On Correlations of A Family of Generalized Geometric Sequences

Wei Sun, Andrew Klapper, Yi Xian Yang

***Abstract*— In this paper we study families of generalized geometric sequences formed by applying a feedforward function to certain sums of decimated m-sequences with elements in a finite field. We compute their correlation functions, which for certain families turn out to be close to the square root of the period. The size of these families equals their period. We also show that in the binary case the linear complexities of these sequences are much larger than those of cascaded geometric sequences, although in these cases the maximum correlations are larger.**

***Index Terms*— Generalized geometric sequence, Correlation function, Character, Linear complexity.**

I. Introduction

SEQUENCES with good correlation properties and high linear complexity are important in code division multiple-access spread-spectrum communication systems and cryptography. Geometric sequences are a very general class of sequences whose correlation properties and linear complexities have been extensively studied. In this paper we use several results of Carlitz on exponential sums [1], [2] to study the correlations of a general class of sequences we call *generalized geometric sequences*. We also analyze the linear complexity of certain of these sequences. In all cases the sizes of the families of cyclically distinct sequences equal their periods. By varying the choices of parameters we can achieve various combinations of maximum correlation and minimum linear complexity. The sequences are determined in part by the choice of a prime number p and pair of natural numbers n and e defining field extensions $GF(p^n)$ and $GF(p^{ne})$ of $GF(p)$.

For example, let n and e be odd integers. Let $n = n_1 n_2 \cdots n_l$ with n_i at least 3 and n_1 at least 5 be an ordered factorization. We describe a family of $2^{ne}-1$ sequences with period $P = 2^{ne}-1$, maximal correlation and shifted autocorrelation at most $2^{ne/2}(2^{2n}-1)+1$, and linear complexity $n_1 n_2^2 n_3^4 \cdots n_l^{2^{l-1}} (2e)^{2^l}$. In other words, when the period is approximately $P = 2^{ne}-1$, the number of sequences in the family is P, and the correlations are at most $P^{1/2+2/e}$. If we take, say $n_1 = 5$ and $n_j = 3$ for $j > 1$ (these are allowable choices according to Theorem 6), then the linear complexity is $\frac{5}{9}(6e)^{2(n/5)^{\log_3(2)}} = \frac{5}{9}(6P/n)^{2(n/5)^{\log_3(2)}}$, which can be shown to be an increasing function of n if $n < P$. Thus if we keep the period P fixed, then we observe a tradeoff: the linear complexity is increased by increasing n (or, equivalently, decreasing e), while the correlations are decreased by decreasing n.

In any case the parameter e must be large for the correlations to be reasonably small. For example, if we take $e = 9$ and $n = 15$, then the period is about 2^{135}, the correlations are at most $P^{1/2+2/9} \sim P^{.72} \sim 2^{97}$ while the linear complexity is about 2^{22}. If we take $e = 9$ and $n = 45$, then the period is about 2^{405}, the correlations are at most $P^{1/2+2/9} \sim P^{.72} \sim 2^{292}$ while the linear complexity is about 2^{45}. While these values are not in a practical range, they are interesting in that it is difficult to achieve even this by other means.

This case is compared to various previously studied families of sequences in Table (I). In this table we consider only binary sequences ($p = 2$). In each case the period is $2^t - 1$. The row labeled "Gen. Geom." corresponds to the choice $n = 5 \cdot 3^k$ for some k. This maximizes the linear complexity.

Family	t	Size of Family	Maximum Correlation	Maximum Linear Complexity
Gold	$2n+1$	2^t+1	$1+2^{\frac{t+1}{2}}$	$2t$
Gold	$4n+2$	2^t-1	$1+2^{\frac{t+2}{2}}$	$2t$
Kasami (Small Set)	$2n$	$2^{\frac{t}{2}}$	$1+2^{\frac{t}{2}}$	$\frac{3t}{2}$
Kasami (Large Set)	$4n+2$	$2^{\frac{t}{2}}(2^t+1)$	$1+2^{\frac{t+2}{2}}$	$\leq \frac{5t}{2}$
Bent	$4n$	$2^{\frac{t}{2}}$	$1+2^{\frac{t}{2}}$	$\binom{t/2}{t/4}2^{\frac{t}{4}}$
No	$2n$	$2^{\frac{t}{2}}$	$1+2^{\frac{t}{2}}$	$n(2^n-1)$
TN	$2kn$	$2^{\frac{t}{2}}$	$1+2^{\frac{t}{2}}$	$> 3nk(3k-1)^{n-2}$
$(0,j)$-QF	ne odd	2^t+1	$1+2^{\frac{t+n}{2}}$	$\sim t2^{n-1}(e-2)^{n-2}$
Gen. Geom.	ne	2^t-1	$2^{t/2}(2^{2n}-1)+1$	$\frac{5}{9}(6e)^{2(n/5)^{\log_3(2)}}$

TABLE I
COMPARISON OF PROPERTIES OF FAMILIES OF SEQUENCES OF PERIOD 2^n-1

The paper is organized as follows. In Section II we define define generalized geometric sequences. In Section III definitions and lemmas about exponential sums are recalled. Correlation functions of generalized geometric sequences are calculated in Section IV in the case when p and en are odd and in Section V in the case when p is odd and en is even. In

Wei Sun and Yi Xian Yang are with the Department of Information Engineering, P. O. Box 145, Beijing University of Posts and Telecomm, Beijing, 100876, People's Republic of China, E-mail: yangsun@bupt.edu.cn, yxyang@bupt.edu.cn The work of the authors was supported by China Natural Science Foundation grant #69802002.

Andrew Klapper is with the Department of Computer Science, 763H Anderson Hall, University of Kentucky, Lexington KY 40506-0046, E-mail: klapper@cs.uky.edu. This research funded in part by NSF grant #NCR-9400762.

Section VI we state the results on correlations in the case when $p = 2$ without proof (the proofs are similar to those when p is odd). In Section VII we consider the linear complexity for certain generalized geometric sequences when $p = 2$. In the last section we put these results together to build families of sequences with low correlations and large linear complexity.

II. Definitions

We begin by defining the sequences of interest. Let p be a prime number, $n, e > 0$ integers, and $q = p^n$. Let $GF(q)$ be a finite field with q elements. The trace function $tr_q^{q^e}(\cdot)$ from $GF(q^e)$ into $GF(q)$ is defined by

$$tr_q^{q^e}(x) = \sum_{i=0}^{e-1} x^{q^i}, x \in GF(q^e).$$

Let α be a primitive element in $GF(q^e)$. The sequence U whose ith term is

$$U(i) = tr_q^{q^e}(\alpha^i),$$

is a maximal length shift register sequence, or simply an m-sequence, over $GF(q)$. Let r be a (possibly different)

prime number. If f is an arbitrary function from $GF(q)$ to $GF(r)$, then the sequence S_f whose ith term is

$$S_f(i) = f(U(i)) = f(tr_q^{q^e}(\alpha^i))$$

is called a *geometric sequence based on* α. These sequences have been studied by a number of authors [3], [8], [11].

Let S and T be any r-ary sequences with period L. If $\omega = e^{2\pi i/r}$ is a complex primitive rth root of unity, then the (periodic) cross-correlation function of S and T is

$$C_{S,T}(\tau) = \sum_{i=0}^{L-1} \omega^{s(i)+t(i+\tau)},$$

for $\tau = 0, 1, \cdots, L-1$. If $S = T$, then $C_{S,T}$ is the (periodic) autocorrelation function of S. Also, for such a function f we denote $F(u) = \omega^{f(u)}$ for $u \in GF(q)$, and we denote

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

the *imbalance of* f. Note that if $r \neq p$, then $I(f)$ cannot be zero.

Suppose that S_f and S_g are geometric sequences based on α and α^k, respectively, with $\gcd(k, q^e - 1) = 1$. Klapper, et al, [11] gave correlations of S_f and S_g when $k = p^l$ and $k = q^a + q^b$. In the same paper, a more general class of sequences was defined as follows. For $A, B \in GF(q^e)$, the sequence ${S_f}^{(A,B)}$ whose ith element is

$${S_f}^{(A,B)}(i) = f(tr_q^{q^e}(A\alpha^i + B\alpha^{ki})) \quad (1)$$

is called a *generalized geometric sequence based on* α *and* k. The problem of calculating correlations of these sequences was left open. Sun and Yang [20] solved the problem in the case when $k = p^l$. In the case when $k = q^a + q^b$, Klapper [8] and Sun and Yang [21] calculated the cross-correlation functions between generalized geometric sequences and geometric sequences.

