Cross-Correlations of Geometric Sequences in Characteristic Two

Andrew Klapper*

Abstract

Cross-correlation functions are determined for a large class of geometric sequences based on m-sequences in characteristic two. These sequences are shown to have low cross-correlation values in certain cases. They are also shown to have significantly higher linear complexities 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.

Keywords: Binary sequence, geometric sequence, cross-correlation, linear complexity, Galois field.

1 Introduction

Easily generated pseudorandom sequences with high linear complexities and low correlation function values are sought in many applications of modern communication systems. For example, sequences with low cross-correlations are necessary in code division multiple access (CDMA) communication systems to determine the sign of the signal being sent on each channel. The smaller the pairwise cross-correlations, the higher the capacity of the system. The sequence is more difficult for an adversary to determine if its linear complexity is high. This lends a degree of security to CDMA systems.

Linear feedback shift registers have long been studied as simple devices that generate statistically random sequences. Particular interest has been given to m-sequences, the maximal period sequences generated by linear feedback shift registers. From a cryptographic point of view, however, these sequences are highly vulnerable to attack, for example, by

*University of Kentucky and University of Manitoba. Project sponsored bythe National Security Agency under Grant Number MDA904-91-H-0012.

the Berlekamp-Massey algorithm [11]. The linear complexity of a sequence is a measure of its resistance to this attack. Thus there is a need for easily generated sequences with high linear complexities and low cross-correlations. In particular, there is interest in sequences generated by devices based on linear feedback shift registers, but with some nonlinearity to increase the linear complexity. Notable early examples are GMW sequences [6] and bent sequences [14]. More general sequences, in which a nonlinear feedforward function is applied to an m-sequence over a finite field, have been studied in the past decade by a number of authors, for example [1, 2, 3, 4, 7, 8]. We call these sequences geometric sequences. This is a very general class of binary pseudorandom sequences which includes m-sequences, GMW sequences, and bent sequences, and is closely related to No sequences [13].

One way to view geometric sequences is as a compromise between m-sequences and general binary sequences. If r is a power of 2, then an arbitrary binary sequence of period $r-1$ can be produced as follows. Choose a function, h, from the field of r elements, $GF(r)$, to $GF(2) = \{0,1\}$. Let α be a primitive element of $GF(r)$, so that the elements $1, \alpha, \alpha^2, \cdots, \alpha^{r-2}$ are distinct. Apply h term-by-term to this sequence. The difficulty with this approach is that h tends to be very difficult to compute if the linear complexity is high. Moreover, finding cross-correlations is difficult in the absence of any algebraic structure. The higher the linear complexity, the more non-linear h must be, and the more non-linear h is, the harder it is to compute cross-correlations. Geometric sequences are produced by restricting h to be a composition: first apply a linear (or nearly linear) function, L, from $GF(r)$ to an intermediate field, $GF(q)$, then apply a highly nonlinear function, f, from $GF(q)$ to $GF(2)$. The function, f, called the *feedforward function*, is applied to a far smaller domain, so we can, if necessary, apply brute force search to obtain f with desirable properties. On the other hand, enough algebraic structure is retained to make the calculation of the cross-correlation of the final sequence easier. The goal then is to do this while keeping the linear complexity high.

The geometric sequences studied to date have m-sequences as their intermediate sequences over $GF(q)$ (equivalently, T is a trace function, as described below). These sequences can be designed to have low cross-correlations and higher linear complexities than m-sequences. However, their cross-correlations are known in only a small number of cases, and their linear complexities are far from the maximum possible for arbitrary sequences. The author (with Chan and Goresky) has previously considered cross-correlation function values of pairs of geometric sequences that are obtained from the same q-ary m-sequence but different nonlinear feedforward functions [4] and of geometric sequences in characteristic two whose underlying m-sequences differ by a quadratic decimation [7]. (A quadratic decimation is a k-fold decimation – every k-th element – where the sum of the coefficients of the base q expansion of k equals two. We refer to this as a quadratic decimation because of the relation to quadric hypersurfaces, as explained later).

In order to find sequences with higher linear complexities than previously studied geometric sequences it is necessary to consider further modifications to m-sequences. In this paper we study cross-correlation function values and linear complexities of geometric sequences whose underlying sequences over $GF(q)$ are sums of pairs of linear feedback shift register sequences, one of which is an m-sequence. Specifically, our main results are the calculation of the cross-correlations of a geometric sequence based on an m-sequence over $GF(q)$, and a geometric sequence based on a sum of the same m-sequence and a quadratic decimation of that m-sequence. The results allow the cross-correlations for particular feedforward functions to be computed inductively in terms of correlation-like functions of much shorter sequences. These shorter sequences depend only on the feedforward functions, and not on the underlying m-sequences. Careful choice of the feedfoward functions gives us sequences with very low cross-correlations. We also describe the number of shifts of the sequences for which each cross-correlation value occurs. Finally, we show that these generalized geometric sequences can be constructed with significantly higher linear complexities than ordinary geometric sequences. These linear complexities may be higher by as much as a factor of q for sequences based on m-sequences over $GF(q)$.

The technique for computing cross-correlations is based on counting the points of intersection of hyperplanes and quadric hypersurfaces over a finite field. To prove our main theorems on cross-correlations, we first give a complete accounting of the cardinalities of these intersections, based on a standard classification of quadratic forms. We next determine the ranks and types in this classification of the quadratic forms that occur in geometric sequences. This allows us to compute the desired cross-correlation functions. These functions may also be interpreted as generalized exponential sums of a type often considered in algebraic geometry and related areas of coding theory [16], though we do not exploit this point of view.

We assume a basic understanding of finite fields and the trace function, since this material is very well explained in the excellent survey papers and books on the subject [5, 10, 12, 15]. Let q be a fixed power of 2 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 $Tr_q^{q^n}(x) = \sum_{i=0}^{n-1} x^{q^i}$. Recall that $Tr_q^{q^n}$ is a $GF(q)$-linear function, that every $GF(q)$-linear function f from $GF(q^n)$ to $GF(q)$ can be written in the form $f(x) = Tr_q^{q^n}(Ax)$ for some $A \in GF(q^n)$, and that, for any $m \geq 1$, $Tr_q^{q^{nm}}(x) = Tr_q^{q^n}(Tr_{q^n}^{q^{nm}}(x))$. Also recall that every element x in a finite field of characteristic two has a unique square root $x^{1/2}$. (This is a consequence of the fact that the function $x \to x^2$ is a linear function with trivial kernel.)

Let α be a primitive element of $GF(q^n)$. The sequence $\mathbf{U}$ whose ith element is $U_i = Tr_q^{q^n}(\alpha^i)$ 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 $GF(q)$ [10]. In particular, they are easy to generate by hardware. Let $k = 1 + q^j$ (that is, k has q-adic weight two) and let γ be any element of $GF(q^n)$. The sequence whose ith element is $Tr_q^{q^n}(\gamma\alpha^{ki})$ is called a *quadratic decimation* of $\mathbf{U}$, and is itself an m-sequence if k is relatively prime to $q^n - 1$. Note that we could take $k = q^\ell + q^j$, but this gives rise to the same sequence as taking $k = 1 + q^{j-\ell}$. More generally, if $\delta \in GF(q^n)$, we consider the sequence $\mathbf{V}$ whose ith term is $V_i = Tr_q^{q^n}(\gamma\alpha^{ki} + \delta\alpha^i)$. (This amounts to adding a shift of $\mathbf{U}$ to $\mathbf{V}$.) The case where k is relatively prime to $q^n - 1$ and $\delta = 0$ (i.e., $\mathbf{V}$ is an m-sequence) has been treated previously by Klapper, Chan, and Goresky [7]. Those results are a special case of the current results. Note that the condition that k is relatively prime to $q^n - 1$ is equivalent to the condition that $n/\gcd(n, j - i)$ is odd, by Lemma 2.1 below.

Let f and g be (nonlinear) functions from $GF(q)$ to $GF(2)$. The sequences $\mathbf{S}$ and $\mathbf{T}$ whose ith elements are $f(U_i)$ and $g(V_i)$, respectively, are called *geometric sequences*, and it is these sequences whose cross-correlation functions we determine. The results are expressed in terms of statistical properties of f and g.

Definition 1.1 *The cross-correlation function of two sequences with period L is*

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{i=1}^{L}(-1)^{S_{i+\tau}}(-1)^{T_i}.$$

In the next subsections we state the main theorems and discuss some of their consequences. In Section 2 some basic facts from number theory and the theory of quadratic forms are recalled. These are useful in finding standard forms for the quadric hypersurfaces that appear and in counting solutions to quadratic equations. Section 3 contains a complete analysis of the numbers of points in the intersections of hyperplanes and quadric hypersurfaces in characteristic two. The forms of the quadrics that appear in the cross-correlation of geometric sequences are determined in Section 4. The proofs of the main theorems are completed in Section 5. The linear complexities of generalized geometric sequences are determined in Section 6.

1.1 Statements of the Main Theorems

In this section we state the main theorems on cross-correlations of geometric sequences. Let q be a power of 2 and f and g be functions from $GF(q)$ to $GF(2)$, $\gamma, \delta \in GF(q)$, $k = 1 + q^j$ and α primitive in $GF(q^n)$. Then $\mathbf{S}$ is the sequence whose ith element is $f(Tr_q^{q^n}(\alpha^i))$ and $\mathbf{T}$ is the sequence whose ith element is $g(Tr_q^{q^n}(\gamma\alpha^i + \delta\alpha^{ki}))$. We let $I(f) = \sum_{x \in GF(q)}(-1)^{f(x)}$, the *imbalance* of f, $F(u) = (-1)^{f(u)}$, and $G(u) = (-1)^{g(u)}$. We write $d = \gcd(n, j)$, $\omega = (-1)^{n/(2d)}$ when n/d is even, and $\eta(s) = -1$ if $s \neq 0$ and $\eta(0) = q - 1$.

For a given shift τ of $\mathbf{S}$, let $H(x) = Tr_q^{q^n}(\alpha^\tau x)$, $L(x) = Tr_q^{q^n}(\gamma x)$, and $R(x) = Tr_q^{q^n}(\delta x^k)$. We often think of $GF(q^n)$ as an n-dimensional vector space over $GF(q)$. When a basis (set of coordinates) has been chosen for $GF(q^n)$ over $GF(q)$, we replace the variable x by $\bar{x} = (x_1, \cdots, x_n)$ and by abuse of notation write $H(\bar{x})$, $L(\bar{x})$, and $R(\bar{x})$. $H(\bar{x})$ and $L(\bar{x})$ are linear functions and $R(\bar{x})$ is a quadratic form (this is proved in Theorem 4.1).

We state our results in three cases, differentiated by whether δ is a kth power and the parity of n/d. As seen in Section 2, every quadratic form can be put into one of three standard types by a change of coordinates. The breakdown into cases corresponds to this classification, as determined by Theorem 4.1. Once coordinates have been chosen so that R is expressed as one of the standard types, if $L(\bar{x}) = \sum_{i=1}^{n} c_i x_i$, then we let $\rho \stackrel{\text{def}}{=} R(c_1, \cdots, c_n)$ and, if R has Type II, $\sigma \stackrel{\text{def}}{=} c_m$, where m is the rank of R (the smallest number of variables that can be used to express R). These values are independent of the choice of coordinates expressing R as a standard type (this fact can be seen, for example, as a consequence of our theorems on the cross-correlation).

