Graph-based and algebraic codes for error-correction and erasure recovery

Rutuja Milind Kshirsagar

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Mathematics

Gretchen L. Matthews, Chair
Nicholas A. Loehr
Felice Manganiello
Constantin L. Mihalcea

February 9, 2022
Blacksburg, Virginia

Keywords: Graph-based code, decoding, local recovery, algebraic geometry code, code-based cryptography.

Graph-based and algebraic codes for error-correction and erasure recovery

Rutuja Milind Kshirsagar

(ABSTRACT)

Expander codes are sparse graph-based codes with good decoding algorithms. We present a linear-time decoding algorithm for $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander codes based on graphs with any expansion factor given that the minimum distances of the inner codes are bounded below. We also design graph-based codes with hierarchical locality. Such codes provide tiered recovery, depending on the number of erasures. A small number of erasures may be handled by only accessing a few other symbols, allowing for small locality, while larger number may involve a greater number of symbols. This provides an alternative to requiring disjoint repair groups. We also consider availability in this context, relying on the interplay between inner codes and the Tanner graph. We define new families of algebraic geometry codes for the purpose of code-based cryptography. In particular, we consider twisted Hermitian codes, twisted codes from a quotient of the Hermitian curve; and twisted norm-trace codes. These codes have Schur squares with large dimensions and hence could be considered as potential replacements for Goppa codes in the McEliece cryptosytem. However, we study the code-based cryptosystem based on twisted Hermitian codes and lay foundations for a potential attack on such a cryptosystem.

Graph-based and algebraic codes for error-correction and erasure recovery

Rutuja Milind Kshirsagar

(GENERAL AUDIENCE ABSTRACT)

Coding theory finds applications in various places such as data transmission, data storage, and even post-quantum cryptography. The goal of data transmission is to ensure fast and efficient information transfer. It is ideal to correct maximum number of errors introduced during transmission by noisy channels. We provide a new construction of expander codes (graph-based codes) and provide a linear-time decoding algorithm which corrects a constant-fraction of errors for these codes given any expansion factor. In this context, channel noise causes distortion of symbols, so that received symbols may be different than those originally sent. We are also interested in codes for erasure recovery, meaning those which restore missing symbols. A recent technique to recover the sent messages is by accesing a small subset of this received information, called locality. We analyze the locality properties of Tanner codes equipped with specific inner code. Code-based cryptography is a leading candidate in the post-quantum setting, meaning it is believed to be secure against quantum algorithms. The McEliece cryptosystem in which the underlying code is a Goppa code is popularly studied and is a top candidate in the NIST competition. However, the adoption of this system is not immediate due to its large key sizes. Code-based cryptosystems based on codes other than Goppa codes might provide a solution. We provide constructions of a new family of codes, called twisted algebraic geomtery codes which may provide alternatives of Goppa codes in the McEliece cryptosystem.

Acknowledgments

I am grateful to my advisor, Dr. Gretchen L. Matthews for her unconditional support through my PhD. She has been my life coach for the past four years. I would have definitely not been here without her patient personal and professional advice. Thank you for bringing me along with you from Clemson University to Virginia Tech. I am also grateful to the Applied Algebra Research group at Virginia Tech for interesting mathematical discussions. I would also like to thank my committee members Dr. Leonardo Mihalchea and Dr. Nicholas Loehr, for their constructive feedback. Special thanks to Dr. Felice Manganiello at Clemson University for being on my committee and teaching me "The theory of error-correcting codes" during my semester at Clemson University. I would also like to thank Dr. Chandrasheel Bhagwat and Dr. Krishna Kaipa at IISER Pune, Dr. Mohan Chintamani at University of Hyderabad, Dr. Prabal Paul and Dr. Tarkeshwar Singh at BITS Goa for their guidance during my undergraduate studies. Thank you Dr. Karim Eldefrawy and Dr. Nicholas Genise at SRI International, Dr. Moti Yung at Google, Dr. Gabriel Perdue and Dr. Prasanth Shyamsundar at FermiLab, who were my mentors in my various internships. I am also thankful to Kelli Karcher for all her help with my TA duties. This section would be imcomplete without the mention of all my collaborators for their contributions to my development.

I am blessed with a wonderful set of parents, Milind and Mugdha; and a lovely sister Soha. They have always been a pillar of strength. I am grateful to them as this journey would

have been impossible without their non-stop encouragement and motivation. I would like to thank my other family members for their support. I would also like to thank my friends Maitreyee, Veda, Vishakha, Mrinalini, Sumukh, Surhud, Aseem, Bhavul, Siddhartha, Janvi, Poojita, Amrita, Supritha, Ashish, Swetha, Swagatika, Manu, Vibin, Jopaul, Ajit, Shravan, Vaishakhi, Sheril, Onima, Bijo, Ayush, and Aidan among others for always having my back.

Contents

List of Figures ix

List of Tables x

1 Introduction 1

1.1 Linear codes . . . 2

1.2 Important families of linear codes . . . 8

1.2.1 Reed-Solomon codes . . . 8

1.3 Local recovery . . . 10

1.3.1 Locally recoverable codes . . . 10

1.4 Algebraic geometry codes . . . 11

1.4.1 Hermitian codes . . . 15

1.4.2 Codes from a quotient of the Hermitian curve . . . 17

1.4.3 Norm-Trace codes . . . 19

2 Constant fraction decoding 22

2.1 Graph-based codes . . . 22
2.1.1 LDPC codes . . . 22
2.1.2 Tanner codes . . . 23
2.1.3 Expander codes . . . 24
2.2 Preliminaries . . . 29
2.3 Algorithm and analysis . . . 34
2.4 Conclusion . . . 41

3 Graph-based codes for hierarchical recovery 42

3.1 Tanner codes for (hierarchical) recovery . . . 46
3.1.1 Tanner codes as LRCs . . . 46
3.1.2 Tanner codes as HLRCs . . . 52
3.2 Stopping Sets & Local Recovery . . . 57
3.3 Conclusion . . . 62

4 Twisted algebraic geometry codes 64

4.1 Code-based cryptography . . . 64
4.1.1 McElice cryptosystem . . . 66
4.1.2 Code-based cryptosystem based on twisted Hermitian codes . . . 68
4.2 Twisted codes from a quotient of the Hermitian curve . . . 73
4.3 Twisted norm-trace codes . . . 87

