Partial Period Cross-Correlations of Geometric Sequences

Andrew Klapper*

January 17, 2003

Abstract

The expectations and variances of partial period cross-correlations for certain geometric sequences are estimated. The expectation of the partial period cross-correlations are shown to be proportional to the periodic cross-correlations. Bounds are found for the variance that show that with high probability the partial period cross-correlations are small if the sequences are balanced.

Keywords: Sequences, Cross-Correlations, Partial Period Correlations, Geometric Sequences, Expectation and Variance.

1 Introduction

In order for binary sequences to be usable in CDMA communication systems, it is essential that their partial period cross-correlation values be provably low, yet there are few such results (see [5] and [8] for surveys of known results up to 1985). In this paper we give explicit partial period cross-correlation estimates for certain pairs of binary pseudorandom sequences, geometric sequences whose underlying m-sequences are related by a linear decimation. These results generalize those of Klapper and Goresky on the partial period autocorrelations of geometric sequences [7].

Geometric sequences are obtained by applying a nonlinear "feedforward function" $f : GF(q) \rightarrow GF(2)$ to a linearly recurrent sequence with values in a finite field $GF(q)$. This

*University of Kentucky, Lexington, KY. Project sponsored by the National Security Agency under Grant Number MDA904-91-H-0012. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation hereon. Parts of this paper have appeared in the 31st Annual Allerton Conference on Communication, Control, and Computing.

large class of pseudorandom sequences includes m-sequences [3], GMW sequences [4, 13], Bent sequences [11, 14], cascaded GMW sequences [6], the Chan-Games stream cipher [1] and many others. They are readily generated using shift register hardware, may have enormous linear span [1, 6, 12], and optimally low periodic cross-correlation values [6], so geometric sequences are natural candidates for use in secure spread spectrum applications.

It is well known [14, 8] that the expectations of the partial period cross-correlation values for a periodic sequence are proportional to the periodic cross-correlation values, which have recently been computed for geometric sequences in the case in question [2]. Thus, if the geometric sequences are chosen so as to have low periodic cross-correlations, the same will be true for the averaged partial period cross-correlation values. This is only useful, however, if we further know that the variance of the partial period cross-correlations is low.

In this paper we consider geometric sequences whose underlying m-sequences are related by a linear decimation, but whose feedforward functions may be distinct. We show that the variance of the partial period cross-correlations is small. We do so by giving an estimate on the variance which does not involve any knowledge of the feedforward functions. We compute the expectation and variance of these partial period correlations based on a distribution in which the window size, D, is kept fixed and the start position of the window is allowed to vary uniformly. This is analogous to the distribution used previously in the case of m-sequences [14]. Several authors who have studied similar questions have averaged these correlation values over all possible start positions *and* all possible shifts τ. The double averaging results in a somewhat easier expression to evaluate but the resulting information may be less significant than that which is derived here.

Let $q = p^e$ be a power of a prime number p, let $n > 0$, and let $\mathbf{S}$ and $\mathbf{T}$ be geometric sequences of period $q^n - 1$ whose underlying m-sequences over $GF(q)$ are related by a linear (that is, a power of p) decimation. The partial period cross-correlation of $\mathbf{S}$ and $\mathbf{T}$ with shift τ, start position k, and window size D is denoted $\Theta_{\mathbf{S},\mathbf{T}}(\tau, k, D)$. The expected partial period cross-correlation is $D/(q^n - 1)$ times the full period cross-correlation. Thus if the full period cross-correlations are small, so are the average partial period cross-correlations. This does not necessarily mean that the partial period cross-correlations are also small. Large positive and negative values might cancel when we compute the expectation. However, Chebyshev's inequality says that for any random variable X and $\epsilon > 0$, $Prob(|X - E[X]| > \epsilon) < V(X)/\epsilon^2$, where $E[X]$ denotes the expectation of X and $V(X)$ denotes the variance of X. Our main result is that

$$V(\Theta_{\mathbf{S},\mathbf{T}}(\tau, k, D)) \leq \frac{q^n D}{q^n - 1} \left\lceil \frac{(q-1)D}{q^n - 1} \right\rceil (q^2 + q + 1).$$

