Correlation Functions of Geometric Sequences

AGNES HUI CHAN, MARK GORESKY AND ANDREW KLAPPER

Northeastern University
Boston, Massachusetts 02115

ABSTRACT

This paper considers the cross-correlation function values of a family of binary sequences obtained from finite geometries. These values are shown to depend on the intersection of hyperplanes in a projective space and the cross-correlation function values of the nonlinear feedforward functions used in the construction of the geometric sequences.

1. Introduction

Maximum period linear feedback shift register sequences with nonlinear feedforward functions have been used in modern communication systems. Many of these sequences are required to have high linear complexities, good autocorrelation and/or cross-correlation function values. Recently, Chan and Games [1] introduced a class of binary sequences obtained from finite geometries using nonlinear feedforward function $\rho : GF(q) \rightarrow GF(2)$, with q odd. They showed that these sequences have high linear complexities. Brynielsson [2] had studied similar problem with q even and established the linear complexities of these sequences in terms of the polynomial expression of the function ρ. In this paper, we consider the autocorrelation and cross-correlation functions of these sequences, and establish their values in terms of the autocorrelation and cross-correlation values of the sequence obtained from $(\rho(\beta^0), \rho(\beta), \ldots, \rho(\beta^{q-2}))$, where β is a primitive element of $GF(q)$. In the case where q is even, we show that the autocorrelation and cross-correlation function values are vastly different, making these geometric sequences viable candidates for applications in spread spectrum communications.

2. Geometric Sequences

Let q be a prime power and $GF(q^n)$ be the field of q^n elements. A q-ary m-sequence $\mathbf{R}$ of span n and period $q^n - 1$ can be generated by choosing a primitive polynomial $f(x)$ over $GF(q)$. A binary sequence $\mathbf{S}$ can be obtained from the m-sequence $\mathbf{R}$ for any choice of mapping $\rho : GF(q) \rightarrow GF(2)$ (sometimes called a "nonlinear feedforward function") by defining $S_i = \rho(R_i)$ for all $i \geq 0$. Such a sequence $\mathbf{S}$ is closely related to finite geometry and is called a *binary geometric sequence*.

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 214-221, 1991.

It is well known that the sequence **R** can be represented as $(Tr(\alpha^0), Tr(\alpha), Tr(\alpha^2), \ldots)$, where α is a root of the primitive polynomial $f(x)$ and $Tr : GF(q^n) \to GF(q)$ is the trace function. Thus

$$S_i = \rho(Tr(\alpha^i))$$

Let $v = (q^n - 1)/(q - 1)$ and $\beta = \alpha^v$. Then β is a primitive element in the base field $GF(q)$ and $Tr(\alpha^{v+i}) = \beta Tr(\alpha^i)$, so $R_{i+v} = \beta R_i$ for all $i \geq 0$. In [1], Chan and Games studied the linear complexities of these binary sequences with q odd, and proved the following result.

THEOREM. *Let* S *be a binary sequence obtained from finite geometries with* q *odd. Then*

$$\textit{linear complexity } (\mathrm{S}) = v * \textit{ linear complexity } (\mathrm{s}).$$

where $\mathrm{s} = (\rho(\beta^0), \rho(\beta), \ldots, \rho(\beta^{q-1}))$.

By choosing ρ appropriately, the linear complexity of s can be made as high as $q-1$, and so the linear complexity of S can reach $q^n - 1$. In [2] Brynielsson considered the linear complexities of binary finite geometric sequences with q even, and proved a similar result:

THEOREM. *Let* $\rho : GF(2^e) \to GF(2)$ *be represented as a polynomial* $\sum_{i=0}^{e-1} A_i x^i$ *over* $GF(2^e)$. *Then*

$$\textit{linear complexity } (\mathrm{S}) = \sum_{A_i \neq 0} n^{|i|}$$

where $|i|$ *denotes the dyadic weight of the integer* i *(i.e. the weight of the binary vector representation of* i*).*

In the latter case, the linear complexity of S is maximal if the polynomial representation of ρ has nonzero terms of every degree. Thus, for q even, the linear complexity of S has $\sum_{d=0}^{e} \binom{e}{d} n^d$ as an upper bound.