The breakdown of cases further depends on relations among three vector spaces. The symmetric bilinear form, D, is defined by $D(\bar{x}, \bar{y}) = R(\bar{x} + \bar{y}) - R(\bar{x}) - R(\bar{y})$. The *null space* of R, denoted by $Null(R)$, is the set of $\bar{w}$ such that $R(\bar{w}) = 0$ and for every $\bar{x}$, $D(\bar{w}, \bar{x}) = 0$. The null space of D, denoted by $Null(D)$, is the set of $\bar{w}$ such that for every $\bar{x}$, $D(\bar{w}, \bar{x}) = 0$. The kernel of L, denoted by $Ker(L)$, is the set of $\bar{w}$ such that $L(\bar{w}) = 0$.

To simplify things, we express our results in terms of $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \Theta_{\mathbf{S},\mathbf{T}}(\tau) - q^{n-2} I(f) I(g) + F(0)G(0)$. Each theorem includes a table of the number of occurrences of each value of $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$, for varying τ. The tables are divided into categories depending on L and ρ. Within each category a listing is given of number of occurrences of each case of the theorem, depending on the parameters r, s, and t used to described the values of $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$. Note that in some cases certain values of these parameters cannot occur.

Theorem 1.2 *Let n/d be even and δ be a kth power in $GF(q^n)$.*

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

1. $\omega q^{n/2+d-2} I(f)(I(g) - qG(\rho))$;
2. $\omega q^{n/2+d-1} F(t)(I(g) - qG(\rho))$;
3. $-\omega q^{n/2+d-1} \sum_{u \neq 0} \sum_{v} (-1)^{Tr_2^q(sv/u^2)} F(u+t) G(v+\rho)$.

Conditions on L, R	*Case*	*Parameters*	*Number of Occurences*
$L = 0$	*1*	–	$q^n - q^{n-2d}$
	2	$t = 0$	$q^{n-2d-1} - \omega(q-1)q^{n/2-d-1} - 1$
	3	$s \neq 0,\ t = 0$	$q^{n-2d-1} + \omega q^{n/2-d-1}$
$L \neq 0,\ \rho = 0$	*1*	–	$q^n - q^{n-2d}$
	2	$t \neq 0$	q^{n-2d-2}
	2	$t = 0$	$q^{n-2d-2} - \omega(q-1)q^{n/2-d-1} - 1$
	3	$s, t \neq 0$	q^{n-2d-2}
	3	$s \neq 0,\ t = 0$	$q^{n-2d-2} + \omega q^{n/2-d-1}$
$\rho \neq 0$	*1*	–	$q^n - q^{n-2d}$
	2	$t \neq 0$	$q^{n-2d-2} - \omega q^{n/2-d-1}$
	2	$t = 0$	$q^{n-2d-2} - 1$
	3	$s, t \neq 0$	$q^{n-2d-2} - \omega(-1)^{Tr_2^q(\rho s/t^2)} q^{n/2-d-1}$
	3	$s \neq 0,\ t = 0$	q^{n-2d-2}

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

1. *0;*
2. $\omega q^{n/2+d-2}(I(f)I(g) - q\sum_u F(u)G(su+t))$*.*

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

Theorem 1.3 *If* n/d *is even and* δ *is not a* $1+q^j$*th power in* $GF(q^n)$*, then* $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ *takes the values*

1. $\omega q^{n/2-1}F(t)(qG(\rho) - I(g))$*;*
2. $\omega q^{n/2-1}\sum_{u\neq 0}\sum_v (-1)^{Tr_2^q(sv/u^2)}F(u+t)G(v+\rho)$*.*

Conditions on L, R	*Case*	*Parameters*	*Number of Occurences*
$L = 0$	*1*	$t = 0$	$q^{n-1} + \omega(q-1)q^{n/2-1} - 1$
	2	$s \neq 0,\, t = 0$	$q^{n-1} - \omega q^{n/2-1}$
$L \neq 0,\ \rho = 0$	*1*	$t \neq 0$	q^{n-2}
	1	$t = 0$	$q^{n-2} + \omega(q-1)q^{n/2-1} - 1$
	2	$s, t \neq 0$	q^{n-2}
	2	$s \neq 0,\, t = 0$	$q^{n-2} - \omega q^{n/2-1}$
$\rho \neq 0$	*1*	$t \neq 0$	$q^{n-2} + \omega q^{n/2-1}$
	1	$t = 0$	$q^{n-2} - 1$
	2	$s, t \neq 0$	$q^{n-2} + \omega(-1)^{Tr_2^q(\rho s/t^2)} q^{n/2-1}$
	2	$s \neq 0,\, t = 0$	q^{n-2}

Theorem 1.4 *Let $n/\gcd(n, j-i)$ be odd.*

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

1. *0;*
2. $-q^{(n+d)/2-2}(I(f)I(g) - q\sum_u F(su)G(u^2+t))$;
3. $q^{(n+d)/2-2}(I(f)I(g) - q\sum_u F(su)G(u^2+t))$.

Conditions on L, R	*Case*	*Parameters*	*Number of Occurences*
$L = 0$	*1*	–	$q^n - q^{n-d+1} + q^{n-d} - 1$
	2	$s \neq 0,\, t = 0$	$(q^{n-d} + q^{(n-d)/2})/2$
	3	$s \neq 0,\, t = 0$	$(q^{n-d} - q^{(n-d)/2})/2$
$L \neq 0$	*1*	–	$q^n - q^{n-d+1} + q^{n-d} - 1$
	2	$s, t \neq 0$	$q^{n-d-1}/2$
	2	$s \neq 0,\, t = 0$	$(q^{n-d-1} + q^{(n-d)/2})/2$
	3	$s, t \neq 0$	$q^{n-d-1}/2$
	3	$s \neq 0,\, t = 0$	$(q^{n-d-1} - q^{(n-d)/2})/2$

B. If $Null(R) \subseteq Ker(L)$, but $Null(D) \not\subseteq Ker(L)$, (i.e., $\sigma \neq 0$) then $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ takes the values

1. $q^{(n+d)/2-2}I(f)\sum_v(-1)^{Tr_2^q(v+1)}G(\sigma^2 v + \rho)$;

2. $q^{(n+d)/2-1}F(t)\sum_v(-1)^{Tr_2^q(v+1)}G(\sigma^2 v+\rho)$;
3. $(-1)^{Tr_2^q((t+\rho)/\sigma^2+1)}q^{(n+d)/2-2}(q\sum_u F(ru+s)G(u^2+\sigma u+t)-I(f)I(g))$.

Conditions on L, R	*Case*	*Parameters*	*Number of Occurences*
$L(\bar{x})=\sigma x_m$	1	–	q^n-q^{n-d+1}
	2	$t\neq 0$	$q^{n-d-1}-q^{(n-d)/2-1}$
	2	$t=0$	$q^{n-d-1}+(q-1)q^{(n-d)/2-1}-1$
	3	$r\neq 0,\ s=0$	$q^{n-d-1}+\eta(\frac{t+\rho}{\sigma^2}+1)q^{(n-d)/2-1}$
$L(\bar{x})\neq\sigma x_m,\ \rho=0$	1	–	q^n-q^{n-d+1}
	2	$t\neq 0$	$q^{n-d-1}-(-1)^{Tr_2^q(\rho/\sigma^2+1)}q^{(n-d)/2-1}$
	2	$t=0$	$q^{n-d-1}+(-1)^{Tr_2^q(\rho/\sigma^2+1)}(q-1)q^{(n-d)/2-1}-1$
	3	$r,s\neq 0$	q^{n-d-2}
	3	$r\neq 0,\ s=0$	$q^{n-d-2}+\eta(\frac{t+\rho}{\sigma^2}+1)q^{(n-d)/2-1}$
$\rho=\sigma^2$	1	–	q^n-q^{n-d+1}
	2	$t\neq 0$	$q^{n-d-1}-q^{(n-d)/2-1}$
	2	$t=0$	$q^{n-d-1}+(q-1)q^{(n-d)/2-1}-1$
	3	$r,s\neq 0$	$q^{n-d-2}+(-1)^{Tr_2^q(r^2(\rho/\sigma^2+1)(t+\rho+\sigma^2)/s^2)}q^{(n-d)/2-1}$
	3	$r\neq 0,\ s=0$	q^{n-d-2}
$\rho\neq\sigma^2,\ \rho\neq 0$	1	–	q^n-q^{n-d+1}
	2	$t\neq 0$	$q^{n-d-1}-(-1)^{Tr_2^q(\rho/\sigma^2+1)}q^{(n-d)/2-1}$
	2	$t=0$	$q^{n-d-1}+(-1)^{Tr_2^q(\rho/\sigma^2+1)}(q-1)q^{(n-d)/2-1}-1$
	3	$r,s\neq 0$	$q^{n-d-2}+(-1)^{Tr_2^q(r^2(\rho/\sigma^2+1)(t+\rho+\sigma^2)/s^2)}q^{(n-d)/2-1}$
	3	$r\neq 0,\ s=0$	q^{n-d-2}

C. *If* $Null(R)\not\subseteq Ker(L)$, *then* $\Gamma_{\mathbf{S},\mathbf{T}}(\tau)$ *takes the values*

1. 0.
2. $q^{(n+d)/2-2}\sum_{u,v}(-1)^{Tr_2^q(ru+tv)}F(u)G(v)$.
3. $-q^{(n+d)/2-2}\sum_{u,v}(-1)^{Tr_2^q(ru+tv)}F(u)G(v)$.

Case	*Parameters*	*Number of Occurences*
1	–	$q^n-(q-1)^2q^{n-d}-1$
2	$r,t\neq 0$	$(q^{n-d}+q^{(n-d)/2})/2$
3	$r,t\neq 0$	$(q^{n-d}-q^{(n-d)/2})/2$

The first step in the proof of the main theorems is a reduction of the expression for the cross-correlation of **S** and **T**.

Proposition 1.5 *Let* $H_u = \{x : Tr_q^{q^n}(\alpha^\tau x) = u\}$ *and* $Q_v = \{x : Tr_q^{q^n}(\gamma x^k + \delta x) = v\}$. *Then*

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

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

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{x \in GF(q^n)} F(Tr_q^{q^n}(\alpha^\tau x))G(Tr_q^{q^n}(\gamma x^k + \delta x)) - F(0)G(0). \tag{1}$$

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 $Tr_q^{q^n}(\gamma x^k + \delta x) = Tr_q^{q^n}(\gamma y^k + \delta y)$. Then x and y contribute the same value to the sum in equation 1. Gathering all such terms together we get the expression for $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$ in the statement of the proposition. $\square$

If we treat $GF(q^n)$ as an n-dimensional affine space over $GF(q)$, then H_u is a hyperplane and Q_v is a (possibly inhomogeneous) quadric hypersurface. We have reduced the problem of computing cross-correlations of geometric sequences to that of finding intersections of hyperplanes and quadric hypersurfaces. More generally, if k has q-adic weight r (i.e., the sum of the coefficients in its base q representation equals r) then Q_v is a hypersurface of degree r.

1.2 Consequences of the Main Theorems

Consider the circumstance in which $f(0) = g(0) = 0$ and f and g are balanced, i.e., $I(f) = I(g) = 0$. These conditions hold, for example, for m-sequences, GMW sequences, and the more general cascaded GMW sequences [8]. They are desirable statistical properties in many applications. Under the hypotheses of Theorem 1.2,

$$|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1| \le q^{n/2+d}(q-1) = q^{n/2+\gcd(n,j)}(q-1).$$

Under the hypotheses of Theorem 1.3,

$$|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1| \le q^{n/2}(q-1).$$

Under the hypotheses of Theorem 1.4

$$|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1| \le q^{(n+d)/2} = q^{(n+\gcd(n,j))/2}.$$

The maximum cross-correlation for the sequences satisfying the hypotheses of Theorem 1.4 is minimized when $d = 1$.

We can improve these bounds by careful choice of f and g, still assuming f and g are balanced. We further assume $d = 1$ in Theorems 1.2 and 1.4. In all cases, minimizing the maximum of $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$ is equivalent to minimizing the maximum of a set of correlation functions or (in Theorem 1.3.2) of triple correlation functions of sequences of period q. There are three types of correlation functions which occur.

