PRIMITIVE TRANSFORMATION SHIFT REGISTERS AND PRIMITIVE ELEMENTS OVER FINITE FIELDS

AMBRISH AWASTHI

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
AUGUST 2018

PRIMITIVE TRANSFORMATION SHIFT REGISTERS AND PRIMITIVE ELEMENTS OVER FINITE FIELDS

by

AMBRISH AWASTHI

Department of Mathematics

Submitted

in fulfillment of the requirements of the degree of Doctor of Philosophy

to the

Indian Institute of Technology Delhi
August 2018

Dedicated to my loving parents, my wife Rashmi and my two litte angels Anika and Shivansh

Certificate

This is to certify that the thesis titled **Primitive transformation shift registers and primitive elements over finite fields** submitted by **Mr. Ambrish Awasthi** to the Indian Institute of Technology Delhi, for the award of the degree of **Doctor of Philosophy**, is a record of the original bona fide research work carried out by him under my supervision and guidance. The thesis has reached the standards fulfilling the requirements of the regulations relating to the degree.

The results contained in this thesis have not been submitted in part or full to any other university or institute for the award of any degree or diploma.

Prof. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
Hauz Khas
New Delhi 110 016

Acknowledgements

Any achievement, no matter how big or small, is not just an individual endeavour but the fructification of the efforts of a lot of people. This thesis is no exception. I hereby acknowledge the people whose involvement, direct or indirect, helped in this thesis seeing the light of the day.

First and foremost, I would like to express my deep sense of respect and gratitude to my thesis supervisor Prof. R. K. Sharma, who has been a constant source of inspiration during the course of this thesis work. He has always been patient and kept encouraging me to work in a better way. Without his help and support, I might have not been able to write this thesis.

I would like to give my special thanks to my SRC (Student Research Committee) members Prof K. Sreenadh, Prof. Ritumoni Sarma, and Prof S. K. Gupta for their valuable time and suggestions. I would also like to thank all the faculty members and staff of Department of Mathematics, IIT Delhi for their co-operation and support.

I wish to express my sincere thanks to the Director, Mrs. Anu Khosla, Scientific Analysis Group (SAG), DRDO for their continuous encouragement and suggestions.

I would like to express my sincere respect and heartiest gratitude to my current and former group heads Dr. Sucheta Chakrabarti and Dr. N. Rajesh Pillai as well as my division head Mrs. Pratibha Yadav for their guidance and encouragement.

I am also thankful to Dr. Sartaj Ul Hasan and my co-author Miss Anju Gupta for their valuable suggestions and comments in improving the quality of my research papers.

I would like to thank all my colleagues at DRDO and especially to Mrs. Neelam Verma (Associate Director), Dr. Indiver Gupta, Mr. Manoj Kumar, Dr Yogesh Lathar, Mr Harish Sahu, Dr Sharwan

Kumar Tiwari and Dr Nupur Gupta for their support and encouragement.

I also thank all my friends at IIT Delhi and especially to Vishal, Yogesh Kumar, Harish, Alok, Ankita, Rohit, Chirag, Yogesh and Rahul for their support.

It would be unfair, if I leave my revered parents as they devoted their whole youth for my well being and progress. They have instilled in me the value of hard work. I am also thankful to my brothers and sisters who have provided their helping hands in each and every walk of my life.

Last, but not the least is the dedicated sacrifice of my loving wife, Rashmi Awasthi who calmly and patiently did everything possible on her part, leaving aside all her comforts and ease of life, just to support me through my research work. I draw a superb and delightful stream of strength from my lovely daughter, Anika and son Shivansh, who have always made the atmosphere at my home very lively and entertaining.

Most importantly, I thank almighty God for his blessings.

New Delhi *Ambrish Awasthi*

Abstract

Linear Feedback Shift Registers (LFSRs) are linear homogeneous recurrence relations used for generating pseudorandom sequences over finite fields for cryptographic applications. Particularly useful are sequences with maximum period which are generated by systems called primitive LFSRs. The present thesis studies vector sequences over finite fields called Transformation Shift Registers (TSRs) which are generalisation of LFSRs. It further extends the theory of TSRs over Galois rings wherein they are termed as Transformation Shift Registers over Galois rings (TSRGs). The TSRs of order n are systems which generate m bit vector sequences over $\mathbb{F}_{q^m}$ compared to LFSRs which output one bit per clock cycle. For cryptographic purpose we are mainly interested in primitive TSRs which generate vector sequences of maximum period. Primitive TSRs answer the challenge proposed by Bart Preneel [27], 2002 to the cryptographic community to come up with new designs which are both fast and secure and use the parallelism inherent in the word operations of modern day processors. Though TSRs were first introduced by Tsaban and Vishne [30] and subsequently studied by Ram [28] and Cohen et. al [7], however a lot of problems related to enumeration, construction, existence and cardinality of primitive TSRs remain unexplored. This has motivated us to take up further study in this area. In our thesis we develop the theory of primitive TSRs

and study questions related to their cardinality and existence. We prove the existence of primitive TSRs of order two over finite fields of characteristic 2 and derive an equivalence between primitive TSRs and primitive polynomials of special kind. Moreover we propose a conjecture regarding the existence of these special type of primitive polynomials. Further, a search algorithm for generating primitive TSRs of odd order over any finite field and in particular of order two over finite fields of characteristic 2 has also been proposed.