5 Conclusions **101**

Bibliography **104**

List of Figures

2.1 A ($\mathfrak{C} = \{2, 3, 4\}, \mathfrak{D} = \{1, 2, 3\}, \alpha = 1/2, \gamma = 3/5$) expander graph G. 26

4.1 McEliece Cryptosystem 66

List of Tables

2.1 Summary of decoding algorithms for various expander codes, where $\ell > 1$, and $t > \frac{1}{\alpha}$. 28

2.2 A $(\{2,3\},\{35,36\},1/2,1/59)$ expander graph $G = (L \dot{\cup} R, E)$ described in terms of neighborhoods of vertices of $R = \{A, B, C, D\}$ 40

Chapter 1

Introduction

Coding theory lies at the intersection of various disciplines such as mathematics, computer science and electrical engineering. Originally, codes were introduced to increase the efficiency of communication. The idea was to ensure that messages transmitted over a noisy communication channel are properly received. Reliability of information passing highly depends on the detection and correction of errors (or recovery of erasures) which are introduced. Error-correcting (erasure-recovering) codes achieve this by addition of redundancy. Now, codes are used in a variety of scenarios. For example, Reed-Solomon codes are used to store information on CDs, DVDs, and other devices; LDPC codes are used in satellite communications; Goppa codes are used in cryptography; and regenerating codes are used for distributed data storage.

In this chapter, we review basic terminology from coding theory and discuss some important families of codes.

1.1 Linear codes

An $[n, k, d]$ linear code $\mathcal{C}$ over a finite field $\mathbb{F}_q$ is a k-dimensional subspace of the n-dimensional vector space $\mathbb{F}_q^n$. Note that n represents the length of the code, k represents the dimension of the code and d represents the minimum distance of the code. Any two elements of $\mathcal{C}$, called codewords, differ in at least d places, that is

$$d = \min\{d(c, c') \,:\, c, c' \in \mathcal{C}, c \neq c'\}$$

where $d(c, c')$ is the Hamming distance, that is

$$d(c, c') = |\{i \,:\, c_i \neq c'_i\}|.$$

The alphabet for $\mathcal{C}$ is $\mathbb{F}_q$. Because all codes considered in this dissertation are linear, we use the term code to mean linear code.

Note that the Hamming distance $d(c, c')$ is a metric. It satisfies the following three properties:

- $d(c, c') \leq d(c, c'') + d(c'', c')$ for all $c, c', c'' \in F_q^n$.
- $d(c, c') = d(c', c)$ for all $c, c' \in \mathbb{F}_q^n$.
- $d(c, c') = 0$ if and only if $c = c'$.

Given a received word in $\mathbb{F}_q^n$, the decoding problem can be loosely phrased as finding a codeword in $\mathcal{C}$ within a distance e from the codeword, where e is as small as possible. An $[n, k, d]$ code is capable of correcting t errors if

$$d \geq 2t + 1.$$

To see this, suppose $c \in \mathcal{C}$ is a sent word, w is the resulting received word and $d(c, w) \leq t$. Consider another codeword $c' \in \mathcal{C} \backslash \{c\}$. If $d(c', w) \leq t$, then

$$d(c, c') \leq d(c, w) + d(w, c') \leq 2t < 2t + 1$$

which contradicts the assumption $d \geq 2t + 1$. Therefore c is the unique codeword nearest to w.

Let $[n] := \{1, \ldots, n\}$. Suppose $w \in \mathbb{F}_q^n$ is a received word resulting from a sent word $c \in \mathcal{C}$ for an $[n, k, d]$ code $\mathcal{C}$. The goal is to determine c. The type of distortion or error depends on the model of the channel used for transmission. An error-correction model assumes that some symbols of c may change during the transmission. In such a model, it is assumed that the location of errors is unknown. The received word is of the form

$$w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n.$$

If the distance between the received word w and sent word c satisfies

$$d(w, c) \leq \lfloor \tfrac{d-1}{2} \rfloor,$$

then c can be recovered from w. In the erasure recovery model, it is assumed that some symbols of c are erased during transmission. In such a model, the received symbols in w are assumed to be corrrect, and the positions of the erasures are known. Here, the received word is of the following form:

$$w \in (\mathbb{F}_q \cup \{?\})^n,$$

where for all $i \in [n]$

$$w_i = \begin{cases} c_i, \\ ? \end{cases}$$

and ? denotes an erasure. If the distance between the received word w and sent word c satisfies

$$d(w, c) \leq d - 1,$$

then c can be recovered from w since $d(w, c) < d$.

The set of all $k \times n$ matrices with entries in $\mathbb{F}_q$ is denoted as $\mathbb{F}_q^{k \times n}$. Since an $[n, k, d]$ code $\mathcal{C}$ is a vector space over $\mathbb{F}_q$, and it has a basis over $\mathbb{F}_q$. Consider a matrix $\mathcal{G} \in \mathbb{F}_q^{k \times n}$ whose rows form a basis of an $[n, k, d]$ code $\mathcal{C}$. Then $\mathcal{G}$ is called a generator matrix of $\mathcal{C}$. The matrix $\mathcal{H} \in \mathbb{F}_q^{(n-k) \times n}$ is a parity-check matrix of the code $\mathcal{C}$ if and only if for all codewords $c \in \mathcal{C}$

$$\mathcal{H}c^T = 0.$$

If $\mathcal{G}$ is a generator matrix and $\mathcal{H}$ is a parity-check matrix of the code $\mathcal{C}$, then

$$\mathcal{G}\mathcal{H}^T = \mathcal{H}\mathcal{G}^T = 0.$$

A code is said to be in the systematic form if it has a generator matrix

$$\mathcal{G} = (I_k | \bar{\mathcal{G}}),$$

where I_k is the $k \times k$ identity matrix and $\bar{\mathcal{G}} \in \mathbb{F}_q^{k \times (n-k)}$. In this case,

$$\mathcal{H} = (-\bar{\mathcal{G}}^T | I_{n-k})$$

is a parity-check matrix of the code.

