Partial Period Autocorrelations of Geometric Sequences*

Andrew Klapper† Mark Goresky‡

Abstract

For a binary pseudorandom sequence $\{\mathbf{S}_i\}$ with period N, the partial period autocorrelation function $A_{\mathbf{S}}(\tau, k, D)$ is defined by correlating the portion of the sequence within a window of size D, and start position k, with the portion in another window of the same size but starting τ steps later in the sequence. A distribution of possible partial period autocorrelation values is obtained by allowing the start position k to vary over all possible values $0 \leq k < N$. The expectation value is proportional to the periodic autocorrelation function $A_{\mathbf{S}}(\tau)$. In this paper the variance in the partial period autocorrelation values is estimated for a large class of binary pseudorandom sequences, the so-called "geometric sequences ". An estimate is given for the minimum window size D which is needed in order to guarantee (with probability of error less than ϵ), that a signal has been synchronized, based on measurement of a single partial period autocorrelation value.

Keywords: Binary Sequence, Aperiodic Autocorrelation, Finite Fields, Spread Spectrum, Synchronization.

1 Introduction

During the last 30 years, a number of efforts have been made at understanding partial period correlation properties of binary pseudorandom sequences. Even today, explicit results are known for only a limited collection of sequences, and these have been difficult to arrive at.

*Parts of this work have been presented at Asiacrypt '91, November, 1991

†University of Kentucky, Lexington, KY, 40506, Northeastern University, and the University of Manitoba. Project sponsored by the National Security Agency under Grant Number MDA904-91-H-0012.

‡Northeastern University, Boston, MA 02115.

(See [9] and [5] for surveys of known results up to 1985.) In this paper we formulate explicit partial period autocorrelation estimates for a large class of binary pseudorandom sequences, the so-called *geometric* sequences. These are obtained by starting with a linear recurrence sequence (or "linear feedback shift register sequence") with values in a finite field $GF(q)$, and filtering the output through a nonlinear "feedforward function" $f : GF(q) \to GF(2)$ which takes binary values. This large class of pseudorandom sequences includes m-sequences [3], GMW sequences [4, 17], Bent sequences [15, 18], cascaded GMW sequences [7], the Chan-Games stream cipher [1] and many others. Because they are readily generated using shift register hardware, may have enormous linear span ([7], [1], [16]), and optimally low periodic autocorrelation values ([7]), the geometric sequences are natural candidates for use in secure spread spectrum applications. Knowledge of their partial period correlation properties is desired for demodulation, synchronization, and evaluation of their cryptographic security (see [16] , [18], and [1]).

It is well known ([18], [9]) that the expected value of the partial period autocorrelation values for a periodic sequence is proportional to the periodic autocorrelation values, which have recently been computed for geometric sequences in general [2]. Thus, if the geometric sequence is chosen so as to have low periodic autocorrelation, the same will be true for the averaged partial period autocorrelation values. However, this information is of little value without further knowledge of the spread of possible values of the partial period autocorrelations. In this paper we compute the expected value and the variance (or second moment) of these partial period values, in a manner analogous to that of [18], where the case of m-sequences was studied. We will show that, for geometric sequences, the variance in partial period autocorrelation values is very small, by giving an estimate on the variance which does not involve any knowledge of the parameters in the feedforward function f.

If $\{\mathbf{S}_1, \mathbf{S}_2, \ldots\}$ is a periodic binary pseudorandom sequence, a *partial period autocorrelation value* is obtained by correlating the portion of the sequence which appears within a "window" of size D, which starts at position k, with the portion of the sequence appearing in another window of the same size, but shifted τ steps later in the sequence. In this paper, "expectation values" are obtained by averaging these values over all possible *start* positions k. Several authors who have studied similar questions average 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 valuable than that which is derived here.

The authors would like to thank Agnes Chan for indicating to us the importance of these questions and W. Casselman for useful conversations.

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 autocorrelation functions of periodic sequences. Geometric sequences are based on algebra over finite fields, and we recall first some of the basic concepts we will use. See Lidl and Niederreiter's or McEliece's book [11, 12] for a more detailed treatment of finite fields.

Let q be a fixed power of a prime number, and let $GF(q)$ denote the Galois field with q elements. We consider this to be a "base" field. For any $n \geq 1$, we denote the *trace function* from $GF(q^n)$ to $GF(q)$ by $Tr_q^{q^n}$, defined by $Tr_q^{q^n}(x) = \sum_{i=0}^{n-1} x^{q^i}$. Then $Tr_q^{q^n}$ is a $GF(q)$-linear function, and 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 $A \in GF(q^n)$. For any $m \geq 1$ we have, $Tr_q^{q^{nm}}(x) = Tr_q^{q^n}(Tr_{q^n}^{q^{nm}}(x))$.

Let α be a primitive element of $GF(q^n)$. This means that every nonzero element of $GF(q^n)$ is some power of α. The infinite periodic sequence $\mathbf{U}$ whose ith term is $\mathbf{U}_i = Tr_q^{q^n}(\alpha^i) \in GF(q)$ is known as an *m-sequence* over $GF(q)$ of span n [11]. (The familiar case of a *binary* m-sequence is obtained by taking $q = 2$.) We may also consider the sequence whose ith term is $Tr_q^{q^n}(A\alpha^i)$ for some fixed element A of $GF(q^n)$. This amounts to a cyclic shift of the first sequence, so we do not consider it to be a distinct sequence here. Note, however, that changing the primitive element α may result in a completely different m-sequence. It is well known that every m-sequence can be generated by a "linear recurrence", or a linear feedback shift register of length n over $GF(q)$. It has period $q^n - 1$, the maximum possible period for a sequence generated by a linear feedback shift register of length n over $GF(q)$. Moreover, every maximal period linear recurrence sequence is (a shift of) an m-sequence [11, pp. 394-410].

Throughout this paper we fix a prime power q, an integer n, a primitive element $\alpha \in GF(q^n)$, and a (possibly nonlinear) "feedforward function" $f : GF(q) \to GF(2)$.

Definition 2.1 (Chan and Games [1]) *The binary sequence* $\mathbf{S}$ *whose ith term is*

$$\mathbf{S}_i = f(Tr_q^{q^n}(\alpha^i)).$$

is the geometric sequence based on the primitive element α *and feedforward function* f.

Such 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 autocorrelations, excellent cross-correlation values, and relatively high linear complexities. Geometric sequences with q odd have been used in applications where easily generated sequences with large linear complexities are needed. The geometric sequence $\mathbf{S}$ is easy to generate if the feedforward function f is easy to compute.

