Notes on q-ary Interleaved Sequences *

Shaoquan Jiang[1], Zongduo Dai[1] and Guang Gong[2]

[1] State Key Lab. of Information Security
Dept. of Math., Graduate School
University of Science and Technology of China
100039-08, Beijing, China
Email: yangdai@mimi.cnc.ac.cn

[2] Department of Combinatorics & Optimization
University of Waterloo,
Waterloo, Ontario N2L 3G1, Canada
Email: ggong@cacr.math.uwaterloo.ca

Abstract. A sequence u over a finite field F_q is called an $(f(x), m)$-interleaved sequence [1] if $f(x)$ is a common characteristic polynomial of all its m-decimated sequences. This paper demonstrate how the subjects such as the minimal polynomial, the linear span, the period and the correlation values of an $(f(x), m)$-interleaved sequence are related to its m-decimated sequences when $f(x)$ is irreducible, and makes a correction to an error made in [1] in studying the same problem. Moreover, this paper shows how to choose the m-decimated sequences to construct some sequences with the optimal auto and cross correlation values among the $(f(x), m)$-interleaved sequences when $f(x)$ is primitive and m is less than the period of $f(x)$.

1 Introduction

A sequence $u = \{u(i)\}_{i=0}^{\infty}$ over a finite field F_q is called an $(f(x), m)$-interleaved sequence [1] if $f(x)$ is a common characteristic polynomial [2] of its m-decimated sequences $u_j = \{u(im + j)\}_{i=0}^{\infty}, 0 \leq j < m$, which will be called its component sequences, where $f(x)$ is a polynomial over F_q and m is an integer greater than 1. When $f(x)$ is irreducible with degree n, if one fixes a root α of $f(x)$, it is clear that there exists a unique m-tuple $\underline{\gamma} = (\gamma_0, \gamma_1, \cdots, \gamma_{m-1})$ over F_{q^n} such that $u(im + j) = Tr_q^{q^n}(\gamma_j \alpha^i), \forall i, j$. (Here $Tr_q^{q^n}(x)$ is the trace function [2] from F_{q^n} to F_q.) Hence the m component sequences of u can be identified with the tuple $\underline{\gamma}$, and the sequence u can be denoted by $u_{\underline{\gamma}}$.

It is pointed out: [1] that many sequences can be considered as $(f(x), m)$-interleaved sequences with $f(x)$ being primitive and $m \geq per(f(x))$, such as multiplexed sequences [3], clock-controlled sequences [4], GMW-sequences [5], cascaded GMW-sequences [6], No sequences [7], and geometric sequences [8],[9], where $per(f(x))$ is the period [2] of $f(x)$. An interesting problem is how to construct some nice $(f(x), m)$-interleaved sequences when $f(x)$ is primitive and

* The work is supported by Chinese Natural Science Fundation.

m is less than $per(f(x))$. A more elementary problem, which is related to the former one, is how to determine subjects such as the minimal polynomial, the linear span, the period and the correlation values of an $(f(x), m)$-interleaved sequence $u_{\underline{\gamma}} = \{u(i)\}_{i=0}^{\infty}$ depend on its component sequences, *i.e.*, the m-tuple $\underline{\gamma}$. The latter problem is studied in [1] but not solved completely and an error is made in Theorem 1 (i) [1] which concerns on the relation between the period of the sequence $u_{\underline{\gamma}}$ and the tuple $\underline{\gamma}$. This paper begins by studying the latter problem, then makes a correction to the error made in Theorem 1 (i) [1], and finally shows how to choose the tuples $\underline{\gamma}$'s to construct some sequences with optimal auto and cross correlation values among all the $(f(x), m)$-interleaved sequences when $f(x)$ is primitive and m is less than $per(f(x))$.

2 Interleaved Sequences $u_{\underline{\gamma}}$ and Tuples $\underline{\gamma}$

In the sequel, we fix the field F_q, the integer $m(>1)$ and the polynomial $f(x)$, and assume $f(x)$ is of degree n and irreducible over F_q. We fix a root of $f(x)$ in F_{q^n} and denote it by α. We let p be the characteristic of F_q.