The dual of the code $\mathcal{C}$ is the vector space orthogonal to the code, meaning

$$\mathcal{C}^{\perp} = \{x \in \mathbb{F}_q^n \,:\, xc^T = 0 \,\forall\, c \in \mathcal{C}\}.$$

The length of $\mathcal{C}^{\perp}$ is n. The dimension of $\mathcal{C}^{\perp}$ is $n-k$. Moreover, the dual of dual of a code is the original code; that is,

$$(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}.$$

If $\mathcal{G}$ is a generator matrix of $\mathcal{C}$, then $\mathcal{G}$ is a parity-check matrix of $\mathcal{C}^{\perp}$. If H is a parity-check matrix of $\mathcal{C}$, then it is a generator matrix of $\mathcal{C}^{\perp}$.

Given a vector $c \in \mathbb{F}_q^n$, the Hamming weight of c is the cardinality of set of all nonzero coordinates of c, that is

$$wt(c) = \mid \{i : c_i \neq 0\} \mid .$$

Moreover weight of the code $\mathcal{C}$ is

$$wt(\mathcal{C}) := |\{i \,:\, c_i \neq 0 \,\forall c \in \mathcal{C}\}|.$$

Consider two codewords $c, c' \in \mathcal{C}$ which differ in d places, that is $d(c, c') = d$, the minimum distance of $\mathcal{C}$. Since $\mathcal{C}$ is a linear code, $c - c' \in \mathcal{C}$. Note the following:

$$\begin{aligned} wt(c - c') &= |\{i \,:\, c_i - c_i' \neq 0\}| \\ &= |\{i \,:\, c_i \neq c_i'\}| \\ &= d(c, c'). \end{aligned}$$

Moreover, $d \geq wt(\mathcal{C})$. If $c' = 0$, then $wt(c - c') = wt(c) \leq d$. Therefore, for a linear code, the

minimum distance d is equal to the smallest Hamming weight of a codeword in $\mathcal{C}$, meaning

$$d = \min\{wt(c) \,:\, c \in \mathcal{C}\backslash\{0\}\}.$$

Given an $[n, k, d]$ code $\mathcal{C}$ and $I := \{i_1, \ldots, i_s\} \subseteq [n]$, a punctured code obtained from $\mathcal{C}$ with respect to I is

$$\mathcal{C}|_I := \{(c_{i_1}, \ldots, c_{i_s}) : c = (c_1, \ldots, c_n) \in \mathcal{C}\}.$$

Note that $\mathcal{C}|_I$ is an $[|I|, k - (n - |I|), d']$ code, where $d' \leq d$.

Let $\mathcal{C}_1$ be an $[n_1, k_1, d_1]$ code and $\mathcal{C}_2$ an $[n_2, k_2, d_2]$ code. Then the concatenated code $\mathcal{C}$ is comprised of codewords obtained by placing the codewords of $\mathcal{C}_1$ and $\mathcal{C}_2$ adjacent to each other in order. Note that the length of the concatenated code $\mathcal{C}$ is $n_1 + n_2$, the dimension of $\mathcal{C}$, denoted $\dim(\mathcal{C})$, is at most $k_1 + k_2$, and the minimum distance of $\mathcal{C}$, denoted $d_{\min}(\mathcal{C})$, is $\min\{d_1, d_2\}$.

Given an $[n, k, d]$ code $\mathcal{C}$, the support of $\mathcal{C}$ is the set of all nonzero coordinates, that is,

$$supp(\mathcal{C}) = \{i \,:\, \exists\, c \in \mathcal{C} \text{ with } c_i \neq 0\}.$$

The rate of an $[n, k, d]$ code $\mathcal{C}$ is

$$r = \tfrac{k}{n}.$$

The capacity of a channel is the measure of the maximum rate of reliable transmission. Shannon's Theorem proves the existence of codes which allow information transmission at the rate approaching the channel capacity. The relative distance of an $[n, k, d]$ code $\mathcal{C}$ is

$$\delta = \tfrac{d}{n}.$$

The relative distance of a code determines an upper bound on the fraction of errors (or erasures) that can be corrected (recovered).

Finding the minimum distance of a code is a widely studied problem, but determining the exact minimum distance of a code is a difficult problem. Several bounds have been given for the minimum distance of codes. For an $[n, k, d]$ code $\mathcal{C}$, the Singleton Bound states:

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

Let $\mathcal{C}' = \mathcal{C}|_I$ such that $I = \{d, \ldots, n\}$. Then $\mathcal{C}'$ is an $[n - d + 1, k', d]$ where $k' = k - d + 1$. Since $k' \leq n$, we have $k - d + 1 \leq n$, that is $d \leq n - k + 1$. Hence

$$\frac{d}{n} + \frac{k}{n} \leq 1 + \frac{1}{n},$$

demonstrates the trade off between rate and relative distance. A code $\mathcal{C}$ is said to be maximum distance separable (MDS) if the Singleton bound is attained, in other words

$$d = n - k + 1.$$

Consider a finite field $\mathbb{F}_q$ and a positive integer n. Let $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ be two vectors. Then the Schur product of the vectors $\mathbf{x}$ and $\mathbf{y}$ is

$$\mathbf{x} * \mathbf{y} := (x_1 y_1, \ldots, x_n y_n) \in \mathbb{F}_q^n.$$

Let $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^n$ be two linear codes. Then the Schur product of $\mathcal{C}_1$ and $\mathcal{C}_2$ is

$$\mathcal{C}_1 * \mathcal{C}_2 := \langle \mathbf{c_1} * \mathbf{c_2} \mid \mathbf{c_1} \in \mathcal{C}_1, \mathbf{c_2} \in \mathcal{C}_2 \rangle \subseteq \mathbb{F}_q^n,$$

meaning $\mathcal{C}_1 * \mathcal{C}_2$ is the span of all vectors of the form $\mathbf{c_1} * \mathbf{c_2}$, where $\mathbf{c_1} \in \mathcal{C}_1, \mathbf{c_2} \in \mathcal{C}_2$ consisting of linear combinations with coefficients in $\mathbb{F}_q$. The Schur square of a linear code $\mathcal{C}$ is

$$\mathcal{C}^2 := \mathcal{C} * \mathcal{C}.$$

Later, codes of interest will be obtained by evaluating sets of functions. Hence, it is useful to consider the Schur product of sets of polynomials. We use the notation $\mathbb{F}_q[x_1, \ldots, x_m]$ to mean set of all polynomials for the form

$$f_1 x_1 + \cdots + f_m x_m,$$

where for all $i \in [m]$, $f_i \in \mathbb{F}_q$ and x_i is an indeterminate. Given $B, B' \subseteq \mathbb{F}_q[x, y]$, let

$$B \underline{*} B' := \{\mathbf{b} \cdot \mathbf{b}' \mid \mathbf{b} \in B, \mathbf{b}' \in B'\} \subseteq \mathbb{F}_q[x, y],$$

and if $B = B'$,

$$B \underline{*} B' = B^{\underline{2}} := B \underline{*} B \subseteq \mathbb{F}_q[x, y].$$