In a later paper, Klapper, et al. [12] defined *cascaded GMW sequences*. These are geometric sequences for which the function f is defined by choosing a tower of finite fields and alternately composing exponentiation functions and trace functions down the tower. The definition is described in detail in Section VII below. Klapper, et al, showed that cascaded GMW sequences have ideal autocorrelations and fairly large linear complexities.

In this paper we study correlation functions between two generalized geometric sequences based on the same α and k in the case when $k = p + 1$. We also calculate the linear complexity of generalized geometric sequences when $p = 2$ and the function f is defined as for cascaded GMW sequences.

III. Results on Exponential Sums

In this section we recall several results on exponential sums that will be useful in what follows. Let

$$\chi_q(x) = e^{2\pi i tr_p^q(x)/p},$$

$x \in GF(q)$, be a canonical character of $GF(q)$ (with values in the complex numbers).

Lemma 1: [15] Let $a \in GF(q)$. Then

$$\sum_{x \in GF(q)} \chi_q(ax) = \begin{cases} q & \text{if } a = 0 \\ 0 & \text{if } a \neq 0. \end{cases}$$

We use the following notation for exponential sums, where $a, b \in GF(q)$:

$$S(a, b) = \sum_{x \in GF(q)} \chi_q(ax^{p+1} + bx).$$

When $b = 0$ we define $S(a) = S(a, 0)$.

Lemma 2: (Carlitz [2]) Let $q = p^n$ and $n = 2m$.

1) If $a \neq 0, b = 0$, then

$$S(a) = \begin{cases} (-1)^{m+1} p^{m+1} & \text{if } a^{(p^n-1)/(p+1)} = (-1)^m \\ (-1)^m p^m & \text{otherwise.} \end{cases}$$

2) If $a \neq 0, b \neq 0$, then $S(a, b) = 0$ if $a^p x^{p^2} + ax + b^p = 0$ is unsolvable in $GF(q)$ and $S(a, b) = (-1)^m p^m \chi_q(ax_0{}^{p+1} + bx_0)$ otherwise, where x_0 is an arbitrary solution in $GF(q)$ of the equation $a^p x^{p^2} + ax + b^p = 0$.

It is known that if $a^{(q-1)/(p+1)} \neq (-1)^m$, then the equation $a^p x^{p^2} + ax + b^p = 0$ has a unique solution. If $a^{(q-1)/(p+1)} = (-1)^m$, then $a^p x^{p^2} + ax + b^p = 0$ is solvable in $GF(q)$ if and only if

$$\sum_{j=0}^{m-1} (a^{-1} b c^{-p})^{p^{2j}} = 0, \quad a^{1-p} = -c^{p^2-1}.$$

Lemma 3: (Carlitz [2]) Let $q = p^n, n = 2m + 1$.

1) If $a \neq 0$ and $b = 0$, then

$$S(a) = S(1)\psi(a)$$

and

$$S(1) = (-1)^{m(p-1)/2} i^{(p-1)^2/4} p^{(2m+1)/2}.$$

2) If $a \neq 0$ and $b \neq 0$, then

$$S(a,b) = \chi_q(ax_0{}^{p+1} + bx_0)S(1)\psi(a),$$

where ψ is the quadratic character of $GF(q)$ and x_0 is the unique solution in $GF(q)$ to the equation $a^p x^{p^2} + ax + b^p = 0$.

IV. Correlations of Generalized Geometric Sequences When $en = 2m+1$

In this section we assume that $q^e = p^{2m+1}$. That is, $en = 2m+1$. Let f and g be possibly nonlinear functions from $GF(q)$ to $GF(r)$, $A, B, A', B' \in GF(q^e)$, and ${S_f}^{(A,B)}, {S_g}^{(A',B')}$ be generalized geometric sequences based on the same α and k. Then

$$C_{{S_f}^{(A,B)},{S_g}^{(A',B')}}(\tau) = \sum_{i=0}^{q^e-2} \omega^{{S_f}^{(A,B)}(i)+{S_g}^{(A',B')}(i+\tau)}.$$

We also let $F(u) = \omega^{f(u)}, G(v) = \omega^{g(v)}$. This section consists of a proof of the following theorem.

Theorem 1: Let ${S_f}^{(A,B)}, {S_g}^{(A',B')}$ be generalized geometric sequences based on the same α and k, as defined in equation (1). Assume that $A, B, A', B' \neq 0$, $k = p+1$, $q^e = p^{en} = p^{2m+1}$, and $0 \leq \tau \leq q^e - 2$. Let $A_1 = A'\alpha^\tau$ and $B_1 = B'\alpha^{(p+1)\tau}$.

1) If $A/A_1 \in GF(q)$ and $A_1 B = AB_1$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-1}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq q^{e/2}(q^2-q).$$

2) If $A/A_1 \in GF(q)$ and $A_1 B \neq AB_1$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + F(0)G(0) - q^{(e-3)/2}\mu\sum_{u,v\in GF(q)}\psi((AB_1 - A_1B)\cdot(A_1u - Av))F(u)G(v)| \leq \begin{cases} q^{e/2}(q^2-2q+1) & \text{if } B/B_1 \in GF(q) \\ q^{e/2}(q^2-q) & \text{if } B/B_1 \notin GF(q) \end{cases}$$

where $\mu \in \{1, -1, i, -i\}$.

3) If $A/A_1 \notin GF(q)$, then

$$|C_{{S_f}^{(A,B)},{S_g}^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + F(0)G(0)| \leq \begin{cases} q^{e/2}(q^2-q) & \text{if } B/B_1 \in GF(q) \\ q^{e/2}(q^2-1) & \text{if } B/B_1 \notin GF(q). \end{cases}$$

Proof: For any τ we have

$$C_{{S_f}^{(A,B)},{S_g}^{(A',B')}}(\tau) = \sum_{u,v\in GF(q)} N_\tau(u,v)F(u)G(v) - F(0)G(0),$$

where $N_\tau(u,v)$ denotes the number of solutions in $GF(q^e)$ to the equations

$$tr_q^{q^e}(Ax + Bx^{p+1}) = u$$
$$tr_q^{q^e}(A'\alpha^\tau x + B'\alpha^{(p+1)\tau}x^{p+1}) = v.$$

It follows from Lemma 1 that

$$\begin{aligned} q^2 N_\tau(u,v) &= \sum_{x\in GF(q^e)}\sum_{\lambda,\xi\in GF(q)} \chi_q[\xi tr_q^{q^e}(Ax+Bx^{p+1}) - \xi u] \\ &\quad \cdot\chi_q[\lambda tr_q^{q^e}(A_1x + B_1x^{p+1}) - \lambda v] \\ &= \sum_{\lambda,\xi\in GF(q)} \chi_q(-\xi u - \lambda v)\sum_{x\in GF(q^e)} \chi_q[tr_q^{q^e}((A\xi + A_1\lambda)x \\ &\quad + (B\xi + B_1\lambda)x^{p+1})] \\ &= \sum_{\lambda,\xi\in GF(q)} \chi_q(-\xi u - \lambda v)\sum_{x\in GF(q^e)} \chi_{q^e}((A\xi + A_1\lambda)x \\ &\quad + (B\xi + B_1\lambda)x^{p+1}) \end{aligned}$$

Thus

$$\begin{aligned} N_\tau(u,v) &= q^{-2}\sum_{\lambda,\xi\in GF(q)} \chi_q(-\xi u - \lambda v) \\ &\quad \sum_{x\in GF(q^e)} \chi_{q^e}((A\xi + A_1\lambda)x + (B\xi + B_1\lambda)x^{p+1}) \\ &= q^{-2}\sum_{\lambda,\xi\in GF(q)} \chi_q(-\xi u - \lambda v)T_\tau(\xi,\lambda). \end{aligned}$$

where

$$T_\tau(\xi,\lambda) = \sum_{x\in GF(q^e)} \chi_{q^e}((A\xi + A_1\lambda)x + (B\xi + B_1\lambda)x^{p+1}).$$

There are two cases.