In this section, we study how the behavior of an $(f(x), m)$-interleaved sequence $u_{\underline{\gamma}}$ is related to the tuple $\underline{\gamma}$. Here by the (periodic) correlation function between two sequences $u_{\underline{\gamma}_1}$ and $u_{\underline{\gamma}_2}$ ($\underline{\gamma}_i \in F_{q^n}^m, i = 1, 2$) we mean

$$c_{\underline{\gamma}_1, \underline{\gamma}_2}(\tau) = \sum_{0 \le k < m(q^n - 1)} \chi(u_{\underline{\gamma}_1}(k) - u_{\underline{\gamma}_2}(k + \tau)), \ \chi(x) = e^{i\frac{2\pi Tr_p^q(x)}{p}}.$$

When $\underline{\gamma}_1 = \underline{\gamma}_2 = \underline{\gamma}$, we write simply $c_{\underline{\gamma}_1, \underline{\gamma}_2}(\tau) = c_{\underline{\gamma}}(\tau)$, which is considered in [1]. All the other concepts are defined in [2],[10] or [11]. In this paper, we identify the m-tuple space $F_{q^n}^m$ to the F_{q^n}-module $F_{q^n}[x]/(x^m - \alpha)$ by the following map:

$$\underline{\gamma} = (\gamma_0, \gamma_1, \cdots, \gamma_{m-1}) \to \underline{\gamma}(x) = \sum_{0 \le i < m} \gamma_i x^{m-i-1}. \tag{1}$$

The following lemma is basic in studying $u_{\underline{\gamma}}$.

Lemma 1. *Given $\underline{\gamma} = (\gamma_0, \gamma_1, \cdots, \gamma_{m-1}) \in F_{q^n}^m$, correspondingly define a sequence over F_{q^n} as follows:*

$$\varphi_{\underline{\gamma}} = \{\gamma_t\}_{t=0}^{\infty}, \ \gamma_{im+j} = \gamma_j \alpha^i, \ \ 0 \le j < m, 0 \le i \tag{2}$$

Let $\varphi_{\underline{\gamma}}(x) = \sum_{k=0}^{\infty} \gamma_t x^{-1-t}$, which is the generating function of $\varphi_{\underline{\gamma}}$. Similarly, let $u_{\underline{\gamma}}(x)$ be the generating function of $u_{\underline{\gamma}}$. Then

$$u_{\underline{\gamma}}(x) = \sum_{k=0}^{n-1} \varphi_{\underline{\gamma}}(x)^{\sigma^k}, \ \ \varphi_{\underline{\gamma}}(x) = \frac{\gamma(x)}{x^m - \alpha}, \ \ and \ \ \varphi_{\underline{\gamma}}^{\sigma^k}(x) = \frac{\gamma(x)^{\sigma^k}}{(x^m - \alpha)^{\sigma^k}},$$

where σ^k means the map which raises the coefficients of the power series or the polynomials to q^k-th power.

Proof The first equation is a simple consequence of the definition of $u_{\underline{\gamma}}$ and $\varphi_{\underline{\gamma}}$:

$$
\begin{aligned}
u_{\underline{\gamma}}(x) &= \sum_{0\le j<m} \sum_{i\ge 0} Tr_q^{q^n}(\gamma_j \alpha^i) x^{-1-j-im} \\
&= \sum_{0\le k<n} \sum_{0\le j<m} \sum_{i\ge 0} \gamma_j \alpha^{iq^k} x^{-1-j-im} = \sum_{0\le k<n} \varphi_{\underline{\gamma}}(x)^{\sigma^k}.
\end{aligned}
$$

The third one is a consequence of the second one as follows:

$$
\begin{aligned}
\varphi_{\underline{\gamma}}(x) &= \sum_{j=0}^{m-1} \sum_{i=0}^{\infty} \gamma_j \alpha^i x^{-1-j-im} \\
&= \sum_{j=0}^{m-1} \gamma_j x^{-1-j} \frac{1}{1-\alpha x^{-m}} = \frac{\underline{\gamma}(x)}{x^m - \alpha}.
\end{aligned}
$$

□

The following lemma is related to the characteristic polynomial $x^m - \alpha$ of the sequence $\varphi_{\underline{\gamma}}$. Its proof is omitted, as it is a simple fact in algebra.

Lemma 2. *Let*

$$T = per(f), \;\; m = tD, \;\; and \;\; D = p^a D_0,$$

where t is the integer such that each of the prime factors of t is a factor of T, $\gcd(D,T) = 1$, and $\gcd(D_0, p) = 1$. Then the polynomial $x^m - \alpha$ has the following factorization:

$$
\begin{aligned}
x^m - \alpha &= a(x)^{p^a}, \\
a(x) &= \prod_{1\le d\le D_0,\; d|D_0} a_d(x), \;\; and \\
a_d(x) &= \prod_{0\le i<D_0} \prod_{0\le j<t, 0<i<d, (i,d)=1} (x - \beta^{1+Tj}\theta^{\frac{D_0 i}{d}}),
\end{aligned}
$$

where $a(x)$ has no multiple roots, β is an element of order tT and $\beta^m = \alpha$, and θ is an element of order D_0.

