Studies on construction and list decoding of codes on some towers of function fields

M. Prem Laxman Das

Stat-Math Unit
Indian Statistical Institute
Kolkata
March 2008

Studies on construction and list decoding of codes on some towers of function fields

M. Prem Laxman Das

Thesis submitted to the Indian Statistical Institute
in partial fulfillment of the requirements
for the award of
Doctor of Philosophy

Thesis supervisors: Profs. K. Sikdar and R. Barua

Stat-Math Unit
Indian Statistical Institute
203, B.T. Road, Kolkata.

To all my teachers

Acknowledgments

It gives me great pleasure in thanking my research guides Prof. Kripasindhu Sikdar and Prof. Rana Barua. This work wouldn't have been possible without their constant support and encouragement.

I wish to thank Prof. Bimal Roy for introducing me to coding theory. His lecturing style ensured that I learnt the subject the right way.

I fondly remember Dr. Amartya Dutta's lectures on algebra and geometry. He introduced me to valuations through a series of lectures. His kind words of advice had helped me a lot in taking crucial decisions. He is like an elder brother to me.

Most importantly, I wish to thank my parents for leaving me be. They had always played a very important role in all my academic pursuits. Shyam is always there with me. This work is the result of blessings of Ajji and Abba.

My friends in ISI have been of great help and support. Ashis and Sanjoy are constant companions. Sumanta and Deepak have been of great support throughout.

I take great pride in calling myself a follower of Srimad Ananda Tirtha, a thirteenth century saint-philosopher, who propounded the Dvaita school of thought. Whatever little I've learnt of his teachings guide me. In the third stotra of his Dvadasha stotrani (Twelve hymns), he advises every human to do his duty without attachment and offer the same at the feet of the Lord. I carry these words around like a talisman. I venture to submit this work at his feet.

Contents

Notations **iii**

List of Publications **v**

List of Figures **vii**

List of Tables **ix**

Introduction **1**

1 Preliminaries and notations **9**
1.1 Function fields 9
1.1.1 Valuations, valuation rings and places 10
1.1.2 Separable extension of function fields 13
1.2 Coding theory 20
1.2.1 Basic definitions 21
1.3 Algebraic-geometric codes: Motivation and definitions 24
1.3.1 Basic definitions 24
1.3.2 Code asymptotics 26
1.4 Towers of function fields and asymptotically good codes 28
1.4.1 Recursively defined towers 29
1.4.2 Examples of optimal towers 30
1.5 List decoding of one-point codes 32
1.5.1 List decoding algorithm for one-point codes 32

2 Regular functions on B-G Tower **35**
2.1 The Bezerra-Garcia tower 37
2.2 Principal divisors on low level function fields 41
2.2.1 Case $m = 2$ 41
2.2.2 Case $m = 3$ 42
2.3 Valuations at places 44
2.4 A dual basis for F_m 46
2.5 Some concluding remarks 50

3 Regular functions on G-S tower **51**
3.1 The Garcia-Stichtenoth tower 52
3.2 Places of degree one and their ramification 55
3.3 Weierstraß semigroups 58
3.4 Construction of spaces $L(D)$ 58
3.5 Lower level function fields 59
3.6 Construction of basis for $L(uP_\infty^{(m)})$ on F_4 63
3.7 Construction of basis for $L(uP_\infty^{(m)})$ on F_5 67
3.8 Some concluding remarks 70

4 List decoding codes on G-S tower using Gröbner basis **71**
4.1 Regular functions on Garcia-Stichtenoth tower 72
4.2 Gröbner basis for modules 73
4.3 O'Keeffe-Fitzpatrick algorithm 73
4.4 List decoding of one-point codes 74
4.5 Interpolation step of list decoding 77
4.6 Some concluding remarks 78

5 Finding non-uniform input on B-G tower **79**
5.1 Kummer's theorem 81
5.2 Number of places of a given degree 82
5.3 Algebraic-geometric codes and their list decoding 83
5.4 Places of a special type of degree r of the tower 85
5.5 Finding non-uniform input on Bezerra-Garcia tower 86
5.6 Some concluding remarks 89

6 Hash functions and list decoding with side information **91**
6.1 List decoding with side information 92
6.2 Hash functions and codes 93
6.3 Amount of side information depends on the hash family 94
6.3.1 Amount of side information using hash family based on RS codes 94
6.3.2 Amount of side information using hash family based on Hermitian codes 96
6.3.3 Amount of side information using hash family based on codes constructed on G-S tower 97
6.4 Some concluding remarks 99

7 Concluding remarks and open problems **101**
7.1 Code construction on towers of function fields 101
7.2 List decoding on towers of function fields 102
7.3 Asymptotically good towers 103

Bibliography **105**

Notations

Coding Theory

$\mathbb{F}_q$	.....	a finite field of cardinality q
$\mathbb{F}_q^*$	.....	$\mathbb{F}_q \setminus \{0\}$
$[n, k, d]_q$	.....	linear code of with parameters n, k and d over $\mathbb{F}_q$
δ	.....	$\frac{d}{n}$
R	.....	$\frac{k}{n}$
H_q	.....	q-ary entropy function
RS code	.....	Reed-Solomon code
AG code	.....	Algebraic-geometric code

Basic Function Fields

$\mathbb{N}_0$	.....	$\mathbb{N} \cup \{0\}$
F/k	.....	a function field with field of constants k
$[E : F]$	.....	Degree of the extension E/F
Tr	.....	Trace map
$\mathbb{P}(F)$	.....	the set of all places of F
P	.....	a place
F_P	.....	the residue field of place P
v_P	.....	the discrete valuation at place P
$\mathcal{O}_P$	.....	the valuation ring of place P
$\deg(P)$	.....	the degree of place P
(x)	.....	the principal divisor of x
$D \succeq 0$	.....	the divisor D is non-negative
$H(P)$	.....	the Weierstraß semigroup of the place P
$L(D)$	.....	the vector space associated with the divisor D
$\dim(D)$	.....	dimension of $L(D)$
$\mathcal{D}_F$	.....	the set of all divisors of F
$g(F)$	.....	the genus of F
$N(F)$	.....	the number of places degree one of F

Separable Extension and Ramification

E/F	.....	a separable extension of function fields
$P' \mid P$	.....	the place $P' \in \mathbb{P}(E)$ contracts to $P \in \mathbb{P}(F)$
$e(P' \mid P)$	.....	the ramification index of $P' \mid P$
$f(P' \mid P)$	.....	the relative degree of $P' \mid P$
$\mathrm{con}_{E/F}(D)$	.....	Conorm of D with respect to E/F
$d(P' \mid P)$	.....	the different exponent of $P' \mid P$
$\mathrm{Diff}(E/F)$	.....	the different of E/F

List of Publications

1. M. P. L. Das. On hash functions and list decoding with side information. *IEICE Transactions*, 90-A(6):1198–1203, 2007. Available at `http://dx.doi.org/10.1093/ietfec/e90-a.6.1198`.

2. M. P. L. Das and K. Sikdar. On the computation of non-uniform input for list decoding on Bezerra-Garcia tower. In Serdar Boztas and Hsiao-feng Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC-17, Bangalore, India, December 16-20, 2007, Proceedings*, volume 4851 of *Lecture Notes in Computer Science*, pages 237–246. Springer, 2007. Available at `http://dx.doi.org/10.1007/978-3-540-77224-8_28`.

3. M. P. L. Das and K. Sikdar. List decoding codes on Garcia-Stictenoth tower using Gröbner basis. *Special Issue of Journal of Symbolic Computation (Gröbner Bases Techniques in Cryptography and Coding Theory)*. To appear in print. Available electronically at `http://dx.doi.org/10.1016/j.jsc.2008.02.004`.

4. M. P. L. Das and K. Sikdar. Regular functions on Bezzera-Garcia tower. *Applicable Algebra in Engineering, Communication and Computing*. Under Revision.

List of Figures

1.1 Coding theory setup 22
1.2 Spheres of radius at most $\lfloor \frac{d-1}{2} \rfloor$ don't touch or intersect, while those of radius $\lfloor \frac{d}{2} \rfloor$ may 22
1.3 Pyramid of function fields up to third level. 28

2.1 Bezerra-Garcia tower is a subtower of Garcia-stichtenoth tower. 40
2.2 Pyramid of function fields up to third level. 43
2.3 Places up to F_3 lying above zeroes and poles of $x(x-1)$. . . . 44
2.4 Ramification of pole of x_m. 47

3.1 Pyramid of function fields up to F_4 58

List of Tables

1.1 Algorithm for list decoding one-point codes 33

2.1 Relationship between valuations of successive coordinate variables 46

3.1 Valuation Table for $m = 3$. 56
3.2 Table of principal divisors for $m = 4$ 57
3.3 Principal Divisors of Some Functions in F_5 67

4.1 Algorithm for finding Gröbner basis for solution submodules . 75

5.1 Algorithm for ROOT-FIND step of list decoding one-point codes 84
5.2 Algorithm for finding non-uniform input on B-G tower 88

Introduction

In everyday life, there arise many situations where two parties, sender and receiver, need to communicate. The channel through which they communicate is assumed to be binary symmetric, that is, it changes 0 to 1 and vice versa with equal probability. At the receiver's end, the sent message has to be recovered from the corrupted received word using some reasonable mechanism. This real life problem has attracted a lot of research in the past few decades. A solution to this problem is obtained by adding redundancy in a systematic manner to the message to construct a *codeword*. The collection of all codewords forms a *code*. Study of codes is referred to as *coding theory*. Reed-Solomon, Reed-Muller, BCH, Goppa, etc., are some well-studied families of codes. There are many applications which use codes. A compact disc (CD) uses Reed-Solomon codes to recover the data from scratches. Cellphones use codes to correct fading and high frequency noises. Satellite communication is another high profile area which uses codes.

Coding theory is a multi-disciplinary subject drawing inputs from electronics, computer science, algebra, geometry, combinatorics, etc. The subject originated with fundamental contributions from Shannon [57] and Hamming [36]. For a fine treatment of the subject refer to [46], [8] and [66].

Coding theory deals with design of codes, efficient encoding and efficient decoding algorithms. Broadly, a code is a collection of tuples. But to make the analysis easier, it is assumed that this collection has some mathematical structure. Normally, the collection is assumed to form a $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$ and such codes are said to be *linear*. Study of codes possessing some nice algebraic structure is called *algebraic coding theory*. This thesis concentrates only on linear codes. A linear code is often represented as a triple $[n, k, d]_q$, where n denotes the length, k the dimension (also the message block length) and d the minimum distance of the code. Here, the distance refers to the Hamming distance between two tuples of length n over $\mathbb{F}_q$, which is the number of coordinates where they differ.

At the sender's end, a message m is encoded using the encoding function E of the underlying code, to obtain codeword c. This codeword is sent over the noisy binary symmetric channel. The channel introduces a random noise e, so that $y = c + e$ is received at the other end. At the receiver's end, the sent message must be recovered form y using some reasonable mechanism.

Let D denote the decoding function, which satisfies $D \cdot E(m) = m$. A Hamming sphere in $\mathbb{F}_q^n$ of radius r centered at x is the collection of all vectors having distance less than r from x. Spheres of radius greater than or equal to $\lfloor \frac{d}{2} \rfloor$ may have common points, but those of radius at most $\lfloor \frac{d-1}{2} \rfloor$ are disjoint. Hence, it is assumed that the channel corrupts at most $\lfloor \frac{d-1}{2} \rfloor$ coordinates. If the received word y ends up in a sphere with centre $c = E(m_1)$, then y is decoded as m_1. This is known as *unique decoding*.

Associated with any linear code are two matrices G and H, which are known as the *generator* and *parity check* matrices respectively. The code C is defined using these matrices as follows:

$$C = \{c \in \mathbb{F}_q^n \mid c = mG,\ m \in \mathbb{F}_q^k\} \text{ and } C = \{c \in \mathbb{F}_q^n \mid Hc^t = 0\}.$$

Codes are compactly represented using their generator and parity check matrices. Encoding and decoding may be efficiently performed if these matrices are given.

Codes are known to satisfy certain bounds. The simplest of them is the Singleton bound, which states that, for a $[n, k, d]$ code $k + d \leq n + 1$. For more bounds refer to [46], [61] and [64]. Reed-Solomon codes are an important class of linear codes which attain the Singleton bound. These are evaluation codes, obtained as follows. A subset $\{\alpha_0, \ldots, \alpha_{n-1}\}$ of $\mathbb{F}_q^*$ is fixed. Define

$$C_{RS} := \{(f(\alpha_0), \ldots, f(\alpha_{n-1})) \in \mathbb{F}_q^n \mid f \in \mathbb{F}_q[X]_k\},$$

where $\mathbb{F}_q[X]_k$ is the set of polynomials of degree less than k.

Reed-Solomon codes are particular examples of a general model. The model comprises of a mathematical object containing $\mathbb{F}_q$, a well-studied $\mathbb{F}_q$-vector subspace of the object, points where elements of the vector space may be evaluated and the evaluation maps at these points. For the Reed-Solomon case, the mathematical object is the polynomial ring in one variable, the vector space is the set of polynomials of degree less than k, points are elements of $\mathbb{F}_q$ and the evaluation maps are the usual polynomial evaluations. Algebraic-geometric codes are generalisations of Reed-Solomon codes which fall in this framework.

Algebraic geometry, generally speaking, is the study of polynomials. Function fields are algebraic analogues of curves. For an algebraic introduction to function fields refer to [61], [9] and [10]. Refer to [24], [17] and [37] for a more geometric treatment. Algebraic-geometric codes were first introduced by Goppa in [29]. Refer to [61] or [54] for a nice introduction. The monograph [60] gives an advanced treatment. Refer also to the article by Hoholdt et. al. [39] for an excellent survey. For a survey on decoding of such codes, refer to Hoholdt et. al. [38]. Such codes are constructed on function fields. Function fields of transcendence degree one are finite algebraic extensions of the field of rational functions. For purposes of coding theory, function fields over a finite field $\mathbb{F}_q$ are most important.

Every element of the function field can be thought of as a function having as domain the set of places of the function field. Points on the underlying curve correspond to discrete valuation rings or their unique maximal ideals called places of the function field. Let P_∞ be a distinguished place of the function field. The set of all functions having poles of degree at most u at this distinguished place form a $\mathbb{F}_q$ vector space. Elements of this vector space may be evaluated at places to obtain elements of a finite field (containing $\mathbb{F}_q$). Formally, these codes are defined as follows. Let $F/\mathbb{F}_q$ be a function field of genus g. Let $P_1, \ldots, P_n$ be distinct places of degree 1. Let $D = P_1 + \ldots + P_n$ and G be another divisor having support disjoint from that of D. Let $L(G)$ be the linear space associated with D. Let

$$C_L(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\} \subseteq \mathbb{F}_q^n.$$

Here each $f(P_i)$, $1 \leq i \leq n$, belongs to $\mathbb{F}_q$. Then C_L is called an a *Algebraic-Geometric(AG) code*. If G has a single place in its support, codes obtained above are called *one-point codes*.

Algorithms exist for construction and unique decoding of algebraic-geometric codes. See, for example, [23] for a simple approach for construction of codes on curves. Earliest decoding algorithms are given in articles by Sakata and others [55], [56] and [40]. Refer also to the article by Feng and Rao [22].

Order domain theory was introduced to give a treatment of algebraic-geometric codes without much usage of function field theory or geometry. Refer to [49], [44], [45], [28] and [2]. Refer to the technical report Geil [27] for a good introduction. Order domains are abstractions of the so called one point codes. These are $\mathbb{F}_q$-algebras for which the Berlekamp-Massey-Sakata algorithm for unique decoding holds. Refer also to [39].

Unique decoding algorithms correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors and output a single codeword. For larger number of errors, a different strategy is used. This is known as *list decoding*. The idea was introduced by Wozencraft [68] and Elias [18]. The first list decoding algorithm for Reed-Solomon codes was given by Madhu Sudan in [62]. Subsequently, such an algorithm for AG-codes was given by Shokrollahi and Wasserman in [58]. Refer to articles by Guruswami and Sudan, namely, [34] and [35] for further developments.

The idea of list decoding is as follows. Instead of returning a single codeword, a small list of codewords is returned. The list size is small compared to the number of codewords in the code. Formally, a code $C : \{0,1\}^k \to \{0,1\}^n$ is (p, L)-list decodable if for every $y \in \{0,1\}^n$, the set $\{x \in \{0,1\}^k \mid \delta(C(x), y) \leq p\}$ has at most L elements, where δ is the normalized Hamming distance.

For every $p < \frac{1}{2}$, there are families of (p, L_p)-list decodable codes for a fixed constant L_p that depends only on p and not on the message length (the dependence is $L_p = O(\frac{1}{\eta^2})$ when $p = \frac{1}{2} - \eta$ for any constant $\eta > 0$). Moreover,

these codes have polynomial time algorithms that output a list of at most L_p codewords that differ from y in a fraction of p or less positions. Thus even when restricted to output a relatively short list, list decoding allows efficient decoding up to any fraction $p < \frac{1}{2}$. For more details refer to Guruswami et. al. [31].

Design of polynomial time algorithms for list decoding of codes is an active area of research. Sudan in [62] gave a polynomial time algorithm for list decoding Reed-Solomon codes. This algorithm formed the model for list decoding algebraic-geometric codes. The first algorithm for AG codes was given in [58]. Later Sudan's algorithm was improved by Guruswami and Sudan in [34] to obtain algorithms for list decoding both these families. This algorithm could correct a larger number of errors due to the usage of the notion of 'multiplicities'. The algorithm of [34] was worked out for Hermitian codes in Nilsen's thesis [47].

List decoding algorithm is a two stage process [58], [34]. The first step is interpolation. For a received word $y = (y_1, \ldots, y_n)$, a polynomial H of suitable degree is constructed such that y is a zero of H of suitable multiplicity. The coefficients of H come from suitable vector subspaces. In case of Reed-Solomon codes, the polynomial H is over $\mathbb{F}_q[X]$, with coefficients satisfying degree bounds. For algebraic-geometric codes, the polynomial is over the function field, with coefficients coming from suitable Riemann-Roch spaces. The next step is root-finding. All zeroes of H which satisfy a distance bound from y are output. For more details refer to [34].

Imposing conditions on the degree and the coefficients of the polynomial guarantees the existence of the interpolation polynomial. The interpolation step may be performed easily. This can be obtained by a Gaussian elimination. Gröbner basis techniques have also been used to obtain an interpolation polynomial in Fitzpatrick and O'Keeffe [48], and Lee and O'Sullivan [42] and [41].

In [58], [3] and [69] strategies for root-finding are discussed. The strategy in [35] is based on finding a non-uniform input which is independent of the received word. The non-uniform input is the evaluations of the basis elements of the underlying Riemann-Roch space modulo a high degree place. The coefficients of H are reduced modulo this place. Thus one obtains a polynomial over a large finite field. Zeroes of the reduced polynomial, over the finite field are found by using some standard algorithm. The zeroes of the reduced polynomial lift uniquely to zeroes of the original polynomial H. The authors of [35] ask whether the non-uniform input may be found and represented efficiently.

In [30], Guruswami described a model for disambiguation of the sent message from the list by using some supplementary information through a costly, error-free channel. The side information is sent using deterministic or randomized schemes. The model is meaningful only if the number of bits of side

information required is much less than the message size. When using deterministic schemes one has to essentially send the entire message through the error free channel. Randomized strategies for both sender and receiver reduce the required number of bits of side information drastically. In Guruswami's work [30], a Reed-Solomon code based hash family is used to construct such randomized schemes. The scheme does not output a wrong message. The scheme with probability at most ε reports failure and returns the whole list. Some theoretical bounds have also been proved which lower bound the bits of side information required. The case of repeated communication is analyzed and the amortised communication complexity is calculated.

Study of places of degree one on function fields F/K has attracted much research. Such a study also finds applications in construction of good codes. See [61] for example. Over $\mathbb{F}_q$ for $g \geq 0$, let

$$N_q(g) = \max\{N(F) \mid F \text{ is a function field of genus } g\},$$

where $N(F)$ is the number of places of degree one of $F/\mathbb{F}q$. Then the quantity $A(q)$ is defined to be

$$A(q) = \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

Drinfeld-Vlăduţ bound states that $A(q) \leq \sqrt{q} - 1$. In fact, Ihara and Tsfasman, Vlăduţ and Zink proved that $A(q) = \sqrt{q} - 1$ when q is a perfect square. This bound is known as TVZ bound. For applications to coding theory, one needs lower bounds on $A(q)$. For more details consult [61].

A *tower of function fields* $\{F_m\}$ is an increasing sequence of function fields $F_i/\mathbb{F}_q$ such that each extension F_{i+1}/F_i is separable of degree $[F_{i+1} : F_i] > 1$ for some $i \geq 1$. By Riemann-Hurwitz genus formula [61, Theorem III.4.12], for a tower, $g_i \to \infty$ as $i \to \infty$. For square alphabets, codes constructed on function fields of a tower attaining the TVZ bound have the best possible asymptotic properties. Therefore, construction of such towers of function fields is useful for coding theory. One also needs the tower to be explicitly specified in terms of generators and relations for code construction. Towers exceeding the Gilbert-Varshamov bound were first constructed in [65]. For a tower of function fields with N_i rational places and genus g_i let

$$\lambda = \lim_{n\to\infty} \frac{N_n}{g_n}.$$

Towers with $\lambda > 0$ are called *asymptotically good* and those attaining the Drinfeld-Vlăduţ bound are called *asymptotically optimal*. If $\lambda = 0$ for a tower, then it is said to be *asymptotically bad*. Refer to [26, Section 2].

A slightly different but related problem is that of construction of function fields with many rational places. In Deolalikar's thesis [16], a machinery is developed for the construction of infinite families of extensions of function

fields in which almost all rational places split completely. This results in function fields with a large number of rational places. The notions of symmetry and quasi-symmetry are used to achieve such a behaviour. This theory is also used to explain many existing examples of function fields with a large number of rational places. The function fields were determined explicitly in terms of generators and relations.

The first tower of function fields attaining the Drinfeld-Vlăduţ bound was given by Garcia and Stichtenoth in [25]. In [67], Voss and Hoholdt analyzed the first few function fields of this tower.

Garcia and Stichtenoth also gave another tower which attains the DV-bound in [26]. This is probably the most well-studied tower. In [26], ramification behaviour of some places are studied. All places which contribute to the different of F_m/F_{m-1} are found with their different exponents. Then the genus g_m is calculated using the Riemann-Hurwitz genus formula [61, III.4.12]. An estimate of the number of rational places is found as $N(F_m) \geq (q^2 - q)q^{m-1}$. Using the values of N_m and g_m, it is shown that this tower attains the Drinfeld-Vlăduţ bound.

The unique pole of x_1 in F_1 is shown to be totally ramified throughout the tower(see [26, Lemma 3.3]). Let P_∞ denote this place. The functions of F_m having poles only at P_∞ are called *regular functions*. An explicit basis for the ring

$$R_m = \cup_{u \geq 0} L(uP_\infty)$$

is needed for construction of codes on these function fields. Towards this end, a local integral basis for F_m at all places other than the unique pole of x_1 and places lying above the zero of x_1, is found in [16]. The first three function fields of the tower are analyzed by Pellikaan in [51]. Following a slightly different strategy, Leonard in [43] gave an algorithm for finding regular functions using a q-th power algorithm. This strategy works not only for towers, but also for more general curves. This algorithm was generalised by Leonard and Pellikaan in [52] to work for 'integral towers'. A pole cancellation algorithm was given by Shum et. al. in [59].

In [6], Bezerra and Garcia define another tower of function fields which attains the Drinfeld-Vlăduţ bound. This tower has non-Galois steps. The recursive defining equation of the tower is a rational function in two variables, rather than a polynomial. Proof that this tower attains the Drinfeld-Vlăduţ bound is based on separable extensions of function fields using additive polynomials [61]. Using Riemann-Hurwitz genus formula, the genus of F_m is calculated. The rational places of F_1 corresponding to the roots of $x_1^q + x_1 - 1 = 0$ are completely splitting throughout the tower. Hence the number of rational places for F_m, denoted by N_m, satisfies $N_m \geq q^m$. Using these values, one obtains that the tower attains the Drinfeld-Vlăduţ bound. This tower is further shown to be a subtower of the Garcia-Stichtenoth tower of [26].

In [19], [21] and [20], Elkies has shown that many of the towers are modular. These towers are obtained from elliptic or Drinfeld modular curves. Further Elkies conjectures that all such recursively obtained optimal towers are modular, often referred to as 'Elkies fantasia' [19].

Connection between asymptotically optimal towers and best list decodable codes are known to exist. In [50], a new family of error correcting codes that have poly-time encoding and list decoding algorithms are introduced, which beat the bound of Guruswami-Sudan algorithm [34]. Capacity achieving list decodable codes based on Reed-Solomon codes are constructed in [33]. The Parvaresh-Vardy construction is generalised for AG-codes in [32]. This construction uses optimality of the tower of [26].

Contributions of this thesis and chapterwise plan: The contributions of this thesis fall in two categories. The first concerns code construction on optimal towers of function fields and the second on list decoding of one-point codes constructed on function fields of such towers. In the first chapter, we recall the preliminaries required for studying this thesis. Basic definitions on function fields are recalled from [61]. An account of basic coding theory is given. The motivation for studying algebraic-geometric codes is recalled. A few facts on towers of function fields are given. The list decoding algorithm of [58] is recalled.

The second chapter deals with construction of regular functions on function fields of Bezerra-Garcia tower. This chapter is based our the preprint [14]. We list below the results proved in this chapter.

1. A closed form expression for the ring of functions having poles only at the unique pole of x_1 of F_2 is given. It is observed that the element $\eta := (x-1)y \in F_2$ has a pole of order one at the places P_∞ and Q_∞ and no other poles.

2. The principal divisors of coordinate variables of F_3 are given, using which the ring of regular functions is partially described.

3. The relationship between valuations of successive coordinate variables at a general place is given for F_m. Using this information, valuations of coordinate variables at certain places are calculated for F_m.

4. A trace basis-dual basis pair for the ring of regular functions of F_m is given. The basis is contained in the ring of regular functions of that level, so that any regular function can be written as a linear combination of elements of this dual basis.

The third chapter deals with finding regular functions on Garcia-Stichtenoth tower of [26]. We have constructed the following:

1. first q^2 basis elements and some basis elements in the range q^4 to $q^4 + q^3 - q^2$ for F_4,

2. some basis elements for F_5.

The fourth chapter deals with list decoding one-point codes on function fields of Garcia-Stichtenoth tower using Gröbner basis. The contents of this chapter have been reported in [13]. Techniques of [48] are used.

The fifth chapter deals with finding non-uniform input on Bezerra-Garcia tower. These results have appeared in [15]. It is observed in this chapter that the asymptotic argument given in [32] is more general and applies to Bezerra-Garcia tower as well. An algorithm [15, Algorithm 2] for finding the non-uniform input, similar to that in [32], is given for the function fields of this tower. The property that regular functions have poles only at zeroes and poles of $x_1(x_1 - 1)$ is used in addition to a technical lemma [15, Lemma 6]. The correctness of the algorithm [15, Theorem 2] follows from Kummer theorem [61, pp. 76].

The sixth chapter deals with list decoding with side information. This chapter is based on the journal paper published by the author of this thesis in IEICE journal on fundamentals [12]. We examine how different choices of hash functions affect the number of bits of side information needed to disambiguate the output list in list decoding in a randomized framework as considered by [30]. We examine several hash families corresponding to certain algebraic-geometric codes and show that some improvements over [30] are indeed possible [12, Theorem 5] and [12, Theorem 6].

We conclude and pose open problems in the seventh chapter.

Chapter 1

Preliminaries and notations

In this chapter preliminaries required for this thesis are recalled. The main object of study of this thesis is one-point code. Understanding function fields is necessary before embarking on the study of these codes. Riemann-Roch spaces of one-point divisors are particularly important. Function field theory required for studying algebraic-geometric codes are recalled in the first section. The treatment is along the lines of [61]. Refer also to [9] and [10]. For a more geometric treatment refer to [24]. Next, we recall some basic facts about coding theory. Refer to [46] and [66] for more details. Refer also to [63] for a nice treatment of this topic. Some preliminaries on code asymptotics are recalled, which motivate the study of algebraic-geometric codes. Some facts about optimal towers are recalled. Finally, list decoding is studied.

The notations of [61] are followed. A list of notations used throughout this thesis has already been given.

1.1 Function fields

In this section, we study some basic properties of algebraic function fields in one variable. The basic reference for this section is [61]. An algebraic function fields in one variable correspond to field of functions on plane curves. These also capture many properties of the underlying algebraic curves. The treatment here, similar to that in [61], is algebraic. For a more geometric treatment refer to [24]. First, some properties of valuation rings of function fields are recalled. The valuation ring, its maximal ideal and the underlying valuation are equivalent. Then, the notion of degree of a place is recalled. Next, some properties of divisors are recalled. Riemann's theorem connecting the degree and dimension of a divisor is stated. The elements of the function field may be thought of as functions on the set of places of the function field. The notions of zeroes and poles of elements of function fields is recalled. Then Weierstraß gap theorem is recalled.

Then separable extensions function fields are studied. Extensions and restrictions of places in such separable extensions of function fields are studied. Briefly, ramification theory is recalled. The fundamental equality is stated. Integral bases for such extensions are studied. The Riemann-Hurwitz genus formula is recalled after a study of different exponent and the different divisor. Then, the definition of trace dual basis is recalled. Some particular separable extensions are studied.

1.1.1 Valuations, valuation rings and places

We begin with the definition of function fields.

Definition 1.1.1. *A function field F/K of one variable is an extension such that F is a finite algebraic extension of $K(x)$, where $x \in F$ is transcendental over K.*

Definition 1.1.2. *A valuation ring $\mathcal{O}$ of F/K is a ring such that $K \subsetneq \mathcal{O} \subsetneq F$ and for any $z \in F$ either $z \in \mathcal{O}$ or $1/z \in \mathcal{O}$.*

Any valuation ring has a unique maximal ideal. We recall a lemma giving some properties of valuation rings of function fields.

Lemma 1.1.3. *Let $\mathcal{O}$ be a valuation ring of the function field F/K and P its unique maximal ideal. Then*

1. *P is a principal ideal. Any generator of P is called the prime element or uniformizing parameter for P.*
2. *If $P = t\mathcal{O}$ then any $0 \neq z \in F$ has a unique representation of the form $z = t^n u$ for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}^*$ (set of units).*
3. *$\mathcal{O}$ is a principal ideal domain. More precisely, if $P = t\mathcal{O}$ and $\{0\} \neq I \subseteq \mathcal{O}$ is an ideal then $I = t^n\mathcal{O}$ for some $n \in \mathcal{N}$.*

Proof. Refer to [61, Page no. 3]. ∎

We have already seen that any valuation ring has a unique maximal ideal. The maximal ideal of a valuation ring is called a place.

Definition 1.1.4. *A place P of a function field is the unique maximal ideal of some valuation ring $\mathcal{O}_P$ of F.*

The set of all places of F will be denoted by $\mathbb{P}(F)$. Next the notion of a discrete valuation is recalled.

Definition 1.1.5. *A discrete valuation of F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:*

1. $v(x) = \infty$ *if and only if* $x = 0$,
2. $v(xy) = v(x) + v(y)$ *for any* x *and* y *in* F,
3. $v(x + y) \geq \min\{v(x), v(y)\}$ *for any* x *and* y *in* F,
4. *There exists an element* $t \in F$ *such that* $v(t) = 1$ *and*
5. $v(a) = 0$ *for any* $a \in K \setminus \{0\}$.

With any valuation ring a valuation may be associated in a natural way.

Definition 1.1.6. *To any place* P *a discrete valuation* v_P *is associated as follows. Choose a prime element* t *for* P. *Any* $z \neq 0$ *in* F *has a unique representation as* $z = t^n u$ *for some* $n \in \mathbb{Z}$ *and* $u \in \mathcal{O}^*$. *Define* $v_P := n$ *and* $v_P(0) := \infty$.

