THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Mat Lab Implementation of Algorithm for Generating Multisequences

Himanshu Sharma
M Tech Scholar, Department of Electronics and Communication
Manipal University Jaipur, Rajasthan, India

Abstract:
In this paper I introduced the concept of multisequences and their extensions. I also discussed the formula to calculate the number of multisequences whose extension have maximum dimension. Further I give an algorithm and MATLAB code for the generation of such sequences.

***Key words**: multisequences, extension, matrix states, algorithm, mat lab code*

1. Introduction

Linear recurring sequences find applications in wide array of areas including error correcting codes [3], spread spectrum communication [4] and cryptography [2].

Multisequence is defined as the sequence of vectors that are extension of a sequence of scalars over the finite field. The generation of multisequences using minimal polynomial has been an important problem motivating papers like [8], [9] and [10].

In this section first I discuss the basic theory of multisequences and then I implement an algorithm on MATLAB to generate multisequences with maximum dimension.

In the remainder of this section F_q denotes a field of cardinality *c*, where *c* is a prime power. $F_q[s]$ denotes the ring of polynomials in *s* with coefficients fromF_q. $G(n, F_q)$represents the group of all full rank matrices. /*S*/ denotes the cardinality of any set *S*.

2. Multisequences

Let *S* denotes a sequence in F_q as mapping from *Z* to F_q. There exists an integer *n* such that *S (k+n) = S (k)* for all *k*, where *n* is known as period of sequence and sequence *S* is called periodic sequence. There are linear recurring relations among these periodic sequence and defined by relation.

$S(k+n) = a_{n-1}S(k+n-1) + a_{n-2}S(k+n-2) + \cdots + a_0 S(k)\ \forall\, k\ ;\ a_i \in F_q$

Where *n* is called as order of linear recurring relation. As I have consider periodic sequence only so let a_0 is not equal 0 [15, theorem6.11] and polynomial associated with linear recurring relation is$p(s) = s^n - a_{n-1}s^{n-1} - a_{n-2}s^{n-2} - \cdots - a_0$.

For any sequence *S*, all the polynomials associated with LRR form an ideal in the polynomial ring$F_q[s]$. since $F_q[s]$ is a principal ideal domain, every ideal has a unique monic generating polynomial which is called as minimal polynomial of the sequence *S* and linear complexity of the sequence is defined as the degree of minimal polynomial.

For a given LRR of degree *n*, there are various sequences and the collection of all sequences that satisfy this relation form a vector space over F_q. If the polynomial associated with the LRR is a primitive polynomial of degree *n*, then every nonzero sequence in the corresponding vector space has a period equal to $q^n - 1$ ([15, Theorem 6.33]).

Let a sequence of complexity *n* having *n* consecutive elements of the sequence, the vector consisting of *n* consecutive elements of the sequence is called the state vector of the sequence. Let the *i-th* state vector of the sequence can be denoted by *x(i)* i.e., *x(i) = [S(i), S(i + 1), . . . , S(i + n − 1)]*.

Let *σS* denote the sequence got by shifting the sequence *S* once to the left i.e., *σS(k) = S(k +1)*. The *k-th* state vector of *σS* is denoted by *σx(k)*. Therefore *σx(k) = x(k + 1)*. Note that *σx(k)= x(k + 1) = x(k)A*, where *A* is the companion matrix of the polynomial *p(s)* and given by:

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & a_0 \\ 1 & 0 & 0 & 0 & a_1 \\ 0 & 1 & 0 & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{bmatrix} \in F_q^{n\times n}$$

This matrix is the companion matrix of the polynomial $p(s) = s^n - a_{n-1}s^{n-1} - a_{n-2}s^{n-2} - \cdots - a_0$. Observe that the companion matrix associated to the polynomial is unique.

Similar to sequences, let us define a multisequence in F_q^m as a map from *Z* to F_q^m. as in the case of scalar sequences, there exist LRR between the elements the multisequences. These relations are of the form

$W(k+n) = a_{n-1}W(k+n-1) + a_{n-2}W(k+n-2) + \cdots + a_0 W(k)\ \forall\, k\ ;\ a_i \in F_q$

Similar to scalar sequences, the polynomials associated to all LRRs of a given periodic multisequence, form an ideal in the principal ideal domain $F_q[s]$ and the monic generator of this ideal is called the minimal polynomial of the multisequence. The *i-th* component of each vector in W gives a sequence of scalars in F_q. Clearly, the minimal polynomial of the multisequence is the least common multiple of the minimal polynomials of the component sequences. Note that multisequence, with linear complexity *n* is completely determined by the first n terms. The state of a multisequence can therefore be thought of as *n* consecutive elements of the multisequence. Each state is thus an $m \times n$ matrix. Let the *k-th* matrix state of the multisequence is denoted by *MW(k)*, i.e. *MW(k) = [W(k),W(k + 1), . . . ,W(n + k − 1)]*.

Definition 2.1: The column span of the matrix states is defined by an in-variance property for a periodic multisequence.