Definition 2.2 *The periodic autocorrelation function $\mathcal{A}_{\mathbf{S}}(\tau)$ of $\mathbf{S}$ is the function whose value at τ is the correlation of the τ-shift of $\mathbf{S}$ with itself.*

$$\mathcal{A}_{\mathbf{S}}(\tau) = \sum_{i=1}^{q^n-1} (-1)^{\mathbf{S}_{i+\tau}} (-1)^{\mathbf{S}_i}$$

We next recall a result due to Chan, Goresky, and Klapper [2] regarding the autocorrelation of a geometric sequence. We use the following notation: $F(x) = (-1)^{f(x)}$ (for $x \in GF(q)$), $I(f) = \sum_{x \in GF(q)} F(x)$, the *imbalance*[1] of f, and $\Delta_a(f) = \sum_{x \in GF(q)} F(ax)F(x)$, the *short autocorrelation function*[2] of f. Set $\nu = (q^n-1)/(q-1)$. Then $\alpha^\tau \in GF(q^n)$ lies in the subfield $GF(q) \iff \tau$ is a multiple of ν.

Theorem 2.3 *The values for the periodic autocorrelation (with shift $\tau \neq 0$) of the geometric sequence $\mathbf{S}$ are:*

1. $\mathcal{A}_{\mathbf{S}}(\tau) = q^{n-2} I(f)^2 - 1$, *if τ is not a multiple of ν.*
2. $\mathcal{A}_{\mathbf{S}}(\tau) = q^{n-1} \Delta_{\alpha^\tau}(f) - 1$, *if ν divides τ.*

Corollary 2.4 *Assume the geometric sequence $\mathbf{S}$ is as balanced as possible, i.e. $I(f) = \pm 1$ if q is odd, and $I(f) = 0$ if q is even. Then for a shift τ that is not a multiple of ν, the periodic autocorrelation of $\mathbf{S}$ is*

$$\mathcal{A}_{\mathbf{S}}(\tau) = q^{n-2} - 1$$

if q is odd, and

$$\mathcal{A}_{\mathbf{S}}(\tau) = -1$$

if q is even. Furthermore, for q even it is possible to choose f so that $\Delta_{\alpha^\tau}(f) = 0$ when $\tau \neq 0$ and $\nu | \tau$ [7]. For such an f, $\mathcal{A}_{\mathbf{S}}(\tau) = -1$ whenever $\tau \neq 0$.

Thus, if q is odd, the autocorrelations are high. This fact, together with the submaximal linear complexity, has been exploited in a cryptologic attack on geometric sequences – the high autocorrelation is used to determine q with high probability [8]. In fact, a more powerful attack can be launched using imbalance properties of these sequences [6]. When q is even, the feedforward function f can be chosen to be balanced, and the shifted autocorrelations are optimal for certain applications.

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

[1] The imbalance of f is equal to the number of x for which $f(x) = 0$ minus the number of x for which $f(x) = 1$.

[2] If γ is a primitive element of $GF(q)$, and $a = \gamma^\sigma$, then $\Delta_a(f) - 1$ is the autocorrelation with shift σ of the sequence whose ith term is $f(\gamma^i)$.

Definition 2.5 *The partial period autocorrelation function of a periodic sequence* $\mathbf{S}$ *is defined to be*

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

It is often hopeless to expect a precise expression for the partial period autocorrelation. We will show, however, that the expected partial period autocorrelation (averaged over the starting position k of the window) is closely related to the full period autocorrelation. We will also show that for certain window sizes the variance of the partial period autocorrelation (with fixed shift τ and window size D, but varying start position k) is low. Thus Chebyshev's inequality tells us that, with high probability, the partial period autocorrelations are low, as described in Section 7.

3 Statement of Results

We denote the *expectation* of a random variable X by $E[X]$. All expectations are taken for fixed window size D and shift τ, assuming a uniform distribution on all start positions k. The *variance* $V(X)$ of a random variable X is given by $V(X) = E[(X - E[X])^2] = E[X^2] - E[X]^2$.

Theorem 3.1 *Suppose the geometric sequence* $\mathbf{S}$ *is as balanced as possible, i.e.* $I(f) = \pm 1$ *if* q *is odd, and* $I(f) = 0$ *if* q *is even. Then for a shift* τ *that is not a multiple of* ν*, the expected partial period autocorrelation of* $\mathbf{S}$ *is*

$$E[\mathcal{A}_{\mathbf{S}}(\tau, k, D)] = D(q^{n-2} - 1)/(q^n - 1)$$

if q *is odd, and*

$$E[\mathcal{A}_{\mathbf{S}}(\tau, k, D)] = -D/(q^n - 1)$$

if q *is even. In this case, if* f *is chosen so that* $\Delta_{\alpha^\tau}(f) = 0$ *whenever* τ *is a nonzero multiple of* ν*, then* $E[\mathcal{A}_{\mathbf{S}}(\tau, k, D)] = -D/(q^n - 1)$ *whenever* $\tau \neq 0$*.*

Theorem 3.2 *For any* τ*, the variance of the partial period autocorrelation of a geometric sequence 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 q *is even and* f *is balanced, the variance is bounded by*

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

These results allow us to detect phase shifts between a transmitter and a receiver using geometric sequences by computing partial period autocorrelations.

Theorem 3.3 *A shifted geometric sequence* $\mathbf{S}$ *with shift* τ *can be distinguished from an unshifted sequence with probability at least* $1-\epsilon$ *by using a partial period autocorrelation with window size* D *satisfying*

$$\nu > D > \frac{(q^2+q+1)(q^n-1)q^n}{\epsilon(q^n-1-|\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.$$

If q *is even and* f *is balanced, this can be improved to*

$$\nu > D > \frac{(q^2+q+2)(q^n-1)q^n}{2\epsilon(q^n-1-|\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.$$

Note that if ϵ is chosen less than

$$\frac{(q^3+q-2)q^n}{2(q^n-1-|\mathcal{A}_{\mathbf{S}}(\tau)|)^2},$$

then it is impossible to pick D in this range. It is tempting to expect that increasing D above ν will allow ϵ to be chosen smaller. While we believe this to be true asymptotically (as D approaches q^n-1), it is quite possible that the probability of error may increase as D becomes slightly larger than ν.

If we choose f balanced and such that $\Delta_{\alpha^\tau}(f)=0$, then $\mathcal{A}_{\mathbf{S}}(\tau)=-1$ for all $\tau\neq 0$ and the error probability is approximately $(q^2+q+2)/(2D)$ (see Corollary 2.4). More generally, if f is balanced, the error probability will be approximately $(q^2+q+2)/(2D)$ when $\nu \not| \tau$, but will be higher when $\nu|\tau$. However, if $\mathcal{A}_{\mathbf{S}}(\tau)$ is approximately $q^{n/2}$ for such τ, then the error probability will be only slightly higher.