1.2 Important families of linear codes

1.2.1 Reed-Solomon codes

Reed-Solomon (RS) codes are a special type of MDS codes defined in [26]. They are perhaps the most commonly used error-correcting codes. Consider a finite field $\mathbb{F}_q$. Let $\alpha_1, \ldots, \alpha_n$ be distinct elements of $\mathbb{F}_q$, so $n \leq q$. Reed-Solomon codes can be expressed as evaluations

of polynomials of degree at most $k-1$, at the $\alpha_i's$ where $k \in \mathbb{Z}$, $k < n < q$.

$$\mathcal{C}_{RS} := \{(f(\alpha_1), \ldots, f(\alpha_n)) \ : \ f \in \mathbb{F}_q[x]_{\leq k-1}\},$$

where $\mathbb{F}_q[x]_{\leq k-1}$ represents the set of all polynomials of degree at most $k-1$ indeterminate x with coefficients in $\mathbb{F}_q$. Let $v_1, \ldots, v_n \in \mathbb{F}_q \backslash \{0\}$. A generalized Reed-Solomon (GRS) code is a linear code

$$\mathcal{C}_{GRS} := \{(v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) \ : \ f \in \mathbb{F}_q[x]_{\leq k-1}\}.$$

A parity-check matrix of a GRS code is

$$\mathcal{H}_{GRS} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_1^{n-k-1} & \alpha_2^{n-k-1} & \ldots & \alpha_n^{n-k-1} \end{bmatrix} \times \begin{bmatrix} v_1 & 0 & \ldots & 0 \\ 0 & v_2 & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & v_n \end{bmatrix}. \tag{1.1}$$

The length n of the generalized Reed-Solomon code is at most q, the size of the finite field. Consider an $[n, k, n-k+1]$ generalized Reed-Solomon code $\mathcal{C}$, then its dual code $\mathcal{C}^{\perp}$ is an $[n, n-k, k+1]$ generalized Reed-Solomon code. Let the parity-check matrix for $\mathcal{C}$ be as given in equation (1.1). Then the generator matrix of $\mathcal{C}$, which is also the parity-check matrix of $\mathcal{C}^{\perp}$ is

$$\mathcal{G}_{GRS} = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \ldots & \alpha_n^2 \\ \vdots & \vdots & \ldots & \vdots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \ldots & \alpha_n^{k-1} \end{bmatrix} \times \begin{bmatrix} v_1' & 0 & \ldots & 0 \\ 0 & v_2' & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & v_n' \end{bmatrix},$$

where $v'_1, \ldots, v'_n \in \mathbb{F}_q \backslash \{0\}$. Note that

$$\begin{aligned}\mathcal{G}_{GRS}\mathcal{H}_{GRS}^T &= \begin{bmatrix} \sum_{i=1}^n v'_i v_i & \sum_{i=1}^n v'_i v_i \alpha_i & \ldots & \sum_{i=1}^n v'_i v_i \alpha_i^{(n-k-1)} \\ \sum_{i=1}^n v'_i v_i \alpha_i & \sum_{i=1}^n v'_i v_i \alpha_i^2 & \ldots & \sum_{i=1}^n v'_i v_i \alpha_i^{(n-k)} \\ \vdots & \vdots & \ldots & \vdots \\ \sum_{i=1}^n v'_i v_i \alpha_i^{(k-1)} & \sum_{i=1}^n v'_i v_i \alpha_i^k & \ldots & \sum_{i=1}^n v'_i v_i \alpha_i^{(n-2)} \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ldots & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix} \\ &= 0^{k \times (n-k)}.\end{aligned}$$

If $v_1 = \ldots = v_n = 1$, then the generalized Reed-Solomon code is the Reed-Solomon code.

1.3 Local recovery

1.3.1 Locally recoverable codes

The notion of locality was first introduced in [11]. Codes with locality, also called locally recoverable codes (LRCs), allow recovery of an erasure by accessing few of the surviving codeword symbols. Formally, LRCs can be defined as follows:

Definition 1.1. An (n, k, r) locally recoverable code $\mathcal{C}$ over $\mathbb{F}_q$ has locality r if for all $i \in \{1, \ldots, n\}$ there exists a set $R_i \subseteq [n] \backslash \{i\}$ such that $|R_i| \leq r$ and there exists a function ϕ_i such that for every codeword $c = (c_1, \ldots, c_n) \in \mathcal{C}$

$$c_i = \phi_i(\{c_j \, : \, j \in R_i\}).$$

The set R_i is called a recovery set of the symbol with index i. Any coordinate can always be recovered by accesing k other coordinates. Hence, we may assume $r \leq k$, where k is the dimension of $\mathcal{C}$. If there are a such disjoint sets of at most r symbols, the code is said to

have an availability a and is denoted as an (n, k, r, a) code.

The idea of locality has been widely explored in the literature. Kamath et al extended the definition of locally recoverable codes to (r, ρ) locality in [19]. These codes allow recovery of up to $\rho - 1$ erasures as we will describe now using the notion of punctured codes.

Definition 1.2. An $[n, k, d]$ code $\mathcal{C}$ is a locally recoverable code with locality (r, ρ) if for all $i \in [n]$ there exists $I_i \subseteq [n] \backslash \{i\}$ such that $\mathcal{C}|_{I_i \cup \{i\}}$ is an $[|I_i| + 1, \leq r, \geq \rho]$ code.

Availability τ means that recovery can be accomplished using τ disjoint sets of symbols.

