Les Cahiers du GERAD ISSN: 0711–2440

$\mathbb{GF}(p^m)$ Valued Pseudorandom Sequences and a Time Invariant Mapping of MPRS$(\mathbb{GF}(p^m), n)$ onto MPRS$(\mathbb{GF}(p), mn)$

Onur Toker
El-Kébir Boukas

G–2003–38

June 2003

$\mathbb{GF}(p^m)$ Valued Pseudorandom Sequences and a Time Invariant Mapping of $\mathrm{MPRS}(\mathbb{GF}(p^m), n)$ onto $\mathrm{MPRS}(\mathbb{GF}(p), mn)$

Onur Toker

Department of Systems Engineering
College of Computer Sciences and Engineering
King Fahd University of Petroleum and Minerals
Dhahran 31261, Saudi Arabia
onur@ccse.kfupm.edu.sa

El-Kébir Boukas

GERAD and Department of Mechanical Engineering
École Polytechnique de Montréal
P.O. Box 6079, Station "Centre-ville"
Montreal, Quebec, Canada, H3C 3A7
El-Kebir.Boukas@polymtl.ca

June, 2003

Les Cahiers du GERAD

G–2003–38

Abstract

Pseudorandom sequences are one of commonly used test signals in system identification [1, 2]. In this report, we first extend the concept of binary pseudorandom sequences to $\mathbb{GF}(q = p^m)$ valued pseudorandom sequences, define maximal length sequences, characterize their generator polynomials, and describe a computationally fast randomized technique for generating such polynomials. The main problem studied in this report is the construction of a time invariant mapping from MPRS$(\mathbb{GF}(p^m), n)$ onto MPRS$(\mathbb{GF}(p), mn)$. It is also shown that this is an m to 1 surjection, and its effect is characterized in frequency domain as well. The problems studied in this report are of more technical nature, and motivated by the problems discussed in [3].

Résumé

Les séquences pseudo-aléatoires sont souvent utilisées dans des signaux tests en identification [1, 2]. Dans ce rapport, nous étendons le concept de séquence pseudo-aléatoire binaire à $\mathbb{GF}(q = p^m)$, définissons la longueur maximal des séquences, caractérisons leurs polynômes générateurs, et décrivons une technique rapide pour la génération de ces polynômes. Le problème étudié dans ce rapport se résume à la construction d'un opérateur de MPRS$(\mathbb{GF}(p^m), n)$ dans MPRS$(\mathbb{GF}(p), mn)$. Certaines propriétés sont aussi démontrées.

Acknowledgments: The author would like to acknowledge the support from KFUPM, and would like to thank Dr. H. E. Emara-Shabaik for various discussions.

1 Introduction

Pseudorandom sequences are one of commonly used test signals in system identification [1, 2]. They can be generated by purely integer operations, more precisely by $\mathbb{GF}(2)$ or $\mathbb{GF}(q)$ type modular or modular-like arithmetic operations. Furthermore, by assigning real values to each element of the corresponding finite field, $\mathbb{GF}(2)$ or $\mathbb{GF}(q)$, one can generate real valued sequences which has statistical properties similar to that of white gaussian noise.

In this report, we study mathematical properties of $\mathbb{GF}(q = p^m)$ valued pseudorandom sequences. As in the binary case, we first study bounds on the periods of $\mathbb{GF}(q)$ valued sequences, then define maximality as being of period $q^n - 1$. We then characterize maximality in terms of certain conditions on the generator polynomial, and define such polynomials as maximal generator. Following this, we show that there are indeed several such maximal generators, derive both general and asymptotic lower bounds on the number of such polynomials. Finally, we describe a computationally fast randomized technique for generating such polynomials.

The main problem studied in this report is the construction of a time invariant mapping from MPRS$(\mathbb{GF}(p^m), n)$ onto MPRS$(\mathbb{GF}(p), mn)$. It is also shown that this is an m to 1 surjection, and its effect is characterized in frequency domain as well. Based on these, one may argue that MPRS$(\mathbb{GF}(p^m), n)$ has a richer structure compared to MPRS$(\mathbb{GF}(p), mn)$. Furthermore, sequences in MPRS$(\mathbb{GF}(p^m), n)$ are takes one of the p^m possible values, whereas the sequences in MPRS$(\mathbb{GF}(p), mn)$ take one of the possible p values, yet they have the same length $p^{mn} - 1$.