In particular, $per(x^m - \alpha) = mT$, and the period of any non-constant factor of $x^m - \alpha$ is of the form $tTd, d|D$. □

Theorem 1. *1. $L^\tau u_{\underline{\gamma}} = u_{x^\tau \underline{\gamma}}$, where L is the left shift operator acting on the sequences, $x^\tau \underline{\gamma}$ is the tuple identifying to the polynomial $x^\tau \underline{\gamma}(x) \pmod{x^m - \alpha}$ of degree less than m.*

2. The minimal polynomial of $u_{\underline{\gamma}}$ is $\prod_{i=0}^{n-1} h(x)^{\sigma^i}$, where $h(x)$ is the minimal polynomial of $\varphi_{\underline{\gamma}}$.

3. $LS(u_{\underline{\gamma}}) = nLS(\varphi_{\underline{\gamma}}) \le mn$.

4. Using the notation from Lemma 2, we have

$$per(u_{\underline{\gamma}}) = per(\varphi_{\underline{\gamma}})$$

and

$$per(u_{\underline{\gamma}}) = dtT \ \textit{if} \ \underline{\gamma} \neq 0,$$

where

$$\begin{aligned} & d = LCM(per(\underline{\gamma}_0), \cdots, per(\underline{\gamma}_{t-1})), \\ & \underline{\gamma}_i = (\gamma_i, \alpha^{-e}\gamma_{i+t}, \cdots, \alpha^{-(D-1)e}\gamma_{i+(D-1)t}) \in F_{q^n}^m, 0 \leq i < t, \ \textit{and} \\ & eD \equiv 1 \pmod T. \end{aligned}$$

5. When $f(x)$ is primitive, i.e., $per(f(x)) = q^n - 1$, we have

$$c_{\underline{\gamma}_1, \underline{\gamma}_2}(\tau) = -m + (m - w_H(\underline{\gamma}_1 - x^\tau \underline{\gamma}_2))q^n$$

for any $\tau \geq 0$, where $\underline{\gamma}_1 - x^\tau \underline{\gamma}_2$ is the tuple identifying to the polynomial $\underline{\gamma}_1(x) - x^\tau \underline{\gamma}_2(x) \pmod{x^m - \alpha}$, and $w_H(\underline{\gamma})$ is the Hamming weight of $\underline{\gamma}$.

Proof From Lemma 1, we have

$$\begin{aligned} L^\tau u_{\underline{\gamma}}(x) &= \sum_{0 \leq k < n} [(L^\tau \varphi_{\underline{\gamma}})(x)]^{\sigma^k} \\ &= \sum_{0 \leq k < n} [\frac{x^\tau \underline{\gamma}(x) \pmod{x^m - \alpha}}{x^m - \alpha}]^{\sigma^k} (\text{ see [12] }) \\ &= \sum_{0 \leq k < n} [\varphi_{x^\tau \underline{\gamma}}(x)]^{\sigma^k} = u_{x^\tau \underline{\gamma}}(x). \end{aligned}$$

which proves the item 1.

Noticing that all the polynomials $(x^m - \alpha)^{\sigma^k}$ $(0 \leq k < n)$ have the same period and are coprime to each other, we get the item 2, 3, and $per(u_{\underline{\gamma}}) = per(\varphi_{\underline{\gamma}})$ follows Lemma 1 easily. It is clear from Lemma 2 that if $\underline{\gamma} \neq 0$, then $per(\varphi_{\underline{\gamma}})$ is of the form $tTd, d|D$. In order to complete the proof of item 4, it is sufficient to prove that

$$per(\varphi_{\underline{\gamma}}) \mid dtT \longleftrightarrow per(\underline{\gamma}_i) \mid d \ \forall 0 \leq i < t. \tag{3}$$

Let $A_\epsilon = \{\gamma_{\epsilon + itT}\}_{i=0}^\infty, 0 \leq \epsilon < tT$, be the tT-decimated sequences of $\varphi_{\underline{\gamma}}$, then

$$per(A_\epsilon)|D, \tag{4}$$

since $per(\varphi_{\underline{\gamma}})|tTD$. It is clear that

$$per(\varphi_{\underline{\gamma}}) \mid dtT \longleftrightarrow per(A_\epsilon) \mid d \ \forall \ 0 \leq \epsilon < tT. \tag{5}$$

