1)/2} \sum_{v \in GF(q_{j-1})} \eta(v)H_{j-1}(v) \\ &= \pm q_{j-1}^{(n_{j-1}-1)/2} q_{j-1}^{1/2} \\ &= \pm q_j^{1/2}. \end{aligned}$$

□

Proposition 7.2 *For any $j \geq 2$, we have $\Theta_{\mathbf{S}^j,\mathbf{T}^j}(\tau) + 1 = \pm q_j^{1/2}$.*

Proof: The cross-correlations are determined by Theorem 2.5, with $\delta = \rho = 0$. The result in case (1) of the theorem follows from Lemma 7.1. We prove case (2) by induction. For $j = 2$ this becomes

$$\pm q_1^{(n_1-1)/2} \sum_{u \in GF(p)} \zeta^{u^2/s-u}$$

for some $s \neq 0 \in GF(p)$. After completing the square, we see that this sum equals $\pm p^{1/2}$. For $j > 2$ we have, for some $s \neq 0 \in GF(q_{j-1})$,

$$\begin{aligned} \pm q_{j-1}^{(n_{j-1}-1)/2} \sum_{u \in GF(q_{j-1})} H_{j-1}(su^2) H'_{j-1}(u) &= \pm q_{j-1}^{(n_{j-1}-1)/2} (\Theta_{\mathbf{S}^{j-1},\mathbf{T}^{j-1}}(\tau') + 1) \\ &= \pm q_{j-1}^{(n_{j-1}-1)/2} q_{j-1}^{1/2} \\ &= \pm q_j^{1/2}. \end{aligned}$$

□

Thus the cross-correlations of such a pair of sequences essentially the square root of the period. This is in contrast to the characteristic zero case where the best we can do for cross-correlations of this type is a factor of $\sqrt{2}$ larger.

8 Conclusions

We have introduced a general class of easily generated binary sequences based on combinations of shift register sequences over an odd characteristic finite field with nonlinear feedforward functions. We have exhibited formulas for the cross-correlation of these sequences with standard geometric sequences in terms of the feedforward functions. The bounds given show that for quite general sequences of this type the cross-correlations are close to optimal. We have shown that in specific cases this allows us to construct pairs of sequences whose cross-correlations are all essentially the square root of the period. Furthermore, these sequences have larger linear span than many other sequences whose correlation properties are known.

We have not computed the cross-correlation of a pair of generalized geometric sequences, or even their autocorrelation functions. Using the approach taken here, this problem leads to the computation of the number of solutions to pairs of quadratic equations. In general this is a hard problem, but in this case there is some hope that the special form of the equations will make it tractable – the equations come from a single quadratic polynomial over $GF(q^n)$, with the variable multiplied by a constant.

Even more general geometric sequences can be considered, say by applying a feedforward function to an arbitrary linear combination of decimations of m-sequences. It is unlikely that much can be said in general about the cross-correlations of such sequences, but there may be other special cases (e.g., particular decimations) which can be approached by the techniques used here. In general the more complex the underlying modified m-sequence, the higher the linear span.

References

[1] M. Antweiller and L. Bohmer, Complex sequences over $GF(p^M)$ with a two-level autocorrelation function and a large linear span, *IEEE Trans. on Inf. Th.*, **38** (1992) pp. 120-130.

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

[3] A.H. Chan, M. Goresky, and A. Klapper, Correlation functions of geometric sequences, *Advances in Cryptology: Proc. Eurocrypt '90, Lecture Notes in Computer Science Vol. 473,* ed. I. B. Damgard, Springer-Verlag: Berlin, pp. 214-221, 1991.

[4] S. Golomb, *Shift Register Sequences,* Aegean Park Press: Laguna Hills, CA, 1982.

[5] B. Gordon, W. H. Mills, and L. R. Welch, Some new Difference Sets, *Canad. J. Math.*, **14** (1962) pp. 614-625.

[6] A. Klapper. Cross-Correlations of Geometric Sequences in Characteristic Two, *Designs, Codes, and Cryptography*, **3** (1993) pp. 347-377.

[7] A. Klapper, A.H. Chan, and M. Goresky, Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences, *Discrete Applied Mathematics*, **46** (1993) pp. 1-20.

[8] A. Klapper, A.H. Chan, and M. Goresky, Cascaded GMW sequences, *IEEE Trans. on Inf. Th.*, **39** (1993) pp. 177-183.

[9] R. Lidl and H. Niederreiter *Finite Fields* in *Encyclopedia of Mathematics vol 20* Cambridge University Press, Cambridge, 1983.

[10] R. McEliece *Finite Fields for Computer Scientists and Engineers,* Kluwer Academic Publishers, Boston, 1987.

[11] J. No and P. V. Kumar, A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, *IEEE Trans. on Inf. Th.* **35** (1989) pp. 371-379.

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

[13] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread-Spectrum Communications*, Volume 1, Computer Science Press, 1985.