4 First Steps

Theorem 3.1 is straightforward and holds in greater generality: if $\mathbf{R}$ is *any* periodic binary sequence with period, say, N then we have:

Theorem 4.1 *The expectation of the partial period autocorrelation is given by*

$$E[\mathcal{A}_{\mathbf{R}}(\tau,k,D)] = \frac{D}{N}\mathcal{A}_{\mathbf{R}}(\tau).$$

Proof:

$$
\begin{aligned}
E[\mathcal{A}_{\mathbf{R}}(\tau,k,D)] &= \frac{1}{N}\sum_{k=0}^{N-1}\mathcal{A}_{\mathbf{R}}(\tau,k,D) \\
&= \frac{1}{N}\sum_{k=0}^{N-1}\sum_{i=k}^{k+D-1}(-1)^{s_{i+\tau}+s_i} \\
&= \frac{1}{N}\sum_{i=0}^{N-1}\sum_{k=i-D+1}^{i}(-1)^{s_{i+\tau}+s_i} \\
&= \frac{1}{N}\sum_{i=0}^{N-1}D(-1)^{s_{i+\tau}+s_i} \\
&= \frac{D}{N}\mathcal{A}_{\mathbf{R}}(\tau).
\end{aligned}
$$

$\square$

We next consider the variance of the partial period autocorrelation. Recall that the variance of a random variable X is defined to be $E[(X - E[X])^2] = E[X^2] - E[X]^2$, so we must determine the second moment $E[\mathcal{A}_{\mathbf{S}}(\tau, k, D)^2]$ of the partial period autocorrelation. The field $GF(q^n)$ is an $n-$dimensional vector space over the base field $GF(q)$. For any $s \in GF(q)$ and $A \neq 0 \in GF(q^n)$, the set

$$H_A^s = \{x \in GF(q^n) : Tr_q^{q^n}(Ax) = s\}$$

is an affine hyperplane in $GF(q^n)$, i.e. a translate of an $n-1$-dimensional subspace. The second moment of the partial period autocorrelation can be expressed in terms of the cardinalities of certain fourfold intersections of these hyperplanes, as follows.

Lemma 4.2 *If* $\mathbf{S}$ *is a geometric sequence, then*

$$E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] \;=\; \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\Big(\sum_{s,t,u,v\in GF(q)} N_{i,j,\tau}(s,t,u,v)F(s)F(t)F(u)F(v) - 1\Big) \quad (1)$$

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:

$$E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] = \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2$$

$$
\begin{aligned}
&= \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}\Big(\sum_{i=k}^{k+D-1} F(Tr_q^{q^n}(\alpha^{i+\tau}))F(Tr_q^{q^n}(\alpha^{i}))\Big)^2 \\
&= \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}\sum_{i,j=k}^{k+D-1} F(Tr_q^{q^n}(\alpha^{i+\tau}))F(Tr_q^{q^n}(\alpha^{i}))F(Tr_q^{q^n}(\alpha^{j+\tau}))F(Tr_q^{q^n}(\alpha^{j})) \\
&= \frac{1}{q^n-1}\sum_{k=0}^{q^n-2}\sum_{i,j=0}^{D-1} F(Tr_q^{q^n}(\alpha^{i+k+\tau}))F(Tr_q^{q^n}(\alpha^{i+k}))F(Tr_q^{q^n}(\alpha^{j+k+\tau}))F(Tr_q^{q^n}(\alpha^{j+k})) \\
&= \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\sum_{k=0}^{q^n-2} F(Tr_q^{q^n}(\alpha^{i+k+\tau}))F(Tr_q^{q^n}(\alpha^{i+k}))F(Tr_q^{q^n}(\alpha^{j+k+\tau}))F(Tr_q^{q^n}(\alpha^{j+k}))
\end{aligned}
$$

Set $x = \alpha^k$ to obtain

$$
E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] = \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\sum_{x\neq 0\in GF(q^n)} F(Tr_q^{q^n}(\alpha^{i+\tau}x))F(Tr_q^{q^n}(\alpha^{i}x))F(Tr_q^{q^n}(\alpha^{j+\tau}x))F(Tr_q^{q^n}(\alpha^{j}x)).
$$

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 may be rewritten

$$
E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] = \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\Big(\sum_{s,t,u,v\in GF(q)} N_{i,j,\tau}(s,t,u,v)F(s)F(t)F(u)F(v) - 1\Big).
$$

□

Our derivation of the bound on the second moment, and therefore the variance (described in Theorem 3.2), proceeds as follows. In Proposition 5.1 we determine, for each i, j, and τ, the number of times that $N_{i,j,\tau}(s,t,u,v)$ is nonzero. We next determine the values of $N_{i,j,\tau}(s,t,u,v)$ (depending on i, j, and τ) in Theorem 5.2. We find that there are three cases depending on whether $\alpha^\tau \in GF(q)$, $\alpha^\tau \in GF(q^2) - GF(q)$, or $\alpha^\tau \in GF(q^n) - GF(q^2)$. Finally, in Section 6, for each of these three cases we count 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 $N_{i,j,\tau}(s,t,u,v)$.

5 Intersections of Hyperplanes

Throughout this section we fix i,j,τ, with $0 \le i,j < D$, $0 \le \tau \le q^n-2$, and let $A = \alpha^i$, $B = \alpha^j$, $C = \alpha^\tau \in GF(q^n)$. For any $s,t,u,v \in GF(q)$, define the affine linear subspace

$$
Z(s,t,u,v) = H_A^s \cap H_{AC}^t \cap H_B^u \cap H_{BC}^v.
$$

Then $N_{i,j,\tau}(s,t,u,v) = |Z(s,t,u,v)|$. 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, depending on the dimension of $Z(s,t,u,v)$. Let r be the dimension of the $GF(q)$-vector space spanned by the elements $\{A, AC, B, BC\}$ when we think of $GF(q^n)$ as a vector space over $GF(q)$.

