Note

Correlation functions of a family of generalized geometric sequences

Wei Sun, Yi Xian Yang*

Department of Information Engineering, Beijing University of Posts and Telecommunications,
P.O. Box 145, Beijing, 100088, PR China

Received 28 May 1996; revised 11 February 1997

Abstract

Explicit formulas for cross-correlation functions of the so-called linearly related generalized geometric sequences are derived, thus an open problem proposed by Klapper et al. (1993) is partially solved. © 1997 Elsevier Science B.V.

1. Introduction

Geometric sequences, including m-sequences, GMW sequences, and Bent sequences, are very useful binary pseudorandom sequences which have been widely used in modern communication systems and cryptography. In 1993, Klapper et al. [1] calculated the cross-correlation functions of geometric sequences obtained from linearly or quadratically related q-ary m-sequences. In the same paper, they defined the generalized geometric sequence (GGS) and proposed an open problem of calculating the correlations of these GGSs. This open problem will be partially solved in this paper by deriving explicit formulas for cross-correlation functions of linearly related GGSs, and the distribution of their cross-correlation function values is also given.

Definition 1. Let \( q \) be a power of a prime \( p \), \( n \) a positive integer, and let \( \alpha \) and \( \beta \) be primitive elements of \( \text{GF}(q^n) \) with \( \beta = \alpha^k \) and \( \gcd(k,q^n - 1) = 1 \). For a nonlinear function \( f \) from \( \text{GF}(q) \) to \( \text{GF}(2) \), the sequence \( S_f^{(A,B)} = \{S_f^{(A,B)}(i) | 0 \leq i \leq q^n - 2 \} \) is called a generalized geometric sequence (GGS), where

\[
S_f^{(A,B)}(i) = f(\text{Tr}(A\alpha^i + B\beta^i)),
\]

* Corresponding author. Email: yxyang@bupt.edu.cn.
A, B \in \text{GF}(q^n), \ Tr(\cdot) \ the \ trace \ function \ from \ \text{GF}(q^n) \ to \ \text{GF}(q), \ i.e., \ Tr(x) = \sum_{i=0}^{n-1} x^i. \ If \ \beta = x^q, \ i.e., \ k = p^c, \ the \ sequence \ S^{(A,B)}_f \ is \ called \ a \ linearly \ related \ GGS.

The period of a GGS is clearly a divisor of \( q^n - 1 \).

**Definition 2.** For two given binary \((0, 1)\) sequences \( S = (S(0), S(1), \ldots, S(L-1)) \) and \( T = (T(0), T(1), \ldots, T(L-1)) \) of length \( L \), the (periodic) cross-correlation function \( C_{ST}(\tau) \) of \( S \) and \( T \) is defined by

\[
C_{ST}(\tau) = \sum_{i=0}^{L-1} (-1)^{S(i \oplus_L \tau) + T(i)}, \quad \tau = 0, \ldots, L - 1.
\]

where \( i \oplus_L \tau \) stands for \((i + \tau) \mod L\).

2. Preliminaries

The finite field \( \text{GF}(q^n) \) is an \( n \)-dimensional vector space over \( \text{GF}(q) \). By [5] and the normal basis theorem (see [4, Theorem 2.35, p. 60]), there exists a primitive element \( \alpha \) of \( \text{GF}(q^n) \) such that \( N = \{ \alpha_0 = \alpha, \alpha_1 = \alpha^q, \ldots, \alpha_{n-1} = \alpha^{q^{n-1}} \} \) forms a normal basis of \( \text{GF}(q^n) \) over \( \text{GF}(q) \), i.e., every element \( x \in \text{GF}(q^n) \) can be represented as a linear combination \( x = \sum_{i=0}^{n-1} x_i \alpha_i \), where \( x_i \in \text{GF}(q) \). In the sequel, \( \alpha \) will always denote a primitive generator of the normal basis \( N \).