Proof. Consider a periodic multisequence W. It is enough to show that *colspan*$(M_W(k))$= *colspan*$(M_W(k+1))$, for any given integer *k*. Let the minimal polynomial of the multi-
sequence be $p(s) = s^n - a_{n-1}s^{n-1} - a_{n-2}s^{n-2} - \cdots - a_0$. Since $W(k+n) = a_{n-1}W(k+n-1) + a_{n-2}W(k+n-2) + \cdots + a_0W(k)$, therefore *W(k + n)*∈*colspan*$(M_W(k))$.

Thus, *colspan*$(M_W(k+1))$⊆*colspan*$(M_W(k))$. Since $a_0 \neq 0$, *W(k)* = $\frac{1}{a_0}$(*W(k + n)*− a_1*W(k + 1)* −a_2*W(k + 2)*− . . .−a_{n-1}*W(k + n − 1))*, i.e., *W(k)* ∈*colspan*$(M_W(k+1))$. Hence *colspan*$(M_W(k))$⊆*colspan*$(M_W(k+1))$.

Therefore *colspan*$(M_W(k+1))$= *colspan*$(M_W(k))$. Hence proved.

Definition 2.2: The dimension of a multisequence W is defined as the rank of its matrix states.

As in the case of scalar sequences, any nonzero multisequence with a primitive minimal polynomial *p(s)* of degree *n*, has a period of $q^n - 1$. In this paper, let us assume that the multisequences having primitive minimal polynomials are considered only.

Now one question that comes to mind is that for any given positive integer *l* and a primitive polynomial *p(s)* of degree *n*, how many multisequences of dimension *l* exist in a field with *p(s)* as its minimal polynomial.

As we know that two multisequences are considered the same if they are shifted versions of one another let $G(l, m, F_q)$ denote the collection of l dimensional subspaces of field and the cardinality is given by:

$|\ G(l, m, F_q)| = \frac{(q^m-1)(q^m-q)\ldots(q^m-q^{l-1})}{(q^l-1)(q^l-q)\ldots(q^l-q^{l-1})}$

Definition 2.3: Given a primitive polynomial p(s) of degree n, the number of multisequences in F_q^m, with minimal polynomial *p(s)*, having dimension *l* is $|\ G(l, m, F_q)|\ \times (q^n - q)\ (q^n - q^2) \ldots (q^n - q^{l-1})$.

Proof: For a multisequence W of dimension *l*, by definition1, the column space of the matrix state $M_W(k)$ is a unique l dimensional subspace of F_q^m. Note that there are $G(l, m, F_q)$ subspaces ofF_q^m that have dimension *l*. Consider one such *l*-dimensional space *V*. Let *T* be the matrix *T* = $[v_1, v_2, \ldots, v_l]$. Any $M \in F_q^{m\times n}$ whose column span is *V* can be written as *M = TB; B*∈ $F_q^{l\times n}$, where no of such matrices *B* is $(q^n - 1)\ (q^n - q) \ldots\ (q^n - q^{l-1})$. As the polynomial *p(s)* is primitive, each multisequence has $q^n - 1$ distinct matrix states, so number of multisequences with *V* is equal to $\frac{(q^n-1)\ (q^n-q)\ldots\ (q^n-q^{l-1})}{q^n-1} = (q^n - q)(q^n - q^2) \ldots\ (q^n - q^{l-1})$. Therefore, given a primitive polynomial p(s) of degree n, the number of multisequences in F_q^m, with minimal polynomial *p(s)*, having dimension *l* is $|\ G(l, m, F_q)|\ \times (q^n - q)\ (q^n - q^2) \ldots (q^n - q^{l-1})$.

If a multisequence in F_q^m has dimension m, its component sequences are linearly independent, and from above Definition 2.3, one can give the following corollary to Definition 2.3.

Corollary: Given a primitive minimal polynomial *p(s)* of degree *n*, the number of multisequences in F_q^m, with minimal polynomial *p(s)*, having linearly independent component sequences is $= (q^n - q)(q^n - q^2) \ldots\ (q^n - q^{m-1})$.

3. Extension of Multisequences

Next task is to extend multisequence W to a new sequence V whose dimension is greater than W. Further let's assume that minimal polynomial of both the sequences are same and this can be done by appending linear combination of W to it. As we know that linear combination is given by $a_1W_1 + a_2W_2 + \cdots + a_nW_n$, thus $W_j = \sum_{i=1}^{m} a_iW_i$ for *j > m*, where $a_i \in F_q$.

Let R = $(r_1, \ldots\ldots, r_m) \in Z_+^m$, with$\sum r_k$ = r. so the *R*- extension of the multisequence W in F_q^m as the multisequence W_R in F_q^r, whose component sequences are obtained from the component sequences of W in the following order : $W_1, \sigma W_1, \ldots \sigma^{r_1-1}W_1, W_2, \sigma W_2, \ldots .\sigma^{r_2-1}W_2, \ldots W_i, \sigma W_i, \ldots \sigma^{r_i-1}W_i, \ldots W_m, \sigma W_m, \ldots \sigma^{r_m-1}W_m$. next question that comes to mind is defined as:

Question 3.1: For R = $(r_1, \ldots\ldots, r_m) \in Z_+^m$, with$\sum r_k$ = r, how many multisequences W of rank m in F_q^m give *R*-extended multisequences in F_q^r whose dimension is equal to r?