Assume $eD = 1 - bT$, and let $B_\epsilon = \{B_\epsilon(i) = \gamma_{\epsilon+ibtT}\}_{i=0}^{\infty}$ be the b-decimated sequence of A_ϵ. Then

$$per(A_\epsilon) = per(B_\epsilon), 0 \le \epsilon < tT, \tag{6}$$

since $\gcd(b, per(A_\epsilon)) = 1$. We notice that

$$B_\epsilon(i) = \gamma_{\epsilon+it(1-eD)} = \gamma_{\epsilon+it-iem} = \alpha^{-ie}\gamma_{\epsilon+it}$$

from (2), so we have

$$B_\delta = (\underline{\gamma}_\delta, \underline{\gamma}_\delta, \cdots, \underline{\gamma}_\delta, \cdots), 0 \le \delta < t.$$

Hence

$$per(B_\delta) = per(\underline{\gamma}_\delta), 0 \le \delta < t. \tag{7}$$

Write $\epsilon = \delta + t\lambda$, $0 \le \delta < t$; then

$$\alpha^{-e\lambda}B_\epsilon(i) = \alpha^{-e(i+\lambda)}\gamma_{\delta+t(i+\lambda} = B_\delta(i+\lambda),$$

so we have

$$per(B_\epsilon) = per(B_\delta), \ if \ \epsilon \equiv \delta \pmod t. \tag{8}$$

The equations (5),(6),(7) and (8) lead to the desired condition (3).

Let $\underline{\beta} = \underline{\gamma}_1 - x^\tau \underline{\gamma}_2 = (\beta_0, \beta_1, \cdots, \beta_{m-1})$. It is clear that

$$u_{\underline{\gamma}_1} - L^\tau u_{\underline{\gamma}_2} = u_{\underline{\gamma}_1 - x^\tau \underline{\gamma}_2}$$

from Lemma 1, so we have

$$\begin{aligned} c_{\underline{\gamma}_1,\underline{\gamma}_2}(\tau) = c_{\underline{\gamma}_1 - x^\tau\underline{\gamma}_2}(0) &= \sum_{0\le j<m} \sum_{0\le i<q^n-1} \chi(Tr_q^{q^n}(\beta_j\alpha^i)) \\ &= -\sum_{0\le j<m, \beta_j\ne 0} 1 + \sum_{0\le j<m,\beta_j=0} (q^n-1) \\ &= -w_H(\underline{\beta}) + (m - w_H(\underline{\beta}))(q^n-1) \\ &= -m + (m - w_H(\underline{\gamma}_1 - x^\tau\underline{\gamma}_2))q^n, \end{aligned}$$

which proves item 5.

□

We get some information about the distribution of the linear spans and the periods of the $(f(x), m)$-interleaved sequences from Theorem 1 easily, as is shown in the following corollary.

Corollary 1.

1. *Let N be the total number of $(f(x), m)$-interleaved sequences whose linear spans equal mn. Then*

$$N = \prod\nolimits_{d|D_0} (q^{np^a n_d} - q^{n(p^a-1)n_d})^{\frac{t\Phi(d)}{n_d}} \ge (q^n-1)^m.$$

Here $\Phi(\cdot)$ is Euler function, and n_d is the smallest positive integer such that $q^{nn_d} \equiv 1 \pmod{tTd}$.

2. *Let M_r be the total number of non-zero $(f(x), m)$-interleaved sequences whose periods equal r. Then $M_r \neq 0$ if and only if $r = tTd, d\ |D$. Moreover, $M_{tT} = q^{nt} - 1$, and*

$$M_{tTd} = q^{ntd} - \sum_{1 \le i \le l} q^{\frac{dnt}{p_i}} + \sum_{1 \le i < j \le l} q^{\frac{dnt}{p_i p_j}} + \cdots + (-1)^l q^{\frac{dnt}{p_1 \cdots p_l}}$$

when $1 < d = p_1^{e_1} \cdots p_l^{e_l}$, where p_i are distint primes, and $e_i > 0\ \forall i$.

Proof

1. It is clear that different $\varphi_{\underline{\gamma}}$ correspond to different $u_{\underline{\gamma}}$, so N_{mn} is exactly the number of all possible sequences $\varphi_{\underline{\gamma}}$ with $LS(\varphi_{\underline{\gamma}}) = m$ from Theorem 1. With notation as in Lemma 2, it is clear that the polynomial $a_d(x)$ has a factorization over F_{q^n} of the form

$$a_d(x) = \prod_{1 \le j \le \frac{t\phi(d)}{n_d}} f_{d,j}(x),$$

where each $f_{d,j}(x)$ is irreducible of degree n_d over F_{q^n}, and $f_{d,j}(x) \neq f_{d,j'}(x)$ if $j \neq j'$. Therefore, the sequence $\varphi_{\underline{\gamma}}(x)$ has a decomposition of the form:

$$\varphi_{\underline{\gamma}}(x) = \frac{\underline{\gamma}(x)}{x^m - \alpha} = \sum_{d|D_0} \sum_{1 \le j \le \frac{t\phi(d)}{n_d}} \frac{h_{d,j}(x)}{f_{d,j}(x)^{p^a}}, \tag{9}$$

$$\text{where} \qquad h_{d,j}(x) \in F_{q^n}[x], \text{ and } deg(h_{d,j}(x)) < p^a n_d \tag{10}$$

from Lemma 1 and Lemma 2. We see that $LS(\varphi_{\underline{\gamma}}(x)) = m$ if and only if $f_{d,j}(x)$ is not a factor of $h_{d,j}(x)$ for all $d|D_0, 1 \le j \le \frac{t\phi(d)}{n_d}$ from (9) and (10). Hence we get

$$\begin{aligned} N &= \prod_{d|D_0} (q^{nn_d p^a} - q^{nn_d p^a - nn_d})^{\frac{t\Phi(d)}{n_d}} \\ &\ge \prod_{d|D_0} [(q^{nn_d} - 1)^{p^a - 1}(q^{nn_d} - 1)]^{\frac{t\Phi(d)}{n_d}} \\ &= \prod_{d|D_0} (q^{nn_d} - 1)^{\frac{t\Phi(d) \cdot p^a}{n_d}} \ge (q^n - 1)^{tp^a \sum_{d|D_0} \Phi(d)} = (q^n - 1)^m. \end{aligned}$$

2. Let $\mathcal{M}_d$ be the set of all $(f(x), m)$-interleaved sequences of periods dividing tTd. From Theorem 1, we see $u_{\underline{\gamma}} \in \mathcal{M}_d$ if and only if that $per(\underline{\gamma}_i)|\ d, \forall 0 \le i < t$, so

$$|\mathcal{M}_d| = q^{ntd}, \text{and } |\mathcal{M}_d| - 1 = \sum_{r|d} M_r.$$

Hence $M_{tT} = q^{nt} - 1$. For $d > 1$, using the Möbius inversion formula [13] and the fact that $\sum_{r|d} \mu(r) = 0$ for $d > 1$, we get

$$M_{tTd} = \sum_{r|d} (|\mathcal{M}_{\frac{d}{r}}| - 1)\mu(r) = \sum_{r|d} |\mathcal{M}_{\frac{d}{r}}|\mu(r),$$

which leads to the desired result.

Remark 1. From Theorem 1 we see that Theorem 1 (i) in [1], which claims that " If $w_H(\underline{\gamma}) < m$, then $per(u_{\underline{\gamma}}) = mT$, $T = per(f(x))$", is not true in general. In fact, Theorem 1 (i) in [1] should be corrected to be the following statement, using the same notation as in Lemma 2.

Statement: Assume $w_H(\underline{\gamma}) < m$. Then $per(u_{\underline{\gamma}}) = mT$ if and only if "$m = t$" or "$m = D$ is a prime."

Proof It is easy to check the "if" part. If the "only if" part is not true, then one has either "$m = tD$ with both $t > 1$ and $D > 1$" or "$m = D$ is not a prime". In the first case, take $\underline{\gamma}(x) = \sum_{j=0}^{D-1} \alpha^{ej} x^{m-1-tj}$, whence $w_H(\underline{\gamma}) = D < m$. But, with the notation as in Theorem 1, we have $\underline{\gamma}_0 = (1, 1, \cdots, 1)$, $\underline{\gamma}_j = \underline{0}\ \forall 0 < j < t$, and $per(\underline{\gamma}_j) = 1\ \forall 0 \leq j < t$. Hence $per(u_{\underline{\gamma}}) = tT < mT$ from Theorem 1, a contradiction. In the second case, we may assume $m = D = bc, b > 1, c > 1$. Take $\underline{\gamma}(x) = \sum_{0 \leq j < c} \alpha^{ebj} x^{m-1-bj}$; then $w_H(\underline{\gamma}) < m$. But $\underline{\gamma}_0 = (1, 1, \cdots, 1)$, $per(\underline{\gamma}_j) = 1\ \forall 0 \leq j < t = 1$, and hence $per(u_{\underline{\gamma}}) = tT < mT$ from Theorem 1, a contradiction again.