A place, its valuation ring and the valuation defined above are equivalent. For any P, in terms of the valuation $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$, $\mathcal{O}_P^* = \{z \in F \mid v_P(z) = 0\}$ and $P = \{z \in F \mid v_P(z) > 0\}$. Given any v a discrete valuation, $P := \{z \in F \mid v_P(z) > 0\}$ is the place associated with v and $\mathcal{O}_P := \{z \in F \mid v_P(z) \geq 0\}$ is the corresponding valuation ring.

Definition 1.1.7. *Let* $z \in F$ *and* $P \in \mathbb{P}(F)$. *A place* P *is said to be a zero of* z *if* $v_P(z) > 0$ *and pole if* $v_P(z) < 0$. *If* $v_P(z) = m > 0$, *then* P *is a zero of order* m *and if* $v_P(z) = -m < 0$, *then* P *is a pole of* z *of order* m.

Any $z \in F$ which is transcendental over K has at least one zero and pole. Any element $z \neq 0$ has only finitely many zeroes and poles.

Definition 1.1.8. *For any* $P \in \mathbb{P}(F)$,

1. *the set* $F_P := \mathcal{O}_P/P$ *is a field containing* K *called the residue class field of* P *and*
2. $\deg P := [F_P : K]$ *is called the degree of* P.

The degree of any place is finite. Hence the full field of constants is a finite extension of K. The elements of a function field may be considered to be functions on set of places. Further, functions may be evaluated at places. Let $z \in F$. Let P be a place. If $z \in \mathcal{O}_P$, then $z(P) := z + P$ and $z(P) := \infty$ otherwise.

Definition 1.1.9. *A divisor of* F *is a finite* $\mathbb{Z}$ *linear combination of places. A divisor* D *is said to be positive, denoted by* $D \succeq 0$, *if the non zero coefficients of places occurring in* D *are all positive.*

The set of divisors of F/K is a additively written free Abelian group generated by places of F, denoted by $\mathcal{D}(F)$. For $x \in F$ let Z and N denote the set of set of zeroes and poles of x respectively. Then $(x)_0 = \sum_{P \in Z} v_P(x)P$ is called the *zero divisor* of x, the divisor $(x)_\infty = \sum_{P \in N}(-v_P(x))P$ is called the *pole divisor* of x and the divisor $(x) = (x)_0 - (x)_\infty$ is called the *principal divisor* of x.

The map $P \mapsto \deg(P)$ on the set of places may be extended linearly to the group of divisors. Let $\deg D$ denote the degree of D. For any D, the set

$$L(D) = \{z \in F \mid D + (z) \succeq 0\}$$

is a K-vector space. The dimension of this vector space is defined to be the dimension of D, denoted by $\dim D$.

Definition 1.1.10. *The genus g of F/K is defined by*

$$g := \max\{\deg A - \dim A + 1 \mid A \in \mathcal{D}(F)\}.$$

Genus is a very important invariant of the underlying function field. Next we recall the Riemann's theorem.

Theorem 1.1.11. *Let F/K be a function field of genus g.*

1. *For any divisor $A \in \mathcal{D}_F$,*

$$\dim A \geq \deg A + 1 - g.$$

2. *There is an integer c, depending on F/K, such that*

$$\dim A = \deg A + 1 - g$$

whenever $\deg A \geq c$.

Proof. Refer to [61, Theorem I.4.17]. ∎

Gaps and non-gaps

Let $P \in \mathbb{P}(F)$ and $n \geq 2g$. There exists an element $x \in F$ such that $(x)_\infty = nP$.

Definition 1.1.12. *Let $P \in \mathbb{P}(F)$. An integer $n \geq 0$ is called a pole number(or non-gap) if there exists an element $x \in F$ such that $(x)_\infty = nP$. Otherwise n is called a gap.*

We now recall the Weierstraß gap theorem from [61].

Theorem 1.1.13. *Suppose F/K has a genus $g > 0$ and P is a place of degree one. Then there exist exactly g gap numbers $i_1 < \ldots < i_g$ of P. We have*

$$i_1 = 1 \text{ and } i_g \leq 2g - 1.$$

Proof. Refer to [61, Theorem I.6.7] ∎

The Weierstraß gap theorem is particularly useful in the study of one-point codes.

1.1.2 Separable extension of function fields

In this section, separable extensions function fields are studied. Extensions and restrictions of places in such separable functions are studied. Briefly, ramification theory is recalled. The fundamental equality is stated. Integral bases for such extensions are studied. The Riemann-Hurwitz genus formula is recalled after a study of different exponent and the different divisor. Then, the definition of trace dual basis is recalled. Some particular separable extensions are studied. The setup is as follows.

Let F'/K' be function field which is a finite algebraic extension of another function field F/K. That is, both $F' \supset F$ and $K' \supset K$ are finite algebraic extensions. The discussion is as in [61, Chapter III].

Basic definitions

Here the notion of extension and restriction of places in separable extension of function fields is first recalled. Then for any such extension, the ramification index and relative degree are defined. The fundamental equality relating these quantities is stated.

Definition 1.1.14. *A place $P' \in \mathbb{P}(F')$ is said to lie over $P \in \mathbb{P}(F)$ if $P \subseteq P'$. This is denoted by $P' \mid P$.*

We now have the following proposition.

Proposition 1.1.15. *The following assertions are equivalent:*

1. *$P' \mid P$,*
2. *$\mathcal{O}_P \subseteq \mathcal{O}_{P'}$ and*
3. *There exists an integer e such that $v_{P'}(x) = ev_P(x)$.*

Moreover if $P' \mid P$ then

$$P = P' \cap F \text{ and } \mathcal{O}_P = \mathcal{O}_{P'} \cap F.$$

Proof. Refer to [61, Theorem III.1.4]. ∎

Consequently, for $P' \mid P$ there is a canonical embedding of the residue class field $F_P = \mathcal{O}_P/P$ into $F'_{P'} = \mathcal{O}_{P'}/P'$.

Definition 1.1.16. *Let $P' \mid P$.*

a. The integer $e(P' \mid P) := e$ with

$$v_{P'}(x) = e v_P(x)$$

is called the ramification index of P' over P. The extension $P' \mid P$ is said to be ramified if $e(P' \mid P) > 1$, otherwise unramified.

b. $f(P' \mid P) := [F'_{P'} : F_P]$ is called the relative degree of P' over P.

Let $F'' \supseteq F' \supseteq F$ be separable extensions of function fields. Let $P'' \in \mathbb{P}(F'')$, $P' \in \mathbb{P}(F')$ and $P \in \mathbb{P}(F)$, such that $P'' \supseteq P' \supseteq P$. The ramification index and relative degree satisfy

$$e(P'' \mid P) = e(P'' \mid P')e(P' \mid P')$$
$$f(P'' \mid P) = f(P'' \mid P')f(P' \mid P').$$

Proposition 1.1.17. *Let F'/K' be a algebraic extension of F/K. Then*

A. For any place $P' \in \mathbb{P}(F')$, there is exactly one place $P \in \mathbb{P}(F)$ such that $P' \mid P$, namely $P = P' \cap P$.

B. Conversely, any place $P \in \mathbb{P}(F)$ has at least one but finitely may $P' \in \mathbb{P}(F')$ such that $P' \mid P$.

Proof. Refer to [61, Proposition III.1.7]. ∎

Hence, for $P \in \mathbb{P}(F)$

$$\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e(P' \mid P)P'$$

is a well-defined divisor. Finally, we recall the fundamental theorem for e and f.

Theorem 1.1.18. *Let $P_1, \ldots, P_m$ be all the places of F' lying above a place P of F. Let $e_i := e(P_i \mid P)$ and $e_i := e(P_i \mid P)$ for $1 \le i \le m$. Then*

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

This is called the fundamental equality for ramification of places.

Proof. Refer to [61, Theorem III.1.11]. ∎

Integral basis

Here, properties of an integral basis for a separable extension of function fields is recalled. After recalling the notion of integrality the definition of integral basis is given. Then existence of integral basis is recalled.

Definition 1.1.19. *Let R be a subring of F/K.*

A. *An element $z \in F$ is said to be integral over R if $f(z) = 0$ for some monic polynomial f over R.*

B. *The set*

$$ic_F(R) := \{z \in F \mid z \text{ is integral over } R\}$$

is called the integral closure of $R \in F$.

C. *Let $F_0 \subseteq F$ denote the quotient field of R. Then R is said to be integrally closed if $ic_{F_0}(R) = R$.*

The definition of integral basis at a place is recalled first from [61, pp. 75].

Definition 1.1.20. *Let $F' \supset F$ be a finite separable extension of the function field F/K with $n = [F' : F]$ and $P \in \mathbb{P}_F$ be a place of F/K. The integral closure of $\mathcal{O}_P$ in F' is denoted by $\mathcal{O}'_P$. There exists a basis $\{u_1, \ldots, u_n\}$ of $F' \supset F$ such that*

$$\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot u_i.$$

Such a basis is called an integral basis of $\mathcal{O}'_P$ over $\mathcal{O}_P$ (or a local integral basis for P).

Here, we recall some basic facts about trace dual basis for function fields. We start with the definition of trace map. For more details consult [61].

Definition 1.1.21. *Let F/K be any finite extension of fields. For any $\alpha \in L$, associate the K-linear map*

$$\begin{aligned} \mu_\alpha : & L \to L \\ & z \mapsto \alpha \cdot z. \end{aligned}$$

Then the trace of α is defined as

$$Tr_{L/K}(\alpha) := trace(\mu_\alpha),$$

where trace denotes the operator trace.

Trace is a K-linear map satisfying, for extensions $M \supset L \supset K$ and $\alpha \in M$

$$\mathrm{Tr}_{M/K}(\alpha) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(\alpha)).$$

For a separable extension of function fields, given any basis, there exists a uniquely determined trace dual basis. We recall the details of this fact from [61, Proposition III.3.3].

Proposition 1.1.22. *Let L/K be a finite separable extension of degree n and consider a basis $\{z_1, \ldots, z_n\}$ of L/K. Then there are uniquely determined $\{z^*, \ldots, z^*\}$ of L such that*

$$Tr_{M/L}(z_i z_j^*) = \delta_{ij},$$

where δ denotes the Kronecker symbol. The set $z_1^*, \ldots, z_n^*$ is a basis of L/K, called the (trace) dual basis of $\{z_1, \ldots, z_n\}$.

Proof. Refer to [61, Proposition III.3.3]. ∎

The result [61, Theorem III.3.4] is used to express a regular function as a suitable linear combination of dual basis elements.

Theorem 1.1.23. *Let R be an integrally closed subring of F/K with quotient field F, and F'/F be a finite separable extension of of degree n. Let $R' = ic_{F'}(R)$ denote the integral closure of R in F'. If $\{z_1, \ldots, z_n\} \subset R'$ denotes a basis and $z_1^*, \ldots, z_n^*$ the corresponding (trace) dual basis, then*

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*.$$

Proof. Refer to [61, Theorem III.3.4]. ∎

Next, the result regarding existence of integral basis for a place is recalled from [61, pp. 75].

Lemma 1.1.24. *Let $F' \supset F$ be a finite separable extension of the function field F/K with $n = [F' : F]$. Then any basis $\{z_1, \ldots, z_n\}$ of $F' \supset F$ is a local integral basis for almost all $P \in \mathbb{P}_F$.*

Proof. Refer to [61, Theorem III.3.6]. ∎

The proof of the above lemma actually finds the set of places for which the given basis is not local integral.

The next lemma is a part of the proof of [61, Theorem III.5.10]. This result is often used to determine a dual basis for a separable extension of function fields.

Lemma 1.1.25. *Let $F' = F(y)$ be a separable extension of function fields of degree n. Let $\varphi(T)$ be the minimal polynomial of y over F. Let $\varphi(T) = (T-y)(c_{n-1}T^{n-1} + \ldots + c_1T + c_0)$ with $c_0, \ldots, c_{n-1} \in F'$ and $c_{n-1} = 1$. Then*

$$\left\{ \frac{c_0}{\varphi'(y)}, \ldots, \frac{c_{n-1}}{\varphi'(y)} \right\}$$

is the dual basis of

$$\{1, y, \ldots, y^{n-1}\}.$$

Proof. See [61, pp. 96]. ∎

Riemann-Hurwitz genus formula

Here the Riemann-Hurwitz genus formula is recalled. First the definitions of different exponent and different divisor are stated. The Dedekind different theorem is also recalled.

Definition 1.1.26. *Let F'/F be a separable extension of function fields. For $P \in \mathbb{P}(F)$, let $\mathcal{O}'_P := ic(\mathcal{O}_P)$ denote the integral closure of $\mathcal{O}_P$ in F'. Then the set*

$$\mathcal{C}_P := \{z \in F' \mid Tr_{F'/F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

is called the complementary module over $\mathcal{O}_P$.

In fact $\mathcal{C}_P$ is a $\mathcal{O}'_P$-module such that $\mathcal{C}_P = t \cdot \mathcal{O}'_P$.

Definition 1.1.27. *The different exponent of $P' \mid P$ is defined to be*

$$d(P' \mid P) := -v_{P'}(t).$$

The different exponent is a well-defined, non-negative quantity. For almost all P and $P' \mid P$, the equality $d(P' \mid P) = 0$ holds.

Definition 1.1.28. *Let F'/F be a separable extension of function fields. The different divisor is defined to be*

$$diff(F'/F) := \sum_{P \in \mathbb{P}(F)} \sum_{P'|P} d(P' \mid P) \cdot P'.$$

The following theorem helps find different exponents of places.

Theorem 1.1.29. *(Dedekind different theorem) For $P' \mid P$,*

1. *$d(P' \mid P) \geq e(P' \mid P) - 1$.*
2. *$d(P' \mid P) = e(P' \mid P) - 1$ if and only if $e(P' \mid P)$ is not divisible by the characteristic of K.*

Proof. Refer to [61, Theorem III.5.1]. ∎

Next, we state the Riemann-Hurwitz genus formula.

Theorem 1.1.30. *Let F/K be a function field of genus g and constant field K and F'/K' a finite separable extension of genus g' and constant field K'. Then*

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \mathit{diff}(F'/F).$$

Proof. Refer to [61, Theorem III.4.12]. ∎

The following lemma regarding ramification in composita of function fields is useful.

Lemma 1.1.31. *[26] Let E/F be a separable extension of function fields over $\mathbb{F}_q$. Assume that H_1 and H_2 are intermediate fields of E/F such that $E = H_1 \cdot H_2$. For a place $P' \in \mathbb{P}(E)$, let $P_i \in \mathbb{P}(H_i)$ be the restriction of P' to H_i, $i = 1, 2$ and let $P \in \mathbb{P}(F)$ be the restriction of P' to F. Suppose that $e(P_1 \mid P)$ and $e(P_2 \mid P)$ are relatively prime. The following hold:*

1. *$e(P' \mid P) = e(P_1 \mid P) \cdot e(P_2 \mid P)$.*
2. *If $P_1 \mid P$ is tame, then*

$$d(P' \mid P_1) = e(P_1 \mid P)d(P_2 \mid P) - (e(P_1 \mid P) - 1)(e(P_2 \mid P) - 1)$$

Proof. Refer to [26]. ∎

Riemann-Hurwitz genus formula is used to determine the genera of function fields of towers of [25], [26] and [6].

Some examples of separable extensions

In this section, we list some properties of two particular separable extensions of functions fields. First, we recollect some properties of a particular form of algebraic extension of function fields called *Artin-Schreier extension.*

Theorem 1.1.32. *[26] Suppose that $F/\mathbb{F}_{q^2}$ is a function field with full field of constants. Let $w \in F$ and assume that there exists a place $P \in \mathbb{P}(F)$ such that*

$$v_P(w) = -m, \ m > 0 \text{ and } (m, q) = 1.$$

Let $E = F(z)$, where z satisfies the equation

$$z^q + z = w.$$

Then the following hold:

1. *The degree of extension* $[E : F] = q$ *and* $\mathbb{F}_{q^2}$ *is algebraically closed in* E.

2. *The place* P *is totally ramified in* E/F, *i.e., there is a unique place* $P' \in \mathbb{P}(E)$ *such that* $P' \mid P$ *and the different exponent of* $P' \mid P$ *is given by*
$$d(P' \mid P) = (q-1)(m+1).$$

3. *Let* $R \in \mathbb{P}(F)$ *and assume that* $w = u^q + u + \mathcal{O}(1)$ *at* R *for some* $u \in F$. *Then the place* R *is unramified in* E/F. *In particular, this is the case if* $v_R(w) = 0$.

4. *Suppose that the place* $Q \in \mathbb{P}(F)$ *is a zero of* $w - \gamma$, $\gamma \in \mathbb{F}_q$. *The equation* $X^q + X = \gamma$ *has* q *distinct roots and for any such root* α, *there is a unique place* $Q_\alpha \in \mathbb{P}(E)$ *such that* $Q_\alpha \mid Q$ *and* Q_α *is a zero of* $z - \alpha$. *In particular, the place* Q *splits completely in* E/F.

Proof. Refer to [26]. ∎

The function fields of [26] falls in this category.

Definition 1.1.33. *A polynomial of the form*

$$a(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \ldots + a_1 T^p + a_0 T \in K[T]$$

(where $p = char(K) > 0$*) is called an additive polynomial.*

An additive polynomial of the above form is separable if and only if $a_0 \neq 0$. Such a polynomial has a property that

$$a(u + v) = a(u) + a(v)$$

for u and v in some extension of K.

We next recall the properties of another separable extension of function fields based on additive polynomials. The treatment is from [61, Proposition III.7.10].

Proposition 1.1.34. *Consider an algebraic function field* F/K *with constant field* K *of characteristic* $p > 0$, *and an additive polynomial* $a(T) \in K[T]$ *of degree* p^n *which has all its zeroes in* K. *Let* $u \in F$. *Suppose that for any* $P \in \mathbb{P}(F)$ *there is an element* $z \in F$ *(depending on* P*) such that*

Case 1.1.35. $v_P(u - a(z)) \geq 0$

or

Case 1.1.36. $v_P(u - a(z)) = -m$, *with* $m > 0$ *and* $m \not\equiv 0 \mod p$

holds. Define $m_P := -1$ *for the first case and* $m_P := m$ *in the second. Then* m_P *is a well-defined integer. Consider the extension field* $F' = F(y)$ *of* F *where* y *satisfies the equation*

$$a(y) = u.$$

If there exists at least one place $Q \in \mathbb{P}(F)$ *with* $m_Q > 0$*, the following hold:*

a. F'/F *is Galois with* $[F' : F] = p^n$ *and the Galois group is isomorphic to the additive group* $\{\alpha \in K \mid a(\alpha) = 0\}$*, hence isomorphic to* $(\mathbb{Z}/p\mathbb{Z})^n$*.*

b. K *is algebraically closed in* F'*.*

c. *Any* $P \in \mathbb{P}(F)$ *with* $m_P = -1$ *is unramified in* F'/F*.*

d. *Any* $P \in \mathbb{P}(F)$ *with* $m_P > 0$ *is totally ramified in* F'/F *and the different exponent* $d(P' \mid P) = (p^n - 1)(m_P + 1)$*.*

e. *Let* g'*(resp.* g*) be the genus of* F'*(resp.* F*). Then*

$$g' = p^n g + \frac{p^n - 1}{2}\left(-2 + \sum_{P \in \mathbb{P}(F)} (m_P + 1) \deg P\right).$$

Proof. Refer to [61, Proposition III.7.10]. ∎

The function fields of [6] falls in this category.

1.2 Coding theory

In everyday life, there arise many situations where two parties, sender and receiver, need to communicate. The channel through which they communicate is assumed to be binary symmetric, that is, it changes 0 to 1 and vice versa with equal probability. At the receiver's end, the sent message has to be recovered from the corrupted received word using some reasonable mechanism. This real life problem has attracted a lot of research in the past few decades. A solution to this problem is obtained by adding redundancy in a systematic manner to the message to construct a *codeword*. The collection of all codewords forms a *code*. Study of codes is referred to as *coding theory*. Reed-Solomon, Reed-Muller, BCH, Goppa, etc., are some well-studied families of codes. There are many applications which use codes. A compact disc (CD) uses Reed-Solomon codes to recover the data from scratches. Cellphones use codes to correct fading and high frequency noises. Satellite communication is another high profile area which uses codes. We recall some facts about coding theory in this section. For a fine treatment of the subject refer to [46], [8] and [66].

1.2.1 Basic definitions

Often a code is abstracted as a collection of tuples of a fixed length over an alphabet. For ease of mathematical analysis, it is assumed that such a collection forms a vector subspace of $\mathbb{F}_q^n$. Thus a code is often represented as a triple $[n, k, d]_q$, where n denotes the length, k the dimension and d the minimum distance of the code. Here, the distance refers to the Hamming distance between to tuples of length n over $\mathbb{F}_q$, which is the number of coordinates where they differ.

Definition 1.2.1. *[46] The Hamming distance Δ between two vectors x and y of length n over some alphabet of size q is defined to be the number of components where they differ.*

A $(n, K, d)_q$ code has K words of length n over some alphabet of size q where d is the minimum distance between any two words.

An $[n, k, d]_q$ linear code C is a vector subspace of $\mathbb{F}_q^k$ of dimension k and having minimum distance d.

Associated with any linear code are two matrices G and H, which are known as the *generator* and *parity check* matrices respectively. The code C is defined using these matrices as follows:

$$C = \{c \in \mathbb{F}_q^n \mid c = mG,\ m \in \mathbb{F}_q^k\}$$

and

$$C = \{c \in \mathbb{F}_q^n \mid Hc^t = 0\}.$$

Refer to [46] for further properties of codes. We recall the definition of Reed-Solomon codes.

Definition 1.2.2. *Let $S = \{\alpha_1, \ldots, \alpha_n\}$ be a set of non-zero elements from $\mathbb{F}_q$. Let $\mathbb{F}_q[x]_k$ denote the vector space of polynomials over $\mathbb{F}_q$ of degree less than k. Let $\mathcal{C} = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in \mathbb{F}_q[x]_k\}$. Then $\mathcal{C}_{RS}$ is called a Reed-Solomon(RS) code.*

There are many other well-studied code families like Reed-Muller, BCH, Goppa, etc.

Decoding problem

Coding theory deals with design of codes, giving efficient encoding and decoding algorithms for them. In this section, we study the decoding problem for codes. If a symbol, of a alphabet of size q, is equally likely to get corrupted to any other symbol then the channel is said to be q-ary symmetric. The setup is depicted in Figure 1.1. In the following discussion, the channel is assumed to be q-ary symmetric. Let C be a $[n, k, d]_q$ code. A message m

of block length k is encoded using the encoding function E of the code. This is a one-to-one function. Let $c := E(m)$ where $m \in \mathbb{F}_q^k$ and $c \in \mathbb{F}_{q^2}^n$. This c is sent over a noisy channel, which gets corrupted and y is received with $y = c + e$, say. Here e denotes the error vector. At the receiving end, the sent message has to be recovered using some 'reasonable mechanism'. Nothing is assumed about the channel.

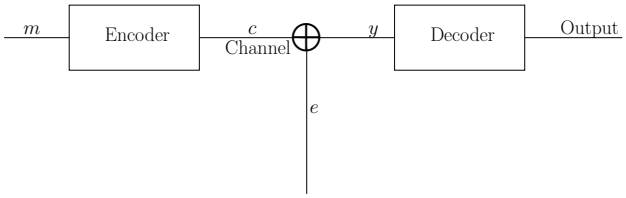

Figure 1.1: *Coding theory setup*

Let D denote the decoding function, which satisfies $D \cdot E(m) = m$. A Hamming sphere in $\mathbb{F}_q^n$ of radius r centered at x is the collection of all vectors having distance less than r from x. Spheres of radius greater than or equal to $\frac{d}{2}$ may have common points, but those of radius at most $\lfloor \frac{d-1}{2} \rfloor$ are disjoint, as depicted in Figure 1.2.

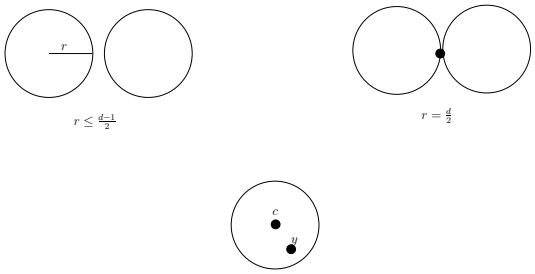

Figure 1.2: *Spheres of radius at most* $\lfloor \frac{d-1}{2} \rfloor$ *don't touch or intersect, while those of radius* $\lfloor \frac{d}{2} \rfloor$ *may*

Hence, it is assumed that the channel corrupts at most $\lfloor \frac{d-1}{2} \rfloor$ coordinates. If the received word y ends up in a sphere with center $c = E(m_1)$, then y is decoded as m_1. This is known as *unique decoding*. This is depicted in Figure 1.2.

Next we recall the notion of syndrome decoding. For $y \in \mathbb{F}_q^n$, the vector $S = Hy^t$ is called the *syndrome*. Using the fact that $y = c + e$, it is easy to see that syndrome of c and e are equal. A table is constructed as follows. The first row of the table is C. The subsequent rows are the non-zero cosets of C in $\mathbb{F}_q^n$. The element with lowest Hamming weight is chosen as the coset representative.

Using this setup, the received word y could be decoded as follows. The syndrome of y is calculated. Using this, the coset to which y belongs can be found. Then y is located in that coset. Finally y is decoded as that codeword lying above it in the table. This is known as syndrome decoding.

Let the minimum distance and the dimension be normalised with respect to length. Let us consider the decoding problems for codes. The sender S encodes using the encoding function E for C a message x and sends $E(x)$ through a channel to receiver R. The channel corrupts the symbols of the code independently according to some probability distribution, hence R receives r. The most fundamental decoding problem is the following:

Problem 1.2.3. *(**Maximal Likelihood Decoding**) Find the x that maximises*

$$P_{Channel}[r = E(x)].$$

Problem 1.2.4. *(**Nearest Codeword Problem**) Find the x that minimises $\Delta(r, E(x))$.*

Unique decoding algorithms decode up to $\lfloor \frac{d-1}{2} \rfloor$ errors and output a single codeword. For larger number of errors, a different strategy is used. This is known as *list decoding*. Instead of returning a single codeword, a small list of codewords is returned. The list size is small compared to the number of codewords in the code. Formally, the list decoding problem is stated in the last section.

Bounds

Codes are known to satisfy certain bounds. The simplest of them is the Singleton bound, is stated in the following theorem.

Theorem 1.2.5. *For a $[n, k, d]$ code*

$$k + d \leq n + 1.$$

Next we recall Plotkin bound. Plotkin Bound says that a code with large distance has a very small number of codewords. Hence, the decoding problems for such codes are trivial. Hereafter, we will assume that the distance of the code is not very large so that the code has exponentially (in n) many codewords.

Theorem 1.2.6. *(Plotkin Bound) If a code over a alphabet of size Q has minimum relative distance $\beta > 1 - \frac{1}{Q}$, then the number of codewords in such a code is at most $\frac{Q\beta}{Q\beta - Q + 1}$.*

Reed-Solomon codes are Minimum Distance Separable (MDS). That is, they satisfy equality in Singleton bound. For more facts on coding theory refer to [46]. Next some facts about algebraic-geometric codes are recalled from [61]. Refer also to [64]. Some fundamentals on construction of asymptotically good codes on optimal towers of function fields are recalled. Then, the list decoding algorithm of [34] is recalled and representation issues discussed.

The next part of this chapter is devoted to the study of construction and list decoding of algebraic-geometric codes. Such codes are generalisations of Reed-Solomon codes. These codes were first introduced in [29]. Refer to [61] or [54] for a nice introduction. Refer also to the article [39] for an excellent survey. Refer also to [38] for an excellent survey on decoding of such codes. Such codes are constructed on function fields of transcendence degree one. As already seen in the earlier part of this chapter, it is possible to evaluate elements of function fields at places. Algebraic-geometric codes are obtained in this fashion. We study the definitions and some basic properties of these codes. We recall some bounds from [61]. Algebraic-geometric codes attain the uniformly best possible asymptotic bounds known. Hence this class of codes is widely studied. The next part deals with the construction of such codes. These codes may be easily constructed, given a basis for the underlying Riemann-Roch spaces. Finally the algorithm [58] is recalled.

1.3 Algebraic-geometric codes: Motivation and definitions

In this section, the basic definition and properties of algebraic-geometric code are recalled. As an example, some properties of Hermitian curves are listed. Then some asymptotic bounds on codes are stated from [61]. Algebraic-geometric codes attain the best known bounds. This motivates the study of such codes.

1.3.1 Basic definitions

Basic reference for this section is [61]. We start with the definition of algebraic-geometric code.

Definition 1.3.1. *Let $F/\mathbb{F}_q$ be a function field genus g. Let $P_1, \ldots, P_n$ be distinct places of degree 1. Let $D = P_1 + \ldots + P_n$ and G be another divisor having support disjoint from that of D. Let*

$$C_L(D, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in L(G)\} \subseteq \mathbb{F}_q^n.$$

Here each $f(P_i)$, $1 \leq i \leq n$, belongs to $\mathbb{F}_q$. Then C_L is called an C_L a Algebraic-Geometric(AG) code. Often, the divisor G is taken to be of the form uP for a place P. Such codes are known as one-point codes.

Next, some properties of these codes are recalled. Let us consider the evaluation map $ev_D : L(G) \longrightarrow \mathbb{F}_q^n$ given by

$$ev_D(x) = (x(P_1), \ldots, x(P_n)) \in \mathbb{F}_q^n.$$

The evaluation map is linear and $C_L(D, G)$ is the image of $L(G)$ under this map. For proof of the following theorem refer to [61, Theorem 2.2].

Theorem 1.3.2. *[61] The code $C_L(D, G)$ is a $[n, k, d]$ code with parameters*

$$k = \dim G - \dim(D - G) \text{ and } d \geq n - \deg G.$$

If degree of G is strictly less than n then the evaluation map

$$ev_D : L(G) \longrightarrow C_L(D, G)$$

is injective and we have:

1. *The code $C_L(D, G)$ is a $[n, k, d]$ code with*

   $$d \geq n - \deg G \text{ and } k = \dim G \geq \deg G + 1 - g.$$

   Hence $k + d \geq n + 1 - g$.

2. *In addition, if $2g - 2 < \deg G < n$, then $k = \deg G + 1 - g$.*

Proof. Refer to [61, Theorem II.2.2]. ∎

Next, the definition of Hermitian curve is recalled and some properties studied in the following remark. Such codes are well-studied and easy to implement.

Definition 1.3.3. *Let $\mathbb{F}_{q^2}$ be a finite field. Then the Hermitian curve χ_H over $\mathbb{F}_{q^2}$ is given by the equation $y^q + y = x^{q+1}$.*

Remark 1.3.4. *The following facts about Hermitian curves may be verified:*

1. *χ_H is a nonsingular, absolutely irreducible curve.*
2. *The genus of χ_H is $g = \frac{q(q-1)}{2}$.*
3. *The places of degree one of χ_H are the unique place $P_{\alpha,\beta}$ of degree one such that $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$ for each pair $(\alpha, \beta) \in \mathbb{F}_{q^2}$ satisfying $\beta^q + \beta = \alpha^{q+1}$ and the common pole P_∞ of x and y. Thus, χ_H has $1 + q^3$ places of degree one.*

4. *The pole order of x at P_∞ is q and that of y is $q+1$. Hence, the semi-group of pole orders at P_∞ is $\{qr+(q+1)s' \mid s, s' \in \mathbb{N} \cup \{0\}\}$.*

5. *This curve is maximal, meaning the number of places of degree one equals $q+1+2q\sqrt{q}$.*

Codes constructed on Hermitian function fields using divisors $D = P_1 + \ldots + P_{q^3}$ and $G = uP_\infty$, where u is suitably chosen, are called *Hermitian codes*.