The rest of the report is organized as follows. In Section 2, we review some preliminaries related to finite fields, and Galois theory. In Section 3, we discuss extensions of many theorems known for binary pseudorandom sequences to $\mathbb{GF}(q = p^m)$ values pseudorandom sequences. Section 4 is devoted to the study of relationship between MPRS$(\mathbb{GF}(p^m), n)$ and MPRS$(\mathbb{GF}(p), mn)$. Finally, in Section 5, we make some concluding remarks.

2 Preliminaries

In this section, we will introduce our notation, and review some preliminaries related to finite fields, and Galois theory. For detailed discussion, we refer to [4].

The set of integers, and the set of positive integers are denoted by $\mathbb{Z}$, and $\mathbb{Z}^+$ respectively. A positive integer p is called a prime number if its is greater than one, and its positive integer divisors are only 1 and p. If p is a prime number, then the finite field with p elements is denoted by $\mathbb{GF}(p)$, which can be viewed as the set $\{0, 1, 2, \cdots, p-1\}$ with the usual modulo p arithmetic. Given any $m \in \mathbb{Z}^+$, there exist at least one irreducible polynomial, $g(z)$, in $\mathbb{GF}(p)[z]$ of degree m. Indeed, the number of irreducible polynomials of degree m in $\mathbb{GF}(p)[z]$, is equal to

$$N(p, m) = \frac{1}{m} \sum_{k|m} p^k \mu\left(\frac{m}{k}\right),$$

where μ is the Möbius function [4]. Furthermore, we have the following lower and upper bounds,

$$\frac{p^m}{m} \geq N(p,m) \geq \frac{p^m - (p^{m/2+1}-1)/(p-1)}{m},$$

Asymptotically, namely for large p or m values, approximate density of irreducible polynomials is $1/m$. One can view $\mathbb{GF}(q = p^m)$ as the quotient, $\mathbb{GF}(p)[z]/(g(z))$, where $g(z)$ is an irreducible polynomial of degree m, and $(g(z))$ is the ideal generated by this polynomial.

The character of a finite field, F, is defined as the smallest positive integer, c, satisfying $c.1_F = 0$ equation. In this case, we write $\mathrm{char}(F) = c$, and it can be shown that c must be a prime number. The number of elements in a finite field is always equal to $(\mathrm{char}(F))^m$ for some $m \in \mathbb{Z}$. If E and F are two finite fields and $E \supseteq F$, then we say E/F is a field extension. In this case, the number of elements of F must divide the number of elements of E exactly, in particular they must have the same character. The set of all automorphisms of E fixing the elements of F is denoted by $\mathrm{Aut}(E/F)$, and the corresponding Galois group is denoted by $\mathrm{Gal}(E/F)$, which is isomorphic to a cyclic group or order equal to the dimension of E as a vector space over F. In particular, this Galois group is generated by the automorphism

$$\begin{array}{rccc} \psi_0 & : & E & \rightarrow & E \\ & & x & \mapsto & x^q \end{array}$$

where q is the number of elements in F.

The set of all non-zero elements of a finite field, E, is denoted by $E^\times$. As a multiplicative group, $E^\times$ is cyclic, namely there exists an $a \in E$ such that $E^\times =< a >:= \{a^k \ : \ k \in \mathbb{Z}\}$. If E/F is a field extension, then we will also have $E = F(a)$, namely every finite field extension is simple. Finite fields are also said to be perfect, meaning that irreducible polynomials in finite fields do not have repeated roots.

Let F be a finite field, F, then the set of all maximal F valued pseudorandom sequences generated by an n^{th} order polynomial is denoted by $\mathrm{MPRS}(F,n)$. The formal definition of pseudorandom sequence and maximality will be given in the next section.

3 Extension of $\mathbb{GF}(2)$ type results for $\mathbb{GF}(p^m)$

3.1 Maximal Pseudorandom Sequences

Let p be a prime number, m a positive integer, and $q = p^m$. Consider the difference equation

$$u[t] = a_1 u[t-1] + \cdots + a_n u[t-n], \tag{1}$$

where $a_1, \cdots, a_n \in \mathbb{GF}(q)$, with a_n not equal to zero, and with initial conditions $u[0] = u_0, \cdots, u[-n+1] = u_{-n+1}$, where $u_0, \cdots, u_{-n+1} \in \mathbb{GF}(q)$. The vector $[u_0, \cdots, u_{-n+1}]^T$ is called the *initial condition vector*, and the equation (1) is called a *pseudorandom sequence generator equation* over $\mathbb{GF}(q)$, and the polynomial $g(z) = z^n - a_1 z^{n-1} \cdots - a_n \in \mathbb{GF}(q)[z]$ is called the *generator polynomial*.