The following linear mapping \( \sigma \), from \( \text{GF}(q^n) \) to \( \text{GF}(q) \), plays an important role which is defined by

\[
\sigma \left( \sum_{i=0}^{n-1} x_i \alpha_i \right) = \sum_{i=0}^{n-1} x_i.
\]

By Eq. (3), we have

**Lemma 3.** If \( \gamma = \sum_{i=0}^{n-1} x_i \alpha_i \), \( \eta = \sum_{j=0}^{n-1} y_j \alpha_j \), \( x_i, y_j \in \text{GF}(q) \), then

\[
\sigma(\gamma \eta) = \sum_{i,j=0}^{n-1} x_i y_j \sigma(\alpha \alpha_j \alpha_i),
\]

\[
\text{Tr}(\gamma) = \sigma(\gamma) \text{Tr}(\alpha),
\]

where \( j \ominus_n i \) denotes \((j - i) \mod n\).

Let \( \gamma = \sum_{i=0}^{n-1} \gamma_i \alpha_i, \ 0 \leq \tau \leq q^n - 2 \), and \( x = \sum_{i=0}^{n-1} x_i \alpha_i \), then by Lemma 3,

\[
a_{\tau,i} = \sum_{j=0}^{n-1} \sigma(\alpha \alpha_j) \gamma_{\tau,j},
\]
\[ \sigma(x^i x) = \sum_{i=0}^{n-1} a_{i,j} x_j, \]  
\[ \text{Tr}(x^i x) = \text{Tr}(x) \sum_{i=0}^{n-1} a_{i,j} x_j. \]  
\[ \sigma(x^i x) = \sum_{i=0}^{n-1} a_{i,j} x_j, \]  
\[ \text{Tr}(x^i x) = \text{Tr}(x) \sum_{i=0}^{n-1} a_{i,j} x_j. \]  

From Eq. (8), we know that the map \( \varphi : \text{GF}(q^n)^* \rightarrow \text{GF}(q)^n \setminus \{(0, 0, \ldots, 0)\}, \) \( \varphi(x^i) = (a_{i,0}, a_{i,1}, \ldots, a_{i,n-1}) \) is one-to-one and \((a_{i,0}, a_{i,1}, \ldots, a_{i,n-1}) \neq (0, 0, \ldots, 0).

For \( u \in \text{GF}(q) \), define a hypersurface by
\[ Q(A, B, \tau, u) = \{ x \in \text{GF}(q^n) \mid A \sigma(x^i x) \text{Tr}(x) + B(\sigma(x^i x) \text{Tr}(x))^k = u \} \]
\[ = \{ x \in \text{GF}(q^n) \mid A \sum_{i=0}^{n-1} a_{i,j} x_j \text{Tr}(x) + B \left( \sum_{i=0}^{n-1} a_{i,j} x_j \text{Tr}(x) \right)^k = u \}. \]

Therefore,
\[ Q(A_1, B_1, 0, v) = \{ x \in \text{GF}(q^n) \mid A_1 \sum_{i=0}^{n-1} x_i \text{Tr}(x) + B_1 \left( \sum_{i=0}^{n-1} x_i \text{Tr}(x) \right)^k = v \}. \]

Let \( \{ X_{\xi} \mid 0 \leq \xi \leq l - 1 \} \) and \( \{ Y_{\eta} \mid 0 \leq \eta \leq t - 1 \} \) be sets of solutions of the following equations
\[ A_1 \text{Tr}(x)X + B_1 \text{Tr}(x)^k X^k = v, \]  
\[ \text{ATr}(x)Y + B \text{Tr}(x)^k Y^k = u, \]
respectively. Assuming
\[ \Omega_{\xi, \eta} = \{ (x_{0}, x_{1}, \ldots, x_{n-1}) \in \text{GF}(q)^n \mid \sum_{i=0}^{n-1} x_i = X_{\xi} \text{ and } \sum_{i=0}^{n-1} a_{i,j} x_i = Y_{\eta} \}, \]
\[ 0 \leq \xi \leq l - 1, \ 0 \leq \eta \leq t - 1, \text{ then the following lemma works.} \]

**Lemma 4.**
\[ Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v) = \bigcup_{\xi, \eta} \Omega_{\xi, \eta}. \]
\[ |Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v)| = \sum_{\eta} |\Omega_{\xi, \eta}|. \]