A. In Theorems 1.2.B.2, 1.4.A.2, 1.4.A.3, and 1.4.B.3 correlation functions of the form $\sum_u F(su)H(u+t)$ occur, with various restrictions on s, and t. H is a function defined in terms of G. Keeping t fixed, and considering the sum over $u \neq 0$, we have the set of shifted correlations of a pair of sequences of period $q-1$. Minimizing the maximum of these values will minimize the maximum of $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$. If we can achieve a value close to $q^{1/2}$, then in Theorems 1.4.A.2, 1.4.A.3, and 1.4.B.3 the maximum of $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$ will be close to $q^{n/2}$. In Theorem 1.2.B.2, $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$ will be close to $q^{(n+1)/2}$.

B. In Theorems 1.4.B.2 and 1.4.C.2 the Walsh transform $\sum_u (-1)^{Tr_2^q(su)} H(u)$ occurs, for various functions H. By Parseval's identity, the smallest maximum value the transform can achieve (subject to the restraint that H is balanced) is $q/(q-1)^{1/2}$. In Theorem 1.4.B.2 this leads to the lower bound of $q^{(n+1)/2}/(q-1)^{1/2} \sim q^{n/2}$ for the maximum of $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$. In Theorem 1.4.C.2 this leads to the lower bound of $q^{(n+1)/2}/(q-1) \sim q^{(n-1)/2}$ for the maximum of $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$.

C. In Theorems 1.2.A.3 and 1.4.2 the sum $\sum_{u \neq 0} \sum_v (-1)^{Tr_2^q(sv/u^2)} F(u+t)G(v+\rho)$ occurs. This can be thought of as a correlation of three sequences of period q, or as the correlation of one sequence with the Walsh transform of another. Thus, it is plausible that we can achieve a maximum value (as s and t vary) of q for this double sum. If so, then in Theorem 1.2.A.3 we can achieve a maximum of $q^{n/2+1}$ for $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$ and in Theorem 1.3.2 we can achieve a maximum of $q^{n/2}$ for $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$.

Assuming these bounds, it follows that we have the following values for the minimum maximum value of $|\Theta_{\mathbf{S},\mathbf{T}}(\tau) + 1|$. We leave the question of whether these values can be achieved (or even improved) to further study.

Theorem	min of max of $\|\Theta_{\mathbf{S},\mathbf{T}}(\tau)+1\|$
1.2.A	$q^{n/2+1}$
1.2.B	$q^{(n+1)/2}$
1.3	$q^{n/2}$
1.4.A	$q^{n/2}$
1.4.B	$q^{n/2}$
1.4.C	$q^{(n-1)/2}$

2 Algebraic Tools

In this section we recall several useful facts from number theory and the theory of quadratic forms over a finite field. These facts will be used in the proofs of the main theorems. More complete treatments can be found in various standard texts such as [10, 12].

As a standard consequence of the division algorithm we have:

Lemma 2.1 *Let b be an even integer and n, i, and j be non-negative integers and set $d = \gcd(n, j)$. Then*

$$\gcd(b^n - 1, b^j - 1) = b^d - 1. \tag{2}$$

$$\gcd(b^n - 1, b^j + 1) = \begin{cases} 1 & \textit{if} \quad n/d \textit{ is odd} \\ 1 + b^d & \textit{if} \quad n/d \textit{ is even.} \end{cases} \tag{3}$$

Recall that a quadratic form over $GF(q)^n$ is a homogeneous polynomial of degree two in n variables with coefficients in $GF(q)$. We are concerned with counting the number of times certain quadratic forms over $GF(q)^n$ take on different values. To do so, it is convenient to represent the quadratic forms by a small number of standard types, by changing coordinates (a change of coordinates has no effect on the number of times a quadratic form takes on a particular value). Such classifications are well known. We follow here the treatment given by Lidl and Niederreiter [10].

Recall that the *rank* of a quadratic form is the smallest number of variables required to represent the quadratic form, up to a change of coordinates. The *co-rank* of a quadratic form in n variables is n minus the rank. A quadratic form is said to be *nonsingular* if it has rank n. If R is a quadratic form, then we define the associated symmetric bilinear form $D(\bar{x}, \bar{y}) = R(\bar{x} + \bar{y}) - R(\bar{x}) - R(\bar{y})$, where $\bar{x} = (x_1, \cdots, x_n)$ and $\bar{y} = (y_1, \cdots, y_n)$. Note that R is not uniquely determined by D if q is even, unlike the the case where q is odd. D may even be zero for nonzero R. We also refer to the *rank* of D, the smallest m such that D can be represented in terms of $x_1, \cdots, x_m, y_1, \cdots, y_m$, after a change of coordinates. The rank of D is at most the rank of R.

Associated with R are two important vector spaces. The *null space* of R, denoted by $Null(R)$, is the set of $\bar{w}$ such that $R(\bar{w}) = 0$ and for every $\bar{x}$, $D(\bar{w}, \bar{x}) = 0$. The null space of D, denoted by $Null(D)$, is the set of $\bar{w}$ such that for every $\bar{x}$, $D(\bar{w}, \bar{x}) = 0$. Associated with the linear function L is the kernel of L, denoted by $Ker(L)$, which consists of those $\bar{w}$ such that $L(\bar{w}) = 0$. We will use properties of these vector spaces to determine the ranks of the quadratic forms that arise.

Lemma 2.2 *The dimension of $Null(R)$ is the co-rank of R. The dimension of $Null(D)$ is the co-rank of D.*

Proof: Let m be the rank of R, and assume that coordinates $x_1, \cdots, x_n$ have been chosen so that R is expressed in terms of $x_1, \cdots, x_m$. Let $V = \{(x_1, \cdots, x_n) : x_1 = \cdots = x_m = 0\}$. The first assertion will be proved by showing $V = Null(R)$ since the dimension of V is $n - m$, the co-rank of R. The inclusion $V \subseteq Null(R)$ is straightforward, so assume the opposite inclusion is false, that is, that there is a $w \in Null(R)$ which is not in V. By changing coordinates, we may assume that w consists of a 1 in the mth coordinate and 0s elsewhere, and the description of V remains unchanged. It follows that for some $a \in GF(q)$, and polynomials $b(x_1, \cdots, x_{m-1})$ and $c(x_1, \cdots, x_{m-1})$ over $GF(q)$,

$$R(\bar{x}) = ax_m^2 + b(\bar{x})x_m + c(\bar{x}).$$

In this representation we have

$$D(\bar{x}, \bar{y}) = 2ax_m y_m + b(\bar{x} + \bar{y})(x_m + y_m) - b(\bar{x})x_m - b(\bar{y})y_m + c(\bar{x} + \bar{y}) - c(\bar{x}) - c(\bar{y}).$$

The fact that $R(w) = 0$ implies $a = 0$. The fact that, for every $\bar{x}$, $D(w, \bar{x}) = 0$ implies that, for every $\bar{x}$, $b(\bar{x})(1 + x_m) - b(\bar{x})x_m = 0$, so $b(\bar{x}) = 0$. Thus R is written in terms of $x_1, \cdots, x_{m-1}$, contradicting the fact that the rank of R is m. Thus $Null(R) \subseteq V$ and so $Null(R) = V$.

The proof of the second assertion is similar. □

We first describe the classification of quadratic forms in two variables. We assume from now on that q is a power of 2.

Lemma 2.3 *Given $c, d, e \in GF(q)$ (not all zero), define the quadratic form $g(x, y) = cx^2 + dxy + ey^2$. Then $g(x, y)$ is nonsingular if and only if $d \neq 0$. Let b be a fixed element of $GF(q)$ satisfying $Tr_2^q(b) = 1$. Under a linear change of coordinates g is equivalent to the quadratic form*

1. *xy, if $d \neq 0$ and $Tr_2^q(ec/d^2) = 0$;*

2. *$bx^2 + xy + by^2$, if $d \neq 0$ and $Tr_2^q(ec/d^2) = 1$;*

3. *x^2, if $d = 0$.*

Let $v \in GF(q)$. In case (1), $g(x, y) = v$ has $2q - 1$ solutions if $v = 0$, and $q - 1$ solutions if $v \neq 0$. In case (2), $g(x, y) = v$ has only the zero solution if $v = 0$, and has $q + 1$ solutions if $v \neq 0$. In case (3), $g(x, y) = v$ has q solutions for every v.

More generally, quadratic forms $R(x_1, \ldots, x_n)$ in n variables over $GF(q)$ (with q even) have been classified [10, Theorem 6.30] as follows. Let $B_m(\bar{x}) = x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m$.

Proposition 2.4 *Every quadratic form R of rank m in n variables over $GF(q)$, q even, is equivalent under a change of coordinates one of the following three standard types:*

Type I: $B_m(\bar{x})$;

Type II: $B_{m-1}(\bar{x}) + x_m^2$;

Type III: $B_{m-2}(\bar{x}) + bx_{m-1}^2 + x_{m-1}x_m + bx_m^2$.

For any $v \in GF(q)$, let $\eta(v) = -1$ if $v \neq 0$ and $\eta(0) = q - 1$. The number of solutions to the equation $R(\bar{x}) = v$ is:

Type I: $q^{n-1} + \eta(v)q^{n-m/2-1}$;

Type II: q^{n-1};

Type III: $q^{n-1} - \eta(v)q^{n-m/2-1}$.

We say that a quadratic form is Type j if it is equivalent to a Type j standard form. We are also concerned with the number of times certain inhomogeneous equations take on different values.

Proposition 2.5 *Let $R(\bar{x})$ be a quadratic form of rank m. The number of solutions to the equation*

$$R(\bar{x}) + \sum_{i=1}^{m} c_i x_i = v \tag{4}$$

is

Type I: $q^{m-1} + \eta(v + R(\bar{c}))q^{m/2-1}$;

Type II: *1.* q^{m-1} *if* $c_m = 0$;

2. $q^{m-1} + (-1)^{Tr_2^q((v+B_{m-1}(barc))/c_m^2)} q^{(m-1)/2}$ *if* $c_m \neq 0$*;*

Type III: $q^{m-1} - \eta(v + R(\bar{c}))q^{m/2-1}$.

Proof: The results for Type I and Type III forms follow from the previous proposition after an affine change of coordinates which replaces x_1 by $x_1 + c_2$, x_2 by $x_2 + c_1$, etc. This eliminates the linear terms and replaces v by $v + R(\bar{c})$.

In the case of a Type II form, we can eliminate the first $m-1$ linear terms by the same change of basis, replacing v by $v + B_{m-1}(\bar{c})$, resulting in

$$R(\bar{x}) + c_m x_m = v + B_{m-1}(\bar{x}). \tag{5}$$

Let $w = v + B_{m-1}(\bar{c})$. We cannot eliminate the remaining linear term $c_m x_m$. If $c_m = 0$, then we are done by the previous proposition. Thus we may assume $c_m \neq 0$.