Solution: R = $(r_1, \ldots\ldots, r_m) \in Z_+^m$ such that r = $\sum r_i$ and let p(s) be a primitive polynomial of degree n. The number of multisequences in F_q^m with minimal polynomial p(s) whose extensions have dimension r is equal to $(q^n - q^{r-m+1})\ (q^n - q^{r-m+2})\ (q^n - q^{r-1})$.starting with a multisequence in F_q^m with dimension m, let us recursively generate a series of multisequences in F_q^m whose *R*- extension has dimension r. so for the constructive proof to this solution, let prove a few preparatory results.

For any G = $(g_1, \ldots\ldots, g_m) \in Z_+^m$ let $G_{max} = max_i g_i$. Let φ define the following map from Z_+^m to Z_+^m.

$\varphi(g_1, \ldots\ldots, g_m) = (g_1, g_2\ \ldots\ldots, g_{c-1}, g_c - 1, g_{c+1}, \ldots, g_m)$ where c is the smallest integer such that $g_c = G_{max}$.

One can observe that repeated action of φ on any element of Z_+^m eventually gives 1 = (1,1,…..,1). Hence for given R = $(r_1, \ldots\ldots, r_m) \in Z_+^m$, φ defines a unique path from R to 1 and can be defined as the '*R*- road'.

Example: the R- road for R = (3,2,5,4,1) is (3,2,4,4,1) (3,2,3,4,1) (3,2,3,3,1) (2,2,3,3,1) (2,2,2,3,1) (2,2,2,2,1) (1,2,2,2,1) (1,1,2,2,1) (1,1,1,2,1) (1,1,1,1,1).

Clearly given any point G = ($g_1, \ldots\ldots, g_m$) on an R-road, for any other point Q = ($q_1, \ldots\ldots, q_m$) lying on the path from R to G, $q_i \geq g_i \forall\, i$ and also note that if $i < j, g_i > g_j$ if and only if $g_i > r_j$. By retracing the R- road from 1 to R, let define following definition.

Definition 3.1: for every point G = ($g_1, \ldots\ldots, g_m$) ≠ R on the R-road, there exists a coordinate g_c which satisfies at least one of the following conditions:

a) $g_c = G_{max} - 1$ and $g_c < r_c$.

b) $g_c = G_{max}$ and $g_c < r_c$.

Proof: For every point G = ($g_1, \ldots\ldots, g_m$) ≠ R on the R- road, there exists a unique point H on the R- road such that φ(H) = G. Now, H = ($g_1, g_2 \ \ldots\ldots, g_{c-1}, g_c - 1, g_{c+1}, \ldots, g_m$), where $g_c + 1 \geq g_i \forall\, i \neq$ c. Also, since H is on the path from R to 1, $g_c + 1 \leq r_c$. Therefore, $g_c < r_c$. If $g_c + 1 > g_i \forall\, i \neq$ c then $g_c = G_{max}$. If instead, there exists an i such that $g_c + 1 = g_i$, then $g_c = G_{max}$- 1. Hence proved.

Definition 3.2: consider an R = ($r_1, \ldots\ldots, r_m$)∈ Z_+^m. For every point G = ($g_1, \ldots\ldots, g_m$) ≠ R, on the R- road the active coordinate is defined as follows :

1. If there exists a coordinate g_c such that $g_c = G_{max} - 1$ and $g_c < r_c$, then the active coordinate is the coordinate corresponding to the largest such c.

2. In the event of there being no g_c that satisfies point 1, the active coordinate is the coordinate corresponding to the largest c such that $g_c = G_{max}$ and $g_c < r_c$.

This can be seen that one can traverse the R – road backwards from 1 to R by repeatedly incrementing the active coordinate at every point as shown in following example:

Example: Let R = (3,2,5,4,1). Starting from 1 the R- road backwards as follows: (1,1,1,<u>1</u>,1) (1,1,<u>1</u>,2,1) (1,<u>1</u>,2,2,1) (<u>1</u>,2,2,2,1) (2,2,2,<u>2</u>,1) (2,2,<u>2</u>,3,1) (<u>2</u>,2,3,3,1) (3,2,3,<u>3</u>,1) (3,2,<u>3</u>,4,1) (3,2,<u>4</u>,4,1) (3,2,5,4,1).

Therefore following steps are used to detect the active coordinate of any point G :

a) Find G_{max}.

b) Find the largest i such that the $i-th$ coordinate has value $G_{max} - 1$ and is less than r_i.

c) If there is no i satisfying the preceding condition, find the largest j such that the $j-th$ coordinate has value G_{max} and is less than r_j.