**Proof.** On one hand, if \((x_{0}, x_{1}, \ldots, x_{n-1}) \in Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v)\), then \( X' = \sum_{i=0}^{n-1} x_i \) and \( Y' = \sum_{i=0}^{n-1} a_{i,j} x_i \) are clearly solutions of Eqs. (10) and (11), respectively. Thus \((x_{0}, x_{1}, \ldots, x_{n-1}) \in \Omega_{\xi, \eta}\) for some \( 0 \leq \xi \leq l - 1 \) and \( 0 \leq \eta \leq t - 1 \).
On the other hand, if \((x_0, x_1, \ldots, x_{n-1}) \in \Omega_{\xi, \eta}\) for some \(0 \leq \xi \leq l - 1\) and \(0 \leq \eta \leq t - 1\), then \(\sum_{i=0}^{\xi+1} x_i = X_\xi\) and \(\sum_{i=0}^{\eta-1} a_{\tau,i}x_i = Y_\eta\), because \(X_\xi\) and \(Y_\eta\) are solutions of Eqs. (10) and (11), respectively, we have \((x_0, x_1, \ldots, x_{n-1}) \in Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v)\). Thus

\[
Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v) = \bigcup_{\xi, \eta} \Omega_{\xi, \eta}.
\]

By the definition of \(\Omega_{\xi, \eta}\), we have \(\Omega_{\xi, \eta} \cap \Omega_{\xi', \eta'} = \emptyset\) for \((\xi, \eta) \neq (\xi', \eta')\), then Eq. (13) follows. \(\square\)

For \(A, B, C \in \text{GF}(q)\), \(k = p^r\), let

\[
\#N(A, B, C) = |\{x \in \text{GF}(q) \mid Ax + Bx^k = C\}|.
\]

**Lemma 5.** If \(\#N(A, B, C) \neq 0\), then \(\#N(A, B, C) = \#N(A, B, 0)\).

Lemma 5 is trivial since the map \(x \rightarrow Ax + Bx^k\) is \(\text{GF}(q)\)-linear.

**Lemma 6.** Let \(a_{\tau,i}\)'s be defined by Eq. (6), then

- **Case 1:** \(a_{\tau,0} = a_{\tau,1} = \cdots = a_{\tau,n-1} \neq 0\)
  - **Case 1.1:** If \(A_1/A = B_1/Ba_{\tau,0}^{-1}\), then

\[
|Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v)| = \begin{cases} 0 & A_1u \neq a_{\tau,0}vA, \\ \#N(A \text{Tr}(\alpha), B \text{Tr}(\alpha)^k, v)q^{n-1} & A_1u = a_{\tau,0}vA. \end{cases}
\]

- **Case 1.2:** If \(A_1/A \neq B_1/Ba_{\tau,0}^{-1}\), then

\[
|Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v)| = \begin{cases} q^{n-1} & \frac{B_1u - va_{\tau,0}B}{a_{\tau,0}(AB_1 - A_1Ba_{\tau,0}^{-1})} = \frac{a_{\tau,0}Av - A_1u}{a_{\tau,0}(AB_1 - A_1Ba_{\tau,0}^{-1})}, \\ 0 & \text{otherwise}. \end{cases}
\]

- **Case 2:** Otherwise

\[
|Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v)| = \#N(A \text{Tr}(\alpha), B \text{Tr}(\alpha)^k, u)\#N(A_1 \text{Tr}(\alpha), B_1 \text{Tr}(\alpha)^k, v)q^{n-2}.
\]
Proof. Case 2: In this case, at least two of \(a_{i,0}, a_{i,1}, \ldots, a_{i,n-1}\) are different, the following system of linear equations

\[
\begin{align*}
\sum_{i=0}^{n-1} x_i &= X_0, \quad \zeta = 0, \ldots, l - 1, \\
\sum_{i=0}^{n-1} a_{i}x_i &= Y_0, \quad \eta = 0, \ldots, l - 1
\end{align*}
\]

has exactly \(q^{n-2}\) solutions. By Lemma 4, Case 2 follows.

Case 1: \(a_{i,0} = a_{i,1} = \cdots = a_{i,n-1} \neq 0\).