This makes it possible to obtain bounds on $\Theta_{\mathbf{S},\mathbf{T}}(\tau, k, D)$ which hold with high probability in many instances. For $D \leq (q^n - 1)/(q - 1)$ the bound on the variance is approximately $D(q^2 + q + 1)$. For $D \leq q^2 + q + 1$, this gives no information – the partial period cross-correlation is at most the window size, so Chebyshev's inequality only gives information if $\epsilon > D$. For $q^2+q+1 < D \le (q^n-1)/(q-1)$, various choices of ϵ give interesting bounds. For example, the probability that the partial period cross-correlation differs from its expectation by more than $\epsilon = (q^2+q+1)D^{1/2}$ is at most $1/(q^2+q+1)$. More generally, we get meaningful bounds as long as $\lceil (q-1)D/(q^n-1) \rceil (q^2+q+1) < D$. For $n \le 3$, this never holds, but for $n \ge 4$, this holds whenever $D \ge (q^n-1)/(q-1)$. For example, if we take $D = (q^n-1)/2$ (or half the period) and $\epsilon = (q^{n+2}(q^2+q+1))^{1/2}$ (or about the square root of the window size), then we get that the probability the partial period cross-correlation differs from its expectation by more than ϵ is at most $1/(4q)$.

2 Geometric Sequences and Correlations

In this section we recall the definition of geometric sequences and some of their basic properties, and the definition of full and partial period cross-correlation functions of periodic sequences. Geometric sequences are based on algebra over finite fields, and we recall first some of the basic concepts we use. See Lidl and Niederreiter's or McEliece's book [9, 10] for a more detailed treatment of finite fields.

Let $q = p^e$ be a fixed power of a prime number p, and let $GF(q)$ denote the Galois field with q elements. For any $n \ge 1$, we denote the *trace function* from $GF(q^n)$ to $GF(q)$ by $Tr_q^{q^n}$, defined by $Tr_q^{q^n}(x) = \sum_{i=0}^{n-1} x^{q^i}$.

We fix a prime power q, an integer n, and a primitive element $\alpha \in GF(q^n)$. The infinite periodic sequence $\mathbf{U}$ whose ith term is $\mathbf{U}_i = Tr_q^{q^n}(\alpha^i) \in GF(q)$ an m-sequence over $GF(q)$ of span n. If $f : GF(q) \to GF(2)$ is any function, then the binary sequence $\mathbf{S}$ whose ith term is $\mathbf{S}_i = f(\mathbf{U}_i)$ is the *geometric sequence* based on the primitive element α and feedforward function f.

A geometric sequence is a binary periodic sequence whose period divides q^n-1. Geometric sequences with q even have been suggested for use in spread spectrum communication systems, due to their (in some cases) optimal cross-correlations, excellent cross-correlation values, and relatively high linear spans. They include commonly studied sequences such as Bent sequences, GMW sequences, and Cascaded GMW sequences, and are closely related to No sequences. The geometric sequence $\mathbf{S}$ is easy to generate if the feedforward function f is easy to compute. If $g : GF(q) \to GF(2)$ is a second function, and $\beta = \alpha^k$ another primitive element in $GF(q^n)$, we denote by $\mathbf{T}$ the geometric sequence whose ith term is

$$\mathbf{T}_i = g(Tr_q^{q^n}(\beta^i)).$$

The sequence $Tr_q^{q^n}(\beta^i)$ is a "linear decimation" of $\mathbf{U}$. In this case

$$\mathbf{T}_i = g(Tr_q^{q^n}(\alpha^{ip^e})) = g((Tr_q^{q^n}(\alpha^i))^{p^e}),$$

so if we replace $g(x)$ by $g'(x) \stackrel{def}{=} g(x^{p^e})$, we can assume that the underlying m-sequences of the two geometric sequences are the same.

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

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau) = \sum_{i=1}^{q^n-1} (-1)^{\mathbf{S}_i}(-1)^{\mathbf{T}_{i+\tau}}.$$

Chan, Goresky, and Klapper [2] computed the cross-correlations of certain pairs of geometric sequence, and we recall the result. We use the notation: $F(x) = (-1)^{f(x)}$, $I(f) = \sum_{x\in GF(q)} F(x)$, the *imbalance* of f (and similarly for g and g'), and

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

the *short cross-correlation function*[1] of f and g. Set $\nu = (q^n-1)/(q-1)$. Then $\alpha^\tau \in GF(q^n)$ lies in the subfield $GF(q)$ if and only if τ is a multiple of ν.