In this paper we consider the crosscorrelation of binary geometric sequences S and Z, each of period $q^n - 1$, where $S_i = \rho(Tr(A\alpha^i))$ and $Z_i = \gamma(Tr(B\alpha^i))$, and where A, B are fixed elements in $GF(q^n)$. Note that S and Z are geometric sequences with same linear feedback functions but different nonlinear feedforward functions ρ and γ. (In a later paper we will consider the crosscorrelation of geometric sequences with different feedback functions.)

3. Hyperplanes in $GF(q^n)$

The geometric sequences are based on the geometry of hyperplanes in the finite field $GF(q^n)$. The crosscorrelation of these geometric sequences is calculated by counting the number of elements in the intersections of two hyperplanes. The use of intersecting hyperplanes for evaluating crosscorrelation of pseudorandom sequences was considered by Games in [3] and our method is similar to his. In this section we review some of the basic facts concerning hyperplanes and their intersections.

Let Tr: $GF(q^n) \rightarrow GF(q)$ denote the trace function. For any $U \in GF(q)$ we define

$$H_U = \{x \in GF(q^n) | Tr(x) = U\}$$

Then H_U is an (affine) hyperplane, i.e. it is an $n-1$ dimensional vector subspace of $GF(q^n)$ which does not necessarily pass through the origin. If $V \in GF(q)$ then the hyperplanes H_U and H_V are parallel, i.e. they have no points of intersection unless $U = V$, in which case they are equal. Now let $b \in GF(q^n)$, $V \in GF(q)$, and consider the hyperplane

$$\begin{aligned} b^{-1}H_V &= \{b^{-1}y | y \in H_V\} \\ &= \{b^{-1}y | Tr(y) = V\} \\ &= \{x | Tr(bx) = V\}. \end{aligned}$$

LEMMA 1. *The hyperplanes H_U and $b^{-1}H_V$ are parallel if and only if $b \in GF(q)$.*

PROOF: If $b \in GF(q)$ then

$$\begin{aligned} b^{-1}H_V &= \{x | Tr(bx) = V\} \\ &= \{x | bTr(x) = V\} \\ &= H_{b^{-1}V}. \end{aligned}$$

Since both b and V are in $GF(q), b^{-1}V \in GF(q)$, so $H_{b^{-1}V}$ is parallel to H_U.

On the other hand, if H_U and $b^{-1}H_V$ are parallel, then we must show that $b \in GF(q)$. Let us first consider the special case when $U = 0$ and the two parallel hyperplanes $H_U = H_0$ and $b^{-1}H_V$ actually coincide. Thus,

$$x \in H_0 \text{ iff } \quad Tr(x) = 0 \text{ iff } \ Tr(bx) = V.$$

By taking $x = 0$ we see immediately that $V = 0$. Now choose $z \in GF(q^n) - H_0$. Since H_0 is a hyperplane, the addition of this one more linearly independent element will span all of $GF(q^n)$. Therefore bz may be written as a linear combination involving z and H_0,

$$bz = az + h$$

for some $a \in GF(q)$ and $h \in H_0$. We will show that $b = a \in GF(q)$. If this were false, we would have $z = h/(b-a)$. But multiplication by a preserves H_0, and multiplication by b also preserves H_0, so multiplication by $(b-a)$ preserves H_0, and so multiplication by $(b-a)^{-1}$ preserves H_0. Therefore $z \in H_0$, and this is a contradiction.

Next we consider the general case of U arbitrary and H_U not necessarily equal to $b^{-1}H_V$. As above, let $H_0 = \{x | Tr(x) = 0\}$. Then H_U, $b^{-1}H_V$, and H_0 are parallel. Thus there are translations x_1, $x_2 \in GF(q^n)$ such that

$$H_0 = H_U - x_1 = b^{-1}H_V - x_2$$

Define $V' = V - Tr(bx_2)$. Then

$$\begin{aligned} b^{-1}H_V - x_2 &= \{b^{-1}x - x_2 | Tr(x) = V\} \\ &= \{y | Tr(by + bx_2) = V\} \\ &= \{y | Tr(by) = V'\} \\ &= b^{-1}H_{V'} \end{aligned}$$

Thus $b^{-1}H_{V'} = H_0$ and the preceding special case applies to this situation, from which we conclude that $b \in GF(q)$.