In this case, the intersection between \(Q(A, B, u)\) and \(Q(A_1, B_1, 0, v)\) is formed by solutions of the system

\[
\begin{align*}
A_1\text{Tr}(x) \sum_{i=0}^{n-1} x_i + B_1\text{Tr}(x)^k \left( \sum_{i=0}^{n-1} x_i \right)^k &= v, \\
A\text{Tr}(x) \sum_{i=0}^{n-1} x_i + B\text{Tr}(x)^k a_{i,0}^{-1} \left( \sum_{i=0}^{n-1} x_i \right)^k &= u/a_{i,0}.
\end{align*}
\]

System (15) has \(\#N(A_1\text{Tr}(x), B_1\text{Tr}(x)^k, v)q^{n-1}\) solutions if \(A_1/A = B_1/B a_{i,0}^{-1}\) and \(A_1u = a_{i,0}vA\).

System (15) has no solution if \(A_1/A = B_1/B a_{i,0}^{-1}\) and \(A_1u \neq a_{i,0}vA\). Case 1.1 follows.

Case 1.2: \(A_1/A \neq B_1/B a_{i,0}^{-1}\), then system (15) is equivalent to

\[
\begin{align*}
\sum_{i=0}^{n-1} x_i &= \frac{B_1u - va_{i,0}B}{a_{i,0}(AB_1 - A_1Ba_{i,0}^{-1})\text{Tr}(x)}, \\
\left( \sum_{i=0}^{n-1} x_i \right)^k &= \frac{a_{i,0}Av - A_1u}{a_{i,0}(AB_1 - A_1Ba_{i,0}^{-1})\text{Tr}(x)^k}.
\end{align*}
\]

So, system (15) has \(q^{n-1}\) solutions if

\[
\frac{B_1u - va_{i,0}B}{a_{i,0}(AB_1 - A_1Ba_{i,0}^{-1})} = \frac{a_{i,0}Av - A_1u}{a_{i,0}(AB_1 - A_1Ba_{i,0}^{-1})}
\]

and no solution otherwise. Case 1.2 follows. \(\Box\)

3. Main results

To describe the main results, we begin this section by introducing the following notations:

\[
F(u) = (-1)^{f(u)},
\]

\[
R(A, B) = \{ u \in GF(q) \mid \#N(A\text{Tr}(x), B\text{Tr}(x)^k, u) > 0 \}.
\]
\[ J(A,B) = \#N(\text{ATr}(x), B\text{Tr}(x^d), 0), \]  
(19)  
\[ K_f(A,B) = \sum_{u \in R(A,B)} F(u), \]  
(20)  
\[ \nabla^\varphi_{f,g}(A,B) = \sum_{u \in R(A,B)} F(au)G(u), \]  
(21)  
\[ H(A,B,a_1,B_1,c,v) = \left\{ x \in \text{GF}(q) \mid \frac{B_1x - ve^k B}{c(AB_1 - A_1Bc^{-1})} \right\}^k = \frac{cA^v - A_1x}{c(AB_1 - A_1Bc^{-1})}, \]  
(22)  
\[ I_f(A,B; A_1,B_1; c) = \sum_{u \in H(A,B,A_1,B_1,c,v)} F(u). \]  
(23)  

**Theorem 7.** Let \( a \) be a primitive generator of the normal basis \( N = \{ x_0 - x, x_1 - x^d, \ldots, x_{n-1} = x^{q^n-1} \} \) of \( \text{GF}(q^n) \) over \( \text{GF}(q) \),  
\[ a^2 = \sum_{i=0}^{n-1} \gamma_{i+1} x_i, \quad a_{\tau,0} = \sum_{j=0}^{n-1} \sigma(aZ_{j0} \odot i) \gamma_{\tau,j}, \quad 0 \leq \tau \leq q^n - 2, \]  
and let \( f \) and \( g \) be two nonlinear functions from \( \text{GF}(q) \) to \( \text{GF}(2) \), then the cross-correlation function \( C(\tau) \) of two linearly related GGSs \( \{ S_{\theta^i}(A,B,A_1,B_1; \alpha) \} \mid 0 \leq i \leq q^n - 2 \} \) and \( \{ S_{\theta^i}(A,B,A_1,B_1; \alpha) \} \mid 0 \leq i \leq q^n - 2 \} \) satisfies  