Proposition 5.1 *If there exist $a, b, c, d \in GF(q)$ such that $aA + bAC + cB + dBC = 0$, and $as + bt + cu + dv \neq 0$, then $Z(s,t,u,v) = \emptyset$ so $N_{i,j,\tau}(s,t,u,v) = 0$. Otherwise, $\dim Z(s,t,u,v) = n - r$ so $N_{i,j,\tau}(s,t,u,v) = q^{n-r}$. There are q^r values of (s,t,u,v) such that $N_{i,j,\tau}(s,t,u,v) = q^{n-r}$.*

Proof: Define $L : GF(q^n) \to GF(q)^4$ by $x \mapsto (Tr_q^{q^n}(Ax), Tr_q^{q^n}(ACx), Tr_q^{q^n}(Bx), Tr_q^{q^n}(BCx))$. Then L is linear and $Z(s,t,u,v) = L^{-1}(s,t,u,v)$. First, consider the case $(s,t,u,v) = (0,0,0,0)$. Then $Z(0,0,0,0) = \ker(L)$ so $|Z(0,0,0,0)| = q^{n-\mathrm{rank}(L)}$. Let us associate to any $E \in GF(q^n)$ the linear function $\Phi(E)$ which is given by $\Phi(E)(x) = Tr_q^{q^n}(Ex)$. Then Φ is a linear isomorphism,

$$\Phi : GF(q^n) \to Hom_{GF(q)}(GF(q^n), GF(q))$$

and the four functions $\{Tr_q^{q^n}(Ax), Tr_q^{q^n}(ACx), Tr_q^{q^n}(Bx), Tr_q^{q^n}(BCx)\}$ which define L are given by $\{\Phi(A), \Phi(AC), \Phi(B), \Phi(BC)\}$. Therefore,

$$\mathrm{rank}(L) = \dim\{\Phi(A), \Phi(AC), \Phi(B), \Phi(BC)\} = \dim\{A, AC, B, BC\} = r$$

which proves that $\dim Z(0,0,0,0) = n - r$ so $N(0,0,0,0) = q^{n-r}$.

Now consider the case of general (s,t,u,v). If $(s,t,u,v) \in GF(q)^4$ is in the image of L, then $Z(s,t,u,v) = L^{-1}(s,t,u,v)$ is a translate of $Z(0,0,0,0)$ so their cardinalities are the same, namely q^{n-r}. If $(s,t,u,v) \notin \mathrm{image}(L)$ then $Z(s,t,u,v) = \emptyset$. Let us determine when this happens.

Whenever $\{A, AC, B, BC\}$ satisfies a linear equation,

$$aA + bAC + cB + dBC = 0 \tag{2}$$

the functions $\{\Phi(A), \Phi(AC), \Phi(B), \Phi(BC)\}$ will satisfy the same equation. For any $x \in GF(q^n)$, the elements $\{s = Tr_q^{q^n}(Ax), t = Tr_q^{q^n}(ACx), u = Tr_q^{q^n}(Bx), v = Tr_q^{q^n}(BCx)\}$ will also satisfy the same equation, so every point $(s,t,u,v) \in \mathrm{image}(L)$ satisfies equation (2). Thus, if (s,t,u,v) do not satisfy this equation then this point is not in the image of L, and $N_{i,j,\tau}(s,t,u,v) = 0$. □

We proceed to determine whether $r = 1$, 2, 3, or 4. We consider $r = 4$ to be the general case and determine, for each i, j, τ, conditions under which each of the other cases occurs.

There is an action of the general linear group over $GF(q)$ of rank two, $G = GL_2(GF(q))$, on $GF(q^n)$ which we shall make use of. Recall that this group is the multiplicative group of two by two matrices with nonzero determinant and with entries in $GF(q)$. The group acts by fractional linear transformations. That is, the matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

acts on the element $C \in GF(q^n)$ by

$$C \mapsto \frac{aC+b}{cC+d} = M(C).$$

It is straightforward to check that if $M, N \in GL_2(GF(q))$, then $(MN)(C) = M(N(C))$. Recall that when a group G acts on a set W, the G-*orbit* of an element $x \in W$ is the set $\text{orbit}(x) = \{M(x) : M \in G\}$.

If $C \notin GF(q)$ then an equation of linear dependence (2),

$$aAC + bA + cBC + dB = 0$$

may be interpreted as an equation $B/A = -M(C)$, where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $ad - bc \neq 0$, then $M \in Gl_2(GF(q))$, in other words, $B/A \in \text{orbit}(C)$. If $ad - bc = 0$ then $B/A \in GF(q)$.

Theorem 5.2 *1. Suppose $C = \alpha^\tau \in GF(q)$. Then:*

(a) If $B/A = \alpha^{j-i} \in GF(q)$, then $r = 1$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-1}$);

(b) otherwise $r = 2$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-2}$);

2. Suppose $C = \alpha^\tau \in GF(q^2) - GF(q)$. Then:

(a) If $B/A = \alpha^{j-i} \in GF(q)$, then $r = 2$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-2}$);

(b) if $\alpha^{j-i} \in \text{orbit}(\alpha^\tau)$, then $r = 2$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-2}$);

(c) otherwise $r = 4$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-4}$);

3. Suppose $C = \alpha^\tau \in GF(q^n) - GF(q^2)$. Then:

(a) If $B/A = \alpha^{j-i} \in GF(q)$, then $r = 2$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-2}$);

(b) if $B/A = \alpha^{j-i} \in \text{orbit}(\alpha^\tau)$, then $r = 3$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-3}$);

(c) otherwise $r = 4$ (so $N_{i,j,\tau}(0,0,0,0) = q^{n-4}$).

Proof: The proof will proceed by considering the different cases for $r = \dim\{A, AC, B, BC\}$.

Case $r = 1$: This occurs when every element of $\{A, AC, B, BC\}$ is a $GF(q)$ multiple of every other element. Thus $\alpha^\tau, \alpha^{j-i} \in GF(q)$, which gives part 1(a) of Theorem 5.2.

Case $r = 2$: This occurs if AC, A, BC, B satisfy two linearly independent equations, say

$$\begin{aligned} aAC + bA + cBC + dB &= 0 \\ eAC + fA + gBC + hB &= 0, \end{aligned} \tag{3}$$

where $a, b, c, d, e, f, g, h \in GF(q)$ and (a, b, c, d) and (e, f, g, h) are independent vectors.

If $C \in GF(q)$, then the span of $\{AC, A, BC, B\}$ equals the span of $\{A, B\}$. We have $\dim\{A, AC, B, BC\}$ equal to two if $B/A = \alpha^{j-i}$ is not in $GF(q)$, (giving part 1(b) of Theorem 5.2, and one otherwise (which gives part 1(a)).

If C is not in $GF(q)$, then we can use each of these equations to write B/A as the result of applying to C a fractional linear transformation with coefficients in $GF(q)$:

$$\frac{B}{A} = -\frac{aC + b}{cC + d} = -\frac{eC + f}{gC + h}.$$

We can use the second equation to find a quadratic equation over $GF(q)$ satisfied by C. This equation is degenerate if and only if $B/A \in GF(q)$ (which gives parts 2(a) and 3(a) of Theorem 5.2). If $B/A = \alpha^{j-i}$ is not in $GF(q)$, then $C = \alpha^\tau$ is in $GF(q^2) - GF(q)$ and $\alpha^{j-i} \in \text{orbit}(\alpha^\tau)$ (which gives part 2(b)).