1) When $B\xi + B_1\lambda = 0$, we have

$$T_\tau(\xi,\lambda) = \begin{cases} q^e & \text{if } A\xi + A_1\lambda = 0 \\ 0 & \text{if } A\xi + A_1\lambda \neq 0. \end{cases}$$

2) When $B\xi + B_1\lambda \neq 0$, we have $T_\tau(\xi,\lambda) = \psi(B\xi + B_1\lambda)S(1)$ if $A\xi + A_1\lambda = 0$ and $T_\tau(\xi,\lambda) = \chi_{q^e}[(A\xi + A_1\lambda)x_0 + (B\xi + B_1\lambda)x_0{}^{p+1}]\cdot\psi(B\xi + B_1\lambda)S(1)$ if $A\xi + A_1\lambda \neq 0$. where x_0 is the unique solution in $GF(q^e)$ to the equation

$$(B\xi + B_1\lambda)^p x^{p^2} + (B\xi + B_1\lambda)x + (A\xi + A_1\lambda)^p = 0.$$

Therefore,

$$\begin{aligned} N_\tau(u,v) &= q^{-2}\Bigg(\sum_{\substack{\lambda,\xi\in GF(q)\\ B\xi+B_1\lambda=0\\ A\xi+A_1\lambda=0}} q^e\chi_q(-\xi u - \lambda v) \\ &\quad + S(1)\sum_{\substack{\lambda,\xi\in GF(q)\\ B\xi+B_1\lambda\neq 0\\ A\xi+A_1\lambda=0}} \chi_q(-\xi u - \lambda v)\psi(B\xi + B_1\lambda) \\ &\quad + S(1)\sum_{\substack{\lambda,\xi\in GF(q)\\ B\xi+B_1\lambda\neq 0\\ A\xi+A_1\lambda\neq 0}} \chi_q(-\xi u - \lambda v) \\ &\quad \cdot\chi_{q^e}[(A\xi + A_1\lambda)x_0 + (B\xi + B_1\lambda)x_0{}^{p+1}] \\ &\quad \cdot\psi(B\xi + B_1\lambda))\Bigg) \\ &= q^{-2}(W_1 + W_2 + W_3). \end{aligned}$$

A. Calculation of W_1

There are two cases for W_1.

1) If $A/A_1 \in GF(q)$, then

$$\begin{aligned} W_1 &= q^e \sum_{\substack{\lambda,\xi \in GF(q) \\ B\xi + B_1\lambda = 0 \\ A\xi + A_1\lambda = 0}} \chi_q(-\xi u - \lambda v) \\ &= \begin{cases} q^e \sum_{\lambda \in GF(q)} \chi_q[(\frac{B_1}{B}u - v)\lambda] & \text{if } A_1B = AB_1 \\ q^e & \text{if } A_1B \neq AB_1 \end{cases} \\ &= \begin{cases} q^{e+1} & \text{if } A_1B = AB_1 \text{and } B_1u = Bv \\ 0 & \text{if } A_1B = AB_1 \text{and } B_1u \neq Bv \\ q^e & \text{if } A_1B \neq AB_1. \end{cases} \end{aligned}$$

2) If $A/A_1 \notin GF(q)$, then $W_1 = q^e$.

B. Calculation of W_2

For W_2, if $A \neq 0$, $A/A_1 \in GF(q)$, $A_1u \neq Av$, and $B_1A \neq A_1B$, then

$$\begin{aligned} W_2 &= S(1) \sum_{\substack{\lambda,\xi \in GF(q) \\ A\xi + A_1\lambda = 0}} \chi_q(-\xi u - \lambda v)\psi(B\xi + B_1\lambda) \\ &= S(1) \sum_{\lambda \in GF(q)} \chi_q\left[\left(\frac{A_1}{A}u - v\right)\lambda\right] \\ &\quad \cdot\psi\left[\left(B_1 - \frac{A_1}{A}B\right)\lambda\right] \\ &= S(1)\psi\left(B_1 - \frac{A_1}{A}B\right) \\ &\quad \cdot \sum_{\lambda \in GF(q)} \chi_q\left[\left(\frac{A_1}{A}u - v\right)\lambda\right]\psi(\lambda) \\ &= S(1)\Gamma(\psi, \chi_q)\psi\left(\frac{AB_1 - A_1B}{A_1u - Av}\right), \end{aligned}$$

where [15, Theorem 5.15]

$$\begin{aligned} \Gamma(\psi, \chi_q) &\stackrel{\text{def}}{=} \sum_{u \in GF(q)} \psi(u)\chi_q(u) \\ &= \begin{cases} (-1)^{n-1}q^{1/2} & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{n-1}i^n q^{1/2} & \text{if } p \equiv 3 \pmod 4. \end{cases} \end{aligned}$$

Note that $\psi(x/y) = \psi(xy)$ for any $y \neq 0$.

We have $W_2 = 0$ in all other cases.

C. Estimation of W_3

Finally, we must compute W_3. Let

$$V = |\left\{(\lambda, \xi) \in GF(q)^2 | B\xi + B_1\lambda \neq 0, A\xi + A_1\lambda \neq 0\right\}|.$$

There are three possibilities for V.

1) If $A/A_1 \in GF(q)$ and $B/B_1 \in GF(q)$, then

$$V = \begin{cases} q^2 - 2q + 1 & \text{if } AB_1 \neq A_1B \\ q^2 - q & \text{if } AB_1 = A_1B. \end{cases}$$

2) If $A/A_1 \in GF(q)$ and $B/B_1 \notin GF(q)$, or $A/A_1 \notin GF(q)$ and $B/B_1 \in GF(q)$, then $V = q^2 - q$.
3) If $A/A_1 \notin GF(q)$ and $B/B_1 \notin GF(q)$, then $V = q^2 - 1$.

This leads to four cases of upper bounds for $|W_3|$, where

$$\begin{aligned} |W_3| &= S(1) \sum_{\substack{\lambda,\xi \in GF(q) \\ B\xi + B_1\lambda \neq 0 \\ A\xi + A_1\lambda \neq 0}} \chi_q(-\xi u - \lambda v)\chi_{q^e}[(A\xi + A_1\lambda)x_0 \\ &\quad + (B\xi + B_1\lambda){x_0}^{p+1}]\psi(B\xi + B_1\lambda) \end{aligned} \tag{2}$$

$$\begin{aligned} &= q^{e/2} \sum_{\substack{\lambda,\xi \in GF(q) \\ B\xi + B_1\lambda \neq 0 \\ A\xi + A_1\lambda \neq 0}} \chi_q(-\xi u - \lambda v)\chi_{q^e}[(A\xi + A_1\lambda)x_0 \\ &\quad + (B\xi + B_1\lambda){x_0}^{p+1}]\psi(B\xi + B_1\lambda), \end{aligned}$$

since $|S(1)| = p^{(2m+1)/2} = p^{en/2} = q^{e/2}$.

1) If $A/A_1 \in GF(q)$, $B/B_1 \in GF(q)$, and $AB_1 \neq A_1B$, then $|W_3| \leq q^{e/2}(q^2 - 2q + 1)$.
2) If $A/A_1 \in GF(q)$ and $AB_1 = A_1B$, then $|W_3| \leq q^{e/2}(q^2 - q)$.
3) If $A/A_1 \in GF(q)$ and $B/B_1 \notin GF(q)$, or $A/A_1 \notin GF(q)$ and $B/B_1 \in GF(q)$, then $|W_3| \leq q^{e/2}(q^2 - q)$.
4) If $A/A_1 \notin GF(q)$ and $B/B_1 \notin GF(q)$, then $|W_3| \leq q^{e/2}(q^2 - 1)$.

D. Bounds for Cross-Correlations

In every case we have

$$\begin{aligned} |N(u, v) - q^{-2}(W_1 + W_2)| &= q^{-2}|W_3| \\ &< \epsilon \end{aligned}$$

for some error term ϵ. It follows that

$$\begin{aligned} |C_{S_f(A,B),S_g(A',B')}(\tau) &- q^{-2} \sum_{u,v \in GF(q)} (W_1 + W_2)F(u)G(v) \\ &\quad + F(0)G(0)| \\ &< q^{-2} \sum_{u,v \in GF(q)} |\epsilon F(u)G(v)| \\ &= q^{-2} \sum_{u,v \in GF(q)} \epsilon \\ &= \epsilon. \end{aligned}$$

Of course W_1 and W_2 depend on u and v.