Let $\mu_m(c_m, w)$ denote the number of solutions to equation (5). By Lemma 2.3, $\mu_1(c_m, w) = 2$ if $Tr_2^q(w/c_m^2) = 0$, and $\mu_1(c_m, w) = 0$ if $Tr_2^q(w/c_m^2) = 1$. In general, letting $\sigma_m(w)$ be the number of solutions to $B_m(\bar{x}) = w$, we have

$$\begin{aligned}
\mu_m(c_m, w) &= \sum_{u \in GF(q)} \mu_1(c_m, u)\sigma_{m-1}(u + w) \\
&= 2 \cdot \sum_{Tr_2^q(u/c_m^2)=0} \sigma_{m-1}(u + w) \\
&= 2 \cdot \sum_{Tr_2^q(u/c_m^2)=0} (q^{m-2} + \eta(u + w)q^{(m-3)/2}) \\
&= \begin{cases} 2 \cdot \frac{q}{2}(q^{m-2} - q^{(m-3)/2}) & \text{if } Tr_2^q(w/c_m^2) = 1 \\ 2\frac{q-1}{2}(q^{m-2} - q^{(m-3)/2}) + 2(q^{m-2} + (q-1)q^{(m-3)/2}) & \text{if } Tr_2^q(w/c_m^2) = 0 \end{cases}
\end{aligned}$$

by Proposition 2.4. The proposition follows. □

3 Intersections of Quadric Hypersurfaces with Hyperplanes

In this section we give a complete description of the cardinalities of the intersections of quadric hypersurfaces with hyperplanes over a finite field of characteristic 2. These cardinalities form the coefficients in Proposition 1.5.

We work in this section in affine n-space $GF(q)^n$ over $GF(q)$, writing $\bar{x}$ for the n-tuple of variables $(x_1, \ldots, x_n)$. We choose a fixed element $b \in GF(q)$ such that $Tr_2^q(b) = 1$. Throughout this section $H(\bar{x}) = \sum_{i=1}^n a_i x_i$ and $L(\bar{x}) = \sum_{1=0}^n c_i x_i$ are linear polynomials and $R(\bar{x})$ is a quadratic form in one of the three standard types. For any $u, v \in GF(q)$, we think of $H(\bar{x}) = u$ as defining a hyperplane, and $Q(\bar{x}) \stackrel{def}{=} R(\bar{x}) + L(\bar{x}) = v$ as defining a quadric hypersurface. The rank of R is denoted by m, and the number of solutions to the simultaneous equations

$$H(\bar{x}) = u \tag{6}$$

$$Q(\bar{x}) = v \tag{7}$$

(i.e., the intersection of a hyperplane with a quadric hypersurface) is denoted by $N(u, v)$.

The analysis of $N(u, v)$ is carried out on a case by case basis. The first two cases apply to arbitrary R, while the remaining cases depend on the type of R.

Proposition 3.1 *Suppose that $c_i a_j \neq c_j a_i$ for some $i, j > m$. Then $N(u, v) = q^{n-2}$.*

Proof: By hypothesis, the linear polynomials $\sum_{r=m+1}^{n} a_r x_r$ and $\sum_{r=m+1}^{n} c_r x_r$ are linearly independent. Therefore, for any fixed values of $x_1, \cdots, x_m$, the equations

$$\sum_{r=m+1}^{n} a_r x_r = u + \sum_{r=1}^{m} a_r x_r$$

and

$$\sum_{r=m+1}^{n} c_r x_r = v + R(\bar{x}) + \sum_{r=1}^{m} c_r x_r$$

have q^{n-m-2} solutions over $x_{m+1}, \cdots, x_n$. The q^m possible values of $x_1, \cdots, x_m$ give q^{n-2} solutions in all. □

Proposition 3.2 *Suppose that $a_{m+1} = \cdots = a_n = 0$ and some $c_i \neq 0$, with $i > m$. Then $N(u, v) = q^{n-2}$.*

Proof: Choose $x_1, \cdots, x_m$ so that $\sum_{r=1}^{m} a_i x_i = 0$. There are q^{m-1} choices for such $x_1, \cdots, x_m$. Then the equation

$$\sum_{r=m+1}^{n} c_r x_r = v + R(\bar{x}) + \sum_{r=1}^{m} c_r x_r$$

has q^{n-m-1} solutions over $x_{m+1}, \cdots, x_n$, for q^{n-2} solutions in all. □

In the following we let $\epsilon = 1$ if R has Type I and $\epsilon = -1$ if R has Type III.

Proposition 3.3 *Suppose that for some $i > m$, $a_i \neq 0$, and $(c_{m+1}, \cdots, c_n) = s(a_{m+1}, \cdots, a_n)$ for some $s \in GF(q)$. Let $d_\ell = c_\ell + s a_\ell$, for $1 \leq \ell \leq n$.*

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

$$N(u,v) = q^{n-2} + \epsilon\eta(v + su + R(\bar{d}))q^{n-m/2-2}.$$

(Note that $R(\bar{d}) = R(\bar{c}) + sD(\bar{c},\bar{a}) + s^2R(\bar{a})$.)

2. *If R has Type II, and $\lambda = Tr_2^q((v + su + B_{m-1}(\bar{d}))/d_m^2)$ when $d_m \neq 0$, then*

$$N(u,v) = \begin{cases} q^{n-2} & \text{if } d_m = 0 \\ q^{n-2} + (-1)^{\lambda} q^{n-m/2-3/2} & \text{if } d_m \neq 0. \end{cases}$$

Proof: It follows from the hypotheses that $N(u,v)$ is the number of solutions to the equations

$$\sum_{j=1}^{n} a_j x_j = u, \tag{8}$$

$$R(\bar{x}) + \sum_{j=1}^{m} d_j x_j = v + su. \tag{9}$$

The variables x_ℓ, $m+1 \leq \ell \leq n$ appear in equation (8) but not in equation (9), so we can choose any values for $x_1, \cdots, x_m$ satisfying equation (9), then find a complete solution by solving

$$\sum_{j=m+1}^{n} a_j x_j = u + \sum_{j=1}^{m} a_j x_j.$$

Thus $N(u,v)$ is q^{n-m-1} times the number of solutions to equation (9). The proposition follows from Proposition 2.5. □

Proposition 3.4 *Suppose that $a_{m+1} = a_{m+2} = \cdots = a_n = c_{m+1} = c_{m+2} \cdots = c_n = 0$, or $m = n$.*

1. *Let R have Type I or Type III, and $\phi = Tr_2^q((v + R(\bar{c}))R(\bar{a})/(u^2 + D(\bar{a},\bar{c})^2))$ when $u \neq D(\bar{a},\bar{c})$.*

   a. *If $R(\bar{a}) \neq 0$, then*

$$N(u,v) = \begin{cases} q^{n-2} + \epsilon(-1)^{\phi} q^{n-m/2-1} & \text{if } u \neq D(\bar{a},\bar{c}) \\ q^{n-2} & \text{if } u = D(\bar{a},\bar{c}). \end{cases}$$

   b. *If $R(\bar{a}) = 0$, then*

$$N(u,v) = \begin{cases} q^{n-2} & \text{if } u \neq D(\bar{a},\bar{c}) \\ q^{n-2} + \epsilon\eta(v + R(\bar{c}))q^{n-m/2-1} & \text{if } u = D(\bar{a},\bar{c}). \end{cases}$$

2. *Let R have Type II.*

   a. *If $a_m = c_m = 0$, then $N(u,v) = q^{n-2}$.*

   b. *If $a_m = 0$ and $c_m \neq 0$, then $N(u,v) = q^{n-2}$ when $u \neq D(\bar{a},\bar{c}) + c_m R(\bar{a})^{1/2}$, and $N(D(\bar{a},\bar{c}) + c_m R(\bar{a})^{1/2}, v) = q^{n-2} + (-1)^{\mu} q^{n-m/2-1/2}$ where $\mu = Tr_2^q((v + B_{m-1}(\bar{c}))/c_m^2)$.*

   c. *Otherwise $N(u,v) = q^{n-2} + (-1)^{\pi}\eta(w) q^{n-m/2-3/2}$ where $\pi = Tr_2^q(B_{m-1}(\bar{a})/a_m^2)$ and $w = v + u^2/a_m^2 + (c_m/a_m)u + R(\bar{c}) + R(\bar{a})c_m^2/a_m^2 + D(\bar{a},\bar{c})c_m/a_m + D(\bar{a},\bar{c})^2/a_m^2$.*

Proof: Suppose first that R has Type I or Type III. After the affine change of coordinates used in Proposition 2.5, we find that $N(u,v)$ is the number of solutions to the equations

$$\sum_{i=1}^{m} a_i x_i = u + D(\bar{a},\bar{c}) \tag{10}$$

and

$$R(\bar{x}) = v + R(\bar{c}). \tag{11}$$

The number of solutions over $x_1, \cdots, x_n$ is q^{n-m} times the number of solutions over $x_1, \cdots, x_m$. Thus we may assume that $n = m$.

Now let R have Type I. By symmetry, we may assume that $a_m \neq 0$. We can solve for x_m in equation (10):

$$x_m = \frac{1}{a_m}(u + D(\bar{a},\bar{c}) + \sum_{i=1}^{m-1} a_i x_i).$$

Thus equation (11) becomes

$$B_{m-2}(\bar{x}) + \sum_{i=1}^{m-1} \frac{a_i}{a_m} x_i x_{m-1} + \frac{u + D(\bar{a},\bar{c})}{a_m} x_{m-1} = v + R(\bar{c}). \tag{12}$$

$N(u,v)$ is q^{n-m} times the number of solutions to this last equation. We next change coordinates by

$$x_{2i-1} \mapsto x_{2i-1} + a_{2i}x_{m-1}, \quad x_{2i} \mapsto x_{2i} + a_{2i-1}x_{m-1}$$

for $1 \leq i \leq m/2 - 1$, and

$$x_{m-1} \mapsto a_m x_{m-1}.$$

Equation (12) becomes

$$B_{m-2}(\bar{x}) + R(\bar{a})x_{m-1}^2 + (u + D(\bar{a},\bar{c}))x_{m-1} = v + R(\bar{c}).$$

If $R(\bar{a}) \neq 0$, then the result follows from Proposition 2.5, while if $R(\bar{a}) = 0$, the result follows from Proposition 2.4. A similar analysis works if R has Type III, though extra care is required if $a_1 = \cdots = a_{m-2} = 0$. The details are left to the reader.

Finally, suppose R has Type II. We can change coordinates affinely to obtain equations

$$\sum_{i=1}^{m} a_i x_i = u + D(\bar{a}, \bar{c}) \tag{13}$$

and

$$B_{m-1}(\bar{x}) + x_m^2 + c_m x_m = v + B_{m-1}(\bar{c}).$$

If $a_1 = \cdots = a_{m-1} = 0$, then $a_m \neq 0$ and $x_m = u/a_m$ (since $D(\bar{a}, \bar{c}) = 0$). The result follows in this case from Proposition 2.4. Otherwise, we may assume by symmetry that $a_{m-1} \neq 0$, solve for x_{m-1} in equation (13), and change coordinates to arrive at the equation

$$B_{m-3}(\bar{x}) + B_{m-1}(\bar{a})x_{m-2}^2 + a_m x_{m-2} x_m + x_m^2 + (u + D(\bar{a}, \bar{c}))x_{m-2} + c_m x_m = v + B_{m-1}(\bar{c}).$$

If $a_m = 0$, we can change coordinates by

$$x_m \mapsto x_m + B_{m-1}(\bar{a})^{1/2} x_{m-2},$$

resulting in the equation

$$B_{m-3}(\bar{x}) + x_m^2 + (u + D(\bar{a}, \bar{c}) + c_m B_{m-1}(\bar{a})^{1/2})x_{m-2} + c_m x_m = v + B_{m-1}(\bar{c}).$$

If, moreover, $c_m = 0$, then we have q^{n-2} solutions. Suppose $c_m \neq 0$. We have q^{n-2} solutions if $u \neq D(\bar{a}, \bar{c}) + c_m B_{m-1}(\bar{a})^{1/2}$. If $u = D(\bar{a}, \bar{c}) + c_m B_{m-1}(\bar{a})^{1/2}$, then we have $q^{n-2} + (-1)^{\mu} q^{n-m/2-1/2}$ solutions.