Case $r = 3$: We have a single equation

$$aAC + bA + cBC + dB = 0,$$

or, equivalently,

$$B = \frac{aC + b}{cC + d}A.$$

As before, $(aC + b)/(cC + d)$ is in $GF(q)$ (and hence $\dim\{A, AC, B, BC\}$ is two) if and only if $ad - bc = 0$. If $C \in GF(q^2)$, then the quadratic equation satisfied by C can be used to produce a second, independent linear equation. Thus $r = 3$ if and only if $\alpha^{j-i} \in \text{orbit}(\alpha^\tau)$ and $\alpha^\tau \notin GF(q^2)$. This gives part 3(b). We remark that this case gives the leading term for all the estimates of the variance. □

6 Variance of Partial Period Correlations

Return to the computation of the variance of the partial period correlation of geometric sequences, Equation (1). We break down our analysis depending upon whether α^τ is in

$GF(q)$, $GF(q^2)-GF(q)$, or $GF(q^n)-GF(q^2)$, corresponding to the three cases of Theorem 5.2. We remark that, if n is odd, then $GF(q^2)$ is not a subfield of $GF(q^n)$, so the middle case will not occur. In order to use parts 2(b) and 3(b) of Theorem 5.2 it will be necessary to determine, for given $0 \le i, j < D$, whether $\alpha^{i-j} \in \mathrm{orbit}(\alpha^\tau)$.

6.1 $\alpha^\tau \in GF(q)$

This section refers to Theorem 5.2 part (1). In this case $N_{i,j,\tau}(0,0,0,0) = q^{n-2}$ if $\alpha^{i-j} \notin GF(q)$, $N_{i,j,\tau}(0,0,0,0) = q^{n-1}$ if $\alpha^{i-j} \in GF(q)$. We have $\alpha^{i-j} \in GF(q)$ if and only if ν divides $i-j$. Thus for a given i, $0 \le i < D$, the number of j, $0 \le j < D$, such that the i,j term contributes to the sum is the number of j in this range such that ν divides $i-j$. This number is

$$\left\lfloor \frac{D-i-1}{\nu} \right\rfloor + \left\lfloor \frac{i}{\nu} \right\rfloor + 1 \le \frac{D-1}{\nu} + 1.$$

Since the number of such j is an integer, we also have that it is at most $\lceil D/\nu \rceil$. By breaking up the sum according to parts 1(a) and 1(b) of Theorem 5.2,we can bound the second moment as follows

$$\begin{aligned}
E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] &= \frac{1}{q^n-1} \sum_{i,j=0}^{D-1} \left(\sum_{s,u \in GF(q)} N_{i,j,\tau}(s,\alpha^\tau s,u,\alpha^\tau u) F(\alpha^\tau t) F(t) F(\alpha^\tau v) F(v) - 1 \right) \\
&= \frac{1}{q^n-1} \left(\sum_{i,j=0}^{D-1} \left(\sum_{s,u \in GF(q)} q^{n-2} F(s) F(\alpha^\tau s) F(u) F(\alpha^\tau u) - 1 \right) \right. \\
&\quad + \sum_{\substack{0 \le i,j < D \\ \nu | (i-j)}} \left(\sum_{u \in GF(q)} q^{n-1} F(\alpha^{i-j} u) F(\alpha^{\tau+i-j} u) F(u) F(\alpha^\tau u) \right. \\
&\quad \left. \left. - \sum_{s,u \in GF(q)} q^{n-2} F(s) F(\alpha^\tau s) F(u) F(\alpha^\tau u) \right) \right) \\
&\le \frac{D^2}{q^n-1} (q^{n-2} \Delta_{\alpha^\tau}(f)^2 - 1) + \frac{D}{q^n-1} (\frac{D-1}{\nu} + 1) q^n.
\end{aligned}$$

The expectation in this case is

$$\frac{D}{q^n-1} (q^{n-1} \Delta_{\alpha^\tau}(f) - 1).$$

Therefore the variance is

$$V(\mathcal{A}_{\mathbf{S}}(\tau,k,D)) = E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] - E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)]^2$$

$$
\begin{aligned}
&\le \frac{D^2}{q^n-1}(q^{n-2}\Delta_{\alpha^\tau}(f)^2-1)+\frac{D}{q^n-1}(\frac{D-1}{\nu}+1)q^n \\
&\quad -\frac{D^2}{(q^n-1)^2}(q^{n-1}\Delta_{\alpha^\tau}(f)-1)^2 \\
&= \frac{q^nD}{q^n-1}((\frac{D-1}{\nu}+1)-\frac{D}{q^n-1}(q-\Delta_{\alpha^\tau}(f))^2) \\
&\le \frac{q^nD}{q^n-1}(\frac{D-1}{\nu}+1).
\end{aligned}
$$

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

6.2 $\alpha^\tau \in GF(q^2)-GF(q)$

This section refers to Theorem 5.2 part (2). If $x \in GF(q^2)$, and $M \in G$, then $M(x) \in GF(q^2)$. If, moreover, $x \notin GF(q)$, then x is a generator for $GF(q^2)$ over $GF(q)$, that is, every element of $GF(q^2)$ can be written in the form $(ax+b)/(cx+d)$ for some $a,b,c,d \in GF(q)$. It follows that $N_{i,j,\tau}(0,0,0,0)$ is q^{n-2} if $\alpha^{i-j} \in GF(q^2)$, i.e., if $\nu_2=(q^n-1)/(q^2-1)$ divides $i-j$. Moreover, for $\alpha^\tau \in GF(q^2)$, $N_{i,j,\tau}(s,t,u,v)=q^{n-2}$ if (s,t,u,v) is in the image of $L=L_{i,j,\tau}$ (where L is as defined in the proof of Theorem 5.2). In all other cases, $N_{i,j,\tau}(s,t,u,v)=q^{n-4}$. As above, by breaking up the sum according to parts 2(a), 2(b), and 2(c) of Theorem 5.2, we can bound the second moment as follows

$$
\begin{aligned}
E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] &= \frac{1}{q^n-1}\sum_{i,j=0}^{D-1}\left(\sum_{s,t,u,v\in GF(q)} N_{i,j,\tau}(s,t,u,v)F(s)F(t)F(u)F(v)-1\right) \\
&= \frac{1}{q^n-1}\left(\sum_{i,j=0}^{D-1}\left(\sum_{s,t,u,v\in GF(q)} q^{n-4}F(s)F(t)F(u)F(v)-1\right)\right. \\
&\qquad + \sum_{\substack{0\le i,j<D\\ \nu_2|(i-j)}}\left(\sum_{\substack{s,t,u,v\in\\ \mathrm{image}(L_{i,j,\tau})}} q^{n-2}F(s)F(t)F(u)F(v)\right. \\
&\qquad\qquad \left.\left.-\sum_{s,t,u,v\in GF(q)} q^{n-4}F(s)F(t)F(u)F(v)\right)\right) \\
&\le \frac{D^2}{q^n-1}(q^{n-4}I(f)^4-1)+\frac{D}{q^n-1}(\frac{D-1}{\nu_2}+1)(q^n-q^{n-4}I(f)^4).
\end{aligned}
$$