Theorem 1 *Let L be the period of the solution of the difference equation (1), and $g(z) = z^n - a_1 z^{n-1} \cdots - a_n \in \mathbb{GF}(q)[z]$. Then*

(a) L is less than or equal to $(q^n - 1)$,

(b) If the polynomial $g(z)$ has no repeated roots, then L divides $(q^n - 1)$ exactly,

(c) L always divides $(q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})$ exactly.

Proof. First consider the difference equation (1) in state space format

$$U[t+1] = AU[t], \tag{2}$$

where

$$A = \left[\begin{array}{cccc|c} a_1 & a_2 & \cdots & a_{n-1} & a_n \\ \hline & & I_{n-1} & & 0_{(n-1)\times 1} \end{array}\right]$$

and the state vector, $U[t]$, is equal to $[u[t], u[t-1], \cdots, u[t-n+1]]^T$. If $L \in \mathbb{Z}$, and we have $u[t+L] = u[t]$ for all $t \in \mathbb{Z}$, then $U[t+L] = U[t]$ for all $t \in \mathbb{Z}$. The converse is also true, therefore $u[t]$ and $U[t]$ must have the same period.

The matrix A is non-singular, because $\det(A) = \pm a_n \neq 0$. Furthermore, all roots of $g(z)$ are non-zero because of $a_n \neq 0$. Consider the set inclusion,

$$\left\{A^t U[0] \ : \ t \in \mathbb{Z}\right\} \subseteq \mathbb{GF}(q)^n \setminus \{0\}.$$

The left hand side can have at most $q^n - 1$ elements, therefore there exists $t_1, t_2 \in \mathbb{Z}^+$ satisfying $q^n - 1 \geq t_1 > t_2 \geq 0$ with $U[t_1] = U[t_2]$. Multiplying both sides by A^{t-t_2} results

$$A^{t+t_1-t_2} U[0] = A^t U[0],$$

which implies that the sequence $U[t]$ is periodic with period at most $q^n - 1$. This proves (a).

Every polynomial in $\mathbb{GF}(q)[z]$ of degree n, splits completely in the extension field $\mathbb{GF}(q^n)$. If $g(z)$ has no repeated roots, then by invoking standard results on solution of difference equations,

$$u[t] = c_1 \lambda_1^t + \cdots + c_n \lambda_n^t, \qquad t \in \mathbb{Z},$$

where c_i's and λ_i's are in $\mathbb{GF}(q^n)$. Every non-zero element of $\mathbb{GF}(q^n)$ satisfies the polynomial equation $z^{q^n-1} - 1 = 0$, and λ_i's are all non-zero, therefore $u[t + q^n - 1] = u[t]$ for all $t \in \mathbb{Z}$. The period, L, is indeed the generator of the $\mathbb{Z}$ module

$$\mathbb{M} = \left\{d \in \mathbb{Z} \ : \ u[t+d] = u[t], \ \forall t \in \mathbb{Z}\right\},$$

and $q^n - 1$ being in this module implies that $L | (q^n - 1)$ and hence proves (b).

Whether $g(z)$ has repeated roots or not, the general linear group $\mathrm{GL}(\mathbb{GF}(q), n)$ has finitely many elements. Indeed, by a simple column counting argument, one can show that

$$|\mathrm{GL}(\mathbb{GF}(q), n)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

By Lagrange's theorem on finite groups, the order of the A matrix, L_A, must divide $(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$. Since $A^{t+L_A}=A^t$, we should have $U[t+L_A]=U[t]$, which implies that the period of $U[t]$ must divide L_A. Namely $L|L_A|(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1})$, and hence part (c) is proved. ■

Motivated by this theorem, we will call a sequence $u[t]$ defined by the difference equation (1), as *maximal*, if it has period equal to q^n-1 for some non-zero initial condition vector. Indeed, if for some non-zero initial condition vector, it has period q^n-1, then it will have period equal to q^n-1 for all non-zero initial condition vectors. Because, if $U[0]$ is a non-zero initial condition vector, and $U[t]$ has period q^n-1, then the inclusion

$$\{U[0],\cdots,U[q^n-2]\}\subseteq \mathbb{GF}(q)^n\setminus\{0\},$$

must be an equality. The right hand side has q^n-1 elements and this is clear. On the left hand side, if we have $U[i]=U[j]$ with $0\le i<j\le q^n-2$, then multiplying both sides by A^{t-i}, we will have $U[t]=U[t+j-i]$, which contradicts with $U[t]$ having period q^n-1. Therefore, the left hand side must also have q^n-1 elements, and inclusion must be indeed an equality. Therefore, all non-zero vectors in $\mathbb{GF}(q)^n\setminus\{0\}$ can be generated from this fixed non-zero initial condition vector, $U[0]$, by repeated multiplications with the matrix A. This means that, changing the initial condition is basically equivalent to a time shift, and hence does not change the period.