Theorem 2.1 *The cross-correlations of the* $\mathbf{S}$ *and* $\mathbf{T}$ *are:*

1. $\Theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-2}I(f)I(g) - F(0)G(0)$, *if* τ *is not a multiple of* ν.
2. $\Theta_{\mathbf{S},\mathbf{T}}(\tau) = q^{n-1}\Delta_{\alpha^\tau}^e(f,g) - F(0)G(0)$, *if* τ *is a multiple of* ν.

Thus if q is even, $\mathbf{S}$ or $\mathbf{T}$ is balanced (i.e. $I(f)=0$ or $I(g)=0$), and τ is not a multiple of ν, then the cross-correlation of $\mathbf{S}$ and $\mathbf{T}$ with shift τ is -1.

The partial period cross-correlation of a sequence is defined by limiting the range of values in the sum defining the periodic cross-correlation to a fixed window. It is parametrized by the start position k and length D of the window, as well as the shift τ:

$$\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D) = \sum_{i=k}^{D+k-1} (-1)^{\mathbf{S}_i}(-1)^{\mathbf{T}_{i+\tau}}.$$

3 Main Theorems

In this section we state precisely and prove our main theorems. All expectations are taken for fixed window size D and shift τ, assuming a uniform distribution on all start positions k.

[1]If γ is a primitive element of $GF(q)$, and $a = \gamma^\sigma$, then $\Delta_a^e(f) - F(0)G(0)$ is the cross-correlation with shift σ of the sequence whose ith term is $f(\gamma^i)$ and the sequence whose ith term is $g(\gamma^{ip^e})$.

Theorem 3.1 *The expected partial period cross-correlation of* $\mathbf{S}$ *and* $\mathbf{T}$ *is*

1. $E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)] = D(q^{n-2}I(f)I(g) - F(0)G(0)))/(q^n-1)$ *if* τ *is not a multiple of* ν.
2. $E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)] = D(q^{n-1}\Delta^e_{\alpha^\tau}(f,g) - F(0)G(0))/(q^n-1)$ *if* τ *is a multiple of* ν.

Proof: For any sequences $\mathbf{S}$ and $\mathbf{T}$ of period N, the expectation of the partial period cross-correlation is given by $E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)] = (1/N)\sum_{k=0}^{N-1}\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)$. An interchange of summations shows that $E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)] = (D/N)\Theta_{\mathbf{S},\mathbf{T}}(\tau)$. Combining this with Theorem 2.1 gives the result. □

The variance of a random variable X is defined as $V(X) = E[(X-E[X])^2] = E[X^2] - E[X]^2$, and is a measure of the deviation of X from its expectation. Thus to compute the variance we must determine the second moment $E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2]$. For any $s \in GF(q)$ and $A \neq 0 \in GF(q^n)$, we let

$$H^s_A = \{x \in GF(q^n) : Tr^{q^n}_q(Ax) = s\}.$$

This can be interpreted as an affine hyperplane over $GF(q)$ in $GF(q^n)$. The second moment of the partial period cross-correlation can be expressed in terms of the cardinalities of certain fourfold intersections of these sets.

Lemma 3.2 *If* $\mathbf{S}$ *and* $\mathbf{T}$ *are geometric sequences, then*

$$E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2] =$$
$$\frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\left(\sum_{s,t,u,v\in GF(q)} N_{i,j,\tau}(s,t,u,v)F(s)G'(t)F(u)G'(v) - 1\right), \quad (1)$$

where $N_{i,j,\tau}(s,t,u,v) = |H^s_{\alpha^i} \cap H^t_{\alpha^{i+\tau}} \cap H^u_{\alpha^j} \cap H^v_{\alpha^{j+\tau}}|$.

Proof: The proof is essentially an interchange of summations.

$$E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2] = \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2$$
$$= \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}(\sum_{i=k}^{k+D-1}F(Tr^{q^n}_q(\alpha^i))G'(Tr^{q^n}_q(\alpha^{i+\tau})))^2$$
$$= \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}\sum_{i,j=k}^{k+D-1}F(Tr^{q^n}_q(\alpha^i))G'(Tr^{q^n}_q(\alpha^{i+\tau}))F(Tr^{q^n}_q(\alpha^j))G'(Tr^{q^n}_q(\alpha^{j+\tau}))$$

$$= \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}\sum_{i,j=0}^{D-1} F(Tr_q^{q^n}(\alpha^{i+k}))G'(Tr_q^{q^n}(\alpha^{i+k+\tau}))F(Tr_q^{q^n}(\alpha^{j+k}))G'(Tr_q^{q^n}(\alpha^{j+k+\tau}))$$