Evaluating these sums in various cases completes the proof of Theorem 1. ■

The bound on $|W_3|$ appears to be rather weak – we have simply assumed that every term in a sum of plus ones and minus ones is a plus one, the worst possible case. It is quite possible that tighter bounds hold. The given bound arises from a sum involving χ_{q^e}, equation (2). We have $\chi_{q^e}(x) = \chi_q(tr_q^{q^e}(x))$. This can be used to rewrite the right hand side of equation (2) in the form

$$|W_3| = q^{e/2}|\sum_{\substack{\lambda,\xi \in GF(q) \\ A\xi + A_1\lambda \neq 0}} \chi_q(C\xi + D\lambda)\psi(B\xi + B_1\lambda)|,$$

which looks like a character sum of a type that has been analyzed. However, the terms C and D depend on x_0, which in turn depends on ξ and λ, so there is no apparent way to simplify this expression and obtain a tighter bound.

V. Correlations of Generalized Geometric Sequences When $en = 2m$

In this section we suppose that $q^e = p^{2m}$. That is, $en = 2m$. The section consists of a proof of the following theorem

Theorem 2: Let ${S_f}^{(A,B)}, {S_g}^{(A',B')}$ be generalized geometric sequences based on the same α and k, as defined in equation (1). Assume that $A, B, A', B' \neq 0$, $k = p+1, q^e = p^{en} = p^{2m}$, and $0 \leq \tau \leq q^e - 2$. Let $A_1 = A'\alpha^\tau$, $B_1 = B'\alpha^{(p+1)\tau}$, and let Δ be as in equation (5). Then

1) If $A/A_1 \in GF(q)$ and $AB_1 = A_1B$, then
$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) + F(0)G(0) - q^{e-1}\sum_{u\in GF(q)} F(u)G\left(\frac{A_1}{A}u\right)| \leq q^{e/2}(q^2-q).$$

2) If e is even, $A/A_1 \in GF(q)$, $AB_1 \neq A_1B$, and $(B_1 - A_1B/A)^{(q^e-1)/(p+1)} \neq (-1)^m$, then
$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - (q^{e-2} - (-1)^m q^{e/2-2})I(f)I(g) - (-1)^m q^{e/2-1}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq \begin{cases} q^{e/2}(q^2-2q+1) & \text{if } B/B_1 \in GF(q) \\ q^{e/2}(q^2-q) & \text{if } B/B_1 \notin GF(q). \end{cases}$$

3) If e is even, $A/A_1 \in GF(q)$, $AB_1 \neq A_1B$, and $(B_1 - A_1B/A)^{(q^e-1)/(p+1)} = (-1)^m$, then
$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - (q^{e-2} + (-1)^m pq^{e/2-2})I(f)I(g) - (-1)^m pq^{e/2-1}(p+1)\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq \begin{cases} q^{e/2}(q^2-2q+1) & \text{if } B/B_1 \in GF(q) \\ q^{e/2}(q^2-q) & \text{if } B/B_1 \notin GF(q). \end{cases}$$

4) If e is odd, $A/A_1 \in GF(q)$, and $AB_1 \neq A_1B$, then
$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - (-1)^m q^{(e-3)/2}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) - (q^{e-2} - q^{(e-3)/2} + (1+(-1)^m)q^{e/2-2})I(f)I(g) - q^{(e-3)/2}(p+1)\sum_{\substack{Av\neq A_1u \\ (\frac{A_1}{A}u - v)(B_1 - \frac{A_1}{A}B) \\ \text{a } (p+1) \text{ power}}} F(u)G(v) + F(0)G(0)| \leq \begin{cases} q^{e/2}(q^2-2q+1) & \text{if } B/B_1 \in GF(q) \\ q^{e/2}(q^2-q) & \text{if } B/B_1 \notin GF(q). \end{cases}$$

5) If $A/A_1 \notin GF(q)$, then
$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + F(0)G(0)| \leq \begin{cases} q^{e/2}(q^2-1) & \text{if } AB_1 = A_1B \text{ or } B/B_1 \notin GF(q) \\ q^{e/2}(q^2-q) & \text{if } AB_1 \neq A_1B \text{ and } B/B_1 \in GF(q). \end{cases}$$

Proof: For any τ, the correlations can be expressed in terms of $N_\tau(u,v)$ and $T_\tau(\xi,\lambda)$ whose definitions are the same as in Section IV. We proceed by a similar analysis.

When $B\xi + B_1\lambda = 0$, we have
$$T_\tau(\xi,\lambda) = \begin{cases} q^e, & A\xi + A_1\lambda = 0, \\ 0, & A\xi + A_1\lambda \neq 0. \end{cases}$$

When $B\xi + B_1\lambda \neq 0$ and $A\xi + A_1\lambda = 0$, by Lemma 2 we have
$$T_\tau(\xi,\lambda) = \begin{cases} (-1)^{m+1}p^{m+1}, & \text{if } (B\xi+B_1\lambda)^{\frac{p^{2m}-1}{p+1}} = (-1)^m, \\ (-1)^m p^m, & \text{otherwise.} \end{cases}$$

When $B\xi + B_1\lambda \neq 0$, and $A\xi + A_1\lambda \neq 0$, we have $T_\tau(\xi,\lambda) \neq 0$ if and only if the equation
$$(B\xi+B_1\lambda)^p x^{p^2} + (B\xi+B_1\lambda)x + (A\xi+A_1\lambda)^p = 0 \quad (3)$$
is solvable in $GF(q^e)$. If so, let x_0 be any solution. Then $T_\tau(\xi,\lambda) = 0$ if (3) is unsolvable in $GF(q^e)$ and $T_\tau(\xi,\lambda) = (-1)^m p^m \chi_{q^e}((A\xi+A_1\lambda)x_0 + (B\xi+B_1\lambda)x_0^{p+1})$ if (3) is solvable in $GF(q^e)$.

It follows that
$$\begin{aligned} N_\tau(u,v) = q^{-2}\Bigg(& \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda=0 \\ A\xi+A_1\lambda=0}} q^e\chi_q(-\xi u-\lambda v) \\ & + \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda\neq 0 \\ A\xi+A_1\lambda=0 \\ (B\xi+B_1\lambda)^{(q^e-1)/(p+1)}=(-1)^m}} (-1)^{m+1}p^{m+1}\chi_q(-\xi u-\lambda v) \\ & + \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda\neq 0 \\ A\xi+A_1\lambda=0 \\ (B\xi+B_1\lambda)^{(q^e-1)/(p+1)}\neq(-1)^m}} (-1)^m p^m\chi_q(-\xi u-\lambda v) \\ & + \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda\neq 0 \\ A\xi+A_1\lambda\neq 0 \\ \text{(3) solvable in } GF(q^e)}} (-1)^m p^m\chi_{q^e}((A\xi+A_1\lambda)x_0 \\ & +(B\xi+B_1\lambda)x_0^{p+1})\chi_q(-\xi u-\lambda v)\Bigg) \\ = \; & q^{-2}(W_1 + (-1)^m p^m U_1 + (-1)^{m+1}p^m(p+1)U_2 \\ & +(-1)^m p^m U_3) \end{aligned}$$
where
$$\begin{aligned} W_1 &= \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda=0 \\ A\xi+A_1\lambda=0}} q^e\chi_q(-\xi u-\lambda v), \\ U_1 &= \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda\neq 0 \\ A\xi+A_1\lambda=0}} \chi_q(-\xi u-\lambda v), \\ U_2 &= \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda\neq 0 \\ A\xi+A_1\lambda=0 \\ (B\xi+B_1\lambda)^{(q^e-1)/(p+1)}=(-1)^m}} \chi_q(-\xi u-\lambda v), \\ U_3 &= \sum_{\substack{\lambda,\xi\in GF(q) \\ B\xi+B_1\lambda\neq 0 \\ A\xi+A_1\lambda\neq 0 \\ \text{(3) solvable in } GF(q^e)}} \chi_{q^e}((A\xi+A_1\lambda)x_0 \\ & +(B\xi+B_1\lambda)x_0^{p+1})\chi_q(-\xi u-\lambda v). \end{aligned}$$

W_1 has been calculated in Section 3.