1.3.2 Code asymptotics

Here, we recall some asymptotic bounds on codes. The treatment is as in [61]. Let C be a $(n, M, d)_q$ code. Define $\delta := \frac{d}{n}$ and $R := \frac{\log_q M}{n}$. Let

$$V_q := \{(\delta(C), R(C)) \in [0,1]^2 \mid C \text{ is a code over } \mathbb{F}_q\}$$

and $U_q \subseteq [0,1]^2$ be the set of limit points of V_q.

The following theorem gives some description of the set U_q.

Theorem 1.3.5. *(Manin) There is a continuous function $\alpha_q(\delta),\ \delta \in [0,1]$ such that*

$$U_q = cl\{(\delta, R) \mid) 0 \leq R \leq \alpha_q(\delta),\ 0 \leq \delta \leq 1\}.$$

Moreover $\alpha_q(0) = 1$ and $\alpha_q(\delta) = 0,\ \delta \in [\frac{q-1}{q}, 1]$ and $\alpha_q(\delta)$ decreases in $[0, \frac{q-1}{q}]$.

Proof. Refer to [61, Proposition VII.2.2]. ∎

Exact value of α_q is not known. Only upper and lower bounds on the quantity is known. Next we recall some asymptotic bounds on α_q.

Theorem 1.3.6. *(Gilbert-Varshamov bound) For $0 \leq \delta \leq 1 - q^{-1}$,*

$$\alpha_q(\delta) \geq 1 - H_q(\delta).$$

Here H_q is the q-ary entropy function $H_q : [0, 1-q^{-1}] \to \mathbb{R}$ is defined by

$$H_q(0) := 0$$
$$H_q(x) := x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x) \text{ for } x \in (0, 1-q^{-1}].$$

Proof. Refer to [61, Proposition VII.2.3]. ∎

A bound on α_q is directly related to a sequence of function fields with a large number of places of degree one relative to their genus. The details are recalled here.

Definition 1.3.7. *For $g \geq 0$ define*

$$N_q(g) = \max\{N(F) \mid F \text{ function field of genus } g\}$$

where $N(F)$ is the number of places of $F/\mathbb{F}_q$ of degree one. The quantity $A(q)$ is defined as follows

$$A(q) = \limsup_{n\to\infty} \frac{N_q(g)}{g}.$$

The Drinfeld-Vlăduţ bound gives an upper bound on quantity $A(q)$.

Theorem 1.3.8. *(Drinfeld-Vlăduţ) The Drinfeld-Vlăduţ bound states that*

$$A(q) \leq \sqrt{q} - 1.$$

Proof. Refer to [61, Theorem V.3.6]. ∎

The following proposition gives the connection between α_q and $A(q)$.

Proposition 1.3.9. *Suppose that $A(q) > 1$. Then*

$$\alpha_q(\delta) \geq (1 - A(q)^{-1}) - \delta$$

in the interval $0 \leq \delta \leq 1 - A(q)^{-1}$.

Proof. Refer to [61, Proposition VII.2.5]. ∎

The Drinfeld-Vlăduţ bound is an upper bound, but we need lower bounds to get meaningful assertion from the above proposition. In fact, Ihara and Tsfasman-Vlăduţ-Zink proved that $A(q) = \sqrt{q}$ when q is a perfect square. Hence

$$\alpha_q(\delta) \geq \left(1 - \frac{1}{q^{1/2} - 1}\right) - \delta \text{ for } 0 \leq \delta \leq 1 - \frac{1}{q^{1/2} - 1}$$

if q is a square. This bound is called *Tsfasman-Vlăduţ-Zink* bound. For $q \geq 49$, it is better than Gilbert-Varshamov bound in certain interval. See Figure 1.3.

Function field towers attaining Drinfeld-Vlăduţ bound give codes with best asymptotic properties. This motivates the problem of explicit construction of such towers.

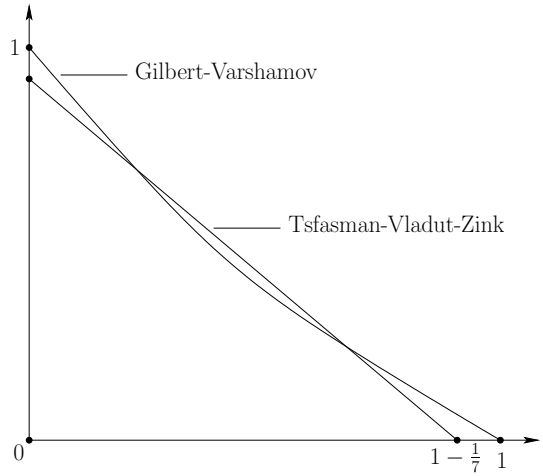

Figure 1.3: *Pyramid of function fields up to third level.*

1.4 Towers of function fields and asymptotically good codes

In this section, we recall some facts on towers of function fields and some examples of those which are optimal. Sequences of codes exceeding the Gilbert-Varshamov bound were first constructed in [65]. The first tower of function fields attaining the Drinfeld-Vlăduţ bound was given by Garcia and Stichtenoth in [25]. The same authors give another tower in [26] and study some properties of function field towers. There exist many such towers which are optimal for square cardinality. A tower with non-Galois step was given in [6]. We first recall the notion of a function field tower. Then give some examples of towers which are optimal. Throughout the description, we assume that the underlying finite field is of square cardinality.

Definition 1.4.1. *[26] A tower of function fields $\{F_m\}$ is a sequence of function fields $F_i/\mathbb{F}_q$ of genus g_i, $i = 1, 2, 3, \ldots$ having the following properties:*

1. *$F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots$,*
2. *For each $i \geq 1$, the extension F_{i+1}/F_i is separable of degree $[F_{i+1} : F_i] > 1$ and*
3. *$g_i > 1$ for some $i \geq 1$.*

By Riemann-Hurwitz genus formula [61, Theorem III.4.12], for a tower $g_i \to \infty$ as $i \to \infty$.

Next, we recall the notion of a subtower from [26].

Definition 1.4.2. *Let $\mathcal{F} = \{F_1, F_2, F_3, \ldots\}$ be a tower of function fields over $\mathbb{F}_q$. Another such tower of function fields $\mathcal{E} = \{E_1, E_2, E_3, \ldots\}$ is called a subtower of $\mathcal{F}$ if there exists an embedding over $\mathbb{F}_q$*

$$\iota : \bigcup_{i \geq 1} E_i \to \bigcup_{i \geq 1} F_i.$$

That is, for any $i \geq 1$ there is an index $m = m(i) \geq 1$ such that $\iota(E_i) \subseteq F_m$.

For a tower of function fields with N_i rational places and genus g_i let

$$\lambda = \lim_{n \to \infty} \frac{N_n}{g_n}.$$

Towers with $\lambda > 0$ are called *asymptotically good* and those attaining the Drinfeld-Vlăduţ bound are called *asymptotically optimal*. If $\lambda = 0$ for a tower, then it is said to be *asymptotically bad*. Next, we recall [26, Corollary 2.4].

Corollary 1.4.3. *Let $\mathcal{F}$ be a function field and $\mathcal{E}$ a subtower of $\mathcal{F}$. Then the following hold:*

1. *If $\mathcal{E}$ asymptotically bad then so is $\mathcal{F}$.*
2. *If $\mathcal{F}$ is optimal then so is $\mathcal{E}$.*

1.4.1 Recursively defined towers

A particular class of towers, which are defined recursively defined by a polynomial are recalled. The discussion is as in [4] and [5].

Definition 1.4.4. *A tower $\mathcal{F}$ is said to be recursively defined by a polynomial $f(X, Y) \in \mathbb{F}_q[X, Y]$ if $F_1 = \mathbb{F}_q(x_1)$ is the rational function field and for each $n \in \mathbb{N}$, the field F_{n+1} is defined by*

$$F_{n+1} = F_n(x_{n+1}) \text{ with } f(x_n, x_{n+1}) = 0.$$

Further $[F_{n+1} : F_n] = \deg_Y f(X, Y)$ for all $n \in \mathbb{N}$ and $\deg_X f(X, Y) = \deg_Y f(X, Y)$.

Some classes of recursive towers are described below:

1. **Kummer towers:** Kummer towers are given recursively by an equation of the form:

$$Y^m = f(X) \text{ where } f(X) \in \mathbb{F}_q(X),\ (m, q) = 1.$$

If $m \mid (q-1)$, each F_{n+1}/F_n in a Kummer tower is cyclic of degree m. A more specific class of towers consists of those of Fermat type, which are given recursively by

$$Y^m = a(X+b)^m + c \text{ with } a, b, c \in \mathbb{F}_q.$$

The above equation gives a tower if and only if $abc \neq 0$.

2. **Artin-Schreier towers:** These towers are given by an equation of the form:
$$\varphi(Y) = \chi(X),$$
where $\varphi(Y) \in \mathbb{F}_q[Y]$ is an additive separable polynomial and $\psi(x) \in \mathbb{F}_q(x)$ is a rational function. If φ has all its roots in the finite field $\mathbb{F}_q$, then each step F_{n+1}/F_n is an elementary Abelian p-extension with $[F_{n+1} : F_n] = \deg\ \varphi(Y)$

For example, the tower of [26] is an Artin-Schreier extension.

1.4.2 Examples of optimal towers

In this section, we recall some well studied towers of function fields. First, we recall the definition of the tower of [25].

Definition 1.4.5. *Let $F_1 = \mathbb{F}_{q^2}(x_1)$ be the rational function field. For $n \geq 1$, let*

$$F_{n+1} := F_n(z_{n+1}),$$

where z_n satisfies the equation

$$z_{n+1}^q + z_{n+1} = x_n^{q+1}$$

with

$$x_n := z_n/x_{n-1} \in F_n,\ n \geq 2.$$

The function field F_2 is the Hermitian function field. The genus and number of places of degree one of $F_m/\mathbb{F}_{q^2}$ are as follows. The genus $g_m = g(F_m)$ is given by the following formula:

$$g_m = \begin{cases} q^m + q^{m-1} - q^{\frac{m+1}{2}} - 2q^{\frac{m-1}{2}} + 1, \text{ for } m \text{ odd} \\ q^m + q^{m-1} - \frac{1}{2}q^{\frac{m}{2}+1} - \frac{3}{2}q^{\frac{m}{2}} - q^{\frac{m}{2}-1} + 1, \text{ for } m \text{ even.} \end{cases}$$

The number of places of degree one satisfies $N_m \geq (q^2-1)q^{m-1} + 2q$. Hence, one may safely say that $N_m \geq n_m = q^m(q-1)$.

The ramification behavior of places is rather complicated. Interested reader may consult [25] for more details. The pole of $x_1 \in F_1$ is totally ramified through out the tower. In other words, there is a unique, degree

one place lying above the pole of $x_1 \in F_1$ through out the tower. Refer to [25, Lemma 2.2].

Next we recall the tower of [26]. This is a recursively defined tower, attaining Drinfeld-Vlăduţ bound.

Definition 1.4.6. *For $K = \mathbb{F}_{q^2}$, the Garcia-Stichtenoth tower is given by*

$$\begin{aligned} F_1 =& K(x_1) \\ F_m =& F_{m-1}(x_m) \end{aligned}$$

where,

$$x_m^q + x_m = \frac{x_{m-1}^q}{x_{m-1}^{q-1} + 1}, \text{ for } m > 1.$$

The following properties of this tower may be verified. The degree of extension $[F_m : F_{m-1}]$ is q. The genus g_m of F_m is given by

$$g_m = \begin{cases} (q^{\frac{m}{2}} - 1)^2 \text{ , for } m \text{ even} \\ (q^{\frac{m+1}{2}} - 1)(q^{\frac{m-1}{2}} - 1) \text{ , for } m \text{ odd.} \end{cases}$$

The number of places of degree one satisfies

$$N(F_m) \geq (q^2 - q)q^{m-1}, \ m \geq 1.$$

Finally we recall the Bezerra-Garcia tower of [6]. This tower has non-Galois steps for $q \neq 2$.

Definition 1.4.7. *Let $K = \mathbb{F}_{q^2}$ and let $F_1 := K(x_1)$, be the rational function field. For each $m \geq 1$, we have $F_{m+1} := F_m(x_{m+1})$, where x_{m+1} satisfies*

$$\frac{x_{m+1} - 1}{x_{m+1}^q} = \frac{x_m^q - 1}{x_m}. \tag{1.4.1}$$

We state some of the main properties of this tower. The degree of the extension $[F_m : F_1] = q^{m-1}$. Each F_i/F_{i-1} is separable for $i \geq 2$. Also $\mathbb{F}_{q^2}$ is the full field of constants for each F_i, for $i \geq 1$. The genus of the mth function field g_m is given by

$$(q-1) \cdot g_m = \begin{cases} \left(q^{\frac{m}{2}} - 1\right)^2, \ m \text{ even} \\ \left(q^{\frac{m-1}{2}} - 1\right)\left(q^{\frac{m+1}{2}} - 1\right), \ m \text{ odd.} \end{cases} \tag{1.4.2}$$

The number of rational places for F_m, denoted by N_m, satisfies

$$N_m \geq q^m. \tag{1.4.3}$$

All these towers may be seen to attain the Drinfeld-Vlăduţ bound. Hence these are important from coding theory point of view. For, the codes constructed on such a tower have best parameters.

1.5 List decoding of one-point codes

In this section we recall the list decoding algorithm of [34] for one-point codes. Unique decoding algorithms decode up to $\lfloor \frac{d-1}{2} \rfloor$ errors and output a single codeword. For larger number of errors, a different strategy is used. This is known as *list decoding*. Instead of returning a single codeword, a small list of codewords is returned. The list size is small compared to the number of codewords in the code. This notion was first introduced independently in [68] and [18]. Formally, the list decoding problem may be stated as follows.

Problem 1.5.1. *(**List Decoding**) Find the list of all codewords* $\{c \in C \mid \Delta(c, r) < t\}$*, for some* t*. List decoding is said to be successful if the sent word is in the output list.*

Let us start with the definition of the notion of list decodability.

Definition 1.5.2. *Let* $0 < p < 1$*. A code* $C : \{0,1\}^k \to \{0,1\}^n$ *is* (p, L)*-list decodable if for every* $y \in \{0,1\}^n$*, the set* $\{x \in \{0,1\}^k \mid \Delta^*(y, C(x)) \leq p\}$ *has at most* L *elements, where* Δ^* *is the normalized Hamming distance.*

Johnson bound says that for small enough sphere about the received word, the number of codewords about it is a polynomial in the message length. Hence, one can hope to decode with small lists.

Theorem 1.5.3. *(Johnson bound)Let* $\mathcal{C}$ *be any* q*-ary code of block length* n *and minimum relative distance* $d = \frac{d'}{n} = (1-\frac{1}{q})(1-\delta)$ *for some* $0 < \delta < 1$*. Let* $e = \frac{e'}{n} = (1-\frac{1}{q})(1-\gamma)$ *for some* $0 < \gamma < 1$ *and let* $x \in \mathbb{F}_q^k$ *be arbitrary. Then provided* $\delta > \sqrt{\gamma}$*, we have* $|\mathbf{B}_q(r, e) \cap \mathcal{C}| \leq \min\{n(q-1), \frac{1-\delta}{\gamma^2-\delta}\}$*. Furthermore, for* $\delta = \sqrt{\gamma}$*, we have* $|\mathbf{B}_q(r, e) \cap \mathcal{C}| \leq 2n(q-1)-1$*. Here* $\mathbf{B}_q(r, e)$ *denotes the ball about* r *of radius* e*.*

1.5.1 List decoding algorithm for one-point codes

The first list decoding algorithm for Reed-Solomon codes was given in [62]. Subsequently, such an algorithm for algebraic-geometric codes was given in [58]. These were generalised to correct more errors in [35]. Here we recall a simple case of the list decoding algorithm of [58]. Let F be a function field having places $P_1, \ldots, P_n; P_\infty$ of degree one. Let $G = \alpha P_\infty$ and $D = P_1 + \ldots + P_n$. Let $y = (y_1, \ldots, y_n)$ be the received word. Let $\delta_0 = \lceil \frac{n+1}{b+1} + \frac{b\alpha}{2} + g - 1 \rceil$ and $\beta = \delta_0$. Thus for any given positive integer b we have an $(n - \beta - 1, b)$ list decoding algorithm for AG codes:

In [58] a method is outlined for reducing the factorisation problem over function fields to factorisation of bivariate polynomial over finite fields. The function field F is assumed to be a separable extension over the field of rational functions in one variable over $\mathbb{F}_q$. Let say $L = \mathbb{F}_q(x)$. Further it

Input: β, b, received word $y = (y_1, \ldots, y_n)$
Output: List of words of distance at most $n - \beta - 1$ from y
1. (Interpolation Step) Find a non-zero polynomial $H(T)$ such that: $H(T) = u_b T^b + \ldots + u_1 T + u_0 \in F[T]$, $u_j \in L(\delta_j P_\infty)$, $0 \leq j \leq b$ $H(P_i, y_i) = \sum_{j=0}^{b} u_j(P_i) y_i^j$ is zero for $i = 1, \ldots, n$.
2. (Factorisation Step) Find all roots ρ of $H(T)$ in F. For each ρ compute $x_\rho = (\rho(P_1), \ldots, \rho(P_n))$. If x_ρ is not defined or if $\Delta(x_\rho, y) > n - \beta - 1$ discard x_ρ else output x_ρ.

Table 1.1: *Algorithm for list decoding one-point codes*

is assumed that a primitive element for the above extension is known. In this setting, a factorisation a polynomial $G \in F[T]$ can be obtained from the factorisation of the norm of G, denoted by $N(G) \in L[T]$. Notice that $N(G)$ is a polynomial in two variables over $\mathbb{F}_q$. However the procedure is not very efficient.

In subsequent chapters we consider a generalisation of this algorithm given by Guruswami and Sudan in [34]. The interpolation and root-finding steps are discussed for function fields of optimal towers. In particular, the strategy of root-finding of [35] is discussed.

The next two chapters deal with code construction on towers of functions fields. In the second chapter, we consider the lesser known Bezerra-Garcia tower of [6] and study regular functions on them. The third chapter deals with regular functions on lower level function fields of Garcia-Stichtenoth tower.

Chapter 2

Regular functions on Bezerra-Garcia tower

Construction of explicit bases for the Riemann-Roch spaces of one point divisors finds applications in coding theory. The problem of constructing good towers of function fields is related to construction of asymptotically good sequences of codes. Pellikaan in [51], gives a closed form expression for any function having poles only at the 'infinite place' is given for the first three function fields of the Garcia-Stichtenoth tower [26]. In [53] the Weierstraß semi-group of this place is calculated. Shum et. al., in [59], give valuations of some important functions at certain places is calculated. Further, a specially designed dual basis is used to give a pole cancellation algorithm for finding the ring of regular functions.

We try to perform the calculations carried out for the Garcia-Stichtenoth tower [26] to obtain some results for the tower of Bazerra and Garcia [6]. It is known from [6] that the unique pole of $x_1 \in F_1$ is totally ramified throughout the tower, as in the case of Garcia-Stichtenoth tower of [26]. By regular functions, we mean functions having poles only at the unique pole of X_1.

We give a description of places of F_2. In F_2, the place P_0 is the common zero of x and y, which is totally ramified in $F_2/\mathbb{F}_{q^2}(x)$. The place P_∞ is the unique pole of x which is a zero of order $q-1$ of y. This place is also totally ramified. The unique zero of $x-1$ in F_1 has places Q_1 and Q_∞ of F_2 lying above it. The place Q_∞ is the unique pole of y which is a zero of order $q-1$ of $x-1$. Finally, the place Q_1 is the common zero of $x-1$ and $y-1$. The ramification description also give the degrees of the places.

We next describe places in F_3. The zero P_0 and pole P_∞ of x are both totally ramified. They are denoted by the same symbol. The pole of y satisfies Possibility 2.1.5. Using Lemma 2.1.6, this place is unramified in F_3/F_2 and there are q such places denoted by $Q_{\infty i},\ i = 1, \ldots, q$. There are two places of F_3 lying above the zero of $x-1$ in F_2. One is R_1, the common

zero of $x-1, y-1, z-1$, with ramification index 1 and the other is R_∞, a zero of $y-1$ and a pole of $z-1$ (and of z), with ramification index $q-1$. Similarly the ramification behavior gives the degrees of the places.

Results about F_2: We prove the following facts for F_2. For the function field F_2 the following hold:

1. The element $\eta := (x-1)y$ has the following principal divisor:
$$(\eta) = Q_1 + P_0 - Q_\infty - P_\infty.$$
2. The set
$$\mathcal{B}_2 := \{x^i(x-1)\eta^j \mid i \geq 0,\ 0 \leq j \leq q-1\}$$
is a $\mathbb{F}_{q^2}$-basis for
$$R_2 := \cup_{u\geq 0} L(uP_\infty).$$

Results about F_3: A partial description of regular functions for F_3 is also given. The details are as follows. The elements $\alpha := (x-1)y$ and $\beta := (x-1)(y-1)yz$ have principal divisors as follows:

a. $((x-1)y) = R_1 + qP_0 + (q-1)R_\infty - qP_\infty - \sum_{i=1}^{q} Q_{\infty i}$.

b. $((x-1)(y-1)yz) = (q+1)R_1 + (q+1)P_0 - P_\infty - 2\sum_{i=1}^{q} Q_{\infty i} - R_\infty$.

These functions are used to give a partial description of regular functions on F_3. This construction also indicates how the trace dual basis may be constructed.

Results about F_m: A special basis-dual basis pair for F_m is given. Let $\rho_i = (x_1-1)^{q^i}$ for $i = 2, \ldots, m$. Let
$$\mathcal{Z} := \prod_{i=2}^{m} \{1, \rho_i x_i, \rho_i x_i^2, \ldots, \rho_i x_i^{q-1}\}$$
and
$$\mathcal{Z}^* := \prod_{i=2}^{m} \left\{ -\frac{x_i-1}{\rho_i x_i^q}, -\frac{x_i-1}{\rho_i x_i^{q-1}}, \ldots, -\frac{x_i-1}{\rho_i x_i^2}, \frac{1}{\rho_i x_i} \right\}$$
be the sets obtaining by taking $m-1$-fold products of the constituent sets. Then
$$\sum_{z\in\mathcal{Z}} R_1 z \subseteq R_m \subseteq \sum_{z^*\in\mathcal{Z}^*} R_1 z^*,$$
where the sums above are finite.

This basis is special because of the following fact. Any element $\zeta \in F_m$ having poles only at P_∞ can be written as a (finite) sum
$$\zeta = \sum_{\xi\in\mathcal{Z}^*} a_\xi(x_1)\xi,$$

where a_ξ is a polynomial in x_1. The valuations of the coordinate variables at places lying above zeroes and poles of $x_1(x_1-1) \in F_m$ are studied.

The following is the plan of this chapter. After recalling some preliminaries on Bezerra-Garcia tower, we make an analysis of the second function field and obtain all regular functions. We give the principal divisors of the coordinate variables of F_3 and obtain a partial description of regular functions. Then, we calculate the valuations of the coordinate variables at some places of F_m. Finally, we compute a basis-(trace)dual basis for F_m. We first obtain a vector space basis for F_m/F_1, which is contained in the regular functions on F_m, by multiplying $\{1, y, \ldots, y^{m-1}\}$ by a suitable 'constant'. We use [61, Theorem III.3.4] and [61, Theorem III.5.10]. The basis is contained in the ring of regular functions of that level, so that any regular function can be written as a linear combination of elements of the dual basis. The contents of this chapter are based on our preprint [14] which will be submitted for publication soon.

2.1 The Bezerra-Garcia tower

In this section, the tower studied in [6] is recalled. This tower has already been defined in the previous chapter. Some important properties of this tower are listed. We start with the definition of the Bezerra-Garcia tower.

Definition 2.1.1. *Let $K = \mathbb{F}_{q^2}$ and let $F_1 := K(x_1)$, be the rational function field. For each $m \geq 1$, we have $F_{m+1} := F_m(x_{m+1})$, where x_{m+1} satisfies*

$$\frac{x_{m+1}-1}{x_{m+1}^q} = \frac{x_m^q - 1}{x_m}. \tag{2.1.1}$$

We recall the the main properties of this tower in the next few lemmas.

Lemma 2.1.2. *The following hold for the Bezerra-Garcia function fields.*

1. *The degree of the extension $[F_m : F_1] = q^{m-1}$.*
2. *Each F_i/F_{i-1} is separable for $i \geq 2$.*
3. *$\mathbb{F}_{q^2}$ is the full field of constants, for each F_i for $i \geq 1$.*

Proof. By definition of the tower, for $i \geq 2$, the function field F_i is obtained by adjoining x_i to F_{i-1}, where x_i has minimal polynomial

$$\psi(T) = T^q - \frac{x_{i-1}}{x_{i-1}^q - 1}T + \frac{x_{i-1}}{x_{i-1}^q - 1}.$$

The polynomial $\phi(T) = \psi(T) - \frac{x_{i-1}}{x_{i-1}^q-1}$ is an additive polynomial satisfying

$$\phi'(T) = -\frac{x_{i-1}}{x_{i-1}^q - 1}.$$

In other words, the polynomial $\phi(T)$ is separable. The function field is obtained by adjoining a root of $\phi(T) + \frac{x_{i-1}}{x_{i-1}^q - 1} = 0$. Now all the assertions follow by Proposition 1.1.34. ■

We have thus shown in the previous lemma that the sequence of extensions indeed form a tower. Following facts regarding ramification of places lying above the pole and zeroes of x_1 and $x_1 - 1$ of F_1 may be recalled from [6]. First we consider which totally ramify.

Lemma 2.1.3. *The following hold for the function field F_m of tower.*

1. *The unique pole of x_1 in F_1 is totally ramified throughout the tower.*
2. *The unique zero of x_1 in F_1 is totally ramified throughout the tower.*

Proof. The proof follows from Proposition 1.1.34. See also [6, Lemma 2]. ■

Next, places of F_m lying above the zero of $x_1 - 1$ are considered. Such a place Q has two possibilities:

Possibility 2.1.4. *The place Q is a common zero of $x_1 - 1, \ldots, x_m - 1$.*

In this case Q is unramified in F_m/F_1 and totally ramified in $F_m/\mathbb{F}_{q^2}(x_m)$.

Possibility 2.1.5. *There exists an index t such that $1 \leq t < n$ such that*

(a). *Q is a common zero of $x_i - 1$ for $i = 1, 2, \ldots, t$,*

(b). *Q is a pole for x_{t+1} and*

(c). *Q is a zero of x_i for $i = t + 2, \ldots, m$.*

In fact, the second item of the above possibility implies the other two. The ramification behaviour in this case is discussed in [6, Lemma 3]. First, we recall some notations from [6]. For $1 \leq k \leq t$

$$E_k := \mathbb{F}_{q^2}(x_{t+1-k}, \ldots, x_{t+k}) \text{ and } H_k := E_k(x_{t+k+1}).$$

The following quantities are also defined:

$$\begin{aligned} X_i &:= x_{i+t+1} - 1, \ i < 0 \text{ and } X_0 := 1/x_{t+1} \\ X_i &:= -x_{i+t+1}, \ i > 0, \\ Y_k &:= \prod_{i=-k}^{-1} X_i \text{ and } Z_k := \prod_{i=1}^{k} X_i \end{aligned}$$

The pole of the function x_{t+1} in the rational function field $H_0 := \mathbb{F}_{q^2}(x_{t+1})$ is denoted by Q_0. The facts regarding ramification of Q_0 are summarised in the following lemma.

Lemma 2.1.6. *For $1 \leq k \leq t$ let E_k and H_k be defined as above. Let Q_k be a place of H_k which is a pole of x_{t+1} and let P_k denote the restriction of Q_k to the field E_k. Then, the following hold:*

1. *The function $f_k := (Z_k - Y_k)/X_0$ is regular at the place Q_k. The minimal polynomial of f_k over E_k is separable modulo the place P_k. In particular, the place Q_k is unramified over E_k, that is $e(Q_k \mid P_k) = 1$.*

2. *The zero orders at Q_k of X_i are*

$$v_{Q_k}(X_i) = \begin{cases} q^{k+i} \cdot (q-1), \text{ if } -k \leq i \leq -1, \\ q^k, \text{ if } i = 0 \\ q^{k-i} \cdot (q-1), \text{ if } 1 \leq i \leq k. \end{cases}$$

3. *For $i = 1, 2, \ldots, k$, we have*

$$v_{Q_k}\left(\frac{X_i - X_{-i}}{X_i}\right) \geq q^{k-i}.$$

Proof. See [6, Lemma 3]. ∎

The lemma further gives the valuations of x_i at Q_k. Putting together all these facts the expression for genus of the function fields may be obtained.

Lemma 2.1.7. *The genus of the mth function field g_m is given by*

$$(q-1) \cdot g_m = \begin{cases} \left(q^{\frac{m}{2}} - 1\right)^2, \ m \text{ even} \\ \left(q^{\frac{m-1}{2}} - 1\right)\left(q^{\frac{m+1}{2}} - 1\right), \ m \text{ odd.} \end{cases} \tag{2.1.2}$$

Hence, the tower attains Drinfeld-Vlăduţ bound (Theorem 1.3.8).

Proof. The following places contribute to the different (see Definition 1.1.28) of F_m/F_{m-1}:

1. The place P_0 corresponding to $x_1 = 0$ is totally ramified and $d(P_0) = q$.

2. The place P_∞ corresponding to $x_1 = \infty$ is totally ramified and $d(P_0) = 2(q-1)$.

3. There are q^t places which correspond to $x_{t+1} = \infty$ for $1 \leq t \leq (m-2)/2$ which are totally ramified and any such place Q has $d(Q) = 2(q-1)$. Notice that this excludes P_∞.

4. The place R corresponding to $x_m = \infty$ is totally ramified and has $d = q - 2$.

Thus, the degree of the different is given by

$$\deg \operatorname{diff}_{F_m/F_{m-1}} = 2(q-1) + 2(q^{[m/2]} - 1),$$

where $[x]$ denotes the integer part of x. The genus can now be calculated using Riemann-Hurwitz genus formula, Theorem 1.1.30.

The rational places of F_1 corresponding to the roots of $x_1^q + x_1 - 1 = 0$ are completely splitting throughout the tower. Hence the number of rational places for F_m, denoted by N_m, satisfies

$$N_m \geq q^m. \tag{2.1.3}$$

Using these values,

$$\lim_{m\to\infty} \frac{N_m}{g_m} = q - 1.$$

In other words, the tower attains Drinfeld-Vlăduţ bound. ■

The Bezerra-Garcia tower is optimal, hence is important from coding theory point of view. The next remark gives another proof of optimality of the tower.

Remark 2.1.8. *The Bezerra-Garcia tower is actually a subtower of the Garcia-Stichtenoth tower. Indeed, let $E_1 \subset E_2 \subset E_3 \subset \ldots$ denote the Garcia-Stichtenoth tower of [26] and $F_1 \subset F_2 \subset F_3 \subset \ldots$ the Bezerra-Garcia tower. The functions*

$$x_n := \frac{1}{y_n^{q-1} + 1}$$

on the Garcia-Stichtenoth tower satisfy the defining equation of the Bezerra-Garcia tower. Each E_n/F_n is a Kummer extension of degree $q-1$ satisfying

$$E_n = F_n(y_1) \text{ with } y_1^{q-1} = \frac{1 - x_1}{x_1}.$$

Here $F_1 = \mathbb{F}_{q^2}(x_1)$. See Figure 2.1.

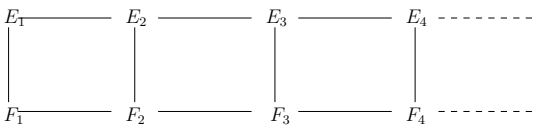

Figure 2.1: *Bezerra-Garcia tower is a subtower of Garcia-stichtenoth tower.*

That the Bezerra-Garcia tower is a subtower of the Garcia-Stichtenoth tower gives another proof of its optimality by Corollary 1.4.3.