If $a_m \neq 0$, we can apply the change of coordinates

$$x_{m-2} \mapsto x_{m-2} + \frac{c_m}{a_m}, \quad x_m \mapsto x_m + \frac{u + D(\bar{a}, \bar{c})}{a_m}$$

to eliminate the linear terms. Proposition 2.4 can then be applied to give the stated value for $N(u, v)$. □

4 Analysis of Types and Ranks

We now begin the proof of Theorems 1.2, 1.3, and 1.4. We first determine the types of the quadratic forms involved. We then use the results of Section 3 to evaluate the coefficients in the expression for the cross-correlation in Proposition 1.5. Any choice of basis $e_1, e_2, \ldots, e_n$

for $GF(q^n)$ as a vector space over $GF(q)$ determines an identification $GF(q)^n \to GF(q^n)$ by $\bar{x} = (x_1, x_2, \ldots, x_n) \mapsto \sum_i x_i e_i = x$. 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 $\delta \neq 0 \in GF(q^n)$ and define the function $R : GF(q)^n \to GF(q)$ by $R(\bar{x}) = Tr_q^{q^n}(\delta x^k)$.

Theorem 4.1 *Suppose $k = 1 + q^j$ (so k has q-adic weight 2). Then $R(\bar{x})$ is a quadratic form.*

1. *If $n/\gcd(n,j)$ is even and δ is not a $(1+q^j)$th power in $GF(q^n)$, then the rank of R is n, hence even. Moreover, if $\frac{n}{2\gcd(n,j)}$ is odd, then R is a Type III quadratic form, while if $\frac{n}{2\gcd(n,j)}$ is even, then R is a Type I quadratic form.*
2. *If $n/\gcd(n,j)$ is even and δ is a $(1+q^j)$th power in $GF(q^n)$, then the rank of R is $n - 2\gcd(n,j)$, hence even. Moreover, if $\frac{n}{2\gcd(n,j)}$ is odd, then R is a Type I quadratic form, while if $\frac{n}{2\gcd(n,j)}$ is even, then R is a Type III quadratic form.*
3. *If $n/\gcd(n,j)$ is odd, then the rank of R is $n - \gcd(n,j) + 1$, hence even. Moreover, R is a Type II quadratic form.*

Proof: If $e_1, e_2, \ldots, e_n$ is a basis for $GF(q^n)$ over $GF(q)$, then

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

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

The third case was handled by Klapper, Chan, and Goresky [7]. Hence we may assume that $n/\gcd(n,j)$ is even. It follows that $j \neq 0$.

Consider the null space, W, of R, defined by

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

W is a $GF(q)$-vector subspace in $GF(q^n)$, and, by Lemma 2.2, the dimension of W is the co-rank of R, which we next determine.

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

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

$$Tr_q^{q^n}(\delta w y^{q^j}) = Tr_q^{q^n}(\delta^{q^j} w^{q^{2j}} y^{q^j}),$$

or

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

for all $y \in GF(q^n)$. This implies that $\delta w = \delta^{q^j} w^{q^{2j}}$.

Let $z = \delta w^{1+q^j}$. Then $w \in W$ if and only if $Tr_q^{q^n}(z) = 0$ and $z^{q^j-1} = 1$, i.e., $z \in GF(q^j)$. This second condition is equivalent to $z \in GF(q^j) \cap GF(q^n) = GF(q^{\gcd(n,j)})$. Moreover, if $y \in GF(q^{\gcd(n,j)})$, then

$$\begin{aligned} Tr_q^{q^n}(y) &= Tr_q^{q^{\gcd(n,j)}}(Tr_{q^{\gcd(n,j)}}^{q^n}(y)) \\ &= Tr_q^{q^{\gcd(n,j)}}(\frac{n}{\gcd(n,j)} y) = 0, \end{aligned}$$

since $n/\gcd(n,j)$ is even. Hence $w \in W$ if and only if $\delta w^{1+q^j} \in GF(q^{\gcd(n,j)})$.

Suppose there is a $w \neq 0 \in W$. Let u satisfy $u^{q^{2\gcd(n,j)}-1} = 1$. We have that $n/\gcd(n,j)$ is even, so $2\gcd(n,j)$ divides n, and thus $q^{2\gcd(n,j)} - 1$ divides $q^n - 1$. Therefore $u \in GF(q^n)$. We have

$$(\delta (uw)^{1+q^j})^{q^{\gcd(n,j)}-1} = 1,$$

that is, $uw \in W$. The cardinality of the set of such u in $GF(q^n)$ is $q^{q\gcd(n,j)} - 1$. Conversely, if $v \in W$, then

$$(v/w)^{(1+q^j)(q^{\gcd(n,j)}-1)} = 1.$$

It follows that

$$(v/w)^{q^{2\gcd(n,j)}-1} = 1,$$

and so W has cardinality $q^{2\gcd(n,j)}$ or has cardinality 1 (i.e., consists of only 0).

We next show that there is a $w \neq 0 \in W$ if and only if δ is a $(1+q^j)$th power. If $\delta = d^{1+q^j}$, then $w = d^{-1} \in W$. Conversely, suppose $v = \delta w^{1+q^j} \in GF(q^{\gcd(n,j)})$. Let u be a primitive $q^{2\gcd(n,j)} - 1$ root of 1 in $GF(q^n)$. Then u^{1+q^j} is a primitive $q^{\gcd(n,j)} - 1$ root of 1, i.e., a primitive element of $GF(q^{\gcd(n,j)})$. It follows that there is an integer m such that $v = u^{(1+q^j)m}$. Therefore, $\delta = (u^m/w)^{1+q^j}$. This proves the assertions regarding the rank of R.

We suppose lastly that δ is not a $1+q^j$th power and determine the type of R. The case where δ is a $1+q^j$th power is similar. Let $b \neq 0 \in GF(q)$. Suppose that R is a Type I quadratic form. Then the equation $R(x) = b$ has $q^{n-1} - q^{n/2-1} = q^{n/2-1}(q^{n/2} - 1)$ solutions by Proposition 2.4. Also, if $R(x) = b$, and $u^{1+q^j} = 1$, then $R(ux) = b$. There are $q^{\gcd(n,j)} + 1$

such u in $GF(q^n)$, so $q^{\gcd(n,j)}+1$ divides $q^{n/2}-1$. By Lemma 2.1, this is only possible if $n/(2\gcd(n,j))$ is even. Similarly, it can be shown that if R is a Type III quadratic form, then $n/(2\gcd(n,j))$ is odd. If R had Type II, then the number of solutions to $R(x)=b$ would be q^{n-1}, which cannot be divisible by $q^{\gcd(n,j)}+1$, so Type II is impossible. The assertions regarding the type of R in this case follow. □

5 Proofs of the Main Theorems

Completing the proofs of the main theorems is now a matter of combining the results of Section 3 with Theorem 4.1. In each case we have a fixed quadratic form $R(\bar{x})$, whose type is established by Theorem 4.1, a linear function $L(\bar{x})$, and a linear function $H(\bar{x})$ whose coefficients are determined by the shift τ (R, L, and H are defined over $GF(q)$). As τ ranges through all possible shifts, H ranges through all possible nonzero linear functions. Thus, in determining the distribution of values of $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$ for fixed geometric sequences $\mathbf{S}$ and $\mathbf{T}$, we keep R and L fixed and let H vary through all nonzero linear functions. For any fixed R, L, and H, one of the propositions of Section 3 applies. The results of that proposition are then used in Proposition 1.5 to determine a value for $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$. The counts of the number of shifts τ giving rise to each value of $\Theta_{\mathbf{S},\mathbf{T}}(\tau)$ are also determined by the propositions of Section 3.

Assume we have chosen coordinates so that $R(\bar{x})$ is in one of the three standard types, with rank m. We write $L(\bar{x})=\sum_{i=1}^{n} c_i x_i$, $H(\bar{x})=\sum_{i=1}^{n} a_i x_i$, and $\rho=R(\bar{c})$. The condition $Null(R)\subseteq Ker(L)$ is equivalent to $c_{m+1}=\cdots=c_n=0$. The condition $Null(D)\subseteq Ker(L)$ is equivalent to $c_m=\cdots=c_n=0$ when R is a Type II quadratic form. We let $\epsilon=1$ if R has Type I, $\epsilon=-1$ if R has Type III, and $\sigma=c_m$ if R has Type II. Thus by Theorem 4.1, $\omega=\epsilon$ if δ is not a kth power (i.e., in Theorem 1.3), and $\omega=-\epsilon$ if δ is a kth power (i.e., in Theorem 1.2). In order to compute the coefficients $N(u,v)$, we must count the simultaneous solutions to

$$H(\bar{x})=u \tag{14}$$

and

$$R(\bar{x})+L(\bar{x})=v, \tag{15}$$

for arbitrary $u,v\in GF(q)$. The proofs are handled in several cases depending on the parameters c_i that determine the shift τ.

A. Suppose that $(c_{m+1},\cdots,c_n)=s(a_{m+1},\cdots,a_n)$ for some s, and there is an $i>m$ such that $a_i\neq 0$. Then we can apply Proposition 3.3. This condition is satisfied by q^n-q^m shifts if $c_{m+1}=\cdots=c_n=0$, and $q^{m+1}-q^m$ shifts otherwise. This gives

1. Case A.1 of Theorem 1.2, when $s = 0$. Here
$$N(u,v) = q^{n-2} + \epsilon\eta(v+\rho)q^{n/2+d-2},$$
so
$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \omega q^{n/2+d-2} I(f)(I(g) - qG(\rho)).$$
This value occurs for $q^n - q^{n-2d}$ shifts.

2. Case B.2 of Theorem 1.2, where
$$N(u,v) = q^{n-2} + \epsilon\eta(v + su + R(\bar{c}) + sD(\bar{c},\bar{a}) + s^2R(\bar{a}))q^{n/2+d-2},$$
so
$$\begin{aligned}\Gamma_{\mathbf{S},\mathbf{T}}(\tau) &= \omega q^{n/2+d-2}(I(f)I(g) - q\sum_u F(u)G(su+\rho+sD(\bar{c},\bar{a})+s^2R(\bar{a}))) \\ &= \omega q^{n/2+d-2}(I(f)I(g) - qF(u)G(su+t)),\end{aligned}$$
where $t = \rho + sD(\bar{c},\bar{a}) + s^2R(\bar{a})$. For a given t, the number of shifts for which this value occurs is the number of $a_1, \cdots, a_m$ such that $t = \rho + sD(\bar{c},\bar{a}) + s^2R(\bar{a})$, which is given by Proposition 2.5 as $q^{n-2d-1} + \epsilon\eta(t)q^{n/2-d-1}$.

3. Case A.1 of Theorem 1.4, when $c_m = s = 0$. Here $N(u,v) = q^{n-2}$, so $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = 0$. This value occurs for $q^n - q^{n-d+1}$ shifts.

4. Case B.1 of Theorem 1.4, when $s = 0$ and $c_m \neq 0$. Here
$$\begin{aligned}N(u,v) &= q^{n-2} + (-1)^{Tr_2^q((v+B_{m-1}(\bar{c}))/c_m^2)}q^{(n+d)/2-2} \\ &= q^{n-2} + (-1)^{Tr_2^q((v+\rho)/\sigma^2+1)}q^{(n+d)/2-2},\end{aligned}$$
so
$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = q^{(n+d)/2-2} I(f) \sum_v (-1)^{Tr_2^q(v+1)} G(\sigma^2 v + \rho),$$
after substituting $\sigma^2 v + \rho$ for v. This value occurs for $q^n - q^{n-d+1}$ shifts.

5. Case C.1 of Theorem 1.4, when $c_m = sa_m \neq 0$. Here $N(u,v) = q^{n-2}$, so $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = 0$. This value occurs for $q^{n-d+1} - q^{n-d}$ shifts.