**Case 1:** If \( a_{\tau,0} = a_{\tau,1} = \cdots = a_{\tau,n-1} \neq 0 \), then  
\[ C(\tau) = \left\{ \begin{array}{ll} q^{n-1}J(A_1,B_1)\nabla^{(A_1)}_{f,q}(A_1,B_1) - F(0)G(0) & A_1 = B_1 = 0, \\ q^{n-1} \sum_{v \in \text{GF}(q)} G(v)L_f(A,B; A_1,B_1; a_{\tau,0}) - F(0)G(0) & \text{otherwise}. \end{array} \right. \]  

**Case 2:** Otherwise  
\[ C(\tau) = q^{n-2}J(A,B)J(A_1,B_1)K_f(A,B)K_g(A_1,B_1) - F(0)G(0). \]  

Furthermore, we have the following statements:  
(1) \( q^{n-2}J(A,B)J(A_1,B_1)K_f(A,B)K_g(A_1,B_1) - F(0)G(0) \) occurs \( q^n - q \) times.  
(2) \( q^{n-1}J(A_1,B_1)\nabla^{(A_1)}_{f,q}(A_1,B_1) - F(0)G(0) \) occurs once for each \( a_{\tau,0} \in \text{GF}(q)^* \) if \( A_1B = 0 \) and \( AB_1 = 0 \).  
(3) \( q^{n-1} \sum_{v \in \text{GF}(q)} G(v)L_f(A,B; A_1,B_1; a_{\tau,0}) - F(0)G(0) \) occurs once for each \( a_{\tau,0} \in \text{GF}(q)^* \) if \( A_1B = 0 \) and \( AB_1 \neq 0 \).  
(4) \( q^{n-1} \sum_{v \in \text{GF}(q)} G(v)L_f(A,B; A_1,B_1; a_{\tau,0}) - F(0)G(0) \) occurs once for each \( a_{\tau,0} \in \text{GF}(q)^* \) if \( A_1B \neq 0 \) and \( AB_1 = 0 \).  
(5) if \( A_1B \neq 0 \) and \( AB_1 \neq 0 \), then \( q^{n-1}J(A_1,B_1)\nabla^{(A_1)}_{f,q}(A_1,B_1) - (0)G(0) \) occurs for \( \sum_{j=0}^{n-1} \lambda^j(AB_1/A_1B) \) elements \( a_{\tau,0} \) in \( \text{GF}(q)^* \); \( q^{n-1} \sum_{v \in \text{GF}(q)} G(v)L_f(A,B); \)}
$A_1, B_1; a_{t,0}) - F(0)G(0)$ occurs for $q - 1 - \sum_{j=0}^{d-1} \lambda^j(AB_1/A_1B)$ elements $a_{t,0}$ in $\text{GF}(q)^*$. where $d = \gcd(k-1, q-1)$ and $\lambda$ is a multiplicative character of $\text{GF}(q)$ of order $d$.

**Proof.** By Definition 2

$$C(\tau) = \sum_{i=0}^{q^t-2} F(\text{ATr}(x^{i+1}) + \text{BTr}(x^{i+kt}))G(A_1\text{Tr}(x^i) + B_1\text{Tr}(x^i))$$

$$= \sum_{u, v \in \text{GF}(q)} |Q(A, B, \tau, u) \cap Q(A_1, B_1, 0, v)|F(u)G(v) - F(0)G(0).$$

**Case 2:** By Case 2 of Lemma 6

$$C(\tau) = q^{n-1} \sum_{u \in \text{GF}(q), A_1u = a_{t,0}A^t} \#N(A_1\text{Tr}(x), B_1\text{Tr}(x^k), v)F(u)G(v) - F(0)G(0)$$

$$= q^{n-1} \sum_{v \in R(A_1, B_1)} J(A_1, B_1)G(v) - F(0)G(0).$$

**Case 1:** If $A_1/A = B_1/Ba_k^{-1}$. then

$$C(\tau) = q^{n-1} \sum_{u, v \in \text{GF}(q), A_1u = a_{t,0}A^t} \#N(A_1\text{Tr}(x), B_1\text{Tr}(x^k), v)F(u)G(v) - F(0)G(0)$$

$$= q^{n-1} \sum_{v \in R(A_1, B_1)} J(A_1, B_1)G(v) - F(0)G(0).$$

If $A_1/A \neq B_1/Ba_k^{-1}$, then

$$C(\tau) = q^{n-1} \sum_{v \in \text{GF}(q)} G(v) - F(0)G(0)$$

$$= q^{n-1} \sum_{v \in \text{GF}(q)} G(v)L_v^f(A, B; A_1, B_1; a_{t,0}) - F(0)G(0).$$