LEMMA 2. *If $b \in GF(q^n) - GF(q)$ then for any $U, V \in GF(q)$, the number of elements in the intersection $H_U \cap b^{-1}H_V$ is precisely q^{n-2}.*

PROOF: By lemma 1, the hyperplaces H_U and $b^{-1}H_V$ are not parallel. If two hyperplanes are not parallel, then their intersection is a hyperplane inside each, i.e. it is an $n-2$ dimensional (affine) subspace of $GF(q^n)$. Therefore it contains q^{n-2} points.

4. Cross-Correlation Functions

In the notation of section 2, we consider a primitive element $\alpha \in GF(q^n)$ and two geometric sequences based on this element,

$$S_i = \rho(Tr(A\alpha^i)), \quad Z_i = \gamma(Tr(B\alpha^i))$$

Recall that the cross-correlation function associated with the sequences S and Z is given by:

$$C_{\mathbf{S},\mathbf{Z}}(\tau) = \sum_{t=0}^{q^n-2} (-1)^{S_t}(-1)^{Z_{t+\tau}},$$

where $0 \le \tau \le q^n - 2$. Using the notation $\Phi(\mu) = (-1)^{\rho(\mu)}$ and $\Gamma(\mu) = (-1)^{\gamma(\mu)}$ for $\mu \in GF(q)$, and denoting by $\beta = \alpha^v$ the corresponding primitive element of $GF(q)$, we have the following definitions.

DEFINITION. *The short cross-correlation function is defined as*

$$c_{\rho,\gamma}(m) = \sum_{\mu \in GF(q)} \Phi(\mu)\Gamma(\mu\beta^m).$$

DEFINITION. *The imbalance of ρ, denoted by $I(\rho)$, is defined by*

$$I(\rho) = \sum_{\mu \in GF(q)} (-1)^{\rho(\mu)}.$$

The imbalance of a nonlinear function ρ measures the difference in the number of 0-images and the number of 1-images under the mapping ρ. Let d represent the phase displacement of the two binary sequences S and Z, that is, $\alpha^d = B/A \in GF(q^n)$, then we prove

THEOREM. *Let* S *and* Z *be two binary geometric sequences of span* n *with period* $q^n - 1$ *as above. Let* d *denote their phase shift and let* $v = (q^n - 1)/(q - 1)$. *Then the cross-correlation function* $C_{\mathbf{S},\mathbf{Z}}(\tau)$ *is given by:*

$$C_{\mathbf{S},\mathbf{Z}}(\tau) = q^{n-1}c_{\rho,\gamma}(m) - \Phi(0)\Gamma(0) \quad \text{if } d + \tau = mv$$

and

$$C_{\mathbf{S},\mathbf{Z}}(\tau) = q^{n-2}I(\rho)I(\gamma) - \Phi(0)\Gamma(0) \qquad \textit{otherwise.}$$

Observe that if q is even then it is possible to choose $\rho : GF(2^e) \to GF(2)$ such that exactly half of the elements in $GF(2^e)$ are mapped to 0 and the other half to 1. Then $C_{\mathbf{S},\mathbf{Z}}(\tau) = \Phi(0)\Gamma(0) = \pm 1$ for $d + \tau \neq iv$. However if q is odd then the imbalance is always at least 1, so the crosscorrelation is always greater than or equal to $q^{n-2} - 1$.

PROOF OF THEOREM:

The cross correlation is

$$C_{\mathbf{S},\mathbf{Z}}(\tau) = \sum_{t=1}^{p^{n-1}} \Phi(Tr(A\alpha^t))\Gamma(Tr(B\alpha^{t+\tau}))$$

Substituting $x = A\alpha^t$, $B/A = \alpha^d$, and $b = \alpha^{d+\tau}$ we obtain,

$$C_{\mathbf{S},\mathbf{Z}}(\tau) = \sum_{x \in GF(q^n)} \Phi(Tr(x))\Gamma(Tr(bx)) - \Phi(Tr(0))\Gamma(Tr(0))$$

