ON THE NORMAL BASES OVER FINITE FIELDS

ALOK MISHRA

DEPARTMENT OF MATHEMATICS
INDIAN INSTITUTE OF TECHNOLOGY DELHI
DECEMBER 2014

ON THE NORMAL BASES OVER FINITE FIELDS

by

ALOK MISHRA

Department of Mathematics

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

to the

Indian Institute of Technology Delhi
December 2014

Dedicated to

My Family

Certificate

This is to certify that the thesis entitled **"On the normal bases over finite fields"** submitted by **Mr. Alok Mishra** 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 our 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.

Dr. R. K. Sharma
Professor
Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110 016

Dr. Wagish Shukla
Retd. Asst. Professor

Acknowledgements

The journey of completing a PhD thesis is culminations of never-ending efforts and in pursue of the same, one requires the involvement of multiple individuals. I take this opportunity to express my thanks to all those who have guided, encouraged, remained patient and showed faith in me to conclude my academic pilgrimage.

First and foremost, I would like to express my deepest regards to my thesis supervisors Prof. R. K. Sharma and Dr. Wagish Shukla. I am extremely fortunate to have supervisors who gave me the freedom to explore on my own, and at the same time the guidance to recover whenever my steps faltered. At every crucial juncture, I was amazed at Prof. Sharma's and Dr Shukla's innate ability to anticipate my concerns and to skillfully guide me to the right direction. Their enthusiasm, knowledge, support and patience throughout the program kept me on track and encouraged me when the going got tougher.

I would like to give my special thanks to my SRC (Student Research Committee) members Dr. R. Sarma, Prof. O. P. Sharma for their valuable time and suggestions. I am greatly indebted to all faculty members of Department of Mathematics IIT Delhi, for their co-operation and support. Many thanks to NBHM, CSIR and IIT Delhi authorities for providing me the research fellowship and necessary facilities all through the PhD program.

The contributions made by my friends Dr. Sunil Kumar, Amit, Dr. Sunil Kumar prajapati, Sarvesh, Dr. Dhirendra, in overcoming the initial hurdles of research orientation are highly appreciated. I am highly grateful to them for being there, when I needed them the most.

I am immeasurably grateful to my family who gently offered counseling and gave unconditional

support at each and every point of my academic journey. It was the patience and silent sacrifice of my father and mother, which led me to complete this sojourn. My achievements are outcome of their dedication and their belief in my potentials. It is their blessings that made me reach this milestone. I would like to thank my uncle and aunt for their support and care. Without them, it would not have been possible. Thanks to all my uncles, aunties, brothers, sisters, sister-in-law, nephews and nieces for their love and kindness through this long process. Last but not the least, I acknowledge my deep gratitude to the memory of my beloved grandfather, grandmother who would have been proud of the biggest accomplishment of their grandson and I thank them for their everlasting blessings which they are still bestowing on me.

I would also like to thank all my friends Dr. Balchand, Dr. Subhabrata, Sudhakar, Dr. Ratikant, Shailesh, Varun, Varsha and all my juniors who generously shared time at different stages of my work, and the enjoyable moments spent with them will always be memorable. I would also like to express thanks and appreciation to Rabia Kamra, for having good time during this sojourn.

It's my fortune to gratefully acknowledge the support of some special individuals. Words fail me to express my appreciation to Soumendu Sarkar, for his support, generous care and the homely feeling at Delhi. I would like to extend huge, warm thanks to Keshav pratap singh, Rakesh Shukla, Aditya dev Mishra, Vandana for their valuable help and support.

Most importantly, I thank almighty god for his blessings in helping me reach this landmark.

New Delhi *Alok Mishra*

Abstract

Efficient field arithmetic is required in various coding, cryptographic and signal processing techniques. Efficiency of field arithmetic operations presumably depends on how the elements are represented. One important factor that affects the finite field computation efficiency is choice of the basis. Normal bases with lowest possible complexities over finite fields are preferred over polynomial bases due to efficient exponentiation and multiplication. In this thesis, we find bounds on the complexity of the normal basis generated by the trace of the dual element of a Type I optimal normal element and provide conditions under which our bounds are better than the known ones. Further, we find bounds on the complexity of the dual basis of the Gaussian normal basis of type (n, t) and also provide conditions under which the complexity of a Gaussian normal basis of type (n, t) is equal to the complexity of the dual basis over any finite field. Finally, we discuss the possibility for a product of two self-dual normal bases generators to be a self-dual normal basis generator and vice versa. In addition, we present a result establishing a relation between the number of self-dual normal bases of $\mathbb{F}_{q^n}$ and $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, when $m|n$ and $gcd(m, q) = 1$.

Contents

i

Certificate **i**

Acknowledgements **iii**

Abstract **v**

List of Symbols **ix**

1 Introduction **1**

1.1 Finite Field Arithmetic 2

1.2 Survey of Literature 3

1.3 A Brief Overview 5

2 Normal Bases **7**

2.1 Introduction 8

2.2 Some preliminaries 12

2.3 Results 14

2.4 Comparison 29

3 Gaussian Normal Bases **31**

3.1 Introduction 31

3.2 Some Preliminaries 35

3.3 Results 38

3.3.1 Dual basis of a Gaussian normal basis of type (n, 3) 38

3.3.2 Dual basis of a Gaussian normal basis of type (n, 4) 43

3.3.3 Dual basis of a Gaussian normal basis of type (n, 5) 47

3.3.4 Dual basis of a Gaussian normal basis of type (n, 6) 52

3.3.5 Dual basis of a Gaussian normal basis of type (n, t) 56

4 Self-dual normal bases **59**

4.1 Introduction 59

4.2 Some Preliminaries 62

4.3 Results 64

4.3.1 Recursive construction of self-dual normal bases 64

4.3.2 Distribution of Self-dual normal bases 66

5 Conclusion and Future Research **73**

5.1 Contributions 73

5.2 Future Research 77

6 Bio-Data **79**

Bibliography **81**

Bio-Data **87**