Since the map $\varphi(x^t) = (a_{t,0}, a_{t,1}, \ldots, a_{t,n-1})$ is one-to-one, the distribution of their cross-correlation function values is easily obtained by counting the number of nonzero solutions of $A_1Bx^{k-1} = AB_1$. $\square$

**Proposition 8.** Given $A, B \in \text{GF}(q)$, then $|\{u \in \text{GF}(q) \mid \#N(A, B, u) > 0\}| = q/\#N(A, B, 0)$. 
Proof. Let \( a \) be a primitive element of \( \text{GF}(q) \), we define a matrix \( H = (h_{ij}) \), where \( i, j = 0, 1, \ldots, q - 2 \), by \( h_{ij} = 1 \) if \( Ax^i + Bx^j = \alpha^i \), and \( h_{ij} = 0 \) otherwise.

For a given \( i \), if \( Ax^i + Bx^j = 0 \), then the \( i \)th row of \( H \) are all zeros. Otherwise the \( i \)th row of \( H \) has only one 1. Thus the number of 1’s in \( H \) is \( q - \#N(A, B, 0) \) since \( \left| \left\{ i \mid Ax^i + Bx^j = 0 \right\} \right| = \#N(A, B, 0) - 1 \).

Suppose there are \( \Delta \) elements \( C \) in \( \text{GF}(q) \) such that \( Ax + Bx^j = C \) has at least one solution in \( \text{GF}(q) \). Then \( \Delta - 1 \) of them are nonzero. For a given \( j \), if \( Ax + Bx^j = \alpha \) has at least one solution, then there are \( \#N(A, B, 0) \) solutions by Lemma 5, and the \( j \)th column of \( H \) has \( \#N(A, B, 0) \) 1’s. Otherwise the \( j \)th column of \( H \) are all zeros, therefore there are \( (\Delta - 1)\#N(A, B, 0) \) 1’s in \( H \). Thus

\[
(\Delta - 1)\#N(A, B, 0) = q - \#N(A, B, 0)
\]

or equivalently, \( \Delta = q/\#N(A, B, 0) \). \( \square \)

Remark 9. When \( q \) is odd, then \( |R(A, B)| \) is odd by Proposition 8, and \( |K_f(A, B)| > 0 \) for any \( A, B \in \text{GF}(q) \) and any nonlinear function \( f \) from \( \text{GF}(q) \) to \( \text{GF}(2) \). Therefore, by Theorem 7, \( |C(\tau)| \ge q^n - 1 \) for at least \( q^n - q \) shifts, which is unacceptably high in applications.

Remark 10. When \( q \) is even, then \( |R(A, B)| \) is even for arbitrary \( A, B \in \text{GF}(q) \) since \( \#N(A, B, 0) = 2^l \) for some integer \( l > 0 \) and \( q = 2^c \). Thus, we may choose \( A, B \in \text{GF}(q) \) and \( f : \text{GF}(q) \to \text{GF}(2) \) such that \( f \) is balanced over \( R(A, B) \), i.e., \( K_f(A, B) = 0 \). In this case, \( C(\tau) = -1 \) for at least \( q^n - q \) shifts by Theorem 7, which is ideal except for several shifts.

Remark 11. When \( A \neq 0, B = 0 \) and \( A_1 = 0, B_1 \neq 0 \), Theorem 7 coincides with Theorem 2.1 of [1].

4. Conclusion

Explicit formulas for cross-correlation functions of linearly related generalized geometric sequences are derived, therefore an open problem posed by Klapper et al. in [1] is partially solved. It is difficult for us to calculate cross-correlation functions of general generalized geometric sequences. We believe that the theory of exponential sums over finite field is useful in solving the difficult problem completely.

Acknowledgements

The authors wish to thank anonymous referees for several valuable suggestions that improved this paper and for pointing out a flaw in Theorem 7 of our original manuscript.
References