Besides studying primitive TSRs over finite fields we have extended the study of similar problems related to TSRs over Galois rings. A Galois ring is a finite commutative ring whose set of non units form a maximal ideal. Considering $R = GR(p^{rm}, p^r)$ to be a Galois ring where p is a prime number, p^r is its characteristic and p^{rm} is its cardinality. We define transformation shift registers (TSRGs) over Galois rings R and focus on TSRGs of maximal period. We obtain useful characterizations for such maximal period TSRGs as well as address the problem of their enumeration.

Apart from studying TSRs, the thesis takes up the problem of existence of primitive pairs over $\mathbb{F}_{2^k}$. A primitive pair is a pair (α, β) of primitive elements α, β where α is a primitive element in $\mathbb{F}_{2^k}$ and $\beta = f(\alpha)$ where $f(X)$ is some rational function over $\mathbb{F}_{2^k}$. Firstly note that given $\alpha, f(\alpha)$ need not be a primitive element for example take $\alpha = 1$ and $f(X) = X + 1$ over $\mathbb{F}_2$. However taking $f(X) = \frac{1}{X}$, we see that $(\alpha, f(\alpha) = \frac{1}{\alpha})$ is always a primitive pair in $\mathbb{F}_{2^k}$, whenever α is primitive. In general the problem of existence of primitive pairs in $\mathbb{F}_{2^k}$ is a challenging one. Anju and Sharma [1] studied the problem of existence of primitive pairs $(\alpha, f(\alpha))$ over $q = p^k$ for some prime $p \neq 3$ where $f(X) = X^2 + X + 1$ [2]. They Further generalised their result by taking $f(X) = \frac{aX^2+bX+c}{dX+e}$ and studying the existence problem of primitive pairs $(\alpha, f(\alpha) = \frac{a\alpha^2+b\alpha+c}{d\alpha+e}) \in \mathbb{F}_{2^k}$. In the present work we give a sufficient condition for the existence of a primitive element α in $\mathbb{F}_{2^k}$ such that $f(\alpha)$ is also primitive in $\mathbb{F}_{2^k}$, where $f(X) = \frac{aX^2+bX+c}{dX^2+eX+f} \in \mathbb{F}_{2^k}(X)$. Subsequently, using this condition we derive the values of k for which $\mathbb{F}_{2^k}$ contains primitive pairs of the form $(\alpha, f(\alpha))$