Corollary 1 *If the sequence $u[t]$ defined by the difference equation (1), has period equal to q^n-1 for some non-zero initial condition vector, then it has the same period for all non-zero initial condition vectors.*

3.2 Maximal Generator Polynomials

Let $u[t]$ be a sequence defined by the difference equation (1). Then the polynomial $g(z)=z^n-a_1z^{n-1}\cdots-a_n\in\mathbb{GF}(q)[z]$ is called its *generator* polynomial. Furthermore, if $u[t]$ is maximal, then $g(z)$ is called a *maximal generator* polynomial.

The following theorem characterizes maximal generator polynomials.

Theorem 2 *The polynomial $g(z)=z^n-a_1z^{n-1}\cdots-a_n$ is a maximal generator polynomial iff*

(I) *It is irreducible in $\mathbb{GF}(q)[z]$, and*

(II) *It is a factor of $z^{q^n-1}-1$, but is not a factor of z^r-1 for $r<q^n-1$.*

Proof. Necessity of (I): If $g(z)$ is reducible, then let $g_1(z)$ be one of its irreducible factors. Let n_1 be the degree of $g_1(z)$, then $n_1<n$. Let $\alpha\in\mathbb{GF}(q^{n_1})$ be a root of $g_1(z)$, possibly not in $\mathbb{GF}(q^n)$. Consider the sequence

$$u[t]=\alpha^t+\alpha^{qt}+\alpha^{q^2t}+\cdots+\alpha^{q^{n_1-1}t}.$$

First of all, $u[t]$ is fixed by all elements of $Aut(\mathbb{GF}(q^{n_1})/\mathbb{GF}(q))$, and hence must be in $\mathbb{GF}(q)$. It has period at most $q^{n_1}-1$ as $\alpha^{q^{n_1}-1}=1$. Finally, $u[t]$ is a non-zero sequence, because

$\alpha, \alpha^q, \alpha^{q^2}, \cdots \alpha^{q^{n_1-1}}$ are the complete set of roots of $g_1(z)$, and the list has no repetitions. By using the standard results from the theory of difference equations, it follows that the above $u[t]$ is generated by the difference equation (1) with some non-zero initial condition vector. Having period at most $q^{n_1} - 1$ contradicts with the maximality of $g(z)$, and this contradiction proves the necessity of irreducibility.

Necessity of (II): Because of the necessity of (I), we can assume that $g(z)$ is irreducible in $\mathbb{GF}(q)[z]$, and hence, all of its roots, $g_1, \cdots, g_n$, are distinct. Let $[u_0, \cdots, u_{-n+1}]^{\mathrm{T}}$ be a non-zero initial condition vector, then

$$u[t] = \sum_{i=1}^{n} C_i g_i^t,$$

for some constants C_i's in $\mathbb{GF}(q^n)$. The polynomial $g(z)$ cannot be a factor of $z^r - 1$ for $r < q^n - 1$, otherwise we will have $g_i^r = 1$, which will imply that $u[t]$ has period at most r. The polynomial $g(z)$ is a factor of $z^{q^n-1} - 1$, because any irreducible polynomial of degree n, divides of $z^{q^n-1} - 1$, if it is non-zero at zero. Since by definition $g(0) \neq 0$, the condition (II) is also necessary.