To each $x \in GF(q^n)$ there corresponds unique elements $U = Tr(x)$ and $V = Tr(bx)$ in $GF(q)$. Thus the elements of $GF(q^n)$ are divided into disjoint subsets of the form $H_U \cap b^{-1}H_V$, so the above sum may be rewritten as,

$$C_{\mathbf{S},\mathbf{Z}}(\tau) = \sum_{U \in GF(q)} \sum_{V \in GF(q)} |H_U \cap b^{-1}H_V|\Phi(U)\Gamma(V) - \Phi(0)\Gamma(0)$$

According to lemma 2, the number of points $|H_U \cap b^{-1}H_V|$ in this intersection is q^{n-2} unless $b \in GF(q)$, i.e. unless $d + \tau$ is a multiple of $v = (q^n - 1)/(q - 1)$. So in the first case we obtain

$$\begin{aligned} C_{\mathbf{S},\mathbf{Z}}(\tau) &= q^{n-2} \sum_U \Phi(U) \sum_V \Gamma(V) - \Phi(0)\Gamma(0) \\ &= q^{n-2}I(\rho)I(\gamma) - \Phi(0)\Gamma(0) \end{aligned}$$

as claimed. In the second case, if $b \in GF(q)$, then $d + \tau$ is some multiple, say m, of $v = (q^n - 1)/(q - 1)$. Thus

$$b = \alpha^{d+\tau} = \beta^m$$

where $\beta = \alpha^v$ is the primitive element of $GF(q)$. As observed above,

$$\beta^{-m} H_V = H_{\beta^{-m} V}$$

which has no points in common with H_U unless $U = \beta^{-m} V$. Therefore the only nonzero terms in the above double sum give

$$\begin{aligned} C_{\mathbf{S},\mathbf{Z}}(\tau) &= q^{n-1} \sum_{U \in GF(q)} \Phi(U)\Gamma(\beta^m U) - \Phi(0)\Gamma(0) \\ &= q^{n-1} c_{\rho,\gamma}(m) - \Phi(0)\Gamma(0) \end{aligned}$$

as claimed.∎

Recall that the autocorrelation function of a sequence S is given by

$$A_{\mathbf{S}}(\tau) = \sum_{t=0}^{q^n-2} (-1)^{S_t} (-1)^{S_{t+\tau}}.$$

To compute the values of $A_{\mathbf{S}}(\tau)$, we simply substitute S with Z in $C_{\mathbf{S},\mathbf{Z}}(\tau)$ and obtain the following result.

COROLLARY. *The autocorrelation function of the sequence* S *is given by:*

$$A_{\mathbf{S}}(\tau) = q^{n-1} c_\rho(m) - 1 \qquad \text{if } \tau = mv$$

and

$$A_{\mathbf{S}}(\tau) = q^{n-2} I(\rho)^2 - 1 \qquad \text{otherwise.}$$

where $c_\rho(m)$ corresponds to the short autocorrelation function, defined as

$$c_\rho(m) = \sum_{mu \in GF(q)} \Phi(\mu)\Phi(\mu\beta^m).$$

5. Absolute Correlation Functions

The notion of "absolute" cross correlation between two pseudorandom sequences with period $q^n - 1$ has also been studied in the literature [3]. The absolute cross correlation counts only the coincident *ones* in the sequences.

DEFINITION. *The absolute cross correlation function between two sequences* S *and* Z *is defined as*

$$B_{\mathbf{S},\mathbf{Z}}(\tau) = \sum_{t=0}^{q^n-2} S_t Z_{t+\tau}.$$

To consider the absolute cross correlation functions of geometric sequences, the same argument as above works, but we must replace the "short" cross correlation with the "absolute short" cross correlation,

$$a_{\rho,\gamma}(m) = \sum_{\mu \in GF(q)} \rho(\mu)\gamma(\mu\beta^m)$$

and we replace the imbalance $I(\rho)$ by the weight, $W(\rho)$, defined by

$$W(\rho) = \sum_{\mu \in GF(q)} \rho(\mu).$$

Then theorem 1 becomes

THEOREM 1'. *With the same hypotheses as theorem 1, the absolute crosscorrelation function of* S *and* Z *is*

$$B_{S,Z}(\tau) = \begin{cases} q^{n-1}a_{\rho,\gamma}(m) - \rho(0)\gamma(0) & \text{if} \quad d+\tau = mv \\ q^{n-2}W(\rho)W(\gamma) - \rho(0)\gamma(0) & \text{otherwise} \end{cases}$$

6. Applications

G.M.W. Sequences. In [3], R. Games calculated the crosscorrelation of an m-sequence and a GMW sequence having the same primitive polynomial. His method involved intersecting hyperplanes, and our theorem 1 is similar to his. In this paragraph, we show how to recover his result.