A. Calculation of U_1

There are two cases for U_1. When $A/A_1 \notin GF(q)$, we have $U_1 = 0$. When $A/A_1 \in GF(q)$, we have

$$\begin{aligned} U_1 &= \sum_{\substack{\lambda \in GF(q) \\ (AB_1 - A_1B)\lambda \neq 0}} \chi_q\left[\left(\frac{A_1}{A}u - v\right)\lambda\right] \\ &= \begin{cases} 0 & \text{if } AB_1 = A_1B \\ \displaystyle\sum_{\lambda \in GF(q)^*} \chi_q\left[(\frac{A_1}{A}u - v)\lambda\right] & \text{if } AB_1 \neq A_1B \end{cases} \\ &= \begin{cases} 0 & \text{if } AB_1 = A_1B \\ q-1 & \text{if } AB_1 \neq A_1B \text{ and } A_1u = Av \\ -1 & \text{if } AB_1 \neq A_1B \text{ and } A_1u \neq Av. \end{cases} \end{aligned}$$

B. Calculation of U_2

There are two cases for U_2. When $A/A_1 \notin GF(q)$, we have $U_2 = 0$. When $A/A_1 \in GF(q)$, we consider the following equation in the unknown λ.

$$[(B_1 - A_1B/A)\lambda]^{(q^e-1)/(p+1)} = (-1)^m. \tag{4}$$

There are two subcases.

1) If $(B_1 - A_1B/A)^{(q^e-1)/(p+1)} \notin GF(q)$, then equation (4) is unsolvable in $GF(q)$, so $U_2 = 0$.
2) If $(B_1 - A_1B/A)^{(q^e-1)/(p+1)} \in GF(q)$, then equation (4) is equivalent to

$$\lambda^{(q^e-1)/(p+1)} = (-1)^m \cdot \left(B_1 - \frac{A_1}{A}B\right)^{(1-q^e)/(p+1)},$$

and the number of solutions in $GF(q)$ of equation (4) is

$$\Delta = \sum_{j=0}^{d-1} \varphi^j\left[(-1)^m \cdot \left(B_1 - \frac{A_1}{A}B\right)^{\frac{1-q^e}{p+1}}\right], \tag{5}$$

where φ is a multiplicative character of $GF(q)$ with degree $d = \gcd((q^e-1)/(p+1), q-1)$.
Thus

$$U_2 = \sum_{\substack{\lambda \in GF(q) \\ (B_1 - A_1B/A)\lambda \neq 0 \\ [(B_1 - A_1B/A)\lambda]^{(q^e-1)/(p+1)} = (-1)^m}} \chi_q\left[\left(\frac{A_1}{A}u - v\right)\lambda\right],$$

we have $U_2 = 0$ if $AB_1 = A_1B$;

$$U_2 = |\{\lambda \in GF(q) | \left[\left(B_1 - \frac{A_1}{A}B\right)\lambda\right]^{(q^e-1)/(p+1)} = (-1)^m\}|$$

if $AB_1 \neq A_1B$ and $Av = A_1u$;

$$U_2 = \sum_{\substack{\lambda \in GF(q) \\ [(B_1 - A_1B/A)\lambda]^{(q^e-1)/(p+1)} = (-1)^m}} \chi_q\left[(\frac{A_1}{A}u - v)\lambda\right]$$

if $AB_1 \neq A_1B$ and $Av \neq A_1u$.

It remains to analyze the condition

$$[(B_1 - A_1B/A)\lambda]^{(q^e-1)/(p+1)} = (-1)^m. \tag{6}$$

To simplify notation, let $\beta = B_1 - A_1B/A$. If m is even, then equation (6) is equivalent to saying that $\beta\lambda$ is a $(p+1)$ power of an element of $GF(q^e)$. If m is odd, it is equivalent to saying that $\beta\lambda$ is a $(p+1)/2$ power of an element of $GF(q^e)$, but not a $(p+1)$ power. Suppose γ is a primitive element in $GF(q^e)$ and $T = (q^e-1)/(q-1)$. We can write $\beta = \gamma^b$ and $\lambda = \gamma^{lT}$. Then equation (6) is equivalent to

$$b + lT = \begin{cases} (p+1)d & \text{for some } d \text{ if } m \text{ is even} \\ \dfrac{(p+1)d}{2} & \text{for some odd } d \text{ if } m \text{ is odd.} \end{cases} \tag{7}$$

We make use of the following lemma.

Lemma 4: For any natural numbers p, e, and n,

$$\gcd\left(p+1, \frac{p^{en}-1}{p^n-1}\right) = \begin{cases} p+1 & \text{if } e \text{ is even} \\ 1 & \text{if } e \text{ is odd.} \end{cases}$$

Proof: We have

$$\begin{aligned} (p^{en}-1)/(p^n-1) &= p^{(e-1)n} + p^{(e-2)n} + \cdots + p^n + 1 \\ &= \begin{cases} (p+1)(p^{(e-2)n} + p^{(e-4)n} + \cdots + 1) & \text{if } e \text{ is even} \\ (p+1)(p^{(e-2)n} + p^{(e-4)n} + \cdots + p) + 1 & \text{if } e \text{ is odd.} \end{cases} \end{aligned}$$

The lemma follows. ∎

There are four cases to consider.

1) Suppose m and e are even. Then equation (7) has a solution for a given l if and only if $(p+1)$ divides b. This is equivalent to β being a $(p+1)$ power. Thus

$$U_2 = \begin{cases} 0 & \text{if } AB_1 = A_1B \text{ or } \beta \text{ is not a } (p+1) \text{ power} \\ q-1 & \text{if } AB_1 \neq A_1B,\ Av = A_1u \\ & \text{and } \beta \text{ is a } (p+1) \text{ power} \\ -1 & \text{otherwise.} \end{cases}$$

2) Suppose m is even and e is odd, so that n is even and $n/2$ is even. Then T and $(p+1)$ are relatively prime, so for each b there is at least one pair (l_0, d_0) that satisfies equation (7). Every other pair that satisfies this equation has the form $(l_0 + i(p+1), d_0 + iT)$. Thus there are $(q-1)/(p+1)$ choices of λ for which equation (7) has a solution. They all have the form $\lambda_0\delta^{i(p+1)}$, where $\delta = \gamma^T$ is primitive in $GF(q)$ and $\lambda_0 = \delta^{l_0}$. Also, for any y, $y\lambda_0$ is a $(p+1)$ power in $GF(q^e)$ if and only if $y\beta$ is a $(p+1)$ power in $GF(q^e)$. It follows that

$$\begin{aligned} U_2 &= \\ &\begin{cases} 0, \text{if } AB_1 = A_1B \\ \dfrac{q-1}{p+1}, \text{if } AB_1 \neq A_1B \text{ and } Av = A_1u \\ \dfrac{1}{p+1}\displaystyle\sum_{x \in GF(q)^*} \chi_q\left[(\frac{A_1}{A}u - v)\lambda_0 x^{p+1}\right], \text{otherwise} \end{cases} \\ &= \begin{cases} 0 & \text{if } AB_1 = A_1B \\ \dfrac{q-1}{p+1} & \text{if } AB_1 \neq A_1B \text{ and } Av = A_1u \\ \dfrac{-p^{n/2+1}-1}{p+1} & \text{if } AB_1 \neq A_1B,\ Av \neq A_1u, \\ & \text{and } (\frac{A_1}{A}u - v)\beta \text{ is a } (p+1) \text{ power} \\ \dfrac{p^{n/2}-1}{p+1} & \text{otherwise.} \end{cases} \end{aligned}$$

3) Suppose m is odd and e is even. Then equation (7) has a solution for a given l if and only if $(p+1)/2$ divides

b and $(p+1)$ does not. This is equivalent to β being a $(p+1)/2$ power but not a $(p+1)$ power. Thus

$$U_2 = \begin{cases} 0 & \text{if } AB_1 = A_1B,\ \beta \text{ is not a } (p+1)/2 \text{ power, or } \beta \text{ is a } (p+1) \text{ power} \\ q-1 & \text{if } AB_1 \neq A_1B,\ Av = A_1u \text{ and } \beta \text{ is a } (p+1)/2 \text{ power but not a } (p+1) \text{ power} \\ -1 & \text{otherwise.} \end{cases}$$

4) Suppose m and e are odd. Thus n is even and $n/2$ is odd. Again, for each b there is at least one pair (l_0, d_0) that satisfies the equation $b + lT = d(p+1)/2$. Every other pair that satisfies this equation has the form $(l_0 + i(p+1)/2, d_0 + iT)$. Since $(p+1)$ is even, T must be odd. In particular, there is a solution with d odd, so we may assume d_0 is odd. Every other solution to equation (7) has the form $(l_0 + i(p+1), d_0 + 2iT)$. As in the case when m is even and e is odd,

$$U_2 = \begin{cases} 0 & \text{if } AB_1 = A_1B \\ \dfrac{q-1}{p+1} & \text{if } AB_1 \neq A_1B \text{ and } Av = A_1u \\ \dfrac{p^{n/2+1}-1}{p+1} & \text{if } AB_1 \neq A_1B,\ Av \neq A_1u, \text{ and } (\frac{A_1}{A}u - v)\beta \text{ is a } (p+1)/2 \text{ power but not a } (p+1) \text{ power} \\ \dfrac{-p^{n/2}-1}{p+1} & \text{otherwise.} \end{cases}$$