6. Cases C.2 and C.3 of Theorem 1.4, when $c_m \neq sa_m$. Here
$$N(u,v) = q^{n-2} + (-1)^{Tr_2^q((v+su+B_{m-1}(\bar{d}))/d_m^2)}q^{(n+d)/2-2}$$

(recall $\bar{d} = \bar{c} + s\bar{a}$), so

$$\begin{aligned}\Gamma_{\mathbf{S},\mathbf{T}}(\tau) &= q^{(n+d)/2-2}\sum_{u,v}(-1)^{Tr_2^q((v+su+B_{m-1}(\bar{d}))/d_m^2)}F(u)G(v)\\ &= (-1)^{Tr_2^q(B_{m-1}(\bar{d})/d_m^2)}\sum_{u,v}(-1)^{Tr_2^q((v+su)/d_m^2)}F(u)G(v).\end{aligned}$$

We have $Tr_2^q(B_{m-1}(\bar{d})/d_m^2) = 1$ whenever there is a $z \in GF(q)$ such that $Tr_2^q(z) = 1$ and $B_{m-1}(\bar{d})/d_m^2 = z$. There are $q/2$ values of z for which $Tr_2^q(z) = 1$, all nonzero, and for each of these, $B_{m-1}(\bar{d})/d_m^2 = z$ for $q^{n-d-1} - q^{(n-d)/2-1}$ values of $d_1, \cdots, d_{m-1}$ for each fixed nonzero d_m. Therefore, $(-1)^{Tr_2^q(B_{m-1}(\bar{d})/d_m^2)} = -1$ for $(q^{n-d} - q^{(n-d)/2})/2$ values of $a_1, \cdots, a_{m-1}$ and $(-1)^{Tr_2^q(B_{m-1}(\bar{d})/d_m^2)} = 1$ for $(q^{n-d} + q^{(n-d)/2})/2$ values of $a_1, \cdots, a_{m-1}$ for each $a_m \neq c_m/s$. Letting $r = s/(c_m^2 + s^2a_m^2)$, and $t = 1/(c_m^2 + s^s a_m^2)$, we find that $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{u,v}(-1)^{Tr_2^q(ru+tv)}F(u)G(v)$ for $(q^{n-d} + q^{(n-d)/2})/2$ shifts and $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = -\sum_{u,v}(-1)^{Tr_2^q(ru+tv)}F(u)G(v)$ for $(q^{n-d} - q^{(n-d)/2})/2$ shifts for each $r \neq 0$ and $t \neq 0$ in $GF(q)$.

B. Suppose there is an $i > m$ such that $c_i \neq 0$, and $a_{m+1} = \cdots a_n = 0$. Equivalently, $Null(R) \not\subseteq Ker(L)$, and $Null(R) \subseteq Ker(H)$. In this case $N(u,v) = q^{n-2}$ for all u and v by Proposition 3.2, so $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = 0$. This contributes $q^m - 1$ shifts to case B.1 of Theorem 1.2, and case C.1 of Theorem 1.4.

C. Suppose $(c_{m+1}, \cdots, c_n)$ and $(a_{m+1}, \cdots, a_n)$ are linearly independent. Then $N(u,v) = q^{n-2}$ by Proposition 3.1, so $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = 0$. This contributes $q^n - q^{m+1}$ shifts to case B.1 of Theorem 1.2 and case C.1 of Theorem 1.4.

In the remaining cases we may assume that $c_{m+1} = \cdots = c_n = a_{m+1} = \cdots = a_n = 0$ and apply Proposition 3.4 to compute $N(u,v)$.

D. Suppose R has Type I or III and $R(\bar{a}) \neq 0$. Then

$$N(u,v) = \begin{cases} q^{n-2} + \epsilon(-1)^{\phi}q^{n-m/2-1} & \text{if } u \neq D(\bar{a},\bar{c}) \\ q^{n-2} & \text{if } u = D(\bar{a},\bar{c}). \end{cases}$$

where $\phi = Tr_2^q((v + R(\bar{c}))R(\bar{a})/(u^2 + D(\bar{a},\bar{c})^2))$ if $u \neq D(\bar{a},\bar{c})$. Consequently

$$\begin{aligned}\Gamma_{\mathbf{S},\mathbf{T}}(\tau) &= \epsilon\sum_{u\neq D(\bar{a},\bar{c})}\sum_{v}(-1)^{\phi}q^{n-m/2-1}F(u)G(v)\\ &= \epsilon q^{n-m/2-1}\sum_{u\neq 0}\sum_{v}(-1)^{Tr_2^q(vR(\bar{a})/u^2)}F(u+D(\bar{a},\bar{c}))G(v+R(\bar{c}))\end{aligned}$$

where we have substituted $u + D(\bar{a}, \bar{c})$ for u, and $v + R(\bar{c})$ for v. We next let

$$t = D(\bar{a}, \bar{c}) \quad \text{and} \quad s = R(\bar{a}). \tag{16}$$

Thus

$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \epsilon q^{n-m/2-1} \sum_{u \neq 0} \sum_{v} (-1)^{Tr_2^q(sv/u^2)} F(u+t) G(v + R(\bar{c})).$$

This gives case A.3 of Theorem 1.2 and case 2 of Theorem 1.3. To count the number of shifts for which these values occur, we apply Proposition 3.4.1 to equation (16).

E. Suppose R has Type I or III and $R(\bar{a}) = 0$. Then

$$N(u, v) = \begin{cases} q^{n-2} & \text{if } u \neq D(\bar{a}, \bar{c}) \\ q^{n-2} + \epsilon\eta(v + R(\bar{c}))q^{n-m/2-1} & \text{if } u = D(\bar{a}, \bar{c}). \end{cases}$$

Consequently,

$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \epsilon q^{n-m/2-1} F(D(\bar{a}, \bar{c}))(qG(R(\bar{c})) - I(g)).$$

Letting $t = D(\bar{a}, \bar{c})$ and $R(\bar{a}) = 0$, we have

$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = \epsilon q^{n-m/2-1} F(t)(qG(R(\bar{c})) - I(g)).$$

This gives case A.2 of Theorem 1.2 and case 1 of Theorem 1.3. We can again count the number of shifts giving rise to these values by applying Proposition 3.4.1.

F. Suppose R has Type II and $c_m = 0$ (i.e., $Null(D) \subseteq Ker(L)$. Note that in this case $\rho = B_{m-1}(\bar{c})$).

1. If $a_m = 0$, then $N(u, v) = q^{n-2}$ by Proposition 3.4. Hence $\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = 0$. This contributes $q^{n-d} - 1$ shifts to case A.1 of Theorem 1.4.

2. If $a_m \neq 0$, $N(u, v) = q^{n-2} + (-1)^{\pi}\eta(w)q^{n-m/2-3/2}$ where $\pi = Tr_2^q(B_{m-1}(\bar{a})/a_m^2)$ and $w = v + u^2/a_m^2 + \rho + D(\bar{a}, \bar{c})^2/a_m^2$, by Proposition 3.4. Thus,

$$\begin{aligned} \Gamma_{\mathbf{S},\mathbf{T}}(\tau) &= (-1)^{\pi} q^{(n+d)/2-2} (q \sum_{u} F(u) G(\frac{u^2}{a_m^2} + \rho + \frac{D(\bar{a}, \bar{c})^2}{a_m^2}) - I(f)I(g)) \\ &= (-1)^{\pi} q^{(n+d)/2-2} (q \sum_{u} F(a_m u) G(u^2 + \rho + \frac{D(\bar{a}, \bar{c})^2}{a_m^2}) - I(f)I(g)). \end{aligned}$$

   Letting $a_m = s \neq 0$, $B_{m-1}(\bar{a}) = a_m^2 r$, and $\rho + D(\bar{a}, \bar{c})^2/a_m^2 = t$, i.e., $D(\bar{a}, \bar{c}) = a_m(t + \rho)^{1/2}$, we have

$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = (-1)^{Tr_2^q(r)} q^{(n+d)/2-2} (q \sum_{u} F(su) G(u^2 + t) - I(f)I(g)).$$

Counting shifts is now a bit more complicated since we would like to determine which sign occurs, thus eliminating r.

If $c_1 = \cdots = c_{m-1} = 0$, then $t = \rho = 0$. For a fixed s, there are $q/2$ values of r for which $Tr_2^q(r) = 0$, including $r = 0$. Thus there are $(q^{n-d} + q^{(n-d)/2})/2$ shifts with a positive sign, and $(q^{n-d} - q^{(n-d)/2})/2$ shifts with a negative sign.

If the c_i are not all zero, we may apply Proposition 3.4 again for fixed r, s, t. If $\rho = 0$, then this value occurs for q^{n-d-2} shifts if $t \neq 0$, and for $q^{n-d-2} + \eta(r)q^{(n-d)/2-1}$ shifts if $t = 0$. To eliminate r, we collect terms for which $Tr_2^q(r) = 0$. We have a plus sign for $q^{n-d-1}/2$ shifts when $t \neq 0$, and for $(q^{n-d-1} + q^{(n-d)/2})/2$ shifts when $t = 0$. We have a minus sign for $q^{n-d-1}/2$ shifts when $t \neq 0$, and for $(q^{n-d-1} - q^{(n-d)/2})/2$ shifts when $t = 0$.

If $\rho \neq 0$, this value occurs for $q^{n-d-2} + (-1)^{Tr_2^q(\rho r/(t+\rho))}q^{(n-d)/2-1}$ shifts if $t \neq \rho$, and for q^{n-d-2} shifts if $t = \rho$. If $t = \rho$, then each sign occurs for $q^{n-d-1}/2$ shifts, so let $t \neq \rho$ be fixed. Then the number of shifts giving a plus sign is given by

$$\begin{aligned}
&|\{r : Tr_2^q(r) = 0\} \cap \{r : Tr_2^q(\frac{\rho}{t+\rho}r) = 0\}|(q^{n-d-2} + q^{(n-d)/2-1}) \\
&\quad + |\{r : Tr_2^q(r) = 0\} \cap \{r : Tr_2^q(\frac{\rho}{t+\rho}r) = 1\}|(q^{n-d-2} - q^{(n-d)/2-1}) \\
= \;& \frac{q^{n-d-1}}{2} + q^{(n-d)/2-1}(2|\{r : Tr_2^q(r) = 0\} \cap \{r : Tr_2^q(\frac{\rho}{t+\rho}r) = 0\}| - \frac{q}{2}).
\end{aligned}$$

If $t \neq 0$, then the intersection is an intersection of two non-parallel hyperplanes (over $GF(2)$), which has cardinality $q/4$, so this reduces to $q^{n-d-1}/2$. If $t = 0$, then the two hyperplanes coincide, so we have $(q^{n-d-1} + q^{(n-d)/2})/2$ shifts. Similarly, we have $q^{n-d-1}/2$ shifts giving a minus sign if $t \neq 0$, and $(q^{n-d-1} - q^{(n-d)/2})/2$ shifts giving a minus sign if $t = 0$.

G. Finally, suppose R has Type II and $c_m \neq 0$ (i.e., $Null(R) \subseteq Ker(L)$, but $Null(D) \not\subseteq Ker(L)$). We have, according to Proposition 3.4, two cases to consider.