So following observation are made : given a matrix $A\in F_q^{l\times l}$ in the companion form and a vector $x = (b_1, \ldots\ldots, b_l) \in F_q^l$, for $k < l$, xA^k has the following form

$$xA^k = (b_{k+1}, b_{k+2}, \ldots\ldots, b_l, \underbrace{*, *, \ldots\ldots, *}_{k\ entries})$$

Where the *s are elements in F_q, whose value depend on the matrix A. Therefore, the matrix $[x; xA; \ldots.; xA^{k-1}]$ has the following structure.

$$\begin{bmatrix} b_1 & b_2 & \cdots & b_{l-k+1} & b_{l-k+2} & \cdots & b_{l-1} & b_l \\ b_2 & b_3 & \cdots & b_{l-k+2} & b_{l-k+3} & \cdots & b_l & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_k & b_{k+1} & \cdots & b_l & * & \cdots & * & * \end{bmatrix}$$

For any G)∈ Z_+^m, let $N(G,k)$ denote the number of multisequences in F_q^m with a given primitive minimal polynomial of degree k, whose G- extensions have maximum dimension.

Definition 3.3: let R = ($r_1, \ldots\ldots, r_m$), and let $G = (g_1, \ldots\ldots, g_m)$ and $\varphi(G)$ be the consecutive points on the R- road. Then,

$$N(G,k) = q^{m-1} N(\varphi(G), k-1)$$

Where k is any integer greater than $g = \sum_{i=1}^m g_i$.

Proof: Let c be the smallest integer such that $g_c = G_{max}$. Therefore $\varphi(G) = (g_1, g_2 \ \ldots\ldots, g_{c-1}, g_c - 1, g_{c+1}, \ldots, g_m)$. Let W be a multisequence in F_q^m whose minimal polynomial p_{k-1}(s) is a primitive polynomial of degree $k-1$. Further assume that the $\varphi(G)$-extension of W has dimension g-1. Each matrix state of W is therefore a matrix in $F_q^{m\times(k-1)}$ with full row rank. As p_{k-1}(s) is a primitive polynomial of degree $k-1$, there exist a matrix state M of W , whose c-th row is e_{k-1}^{k-1} = (0, 0, …., 0, 1). For $i \neq c$, let $x_i = [b_{i1}, b_{i1}, \ldots, b_{i(k-1)}]$ be the $i-th$ row of this M. Therefore, $M = [x_1; x_2; \ldots; x_{c-1}; e_{k-1}^{k-1}; x_{c+1}; \ldots; x_m]$. Now expand M to a matrix $M^* \in F_q^{m\times k}$ as follows:

1) For every $i \neq c$, append the $i-th$ row of M with any element d_i of F_q. Therefore, the $i-th$ row of M^* is $x_i^* = (x_i, d_i) \in F_q^k$, for some d_i of F_q.

2) Let the $c-th$ row of M^* be e_k^k i.e.,(0,0,…,0,1).

If p_k(s) be s primitive polynomial of degree k, then using M^* as a matrix state, one can generate a multisequence W^* with same polynomial. So W^* has a G –extension with dimension g.

As M is a matrix state of W, the following matrix $M_{\varphi(G)}$ is a matrix state of the $\varphi(G)$ –extension of W:

$M_{\varphi(G)} = [x_1; x_1A_{k-1}; \ldots; x_1A_{k-1}^{g_1-1}; x_2; x_2A_{k-1}; \ldots; x_2A_{k-1}^{g_2-1}; x_{c-1}; x_{c-1}A_{k-1}; \ldots; x_{c-1}A_{k-1}^{g_{c-1}-1};$
$e_{k-1}^{k-1}; e_{k-1}^{k-1}A_{k-1}; \ldots\ldots; e_{k-1}^{k-1}A_{k-1}^{g_c-2}; x_{c+1}; x_{c+1}A_{k-1}; \ldots\ldots; x_{c+1}A_{k-1}^{g_{c+1}-1}; \ldots; x_m;$
$x_mA_{k-1}; \ldots; x_mA_{k-1}^{g_m-1}]$,where A_{k-1} is the companion matrix of the polynomial p_{k-1}(s).The $c-th$ block of rows of $M_{\varphi(G)}$ has the following structure:

$$\left[\begin{array}{cccc|cccc} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & * \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & \cdots & * & * \end{array}\right] \in F_q^{(g_c-1)\times(k-1)}$$

For $1 \leq i \neq c \leq m$, let $x_i = (b_{i1}, b_{i1}, \ldots, b_{i(k-1)})$. The corresponding $i-th$ block of rows of $M_{\varphi(G)}$ has the following structure:

$$\left[\begin{array}{cccc|cccccc} b_{i1} & b_{i2} & \cdots & b_{i(k-g_c)} & b_{i(k-g_c+1)} & \cdots & b_{i(k-g_i+1)} & \cdots & b_{i(k-2)} & b_{i(k-1)} \\ b_{i2} & b_{i3} & \cdots & b_{i(k-g_c+1)} & b_{i(k-g_c+2)} & \cdots & b_{i(k-g_i+2)} & \cdots & b_{i(k-1)} & * \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{ig_i} & b_{i(g_i+1)} & \cdots & b_{i(k-g_c+g_i-1)} & b_{i(k-g_c+g_i)} & \cdots & b_{i(k-1)} & \cdots & * & * \end{array}\right]$$