□

3 Sequences $u_{\underline{\gamma}}$ with Optimal Correlation

In this section, we assume $f(x)$ is primitive, *i.e.*, $per(f(x)) = q^n - 1$. We will show that, among all the $(f(x), m)$-interleaved sequences, the sequences with the optimal correlation must have the maximal period. Moreover, we will give a way to construct the sequences with the optimal correlation when $2m$ is less than the period of $f(x)$.
For $\underline{\gamma} \in F_{q^n}^m$, define

$$Max(c_{\underline{\gamma}}) = max\{\ |c_{\underline{\gamma}}(\tau)|\ |\ 0 < \tau < m(q^n - 1)\ \}.$$

For $\underline{\gamma}_i \in F_{q^n}^m (i = 1, 2)$, $\underline{\gamma}_1 \neq \underline{\gamma}_2$, define

$$Max(c_{\underline{\gamma}_1, \underline{\gamma}_2}) = max\{\ |c_{\underline{\gamma}_1, \underline{\gamma}_2}(\tau)|\ |\ 0 \leq \tau < m(q^n - 1)\ \}.$$

Lemma 3. *1. (a)*

$$\sum_{0<\tau<m(q^n-1)} [m - w_H(\underline{\gamma} - x^\tau \underline{\gamma})] = w_H(\underline{\gamma})^2 + (m - w_H(\underline{\gamma}))^2 (q^n - 1) - m.$$

(b) *The conditions "*$m - w_H(\underline{\gamma} - x^{rm}\underline{\gamma}) \le 1\ \forall\ 0 < r < q^n - 1$*" hold if and only if* $w_H(\underline{\gamma}) \ge m - 1$.

(c) *Assume* $w_H(\underline{\gamma}) \ge m - 1$. *For any given* s, $0 < s < m$, *the conditions "*$m - w_H(\underline{\gamma} - x^{rm+s}\underline{\gamma}) \le 1\ \forall 0 \le r < q^n - 1$*" hold if and only if*

$$\gamma_i \gamma_{i+s}^{-1} \ne \gamma_j \gamma_{j+s}^{-1}\ \forall 0 \le i < j < m,$$

whenever $\gamma_i \gamma_{i+s} \gamma_j \gamma_{j+s} \ne 0$.

2. *Assume* $\underline{\gamma}_1 \ne \underline{\gamma}_2$ *and* $w_2 \le w_1$, *where* $w_1 = w_H(\underline{\gamma}_1), w_2 = w_H(\underline{\gamma}_2)$. *We have*

(a)

$$\sum_{0 \le \tau < m(q^n-1)} [m - w_H(\underline{\gamma}_1 - x^\tau \underline{\gamma}_2)] = w_1 w_2 + (m - w_1)(m - w_2)(q^n - 1).$$

(b) *The conditions "*$m - w_H(\underline{\gamma}_1 - x^{rm+s}\underline{\gamma}_2) \le 1\ \forall\ 0 \le r < q^n - 1,\ 0 \le s < m$*" hold if and only if* $w_1 = m$ *and*

$$\gamma_{1,i}\gamma_{2,i+s}^{-1} \ne \gamma_{1,j}\gamma_{2,j+s}^{-1}\ \forall 0 \le i < j < m,\ 0 \le s < m$$

whenever $\gamma_{2,i+s}\gamma_{2,j+s} \ne 0$, *where* $\underline{\gamma}_i = (\gamma_{i,0}, \gamma_{i,1}, \cdots, \gamma_{i,m-1}), i = 1, 2$.

Proof All the parts are easy to check, and hence we omit their proof except for the part that the conditions "$m - w_H(\underline{\gamma}_1 - x^{rm+s}\underline{\gamma}_2) \le 1\ \forall\ 0 \le r < q^n - 1,\ 0 \le s < m$" imply "$w_1 = m$". In fact, if $w_1 \ne m$, then we have $w_2 \le w_1 \le m - 1$. There exist s_1 and s_2, such that

$$x^{s_1}\underline{\gamma}_1 = (0, \rho_1, \rho_2, \cdots, \rho_{m-1}), \rho_1 \ne 0$$

and

$$x^{s_2}\underline{\gamma}_2 = (0, \theta_1, \theta_2, \cdots, \theta_{m-1}), \theta_1 \ne 0.$$

Take r such that $\rho_1 - \alpha^r \theta_1 = 0$, and take $\tau = rm + s_2 - s_1$. Then

$$w_H(\underline{\gamma}_1 - x^\tau \underline{\gamma}_2) = w_H(x^{s_1}\underline{\gamma}_1 - \alpha^r x^{s_2}\underline{\gamma}_2) \le m - 2,$$

a contradiction. □

Theorem 2. *Assume* $q^n \ge 2m$. *Then*

1. (a) $Max(c_{\underline{\gamma}}) \ge -m + q^n$.