Definition 1.3. An $[n, k, d]$ code $\mathcal{C}$ is a locally recoverable code with locality $(r_j, \rho_j)_{1 \leq j \leq \tau}$ and availability τ if for the punctured codes $\mathcal{C}|_{I_{1,i} \cup \{i\}}, \ldots, \mathcal{C}|_{I_{\tau,i} \cup \{i\}}$ such that $I_{1,i}, \ldots, I_{\tau,i} \subseteq [n]$ for all $i \in [n]$, the following conditions hold:

- $i \in \text{supp}(\mathcal{C}|_{I_{j,i} \cup \{i\}})$,
- $\mathcal{C}|_{I_{j,i} \cup \{i\}}$ is an $[|I_{j,i}| + 1, \leq r_j, \geq \rho_j]$ code, and
- the set $\text{supp}(\mathcal{C}|_{I_{j,i} \cup \{i\}}) \backslash \left[\cup_{\ell \in [\tau], \ell \neq j} \text{supp}(\mathcal{C}|_{I_{\ell,i} \cup \{i\}}) \right]$ has $\dim(\mathcal{C}|_{I_{j,i} \cup \{i\}})$ linearly independent coordinates of $\mathcal{C}|_{I_{j,i} \cup \{i\}}$.

1.4 Algebraic geometry codes

Let $\mathcal{X}$ be a curve over a finite field $\mathbb{F}_{q^r}$ defined by $\mathbb{F}_{q^r}(x, y, z) = 0$. Throughout this dissertation, we consider smooth, projective, absolutely irreducible curves. Let $g, h \in \mathbb{F}_{q^r}[X, Y, Z]$ be homogeneous of the same degree. The field of rational functions on $\mathcal{X}$ is

$$\mathbb{F}_{q^r}(\mathcal{X}) := \left(\left\{ \frac{g(X, Y, Z)}{h(X, Y, Z)} \right\} \cup \{0\} \right) / \sim$$

where $\frac{g}{h} \sim \frac{g'}{h'}$ if and only if $gh' - g'h$ is a multiple of $\mathbb{F}_{q^r}(x, y, z)$. Let $\mathbb{Z}$ represent the set of all integers. A divisor D on the curve $\mathcal{X}$ can be represented as

$$D := \sum n_P P,$$

where $n_P \in \mathbb{Z}$ and P is a point on $\mathcal{X}$. The degree of divisor D is

$$deg(D) := \sum n_P \deg(P)$$

and the support of D is

$$supp(D) := \{P \,:\, n_p \neq 0\}.$$

Let $\mathcal{X}$ and $\mathcal{X}'$ be two projective curves over $\mathbb{F}_{q^r}$ defined by polynomials of degree d and e respectively. Let $P_1, \ldots, P_\ell$ be points over $\mathbb{F}_{q^r}$ of degrees $r_1, \ldots, r_\ell$ where $\mathcal{X}$ and $\mathcal{X}'$ intersect. Then the intersection divisor of the curves is

$$\mathcal{X} \cap \mathcal{X}' := P_1 + \cdots + P_\ell.$$

Consider $f := \frac{g}{h} \in \mathbb{F}_{q^r}(\mathcal{X})$. Let $\mathcal{X}_g$ be the curve defined by g and $\mathcal{X}_h$ be the curve defined by h. The divisor of f is defined as

$$div(f) := \sum P - \sum Q,$$

where $\sum P = \mathcal{X} \cap \mathcal{X}_g$ and $\sum Q = \mathcal{X} \cap \mathcal{X}_h$. Let $r \in \mathbb{Z}^+$, where $\mathbb{Z}^+$ represents the set of all positive integers. Let G and $D := P_1 + \cdots + P_n$ be divisors on $\mathcal{X}$ such that $P_1, \ldots, P_n$ are distinct $\mathbb{F}_{q^r}$-rational points and the support of G does not contain any of the P_i. Consider

the space of functions

$$\mathcal{L}(G) = \{f \in \mathbb{F}_{q^r} : (f) \geq -G\} \cup \{0\}$$

on $\mathcal{X}$. An algebraic geometric code is of the form

$$\mathcal{C}(D, G) = \{ev(f) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_{q^r}^n$$

where

$$ev(f) = (f(P_1), f(P_2), \ldots, f(P_n))$$

and

$$\begin{array}{rccc} ev: & \mathcal{L}(G) & \to & \mathbb{F}_{q^r}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)) \,. \end{array}$$

The code $\mathcal{C}(D, G)$ is an $[n, \dim(\mathcal{L}(G)) - \dim(\mathcal{L}(G - D)), \geq n - \deg(G)]$ code [32, Theorem 2.2.2]. If $\deg G < n$, then $\dim(\mathcal{L}(G)) - \dim(\mathcal{L}(G - D)) = \dim(\mathcal{L}(G))$ and $\mathcal{C}(D, G)$ is an $[n, \dim(\mathcal{L}(G)), \geq n - \deg(G)]$ code. Since

$$\dim \mathcal{L}(G) \geq \deg(G) + 1 - g,$$

according to the Riemann-Roch Theorem, where g is the genus of $\mathcal{X}$,

$$\dim(\mathcal{C}) + d \geq n + 1 - g.$$

If $2g - 2 < deg(G) < n$, then

$$\dim(\mathcal{C}) = \deg(G) + 1 - g.$$

If $|supp(G)| = 1$ and D is the sum of the remaining $\mathbb{F}_{q^r}$-rational points, the code is called a one-point code and is denoted by $\mathcal{C}(G)$. If $G \leq G'$, where G' is another divisor on $\mathcal{X}$ whose support does not contain any of the P_i, then $\mathcal{L}(G) \subseteq \mathcal{L}(G')$ and $\mathcal{C}(D, G) \subseteq \mathcal{C}(D, G')$.

The Hasse-Weil Bound provides an upper bound on the number n of $\mathbb{F}_{q^r}$-rational places on the curve $\mathcal{X}$, $r \geq 1$ [32, equation 5.19]. If $\mathcal{X}$ has genus g, then

$$|n - (q^r + 1)| \leq 2gq^{r/2}.$$

Note that if the number of $\mathbb{F}_{q^r}$-rational points on $\mathcal{X}$ with genus g is

$$n = q^r + 1 + 2gq^{r/2}$$

then the curve $\mathcal{X}$ is said to be a maximal curve. Maximal curves support the construction of long algebraic geometry codes.

Example 1.4. Consider $r = 1$. The projective line over $\mathbb{F}_q$ is

$$\mathbb{P}^1(\mathbb{F}_q) := (\mathbb{F}_{q^2} \backslash \{(0,0)\}) \,/\, \sim$$

where $(X_0, Y_0) \sim (X_1, Y_1)$ if and only if there exists $\alpha \in \mathbb{F}_q \backslash \{0\}$ such that $X_1 = \alpha X_0$ and $Y_1 = \alpha Y_0$.