The *s shown in the blocks above represent entries from F_q which depend on the matrix A_{k-1}. Since $g_c \geq g_i \forall\, i$, the *s appear only in the last $g_c - 1$ columns of $M_{\varphi(G)}$. As $\varphi(G)$-extension of W has rank $g-1$, therefore $M_{\varphi(G)}$ has rank $g-1$.

Similarly, corresponding to the matrix state M^* of W^*, the matrix state of the $G-$ extension of W^* is given by:

$M_G^* = [x_1^*;x_1^*A_k;\ldots;x_1^*A_k^{g_1-1}; x_2^*; x_2^*A_k; \ldots; x_2^*A_k^{g_2-1}; x_{c-1}^*; x_{c-1}^*A_k; \ldots; x_{c-1}^*A_k^{g_{c-1}-1};$
$e_k^k; e_k^kA_k; \ldots\ldots; e_k^kA_k^{g_c-1};\ x_{c+1}^*; x_{c+1}^*A_k; \ldots; x_{c+1}^*A_k^{g_{c+1}-1};\ldots; x_m^*;$
$x_m^*A_k;\ldots;x_m^*A_k^{g_m-1}]$,where A_{k-1} is the companion matrix of the polynomialp_k(s).

For $i \neq c$, the $i-th$ block of M_G^* is $[x_i^*;x_i^*A_k;\ldots;x_i^*A_k^{g_i-1}]$. Recall that $x_i^* = (x_i, d_i)$, thus block has the following structure.

$$\left[\begin{array}{cccc|cccc} 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 1 & * \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & \cdots & * & * \end{array}\right] \in F_q^{(g_c)\times k}$$

Let M_G be the submatrix of M_G^* got by removing its last column and the first row of its $c-th$ block. Observe that rank(M_G) = rank(M_G^*)-1. By the structure if the $c-th$ block of M_G one can clearly see that this submatrix M_G can be modified to $M_{\varphi(G)}$ using elementary row operations. Hence this submatrix M_G has rank$g-1$. This implies that M_G^* has rank g. Therefore, W^* does have a $G-$ extension with dimension g.

Note that each of the d_is can be chosen in q ways. Each such choice yields a different matrix M^* and hence a different multisequence W^*. As a result for every multisequence W with minimal polynomial p_{k-1}(s), the above process gives us q^{m-1} multisequences W^* with minimal polynomial p_k(s). Therefore,

$N(G,k) \geq q^{m-1}N(\varphi(G),k-1)$ (A)

Conversely, consider a multisequence U^* in F_q^m with primitive polynomial p_k(s) whose $G-$extension has rank g. Consider its matrix state $M_1^* \in F_q^{m\times k}$ whose $c-th$ row is e_k^k. Now M_1^* can be reduced to a matrix $M_1 \in F_q^{m\times(k-1)}$ as follows:

1) For $i \neq c$ remove the last entry of the $i-th$ row.
2) Let the $c-th$ row of M_1 be e_{k-1}^{k-1}.

Let M_1 generate a multisequence U having primitive minimal polynomial p_{k-1}(s). Using similar arguments as those used earlier in the proof, one can prove that the $\varphi(G)$ –extension of U has dimension $g-1$. Note that the matrix M_1 is independent of the last entries of the rows of M_1^*. Hence, there are q^{m-1} matrices (including M_1^*), with $c-th$ row e_k^k, which have the same first $k-1$ columns as M_1. By the above process each one of these matrices gives the same matrix M_1. Besides if we start with a matrix with $c-th$ row e_k^k which differs from M_1 in any entry corresponding to the first $k-1$ columns, it results in a different M_1. Therefore,

$N(\varphi(G),k-1) \geq \frac{N(G,k)}{q^{m-1}}$ (B)

$\Rightarrow q^{m-1}N(\varphi(G),k-1) \geq N(G,k)$

Thus, from equation (A) and (B) one can conclude that

$N(G,k) = q^{m-1}N(\varphi(G),k-1)$

Using this result, Question 3.1 can be proved in the following manner:

Proof: For each j, such that $n-r+m \leq j \leq n$, let p_j(s) be a given primitive polynomial of degree j. For every point $G = (g_1,\ldots\ldots,g_m)$ on the R-road, let $g = \sum_{i=1}^m g_i$. As seen in the previous definition's proof, starting from a multisequence in F_q^m with dimension m having minimal polynomial p_{n-r+m}(s), one can recursively generate multisequences in F_q^m, with minimal polynomial p_{n-r+g}(s), whose $G-$ extension have maximum dimension, for every G on the R-road.