(b) $Max(c_{\underline{\gamma}}) = -m + q^n$ *if and only if* $w_H(\underline{\gamma}) \ge m - 1$ *and*

$$\gamma_i \gamma_{i+s}^{-1} \ne \gamma_j \gamma_{j+s}^{-1}\ \forall 0 \le i < j < m,\ 0 < s < m, \tag{11}$$

whenever $\gamma_i \gamma_{i+s} \gamma_j \gamma_{j+s} \ne 0$.

(c) *If* $Max(c_{\underline{\gamma}}) = -m + q^n$, *then the correlation function* $c_{\underline{\gamma}}$ *takes on the following two values for* $0 < \tau < m(q^n - 1)$:

$$\begin{array}{ll} -m + q^n & occurs\ m^2 - m\ times, and \\ -m & occurs\ mq^n - m^2 - 1\ times \end{array}$$

when $w_H(\underline{\gamma}) = m$*; and*

$$\begin{array}{ll} -m+q^n & occurs\ q^n-2+(m-1)(m-2)\ times, and \\ -m & occurs\ (m-1)(q^n-1)-(m-1)(m-2)\ times \end{array}$$

when $w_H(\underline{\gamma}) = m-1$.

2. *Assume* $\underline{\gamma}_1 \neq \underline{\gamma}_2$, *and assume* $w_H(\underline{\gamma}_1) \geq w_H(\underline{\gamma}_2)$. *Then*
   (a) $Max(c_{\underline{\gamma}_1,\underline{\gamma}_2}) \geq -m+q^n$
   (b) $Max(c_{\underline{\gamma}_1,\underline{\gamma}_2}) = -m+q^n$ *if and only if* $w_H(\underline{\gamma}_1) = m$, *and*

$$\gamma_{1,i}\gamma_{2,i+s}^{-1} \neq \gamma_{1,j}\gamma_{2,j+s}^{-1},\ \forall 0 \leq i < j < m,\ 0 \leq s < m, \tag{12}$$

   whenever $\gamma_{2,i+s}\gamma_{2,j+s} \neq 0$, *where* $\underline{\gamma}_i = (\gamma_{i,0}, \gamma_{i,1}, \cdots, \gamma_{i,m-1}), i = 1,2$.
   (c) *If* $Max(c_{\underline{\gamma}_1,\underline{\gamma}_2}) = -m+q^n$, *then the cross correlation function* $c_{\underline{\gamma}_1,\underline{\gamma}_2}$ *takes on the following two values:*

$$\begin{array}{ll} -m+q^n & occurs\ mw_H(\underline{\gamma}_2)\ times, and \\ -m & occurs\ m(q^n-1)-mw_H(\underline{\gamma}_2)\ times. \end{array}$$

3. (a) *If* $Max(c_{\underline{\gamma}}) = -m+q^n$, *then* $per(u_{\underline{\gamma}}) = m(q^n-1)$.
   (b) *Assume* $\underline{\gamma}_1 \neq \underline{\gamma}_2$. *If* $Max(c_{\underline{\gamma}_1,\underline{\gamma}_2}) = -m+q^n$, *then* $u_{\underline{\gamma}_1}$ *is not cyclically equivalent to* $u_{\underline{\gamma}_2}$.

Proof Both of items 1(a) and 1(c) are the consequences of Theorem 1(4) and Lemma 3, 1(a). The item 1(b) is a consequence of Theorem 1(4), and Lemma 3, 1(b) and 1(c).

Both of items 2(a) and 2(c) are the consequences of Theorem 1(4) and Lemma 3, 2(a). Item 2(b) is a consequence of Theorem 1(4) and Lemma 3, 2(b).

If item 3(a) is not true, then $per(u_{\underline{\gamma}}) = \tau < m(q^n-1)$ for some τ, hence $c_{\underline{\gamma}}(\tau) = m(q^n-1) > -m+q^n = Max(c_{\underline{\gamma}})$, a contradiction. If item 3(b) is not true, then $u_{\underline{\gamma}_2} = L^\tau u_{\underline{\gamma}_1}$ for some τ. Thus

$$c_{\underline{\gamma}_1,\underline{\gamma}_2}(\tau) = m(q^n-1) > -m+q^n = Max(c_{\underline{\gamma}_1,\underline{\gamma}_2}),$$

a contradiction.