सारांश

रैखिक पुनर्निवेशन परिवर्तन रजिस्टर (एल0एफ0एस0आर0) सीमित क्षेत्रों (फाइनाइट फील्ड) में क्रिप्टोग्राफिक अनुप्रयोगों हेतु छद्म यदृच्छया सीक्वन्स को उत्पन्न करने के लिए रैखिक समांग आवर्ती सम्बन्ध होते है। उच्चिष्ठ समयान्तराल वाली सीक्वन्स जिन्हे मूल रैखिक पुनर्निवेशन परिवर्तन रजिस्टर (प्रिमिटिव एल0एफ0एस0आर0) नाम की प्रणालियों द्वारा उत्पन्न किया जाता है, विशेषतया उपयोगी होती है। प्रस्तुत शोध सीमित क्षेत्रों (फाइनाइट फील्ड्स) जिन्हें टी0एस0आर0 कहा जाता है, और जो टी0एस0आर0जी0 का सामान्यीकृत रूप है में सदिश सीक्वन्स का अध्ययन है। यह शोध आगे गैलोइस रिंग में टी0एस0आर0 के सिद्धान्त जहाँ उन्हे टी0एस0आर0जी0 के नाम से जाना जाता है तक विस्तारित होता है। n-क्रम के टी0एस0आर0 ऐसी प्रणालियाँ होते है जो प्रति क्लॉक–साइकिल एक बिट उत्पन्न करने वाले एल0एफ0एस0आर0 की तुलना में F_{q^m} में m बिट सदिश सीक्वन्स उत्पन्न करते है। मुख्यतया क्रिप्टोग्राफिक उद्देश्य हेतु, हम प्रिमिटिव टी0एस0आर0 जो उच्चिष्ठ समयान्तराल की सदिश सीक्वन्स उत्पन्न करती है, में रूचि रखते है। प्रिमिटिव टी0एस0आर0 बार्ट प्रेनील [4] 2002 द्वारा क्रिप्टोग्राफिक समुदाय के सामने आधुनिक युग के प्रोसेसर में वर्ड ऑपरेशन में अन्तर्निहित समानान्तरवाद के प्रयोग तथा शीघ्रगामी और सुरक्षित डिजाइन के खोजने की चुनौती का उत्तर है। यद्यपि टी0एफ0आर0 का प्रथमतः साबाल और विश्ने [6] द्वारा परिचय कराया गया था और तत्पश्चात् राम [5] और कोहेन आदि [3] द्वारा अध्ययन किया गया था, फिर भी गणना, निर्माण, अस्तित्व और गणनीयता से सम्बन्धित प्रिमिटिव टी0एफ0आर0 की अनेक समस्याओं की खोजबीन नहीं हो सकी। इस स्थिति ने मुझे इस क्षेत्र में आगे के अध्ययन हेतु प्रेरित किया। अपने शोध में हमने प्रिमिटिव टी0एफ0आर0 के सिद्धान्त का विकास किया है और उनकी गणनीयता और अस्तित्व से सम्बन्धित प्रश्नों का अध्यय किया है। हमने दो विशिष्टताओं वाले सीमित फील्ड्स में दो क्रम वाले प्रिमिटिव टी0एस0आर0 के अस्तित्व को सिद्ध किया है तथा टी0एस0आर0 और विशेष प्रकार के प्रिमिटिव बहुपद के मध्य एक समानता का निगमन किया है।इसके अतिरिक्त हम इन विशेष प्रकार के प्रिमिटिव बहुपदों के सम्बन्ध में एक अनुमान को प्रस्तुत करते है। आगे किसी सीमित फील्ड में विषम क्रम वाले प्रिमिटिव टी0एस0आर0 उत्पन्न करने के लिए विशेषतया दो विशिष्टताओं वाले सीमित फील्ड में दो क्रम वाले टी0एस0आर0 के लिए एक शोध अल्गॉरिथम प्रस्तुत की है। सीमित फील्ड्स में प्रिमिटिव टी0एस0आर0 के अध्ययन के अतिरिक्त हमने अपने अध्ययन को गैलवा रिंग्स में टी0एस0आर0 से सम्बन्धित समान प्रकार की समस्याओं तक विस्तारित किया है। एक गैलवा रिंग एक सीमित संचयीरिंग होती है, जिनके नॉन यूनिट्स का समुच्चय एक उच्चिष्ठ आदर्श का निर्माण करता है। यह मानते हुए कि $R = GR\,(p^{rm}, p^r)$ एक गैलवा रिंग हो, जहाँ p एक अभाज्य संख्या है, p^r एक विशिष्टता है और p^{rm} इसकी गणनीयता है। हम गैलवा रिंग R में टी0एस0आर0जी0 को परिभाषित करते है और उच्चिष्ठ समयान्तराल के टी0एस0आर0जी0 पर ध्यान क्रेन्द्रित करते हैं। हम ऐसे उच्चिष्ठ समयान्तराल के टी0एस0आर0जी0 के उपयोगी विशेषताओं को प्राप्त करते है साथ ही साथ उनकी गणना की समस्याओं को हल करते हैं।

टी0एस0आर0 के अध्ययन के अतिरिक्त यह शोध F_{2^k} मे प्रिमिटिव युग्मों के अस्तित्व की समस्या को भी उठाती है।एक प्रिमिटिव युग्म प्रिमिटिव अवयव α, β का युग्म है, जहाँ α F_{2^k} में एक प्रिमिटिव अवयव है और $\beta = f(\alpha)$ जहाँ $f(X)$, F_{2^k} में कोई परिमेय फलन है। प्रथमतः ध्यान देने योग्य है कि किसी दिये गये α के लिए $f(\alpha)$ का प्रिमिटिव अवयव होना आवश्यक नहीं है। उदाहरण के लिए F_2 में $\alpha = 1$ और $F(X) = \frac{1}{X}$ लेने पर, हम देखते हैं कि