2.2 Principal divisors on low level function fields

We consider first few levels of the tower and find the principal divisors of the coordinate variables. We also study the ring of regular functions of these function fields. By regular functions, we mean functions having poles only at the unique pole of x_1. The first function field is just the rational function field. Hence, we start with the second function field of the tower.

2.2.1 Case $m = 2$

Here, we consider the second function field of the tower. The principal divisors of the coordinate variables are obtained. Finally, using these principal divisors, an explicit basis the ring of regular functions is determined. The results here may be compared with those of Pellikaan [51]. The next lemma gives the principal divisors of the coordinate variables.

Lemma 2.2.1. *Let $F_2 = \mathbb{F}_{q^2}(x, y)$, where x and y satisfy Equation 2.1.1. We have the following principal divisors*

$$\begin{aligned} (x) &= qP_0 - qP_\infty \\ (x-1) &= Q_1 + (q-1)Q_\infty - qP_\infty \\ (y) &= P_0 + (q-1)P_\infty - qQ_\infty \\ (y-1) &= qQ_1 - qQ_\infty. \end{aligned} \tag{2.2.1}$$

Proof. The places P_0 and P_∞ are totally ramified throughout the tower. Hence, the principal divisor of x may be immediately obtained. The unique zero of $x-1$ in F_1 has places Q_1 and Q_∞ lying above it. The ramification indices of Q_1 and Q_∞ are respectively 1 and $q-1$. The place Q_1 is the common zero of $x-1$ and $y-1$. Thus the principal divisors of $x-1$ and $y-1$ may be obtained. Both P_0 and P_∞ are zeroes of y. The pole of y in $\mathbb{F}_{q^2}(y)$ is totally ramified in $F_2/\mathbb{F}_{q^2}(y)$. This gives the principal divisor of y, which proves the lemma. ∎

We have already seen that, the unique pole of x is totally ramified in $F_2 \supset F_1$. Hence, the pole of x in F_2 is a place of degree one. The next theorem describes all functions of

$$R_2 := \cup_{u \geq 0} L(uP_\infty),$$

the ring of regular functions.

Theorem 2.2.2. *For the function field F_2 the following hold:*

1. *The element $\eta := (x-1)y$ has principal divisor $(\eta) = Q_1 + P_0 - Q_\infty - P_\infty$.*

2. The set

$$\mathcal{B}_2 := \{x^i(x-1)\eta^j \mid i \geq 0,\ 0 \leq j \leq q-1\}$$

is a $\mathbb{F}_{q^2}$-basis for

$$R_2 := \cup_{u\geq 0} L(uP_\infty).$$

Proof. We prove the two parts one by one.

1. The principal divisor of η may be easily obtained from Equation 2.2.1 as
$$(\eta) = Q_1 + P_0 - Q_\infty - P_\infty.$$
Hence the first part follows.

2. For the second part, notice that the principal divisor of $(x-1)\eta^j$ is of the form
$$\big((x-1)\eta^j\big) = (j+1)Q_1 + jP_0 + (q-j-1)Q_\infty - (q+j)P_\infty.$$
For $i \geq 0$ and $0 \leq j \leq q-1$, the functions $(x-1)x^i\eta^j$ have poles only at P_∞ of order $(i+1)q+j$. These elements have pole orders in the set
$$H_2 = \{0, q, q+1, \ldots\}.$$
In other words, the set H_2 is the Weierstraß semi-group of P_∞. Only the $q-1$ elements $\{1, \ldots, q-1\}$ are gaps for the infinite place. Notice that genus of F_2 is $q-1$. The affirmation follows by Theorem 1.1.13.

Hence the theorem is proved. ∎

Thus, we have obtained a $\mathbb{F}_{q^2}$-basis for the ring of regular functions from the principal divisors of some functions of F_2. Next we study the function field F_3.

2.2.2 Case $m = 3$

In this section, we analyse the third function field of the tower. The places lying above the zeroes and poles of $x(x-1)$ are studied. The pyramid of function fields up to the third level are given in Figure 2.2. The next lemma gives the principal divisors of coordinate variables.

Lemma 2.2.3. *Let $F_3 = F_2(z)$. The principal divisors of the variables are as follows:*

$$(x) = q^2P_0 - q^2P_\infty$$

$$(y) = qP_0 + q(q-1)P_\infty - q\sum_{i=1}^{q} Q_{\infty i}$$

$$(z) = P_0 + (q-1)P_\infty + (q-1)\sum_{i=1}^{q} Q_{\infty i} - q^2R_\infty.$$

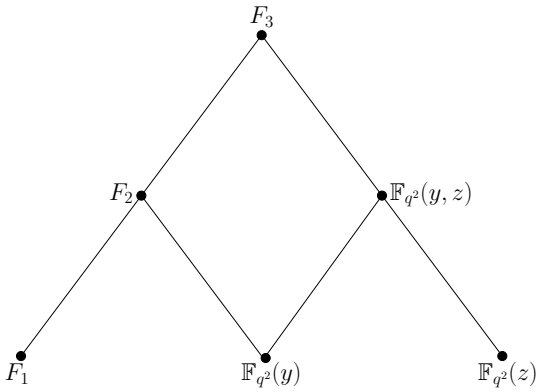

Figure 2.2: *Pyramid of function fields up to third level.*

The following principal divisors may also be easily determined.

$$(x-1) = R_1 + (q-1)R_\infty + (q-1)\sum_{i=1}^{q} Q_{\infty i} - q^2 P_\infty$$

$$(y-1) = qR_1 + q(q-1)R_\infty - q\sum_{i=1}^{q} Q_{\infty i}$$

$$(z-1) = q^2 R_1 - q^2 R_\infty.$$

Proof. The principal divisor of x is easily obtained, since both its zero and pole are totally ramified in F_3/F_2. The same fact again gives the zero divisor of y. The pole of y satisfies Possibility 2.1.5. Using Lemma 2.1.6, this place is unramified in F_3/F_2 and there are q such places denoted by $Q_{\infty i},\ i = 1, \ldots, q$. Thus the principal divisor of y may be obtained. There are two places of F_3 lying above the zero of $x-1$ in F_2. One is R_1, the common zero of $x-1, y-1, z-1$, with ramification index 1 and the other is R_∞, a zero of $y-1$ and a pole of $z-1$ (and of z), with ramification index $q-1$. Hence one obtains the principal divisor of $x-1$. The principal divisor of $y-1$ may also be easily obtained using the above mentioned facts.

The principal divisor of z may be obtained by considering $F_3/K(y,z)$. The common zero of $x-1, y-1, z-1$ is the only zero of $z-1$, which is totally ramified in $F_3/K(y,z)$. The pole of z is also totally ramified in $F_3/K(y,z)$. Hence the lemma. ∎

Ramification behaviour of places which are either zeroes or poles of $x(x-1)$ up to third level are given in Figure 2.3 with their ramification indices. In the next theorem the principal divisors of two useful elements are determined. Some regular functions on F_3 would be described in terms of these elements. This result also indicates how the trace basis-dual basis may be constructed.

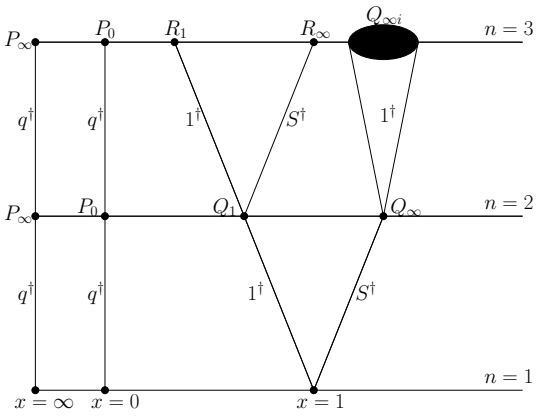

Figure 2.3: *Places up to F_3 lying above zeroes and poles of $x(x-1)$.*

Theorem 2.2.4. *The elements $\alpha := (x-1)y$ and $\beta := (x-1)(y-1)yz$ have principal divisors as follows:*

a. $((x-1)y) = R_1 + qP_0 + (q-1)R_\infty - qP_\infty - \sum_{i=1}^{q} Q_{\infty i}$.

b. $((x-1)(y-1)yz) = (q+1)R_1 + (q+1)P_0 - P_\infty - 2\sum_{i=1}^{q} Q_{\infty i} - R_\infty$.

Proof. The principal divisors follow immediately from the principal divisors of the coordinate variables. ∎

In view of the above lemma, one obtains the following corollary which gives a partial description of the ring of regular functions on F_3.

Corollary 2.2.5. *The elements $(x-1)x^i\alpha^j\beta^k$ for $i \geq 0$ and $0 \leq j, k \leq q-1$ satisfying $j + 2k \leq q-1$ have poles only at P_∞.*

In the next section, the valuations of coordinate variables at various places are calculated.

2.3 Valuations at places

In this section the relationship between valuations of successive coordinate variables at a general place is obtained for F_m. Using this information, valuations of coordinate variables at certain places are calculated for F_m. These results are analogous to those for the Garcia-Stichtenoth tower found in [59].

Let F be the function field $\mathbb{F}_{q^2}(x)(y)$, where x and y satisfy

$$\frac{y-1}{y^q} = \frac{x^q - 1}{x}.$$

Let P be any place of F with the valuation function v_P. At P, the following relation holds

$$\begin{aligned} v_P(y-1) - qv_P(y) &= v_P(x^q - 1) - v_P(x) \\ &= qv_P(x-1) - v_P(x). \end{aligned}$$

First, we observe that only places which are either zeroes or poles of $x(x-1)$ are important. For, let P be such that $v_P(x-1) = v_P(x) = 0$. Under this assumption, one can easily see that $v_P(y) = v_P(y-1) = 0$ holds, as $v_P(y-1) = qv_P(y)$. Thus, enough to consider zeroes and poles of $x(x-1)$. The following cases arise.

Case 2.3.1. *Suppose $v_P(x) = v_P(x-1) < 0$. It is easy to see that $v_P(y) > 0$ and $v_P(y-1) = 0$ is the only possibility, such that*

$$-qv_P(y) = (q-1)v_P(x)$$

holds.

Case 2.3.2. *Suppose $v_P(x) > 0$ so that $v_P(x-1) = 0$. As in the previous case, it is easy to see that $v_P(y) > 0$ and $v_P(y-1) = 0$ is the only possibility, such that*

$$qv_P(y) = v_P(x)$$

holds.

Case 2.3.3. *Suppose $v_P(x-1) > 0$ so that $v_P(x) = 0$. Then, it is easy to see that $v_P(y) = v_P(y-1) < 0$ is one possibility, for which*

$$-(q-1)v_P(y) = qv_P(x-1)$$

holds. The condition that $v_P(y) = 0, v_P(y-1) > 0$ is another possibility, for which

$$v_P(y-1) = qv_P(x-1)$$

holds.

The three cases above (with the third case having two subcases) are tabulated in Table 2.1. This information may be used to calculate the valuation sequence of the successive coordinate variables of the function field F_m of the tower.

Next we obtain the valuations of coordinate variables at some places which are zeroes or poles of $x(x-1)$. Consider the function field F_m of the tower. The unique pole of x_1 is totally ramified in F_m/F_1. This place is a common zero of $x_2, \ldots, x_m$. The valuations at this place are given in the next lemma.

$v_P(x)$	$v_P(x-1)$	$v_P(y)$	$v_P(y-1)$	Relation
<0	<0	>0	$=0$	$-qv_P(y)=(q-1)v_P(x)$
>0	$=0$	>0	$=0$	$qv_P(y)=v_P(x)$
$=0$	>0	<0	<0	$-(q-1)v_P(y)=qv_P(x-1)$
$=0$	>0	$=0$	>0	$v_P(y-1)=qv_P(x-1)$

Table 2.1: *Relationship between valuations of successive coordinate variables*

Lemma 2.3.4. *Let $P=P_\infty$ of F_m, the unique pole of $x_1\in F_m$. Then*

$$v_P(x_1)=-q^{m-1}, v_P(x_2)=(q-1)q^{m-2},\ldots,v_P(x_m)=q-1.$$

There exists a common zero of the functions $x_1-1,\ldots,x_m-1$. This place is unramified in F_m/F_1. The valuations at this place are given in the following lemma.

Lemma 2.3.5. *Let P be the common zero of the functions $x_1-1,\ldots,x_m-1$. Then*

$$v_P(x_1-1)=q^{m-1},\ldots,v_P(x_m-1)=1.$$

There is a unique zero of x_1 in F_m, by Lemma 2.1.3. This place is totally ramified in F_m/F_1. This place is common zero of the functions $x_1,\ldots,x_m$.

Lemma 2.3.6. *Let P be the common zero of the functions $x_1,\ldots,x_m$. Then*

$$v_P(x_1)=q^{m-1}, v_P(x_2)=q^{m-2},\ldots,v_P(x_m)=1.$$

There is a unique pole P of x_m which is totally ramified in $F_m/\mathbb{F}_{q^2}(x_m)$. The valuations of the coordinate variables are given in the next lemma.

Lemma 2.3.7. *Let P be the unique pole of the function x_m. This place is a common zero of $x_1,\ldots,x_{m-1}$. Then*

$$v_P(x_1-1)=q-1, v_P(x_2-1)=(q-1)q,\ldots,v_P(x_m)=-q^{m-1}.$$

Only the poles of $x_2,\ldots,x_{m-1}$ need to be considered for constructing the principal divisors of the coordinate variables. The valuations sequence may be obtained for these places by considering two cases, viz., $1\le t\le (m-1)/2$ and $(m-1)/2<t<m$. This data may be used to construct the principal divisors of $x_1,\ldots,x_m$ and $x_1-1,\ldots,x_m-1$.

2.4 A dual basis for F_m

In this section a trace basis-dual basis pair for the ring of regular functions of F_m is given. Recall the definition of trace dual basis from Proposition 1.1.22.

A basis-dual basis pair for the Garcia-Stichtenoth tower was constructed in [59].

The idea for the construction of a basis-dual basis pair is as follows. For F_m/F_1 the ring $R \subset F_1$ will be taken to be $\mathbb{F}_{q^2}[x_1]$. Then $R' = \mathrm{ic}_{F_m}(R)$ (the integral closure of R) is the ring of functions having poles only at P_∞. We start by considering F_m/F_{m-1}, with $x := x_{m-1}$ and $y := x_m$. The dual basis for the standard basis $\{1, y, \ldots, y^{q-1}\}$ is first constructed using Lemma 1.1.25. Then a basis contained in R' is constructed by multiplying the earlier basis by a constant for the trace map. Finally a basis-dual basis pair as in Theorem 1.1.23 for F_m/F_1 is obtained by taking $m-1$ fold products. The significance of such a pair is that, by Theorem 1.1.23 any regular function can be written as a $\mathbb{F}_{q^2}[x_1]$ linear combination of elements of the dual basis. We begin with the following easy, but useful lemma.

Lemma 2.4.1. *The element $(x_1 - 1)^{q^m} x_m^i \in F_m$ for $0 \leq i \leq q-1$ has poles only at $P_\infty^{(m)}$. Here the place $P_\infty^{(m)}$ denotes the unique pole of x_1 in F_m.*

Proof. The case $m = 2$ has already been dealt in a earlier section. So we assume that $m \geq 3$. We first show that $x_m \in F_m$ has a unique pole.

Let $P \in \mathbb{P}(F_m)$ be a pole of x_m in F_m. Then by [6], the place P is a common zero of $x_1 - 1, \ldots, x_{m-1} - 1$. First consider the contraction of P to F_{m-1}, say P_1. Next consider the contraction of P to $K(x_{m-1}, x_m)$, say P_2.

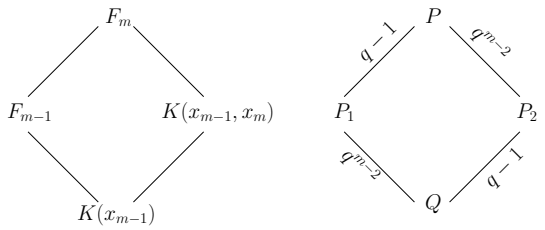

Figure 2.4: *Ramification of pole of x_m.*

We know by Possibility 2.1.4 the common zero of $x_1 - 1, \ldots, x_{m-1} - 1$ is totally ramified in the extension $F_{m-1}/K(x_{m-1})$. The pole of x_m which is a zero of x_{m-1} has ramification index $S = q-1$ in $K(x_{m-1}, x_m)/K(x_{m-1})$. We thus get Figure 2.4, where Q denotes the unique zero of $x_{m-1}-1$ in $K(x_{m-1})$, with the the indices on the arms denoting the ramification indices. Hence, one concludes that x_m has a unique pole. The pole divisor of x_m in F_m is given by

$$(x_m)_\infty = q^{m-1} P.$$

The place P_∞ is the only pole of $x_1 - 1$, which is totally ramified in F_m/F_1. We have already seen that P is a zero of $x_1 - 1$. Hence the lemma. ∎

Let

$$R_n := \cup_{i\geq 0} L(iP_\infty)$$

where P_∞ denotes the unique pole of x_1. Then R_n is the integral closure of $R_1 = \mathbb{F}_{q^2}(x_1)$. We now construct a basis-dual basis pair for F_m. First we look at F_i/F_{i-1} for $2 \leq i \leq m$ with the variables

$$x := x_{i-1} \text{ and } y := x_i$$

satisfying the defining equation of the tower.

Lemma 2.4.2. *For F_i/F_{i-1}, the sets*

$$\{1, y, y^2, \ldots, y^{q-1}\}$$

and

$$\left\{-\left(\frac{x^q-1}{x}\right), -\left(\frac{x^q-1}{x}\right)y, \ldots, -\left(\frac{x^q-1}{x}\right)y^{q-2}, \left(\frac{x^q-1}{x}\right)\left(\frac{y^{q-1}}{y-1}\right)\right\}$$

are a (trace)basis-dual basis pair.

Proof. We first observe that

$$\phi(T) := T^q - \frac{x}{x^q-1}T + \frac{x}{x^q-1}$$

is the minimal polynomial of y over $K(x)$. Since y is a zero of ϕ, we get the following factorisation

$$T^q - \frac{x}{x^q-1}T + \frac{x}{x^q-1} = (T-y)\left(T^{q-1} + yT^{q-2} + \ldots + y^{q-2}T - \frac{y^{q-1}}{y-1}\right).$$

Let ϕ' denote the formal derivative of ϕ. Then

$$\phi'(y) = -\frac{x}{x^q-1}.$$

Take $c_{q-1} = 1, c_{q-2} = y, \ldots, c_0 = -\frac{y^{q-1}}{y-1}$. The result follows by the Lemma 1.1.25. ∎

Observing that, by the defining equation of the tower,

$$\frac{x}{x^q-1} = \frac{y^q}{y-1},$$

we obtain the following corollary.

Corollary 2.4.3. *For F_i/F_{i-1}, the sets*

$$\{1, y, y^2, \ldots, y^{q-1}\} \text{ and } \left\{-\frac{y-1}{y^q}, -\frac{y-1}{y^{q-1}}, \ldots, -\frac{y-1}{y^2}, \frac{1}{y}\right\}$$

are a (trace)basis-dual basis pair.

Next, we use Lemma 2.4.1 so that Theorem 1.1.23 can be applied. In other words, a basis for F_m/F_{m-1} is obtained which has poles only at P_∞. Notice that $x_1 - 1 \in F_1$ which is a constant for the trace map. Hence multiplication by a power of this element multiplies the trace by a constant. We obtain the following corollary.

Corollary 2.4.4. *Let $\rho_i := (x_1 - 1)^{q^i}$ for $i = 2, \ldots, m$. For F_i/F_{i-1}, the sets*

$$\{1, \rho_i y, \rho_i y^2, \ldots, \rho_i y^{q-1}\}$$

and

$$\left\{-\frac{y-1}{\rho_i y^q}, -\frac{y-1}{\rho_i y^{q-1}}, \ldots, -\frac{y-1}{\rho_i y^2}, \frac{1}{\rho_i y}\right\}$$

are a basis-dual basis pair.

The tower is recursively defined and the argument holds for any level. Hence, one can give a dual basis for the ring of regular functions for R_m. This is described below.

Theorem 2.4.5. *Let $\rho_i = (x_1 - 1)^{q^i}$ for $i = 2, \ldots, m$. Let*

$$\mathcal{Z} := \prod_{i=2}^{m} \{1, \rho_i x_i, \rho_i x_i^2, \ldots, \rho_i x_i^{q-1}\}$$

and

$$\mathcal{Z}^* := \prod_{i=2}^{m} \left\{-\frac{x_i - 1}{\rho_i x_i^q}, -\frac{x_i - 1}{\rho_i x_i^{q-1}}, \ldots, -\frac{x_i - 1}{\rho_i x_i^2}, \frac{1}{\rho_i x_i}\right\}$$

be the sets obtaining by taking $m-1$-fold products of the constituent sets. Then

$$\sum_{z \in \mathcal{Z}} R_1 z \subseteq R_m \subseteq \sum_{z^* \in \mathcal{Z}^*} R_1 z^*,$$

where the sums above are finite.

Proof. We have already seen that F_i/F_{i-1} is separable. Clearly the sets $\mathcal{Z}$ and $\mathcal{Z}^*$ are bases of F_m/F_1 which are duals. Notice that each element of $\mathcal{Z}$ is regular at all places except at $P_\infty^{(m)}$, by Lemma 2.4.1. The proof follows by Theorem 1.1.23. ∎

Hence, we have the following corollary.

Corollary 2.4.6. *Any element $\zeta \in F_m$ having poles only at P_∞ can be written as a (finite) sum*

$$\zeta = \sum_{\xi \in \mathcal{Z}^*} a_\xi(x_1)\xi,$$

where a_ξ is a polynomial in x_1.

Remark 2.4.7. *Let $\xi \in \mathcal{Z}^*$. The element ξ may have poles at the zeroes of $x_1 - 1$, zeroes of x_i and poles of $x_i - 1$ for $2 \leq i \leq m$. Thus, the poles of the dual basis are confined to places of F_m lying above the zero of $x_1 - 1$ of F_1.*

2.5 Some concluding remarks

Bezerra and Garcia had introduced a tower with non-Galois steps which attains the Drinfeld-Vladut bound. Such towers are important from coding theory point of view. For, the algebraic geometric codes constructed on such towers attain the best known bounds. Here, the lower level function fields of the Bezerra-Garcia tower of function fields are analysed. A closed form expression of any regular function on the second level is given. Some regular functions on the third level are given. The relationship between valuations of successive coordinate variables at a general place is given for F_m. Using this information, valuations of coordinate variables at certain places are calculated for F_m. A basis-dual basis pair for any function field of the tower is given. The basis is contained in the ring of regular functions of that level, so that any regular function can be written as a linear combination of elements of the dual basis. The next logical step would be to determine the Weierstraß semi-group of the pole of x_1 for any function field. This would aid in the determination of regular functions for any level.

This chapter dealt with the Bezerra-Garcia tower of [6]. In the next chapter we deal with the Garcia-Stichtenoth tower of [26]. Recall that the tower of [6] is a subtower of that from [26]. In the next chapter, some facts about this tower is recalled. Then some regular functions on F_4 and F_5 are constructed. The results use the construction of regular functions on F_3 from [51], to the next levels.

Chapter 3

Construction of regular functions on Garcia-Stichtenoth tower

In [26], Garcia nd Stichtenoth defined a tower of function fields which is optimal. The tower is over a finite field of square cardinality, defined as follows. For $K = \mathbb{F}_{q^2}$,

$$\begin{aligned} F_1 =& K(x_1) \\ F_m =& F_{m-1}(x_m) \end{aligned}$$

where,

$$x_m^q + x_m = \frac{x_{m-1}^q}{x_{m-1}^{q-1} + 1}, \text{ for } m > 1.$$

The first attempts to solve the problem of finding a description for regular functions on this tower were made by Pellikaan in [51]. Bases for Riemann-Roch spaces of the infinite place were constructed for the first three function fields. The construction uses a result proved in the Garcia-Stichtenoth paper [26] to eliminate poles of certain elements at certain places of the function field F_3. The $\xi_3 = x_3 + \frac{x_2^2}{x_1}$ has no poles at any zero of $x_2 - \alpha,\ \alpha \in \Omega^*$. Here

$$\Omega^* = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = 0\} \setminus \{0\}.$$

A full basis is constructed by rearranging the tail terms of a suitable binomial expansion. The construction, due to Pellikaan, is dealt with in Theorem 3.5.5. The same construction is used to give a partial description for the next two levels.

Splitting of places of this tower has been studied by Aleshnikov and others [1]. An algorithm for constructing the required basis on this tower has been discussed by Shum and others [59] for the binary case. This paper tabulated

the principal divisors of all the coordinate variables. The elements of this basis have poles at the infinite place and certain other places above P_0. Each element of the basis is then expanded in series at an unwanted pole Q. The principal part is then dropped from this expansion to obtain an element which is regular at Q. Implementation issues are also discussed in this paper. An upper bound on the overall complexity of the entire process is given in an appendix. Both these methods, ones in [51] and [59], use properties of the tower and hence are applicable only to this tower.

Here, we attempt to carry the programme in [51] forward. In F_3, the regularity properties of ξ_3 is sufficient to give a complete description. We examine the strength of the method when applied to higher level function fields. The basic facts used in the construction are as follows:

- Function field F_m may be considered as a compositum of two copies of F_{m-1}. The basis construction for the constituent function fields has been already carried out.

- Statements regarding the zeroes and poles of elements in lower level function fields carry over to higher function fields. For example, the element $x_4 + \frac{x_3^2}{x_2} \in F_4$ has no poles at any zero of $x_3 - \alpha,\ \alpha \in \Omega^*$. Ramification of the infinite place in the extensions F_m/F_{m-1} and $F_m/\mathbb{F}_{q^2}(x_2, \ldots, x_m)$ has to be taken into account. While the infinite place is totally ramified in the first case, it remains unramified in the second.

In particular, we construct the following elements:

1. first q^2 basis elements and some basis elements in the range q^4 to $q^4 + q^3 - q^2$ for the ring of regular functions on F_4,

2. some basis elements for the ring of regular functions onF_5.

The following is the plan of this chapter. We first recall some basics on the Garcia-Stichtenoth tower from [26]. The ramification behaviour of some places are recalled from [1]. Then Pellikaan's method of finding regular functions for the first three function fields is recalled. Then some regular functions for F_4 and F_5 are constructed.

3.1 The Garcia-Stichtenoth tower

In this section we recollect some properties of the second Garcia-Stichtenoth tower. For detailed proofs refer to [26]. We will follow the convention of [59] while representing the interesting places of the tower.

Definition 3.1.1. *[26] For $K = \mathbb{F}_{q^2}$, the Garcia-Stichtenoth tower is given by*

$$\begin{aligned} F_1 =& K(x_1) \\ F_m =& F_{m-1}(x_m) \end{aligned} \tag{3.1.1}$$

where,

$$x_m^q + x_m = \frac{x_{m-1}^q}{x_{m-1}^{q-1} + 1}, \text{ for } m > 1. \tag{3.1.2}$$

Let us study the lower level function fields in the following two examples.

Example 3.1.2. *The lower level function fields in the tower have been studied in [51]. The first function field is just the rational function field. Let $\Omega = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = 0\}$ and $\Omega^* = \Omega \setminus \{0\}$. In F_1, one has the following principal divisors:*

$$\begin{aligned} (x_1) =& P_0^{(1)} - P_\infty^{(1)} \\ (x_1 - \alpha) =& P_\alpha^{(1)} - P_\infty^{(1)}, \ \alpha \in \Omega^*. \end{aligned} \tag{3.1.3}$$

Example 3.1.3. *Let us consider F_2. Over F_1 consider the equation*

$$X^q + X = \rho,$$

where $\rho = \frac{x_1^q}{x_1^{q-1}+1}$. For ρ, it can be easily seen that $v_{P_\infty^{(1)}}(\rho) = v_{P_\alpha^{(1)}}(\rho) = -1$. By Theorem 1.1.32, we have the following:

1. *The degrees $[F_2 : \mathbb{F}_{q^2}(x_1)] = [F_2 : \mathbb{F}_{q^2}(x_2)] = q$.*
2. *Both $P_\infty^{(1)}$ and $P_\alpha^{(1)}$, $\alpha \in \Omega^*$ are totally ramified in $F_2/\mathbb{F}_{q^2}(x_1)$. Let $P_\infty^{(2)} \in \mathbb{P}(F_2)$ lie above $P_\infty^{(1)} \in \mathbb{P}(F_1)$ and $P_\alpha^{(2)} \in \mathbb{P}(F_2)$ lie above $P_\alpha^{(1)} \in \mathbb{P}(F_1)$, $\alpha \in \Omega^*$. Then each $P_\alpha^{(2)}$, $\alpha \in \Omega^*$ is a pole of $x_2 - \gamma$, $\gamma \in \Omega^*$.*
3. *Now consider $P_0^{(1)}$. The equation $\alpha^q + \alpha = 0$ has q distinct roots. Let the place Q_γ be the unique zero of $x_2 - \gamma$, $\gamma \in \Omega$. Then we have the following principal divisors:*

$$\begin{aligned} (x_1) =& \sum_{\gamma \in \Omega} Q_\gamma - qP_\infty^{(2)}, \\ (x_1 - \alpha) =& qP_\alpha^{(2)} - qP_\infty^{(2)}, \ \alpha \in \Omega^* \text{ and} \\ (x_2 - \gamma) =& qQ_\gamma - P_\infty^{(2)} - \sum_{\alpha \in \Omega^*} P_\alpha^{(2)}, \ \gamma \in \Omega. \end{aligned}$$

The principal divisors of these functions are then used to describe all regular functions over F_2.

In fact, inductively one can discuss the behavior of ramification of the infinite place. The following fact is a consequence of Lemma 1.1.31.

Definition 3.1.4. *Following [26], we define* $T_{i,j} = \mathbb{F}_{q^2}(x_i, \ldots, x_j) \subseteq F_j,\ 1 \leq i \leq j$.

Theorem 3.1.5. *[26] Let* P *be the pole of* $x_1 \in F_m$. *Then* P *is a common pole of* $x_1, \ldots, x_m$. *The place* P *is totally ramified in* $F_m/\mathbb{F}_{q^2}(x_1)$ *and unramified in* $F_m/\mathbb{F}_{q^2}(x_m)$. *Consequently, the place* P *is unramified in* $F_m/T_{2,m}$. *Let* $R \in \mathbb{P}(T_m)$ *be a place which is neither the pole of* x_1 *nor a zero of* $x_1 - \alpha$, *for all* $\alpha \in \Omega$. *Then* R *is unramified in* T_m/T_1.

The following fact about the tower is an easy consequence of Theorem 1.1.32. This fact will be used time and again.

Theorem 3.1.6. *[26] Let* $Q \in \mathbb{P}(F_m)$ *be a zero of* x_1. *Then one has the following possibilities for* Q*:*

A. *The place* Q *is a common zero of* $x_1, \ldots, x_m$

B. *There exists* $t,\ 1 \leq t \leq m$ *such that the place* Q *is a*

- **B1.** *common zero of* $x_1, \ldots, x_t$
- **B2.** *zero of* x_{t+1}
- **B3.** *common pole of* $x_{t+2}, \ldots, x_m$.

In fact, item B2 implies both B1 and B3.

The following theorem helps in computing certain other ramification indices. Using this theorem the pyramid of ramification indices of zero of $x_t - \alpha,\ \alpha \in \Omega^*$ may be completed. This theorem is pivotal for further observations.

Theorem 3.1.7. *[26] For* $1 \leq k \leq t$, *let* $E_k = T_{t+1-k,t+k}$ *and* $H_k = E_k(x_{t+k+1})$. *Suppose* $Q \in \mathbb{P}(H_k)$ *is a zero of* $x_{t+1} - \alpha,\ \alpha \in \Omega^*$. *Then at place* Q *the following holds*

$$x_{t+k+1} = \alpha^{q+1} x_{t+1-k}^{-1} + \mathcal{O}(1)$$

and the place Q *is unramified in the extension* H_k/E_k.