The expectation in this case is

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

Therefore the variance is bounded by:

$$\begin{aligned}
V(\mathcal{A}_{\mathbf{S}}(\tau,k,D)) &= E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] - E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)]^2 \\
&\le \frac{D^2}{q^n-1}(q^{n-4}I(f)^4-1) + \frac{D}{q^n-1}(\frac{D-1}{\nu_2}+1)(q^n-q^{n-4}I(f)^4) \\
&\quad - \frac{D^2}{(q^n-1)^2}(q^{n-1}I(f)^2-1)^2 \\
&= \frac{q^{n-4}D}{q^n-1}((\frac{D-1}{\nu_2}+1)(q^4-I(f)^4) - \frac{D}{q^n-1}(q^2-I(f)^2)^2) \\
&\le \frac{q^nD}{q^n-1}(\frac{D-1}{\nu_2}+1).
\end{aligned}$$

In particular, if $D \le \nu$, then the variance is bounded above by $(q+1)q^nD/(q^n-1)$.

6.3 $\alpha^\tau \in GF(q^n) - GF(q^2)$

This section refers to Theorem 5.2 part (3). Case 3(b) of this calculation gives rise to the leading term in our estimate for the variance. In general, the G-orbit is not uniformly distributed in $GF(q^n)$, so for a fixed i, the number of j in a window with $\dim\{\alpha^{i+\tau},\alpha^i,\alpha^{j+\tau},\alpha^j\}=3$ is not proportional to the size of the window. We settle here for a cruder estimate, based on the structure of the group G. We first determine the size of the G-orbit of α^τ.

Lemma 6.1 *If $x \in GF(q^n) - GF(q)$, then the G-orbit of x has cardinality $q^3 - q$.*

Proof: An element of G is a matrix

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

over $GF(q)$ with nonzero determinant. There are $(q^2-1)(q^2-q)$ such matrices. Two such matrices define the same transformation if they differ by a nonzero multiple, so the cardinality of G is q^3-q. Recall that the stabilizer of an element x is the set of transformations M such that $M(x)=x$. In general, when a group acts on a set, the cardinality of the orbit of x is the cardinality of the group divided by the cardinality of the stabilizer of x. Here M is in the stabilizer if $(ax+b)/(cx+d)=x$, i.e., $ax+b=cx^2+dx$. If $x \notin GF(q^2)$, then we must have $c=b=0$, and $a=d$. That is, the stabilizer of x consists only of the identity transformation. The lemma follows. □

We will next decompose the elements of G into the composition of certain simple types of matrices with scalar multiplication. Since scalar multiplication by elements of $GF(q)$ moves elements large distances, this will allow us to bound the number of elements in an orbit that are in a given small window.

For matrices M and N, we write $M \sim N$ if M and N define the same transformation (i.e., the matrices differ by a scalar multiple). Let

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be an element of G, so $\delta = ad - bc \neq 0$. First suppose $a \neq 0$. Then

$$\begin{aligned} M &\sim \begin{pmatrix} 1 & b/a \\ c/a & d/a \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & \delta/a^2 \end{pmatrix} \begin{pmatrix} 1 & b/a \\ ac/\delta & bc/\delta + 1 \end{pmatrix} \\ &\sim \begin{pmatrix} a^2/\delta & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b/a \\ ac/\delta & bc/\delta + 1 \end{pmatrix}. \end{aligned}$$

Letting $S_x = \{(x+b)/(cx+bc+1)\}$, we have shown that $M(x)$ is a scalar multiple of an element of S_x.

On the other hand, suppose $a = 0$. Then $b \neq 0$ and $c \neq 0$, so

$$\begin{aligned} M &\sim \begin{pmatrix} 0 & b/c \\ 1 & d/c \end{pmatrix} \\ &= \begin{pmatrix} b/c & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & d/c \end{pmatrix}. \end{aligned}$$

Let $T_x = \{1/(x+d)\}$. Then in this case $M(x)$ is a scalar multiple of some element of T_x. We have shown that an arbitrary element of the orbit of x is a scalar multiple of some element of $S_x \cup T_x$.

Consider a window of size ν. If y is any element of $GF(q^n)$, then there is a unique $a \in GF(q)$ such that ay is in the given window. Therefore, for each element y of $S_x \cup T_x$, there is a unique scalar multiple of y, i.e., a unique element of the orbit of x, in the given window.

Proposition 6.2 *If $x \in GF(q^n) - GF(q^2)$, then the intersection of the orbit of x with a window of size at most ν has cardinality at most $|S_x \cup T_x| = q^2 + q$.*

Furthermore, we can write a window of arbitrary size D as the disjoint union of $\lceil D/\nu \rceil$ subwindows of size at most ν, and apply the preceding proposition to each subwindow. This gives us an upper bound in the general case.

Proposition 6.3 *The intersection of the orbit of x with a window of size D, D arbitrary, has cardinality at least $\lfloor D/\nu \rfloor (q^2+q)$ and at most $\lceil D/\nu \rceil (q^2+q)$.*

It follows that the number of i, j such that $0 \le i, j < D$ and $N_{i,j,\tau}(0,0,0,0) = q^{n-3}$ is at most $D \lceil D/\nu \rceil (q^2+q)$. (Another obvious estimate for this number of pairs i, j is D^2. If $D < q^2+q$ then this is even a better estimate. However we have not made use of this improvement since it would make the statement of the result quite complicated.) By Theorem 5.2, for such i, j, the number of s, t, u, v for which $N_{i,j,\tau}(s,t,u,v) = q^{n-3}$ is q^3. Moreover, when $\nu | (i-j)$, $N_{i,j,\tau}(s, t, \alpha^{j-i}s, \alpha^{j-i}t) = q^{n-2}$, and $N_{i,j,\tau}(s,t,u,v) = 0$ if $u \ne \alpha^{j-i}s$ or $u \ne \alpha^{j-i}t$. In all other cases $N_{i,j,\tau}(s,t,u,v) = q^{n-4}$.