Suppose a, b, and r are integers, with a dividing b, and with r relatively prime to $2^a - 1$. Fix a primitive element $\alpha \in GF(2^b)$. The sequence GMW$(b, a; r)$ is the sequence given by

$$S_i = Tr_1^a(Tr_a^b(\alpha^i)^r).$$

The GMW sequence is a geometric sequence in the sense of §2: take $q = 2^a$, $n = b/a$, and $\rho(\mu) = Tr_1^a(\mu^r)$ for any $\mu \in GF(2^a)$. In the notation of §2 we have

$$S_i = \rho(Tr(\alpha^i)).$$

Similarly the m-sequence

$$Z_i = Tr_1^a(Tr_a^b(\alpha^i)) = Tr_1^b(\alpha^i)$$

is the geometric sequence corresponding to $\gamma(\mu) = Tr_1^a(\mu)$. If we apply theorem 1' to find the absolute crosscorrelation between these two sequences, we obtain

COROLLARY 2 [3]. *Given integers a, b, and r, with a dividing b and with $(r, 2^a - 1) = 1$, let S_i be the sequence GMW$(b, a; r)$ and let Z_i be the m-sequence based on the same primitive polynomial. Then*

$$B_{S,Z}(\tau) = \begin{cases} (2^a)^{\frac{b}{a}-1}a_{\rho,\gamma}(k) = 2^{b-a}B_{w,u}(k) & \text{if} \quad \tau = kv \\ (2^a)^{\frac{b}{a}-2}2^{a-1}2^{a-1} = 2^{b-2} & \text{otherwise} \end{cases}$$

where $v = (2^b - 1)/(2^a - 1)$, where u and w are the m-sequences of span a given by

$$u_i = Tr_1^a(\beta^i) \qquad w_i = Tr_1^a(\beta^{ir}).$$

with $\beta = \alpha^v$ a primitive element of $GF(2^a)$.

We remark that for many values of r, these "short" crosscorrelation values are known, or can be estimated [6] [7] .

Bent Sequences. The method in this paper may be used to calculate crosscorrelation values of Bent Sequences [5], the computation is fairly straightforward and will not be carried out here.

ACKNOWLEDGEMENT

We would like to thank R. Games for reading a first draft of this paper and for making several valuable suggestions.

REFERENCES

1. A. H. Chan and R. A. Games, *On the Linear Span of Binary Sequences from Finite Geometries, q Odd*, Proceedings of Crypto86, page 405–417.
2. L. Brynielsson, *On the Linear Complexity of Combined Shift Register*, Proceedings of Eurocrypt84, page 156–160.
3. R. A. Games, *Crosscoreelation of m-Sequences and GMW- Sequences With the Same Primitive Polynomial*, Discrete Applied Mathematics 12 (1985), pages 139–146.
4. R. A. Games, *The Geometry of m-Sequences: Three-Valued Cross-correlations and Quadrics in Finite Projective Geometry*, SIAM J. Alg. Disc. Mathematics, vol 7 (1986), pages 43–52.
5. J. Olson, R. A. Scholtz and L. R. Welch, *Bent Function Sequences*, IEEE Trans. on Information Theory, vol. IT–28 (1982), pages 858–864.
6. T. Helleseth, *Some Results About the Cross-Correlation Function Between Two Maximal Linear Sequences*, Discrete Math 16 (1976), pages 209–232.
7. D. Sarwate and M. Pursley, *Crosscorrelation Properties of Pseudorandom and Related Sequences*, IEEE Proceedings, vol. 68 (1980), pages 593–619.