Ramification occurs after a certain level over the place $P_0^{(1)}$.

Theorem 3.1.8. *[26] Let* $Q \in S_1^{(m)} \cup \ldots \cup S_m^{(m)}$ *and* t *be as in Theorem 3.1.7. Then the following hold:*

1. *For* $m \leq 2t + 1$, *the place* Q *is unramified in* F_m/F_{m-1}.

2. *For $2t+1 < m$, the place Q is totally ramified in F_m/F_{2t+1} and for $2t+1 \leq s \leq m$, the restriction of Q to F_s is unramified in $F_s/\mathbb{F}_{q^2}(x_s)$.*

Next, we consider the places R_α, the zero of $x_1 - \alpha,\ \alpha \notin \Omega$.

Theorem 3.1.9. *Let R_α be the zero of $x_1 - \alpha,\ \alpha \notin \Omega$. Then, this place splits completely through out the tower.*

Using Theorems 3.1.5, 3.1.6, 3.1.7 and 3.1.9, the degree of the different may be determined as

$$D_{m+1} = 2(q^2-1)q^m.$$

From here, using Hurwitz genus formula one can determine the genus of each function field in the tower.

After having studied ramification of degree one places one can give a lower bound on the number of places of degree one in each function field. A good estimate for N_m, the number of places of degree one, is sufficient to prove optimality of the tower.

Theorem 3.1.10. *[26] The genus of function fields in the tower is given by*

$$g(F_m) = \begin{cases} \left(q^{\frac{m}{2}} - 1\right)^2, & m \text{ even} \\ \left(q^{\frac{m-1}{2}} - 1\right)\left(q^{\frac{m+1}{2}} - 1\right), & m \text{ odd.} \end{cases}$$

The number of places of degree one satisfies $N(F_m) \geq (q^2-q)q^{m-1},\ m \geq 1$. Hence $\limsup_{m\to\infty} \frac{N(T_m)}{g(T_m)} = q-1$, i.e, the tower attains the Drinfeld-Vlăduţ bound.

3.2 Places of degree one and their ramification

In this section we discuss how the places of degree one are represented. Essentially, the places are grouped according to some common property. The system uses various results of this section. This is the system used in [59]. The essential features of this representation are as follows:

1. The place $P_\infty^{(m)}$ will denote the unique pole of $x_1 \in F_m,\ m \geq 1$.

2. The set of places of F_m lying above $P_\alpha^{(1)},\ \alpha \in \Omega^*$ is denoted by $S_0^{(m)}$. Since each $P_\alpha^{(1)},\ \alpha \in \Omega^*$ is totally ramified throughout the tower, the set $S_0^{(m)}$ contains $q-1$ places.

3. Let $S_1^{(1)} = P_0^{(1)}$. We know that $P_0^{(1)}$ splits completely into q places, each place being the unique zero of $x_2 - \alpha,\ \alpha \in \Omega$. Let $S_1^{(2)}$ be the

set of zeroes of $x_2 - \alpha,\ \alpha \in \Omega^*$ and $S_2^{(2)}$ the unique zero of $x_2 \in F_2$. Inductively, at any level m, let $S_1^{(m)} \cup \ldots \cup S_m^{(m)}$ be the set of places lying above $P_0^{(1)}$. The single place $S_m^{(m)}$ is the unique zero of x_m. Every place in $S_j^{(m)}$ contracts to $S_j^{(j)}$, the unique zero of x_j in $F_j,\ j = 1, \ldots, m$.

Example 3.2.1. *We consider the function field F_3. The principal divisors of the cooordinate variables are given in [51]. Let $\Omega = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = 0\}$ and $\Omega(\beta) = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = \beta^q\}$.*

$$\begin{aligned}
(x_1 - \alpha) =& q^2 P_\alpha - q^2 P_\infty,\ \alpha \in \Omega^* \\
(x_1) =& \sum_{\beta \in \Omega, \gamma \in \Omega(\beta)} Q_{\beta\gamma} - q^2 P_\infty \\
(x_2 - \beta) =& q \sum_{\gamma \in \Omega(\beta)} Q_{\beta\gamma} - q \sum_{\alpha \in \Omega^*} P_\alpha - q P_\infty,\ \beta \in \Omega \\
(x_3 - \gamma_0) =& q^2 Q_{0\gamma_0} - \sum_{\beta \in \Omega^*, \gamma \in \Omega(\beta)} Q_{\beta\gamma} - \sum_{\alpha \in \Omega^*} P_\alpha - P_\infty,\ \gamma_0 \in \Omega.
\end{aligned} \tag{3.2.1}$$

Under the above representation all the places $P_\alpha,\ \alpha \in \Omega^*$ are collected in the set $S_0^{(3)}$, the places $Q_{\beta\gamma},\ \beta \neq 0$ in $S_1^{(3)}$, the places $Q_{0\gamma},\ \gamma \neq 0$ in $S_2^{(3)}$ and the single place Q_{00} in $S_3^{(3)}$.

Thus the various places are represented in a tabular form as in Table 3.1.

	$P_\infty^{(3)}$	$S_0^{(3)}$	$S_1^{(3)}$	$S_2^{(3)}$	$S_3^{(3)}$
x_1	$-q^2$	0	1	1	1
x_2	$-q$	$-q$	0	q	q
x_3	-1	-1	-1	0	q^2
g_1	$-(q-1)q^2$	q^2	0	0	0
g_2	$-(q-1)q$	$-(q-1)q$	q	0	0
g_2	$-(q-1)$	$-(q-1)$	$-(q-1)$	q^2	0
π_1	$-(q^3-q^2)$	q^2	0	0	0
π_2	$-(q^3-q)$	q	q	0	0
π_3	$-(q^3-1)$	1	1	q^2	0

Table 3.1: *Valuation Table for $m = 3$.*

We now consider the next function field in the tower, namely F_4. The principal divisors of elements involving only x_1, x_2 and x_3 may be readily obtained by first considering these as elements of F_3 and studying how the places involved ramify. That is, we use Theorems 3.1.5, 3.1.6, 3.1.7 and 3.1.8. By the structure of the tower, the coordinate variables x_1, x_2 and x_3 have

zeroes at all the zeroes of $x_4 - \alpha,\ \alpha \in \Omega$. The values at these places of x_2 and x_3 may be obtained by considering $F_4/T_{2,4}$. From these, the values at such places of x_1 is obtained. The values of x_4 is may also be obtained by considering the second extension at places other than those in $S_0^{(4)}$. Values of x_4 may be obtained by considering the ramification of the 'infinite place', from Theorem 3.1.5. Thus, the results from the previous sections are used to obtain the principal divisors of certain important functions.

The principal divisors are now tabulated in Table 3.2. The cardinality of the sets of places may also be determined. Of course $P_\infty^{(4)}$ is a single place, the set $S_0^{(4)}$ has $q-1$ places, the set $S_1^{(4)}$ has $q(q-1)$ places, the set $S_2^{(4)}$ has $q(q-1)$ places, the set $S_3^{(4)}$ has $q-1$ elements and the set $S_4^{(4)}$ is a singleton. It becomes more convenient to consider principal divisors in this form. The set of places $S_i^{(4)},\ 0 \leq i \leq 4$ will be considered as if it is a single place, since the elements we consider would behave in the same fashion at each place in a particular set.

	$P_\infty^{(4)}$	$S_0^{(4)}$	$S_1^{(4)}$	$S_2^{(4)}$	$S_3^{(4)}$	$S_4^{(4)}$
x_1	$-q^3$	0	q	1	1	1
x_2	$-q^2$	$-q^2$	0	q	q	q
x_3	$-q$	$-q$	$-q$	0	q^2	q^2
x_4	-1	-1	-1	$-q$	0	q^3
g_1	$-(q-1)q^3$	q^3	0	0	0	0
g_2	$-(q-1)q^2$	$-(q-1)q^2$	q^2	0	0	0
g_3	$-(q-1)q$	$-(q-1)q$	$-(q-1)q$	q^2	0	0
g_4	$-(q-1)$	$-(q-1)$	$-(q-1)$	$-(q-1)q$	q^3	0
π_1	$-(q^4-q^3)$	q^3	0	0	0	0
π_2	$-(q^4-q^2)$	q^2	q^2	0	0	0
π_3	$-(q^4-q)$	q	q	q^2	0	0
π_4	$-(q^4-1)$	1	1	q	q^3	0

Table 3.2: *Table of principal divisors for $m = 4$*

Using various theorems of the previous section one can get a complete picture of all places in F_4. For more details refer to [1].

Let $\xi_3 = x_3 + \frac{x_2^2}{x_1}$ and $\xi_4 = x_4 + \frac{x_3^2}{x_2}$. The function field F_4 may be considered as a compositum of F_3 and $T_{2,4}$, as shown in Figure 3.1, with the assumption that the successive coordinate variables satisfy the defining equation of the tower. The two constituent function fields are essentially the same as F_3.

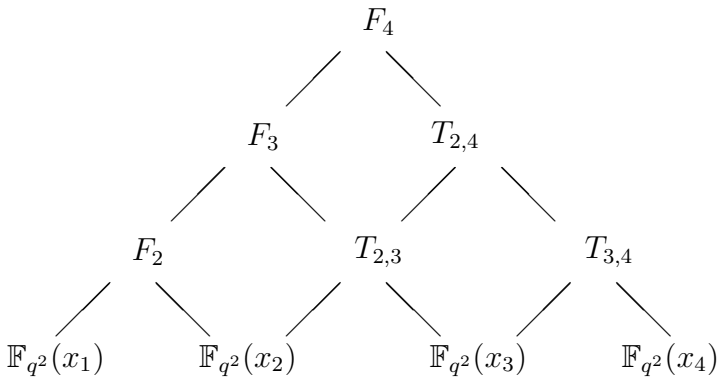

Figure 3.1: *Pyramid of function fields up to F_4*

3.3 Weierstraß semigroups

In this section we mention the known facts about the Weierstraß semigroups of the function fields of the tower. These semigroups have been studied in [53].

Theorem 3.3.1. *[53] For $m \geq 1$ let*

$$c_m = \begin{cases} q^m - q^{\frac{m}{2}}, & m \text{ even}, \\ q^m - q^{\frac{m+1}{2}}, & m \text{ odd}. \end{cases}$$

Let $S_1 = \mathbb{N}_0$ and for $m \geq 1$

$$S_{m+1} = qS_m \cup \{x \in \mathbb{N}_0 \mid x \geq c_{m+1}\}.$$

Then for $m \geq 1$, the Weierstraß semigroup of $P_\infty^{(m)}$, namely H_m, is S_m.

3.4 Construction of spaces $L(D)$

As we have already seen, the Weierstraß semi-group, H_m, of $P_\infty^{(m)}$ has been determined in [53]. In view of the above discussion, it is sufficient to find an explicit element for each of the pole orders in H_m, for each level. Let us recall certain important properties regarding ramification of places in the tower. It is known that the pole of x_1 is totally ramified throughout the tower. Moreover $v_{P_\infty^{(m)}}(x_1) = -q^{m-1}$.

One may consider an inductive strategy for determining bases for one-point divisors. Suppose one element for each non-gap for F_{m-1} is known. Notice the qH_{m-1} part of H_m. For any non-gap $u = u'q \in H_m$, an element with pole order u is available straightaway, namely, the element of H_{m-1} of pole order u'. Thus, enough to consider non-gaps $c_m, c_m + 1, c_m + 2, \ldots$. It

is easy to see that considering non-gaps $c_m, \ldots, c_m + q^{m-1} - 1$ is sufficient, though some non-gaps in this range are of the form $u = u'q$. This is because, an explicit element for higher pole order may be constructed as a product of an element already constructed and a suitable power of x_1. We mention that F_1 is just the rational function field and hence the first non-trivial function field is F_2. In the following sections a solution to Problem 3.4.1 is attempted. Thus, we state the problem formally:

Problem 3.4.1. *For $m > 1$, construct one explicit element for non-gaps $c_m, \ldots, c_m + q^{m-1} - 1$, which is regular at all places except $P_\infty^{(m)}$.*

In [51] this problem is completely solved for the first three function fields of the tower. Let $\Omega = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha + \alpha^q = 0\}$. For F_3, a fact that the element $x_3 + \frac{x_2^2}{x_1}$ has no poles at any zeroes of $x_2 - \alpha,\ \alpha \in \Omega$ is used to construct explicit bases. Here, we explore the possibility of doing something similar for the higher function fields. In fact, we use this construction to the constituent function fields to F_4 to solve this problem. However, this construction, like [51] and [59], is specific to the second tower.

3.5 Construction of basis for $L(uP_\infty^{(m)})$ for lower level function fields

In this section we recall the procedure for basis construction for the function fields on F_1, F_2 and F_3 given in [51]. We use the principal divisors of the cooordinate variables in F_1 and F_2. The results of [51] are summarised in the next theorem. The first two function fields are easy to handle.

Theorem 3.5.1. *[51] Let $F_m,\ m \geq 1$ denote the second Garcia-Stichtenoth tower from [26]. Then the following hold:*

1. *For $m = 1$, the element x_1^u has poles only at $P_\infty^{(1)}$ of order u, $u \geq 0$.*
2. *For $m = 2$, given $u > 0$ one can find positive integers i and j such that the element $(x_1^{q-1} + 1)x_1^i x_2^j$ has poles only at $P_\infty^{(2)}$ of order $u \geq 0$.*

Proof. The function field F_1 is just the rational function field. The principal divisors of x_1 and $x_1 - \alpha,\ \alpha \in \Omega^*$ are given in Example 3.1.2. We know form [53] that the Weierstraß semi-group, H_1, of the infinite place of F_1 is $\mathbb{N}_0$. Thus, the element x_1^u has poles only at $P_\infty^{(1)}$ of order u, $u \geq 0$.

The function field F_2 is obtained by adjoining x_2 to F_1. The principal divisors of coordinate variables are given in Example 3.1.3. The elements $x_2^u,\ u > 0$ has poles at all zeroes of $x_1 - \alpha,\ \alpha \in \Omega^*$. To cancel these poles, we multiply these elements by $x_1^{q-1} + 1$. Hence, the result follows. ∎

We try to solve this problem for higher level function fields in the following sections. The knowledge of principal divisors of coordinate variables is sufficient to give the above description. However, for higher level cases this will not be enough.

After having studied the function fields F_1 and F_2, we now consider F_3. A procedure for basis construction on F_3 has been designed in [51]. Recall that F_3 is obtained by adjoining x_3 to F_2, where x_3 satisfies

$$X^q + X = \frac{x_2^2}{x_2^{q-1} + 1}.$$

We know that $[F_3 : F_2] = q$. Principal divisors of the coordinate variables have already been studied. They are given in Equations 3.2.1. The principal divisors are tabulated in Table 3.1.

The cardinalities of each of the sets in Table 3.1 may be determined. Since the infinite place is totally ramified $P_\infty^{(3)}$ is a single place. The set $S_0^{(3)}$ has $q-1$ places, the set $S_1^{(3)}$ has $q(q-1)$ places, the set $S_2^{(3)}$ has $q-1$ places and the set $S_3^{(3)}$ is a singleton. That the set $S_1^{(3)}$ has $q(q-1)$ places is the subject matter of Theorem 3.5.2.

The pivotal observation is that the element $\xi_3 = \left(x_3 + \frac{x_2^2}{x_1}\right)$ has no poles at any of the zeroes of $x_2 - \beta,\ \beta \in \Omega$. Recall that the set $\Omega = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha + \alpha^q = 0\}$. Hence, the elements $x_2^j \xi_3^k,\ 0 \leq j, k \leq q-1$ have pole at $P_\infty^{(3)}$ of order $0, \ldots, q^2 - 1$ and poles at each $Q \in S_0^{(3)}$. Multiplying these elements with π_1 does not cancel these poles completely. So, these elements are expanded binomially and in this expansion x_2^q is replaced with $-x_2$. We describe the procedure formally.

We know that any $Q \in S_1^{(3)} \cup S_2^{(3)} \cup S_3^{(3)}$ is a zero of $x_2 - \beta,\ \beta \in \Omega$. At such Q, we have the following theorem.

Theorem 3.5.2. *Let R be a zero of $x_2 - \beta \in F_2,\ \beta \in \Omega$, with x_1 as uniformizing parameter. The places lying above R in F_3 are in one-to-one correspondence with the elements of the set $\Omega(\beta)$ consisting of the q distinct solutions of the equation*

$$X^q + X = \beta.$$

Each of these extensions is unramified. At any $Q = Q_{\beta\gamma}$ lying over R we have

$$v_Q(x_2 - \beta) = q$$

and the element

$$\left(x_3 - \frac{\beta^{q+1}}{x_2} - \gamma\right)$$

has a zero at Q. Consequently, one has at Q

$$\left(x_3 - \frac{\beta^{q+1}}{x_2}\right) = \mathcal{O}(1). \tag{3.5.1}$$

Proof. The proof is essentially the same as that of Theorem 3.1.7. Consider the following equalities:

$$\begin{aligned} x_3^q + x_3 =& \frac{x_2^q}{x_2^{q-1}+1} \\ =& x_2^{q+1}\left(\frac{x_1^{q-1}+1}{x_1^q}\right) \\ =& x_2^{q+1}\left(\frac{1}{x_1}+\frac{1}{x_1^q}\right). \end{aligned} \tag{3.5.2}$$

At any Q as in the theorem,

$$\begin{aligned} (x_2^q-\beta)^q + (x_2-\beta) =& x_2^q + x_2 \\ =& \frac{x_1^q}{x_1^{q-1}+1}. \end{aligned} \tag{3.5.3}$$

Therefore,

$$x_2 = \beta + x_1^q + \mathcal{O}(x_1^{2q-1}). \tag{3.5.4}$$

Using Relation 3.5.4 in Equation 3.5.2, we obtain

$$\left(x_3 - \frac{\beta^{q+1}}{x_1}\right)^q + \left(x_3 - \frac{\beta^{q+1}}{x_1}\right) = \beta + \mathcal{O}(x_1^{q-1}). \tag{3.5.5}$$

The assertions now follow by Artin-Schreier Theorem 1.1.32 and the structure of the tower. ∎

The following result is a easy corollary of the above theorem.

Corollary 3.5.3. *Let Q be as in Theorem 3.5.2. Then*

$$v_Q\left(x_3 + \frac{x_2^2}{x_1}\right) \geq 0.$$

Proof. Notice that $\beta^{q+1} = -\beta^2$. Hence, we have at Q

$$\begin{aligned} v_Q\left(x_3 + \frac{x_2^2}{x_1}\right) =& v_Q\left(x_3 + \frac{\beta^2}{x_1} - \frac{\beta^2}{x_1} + \frac{x_2^2}{x_1}\right) \\ =& \min\{v_Q\left(x_3 - \frac{\beta^{q+1}}{x_2}\right), \left(\frac{x_2^2}{x_1} - \frac{\beta^2}{x_1}\right)\} \\ \geq& 0. \end{aligned} \tag{3.5.6}$$

Hence, the corollary. ∎

Thus, $(x_1^{q-1}+1)x_2^j\left(x_3+\frac{x_2^2}{x_1}\right)^k$ have no poles outside P_∞(the common pole of x_1, x_2 and x_3) if $j+2k \leq q$. Now, this expression is expanded binomially and the tail terms are rearranged by replacing x_2^q by $-x_2$. Recall that, the coordinate variables x_1 and x_2 are related by the defining equation of the tower. Now we claim that these elements indeed work. Before going into the proof, we describe formally what we have done.

Set $e(0,j) = j$ and $e(i,j) \in \{1,\ldots,q-1\}$ be the integer congruent to $(2i+j) \mod (q-1)$, for $i>0$. Let $c(i,j) = (-1)^{\lfloor \frac{2i+j-1}{q-1} \rfloor}$.

Definition 3.5.4. *The function $f_{jk} \in F_3$ is defined as*

$$f_{jk} = \sum_{i=0}^{k} \binom{k}{i} c(i,j) \frac{x_2^{e(i,j)}}{x_1^i} x_3^{k-i}.$$

It is readily seen that these elements are obtained as described before. We now go on to prove the claim. This has been done already in [51].

Theorem 3.5.5. *Given $u \geq 0$ a pole number, one can find positive integers $0 \leq j,k \leq q-1$, $i \geq 0$ such that the element $(x_1^{q-1}+1)x_1^i f_{jk}$ has its only pole at P_∞ of order u.*

Proof. It is easy to see that $\beta^{2i+j} = c(i,j)\beta^{e(i,j)}$ and $c(i,j)x_2^{e(i,j)} = \beta^{2i+j} + \mathcal{O}(x_1^q)$. Enough to investigate the behavior of these elements at places P_∞, P_α, $\alpha \in \Omega^*$ and $Q_{\beta\gamma}$. Let $Q = Q_{\beta\gamma}$, $\beta \in \Omega, \gamma \in \Omega(\beta)$. Then clearly $v_Q(x_1^{q-1}+1) \geq 0$. Consider the following equations at $Q_{\beta\gamma}$:

$$\begin{aligned}
x_1^k f_{jk} =& \sum_{i=0}^{k} \binom{k}{i} c(i,j) x_2^{e(i,j)} (x_1x_3)^{k-i}, \text{ by definition} \\
=& \sum_{i=0}^{k} \binom{k}{i} \beta^{2i+j} (x_1x_3)^{k-i} + \mathcal{O}(x_1^q), \text{ as noted earlier} \\
=& x_2^j \sum_{i=0}^{k} \binom{k}{i} \beta^{2i} (x_1x_3)^{k-i} + \mathcal{O}(x_1^q), \text{ Equation 3.5.1} \\
=& x_2^j \left(x_1x_2+\beta^2\right)^k + \mathcal{O}(x_1^q), \text{ by binomial theorem} \\
=& \mathcal{O}(x_1^k), \text{ by Theorem 3.5.2,}
\end{aligned}$$

which show that $v_Q(f_{jk}) \geq 0$.

Let $Q = P_\alpha$, $\alpha \in \Omega^*$. For $i \leq k \leq q-1$ and $j \leq q-1$

$$v_Q\left(\frac{x_2^{e(i,j)}}{x_1^i} x_3^{k-i}\right) = -e(i,j)q - (k-i) \geq -(q-1)q - (q-1) = -q^2+1.$$

But $(x_1^{q-1}+1)$ has a zero of order q^2 at Q.

Let $Q = P_\infty$. For $1 \leq i \leq k \leq q-1$ and $j \leq q-1$

$$v_Q\left(\frac{x_2^{e(i,j)}}{x_1^i}x_3^{k-i}\right) = -e(i,j)q - (k-i) + iq^2 \geq -(q-1)q - (q-1) + q^2 = 1.$$

If $i = 0$, then

$$v_Q\left(\frac{x_2^{e(i,j)}}{x_1^i}x_3^{k-i}\right) = -(jq+k).$$

Moreover $v_Q(x_1^{q-1}+1) = -(q^3-q^2)$. Hence the theorem. ∎

Thus, an element can be explicitly given for each pole order in the Weierstraß semigroup at the infinite place of F_3. We use this construction for constructing some regular elements for F_4 in the next section. Before we end, we illustrate this construction with two examples given in [51]. These examples will be continued in the next section.

Example 3.5.6. *Let $q = 2$. Then $c_3 = 4$. Thus, we need to construct an explicit element for non-gaps $4, \ldots, 7$. Notice that $g_1 = x_1 + 1$. These elements are given below:*

$$g_1 \times \begin{cases} 1, x_3 + \frac{x_2}{x_1}, \\ x_2, x_2x_3 + \frac{x_2}{x_1}. \end{cases}$$

This gives a complete description of the regular functions for this case.

Example 3.5.7. *Let $q = 3$. Then $c_3 = 18$. Thus, we need to construct an explicit element for non-gaps $18, \ldots, 26$. Notice that $g_1 = x_1^2 + 1$. These elements are given below:*

$$g_1 \times \begin{cases} 1, x_3 + \frac{x_2^2}{x_1}, x_3^2 - \frac{x_2^2x_3}{x_1} - \frac{x_2^2}{x_1^2}, \\ x_2, x_2x_3 - \frac{x_2}{x_1}, x_2x_3^2 - \frac{2x_2x_3}{x_1} + \frac{x_2}{x_1^2}, \\ x_2^2, x_2^2x_3 - \frac{x_2^2}{x_1}, x_2^2x_3^2 - \frac{2x_2^2x_3}{x_1} + \frac{x_2^2}{x_1^2}. \end{cases}$$

This gives a complete description of the regular functions for this case.

3.6 Construction of basis for $L(uP_\infty^{(m)})$ on F_4

We begin this section by illustrating the basis construction for the function field F_4 with $q = 2$. This example is continued from the previous section. Some results from the previous section are also used.

Example 3.6.1. *Let $q = 2$. We know that $[F_4 : F_1] = q^3 = 8$. Moreover $c_4 = q^4 - q^2 = 12$ and $v_{P_\infty^{(4)}}(x_1) = -q^3 = -8$. We need to construct an explicit element for each of the non-gaps $12, \ldots, 19$.*

First consider $T_{2,4} = \mathbb{F}_{q^2}(x_2, x_3, x_4)$. We have already seen that F_4 is a compositum of F_3 and $T_{2,4}$. Moreover, the fields F_3 and $T_{2,4}$ are isomorphic. Hence Pellikaan's construction for F_3 may be applied to $T_{2,4}$ to obtain elements

$$g_2 \times \begin{cases} 1, x_4 + \frac{x_3}{x_2}, \\ x_3, x_3x_4 + \frac{x_3}{x_2}. \end{cases}$$

But the above elements have poles at all $S_0^{(4)}$ apart from $P_\infty^{(4)}$. This is because, the pole of x_2 in $T_{2,4}$ remains unramified in $F_4/T_{2,4}$. It is easy to see that elements with pole orders $12, \ldots, 15$ may be obtained by multiplying these elements with g_1. These elements are listed below:

$$\pi_2 \times \begin{cases} 1, x_4 + \frac{x_3}{x_2}, \\ x_3, x_3x_4 + \frac{x_3}{x_2}. \end{cases}$$

Thus the non-gaps $16, \ldots, 19$ remain. We start by considering the element

$$\eta = x_4 + \frac{\left(x_3 + \frac{x_2^2}{x_1}\right)^2}{x_2} = x_4 + \frac{x_3^2}{x_2} + \frac{x_2^3}{x_1^2}.$$

In η, we replace x_2^2 with x_2 to obtain:

$$\eta' = x_4 + \frac{x_3^2}{x_2} + \frac{x_2}{x_1^2}.$$

It is easy to obtain the following structures of principal divisors for $x_3 + \frac{x_2}{x_1}$ and $x_4 + \frac{x_3^2}{x_2}$ as elements of F_4:

$$\left(x_3 + \frac{x_2}{x_1}\right) = -qP_\infty^{(4)} - q^2 \sum_{Q \in S_0^{(4)}} Q + \mathcal{A},$$

$$\left(x_4 + \frac{x_3^2}{x_2}\right) = -P_\infty^{(4)} - \sum_{Q \in S_0^{(4)}} Q - 2q \sum_{Q \in S_1^{(4)}} Q + \mathcal{B},$$

where $\mathcal{A}$ and $\mathcal{B}$ are positive divisors. Notice that we haven't determined the zero divisors exactly. It is not important for our construction. From the principal divisor of $x_4 + \frac{x_3^2}{x_2}$, one can immediately see that η' has a pole of order one at $P_\infty^{(4)}$ and poles of order q^2 at each $Q \in S_0^{(4)}$. It is easy to see that

$$x_4 + \frac{x_3^2}{x_2} + \frac{x_2}{x_1^2} = x_4 + \frac{\left(x_3 + \frac{x_2}{x_1}\right)^2}{x_2}.$$

The element $\left(x_3 + \frac{x_2}{x_1}\right)$ *does not have any poles at* $Q \in S_1^{(4)}$. *Consequently* η' *has a pole of order* 1 *at every* $Q \in S_1^{(4)}$. *From this discussion we get the structure of principal divisor of* η'*:*

$$(\eta') = -P_\infty^{(4)} - q^2 \sum_{Q \in S_0^{(4)}} Q - \sum_{Q \in S_1^{(4)}} Q + \mathcal{A},$$

where $\mathcal{A} \succeq 0$. *The element* $\pi_1 x_1$ *has principal divisor of the form*

$$(\pi_1 x_1) = -q^4 P_\infty^{(4)} + q^3 \sum_{Q \in S_0^{(4)}} Q + q \sum_{Q \in S_1^{(4)}} Q + \sum_{Q \in S_2^{(4)} \cup S_3^{(4)} \cup S_4^{(4)}} Q.$$

Hence the elements for the non-gaps $16, \ldots, 19$ *are obtained as follows:*

$$\pi_1 x_1 \times \begin{cases} 1, \eta', \\ x_3 + \frac{x_2}{x_1}, \left(x_3 + \frac{x_2}{x_1}\right)\eta'. \end{cases}$$

This completes basis construction for F_4 *with* $q = 2$.

We now consider general q. The programme carried out for F_3 when implemented over $T_{2,4}$ gives some regular functions for F_4. Recall that F_3 and $T_{2,4}$ are isomorphic function fields. But these functions don't give a complete description. Hence, the complete description is given in two steps. In the first step, the result for $T_{2,4}$ is lifted to F_4 and in the second the functions ξ_3 and ξ_4 are composed suitably to obtain η to complete the description. But the ramification behavior of the infinite place in F_4/F_3 and $F_4/T_{2,4}$ are different. While the infinite place is totally ramified in the first case, it remains unramified in the second, by Theorem 3.1.5. One has to take this into account while analysing $F_4/T_{2,4}$. The details are given below.

We will for a while work in $T_{2,4}$. The construction of bases here follows verbatim the F_3 case, which has already been dealt with in [51]. The pivotal observation is that the element ξ_4 has no poles at zeroes of $x_3 - \beta,\ \beta \in \Omega^*$. Let $\Omega = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = 0\}$ and $\Omega(\beta) = \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = \beta^q\}$. As a consequence, as in [51], we have the following result.

Set $e(0, j) = j$ and $e(i, j) \in \{1, \ldots, q-1\}$ be the integer congruent to $(2i + j) \mod (q-1)$, for $i > 0$. Let $c(i, j) = (-1)^{\lfloor \frac{2i+j-1}{q-1} \rfloor}$.

Theorem 3.6.2. *The function* $h_{jk} \in T_{2,4}$ *is defined as*

$$h_{jk} = \sum_{i=0}^{k} \binom{k}{i} c(i, j) \frac{x_3^{e(i,j)}}{x_2^i} x_4^{k-i}.$$

Given $u \geq 0$, *one can find positive integers* $0 \leq j, k \leq q-1,\ i \geq 0$ *such that the element* $(x_2^{q-1} + 1)x_2^i h_{jk}$ *has its only pole at* P_∞, *the common pole of* x_2, x_3 *and* x_4, *of order* u.

We would consider functions in the above theorem with $i = 0$, i.e., the first q^2 elements. These elements may be considered as elements of F_4. But as mentioned earlier, the common pole P of x_2, x_3 and x_4 in $T_{2,4}$ remains unramified in $F_4/T_{2,4}$. That is,

$$\mathrm{con}_{F_4/T_{2,4}}(P) = P_\infty^{(4)} + \sum_{Q \in S_0^{(4)}} Q$$

By splitting of infinite place, all these functions would have poles at each of the places in $S_0^{(4)}$ in addition to $P_\infty^{(4)}$. Already we have $v_{P_\infty^{(4)}}((x_2^{q-1}+1)h_{jk}) = -(q^3-q^2)-qj-k$. Multiplying these functions by $(x_1^{q-1}+1)$ to cancel the additional poles, we obtain $v_{P_\infty^{(4)}}(\pi_2 h_{jk}) = -(q^4-q^3)-(q^3-q^2)-qj-k = -(q^4-q^2)-qj-k$. Thus we have the following theorem.