1. If $a_m = 0$, then $N(u, v) = q^{n-2}$ when $u \neq D(\bar{a}, \bar{c}) + c_m R(\bar{a})^{1/2}$, and $N(D(\bar{a}, \bar{c}) + c_m R(\bar{a})^{1/2}, v) = q^{n-2} + (-1)^\mu q^{n-m/2-1/2}$, where $\mu = Tr_2^q((v + B_{m-1}(\bar{c}))/c_m^2)$. Thus

$$\begin{aligned}
\Gamma_{\mathbf{S},\mathbf{T}}(\tau) &= q^{(n+d)/2-1}F(D(\bar{a}, \bar{c}) + c_m R(\bar{a})^{1/2}) \sum_v (-1)^\mu G(v) \\
&= q^{(n+d)/2-1}F(D(\bar{a}, \bar{c}) + \sigma R(\bar{a})^{1/2}) \sum_v (-1)^{Tr_2^q(v+1)} G(\sigma^2 v + \rho),
\end{aligned}$$

where we have substituted $\sigma^2 v+\rho = c_m^2 v + B_{m-1}(\bar{c}) + c_m^2$ for v. Letting $s = D(\bar{a},\bar{c})$ and $r^2 = R(\bar{a}) = B_{m-1}(\bar{a})$, we see that

$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = q^{(n+d)/2-1}F(s+\sigma r)\sum_v (-1)^{Tr_2^q(v+1)}G(\sigma^2 v+\rho).$$

For fixed s and r, the number, K, of shifts that give this value is, according to Propositions 2.4 and 3.4, given by one of the following.

(a) If $L(\bar{x}) = \sigma x_m$, then $s = 0$ and

$$K = \begin{cases} q^{n-d-1} - q^{(n-d)/2-1} & \text{if } r \neq 0 \\ q^{n-d-1} + (q-1)q^{(n-d)/2-1} - 1 & \text{if } r = 0. \end{cases}$$

(b) If $L(\bar{x}) \neq \sigma x_m$ but $B_{m-1}(\bar{c}) = 0$ (i.e., $\rho = \sigma^2$), then

$$K = \begin{cases} q^{n-d-2} & \text{if } s \neq 0 \\ q^{n-d-2} - q^{(n-d)/2-1} & \text{if } s = 0, r \neq 0 \\ q^{n-d-2} + (q-1)q^{(n-d)/2-1} - 1 & \text{if } s = r = 0. \end{cases}$$

(c) If $B_{m-1}(\bar{c}) \neq 0$ (i.e., $\rho \neq \sigma^2$), then

$$K = \begin{cases} q^{n-d-2} + (-1)^{Tr_2^q(B_{m-1}(\bar{c})r^2/s^2)}q^{(n-d)/2-1} & \text{if } s \neq 0 \\ q^{n-d-2} & \text{if } s = 0, r \neq 0 \\ q^{n-d-2} - 1 & \text{if } s = r = 0. \end{cases}$$

Let $t = s + \sigma r$, so

$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = q^{(n+d)/2-1}F(t)\sum_v (-1)^{Tr_2^q(v+1)}G(\sigma^2 v+\rho).$$

To count the number of shifts giving this value we must sum over all s and r such that $t = s+\sigma r$. Suppose first that $L(\bar{x}) = \sigma x_m$. Then $s = 0$, and $t = \sigma r$, so the number of shifts giving this value is $q^{n-d-1} - q^{(n-d)/2-1}$ if $t \neq 0$ and $q^{n-d-1} + (q-1)q^{(n-d)/2-1} - 1$ if $t = 0$.

Suppose next that $L(\bar{x}) \neq \sigma x_m$, but $B_{m-1}(\bar{c}) = 0$. If $t = 0$, then the number of shifts giving this value is $(q-1)q^{n-d-2} + q^{n-d-2} + (q-1)q^{(n-d)/2-1} - 1 = q^{n-d-1} + (q-1)q^{(n-d)/2-1} - 1$. If $t \neq 0$, then the number of shifts giving this value is $(q-1)q^{n-d-2} + q^{n-d-2} - q^{(n-d)/2-1} = q^{n-d-1} - q^{(n-d)/2-1}$.

Suppose last that $B_{m-1}(\bar{c}) \neq 0$. If $t = 0$, then $s = \sigma r$, so the number of shifts giving this value is $(q-1)(q^{n-d-2} + (-1)^{Tr_2^q(B_{m-1}(\bar{c})/\sigma^2)}q^{(n-d)/2-1}) + q^{n-d-2} - 1 = q^{n-d-1} +$

$(-1)^{Tr_2^q(B_{m-1}(\bar{c})/\sigma^2)}(q-1)q^{(n-d)/2-1}-1$. If $t \neq 0$, then the number of shifts giving this value is

$$\begin{aligned}
&\sum_{s\neq 0}(q^{n-d-2}+(-1)^{Tr_2^q(B_{m-1}(\bar{c})\frac{s^2+t^2}{\sigma^2 s^2})}q^{\frac{n-d}{2}-1})+q^{n-d-2}\\
&= q^{n-d-1}+(-1)^{Tr_2^q(\frac{B_{m-1}(\bar{c})}{\sigma^2})}q^{\frac{n-d}{2}-1}\sum_{s\neq 0}(-1)^{Tr_2^q(s)}\\
&= q^{n-d-1}-(-1)^{Tr_2^q(\frac{B_{m-1}(\bar{c})}{\sigma^2})}q^{\frac{n-d}{2}-1}.
\end{aligned}$$

Note that $R(\bar{c}) = B_{m-1}(\bar{c})+\sigma^2$.

2. If $a_m \neq 0$, then $N(u,v) = q^{n-2}+(-1)^{Tr_2^q(B_{m-1}(\bar{a})/a_m^2)}\eta(v+u^2/a_m^2+\sigma u/a_m+\rho+R(\bar{a})\sigma^2/a_m^2+D(\bar{a},\bar{c})\sigma/a_m+D(\bar{a},\bar{c})^2/a_m^2)q^{n-m/2-3/2}$. Thus

$$\begin{aligned}
\Gamma_{\mathbf{S},\mathbf{T}}(\tau) =&\\
&(-1)^{Tr_2^q(B_{m-1}(\bar{a})/a_m^2)}q^{(n+d)/2-2}(q\sum_u F(u)G(\frac{u^2}{a_m^2}+\frac{\sigma u}{a_m}+\rho+\frac{R(\bar{a})\sigma^2}{a_m^2}\\
&+\frac{D(\bar{a},\bar{c})\sigma}{a_m}+\frac{D(\bar{a},\bar{c})^2}{a_m^2})-I(f)I(g))\\
=\ &(-1)^{Tr_2^q(B_{m-1}(\bar{a})/a_m^2)}q^{(n+d)/2-2}(q\sum_u F(a_m u+D(\bar{a},\bar{c}))G(u^2+\sigma u+\rho+\frac{R(\bar{a})\sigma^2}{a_m^2})\\
&-I(f)I(g)),
\end{aligned}$$

where we have substituted $a_m u + D(\bar{a},\bar{c})$ for u. To count shifts, we let $r = a_m$, $s = D(\bar{a},\bar{c})$, and $t = \rho + R(\bar{a})\sigma^2/a_m^2 = \rho+\sigma^2+B_{m-1}(\bar{a})\sigma^2/a_m^2$. Then

$$\Gamma_{\mathbf{S},\mathbf{T}}(\tau) = (-1)^{Tr_2^q((t+\rho)/\sigma^2+1)}q^{(n+d)/2-2}(q\sum_u F(ru+s)G(u^2+\sigma u+t)-I(f)I(g)).$$

If $L(\bar{x}) = \sigma x_m$, then $s=0$ and this value occurs for $q^{n-d-1}+\eta(\frac{t+\rho}{\sigma^2}+1)q^{(n-d)/2-1}$ shifts for each $r\neq 0$ and t in $GF(q)$. If $L(\bar{x}) \neq \sigma x_m$, but $\rho = 0$, this value occurs for q^{n-d-2} shifts for each $r \neq 0$, $s\neq 0$, and t in $GF(q)$ and for $q^{n-d-2}+\eta(\frac{t+\rho}{\sigma^2}+1)q^{(n-d)/2-1}$ shifts for $s=0$ and each $r\neq 0$ and t in $GF(q)$. If $\rho\neq 0$, this value occurs for $q^{n-d-2}+(-1)^{Tr_2^q(r^2(\rho/\sigma^2+1)(t+\rho+\sigma^2)/s^2)}q^{(n-d)/2-1}$ shifts for each $r\neq 0$, $s\neq 0$, and t in $GF(q)$ and for q^{n-d-2} shifts for $s=0$ and each $r\neq 0$ and t in $GF(q)$.

This concludes the proofs of the three main theorems.

6 Linear Complexity

In this section we compute the linear complexity of the geometric sequences considered in the previous section. Our results are based on the work of Zierler and Mills [17] on the linear complexity of algebraic combinations of sequences. Zierler and Mills considered general recurrent sequences over a field F. These are sequences of elements of F (or sequences over F) which satisfy linear recurrences whose coefficients are in F. Let $\mathbf{S}$ be a sequence over F. A recurrence,

$$\forall k \geq 0 : \mathbf{S}_{k+n} = \sum_{i=0}^{n-1} a_i \mathbf{S}_{i+k}, \tag{17}$$

is said to have *length* n. The smallest n such that $\mathbf{S}$ satisfies a recurrence of length n is the *linear complexity* of $\mathbf{S}$, denoted by $\lambda_F(\mathbf{S})$. We will write λ_q for $\lambda_{GF(q)}$. It is well known that if $2\lambda_F(\mathbf{S})$ consecutive elements of $\mathbf{S}$ are known, then $\mathbf{S}$ can be (efficiently) determined by the Berlekamp-Massey algorithm [11]. Thus sequences that are used in cryptographically sensitive applications must have large linear complexities.

If equation (17) is the (necessarily unique) minimal length recurrence satisfied by $\mathbf{S}$, then the *connection polynomial* of $\mathbf{S}$ is the polynomial

$$f_{\mathbf{S}}(t) = t^n - \sum_{i=0}^{n-1} a_i t^i.$$

If we think of t as the shift operator on sequences, then $f_{\mathbf{S}}(t)$ is the unique monic generator of the ideal of annihilators of $\mathbf{S}$ in the ring $F[t]$. If $f_{\mathbf{S}}(t)$ has roots $\alpha_1, \cdots, \alpha_n$ (over an algebraic closure $\bar{F}$ of F), then $\mathbf{S}$ can be written uniquely as

$$\mathbf{S}_i = \sum_{j=1}^{n} c_j \alpha_j^i, \tag{18}$$

for some $c_j \neq 0 \in \bar{F}$. In particular, the number of terms in a representation of $\mathbf{S}$ such as in equation (18) equals the linear complexity.

Zierler and Mills studied these notions from the point of view of the set of sequences annihilated by a polynomial $f(t)$, and considered what polynomials annihilate sums and products of such sets of sequences. Their results can be used to describe the connection polynomials of term-by-term sums and products of pairs of sequences. If $f_1(t)$ and $f_2(t)$ are polynomials, then $(f_1 \vee f_2)(t)$ is the polynomial whose roots are the distinct products $\alpha\beta$, where α is a root of $f_1(t)$ and β is a root of $f_2(t)$. Note that if f_1 and f_2 have coefficients in F, then $f_1 \vee f_2$ does as well, by Galois theory.

Proposition 6.1 *Let $\mathbf{S}$ and $\mathbf{T}$ be linearly recurrent sequences over F. Then*

1. *$f_{\mathbf{S}+\mathbf{T}}$ divides the least common multiple of $f_{\mathbf{S}}$ and $f_{\mathbf{T}}$, and*

$$\lambda_F(\mathbf{S}+\mathbf{T}) \leq \lambda_F(\mathbf{S}) + \lambda_F(\mathbf{T}). \tag{19}$$

If, moreover, $f_{\mathbf{S}}$ and $f_{\mathbf{T}}$ have no roots in common, then $f_{\mathbf{S}+\mathbf{T}} = f_{\mathbf{S}} f_{\mathbf{T}}$ and we have equality in equation (19).