$\left(\alpha, f(\alpha) = \frac{1}{\alpha}\right), F_{2^k}$ में सदैव एक प्रिमिटिव युग्म है, जब α प्रिमिटिव हो। सामान्य रूप से F_{2^k} में प्रिमिटिव युग्मों के अस्तित्व की समस्या चुनौती पूर्ण है। अंजू और शर्मा [1] ने किसी अभाज्य $P \neq 3$ के लिए जहाँ $f(X) = X^2 + X + 1$[2] हो, $q = p^k$ में प्रिमिटिव युग्म $\left(\alpha, f(\alpha)\right)$ के अस्तित्व की समस्या का अध्ययन किया था। उन्होंने आगे अपने निष्कर्ष को $f(X) = \frac{aX^2+bX+c}{dX+e}$ लेकर और प्रिमिटिव युग्म $\left(\alpha, f(\alpha) = \frac{a\alpha^2+b\alpha+c}{d\alpha+e}\right) \epsilon F_{2^k}$ का अध्ययन करते हुए सामान्यीकृत किया था। प्रस्तुत कार्य मे हम F_{2^k} में प्रिमिटिव अवयव α के अस्तित्व के लिए पर्याप्त दशाओं को देते हैं। जैसे कि $f(\alpha)$ भी F_{2^k} में प्रिमिटिव है जहाँ $f(X) = \frac{aX^2+bX+C}{dX^2+eX+f} \epsilon F_{2^k}(X)$ बाद में, इस शर्त का प्रयोग करते हुए हम k के मानों की गणना करते हैं जिनके लिए $\left(\alpha, f(\alpha)\right)$ रूप के प्रिमिटिव युग्म F_{2^k} में निहित होते हैं।

सन्दर्भ सूची–

[1] अंजू और आर0के0 शर्मा– एग्जिस्टन्स आफ सम स्पेशल प्रिमिटिव नार्मल एलिमन्ट्स ओवर फाइनाइट फील्ड्स

[2] अंजू और आर0के0 शर्मा– ऑन प्रिमिटिव नार्मल एलिमन्ट्स ओवर फाइनाइट फील्ड्स– एशियन यूरोपियन जे0 मैथ 2017

[3] एस0डी0 कोहेन, एस0यू0 हसन, पी0 डैनियल एण्ड डब्लू किंअग– एन, ऐसिम्पटोटिक फार्मूला फार दि नम्बर आफ इररिड्यूसिबल ट्रान्सफारमेशन शिफ्ट रेजिस्टर्स लीनियर अल्जेब्रा अप्ली0 484:46–72, 2015

[4] बी0 प्रेनील– इन्ट्रोडक्शन टू दि प्रोसीडिंग्स आफ दी सेकेण्ड वर्कशाप आन फास्ट साफ्टवेयर एनक्रिप्शन इन फास्ट साफ्टवेयर एनक्रिप्शन वॉल्यूम 1008 आफ लेक्चर नोट्स इन कम्प्यूटर साइंस, स्प्रिन्गर, पेजेज 1–5, 1995

[5] एस0 राम– इन्यूमेरेशन आफ लीनियर ट्रान्सफारमेशन शिफ्ट रेजिस्टर्स डिस0 कोड्स क्रिप्टोग्रा0 75:301–314, 2014

[6] बी0 साबाल एण्ड यू0 विश्ने– इफिशंट फीडबैक शिफ्ट रेजिस्टर्स विथ मैक्सिमल पीरियड फाइनाइट फील्ड्स ऐप्लि0 8:256–267, 2002

Contents

List of Tables

List of Symbols

p	Prime
q	a prime power
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{F}_q^*$	the multiplicative group of nonzero elements of $\mathbb{F}_q$
$\mathbb{F}_q[X]$	Ring of polynomials with coefficients in $\mathbb{F}_q$
$\|S\|$	the cardinality (= number of elements) of a finite set S
$M_d(\mathbb{F}_q)$	Set of all $d \times d$ matrices with entries in $\mathbb{F}_q$
$\mathbb{GL}_m(\mathbb{F}_q)$	Set of all $m \times m$ non singular matrices over $\mathbb{F}_q$
$Gal(\mathbb{F}_{q^m}/\mathbb{F}_q)$	Galois group of automorphisms of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$
$\langle a \rangle$	the cyclic group generated by a
$\mathbb{Z}$	the set of integers
$\mathbb{Z}_{p^r}$	Ring of Integers modulo p^r
$GR(p^{rm}, p^r)$	Galois ring of order p^{rm} and characteristic p^r
$\forall x$	for all x
$x \in X$	x is a member of X
$\phi(n)$	Euler's totient function of n
R	Galois ring of order p^{rm} and characteristic p^r
R^*	The group of units of R
χ_d	Multiplicative character of order d

l	Any positive integer
$\omega(l)$	Number of prime divisors of l
$W(l)$	Number of square free divisors of l
μ	is Möbius function
$x \notin X$	x is not a member of X
$A \subseteq X$	A is a subset of X
$a \equiv b \pmod{n}$	a congruent to b modulo n
$a \not\equiv b \pmod{n}$	a not-congruent to b modulo n