C. Estimation of U_3

To upper bound U_3 it is useful to first compute the following cardinalities:

$$|\{(\xi,\lambda) \in GF(q)^2 | B\xi + B_1\lambda \neq 0, A\xi + A_1\lambda = 0\}| = \begin{cases} q-1 & \text{if } A/A_1 \in GF(q) \text{ and } AB_1 \neq A_1B \\ 0 & \text{otherwise,} \end{cases}$$

$$|\{(\xi,\lambda) \in GF(q)^2 | B\xi + B_1\lambda = 0, A\xi + A_1\lambda = 0\}| = \begin{cases} q & \text{if } A/A_1 \in GF(q) \text{ and } AB_1 = A_1B \\ 1 & \text{otherwise,} \end{cases}$$

$$|\{(\xi,\lambda) \in GF(q)^2 | B\xi + B_1\lambda = 0, A\xi + A_1\lambda \neq 0\}| = \begin{cases} q-1 & \text{if } B/B_1 \in GF(q) \text{ and } AB_1 \neq A_1B \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$\begin{aligned} |U_3| &\leq |\{(\xi,\lambda) \in GF(q)^2 | B\xi + B_1\lambda \neq 0, A\xi + A_1\lambda \neq 0, \text{ and equation (3) is solvable in } GF(q^e)\}| \\ &\leq |\{(\xi,\lambda) \in GF(q)^2 | B\xi + B_1\lambda \neq 0, A\xi + A_1\lambda \neq 0\}| \\ &= \begin{cases} q^2-2q+1 & \text{if } A/A_1 \in GF(q), AB_1 \neq A_1B, \text{ and } B/B_1 \in GF(q) \\ q^2-q & \text{if } A/A_1 \in GF(q), AB_1 \neq A_1B, \text{ and } B/B_1 \notin GF(q) \\ q^2-q & \text{if } A/A_1 \in GF(q) \text{ and } AB_1 = A_1B \\ q^2-q & \text{if } A/A_1 \notin GF(q), AB_1 \neq A_1B, \text{ and } B/B_1 \in GF(q) \\ q^2-1 & \text{if } A/A_1 \notin GF(q), AB_1 \neq A_1B, \text{ and } B/B_1 \notin GF(q) \\ q^2-1 & \text{if } A/A_1 \notin GF(q) \text{ and } AB_1 = A_1B. \end{cases} \end{aligned}$$

D. Bounds for Cross-Correlations

As before, we have

$$\begin{aligned} N_\tau(u,v) - q^{-2}(W_1 + (-1)^m p^m U_1 + (-1)^{m+1} p^m (p+1) U_2) \\ = (-1)^m q^{-2} p^m U_3 \leq \epsilon \end{aligned}$$

for some error term ϵ. It follows that

$$\begin{aligned} &|C_{S_f{}^{(A,B)}, S_g{}^{(A',B')}}(\tau) + F(0)G(0) \\ &\quad - q^{-2} \sum_{u,v \in GF(q)} (W_1 + (-1)^m p^m U_1 \\ &\quad + (-1)^{m+1} p^m (p+1) U_2) F(u)G(v)| \\ &\quad < q^{-2} \sum_{u,v \in GF(q)} |\epsilon F(u)G(v)| \\ &\quad = q^{-2} \sum_{u,v \in GF(q)} \epsilon. \end{aligned}$$

Again, W_1, U_1, U_2, and ϵ depend on u and v.

Computing the sums for W_1 and U_1 is straightforward. For U_2, suppose first that e is even. The only nonzero case is when $A/A_1 \in GF(q)$ and $\beta = B_1 - A_1B/A$ is not a $(p+1)$ power. In this case we have

$$\sum_{u,v} U_2 F(u)G(v) = q \sum_u F(u) G(\frac{A_1}{A}u) - I(f)I(g).$$

Now suppose that e is odd. The only nonzero case is when $A/A_1 \in GF(q)$ and $AB_1 \neq A_1B$. In this case we have

$$\begin{aligned} \sum_{u,v} U_2 F(u)G(v) &= \frac{q-1}{p+1} \sum_u F(u) G(\frac{A_1}{A}u) \\ &\quad + \frac{(-1)^{m+1} p q^{1/2} - 1}{p+1} \sum_{\substack{Av \neq A_1u \\ (\frac{A_1}{A}u - v)(B_1 - A_1\frac{B}{A}) \text{ a } (p+1) \text{ power}}} F(u)G(v) \\ &\quad + \frac{(-1)^m q^{1/2} - 1}{p+1} \sum_{\substack{Av \neq A_1u \\ (\frac{A_1}{A}u - v)(B_1 - A_1\frac{B}{A}) \text{ not a } (p+1) \text{ power}}} F(u)G(v) \\ &= \frac{q-1}{p+1} \sum_u F(u) G(\frac{A_1}{A}u) \\ &\quad - (-1)^m q^{1/2} \sum_{\substack{Av \neq A_1u \\ (\frac{A_1}{A}u - v)(B_1 - A_1\frac{B}{A}) \text{ a } (p+1) \text{ power}}} F(u)G(v) \\ &\quad + \frac{(-1)^m q^{1/2} - 1}{p+1} \sum_{Av \neq A_1u} F(u)G(v) \\ &= \left(\frac{q - (-1)^m q^{1/2}}{p+1}\right) \sum_u F(u) G(\frac{A_1}{A}u) \\ &\quad - (-1)^m q^{1/2} \sum_{\substack{Av \neq A_1u \\ (\frac{A_1}{A}u - v)(B_1 - A_1\frac{B}{A}) \text{ a } (p+1) \text{ power}}} F(u)G(v) \\ &\quad + \frac{(-1)^m q^{1/2} - 1}{p+1} I(f)I(g). \end{aligned}$$

This completes the proof of Theorem 2. ■

VI. Characteristic Two

A similar analysis can be given in the case when $p = 2$. The major change is that we must use different character sum results [1]. We state the results here but omit the proofs.

Theorem 3: Suppose that $p = 2$. Let ${S_f}^{(A,B)}, {S_g}^{(A',B')}$ be generalized geometric sequences based on the same α and k, as defined in equation (1). Assume that $A, B, A', B' \neq 0$, $k = p + 1$, $q^e = p^{en} = p^{2m+1}$, and $0 \leq \tau \leq q^e - 2$. Let $A_1 = A'\alpha^\tau$ and $B_1 = B'\alpha^{(p+1)\tau}$.

1) If $A/A_1 \in GF(q)$ and $A_1B = AB_1$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-1}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq q^{(e+3)/2}.$$

2) If $A/A_1 \notin GF(q)$ and $A_1B = AB_1$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-1}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq q^{e/2}(q^2-1).$$

3) If $A_1B \neq AB_1$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + F(0)G(0)| \leq \begin{cases} q^{(e+3)/2} + q^{(e+1)/2} & \text{if } A/A_1 \in GF(q) \\ & \text{and } B/B_1 \in GF(q), \\ q^{e/2}(q^2-1) & \text{if } A/A_1 \notin GF(q) \\ & \text{and } B/B_1 \notin GF(q) \\ q^{(e+3)/2} & \text{otherwise.} \end{cases}$$

Theorem 4: Suppose that $p = 2$ and e is even. Let ${S_f}^{(A,B)}, {S_g}^{(A',B')}$ be generalized geometric sequences based on the same α and k, as defined in equation (1). Assume that $A, B, A', B' \neq 0$, $k = p + 1$, $q^e = p^{en} = p^{2m}$, and $0 \leq \tau \leq q^e - 2$. Let $A_1 = A'\alpha^\tau$ and $B_1 = B'\alpha^{(p+1)\tau}$.