Sufficiency of (I) and (II):Let $g(z)$ be a polynomial satisfying (I) and (II). Furthermore, let $[u_0, \cdots, u_{-n+1}]^{\mathrm{T}}$ be a non-zero initial condition vector. Because of irreducibility, $g(z)$ has distinct roots $g_1, \cdots, g_n \in \mathbb{GF}(q^n)$, and

$$u[t] = \sum_{i=1}^{n} C_i g_i^t,$$

for some constants C_i's in $\mathbb{GF}(p^n)$. Since $g(z)$ divides $z^{q^n-1} - 1$, we have

$$g_i^{q^n-1} = 1,$$

and hence

$$u[t + q^n - 1] = u[t].$$

Therefore, the period of $u[t]$ is at most $q^n - 1$. The period of $u[t]$ cannot be smaller than $q^n - 1$, because an identity of the form

$$u[t + r] = u[t],$$

for some $r > 0$ would imply that

$$\sum_{i=1}^{n} (C_i g_i^r) g_i^t = \sum_{i=1}^{n} C_i g_i^t,$$

for all t. Consider this equality for $t = 0, \cdots, n-1$. Since g_i's are distinct, the Vandermode matrix associated with g_i's is non-singular, and hence

$$C_i g_i^r = C_i,$$

for all $i = 1, \cdots, n$. Since by definition a pseudorandom sequence is non-zero, at least one C_i must be non-zero, and hence there exists an $i \in \{1, \cdots, n\}$ such that $g_i^r = 1$. This means that the irreducible polynomial $g(z)$ has a common root with the polynomial $z^r - 1$, and hence divides it. This contradiction shows that, $u[t]$ cannot have a period smaller than $q^n - 1$. ■

The condition (II) in Theorem 2 can be checked in a simpler way. Because, if g_0 is a root of the irreducible polynomial $g(z)$, then roots of $g(z)$ will be equal to $g_0, g_0^q, \cdots, g_0^{q^{n-1}}$. The smallest r such that $g(z)|z^r - 1$ is equal to the multiplicative order of g_0, which is a factor of $q^n - 1$. Therefore, to check the condition (II), it is enough to consider only divisors of $q^n - 1$ as possible r values. This is expressed formally in the following corollary.

Corollary 2 *The polynomial $g(z) = z^n - a_1 z^{n-1} \cdots - a_n$ is a maximal generator polynomial iff*

(I) *It is irreducible in $\mathbb{GF}(q)[z]$, and*

(II) *It is a factor of $z^{q^n-1} - 1$,*

(III) *For any $r < q^n - 1$ and $r|q^n - 1$, the polynomial $g(z) \not| z^r - 1$.*

An alternative characterization which we will use later is the following:

Theorem 3 *The polynomial $g(z) = z^n - a_1 z^{n-1} \cdots - a_n$ is a maximal generator polynomial iff it is equal to $(z - g_0)(z - g_0^q)(z - g_0^{q^2}) \cdots (z - g_0^{q^{n-1}})$ for some generator g_0 of the multiplicative group $\mathbb{GF}(q^n)^\times$.*

Proof. If g_0 is a generator of $\mathbb{GF}(q^n)^\times$, then its minimal polynomial over $\mathbb{GF}(q)$ will have degree n. Therefore, $(z-g_0)(z-g_0^q)(z-g_0^{q^2}) \cdots (z-g_0^{q^{n-1}})$ must be the minimal polynomial and hence is irreducible. It is clear that the minimal polynomial divides $z^{q^n-1} - 1$, because $g_0^{q^i(q^n-1)} = 1$ for $i = 0, \cdots, n-1$. However, the same minimal polynomial does not divide $z^r - 1$ for any $r < q^n - 1$. This is because the multiplicative order of g_0 is exactly $q^n - 1$ and not smaller. Therefore, the minimal polynomial is indeed a maximal generator polynomial by Theorem 2.

If $g(z)$ is a maximal generator polynomial, then by Theorem 2 it must be irreducible. Let g_0 be one of its roots, since $g(z)$ does not divide $z^r - 1$ for any $r < q^n - 1$, g_0 must have order exactly equal to $q^n - 1$. Namely g_0 must be a generator of the multiplicative group $\mathbb{GF}(q^n)^\times$. Since $g(z)$ is irreducible it will be equal to $(z-g_0)(z-g_0^q)(z-g_0^{q^2}) \cdots (z-g_0^{q^{n-1}})$, where g_0 being a generator of $\mathbb{GF}(q^n)^\times$. ■

3.3 Distributional Properties of Maximal Pseudorandom Sequences

The following theorem gives some information about distribution of values in maximal pseudorandom sequences.