Theorem 3.6.3. *The functions $\pi_2 h_{jk} \in F_4$ have their unique pole at $P_\infty^{(4)}$ of order $(q^4-q^2)+qj+k,\ 0 \le j,k \le q-1$.*

Proof. Enough to prove that each $\pi_2 h_{jk}$ has no pole at every $Q \in S_0^{(4)}$. We have,

$$v_Q(x_2^{-i} x_3^{e(i,j)} x_4^{k-i}) = iq^2 - e(i,j)q - (k-i).$$

If $i = 0$, then $v_Q(x_3^j x_4^k) = -(qj+k) \ge -(q^2-1)$. On the other hand for $i \ge 1$, we have $v_Q(x_2^{-i} x_3^{e(i,j)} x_4^{k-i}) \ge 1$. But π_2 has zero of order q^2 at the place Q. That completes the proof of the theorem. ∎

To complete the description one needs to describe elements having pole orders q^4+1 through $q^4-q^2+q^3$. Let $\eta = x_4 + \frac{\xi_3^2}{x_2}$. Then

$$\eta = \xi_4 + \frac{(\xi_3+x_3)x_2}{x_1} = x_4 + \frac{x_3^2}{x_2} + \frac{x_2^3}{x_1^2} + \frac{2x_2x_3}{x_1}.$$

Clearly $v_Q(\eta) = -1,\ Q \in P_\infty^{(4)} \cup S_1^{(4)}$ and $v_Q(\eta) = -3q^2,\ Q \in S_0^{(4)}$.

Lemma 3.6.4. *Let $Q \in S_2^{(4)}$. Then $v_Q(\eta) \ge 0$.*

Proof. Let $Q \in S_2^{(4)}$. Then the following hold:

$$\begin{aligned} v_Q(\eta) =& v_Q\left(x_4 + \frac{x_3^2}{x_2} + \frac{x_2^3}{x_1^2} + \frac{2x_2x_3}{x_1}\right) \\ \ge& \min\{v_Q(\xi_4), 3q-2, q-1\} \\ \ge& 0. \end{aligned}$$

The last inequality above is due to the fact that $\xi_4 \in T_{2,4}$ has no poles at zeroes of $x_3 - \alpha,\ \alpha \in \Omega^*$ and $Q \in S_2^{(4)}$ lies above such a place. ∎

The following is an easy consequence of the above theorem.

Theorem 3.6.5. *The functions* $(x_1^{q-1}+1)x_1x_2^l\xi_3^j\eta^k \in F_4$ *have poles only at* $P_\infty^{(4)}$ *if* $l+2j+3k \leq q-1$ *holds for* $0 \leq j,k \leq q-1,\ 0 \leq l \leq q-2$.

But, we don't get a complete description for such l, j and k from the above theorem. It remains to be explored whether a complete description may be obtained by expanding binomially the functions $x_2^l\xi_3^j\eta^k$ and rearranging the tail terms suitably. Notice that for the first half of the description it was enough to restrict to $T_{2,4}$. However, for the second part one has to work in full F_4.

3.7 Construction of basis for $L(uP_\infty^{(m)})$ on F_5

Let us now consider F_5. We would make statements which hold for general q. By arguing as in the four case the principal divisors of various functions may be determined. The principal divisors of standard functions in F_m are tabulated in Table 3.3. As before, the sets of places would be treated as if they are single places. Let us recall that we proved regularity properties of an

	$P_\infty^{(5)}$	$S_0^{(5)}$	$S_1^{(5)}$	$S_2^{(5)}$	$S_3^{(5)}$	$S_4^{(5)}$	$S_5^{(5)}$
x_1	$-q^4$	0	q^2	1	1	1	1
x_2	$-q^3$	$-q^3$	0	q	q	q	q
x_3	$-q^2$	$-q^2$	$-q^2$	0	q^2	q^2	q^2
x_4	$-q$	$-q$	$-q$	$-q$	0	q^3	q^3
x_5	-1	-1	-1	-1	$-q^2$	0	q^4
g_1	$-(q-1)q^4$	q^4	0	0	0	0	0
g_2	$-(q-1)q^3$	$-(q-1)q^3$	q^3	0	0	0	0
g_3	$-(q-1)q^2$	$-(q-1)q^2$	$-(q-1)q^2$	q^2	0	0	0
g_4	$-(q-1)q$	$-(q-1)q$	$-(q-1)q$	$-(q-1)q$	q^3	0	0
g_5	$-(q-1)$	$-(q-1)$	$-(q-1)$	$-(q-1)$	$-(q-1)q^2$	q^4	0
π_1	$-(q^5-q^4)$	q^4	0	0	0	0	0
π_2	$-(q^5-q^3)$	q^3	q^3	0	0	0	0
π_3	$-(q^5-q^2)$	q^2	q^2	q^2	0	0	0
π_4	$-(q^5-q)$	q	q	q	q^3	0	0
π_5	$-(q^5-1)$	1	1	1	q^2	q^4	0

Table 3.3: *Principal Divisors of Some Functions in* F_5

element ξ_3 in F_3. However, we did not determine the exact principal divisor of the element. The set of all zeroes of the element was not determined. That will not be needed for our construction as long as we don't divide by ξ_3. The crux of the matter is that, it is sufficient to determine the poles of such elements. We use the properties of discrete valuations to determine the poles of some functions. Here, the notation $\geq val$ is used to indicate that the value at the place or at each place in the set is at least val.

We again consider F_5 as a compositum of F_4 and $T_{2,5}$. Recall that $T_{2,5}$ is isomorphic to F_4. We then use regular functions constructed on F_4 to

construct regular functions on F_5. However, we don't get the first q^2 regular functions as in F_5. This issue will require a separate treatment.

Theorem 3.7.1. *Let us consider regular functions for $T_{2,5}$ with pole orders $q^4-q^2,\ldots,q^4$. Regular functions for F_5 of pole orders $q^5-q^2,\ldots,q^5$ may be obtained by multiplying the above functions with g_1.*

Proof. The main fact we use here, again, is the ramification of infinite place:

$$con_{F_5/T_{2,5}} = P_\infty^{(5)} + \sum_{Q\in S_0^{(5)}} Q.$$

The regular functions in $T_{2,5}$ of pole orders $q^4-q^2,\ldots,q^4$, when considered as elements of F_5, would have poles of same order at each $Q\in S_0^{(5)}$. But the principal divisor of g_1 from Table 3.3 is

$$(g_1) = -(q^5-q^4)P_\infty^{(5)} + q^4\sum_{Q\in S_0^{(5)}} Q.$$

Thus, multiplying these elements with g_1 would cancel each pole at $Q\in S_0^{(5)}$ and the pole orders at $P_\infty^{(5)}$ of the resulting elements would be $q^5-q^2,\ldots,q^5$. Hence the result. ∎

We start by proving the following simple lemma.

Lemma 3.7.2. *The following statements hold for elements in F_5:*

1. *The principal divisor of the element $\eta_1 = x_5 + \frac{\xi_4^2}{x_3} + \frac{x_3^2}{x_1} \in F_5$ is of the form*
$$(\eta_1) = -P_\infty^{(5)} - 2q^2\sum_{Q\in S_0^{(5)}} Q - \sum_{Q\in S_1^{(5)}} r_Q Q + \mathcal{A},$$
where $r_Q \geq -3q^2$ are integers and $A \succeq 0$.

2. *The principal divisor of the element $\eta_2 = \xi_5 + \frac{\xi_3\left(x_4+x_4+\frac{\xi_3^2}{x_2}\right)}{x_2} \in F_5$ is of the form*
$$(\eta_2) = -P_\infty^{(5)} - 4q^3\sum_{Q\in S_0^{(5)}} Q - \sum_{Q\in S_1^{(5)}} r_Q Q + \mathcal{B},$$
where $r_Q \geq -q$ are integers and $B \succeq 0$.

Proof. The prove the two parts one by one.
1. First consider $x_5 + \frac{\xi_4^2}{x_3} \in T_{2,5}$. The principal divisor of this element has been already calculated in the four case. As an element of F_5 this has a principal divisor of the form

$$\left(x_5 + \frac{\xi_4^2}{x_3}\right) = -P_\infty^{(5)} - \sum_{Q \in S_0^{(5)}} Q - 3q^2 \sum_{Q \in S_1^{(5)}} Q - \sum_{Q \in S_2^{(5)}} Q + \mathcal{C},$$

where $\mathcal{C} \succeq 0$. Notice also that $\frac{\xi_4^2}{x_3} \in F_5$ has no poles at any $Q \in S_2^{(5)}$. By Theorem 3.1.7 the element $x_5 + \frac{x_3^2}{x_1}$ has no poles at any $Q \in S_2^{(5)}$. Hence $x_5 + \frac{\xi_4^2}{x_3} + \frac{x_3^2}{x_1} \in F_5$ has principal divisor of above mentioned form.
2. Let us now consider the second element. It is easy to see that the principal divisor of this element is of the form

$$(\eta_2) = -P_\infty^{(5)} - 4q^3 \sum_{Q \in S_0^{(5)}} Q - \sum_{Q \in S_1^{(5)}} r_Q Q + \sum_{Q \in S_2^{(5)}} s_Q Q + \mathcal{B},$$

where $r_Q \geq -q$ and $s_Q \geq -2q$ are integers and $B \succeq 0$.

We claim that each $s_Q \geq 0$. For this we rewrite the element η_2 as

$$\begin{aligned}
\eta_2 =& x_5 + \frac{x_4^2}{x_3} + \frac{\xi_3\left(x_4 + x_4 + \frac{\xi_3^2}{x_2}\right)}{x_2} \\
=& x_5 + \frac{x_4^2}{x_3} + \frac{\left(2x_2x_3x_4 + x_3^3 + \frac{x_3x_2^4}{x_1^2} + \frac{2x_2^2x_3^2}{x_1} + \frac{2x_2^3x_4}{x_1} + \frac{x_2^2x_3^2}{x_1} + \frac{x_2^6}{x_1^3} + \frac{2x_2^4x_3}{x_1^2}\right)}{x_2^2} \\
=& x_5 + \frac{x_3^2}{x_1} + \left(\frac{x_4^2}{x_3} + \frac{2x_3x_4}{x_2} + \frac{x_3^3}{x_2^2}\right) + \left(\frac{2x_3^2}{x_1} + \frac{2x_2x_4}{x_1}\right) \\
&+ \left(\frac{x_2^2x_3}{x_1^2} + \frac{x_2^4}{x_1^3} + \frac{2x_2^2x_3}{x_1^2}\right) \\
=& x_5 + \frac{x_3^2}{x_1} + \frac{\xi_4^2}{x_3} + \frac{2x_2\xi_4}{x_1} + \frac{x_2^2\left(2x_3 + \xi_3\right)}{x_1^2}.
\end{aligned}$$

Notice that the element $\frac{\xi_4^2}{x_3} + \frac{2x_2\xi_4}{x_1} + \frac{x_2^2(2x_3+\xi_3)}{x_1^2}$ has no poles at any $Q \in S_2^{(5)}$. Moreover $x_5 + \frac{x_3^2}{x_1} \in F_5$ has no poles at any $Q \in S_2^{(5)}$ by Theorem 3.1.7. Hence η_2 has principal divisor as mentioned. ∎

As in the four case, the description proceeds in two stages. The following theorem is an easy consequence of the above lemma and some other earlier results.

Theorem 3.7.3. *1. The elements $\pi_2 x_3^l \xi_4^j \eta_1^k$, where $0 \leq l, j, k \leq q-1$ have poles only at $P_\infty^{(5)}$ if $lq^2 + jq + 2kq^2 \leq q^3$ and $lq^2 + 2jq^2 + 3kq^2 \leq q^3$ hold simultaneously.*

2. *Similarly, the elements* $\pi_1 x_1 x_2^n \xi_3^l \left(x_4 + \frac{\xi_3^2}{x_2}\right)^j \eta_2^k$, *where* $0 \leq n \leq q-2$ *and* $0 \leq l, j, k \leq q-1$ *have poles only at* $P_\infty^{(5)}$ *if* $nq^3+2lq^3+3jq^3+4kq^3 \leq q^4$ *and* $jq + kq \leq q^2$ *hold simultaneously.*

However, the above theorem does not give functions for each pole order. In the first stage q^3 elements are obtained by rewriting the tail terms of the binomial expansion of $x_3^l \xi_4^j \eta_1^k$, where $0 \leq l, j, k \leq q-1$. It remains to be explored whether the remaining basis elements are obtained by suitably rewriting the binomial expansion of $x_2^n \xi_3^l \left(x_4 + \frac{\xi_3^2}{x_2}\right)^j \eta_2^k$, where $0 \leq n \leq q-2$ and $0 \leq l, j, k \leq q-1$.

3.8 Some concluding remarks

Thus, we have constructed here

1. first q^2 basis elements and some basis elements in the range q^4 to $q^4 + q^3 - q^2$ for F_4,
2. some basis elements for F_5.

But the descriptions obtained for F_4 and F_5 are not complete. Whether Theorem 3.1.7 is enough to give a complete description of regular functions similar to F_3 remains to be explored.

The next three chapters deal with the various steps involved in list decoding of one-point codes. The fourth chapter studies construction of an interpolation polynomial for list decoding one-point codes on Garcia-Stichtenoth tower using Gröbner basis. The fifth chapter deals with the construction of the non-uniform input required for list decoding codes on Bezerra-Garcia tower. The procedure is similar to that in [32]. The sixth chapter deals with the disambiguation problem from [30].

Chapter 4

List decoding codes on Garcia-Stictenoth tower using Gröbner basis

Towers of function fields which attain the Drinfeld-Vlăduţ bound are interesting from coding theory perspective. In Garcia and Stichtenoth [26] second explicit example of a tower of function fields was given which attains the above bound. The Weierstraß semi-group of the infinite place is known. Construction of the Riemann-Roch spaces $L(uP_\infty^{(m)})$ was dealt with by Shum and others in [59].

Much work has been done on list decoding of one-point codes constructed on function fields. List decoding algorithm for such one-point codes was given in [34]. The algorithm is a interpolate and root-find strategy. A polynomial over the underlying function field is found which 'passes through' the points $(P_1, y_1), \ldots, (P_1, y_1)$ with a multiplicity. Conditions are imposed on the coefficients so that one such polynomial may be found and the sent message is an element of the output list. The roots of the interpolation polynomial are known to be elements of $L(D)$ for a suitable divisor D. This data may be used to design efficient root finding algorithms over function fields. In [35] the authors discuss a suitable representation of the function field elements which aids in efficient list decoding.

Here, we discuss how the interpolation step of list decoding of codes over Garcia-Stictenoth tower may be performed. In [48], an algorithm for recursive computation of Gröbner basis is given. For mode details on this topic, refer to [11] and [17]. For a polynomial ring A, congruence of the form

$$H^{(k)}(b) \equiv 0 \bmod M^{(k)},\ k = 1, \ldots, p$$

where $b \in A^q$ and $M^{(k)}$ are A-modules with functions $H^{(h)},\ k = 1, \ldots, p$ are solved using a recursive computation. The functions are such that the the set of solutions forms a submodule of M. The interpolation step of

the list decoding algorithm may be reduced to such a problem, so that this algorithm may be applied. The main observation is that the set of solutions that satisfy the zero multiplicity condition form a submodule of a free module over a polynomial ring of one variable. A solution is found as the minimal element of a Gröbner basis with respect to a suitable term order.

The root-find step may be reduced to solving a set of linear equations by going modulo a large degree place. The large place is represented as a tuple of evaluations at the coordinate variables. Then the reduced equation is solved over a large finite field and the roots are lifted to the roots of the original polynomial. Places of large degree may be found for the tower by solving a system of equations. Thus, the root-find step is reduced to root-finding over finite fields and solving a system of linear equations.

After recalling some basic facts about list decoding of one-point codes and about the tower, an account of the interpolation and the root-finding steps of list decoding of one point codes is given. The results reported in this chapter appear in [13].

4.1 Regular functions on Garcia-Stichtenoth tower

We study regular functions on the function fields of the tower in [26]. We recall the pole cancellation algorithm described in [59] for finding a $\mathbb{F}_{q^2}$ basis for $L(uP_\infty^{(m)})$. The algorithm outputs a basis for $L(uP_\infty^{(m)})$ and its evaluation at code places.

Definition 4.1.1. *Let* $\mathcal{E} = \{(e_2, \ldots, e_m) \mid 0 \leq e_2, \ldots, e_m \leq q-1\}$. *Let* $\mathcal{E}_1$ *and* $\mathcal{E}_2$ *be the set of* $m-1$*-tuples from* $\mathcal{E}$ *satisfying*

$$\sum_{j=2}^{m} q^{m-j} e_j + q^{m-1} + \cdots + q \leq 2q^{m-1}$$

$$\sum_{j=2}^{m} q^{m-j} e_j + q^{m-1} + \cdots + q > 2q^{m-1}$$

respectively.

The algorithm uses the expression of regular functions as a linear combination of the quasi-regular functions. Each summand in the theorem below is called *quasi-regular*.

Theorem 4.1.2. *Every function, whose poles are confined to the infinite place has an expression of the form*

$$x_1^l \left(\sum_{e_1=0}^{(m-2)q+1} \sum_{e \in \mathcal{E}_1} c_e g_1 \frac{x_1^{e_1} \cdots x_m^{e_m}}{\pi_2 \cdots \pi_{m-1}} \right) + x_1^l \left(\sum_{e_1=0}^{(m-2)q+1} \sum_{e \in \mathcal{E}_2} c_e g_1^2 \frac{x_1^{e_1} \cdots x_m^{e_m}}{\pi_2 \cdots \pi_{m-1}} \right),$$

where $l \geq 0$ *and* $c_e \in \mathbb{F}_{q^2}$.

The unwanted poles are cancelled using the expansion of these quasi-regular functions at these places. Implementation issues such as power series computation are discussed in [59]. An upper bound on the complexity of the algorithm in terms of the number of finite field operations is given there.

4.2 Gröbner basis for modules

In this section, following [48], we recall very few preliminaries about Gröbner basis of modules. Let $A = k[x] = k[x_1, \ldots, k_{x_n}]$. A *monomial order* on A is a total order $>$ on the set of monomials $\{x^\alpha \mid \alpha \in \mathbb{N}_0^n\}$ which is multiplicative:

$$x^\alpha > x^\beta \Rightarrow x^\alpha x^\gamma > x^\beta x^\gamma.$$

With respect to γ, we say that $ax^\alpha > bx^\beta$ if $x^\alpha > x^\beta$. Thus $f \in k[x]$ may be written as a linear combination of terms which are ordered according to $>$. The largest term of f with respect to $>$ is called *leading term*(denoted $lt(f)$) and the largest monomial of f with respect to $>$ is called *leading monomial* (denoted $lm(f)$).

Let M be a free A-module with basis $\{e_1, \ldots, e_s\}$. Elements of the form $x^\alpha e_i$ are called *monomials* and $ax^\alpha e_i$ are called *terms*. Monomials orders on terms of M may be defined similarly with

$$x^\alpha e_i > x^\beta e_i \Longleftrightarrow x^\alpha e_j > x^\beta e_j,$$

for all i, j. The monomial $x^\alpha e_i$ is said to *divide* $x^\beta e_j$ if x^α divides x^β in A.

Definition 4.2.1. *A set of non-zero elements* $\{g_1, \ldots, g_r\}$ *contained in a submodule* N *of* M *is said to be a Gröbner basis of* N *if for all* $m \in N$*, there exists a* g_i *such that* $lt(g_i)$ *divides* $lt(f)$*, where* $1 \leq i \leq r$.

A Gröbner basis is said to be *strictly ordered* if there are no duplicates among its leading terms, and its elements are in increasing order of leading term.

Any Gröbner basis is actually a basis of N. Each $m \in N$ has a *standard expression* with respect to a Gröbner basis as $m = \sum_{i=1}^{r} f_i g_i$, where $f_i \in A$ and $lt(f_i g_i) \leq lt(m)$, for $1 \leq i \leq r$.

4.3 O'Keeffe-Fitzpatrick algorithm

We recall the algorithm of O'Keeffe and Fitzpatrick of [48]. The setup is as follows. Let F be a field and $A = F[x_1, \ldots, x_s]$. The solution set which satisfies the following sequence of congruences is sought:

$$H^{(k)}(\mathbf{b}) \equiv 0 \mod M^{(k)}, k = 1, \ldots, p,$$

where $M^{(k)}$ are A-modules. Each $H^{(k)}$ is an F-linear function such that for each $i,\ 1 \leq i \leq s$ there exists $\gamma_i^{(k)} \in F$ satisfying

$$H^{(k)}(x_i \mathbf{b}) = (x_i + \gamma_i^{(k)}) H^{(k)}(\mathbf{b})$$

for all $\mathbf{b} = (b_1, \ldots, b_L) \in A^L$.

The algorithm applies in the case when a descending chain of modules $M_0^{(k)}, \ldots, M_l^{(k)} \ldots, M_{N_k}^{(k)} = M^{(k)}$ with F-homomorphisms θ_l so that for each index l

$$M_l^{(k)} \supseteq M_{l+1}^{(k)}$$
$$\theta_l^{(k)} : M_l^{(k)} \longrightarrow F,\ \ker(\theta_l^{(k)}) = M_{l+1}^{(k)}$$

exist. Hence, there are constants $\beta_i^{(l,k)}$ where $(x_i - \beta_i^{(l,k)}) M_l^{(k)} \subseteq M_{l+1}^{(k)},\ 1 \leq i \leq s$.

The Gröbner basis output in the current step forms the input of the next step of the iterative algorithm. Let $T^{(i)} = T_{(j_1,\ldots,j_p)}$ be a submodule of A^L which satisfies

$$H^{(k)}(\mathbf{b}) \equiv 0 \mod M_{j_k}^{(k)}, k = 1, \ldots, p$$

and let $T^{(0)} = T_{(0,\ldots,0)}$ be an initial module for which a Gröbner basis is known. A Gröbner basis for the submodule $T = T_{(N_1,\ldots,N_p)}$ is sought. For increasing indices one obtains a decreasing chain of modules $T^{(0)} \supseteq \ldots \supseteq T^{(j)} \supseteq \ldots T$. If a Gröbner basis for $T^{(i)} = T_{(j_i,\ldots,j_p)}$ is known, then if $j'_k = j_k + 1$ for exactly one $k \in \{1, \ldots, p\}$, and $j'_k = j_k$ otherwise, the incremental step gives a Gröbner basis for $T^{(i+1)} = T_{j'_1,\ldots,j'_p}$. The resulting basis is converted into a strictly ordered one using the function *ord*. The function *nextmod* selects the next module in the decreasing chain. The algorithm is given below.

4.4 List decoding of one-point codes

In this section we recall the list decoding algorithm of [34] for one-point codes. First, we recall the notion of list decodability.

Definition 4.4.1. *A linear code C of block length n over $\mathbb{F}_q$ is said to be (e, b)-decodable if every Hamming sphere of radius e in $\mathbb{F}_q^n$ contains at most b codewords.*

List decoding of algebraic-geometric codes was first considered in [58]. An algorithm which corrects up to $e < n - \sqrt{2n(n-d)} - g + 1$ errors was given. This algorithm was improved to correct $e < n - \sqrt{n(n-d)}$ in [34] by introduction of the notion of multiplicities. Both these algorithms are based on a interpolate and root-find strategy. We recall the algorithm of [34] from

Input: $\mathcal{B}_0$ is a strictly ordered Gröbner basis for $T^{(0)}$
Output: $\mathcal{B}$ a strictly ordered Gröbner basis for T

1. $\mathcal{B} := \mathcal{B}_0$
2. For each module from $T^{(0)}$ to T do
   $(k, \theta_l) = nextmod(\text{module})$
   $\Delta_j := \theta_l(\mathcal{B}[j])$ for $j \in 1, \ldots, \#(\mathcal{B})$
   If $\Delta_j = 0$ for all j then $\mathcal{B}' := \mathcal{B}$
   else
      j^*:= least j such that $\Delta_j \neq 0$
      $\mathcal{B}_1 := \{\mathcal{B}_| : j < j^*\}$
      $\mathcal{B}_2 := \{(x_i - (\beta_i^{(k,l)} + \gamma_i^{(k)}))\mathcal{B}[j^*] : 1 \leq i \leq s\}$
      $\mathcal{B}_3 := \mathcal{B}[j] - (\Delta_j/\Delta_{j^*})\mathcal{B}[j^*] : j > j^*$
      $\mathcal{B}' := \mathcal{B}_1 \bigcup \mathcal{B}_2 \bigcup \mathcal{B}_3$
   $\mathcal{B} := ord(\mathcal{B}')$

Table 4.1: *Algorithm for finding Gröbner basis for solution submodules*

the tower point of view, which corrects $n - t - 1$ errors. Thus this algorithm is a $(n - t - 1, s)$ list decoding algorithm.

The first step of the list decoding algorithm is an interpolation step, which finds a polynomial $Q(T) \in F_m[T]$ satisfying

A. (Multiplicity condition) $Q(y_i)$ vanishes 'to the order r' at P_i for $1 \leq i \leq n$ and

B. (Degree condition) $v_{P_\infty}(Q(f)) \leq l$ for $f \in L(uP_\infty)$, where l is a parameter which will be fixed later.

The second condition may be imposed as follows. Let

$$Q(T) = \sum_{b=0}^{s} q_b T^b, \tag{4.4.1}$$

where $q_b \in L(\rho_b P_\infty)$, where $\dim(\rho_b P_\infty) = l - g + 1 - ub$(recall that g is the genus of the underlying function field).

Remark 4.4.2. *The algorithm assumes that*

1. *an increasing pole order basis* $\{\Phi_1, \ldots, \Phi_{l-g+1}\}$ *is known and*
2. *for each place* P_b*, a set* $\{\psi_1^{(f)}, \ldots, \psi_{l-g+1}^{(f)}\}$ *may be computed such that*

$$v_{P_\infty}(\psi_j^{(f)}) \leq 1 - j$$

and

$$\Phi_j = \sum_{w=1}^{l-g+1} \alpha_{j,w}^{(f)} \psi_w^{(f)},\ 1 \leq j \leq l-g+1. \tag{4.4.2}$$

In fact [34, Lemma 21] computes such a set of basis elements from a given set of ϕ_js.

In view of the dimension criteria, the coefficients q_b may be represented as

$$q_b = \sum_{j=1}^{l-g+1-ub} q_{b,j} \Phi_j. \tag{4.4.3}$$

Using Equations 4.4.2 and 4.4.3 in Equation 4.4.1, one obtains,

$$Q(T) = \sum_{b=0}^{s} \sum_{j=1}^{l-g+1-ub} \sum_{w=1}^{l-g+1} q_{b,j} \alpha_{j,w}^{(f)} \psi_w^{(f)} T^b. \tag{4.4.4}$$

Let

$$Q(P,T) := Q(T)(P)$$

and

$$Q^{(f)}(P_f,T) := Q(T+y_f)(P_f),\ 1 \leq f \leq n.$$

Thus

$$Q^{(f)}(P_f,T) = \sum_{b=0}^{s} \sum_{w=1}^{l-g+1} \beta_{b,w}^{(f)} \psi_w^{(f)}(P_f) T^b \tag{4.4.5}$$

where

$$\beta_{b,w}^{(f)} := \sum_{c=b}^{s} \sum_{j=1}^{l-g+1-uc} \binom{c}{b} y_f^{c-b} q_{c,j} \alpha_{j,w}^{(f)}. \tag{4.4.6}$$

Having done this one may impose the first condition as follows. Insist

$$\beta_{b,w}^{(f)} = 0, \tag{4.4.7}$$

for $w \geq 1$, $b \geq 0$ and $b + w - 1 < r$.

Finally, the parameters r and l are set as

$$r := 1 + \left\lfloor \frac{2gt + un + \sqrt{(2gt+un)^2 - 4(g^2-1)(t^2-un)}}{2(t^2-un)} \right\rfloor$$
$$l := rt - 1.$$

Those roots h of Q which satisfy $h(P_i) = y_i$ for at least t values of $i \in \{1, \ldots, n\}$ are incudes in the output list. Thus the algorithm gives as output a list of size at most s.

4.5 Interpolation step of list decoding

We give a module formulation of the interpolation step along the lines of [48]. The solution polynomial of the interpolation step is seen as an element of a suitable free module. The dimension and the order conditions in the list decoding algorithm studied in earlier section is translated into conditions on terms of a suitable module. The techniques of [48] are used to determine such a solution.

Let $L := l - g + 1$. Let $A = \mathbb{F}_{q^2}[T]$ and M a free module A^L with basis $\{e_1, \ldots, e_L\}$. Recall that the interpolation polynomial is of the form

$$Q(T) = \sum_{b=0}^{s} \sum_{j=1}^{l-g+1-ub} q_{b,j} \Phi_j T^b. \tag{4.5.1}$$

Want $Q(T) \neq 0$ such that $\beta_{b,w}^{(f)} = 0$ for $w \geq 1$, $b \geq 0$ and $b + w - 1 < r$.

The maps $\Phi_i \mapsto e_i$ and for a fixed f, $\psi_i^{(f)} \mapsto e_i$ are module maps. Let $H^{(f)} : M \to M$ be the map which identifies Q with $Q^{(f)}(P_f, T)$ using the earlier maps. Then the map $H^{(f)}$ is $\mathbb{F}_{q^2}$ linear and the structure of Q and $Q^{(f)}$ implies that $H^{(f)}(Tv) = (T + y_f)H^{(f)}(v)$ for $v \in M$. We need to find elements $v \in M$ where for each f the following conditions are satisfied:

1. (Degree criterion) Terms $T^b e_w$ satisfy $ub + (w - 1) < L$. This is just a restatement of the condition that the coefficients of the interpolation polynomial come from a suitable L-space.

2. (Zero multiplicity criterion) Coefficients of $H^{(f)}(v)$ are zero for terms $T^b e_w$ with $b + (w - 1) < r$. Notice that this condition is same as the condition in Equation 4.4.7.

In [48], an algorithm for recursive computation of Gröbner basis is given. Congruences of the form

$$H^{(k)}(b) \equiv 0 \bmod M^{(k)},\ k = 1, \ldots, p$$

where $b \in A^q$ and $M^{(k)}$ are A-modules with functions $H^{(k)},\ k = 1, \ldots, p$ are solved using a recursive computation. The functions are such that the the set of solutions forms a submodule of M. We mention how the algorithm may be used to solve the problem on hand.

A term order $<_{\delta,\rho}$ of the submodule for $\rho = (\rho_1, \ldots, \rho_L) \in \mathbb{N}^L$ and $\delta \geq 1 \in \mathbb{N}$ is defined such that

$$T^n e_j <_{\delta,\rho} T^m e_i$$

if $\delta n + \rho_j < \delta m + \rho_i$ or $\delta n + \rho_j = \delta m + \rho_i$ and $i < j$.

Now, consider the set of solutions satisfying only the zero multiplicity condition. This set forms a submodule of M. The parameters are so chosen that $v \in M$ exist satisfying both the degree and the zero multiplicity conditions. Thus, a minimal element with respect to $<_{\delta,\rho}$ is a solution. We have n maps $H^{(1)}, \ldots, H^{(n)}$. Consider

$$\langle \{T^b e_w \mid b + (w-1) = r\} \rangle$$

a submodule of M. A sequence of modules decreasing from M to $\langle \{T^b e_w \mid b + (w-1) = r\} \rangle$ are created to apply the algorithm of [48] may be applied.

Thus the problem of interpolation in list decoding algorithm is reduced to the problem of finding a Gröbner basis for a free module over a polynomial ring of one variable.