1) If $A/A_1 \in GF(q)$ and $A_1B = AB_1$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-1}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq 2q^{e/2}(q^2-q).$$

2) If $A/A_1 \in GF(q)$, $AB_1 \neq A_1B$, and $B + AB_1/A_1$ is a nonzero cube, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + (-1)^m 2q^{e/2-1}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq \begin{cases} 2q^{e/2}(q^2-2q+1) & \text{if } B/B_1 \in GF(q) \\ 2q^{e/2}(q^2-q) & \text{if } B/B_1 \notin GF(q). \end{cases}$$

3) If $A/A_1 \in GF(q)$, $AB_1 \neq A_1B$, and $B + AB_1/A_1$ is not a cube, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + (-1)^m 3q^{e/2-1}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) + F(0)G(0)| \leq \begin{cases} 2q^{e/2}(q^2-2q+1) & \text{if } B/B_1 \in GF(q) \\ 2q^{e/2}(q^2-q) & \text{if } B/B_1 \notin GF(q). \end{cases}$$

4) If $A/A_1 \notin GF(q)$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + F(0)G(0)| \leq \begin{cases} 2q^{e/2}(q^2-q) & \text{if } B/B_1 \in GF(q) \\ & \text{and } AB_1 \neq A_1B \\ 2q^{e/2}(q^2-1) & \text{otherwise.} \end{cases}$$

Theorem 5: Suppose that $p = 2$ and e is odd. Let ${S_f}^{(A,B)}, {S_g}^{(A',B')}$ be generalized geometric sequences based on the same α and k, as defined in equation (1). Assume that $A, B, A', B' \neq 0$, $k = p + 1$, $q^e = p^{en} = p^{2m}$, and $0 \leq \tau \leq q^e - 2$. Let $A_1 = A'\alpha^\tau$ and $B_1 = B'\alpha^{(p+1)\tau}$. Then

1) If $A/A_1 \in GF(q)$ and $AB_1 = A_1B$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-1}\sum_{u\in GF(q)} F(u)G\left(\frac{A_1}{A}u\right) + F(0)G(0)| \leq \frac{4q^{e/2}(q^2-q)}{3}.$$

2) If $A/A_1 \in GF(q)$, $AB_1 \neq A_1B$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau) - q^{e-2}I(f)I(g) + F(0)G(0) - (-1)^m q^{e/2-2}\sum_{u\in GF(q)} F(u)G(\frac{A_1}{A}u) - (-1)^{n+m}3q^{e/2-1}\sum_{\substack{(u+\frac{A}{A_1}v)(B+\frac{A}{A_1}B_1) \\ \text{a nonzero cube}}} F(u)G(v)| \leq \begin{cases} \frac{4}{3}q^{e/2}(q^2-2q+1) & \text{if } B/B_1 \in GF(q) \\ \frac{4}{3}q^{e/2}(q^2-q) & \text{if } B/B_1 \notin GF(q). \end{cases}$$

3) If $A/A_1 \notin GF(q)$, then

$$|C_{S_f^{(A,B)},S_g^{(A',B')}}(\tau)) - q^{e-2}I(f)I(g) + F(0)G(0)| \leq \begin{cases} \frac{4}{3}q^{e/2}(q^2-q) & \text{if } AB_1 \neq A_1B \text{ and } \frac{B}{B_1} \in GF(q). \\ \frac{4}{3}q^{e/2}(q^2-1) & \text{otherwise.} \end{cases}$$

VII. Linear Complexity

In this section we consider the linear complexity of certain generalized geometric sequences. We denote by $\lambda(S)$ the linear complexity of a sequence S. Let $p = 2$ and let $n_1, n_2, \cdots, n_l$ be natural numbers with n_i at least 3. Let $n = n_1 n_2 \cdots n_l$, $q_0 = 2$, and $q_i = q_{i-1}^{n_i}$, so in particular $q = q_l$. We also let $r_1, \cdots, r_l$ be integers, with $1 \leq r_i < n_i$, let $k_i = 1 + q_{i-1}^{r_i}$, and define $f : GF(q) \to GF(2)$ by

$$f(x) = tr_{q_0}^{q_1}(tr_{q_1}^{q_2}(\cdots tr_{q_{l-1}}^{q_l}(x)^{k_{l-1}}\cdots)^{k_1}).$$

If β is primitive in $GF(q)$, then the sequence T whose ith term is $T(i) = f(\beta^i)$ is a *cascaded GMW sequence* [12]. This sequence has shifted autocorrelations equal to -1. It's linear complexity is

$$\lambda(T) = n_1 n_2^2 n_3^4 \cdots n_l^{2^{l-1}}$$

(See [12]). In this section we consider the generalized geometric sequence S whose ith term is

$$S(i) = f(tr_q^{q^e}(\alpha^i + B\alpha^{3i}))$$

for some $B \neq 0$. Also, for convenience we write $n_{l+1} = e$.

Theorem 6: If $2 \leq r_1 \leq n_1 - 2$, $1 \leq r_j \leq n_j - 2$ for $j = 2, \cdots, l-1$, and $2r_j \not\equiv 0 \pmod{n_j}$ for $j = 1, \cdots, l-1$, then the linear complexity of S is

$$\lambda(S) = n_1 n_2^2 n_3^4 \cdots n_l^{2^{l-1}} (2e)^{2^l}.$$

Proof: Key showed that the linear complexity of such a sequence equals the number of nonzero coefficients when the function

$$g(x) = f(tr_q^{q^e}(x + Bx^3)) \tag{8}$$

is expressed a polynomial [7]. Let

$$K = \{\bar{t} = (t_1, t_2, \cdots, t_l) : t_i \in \{0, r_i\}\}.$$

Let $s : K \to \{(s_1, s_2, \cdots, s_l, s_{l+1}) : 0 \leq s_i < n_i\}$ be a function with the property that whenever $\bar{t}, \bar{t}' \in K$ satisfy $t_1 = t_1', \cdots, t_j = t_j'$ for some j, s satisfies $s(\bar{t})_1 = s(\bar{t}')_1, s(\bar{t})_2 = s(\bar{t}')_2, \cdots, s(\bar{t})_{j+1} = s(\bar{t}')_{j+1}$. For any such s and $a : K \to \{1, 3\}$, let

$$\begin{aligned} h(s,a) &= \sum_{\bar{t} \in K} a(\bar{t}) \prod_{j=1}^{l} q_{j-1}^{s(\bar{t})_j + t_j} q_l^{s(\bar{t})_{l+1}} \\ &= \sum_{\bar{t} \in K} a(\bar{t}) z(\bar{t}). \end{aligned}$$

If we expand the right hand side of equation (8), the resulting polynomial can be expressed as a sum of the monomials whose exponents are the $h(s,a)$s over all possible s and a. Thus we need to see that these are all distinct.

First suppose that for some fixed s and a and for some $\bar{t} \neq \bar{t}' \in K$, the base 2 expansions of $a(\bar{t})z(\bar{t})$ and $a(\bar{t}')z(\bar{t}')$ have some nonzero term in common. We may assume that for some j, $t_1 = t_1', \cdots, t_{j-1} = t_{j-1}'$, $t_j = 0$, and $t_j' = r_j$. Then for some x (which is a power of 2), b, and c we have $z(\bar{t}) = xq_{j+1}^b$ and $z(\bar{t}') = xq_j^{r_j} q_{j+1}^c$. There are two possibilities.

1) If $z(\bar{t}) < z(\bar{t}')$, then we must have $a(\bar{t}) = 3$ and $3z(\bar{t}) \geq z(\bar{t}')$. It follows that $2z(\bar{t}) = z(\bar{t}')$. Therefore $2 = q_j^{r_j}$, which is impossible by the hypotheses.
2) If $z(\bar{t}) > z(\bar{t}')$, then we must have $a(\bar{t}') = 3$ and $3z(\bar{t}') \geq z(\bar{t})$. It follows that $2z(\bar{t}') = z(\bar{t}')$. Therefore $2q_j^{r_j} = q_{j+1}$, which is impossible by the hypotheses.

Now suppose that $h(s,a) = h(s',a')$ for some s, s', a, a'. It follows first that the number of 1s among the $a(\bar{t})$s equals the number of 1s among the $a'(\bar{t})$s. Note also that $s_1 = s_1(\bar{t})$ and $s_1' = s_1'(\bar{t})$ are independent of $\bar{t}$. If we take the reductions modulo n_1 of the exponents that occur on nonzero terms in the base two expansion of $h(s,a)$, we obtain $\{s_1, s_1 + r_1\}$ if all $a(\bar{t}) = 1$, and $\{s_1, 1 + s_1, s_1 + r_1, 1 + s_1 + r_1\}$ otherwise. We obtain $\{s_1', s_1' + r_1\}$ if all $a(\bar{t}) = 1$, and $\{s_1', 1 + s_1', s_1' + r_1, 1 + s_1' + r_1\}$ otherwise for $h(s',a')$. These sets must be equal if $h(s,a) = h(s',a')$. If $s_1 \equiv s_1' + r_1 \pmod{n_1}$ and $s_1' \equiv s_1 + r_1 \pmod{n_1}$ then $2r_1 \equiv 0 \pmod{n_1}$. This is false by hypothesis. Therefore $s_1 = s_1'$. Also, all terms with $t_1 = 1$ or $t_1' = 1$ map to $\{s_1, 1 + s_1\}$ when we reduce exponents modulo n_1, so the sum of such terms in $h(s,a)$ equals the sum of such terms in $h(s',a')$. Similarly for the terms that map to $\{s_1 + r_1, 1 + s_1 + r_1\}$. By induction, $s = s'$ and it then follows that $a = a'$.