2. *$f_{\mathbf{ST}}$ divides $f_{\mathbf{S}} \vee f_{\mathbf{T}}$ and*

$$\begin{aligned} \lambda_F(\mathbf{ST}) &\leq \lambda_F(\mathbf{S})\lambda_F(\mathbf{T}) \\ &= \text{the number of distinct root products } \gamma\delta,\ \gamma \text{ a root of } f_{\mathbf{S}},\ \delta \text{ a root of } f_{\mathbf{T}}. \end{aligned}$$

If, moreover, all the root products from $f_{\mathbf{S}}$ and $f_{\mathbf{T}}$ are distinct, then $f_{\mathbf{ST}} = f_{\mathbf{S}} \vee f_{\mathbf{T}}$ and $\lambda_F(\mathbf{ST}) = \lambda_F(\mathbf{S})\lambda_F(\mathbf{T})$.

Details of the proofs of this proposition can be found in [9].

In our situation we have two sequences $\mathbf{U}$ and $\mathbf{V}$ over $GF(q)$, defined by

$$\mathbf{U}_i = Tr_q^{q^n}(\gamma\alpha^i) = \sum_{j=0}^{n-1} \gamma^{q^j} \alpha^{iq^j}$$

and

$$\mathbf{V}_i = Tr_q^{q^n}(\delta\alpha^{ki}) = \sum_{j=0}^{n-1} \delta^{q^j} \alpha^{kiq^j},$$

where α is a primitive element of $GF(q^n)$ $\gamma \neq 0 \in GF(q^n)$, $\delta \in GF(q^n)$, and $k \neq 0$. We also have a function $g : GF(q) \to GF(2)$, and define $\mathbf{S}_i = g(\mathbf{U}_i + \mathbf{V}_i)$. We can, however, think of g as having range $GF(q)$ and therefore express it as a polynomial, $g(x) = \sum_{i=0}^{q-1} a_i x^i$. The image of g is in $GF(2)$ if and only if $a_0, a_{q-1} \in GF(2)$, and for $i \leq i \leq q-2$, $a_i^2 = a_{(2i \bmod q-1)}$. It is straightforward, however, to see that $\lambda_2(\mathbf{S}) = \lambda_q(\mathbf{S})$, so from now on we will put no restriction on g. In case $\delta = 0$, the linear complexity of $\mathbf{S}$ has been computed as

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

where $wt(i)$ is the number of ones in the binary expansion of i [2, 9]. We will therefore assume that $\delta \neq 0$. $\mathbf{S}$ can be built from $\mathbf{U}$ and $\mathbf{V}$ by a series of algebraic operations, and we will keep track of what happens to the linear complexity as we do so. For any $k < q^n - 1$, we denote by $\chi(k)$ the number of distinct elements of the form α^{kq^j}, i.e., the size of the Galois coset of α^k. $\chi(k)$ can be computed as the least r such that $q^n - 1$ divides $(q^r - 1)k$. In particular, $\chi(k) = n$ if $\gcd(k, q^n - 1) = 1$.

1. $f_{\mathbf{U}}(t)$ has roots $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ and $\lambda_q(\mathbf{U}) = n$.

2. $f_{\mathbf{V}}(t)$ has roots $\{\alpha^k, \alpha^{kq}, \cdots, \alpha^{kq^{n-1}}\}$ and $\lambda_q(\mathbf{U}) = \chi(k)$.

3. Suppose k is not a power of q. Then $f_{\mathbf{U}}$ and $f_{\mathbf{V}}$ have distinct roots, so $f_{\mathbf{U}+\mathbf{V}} = f_{\mathbf{U}} f_{\mathbf{V}}$, which has roots $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\} \cup \{\alpha^k, \alpha^{kq}, \cdots, \alpha^{kq^{n-1}}\}$. Thus $\lambda_q(\mathbf{U}+\mathbf{V}) = n + \chi(k)$.

4. Suppose $g(x) = x^{2^i}$, and k is not a power of q. Then the roots of $f_{\mathbf{S}}$ are the 2^ith powers of the roots of $f_{\mathbf{U}+\mathbf{V}}$, $\{\alpha^{2^i}, \alpha^{2^i q}, \cdots, \alpha^{2^i q^{n-1}}\} \cup \{\alpha^{2^i k}, \alpha^{2^i kq}, \cdots, \alpha^{2^i kq^{n-1}}\}$ and $\lambda_q(\mathbf{S}) = n + \chi(k)$.

5. Suppose $g(x) = x^b$, $1 \le b \le q-1$, and k is a sum of at least two distinct powers of q. Let $b = \sum_{j=0}^{e-1} b_j 2^j$, $b_j \in \{0,1\}$, $q = 2^e$. Then $\mathbf{S}$ is a product of sequences of the form considered in the preceding paragraph, one for each $b_j = 1$. The set of roots of $f_{\mathbf{S}}(t)$ is thus a subset of
$$C = \{\prod_{b_j=1} \alpha^{2^j k^{r_j} q^{m_j}} = \alpha^{\sum_{b_j=1} 2^j k^{r_j} q^{m_j}} : r_j \in \{0,1\}, 0 \le m_j \le n-1\}.$$
In fact, if $i \ne j$, then $2^i k^{r_i} q^{m_i}$ and $2^j k^{r_j} q^{m_j}$ have no terms in common in their binary expansions. Therefore $2^i k^{r_i} q^{m_i} \not\equiv 2^j k^{r_j} q^{m_j} \pmod{q^n - 1}$, so by Proposition 6.1, C is precisely the set of roots of $f_{\mathbf{S}}(t)$. Similarly, all the root products in C are distinct, so $\lambda_q(\mathbf{S}) = |C| = (n + \chi(k))^{wt(b)}$.

6. A similar argument shows that the sets of root products that arise for distinct bs are disjoint. We have proved

Theorem 6.2 *Let $g : GF(q) \to GF(q)$, $g(x) = \sum_{i=0}^{q-1} a_i x^i$. Let $k < q^n$ be a sum of at least two distinct powers of q, and let $\gamma \ne 0$, $\delta \ne 0$ be elements of $GF(q^n)$. Then the sequence whose ith term is $g(Tr_q^{q^n}(\gamma\alpha^i + \delta\alpha^{ki}))$ has linear complexity*
$$\lambda_q(\mathbf{S}) = \sum_{a_i \ne 0} (n + \chi(k))^{wt(i)}.$$

Thus the linear complexity of these sequences is higher than that of previously studied geometric sequences. $\chi(k)$ can be as large as n, so the largest possible linear complexity we can achieve here is
$$\begin{aligned} \sum_{a_i \ne 0} (2n)^{wt(i)} &= \sum_{r=0}^{\log q} \binom{\log q}{r} (2n)^r \\ &= (2n+1)^{\log q}, \end{aligned}$$

which is approximately $q(n+1)^{\log q}$, i.e., q times greater than the maximum linear complexity achievable with previously studied geometric sequences.

More generally, let $\{k_1, \cdots, k_d\}$ be a set of integers such that each $k_i < q^n$ is a sum of distinct powers of q, and for $i \neq j$, there is no r such that $k_i \equiv q^r k_j \pmod{q^n - 1}$ (this holds, for example, if $wt(k_i) \neq wt(k_j)$). Let

$$\mathbf{S}_i = g(Tr_q^{q^n}(\sum_{j=1}^{d} \gamma_j \alpha^{k_j i})),$$

where $\sum_{i=0}^{q-1} a_i x^i$ and each γ_j is nonzero. Then $\mathbf{S}$ has linear complexity

$$\lambda_q(\mathbf{S}) = \sum_{a_i \neq 0} (\sum_{j=1}^{d} \chi(k_j))^{wt(i)}.$$

7 Conclusions

In this paper we introduce a general class of easily generated binary sequences based on combinations of shift register sequences over a 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 cross-correlations can be minimized either by exhaustive search or by further analysis. It may be possible, for example, to apply these formulas recursively.

We have also expressed the linear complexity of these generalized geometric sequences in terms of algebraic expressions for the feedforward functions. These sequences are seen to have higher linear complexities than standard geometric sequences by a factor of as much as q.

Several questions remain. First, it is as yet unclear whether feedforward functions can be chosen to minimize the cross-correlation values while simultaneously making the linear complexity close to maximal. Second, 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 points in the intersection of pairs of degree two hypersurfaces. 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. Finally, much 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) in which inductive formulas can be found. This would likely lead to sequences with higher linear complexity, since the linear complexity tends to go up both with the number of m-sequences in the linear combination, and with the degree of the decimation.

The geometric sequences studied here are closely related to No sequences [13]. Let $n = 2$, $T = q + 1$ (so α^T is a primitive element of $GF(q)$), $\gcd(r, q-1) = 1$, $g(x) = Tr_2^q(x^r)$, and $\delta \in GF(q^{n_1})$. Then the sequence $\mathbf{V}$ whose ith element is $V_i = g(Tr_q^{q^2}(\alpha^{2i} + \delta\alpha^{Ti}))$ is a No sequence (No and Kumar described their sequences slightly differently, but this description is equivalent). This is not quite the form of sequences studied here due to the squaring of α in the first term. However, it is likely that the cross-correlation of an m-sequence with a No sequence or even more general sequences can be computed using similar techniques. The hope is that we can find large families of sequences with low cross-correlations and high linear complexities.

8 Acknowledgements

The author thanks Mark Goresky and Agnes Chan for many valuable discussions on correlations and related topics. Their feedback and support has been invaluable. The author also thanks Judy Goldsmith for several useful suggestions on the final manuscript.

References

[1] M. Antweiller and L. Bohmer, "Complex sequences over $GF(p^M)$ with a two-level autocorrelation function and a large linear span," manuscript.

[2] L. Brynielsson, "On the linear complexity of combined shift registers," in *Proc. Eurocrypt '84,* pp. 156-160, 1984.

[3] A. H. Chan, and R. Games, "On the linear span of binary sequences from finite geometries, q odd," in *Advances in Cryptology: Proc. Crypto '86, Lecture Notes in Computer Science*, Springer-Verlag: Berlin, pp. 405-417, 1987.

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

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

[6] B. Gordon, W. H. Mills, and L. R. Welch, "Some new difference sets," *Canad. J. Math.* vol. 14 pp. 614-625, 1962.

[7] A. Klapper, A.H. Chan, and M. Goresky, "Cross-correlations of linearly and quadratically related geometric sequences and GMW Sequences," in press, *Discrete Applied Mathematics.*

[8] A. Klapper, A.H. Chan, and M. Goresky, *Cascaded GMW Sequences*, Northeastern Univ. College of Comp. Sci. Tech Report NU-CCS-91-4 and *Proc. Twenty-Eighth Annual Allerton Conference on Communication, Control, and Computing*, 1990.

[9] A. Klapper, "The vulnerability of geometric sequences based on fields of odd characteristic," University of Manitoba Computer Science Department Technical Report #92-1, 1992. Submitted to Crypto '92 and *The Journal of Cryptology.*

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

[11] J.L. Massey, "Shift register sequences and BCH decoding," *IEEE Trans. Info. Thy.* vol. IT-15, pp. 122-127, 1969.

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

[13] 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.* vol. 35, pp. 371-379, 1989.

[14] O. Rothaus, "On bent functions," *Journal of Combinatorial Theory Series A* vol. 20, pp. 300-305, 1976.

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

[16] J. Wolfmann, "New bounds on cyclic codes from algebraic curves," in *Proc. 1988 Conference on Coding Theory and Its Applications,* G. Cohen, J. Wolfmann, Eds., *Lecture Notes in Computer Science Vol. 388*, Springer-Verlag: Berlin, pp. 47-62, 1989.

[17] N. Zierler and W. Mills, "Products of linearly recurring sequences," *Journal of Algebra* vol. 27, pp. 147-157, 1973.

Keywords:
Binary pseudorandom sequences, cross-correlations, linear complexity, cryptography