$$= \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\sum_{k=0}^{q^n-2} F(Tr_q^{q^n}(\alpha^{i+k}))G'(Tr_q^{q^n}(\alpha^{i+k+\tau}))F(Tr_q^{q^n}(\alpha^{j+k}))G'(Tr_q^{q^n}(\alpha^{j+k+\tau}))$$

$$= \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\sum_{x\in GF(q^n)^*} F(Tr_q^{q^n}(\alpha^{i}x))G'(Tr_q^{q^n}(\alpha^{i+\tau}x))F(Tr_q^{q^n}(\alpha^{j}x))G'(Tr_q^{q^n}(\alpha^{j+\tau}x)).$$

Set $s = Tr_q^{q^n}(\alpha^i x)$, $t = Tr_q^{q^n}(\alpha^{i+\tau}x)$, $u = Tr_q^{q^n}(\alpha^j x)$, and $v = Tr_q^{q^n}(\alpha^{j+\tau}x)$. Then the sum can be rewritten

$$E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2] = \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\left(\sum_{s,t,u,v\in GF(q)} N_{i,j,\tau}(s,t,u,v)F(s)G'(t)F(u)G'(v)-1\right).$$

□

The results of [7], which we next review, give the number of times that $N_{i,j,\tau}(s,t,u,v)$ is nonzero and its nonzero values for each i, j, and τ. There are three cases depending on whether $\alpha^\tau \in GF(q)$, $\alpha^\tau \in GF(q^2) - GF(q)$, or $\alpha^\tau \in GF(q^n) - GF(q^2)$. For each of these three cases we need to know the number of times each value of $N_{i,j,\tau}(s,t,u,v)$ occurs. This allows us to decompose the sum in equation (1) according to the values of $N_{i,j,\tau}(s,t,u,v)$. Fix i, j, τ, with $0 \le i,j < D$, $0 \le \tau \le q^n - 2$. There are five possible values for $N_{i,j,\tau}(s,t,u,v)$: q^{n-4}, q^{n-3}, q^{n-2}, q^{n-1}, and 0.

Lemma 3.3 *(see [7]) $N_{i,j,\tau}(s,t,u,v)$ is nonzero exactly when (s,t,u,v) is in the image of the function*

$$L_{i,j,\tau}(x) = (Tr_q^{q^n}(\alpha^i x), Tr_q^{q^n}(\alpha^{i+\tau}x), Tr_q^{q^n}(\alpha^j x), Tr_q^{q^n}(\alpha^{j+\tau}x)).$$

If r is the dimension of this image, then for each such (s,t,u,v), we have $N_{i,j,\tau} \stackrel{def}{=} N_{i,j,\tau}(s,t,u,v) = q^{n-r}$.

There is an action of the general linear group over $GF(q)$ of rank two, $\Gamma = GL_2(GF(q))$, on $GF(q^n)$. The Γ-*orbit* of an element $x \in GF(q^n)$ under this action is denoted orbit(x). This action can be used to describe the cardinalities of the sets $N_{i,j,\tau}(s,t,u,v)$ as follows.

Lemma 3.4 *(see [7]) In the following table, each row corresponds to certain values of i, j, and τ. For a given τ, W is the number of i, j in the given row, and $\nu_2 = (q^n-1)/(q-1)$.*

$\alpha^\tau \in$	$\alpha^{j-i} \in$	$N_{i,j,\tau}$	W
$GF(q)$	$GF(q)$	q^{n-1}	$\leq D\lceil D/\nu \rceil$
	elsewhere	q^{n-2}	*all others*
$GF(q^2)-GF(q)$	$GF(q)$	q^{n-2}	$\leq D\lceil D/\nu \rceil$
	orbit(α^τ)	q^{n-2}	$\leq D\lceil D/\nu_2 \rceil$
	elsewhere	q^{n-4}	*all others*
$GF(q^n)-GF(q)$	$GF(q)$	q^{n-2}	$\leq D\lceil D/\nu \rceil$
	orbit(α^τ)	q^{n-3}	$\leq D\lceil D/\nu \rceil (q^2+q)$
	elsewhere	q^{n-4}	*all others*

We can now prove our main theorem.