The unique point at infinity on this curve is $P_\infty := (1 : 0)$. Consider the divisors $G = (k-1)P_\infty$; and D to be the sum of all other rational points on $\mathcal{X}$, and the vector space $\mathcal{L}(G)$. Then the algebraic geometry code

$$\mathcal{C}(D, G) = \{ev(f) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n$$

is an $[n, k, d]$ code. Note that $\deg(G) = k-1$ and $d \geq n - \deg(G)$, therefore $d \geq n-(k-1)$. By Singleton Bound $d \leq n-k+1$, we have $d = n-k+1$. That is, $\mathcal{C}(D, G)$ is an MDS code. Therefore Reed-Solomon codes are one-point codes on $\mathcal{X} = \mathbb{P}^1(\mathbb{F}_q)$, the projective line. The alphabet size (cardinality of the field $\mathbb{F}_q$) is at least n; thus, to define a Reed-Solomon code of length n requires that $n \leq q$.

Given $n = q^r + 1 + 2gq^{r/2}$, to construct longer codes over $\mathbb{F}_{q^r}$ requires larger genus curves. This motivates the next family of codes.

1.4.1 Hermitian codes

Beyond Reed-Solomon codes, the best understood algebraic geometry codes are Hermitian codes. There are a number of excellent references such as [29], [30], [32], or [33] which provide more comprehensive surveys.

Hermitian codes are special types of algebraic geometry codes based on Hermitian curves. Consider the Hermitian curve

$$\mathcal{X}_q \ : \ y^q + y = x^{q+1}$$

over the finite field $\mathbb{F}_{q^2}$. Note that $\mathcal{X}_q$ has genus

$$g = \frac{q(q-1)}{2}.$$

There are q^3 affine $\mathbb{F}_{q^2}$-rational points of the form

$$(a : b : 1) \in \mathbb{P}^2\left(\mathbb{F}_{q^2}\right)$$

where $b^q + b = a^{q+1}$, since for every $a \in \mathbb{F}_{q^2}$ there are exactly q values of $b \in \mathbb{F}_{q^2}$ which satisfy

the equation $y^q + y = a^{q+1}$. We call these points the affine points of $\mathcal{X}_q$. Also note that $\mathcal{X}_q$ has a point at infinity, $P_\infty := (0 : 1 : 0)$. The number of $\mathbb{F}_{q^2}$-rational points on $\mathcal{X}_q$ satisfies

$$q^2 + 1 + 2gq^{2/2} = q^2 + 1 + q(q-1)q = q^2 + 1 + q^3 - q^2 = q^3.$$

Therefore, the Hermitian curve is a maximal curve. Let

$$n := q^3$$

and $P_1, \ldots, P_n$ be the affine points of $\mathcal{X}_q$. Given a vector space V of functions on $\mathcal{X}_q$ which do not have poles at any of the P_i, $1 \leq i \leq n$, consider the map

$$\begin{array}{rccc} ev_H : & V & \to & \mathbb{F}_{q^2}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)) . \end{array}$$

Then $\mathcal{C} := ev_H(V)$ is a code of length n. For $\alpha \in \mathbb{N}$, where $\mathbb{N}$ represents the set of all nonnegative integers, with $2g - 2 < \alpha < n$, consider the space of functions $\mathcal{L}(\alpha P_\infty)$. It can be shown that

$$\{x^i y^j : i, j \in \mathbb{N}, j \leq q-1, \delta_H(x^i y^j) \leq \alpha\}$$

is a basis for $\mathcal{L}(\alpha P_\infty)$, where

$$\delta_H(x^i y^j) := iq + j(q+1)$$

is the pole order of $x^i y^j$ at P_∞. The one-point Hermitian code determined by α is the algebraic geometry code

$$\mathcal{C}(\alpha P_\infty) = ev_H\left(\mathcal{L}\left(\alpha P_\infty\right)\right).$$

Note that the length of $\mathcal{C}(\alpha P_\infty)$ is q^3. Its dimension is bounded below by $\alpha + 1 - g$, with equality achieved when $\alpha \geq 2g - 1$, and minimum distance as given in [35]. In general, the

minimum distance d satisfies the inequality

$$d \geq q^3 - \alpha.$$

1.4.2 Codes from a quotient of the Hermitian curve

Next we consider codes on a quotient of the Hermitian curve, given by

$$\mathcal{X}_{q,m} \, : \, y^q + y = x^m$$

over the finite field $\mathbb{F}_{q^2}$ where $m|q+1$. If $m = q+1$, then we get the Hermitian curve. The genus of $\mathcal{X}_{q,m}$ is

$$g = \frac{(m-1)(q-1)}{2}.$$

As we will see, there are $q(m(q-1)+1)$ affine $\mathbb{F}_{q^2}$-rational points of the form

$$(a : b : 1) \in \mathbb{P}^2 \left(\mathbb{F}_{q^2}\right)$$

where $b^q + b = a^m$. Note that unlike in the case of the Hermitian curve, every $a \in \mathbb{F}_{q^2}$ does not have a corresponding $b \in \mathbb{F}_{q^2}$ satisfying a quotient of the Hermitian curve $\mathcal{X}_{q,m}$ since the order of a^m must divide $q-1$. There are $m(q-1)+1$ choices for $a \in \mathbb{F}_{q^2}$ and each one has q corresponding values of $b \in \mathbb{F}_{q^2}$ which satisfies a quotient of the Hermitian curve $\mathcal{X}_{q,m}$. The number of $\mathbb{F}_{q^2}$-rational points on $\mathcal{X}_{q,m}$ satisfies

$$q^2+1+2gq^{2/2} = q^2+1+(m-1)(q-1)q = q^2+1+mq^2-mq-q^2+q = q(m(q-1)+1)+1.$$

Therefore a quotient of the Hermitian curve is a maximal curve with $(q(m(q-1)+1)$ affine points and one point at infinity, $P_\infty := (1:0:0)$. Let

$$n := q(m(q-1)+1)$$

and $P_1, \ldots, P_n$ be affine points of $\mathcal{X}_{q,m}$. Given a vector space V of functions on $\mathcal{X}_{q,m}$ which do not have poles at any of the P_i, $1 \leq i \leq n$, consider the map

$$\begin{array}{rccc} ev_{QH}: & V & \to & \mathbb{F}_{q^2}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)) \,. \end{array}$$