Lemma 6.4 *If q is even and f is balanced, then for any D and τ such that $\alpha^\tau \notin GF(q^2)$,*

$$\sum_{\substack{0 \le i,j < D \\ \alpha^{j-i} \in \mathrm{orbit}(\alpha^\tau)}} \sum_{\substack{s,t,u,v \in \\ \mathrm{image}(L_{i,j,\tau})}} F(s)F(t)F(u)F(v) \le \frac{D \lceil D/\nu \rceil (q^2+q)}{2} q^3.$$

Proof: Proof Sketch The naive bound on the inner sum is q^3 since there is one linear constraint on (s,t,u,v). This would give a total bound of $D \lceil D/\nu \rceil (q^2+q)q^3$. We can do slightly better. For each j in the outer sum, letting i vary, we have a window $j, j+1, \cdots, j+D-1$ of size D. It is possible to pair the orbit elements in such a window so that half their terms in the inner sums cancel, giving the improved bound. $\square$

Thus we can bound the second moment as follows

$$\begin{aligned}
E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] &= \frac{1}{q^n-1} \sum_{i,j=0}^{D-1} \left(\sum_{s,t,u,v \in GF(q)} N_{i,j,\tau}(s,t,u,v) F(s)F(t)F(u)F(v) - 1 \right) \\
&\le \frac{1}{q^n-1} \left(\sum_{i,j=0}^{D-1} \left(\sum_{s,t,u,v \in GF(q)} q^{n-4} F(s)F(t)F(u)F(v) - 1 \right) \right. \\
&\quad + \sum_{\substack{0 \le i,j < D \\ \alpha^{j-i} \in \mathrm{orbit}(\alpha^\tau)}} \left(\sum_{\substack{s,t,u,v \in \\ \mathrm{image}(L_{i,j,\tau})}} q^{n-3} F(s)F(t)F(u)F(v) \right. \\
&\qquad \left. - \sum_{s,t,u,v \in GF(q)} q^{n-4} F(s)F(t)F(u)F(v) \right) \\
&\quad + \sum_{\substack{0 \le i,j < D \\ \nu | (i-j)}} \left(\sum_{\substack{s,t,u,v \in \\ \mathrm{image}(L_{i,j,\tau})}} q^{n-2} F(s)F(t)F(u)F(v) \right.
\end{aligned}$$

$$
\left. \left. - \sum_{s,t,u,v\in GF(q)} q^{n-4}F(s)F(t)F(u)F(v) \right) \right)
$$

$$
\leq \frac{D^2}{q^n-1}(q^{n-4}I(f)^4-1) + \frac{D\lceil D/\nu\rceil}{q^n-1}(q^2+q+1)(q^n-q^{n-4}I(f)^4).
$$

The expectation in this case is

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

Therefore the variance is

$$
\begin{aligned}
V(\mathcal{A}_{\mathbf{S}}(\tau,k,D)) &= E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)^2] - E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)]^2 \\
&\leq \frac{D^2}{q^n-1}(q^{n-4}I(f)^4-1) + \frac{D\lceil D/\nu\rceil}{q^n-1}(q^2+q+1)(q^n-q^{n-4}I(f)^4) \\
&\quad - \frac{D^2}{(q^n-1)^2}(q^{n-2}I(f)^2-1)^2 \\
&= \frac{q^{n-4}D\lceil D/\nu\rceil}{q^n-1}(q^2+q+1)(q^4-I(f)^4) - \frac{Dq^{n-4}}{(q^n-1)^2}(q^2-I(f)^2)^2 \\
&\leq \frac{q^nD}{q^n-1}\left\lceil\frac{(q-1)D}{q^n-1}\right\rceil(q^2+q+1).
\end{aligned}
$$

6.4 Summary

We have now developed the estimates which are needed in order to prove:

Theorem 3.2 *For any τ, the variance of the partial period autocorrelation of a geometric sequence with shift τ and window size D is bounded above by*

$$
\frac{q^nD}{q^n-1}\left\lceil\frac{(q-1)D}{q^n-1}\right\rceil(q^2+q+1). \tag{4}
$$

If q is even and f is balanced, then

$$
\frac{q^nD}{q^n-1}\left\lceil\frac{(q-1)D}{q^n-1}\right\rceil\frac{(q^2+q+2)}{2}. \tag{5}
$$

Proof: For any τ one of the three preceeding subsections applies. In each case the bound we have found for the variance of the partial period autocorrelation is less than or equal to the quantity in equation (4). The reduction by a factor of almost one half that occurs in equation (5) follows from Lemma 6.4. $\square$

This value has a bound of approximately $D^2/(2q^{n-3}) + q^2D/2$. For large D, this is dominated by the first term.

7 Application to the Detection of Phase Shifts

In this section we show how, by computing a partial period autocorrelation, these results, together with Chebyshev's inequality, can be used to detect phase shifts between a transmitter and a receiver using the same geometric sequence. Chebyshev's inequality gives bounds in terms of the variance on the probability that a random variable is far from its expectation. Specifically, if X is any random variable, and $\epsilon > 0$ is any real number, then

$$Prob(|X - E[X]| > \epsilon) < V(X)/\epsilon^2.$$

Noting that a partial period autocorrelation with window size D is at most D, we may ask how likely it is that the partial period autocorrelation is less than a fixed fraction $1/\delta$ of D. By Theorem 4.1, $E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)] = D\mathcal{A}_{\mathbf{S}}(\tau)/(q^n-1)$, so $|\mathcal{A}_{\mathbf{S}}(\tau,k,D)| < D/\delta$ whenever

$$|\mathcal{A}_{\mathbf{S}}(\tau,k,D) - E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)]| < D\left(\frac{1}{\delta} + \frac{|\mathcal{A}_{\mathbf{S}}(\tau)|}{q^n-1}\right) = D\frac{q^n-1-\delta|\mathcal{A}_{\mathbf{S}}(\tau)|}{\delta(q^n-1)}.$$

Consequently

$$\begin{aligned}
&Prob(|\mathcal{A}_{\mathbf{S}}(\tau,k,D)| < D/\delta) \\
&\quad\geq\ Prob(|\mathcal{A}_{\mathbf{S}}(\tau,k,D) - E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)]| < D\frac{q^n-1-\delta|\mathcal{A}_{\mathbf{S}}(\tau)|}{\delta(q^n-1)}) \\
&\quad=\ 1 - Prob(|\mathcal{A}_{\mathbf{S}}(\tau,k,D) - E[\mathcal{A}_{\mathbf{S}}(\tau,k,D)]| > D\frac{q^n-1-\delta|\mathcal{A}_{\mathbf{S}}(\tau)|}{\delta(q^n-1)}) \\
&\quad>\ 1 - \frac{V(\mathcal{A}_{\mathbf{S}}(\tau,k,D))(q^n-1)^2\delta^2}{D^2(q^n-1-\delta|\mathcal{A}_{\mathbf{S}}(\tau)|)^2} \\
&\quad>\ 1 - \frac{q^nD}{q^n-1}\left\lceil\frac{(q-1)D}{q^n-1}\right\rceil\frac{(q^2+q+1)(q^n-1)^2\delta^2}{D^2(q^n-1-\delta|\mathcal{A}_{\mathbf{S}}(\tau)|)^2} \\
&\quad=\ 1 - \left\lceil\frac{(q-1)D}{q^n-1}\right\rceil\frac{(q^2+q+1)(q^n-1)q^n\delta^2}{D(q^n-1-\delta|\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.
\end{aligned}$$