Theorem 3.5 *For any τ, the variance of the partial period cross-correlation of geometric sequences $\mathbf{S}$ and $\mathbf{T}$ with shift τ and window size D is bounded above by*

$$\frac{q^n D}{q^n-1}\left\lceil \frac{(q-1)D}{q^n-1} \right\rceil (q^2+q+1).$$

If f or g is balanced, this can be reduced to

$$\frac{q^n D}{q^n-1}\left\lceil \frac{(q-1)D}{q^n-1} \right\rceil \frac{(q^2+q+2)}{2}.$$

Proof: We break down the computation of the variance into cases depending on whether α^τ is in $GF(q)$, $GF(q^2)-GF(q)$, or $GF(q^n)-GF(q^2)$. If n is odd, then $GF(q^2)$ is not a subfield of $GF(q^n)$, so the middle case does not occur. We treat in detail only the most difficult case, when $\alpha^\tau \in GF(q^n)-GF(q^2)$. The seventh row of the table in Lemma 3.4 gives rise to the leading term in our estimate for the variance.

We bound the second moment as follows

$$E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2] = \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\left(\sum_{s,t,u,v\in GF(q)} N_{i,j,\tau}(s,t,u,v)F(s)G'(t)F(u)G'(v)-1\right)$$

$$= \frac{1}{q^n-1}\left(\sum_{i,j=0}^{D-1}\left(\sum_{s,t,u,v\in GF(q)} q^{n-4}F(s)G'(t)F(u)G'(v)-1\right)\right.$$

$$+\sum_{\substack{0\leq i,j<D \\ \alpha^{j-i}\in \mathrm{orbit}(\alpha^\tau)}}\left(\sum_{\substack{s,t,u,v\in \\ \mathrm{image}(L_{i,j,\tau})}} q^{n-3}F(s)G'(t)F(u)G'(v)\right.$$

$$
\begin{aligned}
& \qquad - \sum_{s,t,u,v \in GF(q)} q^{n-4} F(s)G'(t)F(u)G'(v) \Bigg) \\
& + \sum_{\substack{0 \le i,j < D \\ \nu | (i-j)}} \left(\sum_{\substack{s,t,u,v \in \\ \text{image}(L_{i,j,\tau})}} q^{n-2} F(s)G'(t)F(u)G'(v) \right. \\
& \qquad \left. - \sum_{s,t,u,v \in GF(q)} q^{n-4} F(s)G'(t)F(u)G'(v) \right) \Bigg) \\
\le\ & \frac{D^2}{q^n - 1}(q^{n-4} I(f)^2 I(g)^2 - 1) + \frac{D \lceil D/\nu \rceil}{q^n - 1}(q^2 + q + 1)(q^n - q^{n-4} I(f)^2 I(g)^2).
\end{aligned}
$$

The expectation in this case is

$$
\frac{D}{q^n - 1}(q^{n-2} I(f) I(g) - 1).
$$

Therefore the variance is

$$
\begin{aligned}
& V(\Theta_{\mathbf{S},\mathbf{T}}(\tau, k, D)) = E[\Theta_{\mathbf{S},\mathbf{T}}(\tau, k, D)^2] - E[\Theta_{\mathbf{S},\mathbf{T}}(\tau, k, D)]^2 \\
\le\ & \frac{D^2}{q^n - 1}(q^{n-4} I(f)^2 I(g)^2 - 1) + \frac{D \lceil D/\nu \rceil}{q^n - 1}(q^2 + q + 1)(q^n - q^{n-4} I(f)^2 I(g)^2) \\
& - \frac{D^2}{(q^n - 1)^2}(q^{n-2} I(f) I(g) - 1)^2 \\
=\ & \frac{q^{n-4} D \lceil D/\nu \rceil}{q^n - 1}(q^2 + q + 1)(q^4 - I(f)^2 I(g)^2) - \frac{D q^{n-4}}{(q^n - 1)^2}(q^2 - I(f) I(g))^2 \\
\le\ & \frac{q^n D}{q^n - 1} \left\lceil \frac{(q-1)D}{q^n - 1} \right\rceil (q^2 + q + 1).
\end{aligned}
$$

Furthermore, when one of the feedforward functions is balanced (that is, $I(f) = 0$ or $I(g) = 0$), we can guarantee a certain amount of cancellation. Specifically, if f or g is balanced, then for any D and τ such that $\alpha^\tau \notin GF(q^2)$,

$$
\sum_{\substack{0 \le i,j < D \\ \alpha^{j-i} \in \text{orbit}(\alpha^\tau)}} \sum_{\substack{s,t,u,v \in \\ \text{image}(L_{i,j,\tau})}} F(s)G'(t)F(u)G'(v) \le \frac{D \lceil D/\nu \rceil (q^2 + q)}{2} q^3.
$$

The proof of this is similar to that of Lemma 16 of [7]. This gives the reduction by a factor of almost one half in the second assertion of the theorem.