□

Theorem 3. *Suppose we construct as many integer tuples as possible, say* N *as follows:*

$$\underline{d}_j = (d_{j,0}, d_{j,1}, \cdots, d_{j,m-1}), 1 \leq j \leq N,$$

such that they satisfy the following conditions:

$$d_{j,0} = 0,\ 1 \leq j \leq N,$$
$$0 < d_{j,i} < d_{j,i'} < d_{j',i} < d_{j',i'}\ \forall 0 \leq i < i' < m, 1 \leq j < j' \leq N,\ and$$
$$\sum_{0 \leq i < m} d_{N,i} < (q^n-1)/2.$$

Correspondingly, let $\underline{\gamma}_j \in F_{q^n}^m$ *be determined by* $\underline{d}_j$ *as follows:*

$$\underline{\gamma}_j = (\gamma_{j,0}, \gamma_{j,1}, \cdots, \gamma_{j,m-1}), \text{ and}$$
$$\gamma_{j,i} = \alpha^{a_{j,i}}, a_{j,i} = \sum_{0 \le k \le i} d_{j,k}.$$

Then

$$Max(c_{\underline{\gamma}_i}) = Max(c_{\underline{\gamma}_j, \underline{\gamma}_k}) = -m + q^n \ \forall 1 \le i \le N, \ 1 \le j \ne k \le N, \text{ and}$$

they attain the minimum among all the $(f(x), m)$*-interleaved sequences.*

Proof Write $a_{j,k+s} = a_{j,k+s-m} + 1$ if $m \le k + s < m + s$. For any $1 \le j \le N$, it is easy to check $(T = q^n - 1)$ that

$$-T/2 < a_{j,k'+s} - a_{j,k'} < a_{j,k+s} - a_{j,k} < a_{j,i+s} - a_{j,i} < a_{j,i'+s} - a_{j,i'} < T/2, \quad (13)$$

if

$$s \le i + s < i' + s < m \le k + s < k' + s < m + s, \ 0 \le s < m.$$

The conditions (13) are equivalent to the conditions (11), hence $Max(c_{\underline{\gamma}_j}) = q^n - m$ from Theorem 2. For any $1 \le j < k \le N$, it is easy to check that

$$-(q^n - 1)/2 < a_{k,i} - a_{j,i+s} < a_{k,l} - a_{j,l+s} < (q^n - 1)/2, \quad (14)$$

if

$$0 \le i < l < m, \ 0 \le s < m.$$

The conditions (14) are equivalent to the conditions (12). Hence $Max(c_{\underline{\gamma}_j, \underline{\gamma}_k}) = q^n - m$ from Theorem 2. □

References

1. G.Gong, "Theory and application of q-ary interleaved sequences," *IEEE Trans. Inform. Theory,* Vol. 41, No.2, pp. 400-411,March,1995.
2. Rudolf Lidl, Harald Niederreiter, "Finite Fields," Addison-Wesley Publishing Company.
3. S.M.Jennings, "Multiplexed sequences: some properties of minimum polynomial," *in proc. EUROCRYPT'82,* Lecture Notes in Computer Science, vol. 149. New York: Springer-Verlag, 1983.
4. D.Gollman and W.G.Chambers, "Clock-controlled shift register: A review," *IEEE J.Selected Areas Commun.,* vol.7, no.4, pp.525-533,May 1989.
5. R.A.Scholz and L.R.Welch, "GMW sequences," *IEEE Trans. Inform. Theory,* vol. IT-30, no.3, pp. 548-553, May. 1984.
6. A.H. and M.Goresky, "Cascaded GMW sequences," *IEEE Trans. Inform. Theory,* Vol. 39, pp. 177-183, Jan. 1993.
7. J.S.No and P.V. Kumar, "A new family of binary pseudorandom from sequeces having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory,* Vol. 35, No.2, pp. 371-379, Mar. 1989.

8. A.H.Chan and R.A.Games, "On the linear span of binary sequences from finite geometries, q odd," *in Proc. Crypto'86,* pp.405-417.
9. A.H.Chan and R.A.Games, " On the linear span of binary sequences obtained from Q-ary M-sequences, Q odd," *IEEE Trans. Inform. Theory.* Vol. 36, no.3, pp. 548-522, May 1990.
10. Wan Z.X. "Algebra and coding theory," (in Chinese) Beijing, science press, 1979.
11. Ding CunSheng, Xiao Guozhen, "Stream cipher and application," (in Chinese), 1994.
12. Z.D.Dai, X.N.Feng, M.L.Liu and Z.X.Wan, "Nonlinear Feedforwad Sequences of m-Sequences I," *Discrete Mathematics* 123 (1993), North Holland. pp.17-34.
13. LuoGeng Hua, "Introduction of Number Theory," (In chinese), Science Press,1975.