4.6 Some concluding remarks

Codes on the Garcia-Stichtenoth towers are important for their asymptotic properties. An account of the list decoding procedure for one-point codes constructed on this tower is given. In particular the recursive algorithm of [48] is applied to perform the interpolation step. It is known from [35] that the root-finding step may be reduced to factorising polynomials over a large finite field. Then the roots of the reduced polynomials are lifted to the roots of the original polynomial by solving a system of linear equations.

The fifth chapter deals with the construction of the non-uniform input required for list decoding codes on Bezerra-Garcia tower.

Chapter 5

On finding the non-uniform input for list decoding codes on function fields

Algebraic-geometric codes are evaluation codes similar to Reed-Solomon codes. See Definition 1.3.1. These codes are constructed over function fields, F, of transcendence degree one over a finite field. Such codes are well-studied for their asymptotic properties. In fact, codes constructed on the tower of function fields introduced by Garcia and Stichtenoth in [26] attain best known bounds. See Chapter 1 for more details. Encoding and decoding procedures for linear codes constructed on function fields have attracted much research in the last two decades. The encoding procedure involves finding a basis for Riemann-Roch spaces of divisors. The functions of $L(uQ)$ are evaluated at some places of degree one to obtain the code. If $F/\mathbb{F}_q$ is the underlying function field, then $L(uQ)$ is a finite dimensional vector space over $\mathbb{F}_q$.

A list decoding algorithm for a code gives as output a small list of codewords, but corrects more errors than a classical algorithm can. Such an algorithm for one-point codes was given by Guruswami and Sudan in [34] and a suitable representation of the data involved was discussed by Guruswami and Sudan in [35]. The algorithm is based on a interpolate and root-find strategy. For a received word $y = (y_1, \ldots, y_n)$ a polynomial in one variable over F is found, such that each coefficient lies in $L(D)$, where D is the underlying divisor and the zeroes of this polynomial are the required words. Then the zeroes of the interpolation polynomial are found and those which lie sufficiently close to the received word are output. The zeros of the interpolation polynomial are known to be elements of $L(D)$ for the underlying divisor D. This data may be used to design efficient root finding algorithms over function fields. Here the focus is on the root finding step of the list decoding algorithm. In [35], the root-find step involves computation of a non-uniform input, which is a evaluation of the basis elements of $L(D)$ at a large degree

place. Hence, the non-uniform input is independent of the received word.

In [32] Guruswami and Patthak, among many other results, find the non-uniform input for the function fields of the Garcia-Stichtenoth tower [26]. They use the structure of the quasi-regular functions used in the pole cancellation algorithm of [59]. Their procedure for finding the non-uniform input is randomised, making uniformly random choices for irreducible polynomials of a given degree over $\mathbb{F}_{q^2}$. A simple counting argument shows that there exist places of degree r of F_m lying above places of same degree of F_1. Here $F_1 \subset F_2 \subset F_3 \subset \ldots$ is the tower. The required non-uniform input is obtained as a solution to a system of linearised equations, using Kummer theorem (see [61, pp. 76]).

A similar procedure for the Bezerra-Garcia tower [6] is given here. There is a unique of $x_1 \in F_m$, which is totally ramified throughout the tower. For construction of codes, divisors of the form uP_∞ are chosen. A nice dual basis for the ring of such regular functions exist, such that it is sufficient of determine the evaluations of the coordinate variables at a large degree place to evaluate the basis elements themselves. There exist places of F_m of degree r lying above a place of same degree of F_1 for large enough r. The set $\{1, y, \ldots, y^{q-1}\}$ is a integral basis for the large degree place. Let $\rho_i = (x_1 - 1)^{q^i}$ for $i = 2, \ldots, m$. Let

$$\mathcal{Z} := \prod_{i=2}^{m} \{1, \rho_i x_i, \rho_i x_i^2, \ldots, \rho_i x_i^{q-1}\}$$

and

$$\mathcal{Z}^* := \prod_{i=2}^{m} \left\{ -\frac{x_i - 1}{\rho_i x_i^q}, -\frac{x_i - 1}{\rho_i x_i^{q-1}}, \ldots, -\frac{x_i - 1}{\rho_i x_i^2}, \frac{1}{\rho_i x_i} \right\}$$

be the sets obtaining by taking $m-1$-fold products of the constituent sets. Then

$$\sum_{z \in \mathcal{Z}} R_1 z \subseteq R_m \subseteq \sum_{z^* \in \mathcal{Z}^*} R_1 z^*,$$

where the sums above are finite. The sets $\mathcal{Z}$ and $\mathcal{Z}^*$ form a trace basis-dual basis pair. Any regular function is a linear combination of elements of $\mathcal{Z}^*$ and the elements of this set cannot have poles at high degree places. The required evaluations of the coordinate variables are obtained by solving a system of linearised equations, using Kummer's theorem.

The plan of this chapter is as follows. First the Kummer's theorem is recalled. Then some facts on number of places of a given degree of a function field $F/\mathbb{F}_q$ of genus g are recalled from [61]. List decoding procedure for one point codes is recalled. A bound on the number of places of F_1 of degree r lying below a place of the same degree of F_m is obtained. Hence, the probability that a place of degree r of F_1 chosen at random having the above property is calculated. Finally, the randomised algorithm for finding

the non-uniform input on the function fields of the Bezerra-Garcia tower is given. The results appearing in this chapter were presented at AAECC 2007 conference and appear in [15].

5.1 Kummer's theorem

Kummer theorem is stated from [61, pp. 76] for completeness. This is studying ramification of places in separable extensions of function fields. For $P \in \mathbb{P}(F)$, let $\overline{a} := a(P)$, for $a \in \mathcal{O}_P$. For a polynomial $\psi(T) = \sum_{i=0}^{n} a_i T^i \in \mathcal{O}_P[T]$, the reduced polynomial $\overline{\psi}(T) = \sum_{i=0}^{n} \overline{a_i} T^i$.

Theorem 5.1.1. *Suppose that $F' = F(y)$, with $n = [F' : F]$ where y is integral over $\mathcal{O}_P$ and consider the minimal polynomial $\phi(T) \in \mathcal{O}_P[T]$ of y over F. Let*

$$\overline{\phi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i}$$

be the decomposition of $\overline{\phi}(T)$ into irreducible factors over F_P, the residue class field of P. Choose monic polynomials $\phi_i(T) \in \mathcal{O}_P[T]$ with

$$\overline{\phi_i}(T) = \gamma_i(T) \text{ and } \deg \phi_i(T) = \deg \gamma_i(T).$$

Then for $1 \leq i \leq r$, there are places $P_i \in \mathbb{P}(F')$ satisfying

$$P_i \mid P, \ \phi_i(y) \in P_i \text{ and } f(P_i \mid P) \geq \deg \gamma_i(T).$$

Moreover $P_i \neq P_j$ for $1 \leq i \neq j \leq r$.

Suppose, further, that at least one of the following two assumptions hold:

K1. *$\varepsilon_i = 1$ for $i = 1, \ldots, r$*

K2. *$\{1, y, \ldots, y^n\}$ is an integral basis for P.*

Then, there exists, for $1 \leq i \leq r$, exactly one place $P_i \in \mathbb{P}(F')$ with $P_i \mid P$ and $\phi_i(y) \in P_i$. The places $P_1, \ldots, P_r$ are all the places of F' lying over P and we have,

$$Con_{F'|F}(P) = \sum_{i=1}^{r} \varepsilon_i P_i,$$

i.e., $\varepsilon_i = e(P_i \mid P)$. The residue class field $F_{P_i} = \mathcal{O}_{P_i}/P_i$ is isomorphic to $F_P[T]/(\gamma_i(T))$, hence $f(P_i \mid P) = \deg \gamma_i(T)$.

Proof. Refer to [61, Theorem III.3.7]. ∎

5.2 Number of places of a given degree

Here, estimates on the number of places of a given degree of a function field over a finite field are recalled. Basic reference for this topic is [61, Chapter V]. In this discussion, function field F of genus g over $\mathbb{F}_q$ is considered. We recall some definitions

Definition 5.2.1. *For a function field $F/\mathbb{F}_q$,*

1. *$N(F)$ denotes the number of places of F of degree one,*
2. *$N_r(F)$ denotes the number of places of degree one in the constant field extension $F_r = F\mathbb{F}_{q^r}$ and*
3. *B_r denotes the number of places of F of degree r.*

Let us first recall Hasse-Weil bound.

Theorem 5.2.2. *(Hasse-Weil bound) The number $N = N(F)$ of places of $F/\mathbb{F}_q$ of degree one can be estimated by*

$$|N - (q+1)| \leq 2gq^{1/2}.$$

Proof. Refer to [61, Theorem V.2.3]. ∎

Applying Hasse-Weil bound to the function field F_r yields the following corollary.

Corollary 5.2.3. *For the function field F_r the following estimate holds*

$$|N_r - (q^r + 1)| \leq 2gq^{r/2},$$

for any $r \geq 1$.

One can bound the number of places of a fixed degree of a given function field using Hasse-Weil bound. Recall that B_r is the number of places of F of degree r. The required bound may be obtained using the following relation between B_r and N_s for $r \geq 1$ and $s \leq r$.

Lemma 5.2.4. *The quantities B_r and N_s for $r \geq 1$ and $s \leq r$ are related as*

$$N_r = \sum_{d|r} dB_d,$$

where the sum runs over all the divisors $d \geq 1$ of r.

The above results will be used to obtain bounds on the number of places of a particular degree on arbitrary function fields. The bound on B_r from [61, Corollary V.2.10] is recalled.

Proposition 5.2.5. *The estimate*

$$|B_r - \frac{q^r}{r}| < (2 + 7g)\frac{q^{r/2}}{r}.$$

This bound will be used to obtain an estimate of the number of places of degree r of F_1 lying below places of same degree of F_m of the tower.

5.3 Algebraic-geometric codes and their list decoding

In this section list decoding algorithm of [34] is outlined. Let us first recall the definition of one-point algebraic-geometric codes on a function field. This has already been defined in Chapter 1. We specizlize the definition for D of the type uQ.

Definition 5.3.1. *Let $F \supset \mathbb{F}_q$ be a function field of genus g. Let $P_1, \ldots, P_n$ be distinct places of degree 1, all distinct from a place Q. Let $G = P_1 + \ldots + P_n$ and uQ. Let*

$$C_L(u, G) = \{(f(P_1), \ldots, f(P_n)) \mid f \in L(uQ)\} \subseteq \mathbb{F}_q^n.$$

The code C_L is known as a (One-point)Algebraic-Geometric(AG) code.

Henceforth we consider only one-point codes. The next lemma gives bounds on the parameters of the one-point codes.

Lemma 5.3.2. *Assume that $u < n$. Then $C_L(u, G)$ is an $[n, k, d]_q$ code with $k \geq u - g + 1$ and $d \geq n - u$.*

It is assumed henceforth that $u < n$, so that the above lemma holds. List decoding algorithm for such one-point codes was given in [34] and a suitable representation of the data involved was discussed in [35]. Suppose that the channel corrupts at most $n - t$ places of the sent word and $y = (y_1, \ldots, y_n)$ is received. The list decoding algorithm of [34] finds an interpolation polynomial for y as the first step. This polynomial has degree s for a suitably chosen parameter s and has coefficients in $L(D)$ for a suitably chosen divisor D. For more details consult [34]. The required list of decoded words comprises of those zeroes of the interpolation polynomial in $L(uQ)$ whose evaluations at P_i agree with y_i for at least t coordinates.

In [35] the representation issues related to the list decoding algorithm are discussed. A strategy for finding the zeroes of the interpolation polynomial is given. This strategy is based on finding a non-uniform input which does not depend on the received word. A basis for $L(D)$ is assumed to be computable. The non-uniform input is described below:

Non-Uniform Input: A l-tuple $(\zeta_1^R, \ldots, \zeta_l^R)$ over $\mathbb{F}_{q^r}$, obtained by evaluating a increasing basis $(\Phi_1, \ldots, \Phi_l)$ of $L(D)$ at place R, where R has degree r greater than $\deg D$.

Let us begin by recalling [35, Lemma 5].

Lemma 5.3.3. *If $f_1, f_2 \in L(A)$ for $A \succeq 0$ and $f_1(R) = f_2(R)$ for some place R of degree bigger than $\deg(A)$. Then $f_1 = f_2$.*

The strategy now is to first reduce the interpolation polynomial $H(T)$ modulo R to obtain $h(T)$ over the underlying finite field and find the zeroes of the polynomial equation $h(T) = 0$ using some standard algorithm. Then for each root compute $\beta_i \in L(D)$, if any, such that $\beta_i(R) = \alpha_i$. This β_i, by Lemma 5.3.3, is unique. Those elements of the list $\beta_1, \ldots, \beta_t$ are output which meet the distance criterion. The root-find procedure of [35] is given below.

Input: A degree d polynomial $H(T) = \sum_{i=0}^{d} a_i T^i \in F[T],\ a_i \in L(D)$.
Output: All zeroes of H that lie in $L(D)$
1. Reduce H modulo a place R of large enough degree r to obtain $h(T)$.
2. Compute the zeroes, say $\alpha_1, \ldots, \alpha_t$ of $h(T)$.
3. For each α_i find the unique $\beta_i \in L(D)$, if any, such that $\beta_i(R) = \alpha_i$.
4. Output such β_i.

Table 5.1: *Algorithm for ROOT-FIND step of list decoding one-point codes*

The correctness of the algorithm hinges on the following remark.

Remark 5.3.4. *If* $\beta_i = \sum_{j=1}^{l(D)} a_j \Phi_j$, *then*

$$\sum_{j=1}^{l(D)} a_j \Phi_j(R) = \alpha_i$$

may be considered as a system of linear equations with $a_1, \ldots, a_{l(D)}$ *as indeterminate over* $\mathbb{F}_q$ *after fixing a representation for* $\mathbb{F}_{q^r} \supset \mathbb{F}_q$. *This system has a unique solution by Lemma 5.3.3.*

From the above discussion, it is clear that given

1. the non-uniform input,
2. a root-finding algorithm over a large finite field and
3. a procedure for solving a system of linear equations over $\mathbb{F}_q$

the root finding algorithm may be efficiently implemented. There exist algorithms to perform the second and third tasks above. Hence, given the non-uniform input the entire root-find step of the list decoding algorithm may be efficiently implemented.

In [32] the authors, among many other results, find the non-uniform input for the function fields of the Garcia-Stichtenoth tower [26]. Suppose

$$F_1 \subset F_2 \subset F_3 \subset \ldots$$

denotes the tower and $P_\infty^{(m)}$ the unique pole of x_1 in F_m. In [59] a pole cancellation based algorithm for determining a basis for $L(uP_\infty^{(m)})$ is given, which uses regular functions defined there. The procedure of [32] makes use of the structure of quasi-regular functions. A simple counting argument of [32] shows that there exist places of degree r of F_m lying above places of F_1 of same degree. Their procedure for finding the non-uniform input is randomised, making uniformly random choices for irreducible polynomials of a given degree over $\mathbb{F}_q$. The required non-uniform input is obtained as a solution of a system of linearised equations using Kummer's theorem.

5.4 Places of a special type of degree r of the tower

We restrict our attention to function fields over finite fields of the type $\mathbb{F}_{q^2}$. A bound on the number of places of F_1 of degree r lying below a place of the same degree of F_m is obtained. Hence, the probability that a place of degree r of F_1 chosen at random having the above property is calculated. Techniques used in this section are from [61, Chapter V].

In the following the superscript m denotes the function field F_m of the tower. Thus $B_r^{(m)}$ denotes the number of places of degree r of $F_m/\mathbb{F}_{q^2}$.

For F_m, let $U_r^{(m)}$ denote the number of places of places of F_1 of degree r lying below a degree r place of F_m. Let

$$\begin{aligned} B_{r,1}^{(m)} :=& \text{the number of degree } r \text{ places of } F_m \text{ lying above a degree } r \\ & \text{place of } F_1 \text{ and} \\ B_{r,2}^{(m)} :=& \text{the number of degree } r \text{ places of } F_m \text{ not lying above a} \\ & \text{degree } r \text{ place of } F_1. \end{aligned}$$

Clearly we have $B_r^{(m)} = B_{r,1}^{(m)} + B_{r,2}^{(m)}$. We have

$$B_{r,1}^{(m)} \leq U_r^{(m)} \cdot [F_m : F_1]. \tag{5.4.1}$$

Now, we shall estimate $B_{r,2}^{(m)}$. We know that places of degree r of F_1 are in one-to-one correspondence with monic irreducible polynomials of degree r over $\mathbb{F}_{q^2}$. If $P' \mid P$ then $\deg(P)$ divides $\deg(P')$. Hence $B_{r,2}^{(m)}$ is at most the number of monic irreducible polynomials of degree at most $r/2$ over $\mathbb{F}_{q^2}$. Thus

$$\begin{aligned} B_{r,2}^{(m)} &\leq \sum_{d=1}^{r/2} \frac{q^{2d} - q^2}{d} \\ &\leq q^{r+1}. \end{aligned} \tag{5.4.2}$$

Next, we state and prove a simple lemma.

Lemma 5.4.1. *[15, Lemma 5] For $r \geq m + 16$ the following holds*

$$q^{m-1} \cdot U_r^{(m)} \geq \frac{q^{2r}}{2r}.$$

Proof. Using Equations 5.4.1 and 5.4.2 and the bound on B_r in Proposition 5.2.5, we obtain

$$q^{m-1} \cdot U_r^{(m)} \geq \frac{q^{2r}}{r} - \frac{8g_m q^r}{r} - q^{r+1}.$$

Using the fact that $g_m \leq q^m$, we obtain

$$q^{m-1} \cdot U_r^{(m)} \geq \frac{q^{2r}}{r} - \frac{8q^{r+m}}{r} - q^{r+1}.$$

Consequently, for $r \geq m + 16$ the following holds

$$q^{m-1} \cdot U_r^{(m)} \geq \frac{q^{2r}}{2r}.$$

hence, the result. ∎

Finally we estimate the probability with which a degree r place of F_1 chosen uniformly at random has a degree r place of F_m above it. Notice that choosing a degree r place of F_1 is equivalent to choosing an irreducible polynomial of degree r over $\mathbb{F}_{q^2}$. The following is a easy corollary to the above lemma.

Corollary 5.4.2. *[15, Corollary 2] Let the notations be as in the previous lemma. Let $r \geq m+16$. Then $p_{r,m}$, the probability that a place of F_1 of degree r chosen uniformly at random lies below a degree r place of F_m, satisfies*

$$p_{r,m} \geq \frac{1}{2rq^{m+1}}.$$

Thus with non-zero probability a degree r place of F_1 chosen uniformly at random has a degree r place of F_m above it. We use this fact to construct a randomised algorithm for finding the non-uniform input in the next section.

5.5 Finding non-uniform input on Bezerra-Garcia tower

In this section, a randomised procedure for finding the required non-uniform input is given. A basis for the underlying vector space $\Phi_1, \ldots, \Phi_l$ is assumed to be given. The procedure of [32] applies for this tower too. The procedure, initially, makes a random choice of an irreducible polynomial. The required

data is obtained as a solution of a system of linearised equations, by Kummer's theorem. It is been shown in the last section that there exist places of F_1 having a place of F_m of same degree above them. Thus the procedure must terminate in expected polynomial time in the length of the code.

For the Bezerra-Garcia tower, since the unique pole of x_1 is totally ramified throughout the tower, for each level, a divisor $D_m = u_m P_\infty^{(m)}$ is chosen. There are at least q^m places of degree one for F_m, not lying above zeroes and poles of $x_1(x_1 - 1)$. The code is obtained by evaluating elements of $L(u_m P_\infty^{(m)})$ at these q^m places.

There exist algorithms for finding a basis for the ring of regular functions on Garcia-Stichtenoth tower. See [59] for example. But such an explicit algorithm does not exist for the Bezerra-Garcia tower. So, the entire exercise assumes that a basis for the underlying vector space is given. The non-uniform input is calculated by evaluating these basis elements at a high degree place. However, the result in Theorem 2.4.5 guarantees that the non-uniform input may be effectively computed.

Recall that, list decoding one-point codes uses a non-uniform input for the root-finding step. Let r be chosen such that both:

(a). $r > u_m$ and

(b). $r \geq m + 16$

hold. A place of F_m of degree r may be constructed as follows. Places of degree r of F_1 are in one-to-one correspondence with monic irreducible polynomials of degree r over $\mathbb{F}_{q^2}$. Such a polynomial is chosen at random. Denote the place determined by this polynomial by ρ_1. Let $\gamma_2 = \left(\frac{x_1}{x_1^q - 1}\right)(\rho_1)$. Consider the system of linearised equations.

$$\begin{aligned} x_2^q - \frac{x_1}{x_1^q - 1} x_2 &= -\gamma_2 \\ x_3^q + \frac{x_2}{x_2^q - 1} x_3 &= -\frac{x_2}{x_2^q - 1} \\ &\vdots \\ x_m^q + \frac{x_{m-1}}{x_{m-1}^q - 1} x_m &= -\frac{x_{m-1}}{x_{m-1}^q - 1} \end{aligned} \tag{5.5.1}$$

A solution to this system gives a place of degree r, by Kummer's theorem(refer to [61, pp. 76]). We first state the algorithm [15, Algorithm 2] for finding the non-uniform input and then prove its correctness.

Notice that only the choice of irreducible polynomial is random. Rest of the steps in the computation of the non-uniform input are deterministic. Thus with probability $p(r, m)$ the algorithm outputs the non-uniform input.

Input: m, r and $\Phi_1, \ldots, \Phi_l$
Output: $(\alpha_1, \ldots, \alpha_m)$
1. Choose an irreducible polynomial f of degree r over $\mathbb{F}_{q^2}$.
2. Set $\alpha_1 = x_1(\rho_1)$ and $\gamma_2 = \left(\frac{x_1}{x_1^q - 1}\right)(\rho_1)$.
3. Solve the system of equations 5.5.1.
4. If a solution $(\alpha_2, \ldots, \alpha_m)$ exists then compute the evaluations of $\Phi_1, \ldots, \Phi_l$ else report failure.

Table 5.2: *Algorithm for finding non-uniform input on B-G tower*

The rest of the steps of the list decoding algorithm may be carried out efficiently once the non-uniform input is given, as discussed earlier. We start the proof of correctness of this algorithm with a simple technical lemma.

Lemma 5.5.1. *[15, Lemma 6] Let P_j and P_{j-1} be places of F_j and F_{j-1} with $P_j \mid P_{j-1}$ not lying above zeroes and poles of $x_1(x_1 - 1) \in F_1$. The set $\{1, x_j, \ldots, x_j^{q-1}\}$ is an integral basis for $F_j/F_{j-1},\ j \geq 2$ at $P_j \mid P_{j-1}$.*

Proof. By [61, Theorem III.5.10], the set $\{1, x_j, \ldots, x_j^{q-1}\}$ is an integral basis for $P_j \mid P_{j-1}$ if and only if $d(P_j \mid P_{j-1}) = v_{P_j}(\phi_j'(y))$. Here ϕ' denotes the formal derivative. We have

$$\begin{aligned} v_{P_j}(\phi_j'(y)) &= v_{P_j}\left(\frac{x_{j-1}}{x_{j-1}^q - 1}\right) \\ &= 0. \end{aligned}$$

By [6, Lemma 2], we have $P_j \mid P_{j-1}$ is unramified. Thus

$$d(P_j \mid P_{j-1}) = e(P_j \mid P_{j-1}) - 1 = 0,$$

by Dedekind's different theorem([61, Theorem III.5.1]). Thus

$$\{1, x_j, \ldots, x_j^{q-1}\}$$

is an integral basis for the extension $F_j/F_{j-1},\ j \geq 2$ at $P_j \mid P_{j-1}$. ∎

We are now in a position to give the proof of correctness of the above algorithm.

Theorem 5.5.2. *[15, Theorem 2] The algorithm in Table 5.2 gives the required non-uniform input.*

Proof. For any level, we have shown that set $\{1, x_j, \ldots, x_j^{q-1}\}$ is an integral basis for $F_j/F_{j-1},\ j \geq 2$ at $P_j \mid P_{j-1}$. Notice that all the conditions of Kummer theorem are satisfied. The first equation of the system is the reduced form the defining equation. If a solution to the system of linearised equations exists, then $(\alpha_1, \ldots, \alpha_m)$ is the evaluation of the coordinate variables at a degree r place of F_m. By Lemma 2.4.5, the basis elements may be evaluated using this tuple $(\alpha_1, \ldots, \alpha_m)$, since the denominator of the dual basis involves only $x_1 - 1$ and the x_j's. Hence the correctness of the algorithm is verified. ■

Complexity: The main computational tasks involved in the procedure are the following:

1. checking whether a given polynomial is irreducible or not and
2. finding a solution to a system of linear equations.

There exist deterministic algorithms for performing both the tasks. The procedure gives the required non-uniform input in expected polynomial time in the length of the code.

5.6 Some concluding remarks

It has been observed in this chapter that the asymptotic argument given in [32] is more general and applies to Bezerra-Garcia tower also. An algorithm for finding the non-uniform input, similar to that in [32], was given for the function fields of this tower. The expression for regular functions obtained in earlier chapter was used. The correctness of the algorithm followed from Kummer theorem.

The next chapter deals with the disambiguation problem of [30].

Chapter 6

Hash functions and list decoding with side information

We examine how different choices of hash functions affect the number of bits of side information needed to disambiguate the output list in list decoding in a randomised framework as considered by [30]. The discussion is based on [12]. Suppose a sender S sends a message $x \in \{0,1\}^k$, encoded as a string $C(x)$ using a (p, L)-list decodable code $C : \{0,1\}^k \to \{0,1\}^n$, through a noisy channel to a receiver R who receives a string $y \in \{0,1\}^n$ which may differ from $C(x)$ in a fraction p of coordinates. In order that the receiver R can correctly disambiguate the list of possible messages $\{y_1, \ldots, y_L\}$ obtained by list decoding y to determine the sent message x, Guruswami considers the scenario where S sends some side information regarding x through a secondary, costly, error-free channel to R and R makes use of this to find x. Guruswami noted in [30] that in a deterministic setting S has to send essentially the entire message string x as side information but randomisation helps to reduce the amount of side information needed considerably. In the randomised model he considered the situation where S sends a pair $(f, f(x))$ where f is a randomly chosen hash function belonging to a nice hash family and, based on this input from S, receiver is then able to find x correctly with probability at least $1-\varepsilon$, $\varepsilon > 0$ real, by selecting an appropriate hash family. The scheme with probability at most ε reports failure and returns the whole list. The scheme does not output a wrong message. The number of bits of side information needed here is a sum of the logarithms of the sizes of hash family and hashed value. Using a hash family based on Reed-Solomon codes he showed that the number of bits of side information sender needs is

$$2\log k + 2\log L + 2\log\left(\frac{1}{\varepsilon}\right) + O(1). \tag{6.0.1}$$

He also obtained some lower bounds and showed that the above scheme is optimal up to a constant factor. However, whether the gap between upper

and the lower bounds on the number of bits of side information sender needs to send can be reduced by using the same basic scheme but different hash families is of some interest. We examine several hash families corresponding to certain algebraic-geometric codes and show that some improvements are indeed possible. Specifically, we show that using Hermitian codes we can reduce the constant factor 2 in Expression 6.0.1 to 5/3 and using codes on the Garcia-Stichtenoth towers the constant can be further reduced.

6.1 List decoding with side information

Suppose sender S wants to send a message, say a binary string $x \in \{0,1\}^k$, to receiver R through a noisy channel which may corrupt a fraction p of the symbols in the message but yet R should be able to determine x correctly. In order that the necessary error correction can be done S uses a $[n, k, d]$ code $C : \{0,1\}^k \to \{0,1\}^n$, to encode the message x as $C(x)$ and send it to R. Let $\delta(c_1, c_2)$ denote the fraction of the coordinates where two strings c_1 and c_2 in $\{0,1\}^n$ differ. If y is the string received by R and $\delta(C(x), y) \leq p$, then R can decode y to retrieve x correctly provided the minimum distance of the code $\gamma = \frac{d}{n} \geq 2p$. For $\gamma > \frac{1}{2}$, by Plotkin bound, a binary code can encode at most a constant number of messages. So, for $p > \frac{1}{4}$, unique decoding is not possible. Instead, it is possible to obtain a list of possible candidate messages which may contain the actual message. This is called *list decoding* and it is said to be *successful* if the list contains the actual message x.

Definition 6.1.1. *A code $C : \{0,1\}^k \to \{0,1\}^n$ is (p, L)-list decodable if for every $y \in \{0,1\}^n$, the set $\{x \in \{0,1\}^k \mid \delta(C(x), y) \leq p\}$ has at most L elements.*

For every $p < \frac{1}{2}$, there are families of (p, L_p)-list decodable codes for a fixed constant L_p that depends only on p and not on message length(the dependence is $L_p = O(\frac{1}{\eta^2})$ when $p = \frac{1}{2} - \eta$ for any constant $\eta > 0$). Moreover, these codes have polynomial time algorithms that output a list of at most L_p codewords that differ from y in a fraction of p or less positions. Thus even when constrained to output a relatively short list, list decoding allows efficient decoding up to any fraction $p < \frac{1}{2}$. For more details refer to [31].

Though in many cases, outputting a small list of candidate messages suffice, there are situations when the sent message is to be determined unambiguously. In [30], Guruswami considers a scenario when S sends some side information related to the sent message x to R through a error-free channel that allows R to find the correct message from the list. He showed that in deterministic scheme, in order that R should always be able to determine the message sent correctly, essentially S has to send the entire message through the error-free channel. He then presented probabilistic scheme where

S sends $2\log\left(\frac{kL}{\varepsilon}\right) + O(1)$ bits of side information that permits R to recover the correct message with probability at least $1-\varepsilon$. The receiver never makes a mistake, as either R correctly finds the message or reports failure in returning the sent message, the latter can happen with probability at most ε. The randomised scheme uses hash families with low collision probabilities for subsets of messages of certain size.

The scheme is as follows. After receiving y the receiver list decodes y to get a list $\{z_1, \ldots, z_L\}$ of possible messages. The list decoding is assumed to be successful. Sender S sends $(f, f(x))$ where f is chosen uniformly at random from the hash family, R then checks if there is some $1 \leq i \leq L$ such that $f(x) = f(z_i)$; if so R outputs z_i, else failure. The number of bits of side information needed in this scheme is the sum of logarithms of the sizes of hash family and hashed value. Guruswami took a hash family based on an appropriate Reed-Solomon code and obtained the above mentioned bound. He also obtained some lower bounds which suggest that the above bound is optimal up to a constant factor. Obviously, exact number of bits of side information in the above scheme depends on the hash family used. We examine this by choosing different hash families based on different codes.

6.2 Hash functions and codes

We briefly recall a few facts about the connection between hash functions and codes. We now define universal hash families. Further properties and constructions of hash families may be found in [7].

Definition 6.2.1. *Let $\varepsilon > 0$. A multiset Σ of b functions from a k-set X to a v-set Y is ε-almost universal(ε-AU) if for every pair $u_1, u_2 \in X$ such that $u_1 \neq u_2$ the number $\delta(u_1, u_2)$ of elements $f \in \Sigma$ such that $f(u_1) = f(u_2)$ satisfies $\delta(u_1, u_2) \leq \varepsilon b$.*

The connections between hash families and codes is well studied. We state a well-known and useful fact. AU classes admit a neat description : the columns of an AU class form the words of a code. For more details on the interplay between codes and hash functions refer to [7]. The following lemma is simple but important.

Lemma 6.2.2. *[7] Let $\varepsilon > 0$, $|X| = k$, $|Y| = v$ and Σ an array of n functions from X to Y. Then the following are equivalent:*

1. *Σ is an ε-AU class of hash functions.*
2. *The columns of Σ form the words of a v-ary code of length n with minimum distance d, where $1 - \frac{d}{n} \leq \varepsilon$.*

The following lemma follows easily from the above lemma.