Theorem 4 *Let $u[t]$ be a maximal pseudorandom sequence over $\mathbb{GF}(q)$. Then the state vector $U[t]$ takes all possible non-zero vectors in $\mathbb{GF}(q)^n$. Furthermore, in a period of $u[t]$,*

it takes each value in $\mathbb{GF}(q) \setminus \{0\}$ *exactly* q^{n-1} *times, and the value* 0 *exactly* $q^{n-1}-1$ *times.*

Proof. The first statement is already proved. Consider the non-zero vectors in $\mathbb{GF}(q^m)$. When we count their first coordinates, clearly every value except 0 will appear exactly q^{n-1} times, and 0 will appear exactly $q^{n-1}-1$ times. ■

3.4 How to find a Maximal Generator Polynomial ?

In this section, we will discuss a randomized method to find a maximal generator. First, we will derive general and asymptotic lower bounds for the number of maximal generators in $\mathbb{GF}(q)[z]$. Then, we will present a computational quite efficient procedure to check whether a generator polynomial is a maximal one.

The multiplicative group, $\mathbb{GF}(q^n)^\times$, has q^n-1 elements and hence has $\phi(q^n-1)$ generators. By Theorem 3, it is clear that all generator polynomials must be of the form

$$(z-g_0)(z-g_0^q)(z-g_0^{q^2})\cdots(z-g_0^{q^{n-1}}).$$

Therefore, there are total $\phi(q^n-1)/n$ such polynomials.

A positive integer x can have at most $\log_2(x)$ distinct prime factors. Therefore,

$$\phi(x) \geq \frac{1}{2}\left(\frac{2}{3}\right)^{\log_2(x)-1} x \geq 0.75x^{0.415}.$$

Therefore, the number of maximal generator polynomials will be at least $0.75(q^n-1)^{0.415}/n$, namely the number grows at least exponentially by n. Clearly, the number of such polynomials is bounded by q^n-1, therefore the number of maximal generator polynomials is bounded from below and above by exponentially growing functions of n.

By using the asymptotic growth results of the Euler function [5], it follows that

$$\frac{\phi(q^n-1)}{n(q^n-1)} \geq \frac{1}{2}\frac{q^n-1}{\log(n\log(q))n(q^n-1)} = \frac{1}{2n(\log(n)+\log(\log(q)))}, \qquad q \text{ or } n \to \infty.$$

Corollary 3 *If* q *or* n *are large enough, than in* $2n(\log(n)+\log(\log(q))\log(1/\epsilon)$ *randomly generated non-zero polynomials in* $\mathbb{GF}(q)[z]$*, with probability* $1-\epsilon$*, there will be at least one maximal generator polynomial. In particular, in* $461n(\log(n)+\log(\log(q))$ *randomly generated non-zero polynomials in* $\mathbb{GF}(q)[z]$*, with probability* $1-10^{-100}$*, there will be at least one maximal generator polynomial.*

Based on the previous corollary, one can try to generate several random n^{th} order polynomials in $\mathbb{GF}(q)[z]$ and check whether they are maximal or not. However, for this to be a computational fast method, one needs a quick maximality test. The following Theorem answers this question.

Theorem 5 *A sequence* $u[t]$ *is maximal iff the corresponding A matrix multiplicative has order* q^n-1*.*

Proof. If $u[t]$ is maximal, then

$$A^{q^n-1}A^tU[0] = A^tU[0].$$

By using the distributional properties, it follows that, as t varies over $\mathbb{Z}$, $A^tU[0]$ takes all possible values in $GF(q)^m \setminus \{0\}$. Therefore, $A^{q^n-1} = I$. If $A^d = I$, then $u[t+d] = u[t]$ for all $t \in \mathbb{Z}$, and hence $d \geq q^n - 1$. These results imply that the order of A must be $q^n - 1$.

If the A matrix has multiplicative order $q^n - 1$, then it satisfies the polynomial equation $z^{q^n-1} - 1 = 0$. Note that this polynomial has no repeated roots, therefore the minimal polynomial of A has no repeated roots. Consider the Jordan decomposition of A. At least one eigenvalue, λ, must have multiplicative order $q^n - 1$. Furthermore, all other roots of the minimal polynomial must be of the form λ^{q^k}, for some $k \in \mathbb{Z}^+$, and hence must be of multiplicative order $q^n - 1$. Therefore, all eigenvalues of A has order $q^n - 1$. This strong result implies that

$$\det(A^d - I) \neq 0, \quad 0 < d < q^n - 1,$$

and hence $U[t+d] \neq U[t]$, if $0 < d < q^n - 1$, no matter which non-zero initial condition vector is chosen. ■

To check whether a given matrix over $\mathbb{GF}(q)$ has multiplicative order $q^n - 1$, one can find all prime factors, $p_1, \cdots, p_f$, of $q^n - 1$, and check whether

$$A^{(q^n-1)/p_i} \neq I, \qquad i = 1, \cdots, f.$$

Furthermore, the matrix exponentiation can be computed in $O(n\log(q))$ matrix squaring and multiplication operations, by using the binary representation of the exponent $(q^n - 1)/p_i$. For example,

$$A^{37} = A^{(100101)_2} = A^{2^5}A^{2^2}A,$$

so by 5 matrix squaring and 2 matrix multiplication operations, result can be computed, see [6] for details.