By above definition for any two consecutive points, $\varphi(G)$ and $G = (g_1,\ldots\ldots,g_m)$ in the path from 1 = (1,1,…,1) to R, $N(G,n-r+g) = q^{m-1}N(\varphi(G),n-r+g-1)$ where $g = \sum_{i=1}^m g_i$. The path from 1 to R has $r-m$ such steps. Therefore,

$N(R,n) = (q^{m-1})^{r-m}N(1,n-r+m)$

However, $N(1,n-r+m)$ is the number of multisequences in F_q^m of dimension m, with a given primitive minimal polynomial p_{n-r+m}(s) of degree $n-r+m$. Therefore, by corollary, $N(1,n-r+m) = (q^{n-r+m}-q)\,(q^{n-r+m}-q^2)\ldots(q^{n-r+m}-q^{m-1})$.
Hence,

$N(R,n) = (q^{m-1})^{r-m}(q^{n-r+m}-q)\,(q^{n-r+m}-q^2)\ldots(q^{n-r+m}-q^{m-1})$
$= (q^n-q^{r-m+1})\,(q^n-q^{r-m+2})\ldots(q^n-q^{r-1})$.

Hence proved. Note that $N(R,n)$ does not depend on the integers $(r_1,\ldots\ldots,r_m)$ but just their sum.Further recall the question as:

Question 3.2: given any r$\geq m$, how many multisequences in F_q^r having dimension r are R-extensions of multisequences in F_q^m for some $R = (r_1,\ldots\ldots,r_m) \in Z_+^m$ where $\sum r_i$ = r.

Solution: the number of multisequences in F_q^r which are R-extensions of multisequences in F_q^m is given by:
$N_r = \binom{r-1}{r-m}(q^n - q^{r-m+1})\,(q^n - q^{r-m+2})\ldots(q^n - q^{r-1})$.
Proof: for any r $\in Z_+$, define the following subset R_r of Z_+^m.
$R_r = \{(r_1, \ldots, r_m) \in Z_+^m \mid \sum_{i=1}^m r_i = r\}$
Therefore,
$N_r = |R_r| \times (q^n - q^{r-m+1})\,(q^n - q^{r-m+2})\ldots(q^n - q^{r-1})$
Corresponding to each element of R_r, say $(r_1, \ldots, r_m)$, we can define a monomial, $x_1^{r_1} x_2^{r_2} \ldots x_m^{r_m}$. Therefore, calculating $|R_r|$ is equivalent to finding the number of monomials of degree r. Consequently, the cardinality of R_r is equal to the number of monomials of degree $r - m$. This number is equal to $\binom{(r-m)+m-1}{r-m} = \binom{r-1}{r-m}$. As a result,
$N_r = \binom{r-1}{r-m}(q^n - q^{r-m+1})\,(q^n - q^{r-m+2})\ldots(q^n - q^{r-1})$.
Given R = $(r_1, \ldots, r_m) \in Z_+^m$, let $\sum_{i=1}^m r_i = r$. $\{p_j(\mathrm{s})\}_{j=n-r+m}^{n}$ be a series of primitive polynomial where the index j denotes the degree of the respective polynomial. Let A_js be their corresponding companion matrices. Let $\varphi(G)$ and G be consecutive points on the R-road. Also c define the position of the active coordinate of $\varphi(G)$. Consider a multisequence U in F_q^m with a minimal polynomial $p_{n-r+g-1}$(s), whose $\varphi(G)$ −extension has maximum dimension.its matrix state is denoted by M_U having $c - th$ row equal to $e_{n-r+g-1}^{n-r+g-1}$. As definition tells about the procedure to find matrix state, one can generate a sequence of matrices $\{M_j\}_{j=n-r+m}^{m}$ starting with a matrix $M_{n-r+m} \in F_q^{m\times(n-r+m)}$ having full rank and culminating in a matrix $M_n \in F_q^{m\times n}$. Each matrix M_j in the above sequence uniquely corresponds to a point G on the R-road and can br seen as a matrix state of a multisequense with minimal polynomial p_j(s) whose corresponding G-extension has maximum dimension.

4. Algorithm for the Generation of Multisequences

The variable M is used to store the respective matrix state at every step of the algorithm. The current point in the path from 1 to R is stored in the variable $G = (g_1, \ldots, g_m)$. The variable c stores the summation of the values of the coordinates of G.
Initialization:
Step1. Initialize G to 1.
Step 2. Initialize the value of g to m.
Step 3. Initialize M to any matrix in $F_q^{m\times(n-r+m)}$ that has full rank.
Main loop:
Step 4. While $g < r$

- Find the position of the active coordinate of G and store it in c.
- Find a polynomial $f(s)$ such that $M(c,:)f(A_{n-r+g}) = e_{n-r+g}^{n-r+g}$.
- $M = M\,f(A_{n-r+g})$.(This gives us the matrix state whose $c - th$ row is e_{n-r+g}^{n-r+g}).
- For all $i \neq c$ append the $i - th$ rowof M with any $d_i \in F_q$ to get the row vector $(M(i,:), d_i)$.
- Change the $c - th$ row of M to $e_{n-r+g+1}^{n-r+g+1}$.
- Increment of g and g_c by 1.