Then $\mathcal{C} := ev_{QH}(V)$ is a code of length n, called a code from a quotient of the Hermitian curve. For $\alpha \in \mathbb{N}$ with $2g-2 < \alpha < n$, consider the space of functions $\mathcal{L}(\alpha P_\infty)$. It can be shown that

$$\{x^i y^j : i, j \in \mathbb{N}, j \leq q-1, \delta_{QH}(x^i y^j) \leq \alpha\}$$

is a basis for $\mathcal{L}(\alpha P_\infty)$ where

$$\delta_{QH}(x^i y^j) := iq + jm$$

is the pole order of $x^i y^j$ at P_∞. The one-point code from a quotient of the Hermitian curve determined by α is the algebraic geometry code

$$\mathcal{C}(\alpha P_\infty) = ev_{QH}\left(\mathcal{L}\left(\alpha P_\infty\right)\right).$$

Note that the length of the code $\mathcal{C}(\alpha P_\infty)$ is $q(m(q-1)+1)$. Its dimension is bounded below by $\alpha + 1 - g$, with equality achieved when $\alpha \geq 2g-1$, and minimum distance as given in [21].

1.4.3 Norm-Trace codes

Norm-trace codes are a natural extension of Hermitian codes. These codes based on norm-trace curves. Consider the norm-trace curve

$$\mathcal{X}_q^r : Tr(y) = N(x)$$

over the finite field $\mathbb{F}_{q^r}$ where $r \in \mathbb{N}$, where

$$Tr(y) = y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y$$

is the trace of y and

$$N(x) = x^{\frac{q^r-1}{q-1}}$$

is the norm of x. If $r = 2$, then the norm-trace curve is essentially the Hermitian curve. The genus of the norm-trace curve $\mathcal{X}_q^r$ is

$$g = \frac{q^{r-1}\left(\frac{q^r-1}{q-1}\right)}{2}.$$

There are q^{2r-1} affine $\mathbb{F}_{q^r}$-rational points of the form

$$(a : b : 1) \in \mathbb{P}^2\left(\mathbb{F}_{q^r}\right)$$

where $b^{q^{r-1}} + b^{q^{r-2}} + \cdots + b = a^{\frac{q^r-1}{q-1}}$, since for every $a \in \mathbb{F}_{q^r}$ there are exactly q values of $b \in \mathbb{F}_{q^r}$ which satisfiy the equation $Tr(b) = N(a)$. Unlike the Hermitian curve and a quotient of the Hermitian curve, the norm-trace curve, $\mathcal{X}_q^r$ is not maximal; the number of rational

points of $\mathcal{X}_q^r$ does not meet the upper limit of the Hasse-Weil bound

$$\left(q^{r-1}\left(\frac{q^r-1}{q-1}\right)q^{r/2}+q^r+1\right).$$

Let

$$n := q^{2r-1}$$

and $P_1, \ldots, P_n$ be affine rational points of $\mathcal{X}_q^r$. Given a vector space V of functions on $\mathcal{X}_q^r$ which do not have poles at any of the P_i, $1 \leq i \leq n$, consider the map

$$\begin{array}{rccc} ev_{NT}: & V & \to & \mathbb{F}_{q^r}^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)). \end{array}$$

Then $\mathcal{C} := ev_{NT}(V)$ is a code of length n, called a norm-trace code. For $\alpha \in \mathbb{N}$ with $2g-2 < \alpha < n$, consider the space of functions $\mathcal{L}(\alpha P_\infty)$. It can be shown that

$$\{x^i y^j : i, j \in \mathbb{N}, j \leq q^{r-1}-1, \delta_{NT}(x^i y^j) \leq \alpha\}$$

is a basis for $\mathcal{L}(\alpha P_\infty)$ where

$$\delta_{NT}(x^i y^j) := i\left(q^{r-1}\right) + j\left(\frac{q^r-1}{q-1}\right)$$

is the pole order of $x^i y^j$ at $P_\infty := (0:1:0)$. The one-point norm-trace code determined by α is the algebraic geometry code

$$\mathcal{C}(\alpha P_\infty) = ev_{NT}\left(\mathcal{L}\left(\alpha P_\infty\right)\right).$$

Note that the length of the code $\mathcal{C}(\alpha P_\infty)$ is q^{2r-1}. Its dimension is bounded below by $\alpha+1-g$, with equality achieved when $\alpha \geq 2g-1$, and minimum distance as given in [22].

Chapter 2

Constant fraction decoding

2.1 Graph-based codes

2.1.1 LDPC codes

Low density parity-check (LDPC) codes were introduced in [23] by Galleger but were relatively unnoticed until the 1990s when turbo codes were introduced. It was noticed that the turbo codes have many similarities with LDPC codes, in particular the decoding algorithm for turbo codes is a special case for the decoding algorithm for LDPC codes. LDPC codes derive their name from the fact that it has a sparse parity-check matrix. A Tanner graph of an $[n, k, d]$ binary code $\mathcal{C}$ can be constructed using a parity-check matrix $H \in \mathbb{F}_2^{(n-k)\times n}$ of the code. Let $G = (L \dot{\cup} R, E)$ be a bipartite graph. The nodes in $L = \{c_i : i \in [n]\}$ are called variable nodes whereas nodes in $R = \{y_j : j \in [m]\}$ are called check nodes. The graph G is a Tanner graph of a (w_r, w_c)-LDPC code, $\mathcal{C}$ if it satisfies the following properties:

- Every node in L denotes a codeword symbol and every node in R represents a parity-

check condition given by a row of H. That is, for every $i \in [n]$, the neighbors of c_i in R sum up to zero.

- The set $\{c_i, y_j\}$ represents an edge in E if and only if the entry in H corresponding to row j and column i, $H_{j,i} \neq 0$.

- If each row of H has w_r 1's and each column of H has w_c 1's, then $w_c << n$ and $w_r << m$.

2.1.2 Tanner codes

A Tanner code (or generalized LDPC codes) is an LDPC code where the check-nodes of the bipartite graph representing the parity-check matrix are replaced with shorter codes called inner codes, rather than being treated as simple parity checks.