4 Mapping $\mathrm{MPRS}(\mathbb{GF}(p^m), n)$ onto $\mathrm{MPRS}(\mathbb{GF}(p), mn)$

In this section, we will construct a time invariant mapping from $\mathrm{MPRS}(\mathbb{GF}(p^m), n)$ onto $\mathrm{MPRS}(\mathbb{GF}(p), mn)$. We will prove that this is an m to 1 surjection, and describe its action both in time and frequency domains.

We start with a structural lemma.

Lemma 1 *Let α be a fixed generator of the multiplicative group, $\mathbb{GF}(q^n)^\times$. Then all maximal pseudorandom sequences must be of the form $u[t] = u_0[ct + d]$, where*

$$u_0[t] := \alpha^t + \alpha^{qt} + \alpha^{q^2t} + \cdots + \alpha^{q^{n-1}t},$$

$c, d \in \mathbb{Z}$ and c is relatively prime to $q^n - 1$.

Proof. If $u[t] = u_0[ct + d]$, then

$$u[t] := \alpha^d \alpha^c t + \alpha^{qd} \alpha^{qct} + \alpha^{q^2 d} \alpha^{q^2 ct} + \cdots + \alpha^{q^{n-1} d} \alpha^{q^{n-1} ct}.$$

Note that, α^c is also a generator of the multiplicative group, $\mathbb{GF}(q^n)^\times$. Furthermore, $u[t]$ is non-zero (by a simple Vandermode matrix type argument), is in $\mathbb{GF}(q)$, and is generated by the polynomial

$$(z - \alpha^c)(z - \alpha^{qc})(z - \alpha^{q^2 c}) \cdots (z - \alpha^{q^{n-1} c}).$$

Therefore, according to Theorem 3, $u[t]$ is a maximal pseudorandom sequence.

Now consider a maximal pseudorandom sequence, $u[t]$, and let $g(z)$ be its generator polynomial. Let g_0 be a root of $g(z)$. Then by Theorem 3, g_0 generates $\mathbb{GF}(q^n)^\times$, and the set of all roots of $g(z)$ are $g_0, g_0^q, \cdots, g_0^{q^{n-1}}$. Therefore,

$$u[t] = \sum_{k=0}^{n-1} C_k g_0^{q^k t},$$

for some C_k's in $\mathbb{GF}(q^n)$. Since $u[t] \in \mathbb{GF}(q)$, it is fixed under $\psi_0 : x \mapsto x^q$, i.e.

$$\sum_{k=0}^{n-1} \psi_0(C_k) g_0^{q^{k+1} t} = \sum_{k=0}^{n-1} C_k g_0^{p^k t}.$$

By using the nonsingularity of the Vandermode matrix, it easily follows that $\psi_0(C_k) = C_{(k+1) \bmod n}$, and therefore, $C_1 = C_0^q$, $C_2 = C_1^q = C_0^{q^2}, \cdots, C_{n-1} = C_0^{q^{n-1}}$.

Since $u[t]$ is non-zero, C_0 must also be non-zero. It is given that $\mathbb{GF}(q^n)^\times =< \alpha >$ which implies that $C_0 = \alpha^d$ for some integer d. Similarly, g_0 must be equal to α^c for some $c \in \mathbb{Z}$, and c must be relatively prime to $q^n - 1$. Therefore,

$$u[t] = \sum_{k=0}^{n-1} \alpha^{q^k d} \alpha^{c q^k t} = \sum_{k=0}^{n-1} \alpha^{q^k (ct+d)} = u_0[ct + d].$$

■

Now, we are ready to prove the main theorem.