Lemma 6.2.3. *Let Σ be a $\frac{\varepsilon}{2L}$-almost universal family. Then, for any L, $1 \leq L < v$, any $x \in X$ and any $\{z_1, \ldots, z_{L-1}\} \subseteq X \setminus \{x\}$ with distinct elements*

$$Pr[f(x) \notin \{f(z_1), \ldots, f(z_{L-1})\}] \geq 1 - \varepsilon.$$

6.3 Amount of side information depends on the hash family

We now examine the dependence of the number of bits of side information, needed in the randomised scheme for list decoding with side information, on the choice of hash family by considering several specific hash families based on algebraic-geometric codes.

If we examine the randomised scheme in [30] for disambiguating the list $\{z_1, \ldots, z_L\}$, obtained by list decoding the string y received by R, we may note that, given $\varepsilon > 0$, the probability of failure, sender should make use of an $\frac{\varepsilon}{2L}$-almost universal hash family, based on a code, $\mathcal{F} = \{f_i : \{0,1\}^k \rightarrow \{0,1\}^v\}$, for some suitable v, such that, for any $x \in \{0,1\}^k$ and any $\{z_1, \ldots, z_{L-1}\} \subseteq \{0,1\}^k \setminus \{x\}$, the probability $Pr[f(x) \notin \{f(z_1), \ldots, f(z_{L-1})\}]$ which is by Lemma 6.2.2 and Lemma 6.2.3 at least $1 - \varepsilon$. Thus, if the hash family is based on some $[n, k, d]_q$ code for some appropriate q, then we must have, by Lemma 6.2.3, $1 - \frac{d}{n} \leq \frac{\varepsilon}{2L}$, that is $\frac{d}{n} \geq 1 - \frac{\varepsilon}{2L}$. As S sends as side information $(f, f(x))$, for any given x, where f is chosen uniformly at random from the hash family used, the number of bits of side information used will be the sum of the logarithms of the sizes of $\mathcal{F}$ and the range space. This in turn depends on the actual code from which the hash family is obtained.

We now turn to examples of specific codes from which an appropriate hash family is obtained and see how that determines the actual number of bits of side information S sends to R in the randomised scheme for the single message case.

6.3.1 Amount of side information using hash family based on RS codes

In [30], Guruswami suggested the use of Reed-Solomon codes as follows. Consider $\mathbb{F}_q$, where we assume $q = 2^t$, $t > 0$. Let $\mathbb{F}_q[x]_{k'}$ denote the set of all polynomials over $\mathbb{F}_q$ of degree at most k'. The Reed-Solomon code, denoted by C_{RS}, is defined as follows:

For $(c_0, \ldots, c_{k'-1}) \in \mathbb{F}_q^{k'}$ associate a polynomial

$$\phi(x) = c_0 + c_1 x + \ldots + c_{k'-1} x^{k'-1} \in \mathbb{F}_q[x]_{k'}$$

and then define the corresponding codeword as

$$(\psi_0, \ldots, \psi_{q-1}) = (\phi(0), \phi(\alpha_1), \ldots, \phi(\alpha_{q-1})),$$

where we take $\mathbb{F}_q = \{0, \alpha_1, \ldots, \alpha_{q-1}\}$. This defines a $[q, k', d]_q$ code with $d = q - k' + 1$. Then the associated hash family $\mathcal{F}_{RS} = \{f_i \mid 0 \leq i \leq q-1\}$ where $f_i(c_0, \ldots, c_{k'-1}) = \psi_i$, for $0 \leq i \leq q-1$. Then in order that such a hash family can be used in the randomised scheme for the disambiguation problem with message space $\{0,1\}^k$, we may first identify $\{0,1\}^k$ with $\mathbb{F}_q^{k'}$ as follows. Let $x = (x_1, \ldots, x_k) \in \{0,1\}^k$. Split x into $\frac{k}{t}$ substrings such that ith substring represents an element $c_i \in \mathbb{F}_q$ for $0 \leq i \leq q$. Only thing remains to do is to choose the value of q so that we get an AU hash family such that $\frac{d}{n} \geq (1 - \frac{\varepsilon}{2L})$ for given ε and L. Thus we need to choose q, by Lemma 6.2.3, such that

$$\begin{aligned}\frac{d}{n} =& \frac{\left(q - \frac{k}{t} + 1\right)}{q} \\ =& 1 - \frac{k}{qt} + \frac{1}{q} \\ \geq& 1 - \frac{\varepsilon}{2L}.\end{aligned}$$

to meet the collision probability condition. Now as $1 - \frac{k}{qt} + \frac{1}{q} > 1 - \frac{k}{q}$, we may choose a $q = 2^t$ such that $\frac{k}{q} \leq \frac{\varepsilon}{2L}$, that is, $q \geq \frac{2kL}{\varepsilon}$; for this find a t such that $2^{t-1} \leq \frac{2kL}{\varepsilon} < 2^t$ and take $q = 2^t$. We have already seen that in our scheme, the sender sends the pair $(f, f(x))$, which would require sending $2 \log q$ bits of side information. With this choice of q and using the hash family $\mathcal{F}_{RS}$ discussed above, sender sends

$$2 \log q = 2 \log k + 2 \log L + 2 \log \frac{1}{\varepsilon} + O(1)$$

bits of side information in the randomised scheme described in [30]. We state [30, Theorem 2] for the sake of completeness.

Theorem 6.3.1. *For every $p < 1/2$ and every $\varepsilon > 0$, there are probabilistic polynomial time strategies for S and R under which S sends*

$$2 \log q = 2 \log k + 2 \log L + 2 \log \frac{1}{\varepsilon} + O(1)$$

bits of side information which enables R to recover the correct sent message with probability at least $1 - \varepsilon$ when it receives an arbitrary y that satisfies $\delta(y, C(x)) \leq p$. Further, if unable to recover the correct x, R will report a failure.

6.3.2 Amount of side information using hash family based on Hermitian codes

Next we consider hash family corresponding to the Hermitian code discussed in the previous section. Recall that this code is defined over $\mathbb{F}_{q^2}$, for some q that is to be chosen, and the divisors $D = P_1 + \ldots + P_{q^3}$ and $G = uP_\infty$, for some u to be chosen appropriately, where P_i's and P_∞ are all the places of degree one of the Hermitian curve. Note that our message space is $\{0,1\}^k$ and the Hermitian code C_H is the image of $L(G)$ under the evaluation map $ev_D : L(G) \to \mathbb{F}_{q^2}^{q^3}$. Assume that $q = 2^t,\ t > 0$. We then identify $\{0,1\}^k$ with $\mathbb{F}_{q^2}^{k'}$, and the latter with a subspace of $L(G)$.

Theorem 6.3.2. *[12, Theorem 5] There exist randomised strategies for S and R, in which S will have to send* $5 \log q$ *bits of side information for R to find the sent message from the decoded list of messages, where q is given by*

$$q \geq \max \left\{ \frac{3k^{\frac{1}{3}}}{\left(\frac{\varepsilon}{L}\right)^{\frac{1}{3}}}, \frac{2}{\left(\frac{\varepsilon}{L}\right)} \right\} \tag{6.3.1}$$

Proof. We use Hermitian code over $\mathbb{F}_{q^2}$. Let $P_1, \ldots, P_{q^3}; P_\infty$ be all places of degree one of a Hermitian curve. Let $D = P_1 + \ldots + P_{q^3}$ and $G = uP_\infty$ where, $u = \frac{k}{2 \log q} + g$. We are given a message of length k, which is a binary string. This binary string may be thought of as a length $\frac{k}{2 \log q} + 1$ string over the alphabet $\mathbb{F}_{q^2}$. Then by Theorem 1.3.2, the code $C_L(D, G)$ has dimension at least $\frac{k}{2 \log q} + 1$, provided $u < q^3$. Thus, the condition on dimension may be stated as

$$\frac{k}{2 \log q} + g < q^3. \tag{6.3.2}$$

Let us now consider the collision probability requirement. By Lemma 6.2.3, we need to choose a q such that $\frac{d}{q^3} \geq 1 - \frac{\varepsilon}{2L}$. Since $d \geq q^3 - \deg G$, we have $\frac{u}{q^3} \geq 1 - \frac{d}{q^3}$. Hence, it would be sufficient to choose a q such that $\frac{\varepsilon}{2L} \geq \frac{u}{q^3}$. Equivalently,

$$\begin{aligned} \frac{\varepsilon}{2L} &\geq \frac{k}{2q^3 \log q} + \frac{g}{q^3} \\ \frac{\varepsilon q^3}{2L} &\geq \frac{k}{2 \log q} + \frac{q(q-1)}{2} \\ \frac{\varepsilon q^3 \log q}{L} &\geq k + q(q-1) \log q \end{aligned}$$

$$\left(\frac{\varepsilon q^3}{L} - q^2 + q \right) \log q \geq k. \tag{6.3.3}$$

But, if q is chosen to satisfy Condition 6.3.3 then such a q would satisfy Condition 6.3.2 automatically. So, sufficient to find a q satisfying condition 6.3.3. Let $a^3 = \frac{\varepsilon}{L}$. Then, it is easy to see that Condition 6.3.3 may be rewritten as

$$\left(\left(aq - \frac{1}{a^2}\right)^3 + 2q^2 - \left(\frac{3}{a^2} - 1\right)q + \frac{1}{a^6}\right)\log q \geq k.$$

Enough to choose a q which satisfies

$$\left(aq - \frac{1}{a^2}\right)^3 \log q \geq k \tag{6.3.4}$$

and

$$\left(2q^2 - \left(\frac{3}{a^2} - 1\right)q\right)\log q \geq 0 \tag{6.3.5}$$

simultaneously hold.

Clearly, Condition 6.3.5 would hold when $q > \frac{2}{a^3}$. Notice that $\left(aq - \frac{1}{a^2}\right)^3 \log q$ increases and hence any $q \geq \frac{3k^{\frac{1}{3}}}{a}$ satisfies Condition 6.3.4. Hence sufficient to choose a q as in Expression 6.3.1 for Condition 6.3.3 to be satisfied. Next we compute the number bits of side information involved in the scheme.

Recall that the sender picks one f from the family uniformly at random and sends to the receiver the pair $(f, f(x))$, where x is the message. Hence, S will have to send in all $5\log q$ bits as side information. By construction of the hash family, the receiver will be able to disambiguate the sent message from the list of decoded messages with probability at least $1 - \varepsilon$, provided list decoding was a success. Now, we use the value of q from Expression 6.3.1 to obtain a bound on the number of bits of side information. It may be seen that, since ε and L are constants S will have to send asymptotically

$$\frac{5}{3}\log k + \frac{5}{3}\log\frac{L}{\varepsilon} + O(1)$$

bits of side information. ∎

Thus using codes constructed on Hermitian curves instead of Reed Solomon codes, we have reduced the number of bits of side information, thereby obtaining an improvement over [30, Theorem 2].

6.3.3 Amount of side information using hash family based on codes constructed on G-S tower

In this section, we use a suitable higher level function field of the Garcia-Stichtenoth tower to construct the underlying hash family. The strategies for

R and S remain essentially the same. The sender chooses a suitable function field from the tower before constructing the hash family. Then S constructs the code(equivalently, the hash family) by choosing suitable divisors from that function field. The pair $(f, f(x))$ is sent to R as side information, where x is a suitable encoding of the message and f a function chosen at random from the hash family. The receiver, after list decoding the received word, matches $f(z_i)$ with $f(x)$ to disambiguate the list, where $\{z_i \mid 1 \leq i \leq L\}$ is the decoded list. As S sends $(f, f(x))$ receiver needs no knowledge of the underlying function field. The details are given below.

Let us first recall the definition of the second Garcia-Stichtenoth tower defined in the previous section. As we had seen earlier the function field has $N_m > n_m = (q^2 - q)q^{m-1}$ places of degree one and genus $g_m < q^m + q^{m-1}$. Consider a code constructed with $D_m = P_1 + \ldots + P_{n_m}$ and $G_m = \left(\frac{k}{2\log q} + g_m\right) P_\infty$, where support of D_m is disjoint from that of G_m. The subscript m in the divisors indicates that the divisors are from the mth function field of the tower. We now choose a higher function field in the Garcia-Stichtenoth tower judiciously and construct the hash family on it. Notice that in view of the bound on the genus of the mth level, we have

$$\frac{\frac{k}{2\log q} + g_m}{n_m} < \frac{\frac{k}{2\log q} + q^m + q^{m-1}}{n_m}. \tag{6.3.6}$$

Theorem 6.3.3. *[12, Theorem 6] Let $m \geq 3$ be a fixed positive integer. Let $\alpha < 0 < \beta$ be the zeroes of $q^2 - q\left(1 + \frac{2L}{\varepsilon}\right) - \left(1 + \frac{2L}{\varepsilon}\right)$. Then, using a hash functions, one can devise strategies for S and R which use $(m+3)\log q$ bits of side information, where*

$$q \geq \max\left\{\beta, \left(\frac{kL}{\varepsilon}\right)^{\frac{1}{m-1}}\right\}$$

Proof. We use the code constructed on the mth function field of the Garcia-Stichtenoth tower over $\mathbb{F}_{q^2}$, where q will be specified shortly. Let $P_1, \ldots, P_{n_m}; P_\infty$ be a few places of degree one, where P_∞ is the pole of x_1. Let $D = P_1 + \ldots + P_{n_m}$ and $G = uP_\infty$ where, $u = \frac{k}{2\log q} + g_m$. Then by Theorem 1.3.2, the code $C_L(D, G)$ has at least the required dimension, namely $\frac{k}{2\log q} + 1$, provided $u < n_m$. Thus, the condition on dimension may be stated as

$$\frac{k}{2\log q} + g_m < n_m. \tag{6.3.7}$$

Let us now consider the collision probability requirement. In view of ,Lemma 6.2.3 since $d \geq n_m - \deg G$, enough to make

$$\frac{\varepsilon}{2L} \geq \frac{u}{n_m}. \tag{6.3.8}$$

Notice that if a q is chosen to satisfy Condition 6.3.8, then Condition 6.3.7 automatically holds. This may be rewritten, using Inequality 6.3.6, as follows

$$\frac{\varepsilon}{L}q^{m-1}\left(q^2-q-(q+1)\frac{2L}{\varepsilon}\right)\log q \geq k. \tag{6.3.9}$$

Clearly, condition 6.3.9 will hold if

$$\frac{\varepsilon}{L}q^{m-1} \geq k \tag{6.3.10}$$

and

$$\left(q^2-q-(q+1)\frac{2L}{\varepsilon}\right) \geq 1 \tag{6.3.11}$$

simultaneously hold. Condition 6.3.10 holds for $q \geq \left(\frac{kL}{\varepsilon}\right)^{\frac{1}{m-1}}$. Let $\alpha < 0 < \beta$ be the zeroes of $q^2 - q\left(1+\frac{2L}{\varepsilon}\right) - \left(1+\frac{2L}{\varepsilon}\right)$. Then Condition 6.3.11 would be satisfied for $q > \beta$. Notice that β is a constant for a given L and ε. As k tends to infinity $\left(\frac{kL}{\varepsilon}\right)^{\frac{1}{m-1}} > \beta$.

Clearly, $n_m < q^{m+1}$. There are less than q^{m+1} functions in the hash family and each function takes values in alphabet of size q^2. Thus $(m+3)\log q$ bits are sufficient to represent $(f, f(x))$ for $x \in \{0,1\}^k$. Asymptotically, as k increases, in all S needs to send $\left(\frac{m+3}{m-1}\right)\log k + \left(\frac{m+3}{m-1}\right)\log\left(\frac{L}{\varepsilon}\right) + O(1)$ bits of side information. ■

Thus using codes constructed on a suitably chosen higher level function field of the second Garcia-Stichtenoth tower instead of Reed Solomon codes, one can have probabilistic schemes which use lesser number of bits of side information, thereby obtaining an improvement over [30, Theorem 2].

Remark 6.3.4. *The problem of effectively constructing codes on the function field of the tower has been considered in [59]. Here a pole cancellation type algorithm is given for this problem. However construction of such codes is not as easy as Reed Solomon codes.*

6.4 Some concluding remarks

This chapter dealt with list decoding with side information. Randomised strategies for both sender and receiver was seen to reduce the required number of bits of side information drastically. In Guruswami's paper, a Reed-Solomon code based hash family is used to construct such randomised schemes. The scheme with probability at most ε reports failure and returns the whole list. The scheme does not output a wrong message. In Guruswami's paper some theoretical bounds have been proved which lower

bound the bits of side information required. We examined whether the gap between the theoretical bounds and existing schemes could be narrowed. Particularly, we used the same scheme as in Guruswami's paper, but used hash families based on Hermitian curve and function fields of Garcia-Stichtenoth tower and analysed the number of bits of side information required for the scheme. A similar analysis for amortised communication complexity for the repeated communication case may be carried out. Already the Reed-Solomon code based randomised schemes have been analysed in [30].

Chapter 7

Concluding remarks and open problems

In this chapter, we recall the contributions of this thesis and state some open problems. This chapter is divided into three sections.

7.1 Code construction on towers of function fields

Bezerra and Garcia had introduced a tower with non-Galois steps which attains the Drinfeld-Vladut bound. In Chapter 2, a basis-dual basis pair for any function field of the tower is given. The basis is contained in the ring of regular functions of that level, so that any regular function can be written as a linear combination of elements of the dual basis.

Problem 7.1.1. *Determine the Weierstraß semi-group of the pole of x_1 for any function field.*

This would aid in the determination of regular functions for any level. The next problem asks for an algorithm for finding regular functions.

Problem 7.1.2. *Give a pole cancellation algorithm, as in [59], for Bezerra-Garcia tower.*

The second tower of Garcia and Stichtenoth proved to be easier to study than the first one. The Bezerra-Garcia tower is known to be a sub tower of the tower from [26]. It remains to be explored whether the Bezerra-Garcia tower is easier to study than the Garcia-Stichtenoth tower. The next problem asks for alternative algorithms for finding regular functions.

Problem 7.1.3. *Can one give an algorithm similar to [52] for finding regular functions on Bezerra-Garcia tower?*

In Chapter 3, for the Garcia-Stichtenoth tower of [26], the following regular elements could be constructed:

1. first q^2 basis elements and some basis elements in the range q^4 to $q^4 + q^3 - q^2$ for F_4 and
2. some basis elements for F_5 for some values of q.

But the descriptions obtained for F_4 and F_5 are not complete. Whether Theorem 3.1.7 is enough to give a complete description of regular functions similar to F_3 remains to be explored.

Problem 7.1.4. *Give closed form expressions for regular functions in low level function fields of the Garcia-Stichtenoth tower of [26].*

Of course, a similar problem may be asked for Bezerra-Garcia tower also.

7.2 List decoding on towers of function fields

Chapter 4 dealt with the interpolation step of list decoding codes on the Garcia-Stichtenoth tower. Recently, many results applying Gröbner basis techniques to coding theory have been proved. Many questions in this area are open still.

Chapter 5 dealt with finding the non-uniform input required for the root-finding step of list decoding algorithm for algebraic-geometric codes. Codes on towers of function field towers are still not very well understood. Many tasks involved in encoding and list decoding codes on such towers are still cumbersome. A lot is known about the tower of [26]. This work studied the tower of [6]. The strategy for finding non-uniform input on Garcia-Stichtenoth tower was applied for finding the same on the Bezerra-Garcia tower.

Problem 7.2.1. *What is the general class of function fields for which the strategy of Chapter 5 applies?*

Chapter 6 dealt with list decoding with side information. Randomised strategies for both sender and receiver was seen to reduce the required number of bits of side information drastically. In Guruswami's paper, a Reed-Solomon code based hash family is used to construct such randomised schemes. The scheme with probability at most ε reports failure and returns the whole list. The scheme does not output a wrong message. Also, in Guruswami's paper some theoretical bounds have been proved which lower bound the bits of side information required. We examined whether the gap between the theoretical bounds and existing schemes could be narrowed. Particularly, we used the same scheme as in Guruswami's paper, but used hash

families based on Hermitian curve and function fields of Garcia-Stichtenoth tower and analysed the number of bits of side information required for the scheme. A similar analysis for amortised communication complexity for the repeated communication case may be carried out. Already the Reed-Solomon code based randomised schemes have been analysed in [30].

7.3 Asymptotically good towers

The quest for more optimal towers continues. Various techniques derived from class field theory, modular curves etc have been used to construct more optimal towers. The connection between optimality of the towers and modularity has been explored by Elkies. The complete picture is still not clear. In [19], [21] and [20], it is shown that many of the towers are modular. These towers are obtained from elliptic or Drinfeld modular curves. Further Ekies conjectures that all optimal towers are modular, often referred to as 'Elkies fantasia'.

Problem 7.3.1. *Explore the connection between optimality of towers and their modularity.*

We have thus listed only a few open problems of interest related to this thesis. There are many more which may be listed. Thus, the interplay between coding theory and geometry is interesting and deep.

Bibliography

[1] I. Aleshnikov, P. V. Kumar, K. Shum, and H. Stichtenoth. On the splitting of places in a tower of function fields meeting the Drinfeld-Vladut Bound. *IEEE Transactions on Information Theory*, 47(4):1613–1619, 2001.

[2] H. E. Andersen and O. Geil. Evaluation codes from order domain theory. *Finite Fields and their Applications*, 14(1):92–123, 2008.

[3] D. Augot and L. Pecquet. A Hensel lifting to replace factorization in list decoding of algebraic-geometric and Reed-Solomon codes. *IEEE Transactions on Information Theory*, 46(7):2605–2613, 2000.

[4] P. Beelen. Graphs and recursively defined towers of function fields. *Jounal of Number Theory*, 108:217–240, 2004.

[5] P. Beelen, A. Garcia, and H. Stichtenoth. On towers of function fields over finite fields. *Séminaires et Congrès*, 11:1–20, 2005.

[6] J. Bezerra and A. Garcia. A tower with non-Galois steps which attains the Drinfeld-Vladut bound. *Journal of Number Theory*, 106(1):142–154, 2004.

[7] J. Bierbrauer. Universal hashing and geometric codes. *Designs, Codes, Cryptography*, 11(3):201–221, 1997.

[8] R. E. Blahut. *Theory and practice of error control codes.* Addison-Wesley, Massachusetts, 1983.

[9] C. Chevalley. *Introduction to the theory of algebraic functions in one variable.* Number VI in Math Surveys. AMS, Providence, 1951.

[10] P. M. Cohn. *Algebraic numbers and algebraic functions.* Chapman Hall, 1991.

[11] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms: An introduction to computational algebraic geometry and commutative algebra.* Undergraduate Texts in Mathematics. Springer, 1996.

[12] M. P. L. Das. On hash functions and list decoding with side information. *IEICE Transactions*, 90-A(6):1198–1203, 2007. Available at `http://dx.doi.org/10.1093/ietfec/e90-a.6.1198`.

[13] M. P. L. Das and K. Sikdar. List decoding codes on Garcia-Stictenoth tower using Gröbner basis. *Special Issue of Journal of Symbolic Computation (Gröbner Bases Techniques in Cryptography and Coding Theory)*. To appear in print. Available electronically at `http://dx.doi.org/10.1016/j.jsc.2008.02.004`.

[14] M. P. L. Das and K. Sikdar. Regular functions on Bezzera-Garcia tower. *Applicable Algebra in Engineering, Communication and Computing*. Under Revision.

[15] M. P. L. Das and K. Sikdar. On the computation of non-uniform input for list decoding on Bezerra-Garcia tower. In Serdar Boztas and Hsiao-feng Lu, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 17th International Symposium, AAECC-17, Bangalore, India, December 16-20, 2007, Proceedings*, volume 4851 of *Lecture Notes in Computer Science*, pages 237–246. Springer, 2007. Available at `http://dx.doi.org/10.1007/978-3-540-77224-8_28`.

[16] V. Deolalikar. *On splitting places of degree one in extensions of algebraic function fields, towers of function fields meeting asymptotic bounds, and basis constructions for algebraic-geometric codes*. PhD thesis, University of Southern California, 1999.

[17] D. Eisenbud. *Commutative Algebra: With a view toward algebraic geometry*. Number 150 in Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1995.

[18] P. Elias. Coding for noisy channels. Technical report, Research Lab of Electronics, MIT, 1957.

[19] N. D. Elkies. Explicit modular towers. In T. Basar and A. Vardy, editors, *Proceedings of 35th Allerton Conference on Communication, Control and Computing*, pages 23–32, 1997.

[20] N. D. Elkies. Explicit towers of Drinfeld modular curves. *Progress in Mathematics*, 202:189–198, 2001.

[21] N. D. Elkies, E. W. Howe, A. Kresch, B. Poonen, J. L. Wetherell, and M. E. Zieve. Curves of every genus with many points 2: Asymptotically good families. *Duke Mathematical Journal*, 122(2):399–422, 2004.

[22] G. -L. Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Transactions on Information Theory*, 39(1):37–45, 1993.

[23] G. -L. Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Transactions on Information Theory*, 40(4):1003–1012, 1994.

[24] W. Fulton. *Algebraic curves*. Benjamin, Massachusetts, 1969.

[25] A. Garcia and H. Stichtenoth. A tower of Artin-Schreier extensions function fields attaining the Drinfeld-Vladut Bound. *Inventions Mathematicae*, 121:211–222, 1995.

[26] A. Garcia and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[27] O. Geil. Order domains and their application in coding theory. Technical Report R-00-2012, Aalborg University, Available at: `http://www.math.aau.dk/research/reports/2000.htm`[1], 2000.

[28] O. Geil and R. Pellikaan. On the structure of order domains. *Finite Fields and their Applications*, 8(3):369–396, 2002.

[29] V. D. Goppa. Codes on algebraic curves. *Soviet Math. Doklady*, 24:170–172, 1981.

[30] V. Guruswami. List decoding with side information. In *IEEE Conference on Computational Complexity*, pages 300–309. IEEE Computer Society, 2003.

[31] V. Guruswami, J. Håstad, Madhu Sudan, and D. Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, 48(5):1021–1034, 2002.

[32] V. Guruswami and A. Patthak. Correlated algebraic-geometric codes: Improved list decoding over bounded alphabets. *Mathematics of Computation*, 77:447–473, 2008.

[33] V. Guruswami and A. Rudra. Explicit capacity-achieving list-decodable codes. In J. M. Kleinberg, editor, *Proceedings of the 38th Annual ACM Symposium on Theory of Computing (STOC), Seattle, WA, USA, May 21-23, 2006*, pages 1–10. ACM, 2006.

[34] V. Guruswami and Madhu Sudan. Improved decoding of Reed-Solomon and algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[35] V. Guruswami and Madhu Sudan. On representations of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 47(4):1610–1613, 2001.

[36] R. W. Hamming. Error detecting and error correcting codes. *Bell System Technical Journal*, 29:147–160, 1950.

[37] R. Hartshorne. *Algebraic Geometry*. Springer-Verlag, New York, 1977.

[38] T. Høholdt and R. Pellikaan. On the decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 41(6):1589–1614, 1995.

[39] T. Høholdt, J. H. van Lint, and R. Pellikaan. *Handbook of coding theory*, volume 1, chapter Algebraic-Geometric Codes, pages 871–961. Elsevier, 1998.

[40] J. Justesen, K. J. Larsen, H. E. Jensen, and T. Høholdt. Fast decoding of codes from algebraic plane curves. *IEEE Transactions on Information Theory*, 38(1):111–119, 1992.

[41] K. Lee and M. E. O'Sullivan. List decoding of Hermitian codes using Gröbner bases. Arxiv, 2006. Available at: `http://arxiv.org/abs/cs.IT/0610132`[1].

[42] K. Lee and M. E. O'Sullivan. Sudan's list decoding of Reed-Solomon codes from a Gröbner basis perspective. Arxiv, 2006. Available at: `http://www.arxiv.org/abs/math.AC/0601022`[1].

[43] D. A. Leonard. Finding the defining functions for one-point algebraic-geometry codes. *IEEE Transactions on Information Theory*, 47(6):2566–2573, 2001.

[44] J. B. Little. A key equation and the computation of error values for codes from order domains. Arxiv, 2003. Available at: `http://www.arxiv.org/abs/math.AC/0303299`[1].

[45] J. B. Little. The ubiquity of order domains for the construction of error control codes. Arxiv, 2003. Available at: `http://www.arxiv.org/abs/math.AC/0304292`[1].

[46] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes*. Elsevier/North-Holland, Amsterdam, 1981.

[47] R. R. Nilsen. *List decoding of linear block codes*. PhD thesis, Technical University of Denmark, 2001.

[48] H. O'Keeffe and P. Fitzpatrick. Gröbner basis solution of constrained interpolation problems. *Linear Algebra and Applications*, 351-352:533–551, 2002.

[49] M. E. O'Sullivan. New codes for the Berlekamp-Massey-Sakata algorithm. *Finite Fields and their Applications*, 7(2):293–317, 2001.

[50] F. Parvaresh and A. Vardy. Correcting errors beyond the guruswami-sudan radius in polynomial time. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23-25 October 2005, Pittsburgh, PA, USA, Proceedings*, pages 285–294. IEEE Computer Society, 2005.

[51] R. Pellikaan. On the missing functions of a pyramid of curves. In T. Basar and A. Vardy, editors, *Proceedings of 35th Allerton Conference on Communication, Control and Computing*, pages 33–40, 1997.

[52] R. Pellikaan and D. A. Leonard. Integral closures and weight functions over finite fields. *Finite Fields and their Applications*, 9(4):479–504, 2003.

[53] R. Pellikaan, H. Stichtenoth, and F. Torres. Weierstrass semigroups of an asymptotically good tower of function fields. *Finite Fields and their Applications*, 4:381–392, 1998.

[54] O. Pretzel. *Codes and algebraic curves*. Number 8 in Oxford Lecture Series in Mathematics and Its Applications. Clarendon Press, 1998.

[55] S. Sakata. Extension of Berlekamp-Massey algorithm to N dimensions. *Information and Computation*, 84(2):207–239, 1990.

[56] S. Sakata, J. Justesen, Y. Madelung, H. E. Jensen, and T. Høholdt. Fast decoding of algebraic-geometric codes up to the designed minimum distance. *IEEE Transactions on Information Theory*, 41(6):1672–1677, 1995.

[57] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 1948.

[58] A. Shokrollahi and H. Wasserman. List decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 45(2):432–437, 1999.

[59] K. Shum, I. Aleshnikov, P. V. Kumar, H. Stichtenoth, and V. Deolalikar. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound. *IEEE Transactions on Information Theory*, 47(6):2225–2241, 2001.

[60] S. A. Stepanov. *Codes on algebraic curves*. Kluwer Academic/Plenum, N.Y, 1999.

[61] H. Stichtenoth. *Algebraic function fields and codes*. Universitext. Springer-Verlag, 1993.

[62] Madhu Sudan. Decoding Reed-Solomon codes beyond error correction bound. *Journal of complexity*, 13(1):180–193, 1997.

[63] Madhu Sudan. Algorithmic introduction to coding theory. Course notes, 2001. Available at: `http://theory.lcs.mit.edu/~madhu/FT01/course.html`[1].

[64] M. A. Tsfasman and S. Vladut. *Algebraic-geometric codes*. Number 58 in Mathematics and its Applications (Soviet Series). Kluwer Academic Publishers Group, Dordrecht, 1991.

[65] M. A. Tsfasman, S. G. Vladut, and T. Zink. Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert Bound. *Mathematische Nachrichten*, 109:21–28, 1982.

[66] J. H. van Lint. *Introduction to coding theory*. Springer, 1998.

[67] C. Voss and T. Høholdt. An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink Bound. The first steps. *IEEE Transactions on Information Theory*, 43(1):128–135, 1997.

[68] J. M. Wozencraft. List decoding. Quarterly progress report, Research Lab of Electronics, MIT, 1958.

[69] X. -W. Wu and P. H. Siegel. Efficient root-finding algorithm with applications to list-decoding of algebraic-geometric codes. *IEEE Transactions on Information Theory*, 47(6):2579–2587, 2001.

[1] Article is available at the mentioned url as on March 4, 2008.