To find the polynomial $f(s)$, the following subloop is used as:
Subloop:
Step 1. Construct the matrix $\mathcal{M} = [M(c,:); M(c,:)A_{n-r+g}; \ldots; M(c,:)A_{n-r+g}^{n-r+g-1}]$
Step 2. Solve the set of linear equations

$$a\mathcal{M} = e_{n-r+g}^{n-r+g} \; for \; a \in F_q^{n-r+g}$$

Step 3. If $a = (a_1, a_2, \ldots, a_{n-r+g-1})$ is the solution to above set of equations, $a_0 M(c,:) + a_1 M(c,:)A_{n-r+g} + \cdots + a_{n-r+g-1} M(c,:)A_{n-r+g}^{n-r+g-1} = e_{n-r+g}^{n-r+g}$. Therefore $f(s) = a_0 + a_1 s + \cdots + a_{n-r+g-1} s^{n-r+g-1}$.
Let c_1 and c_2 be the active coordinates of 1 and $\varphi(R)$ respectively. So above algorithm can be thought of as a map from the space of matrices in $F_q^{m\times(n-r+m)}$ which have full row rank and whose c_1 −th rows are e_{n-r+m}^{n-r+m}, to the space of matrices in $F_q^{m\times n}$ which have full row rank and whose c_2 −th rows are e_n^n. There are precisely $(q^{n-r+m} - q)\,(q^{n-r+m} - q^2)\ldots(q^{n-r+m} - q^{m-1})$ matrices in $F_q^{m\times(n-r+m)}$ whose c_1 −th rows are e_{n-r+m}^{n-r+m}. During each iteration of the while loop one can chose d_is in q^{m-1} ways. Therefore, corresponding to each choice of matrix M_{n-r+m} can give the same M_n. Therefore, there are $(q^n - q^{r-m+1})\,(q^n - q^{r-m+2})\ldots(q^n - q^{r-1})$ possible matrices which can occur as an output to yhis algorithm. The number of full row rank matrices in $F_q^{m\times n}$, whose c_2 −th row is e_n^n, is however $(q^n - q)\,(q^n - q^2)\ldots(q^n - q^{m-1})$. Out of these matrices, precisely those matrices that occur as matrix states of multisequences whose R-extension have full rank are the ones that can be obtained from the above algorithm.

5. Program

```
clc;
clear all ;
R = input('enter the matrix R =');
G = input('enter the matrix G =');
r = sum(R);
g = sum(G);
k = length(G);
i = k;
e=k;
if G(k) == R(k)
m=triu(ones(k,g+1));
else
m=triu(ones(k,g))
w = gf(rand([e,1]));
t = zeros(1,g+1);
t(g+1)=1;
m=[m w];
m(g,:)=t;
m=m
end
while i  > 0 && i ~= 0
if G(i) == R(i)
if i-1 >= 1
if G(i-1) == R(i-1) && sum(G)== sum(R)-1
[y c]=max(R);
i=c;
G(c)=G(c)+1;
G=G
g=sum(G);
[y c]=max(G);
c=c
m = gf(m);
p1 = gfprimfd(g,'min',2)
p2= p1(:,1:g);
p= p2';
a = gf([[zeros(1,g-1);eye(g-1,g-1)] p]);
t =gf(ones(g-1,g));
for j = 1:g-1
n = gf(m(c,:)*(a^j));
t(j,:)=n;
end
M = [m(c,:);t];
b = zeros(g,1);
b(g)=1;
x = inv(M)*b;
s = zeros(g,g);
for j = 1:g-1
f= gf(x(j+1)*(a^j));
s=s+f;
s=gf(m*s);
f = gf((x(1,:)*m)+ s);
m=f
if sum(G) == sum(R)
return;
else w = gf(rand([e,1]));
t = zeros(1,g+1);
t(g+1)=1;
m=[m w];
m(c,:)=t;
m=m
end
```

```
return;
elseif G(i-1) == R(i-1)
G=G
g=sum(G);
[y c]=max(G);
c=c
m = gf(m);
p1 = gfprimfd(g,'min',2)
p2= p1(:,1:g);
p= p2';
a = gf([[zeros(1,g-1);eye(g-1,g-1)] p]);
t =gf(ones(g-1,g));
for j = 1:g-1
n = gf(m(c,:)*(a^j));
t(j,:)=n;
end
M = [m(c,:);t];
b = zeros(g,1);
b(g)=1;
x = inv(M)*b;
s = zeros(g,g);
for j = 1:g-1
f= gf(x(j+1)*(a^j));
s=s+f;
end
s=gf(m*s);
f = gf((x(1,:)*m)+ s);
m=f
if sum(G) == sum(R)
return;
else w = gf(rand([e,1]));
t = zeros(1,g+1);
t(g+1)=1;
m=[m w];
m(c,:)=t;
m=m
end
i = i-2;
else
G(i-1)=G(i-1)+1;
G=G
g=sum(G);
[y c]=max(G);
c=c
m = gf(m);
p1 = gfprimfd(g,'min',2)
p2= p1(:,1:g);
p= p2';
a = gf([[zeros(1,g-1);eye(g-1,g-1)] p]);
t =gf(ones(g-1,g));
for j = 1:g-1
n = gf(m(c,:)*(a^j));
t(j,:)=n;
end
M = [m(c,:);t];
b = zeros(g,1);
b(g)=1;
x = inv(M)*b;
s = zeros(g,g);
for j = 1:g-1
f= gf(x(j+1)*(a^j));
s=s+f;
```

```
end
s=gf(m*s);
f = gf((x(1,:)*m)+ s);
m=f
if sum(G) == sum(R)
return;
else w = gf(rand([e,1]));
t = zeros(1,g+1);
t(g+1)=1;
m=[m w];
m(c,:)=t;
m=m
end
i = i-2;
end
elseif sum(G) == sum(R)
G=G;
g= sum(G);
return;
else
i = n;
end
else
G(i) = G(i) + 1;
G=G
g=sum(G);
[y c]=max(G);
c=c
m = gf(m);
p1 = gfprimfd(g,'min',2)
p2= p1(:,1:g);
p= p2';
a = gf([[zeros(1,g-1);eye(g-1,g-1)] p]);
t =gf(ones(g-1,g));
for j = 1:g-1
n = gf(m(c,:)*(a^j));
t(j,:)=n;
end
M = [m(c,:);t];
b = zeros(g,1);
b(g)=1;
x = inv(M)*b;
s = zeros(g,g);
for j = 1:g-1
f= gf(x(j+1)*(a^j));
s=s+f;
end
s=gf(m*s);
f = gf((x(1,:)*m)+ s);
m=f
if sum(G) == sum(R)
return;
else w = gf(rand([e,1]));
t = zeros(1,g+1);
t(g+1)=1;
m=[m w];
m(c,:)=t;
m=m
end
i=i-1;
end
G=G;
```

```
g= sum(G);
i = i;
while i == 0 && sum(G) < sum(R)
i = k;end
end
```