When $\alpha^\tau \in GF(q)$ (that is, case (1) of Lemma 3.4), we have

$$E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2] \le \frac{D^2}{q^n-1}(q^{n-2}\Delta^e_{\alpha^\tau}(f,g)^2-1)+\frac{D}{q^n-1}(\frac{D-1}{\nu}+1)q^n.$$

The expectation in this case is

$$\frac{D}{q^n-1}(q^{n-1}\Delta^e_{\alpha^\tau}(f,g)-1).$$

Therefore the variance is bounded by:

$$V(\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)) \le \frac{q^n D}{q^n-1}(\frac{D-1}{\nu}+1),$$

which is approximately $D^2/q^{n-1}+D$.

When $\alpha^\tau \in GF(q^2)-GF(q)$ (that is, case (2) of Lemma 3.4), we have

$$E[\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)^2] \le \frac{D^2}{q^n-1}(q^{n-4}I(f)^2I(g)^2-1)+\frac{D}{q^n-1}(\frac{D-1}{\nu_2}+1)(q^n-q^{n-4}I(f)^2I(g)^2).$$

The expectation in this case is

$$\frac{D}{q^n-1}(q^{n-2}I(f)I(g)-1).$$

Therefore the variance is bounded by:

$$V(\Theta_{\mathbf{S},\mathbf{T}}(\tau,k,D)) \le \frac{q^n D}{q^n-1}(\frac{D-1}{\nu_2}+1).$$

This concludes the proof of Theorem 3.5. □

References

[1] A. H. Chan and R. Games, On the linear span of binary sequences from finite geometries, q odd, *in Proceedings of Crypto 1986,* pp. 405-417, Santa Barbara.

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

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

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

[5] T. Hoholdt, H. E. Jensen, and J. Justesen, Aperiodic correlations and the merit factor of a class of binary sequences, *IEEE Trans. on Inf. Th.* **31** (1985), pp. 549-552.

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

[7] A. Klapper and M. Goresky, Partial period autocorrelations of geometric sequences, in press, *IEEE Trans. Inf. Thy.*

[8] P. V. Kumar, The partial-period correlation moments of arbitrary binary sequences, *GLOBECOM '85*, IEEE Global Telecommunications Conference – Conference Record, IEEE Publications, N.Y., New York (1985).

[9] R. Lidl and H. Niederreiter, *Finite Fields, 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] O. Rothaus, On bent functions, *J. of Combinatorial Theory, Series A* **20** (1976), pp. 300-305.

[12] R. A. Rueppel *Analysis and Design of Stream Ciphers*, Springer Verlag, New York, 1986.

[13] R. A. Scholtz and L. R. Welch, GMW sequences, *IEEE Trans. Inf. Theory* **IT-30**, pp. 548-553.

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

Table from Lemma 3, Page 10

$\alpha^\tau \in$	$\alpha^{j-i} \in$	$N_{i,j,\tau}$	W
$GF(q)$	$GF(q)$	q^{n-1}	$\leq D\lceil D/\nu \rceil$
	elsewhere	q^{n-2}	all others
$GF(q^2)-GF(q)$	$GF(q)$	q^{n-2}	$\leq D\lceil D/\nu \rceil$
	orbit(α^τ)	q^{n-2}	$\leq D\lceil D/\nu_2 \rceil$
	elsewhere	q^{n-4}	all others
$GF(q^n)-GF(q)$	$GF(q)$	q^{n-2}	$\leq D\lceil D/\nu \rceil$
	orbit(α^τ)	q^{n-3}	$\leq D\lceil D/\nu \rceil (q^2+q)$
	elsewhere	q^{n-4}	all others

Footnote from page 6

If γ is a primitive element of $GF(q)$, and $a = \gamma^\sigma$, then $\Delta_a^e(f) - F(0)G(0)$ is the cross-correlation with shift σ of the sequence whose ith term is $f(\gamma^i)$ and the sequence whose ith term is $g(\gamma^{ip^e})$.