Theorem 6 *There is an m to 1 surjection from* $\mathrm{MPRS}(\mathbb{GF}(p^m), n)$ *to* $\mathrm{MPRS}(\mathbb{GF}(p), mn)$ *defined by the transformation:*

$$\begin{array}{rccc} T & : & \mathrm{MPRS}(\mathbb{GF}(p^m), n) & \to & \mathrm{MPRS}(\mathbb{GF}(p), mn) \\ & & u[t] & \mapsto & \sum_{i=0}^{m-1} u[p^i t] \end{array}$$

In the frequency domain, T can be described by its effect on maximal generator polynomials:

$$\begin{array}{rccc} T_f & : & \mathbb{GF}(p^m)[z] & \to & \mathbb{GF}(p)[z] \\ & & g(z) & \mapsto & \prod_{i=0}^{m-1} \psi_0^i g(z) \end{array}$$

where ψ_0 is the generator of $\mathrm{Aut}(\mathbb{GF}(q^n)/\mathbb{GF}(q))$ *defined by $\psi_0(x) = x^q$.*

Proof. Now, we have a clear description of maximal pseudorandom sequences. At this point it is natural to ask whether

$$\sum_{k=0}^{n-1} \alpha^{q^k(c_1 t+d_1)} = \sum_{k=0}^{n-1} \alpha^{q^k(c_2 t+d_2)}, \qquad \forall t \in \mathbb{Z},$$

if and only if $c_1 = c_2 q^i \pmod{q^n-1}$ and $d_1 = d_2 q^i \pmod{q^n-1}$. Sufficiency part is clear. Now if we have the above equality, then by using a Vandermode matrix type argument, we can conclude that on both sides we should the same exponential functions, i.e.

$$\left\{\alpha^{q^k c_1} \ : \ k \in \mathbb{Z}\right\} = \left\{\alpha^{q^k c_2} \ : \ k \in \mathbb{Z}\right\}.$$

This implies that $\alpha^{c_1} = \alpha^{q^i c_2}$ for some $i \in \mathbb{Z}^+$, namely $c_1 = c_2 q^i \pmod{q^n-1}$. By simple substitution and change of indices, we can get

$$\sum_{k=0}^{n-1} \alpha^{q^k(c_1 t+d_1)} = \sum_{k=0}^{n-1} \alpha^{q^k(c_1 t+q^i d_2)}, \qquad \forall t \in \mathbb{Z},$$

This implies that $\alpha^{d_1} = \alpha^{q^i d_2}$, i.e. $d_1 = d_2 q^i \pmod{q^n-1}$.

Let $u_1[t] \in \mathrm{MPRS}(\mathbb{GF}(p^m), n)$ be equal to

$$u_1[t] = \sum_{k=0}^{n-1} \alpha^{q^k(c_1 t+d_1)},$$

and $u_2[t] \in \mathrm{MPRS}(\mathbb{GF}(p), mn)$ be equal to

$$u_2[t] = \sum_{k=0}^{mn-1} \alpha^{p^k(c_1 t+d_1)}.$$

Clearly, $T(u_1) = u_2$. The structure lemma, and what is proved in the previous paragraph, it is clear that T is a time invariant surjection, and is m to 1. Finally, by Theorem 3, the action at the generator polynomial level will be given by T_f. ■

Now the following corollary is immediate.

Corollary 4 *There are basically $\phi(q^n-1)/n$ different $\mathbb{GF}(q)$ valued maximal pseudorandom sequences, when shifted versions of the same sequence are not counted as "different" sequences. If all of them are counted as "different", then there are total $q^n\phi(q^n-1)/n$ different $\mathbb{GF}(q)$ valued maximal pseudorandom sequences.*

5 Conclusion

In this report, we basically extended the concept of binary pseudorandom sequences to $\mathbb{GF}(q = p^m)$ valued pseudorandom sequences, defined maximal length sequences, characterizes their generator polynomials, and described a computationally fast randomized technique for generating such polynomials. The main goal was the construction of a time invariant mapping from MPRS$(\mathbb{GF}(p^m), n)$ onto MPRS$(\mathbb{GF}(p), mn)$. It is shown that this is an m to 1 surjection, and its effect is characterized both in time and frequency domains.

References

[1] L. Ljung, *System Identification: Theory for the user*, Prentica-Hall, New Jersey, 1999.

[2] T. Soderstrom and P. G. Stoica, *System Indetification*, Prentice Hall International, Englewood Cliffs, NJ, 1989.

[3] O. Toker and H. E. Emara-Shabaik, "Pseudorandom multilevel sequences: Spectral properties and identification of hammerstein systems," submitted for publication, 2002.

[4] N. Jacobson, *Basic Algebra*, Vols. I, and II, W.H. Freeman, San Francisco, 1985, 1989.

[5] T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, London, 1995.

[6] D. Knuth, *Seminumerical Algorithms, The Art of Computer Programming*, Vol. 2, 3rd Edition, Addison Wesley, 1997.