In case $D < \nu$, this is

$$Prob(|\mathcal{A}_{\mathbf{S}}(\tau,k,D)| < D/\delta)\ \geq\ 1 - \frac{(q^2+q+1)(q^n-1)q^n\delta^2}{D(q^n-1-\delta|\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.$$

Thus, for large enough period, $\mathcal{A}_{\mathbf{S}}(\tau, k, D)$ is close to its expectation with high probability. Again, if q is even and f is balanced, this improves by nearly one half.

These results can be used to distinguish between a shifted and an unshifted signal by computing a partial period autocorrelation with a small window size D. An unshifted partial period autocorrelation with window size D always equals D. A shifted partial period autocorrelation can be distinguished from an unshifted partial period autocorrelation if its absolute value is less than D. Thus we want to know that $Prob(|\mathcal{A}_{\mathbf{S}}(\tau, k, D)| < D)$ is large. By the results of the preceeding paragraph with $\delta = 1$,

$$Prob(|\mathcal{A}_{\mathbf{S}}(\tau, k, D)| < D) > 1 - \left\lceil \frac{(q-1)D}{q^n - 1} \right\rceil \frac{(q^2+q+1)(q^n-1)q^n}{D(q^n - 1 - |\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.$$

For $D < \nu$ this reduces to

$$Prob(|\mathcal{A}_{\mathbf{S}}(\tau, k, D)| < D) > 1 - \frac{(q^2+q+1)(q^n-1)q^n}{D(q^n - 1 - |\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.$$

This proves the following theorem.

Theorem 3.3 *A shifted geometric sequence* $\mathbf{S}$ *with shift* τ *can be distinguished from an unshifted sequence with probability at least* $1 - \epsilon$ *by using a partial period autocorrelation with window size* D *satisfying*

$$\frac{q^n - 1}{q - 1} > D > \frac{(q^2+q+1)(q^n-1)q^n}{\epsilon(q^n - 1 - |\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.$$

If q *is even and* f *is balanced, this can be improved to*

$$\frac{q^n - 1}{q - 1} > D > \frac{(q^2+q+2)(q^n-1)q^n}{2\epsilon(q^n - 1 - |\mathcal{A}_{\mathbf{S}}(\tau)|)^2}.$$

8 Conclusions

We have shown that the expectation of the partial period autocorrelations of geometric sequences (for even q) is low, and that for all q, the variance is bounded by approximately $D^2/q^{n-3} + q^2 D$. To put this in some perspective, observe that for a sequence of period $q^n - 1$, with no restrictions at all, the variance of the partial period autocorrelations could be as high as $D^2(q^n - 1)$. In fact, even for the balanced sequence consisting of $\lceil (q^n-1)/2 \rceil$ ones followed by $\lfloor (q^n-1)/2 \rfloor$ zeros, the variance with shift $\tau = 1$ is $D^2(q^n - 5) + 4D$. Thus our bound for geometric sequences is quite far from the maximum.

In the case of an m-sequence, one can do better. Here the variance can be computed precisely as

$$D\left(1+\frac{1}{q^n-1}\right)\left(1-\frac{D}{q^n-1}\right) < D$$

as is shown in [18].

The bound in case of a general geometric sequence is not too far off from this. It would be interesting to find other special cases of geometric sequences in which one can do better than the bound proven here with the linear complexity larger than that of an m-sequence.

A critical part of the calculation of the bound on the variance involves understanding how uniformly each orbit of the action of $GL_2(GF(q))$ on $GF(q^n)$ by fractional linear transformations is distributed in $GF(q^n)$. In sections 6.2 and 6.3 we make estimates that we expect can be improved, thus sharpening the bounds. We have evidence, based on simulations in the case in which q is even, that for small D the bound on the size of the intersection of an orbit of this group action with a range of powers of a primitive element of $GF(q^n)$ may be too high. The estimate we have made does not vary for $D < \nu$. We believe, however, that the size of the intersection of orbit(x) with a window of size D is approximately proportional to D. Proving this depends on a better understanding of this group action, and is an interesting algebraic question. We make the following conjecture:

Conjecture 8.1 *There is a constant c, independent of q, n, and D, such that for any τ the variance of the partial period autocorrelation of a geometric sequence with shift τ and window $D < \nu$ is bounded above by*

$$cD\left\lceil \frac{D}{q^{n-3}} \right\rceil .$$

Moreover, there is evidence based on computer searches that the sums of the form in Lemma 6.4 are, in fact, far smaller than our estimates. Consider, for example, the case $q = 16$. Based on bounds on these sums computed for all balanced functions from $GF(16)$ to $GF(2)$, we can reduce our estimate of the variance by factors depending on D as given in Table 1. These results apply for all n. We believe that similar reductions are possible for all q.

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.

$\lceil D/\nu \rceil$	Reduction in V
1	16.33
2	23.65
3	27.75
4	31.80
5	36.27
6	41.14
7	46.51
8	53.15
9	60.19
10	70.65
11	84.95
12	107.35
13	143.32
14	200.42

Table 1: Factor by which V can be reduced for $q = 16$.

[2] A. H. Chan, M. Goresky, and A. Klapper, Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences, to appear, *Discrete Applied Mathematics.*

[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, The vulnerability of geometric sequences based on fields of odd characteristic, to appear, *Journal of Cryptology.*

[7] A. Klapper, A.H. Chan, and M. Goresky, Cascaded GMW sequences, *IEEE Trans. Inf. Thy.*.

[8] A. Klapper and M. Goresky, Revealing information with partial period autocorrelations, *in Proceedings of Asiacrypt '91*, Fujyoshida, Japan, 1991.

[9] 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).

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

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

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

[13] J. S. No and P. V. Kumar, On the partial-period correlation moments of GMW sequences, *MILCOM 87: 1987 IEEE Military Communications Conference - Conference Record.* , IEEE Publications, N.Y., New York (1987).

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

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

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

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

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