This code will generate mutlisequence W and also extension of W which have maximum dimension. This theory can be used to implement Linear Feedback Shift Register (LFSR) configurations.

6. Conclusion

In this paper I have introduced the concept of matrix states which defined the dimension of multisequence and calculated the number of multisequence. The concept of R-extension is given and also calculated the number of multisequence whose R-extension have maximum dimension. At last I have write the MATLAB code for the generation of such multisequences.

7. References

1. S. W. Golomb, Shift Register Sequence. Cambridge University Press, 1967.
2. B. Schneier, Applied Cryptography: protocols, algorithms and source code in C. John Willey and Sons Inc, New York, 1996.
3. W. W. Peterson, Error Correcting Codes. John Willey and Sons Inc, New York, 1961.
4. R. Pickholtz, D. L. Schilling, and L. B. Milstein, “Theory of spread spectrum communications- a tutorial,” IEEE Transactions on Communications, vol. 30, no. 5, pp. 855-884, 1982.
5. D. E. Daykin, “On linear sequence over a finite field,” The American Mathematical Monthly, 1962.
6. W. S. Chou and G. L. Mullen, “Generating linear span over finite fields,” ACTA Mathemation, pp. 183-191, 1992.
7. R. Fitzgerald and J. Yucas, “On generating linear span over gf(p),” Congr. Numer., vol. 69, pp. 55-60, 1989.
8. L’Ecuyer, “Random number for simulation,” Comm. ACM, vol. 33, no. 10, pp. 85-97, 1990.
9. R. Neiderreiter, “The multiple recursive matrix method for pseudorandom vector generation,” Finite Fields and Application, vol. 3, no. 30, 1995.
10. R. Neiderreiter, “Pseudorandom vector generation by multiple recursive matrix method,” Mathematics of Computation, vol. 64, no. 209, pp. 279-294, 1995.
11. B. Preneel, “Introduction,” in Proc. Fast Software Encryption 1994 Workshop(Lecture Notes in Computer Science), vol. 1008, pp. 1-5, Springer- Verlag, 1995.
12. B. Tsaban and U. Vishne, “Efficient Linear feedback shift registers with maximal period,” Finite Fields and Their Applications, vol. 8, no.2, pp. 256-267, 2002.
13. G. Zeng, W. Han, and K. He, “High efficiency feedback shift register: σ-LFSR,” IACR Eprint archive, 2007.
14. M. A. Hassan and A. A. Hassan, “Hankel matrices of finite rank with application to signal processing and polynomials,” Journal of Mathematical Analysis and Applications, vol. 208, pp. 218-242, 1997.
15. R. Lidl and H. Neiderrieter, Introduction to Finite Fields and their Applications. Cambridge University Press, 1986.