Consequently, the linear complexity of S is the number of pairs of functions (s,a), which is the quantity given in the statement of the theorem. ∎

Thus the linear complexity for these generalized geometric sequences is larger than the linear complexity of a cascaded GMW sequence based on the same tower of fields and the same exponents by a factor of 2^{2^l}.

VIII. Conclusions - Families of Sequences

In this section we use the results of the previous sections to construct families of sequences with good pairwise correlations. We fix prime numbers p and r, natural numbers e and n, a primitive element α in $GF(p^{ne})$, and a function f from $GF(p^n)$ to $GF(r)$. As above, we let $q = p^n$ and $F(u) = \omega^u$ where ω is a complex primitive rth root of unity. Let $S_f(A,B)$ be the sequence defined in equation (1). Note that every sequence $S_f^{(A,B)}$ has a cyclic shift of the form $S_f^{(1,B)}$. Assume that f is balanced. That is, $I(f) = 0$. This is only possible if $r = p$, so we are assuming this. We also assume that f has ideal autocorrelations in the sense that

$$\sum_{u \in GF(q)} F(u)F(xu) = \begin{cases} 0 & \text{if } x \neq 1 \\ q & \text{if } x = 1. \end{cases}$$

This is equivalent to saying that the sequence whose jth element is $f(\beta^j)$, where β is a primitive element in $GF(q)$, has ideal autocorrelations. There are many examples of such sequences (for example, m-sequences, GMW sequences, and cascaded GMW sequences). Let $\mathcal{S} = \{S_f^{(1,B)} : B \in GF(q^e), B \neq 0\}$. We want to show that every pair of sequences in this set is cyclically distinct. By Theorems 1 and 2, if p is odd, then for any two sequences $S_f^{(1,B)}$ and $S_f^{(1,B')}$ in $\mathcal{S}$ and any τ,

$$|C_{S_f^{(1,B)}, S_f^{(1,B')}}(\tau)| \leq q^{e/2}(q^2 - 1) + 1 \tag{9}$$

unless

$$\begin{aligned} &\alpha^\tau \in GF(q), \alpha^\tau B = \alpha^{(p+1)\tau} B' \\ &\text{and} \sum_{u \in GF(q)} F(u)F(\alpha^\tau u) \neq 0. \end{aligned} \tag{10}$$

It follows from our assumption on the autocorrelations of f that if condition (10) holds, then $\tau = 0$, and therefore that $B = B'$. Thus the only correlation that fails to satisfy inequality (9) is

$$C_{S_f^{(1,B)}, S_f^{(1,B)}}(\tau) = q^e - 1.$$

This also implies that any two sequences in $\mathcal{S}$ are cyclically distinct and proves the following theorem.

Theorem 7: If p is odd, then $\mathcal{S}$ is a family of $q^e - 1$ $GF(p)$-ary sequences of period $q^e - 1$ all of whose cross-correlations and shifted autocorellations are bounded by

$$|C_{S_f^{(1,B)}, S_f^{(1,B')}}(\tau)| \leq q^{e/2}(q^2 - 1) + 1. \tag{11}$$

We have a similar family when p is even.

Theorem 8: If $p = 2$, then $\mathcal{S}$ is a family of $q^e - 1$ binary sequences of period $q^e - 1$ all of whose cross-correlations and shifted autocorellations are bounded by

$$|C_{S_f^{(1,B)},S_f^{(1,B')}}(\tau)| \leq \begin{cases} 2q^{e/2}(q^2-1)+1 & \text{if } e \text{ is even} \\ \frac{4}{3}q^{e/2}(q^2-1)+1 & \text{if } e \text{ is odd and } n \text{ is even} \\ q^{e/2}(q^2-1)+1 & \text{if } e \text{ and } n \text{ are odd.} \end{cases}$$

In particular, if f is as in Section VII, then the linear complexity of every sequence in $\mathcal{S}$ is large as well.

When $n = 1$ the sequences studied here reduce to one case of Gold's sequences. However, in this case our estimates of the cross-correlations are too high. For example, when $p = 2$ and e is odd, they are too high by a factor of three. We conjecture, therefore, that our estimates are too high in general. In the case when when p is odd and $en = 2m + 1$, some improvement would come if we could choose f so that $\psi(Cu + Dv)F(u)F(v)$ is small for every $C, D \in GF(q^e)$. However, the greatest improvement would come from sharper bounds on W_3. The situation is similar when en is even and when $p = 2$.

REFERENCES

[1] L. Carlitz, *Explicit evaluation of certain exponential sums*, Math. Scand., vol. 44, pp. 5–16, 1979.

[2] L. Carlitz, *Evaluation of some exponential sums over finite fields*, Math. Nachr., 1980, pp. 319–339, 1980.

[3] A. H. Chan and R. Games, *On the linear span of binary sequences from finite geometries, q odd*, IEEE Trans. Info. Theory, vol. 36, no. 3, pp. 548–552, 1990.

[4] R. Gold, *Optimal binary sequences for spread spectrum multiplexing*, IEEE Trans. Info. Theory, vol. 13, pp. 619–620, 1967.

[5] T. Kasami, *Weight distribution formula for some classes of cyclic codes*, Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R–285 (AD632574), 1966.

[6] T. Kasami, *Weight distribution of Bose-Chaudhuri-Hocquenghem codes*, Combinatorial Mathematics and its Applications. Chapel Hill, NC: University of North Carolina Press, 1969.

[7] E. L. Key, *An Analysis of the structure and complexity of nonlinear binary sequence generators*, IEEE Trans. Info. Theory, vol. IT-22, pp. 732–736, 1976.

[8] A. Klapper, *Cross-correlations of geometric sequences in characteristic two*, Designs, Codes, and Cryptography, vol. 3, pp. 347–377, 1993.

[9] A. Klapper, *d-form sequences: families of sequences with low correlation values and large linear span*, IEEE Trans. Info. Theory, vol. 41, pp. 423–431, 1995.

[10] A. Klapper, *Large families of sequences with low correlations and large linear span*, IEEE Trans. Info. Theory, vol. 42, pp. 1241–1248, 1996.

[11] A. Klapper, A. H. Chan, and M. Goresky, *Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences*, Discrete Appl. Math., vol. 46, pp. 1–20, 1993.

[12] A. Klapper, A. H. Chan, and M. Goresky, *Cascaded GMW sequences*, IEEE Trans. Info. Theory, vol. 39, pp. 177–183, 1993.

[13] P. V. Kumar and R. A. Scholtz, *Bounds on the linear span of bent sequences*, IEEE Trans. Info. Theory, vol. IT-29, pp. 854–862, 1983.

[14] A. Lempel and M. Cohn, *Maximal families of bent sequences*, IEEE Trans. Info. Theory, vol. IT-28, pp. 865–868, 1982.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, Encycl. Math. Appl., vol. 20 Reading, MA:Addision Wesley, 1983.

[16] J. No, *A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span*, Doctoral Dissertation, University of Southern California, 1988.

[17] J. No and P. V. Kumar, *A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span*, IEEE Trans. Info. Theory, vol. 35, pp. 371–379, 1989.

[18] J. D. Olsen, R. A. Scholtz, and L. R. Welch, *Bent-function sequences*, IEEE Trans. Info. Theory, vol. IT-28, pp. 858–864, 1982.

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

[20] W. Sun and Y. X. Yang, *Correlation functions of a family of generalized geometric sequences*, Discrete Appl. Math., vol. 80, pp. 193–201, 1997.

[21] W. Sun and Y. X. Yang, *Correlations of pseudo-generalized geometric sequences*, IEEE International Symposium on Information Theory, Ulm, Germany, 1997, pp. 44.