Definition 2.1. Let $G = (L \dot{\cup} R, E)$ be a bipartite graph. Suppose the nodes in L have degrees which are elements of the set $\mathfrak{C} := \{\mathfrak{c}_1, \ldots, \mathfrak{c}_{\ell_1}\}$ for some $\ell_1 \in \mathbb{Z}^+$, $|L| = n$, and the nodes in R have degrees which are elements of the set $\mathfrak{D} := \{\mathfrak{d}_1, \ldots, \mathfrak{d}_{\ell_2}\}$ for $\ell_2 \in \mathbb{Z}^+$, $|R| = m$. Given $s \in [\ell_2]$, let $\mathcal{C}_s \subseteq \mathbb{F}_q^{\mathfrak{d}_s}$ be a linear code of length $\mathfrak{d}_s$. Assume that the neighborhood of $j \in R$,

$$N(j) := \{i : (i, j) \in E\} \subseteq L,$$

is ordered so that for any vector $\mathbf{x} = (x_i)_{i \in L} \in \mathbb{F}_q^n$, $\mathbf{x}|_{N(j)}$ denotes $(x_i)_{i \in N(j)}$. The associated Tanner code can be defined as follows:

$$\mathcal{T}(G, \{\mathcal{C}_1, \ldots, \mathcal{C}_{\ell_2}\}) = \{c : c|_{N(j)} \in \mathcal{C}_j \, \forall \, j \in R\} \subseteq \mathbb{F}_q^n.$$

This definition is not standardized in the literature. If

$$\mathfrak{c}_1 = \cdots = \mathfrak{c}_\ell = \mathfrak{c}$$

and

$$\mathfrak{d}_1 = \cdots = \mathfrak{d}_{\ell_2} = \mathfrak{d},$$

then we get the standard definition of Tanner codes, where $\mathcal{C}$ is the inner code associated every parity-check node:

$$\mathcal{T}(G, \{\mathcal{C}\}) = \{c : c|_{N(j)} \in \mathcal{C}\} \subseteq \mathbb{F}_q^n.$$

2.1.3 Expander codes

Expander codes [1] are Tanner codes formed using expander graphs. Let $G = (L \dot{\cup} R, E)$ be a bipartite graph where the nodes in L have degrees which are elements of the set $\mathfrak{C} := \{\mathfrak{c}_1, \ldots, \mathfrak{c}_{\ell_1}\}$ for some positive integer ℓ_1, $|L| = n$, and the nodes in R have degrees which are elements of the set $\mathfrak{D} := \{\mathfrak{d}_1, \ldots, \mathfrak{d}_{\ell_2}\}$ for some positive integer ℓ_2. Given $s \in [\ell_2]$, let $\mathcal{C}_s \subseteq \mathbb{F}_q^{\mathfrak{d}_s}$ be a linear code of length $\mathfrak{d}_s$. Assume that the neighborhood of $j \in R$,

$$N(j) := \{i : (i, j) \in E\} \subseteq L,$$

is ordered so that for any vector $\mathbf{x} = (x_i)_{i \in L} \in \mathbb{F}_q^n$, $\mathbf{x}|_{N(j)}$ denotes $(x_i)_{i \in N(j)}$. Assume $\mathfrak{c}_1 < \cdots < \mathfrak{c}_{\ell_1}$ and $\mathfrak{d}_1 < \cdots < \mathfrak{d}_{\ell_2}$.

Definition 2.2. If for every subset of variable nodes, $S \subseteq L$ whose cardinality is bounded above, that is $|S| \leq \gamma n$, the cardinality of set of all neighbors of S in R, $|N(S)|$ is bounded

below:

$$|N(S)| \geq \alpha \mathfrak{c}_1 |S|,$$

then the graph G is called a $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander graph.

Here, α is called the expansion factor of G. If the underlying bipartite graph in a Tanner code, $\mathcal{T}(G, \{\mathcal{C}_1, \ldots, \mathcal{C}_{\ell_2}\})$ is an expander graph, then the Tanner code is an expander code. We refer to these codes as $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander codes. If

$$\mathfrak{c}_1 = \cdots = \mathfrak{c}_{\ell_1} = \mathfrak{c}$$

and

$$\mathfrak{d}_1 = \cdots = \mathfrak{d}_{\ell_2} = \mathfrak{d},$$

then we get vertex expander codes as defined in literature. We refer to these codes as $(\mathfrak{c}, \mathfrak{d}, \gamma, \alpha)$ expander codes.

Example 2.3. While Figure 2.1 provides a small, toy example, expander graphs on more vertices are sparse and highly connected meaning that small subsets of L have unique neighbors. Consider the graph G as in Figure 2.1. Let $\mathcal{C}_j$ be the inner code associated with parity-check node $y_j \in R$ for all $j \in [6]$. The parity-check matrix for the associated Tanner code, $\mathcal{T}$ is:

$$H = \begin{bmatrix} H(\mathcal{C}_1) & H(\mathcal{C}_2) & 0 & 0 & 0 & 0 \\ H(\mathcal{C}_1) & 0 & H(\mathcal{C}_3) & 0 & 0 & 0 \\ H(\mathcal{C}_1) & 0 & 0 & H(\mathcal{C}_4) & H(\mathcal{C}_5) & 0 \\ 0 & H(\mathcal{C}_2) & H(\mathcal{C}_3) & 0 & H(\mathcal{C}_5) & 0 \\ 0 & H(\mathcal{C}_2) & H(\mathcal{C}_3) & 0 & 0 & H(\mathcal{C}_6) \end{bmatrix},$$

where $H(\mathcal{C}_j)$ is the parity-check matrix of the inner code $\mathcal{C}_j$.

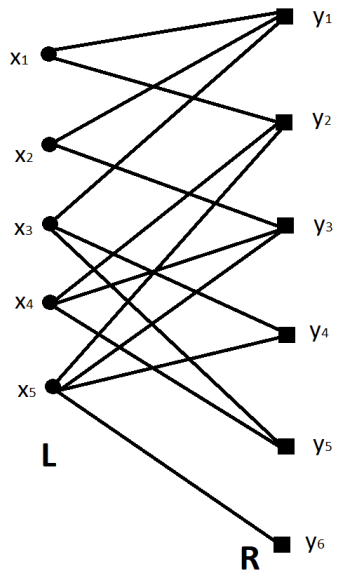

Figure 2.1: A $(\mathfrak{C} = \{2, 3, 4\}, \mathfrak{D} = \{1, 2, 3\}, \alpha = 1/2, \gamma = 3/5)$ expander graph G.

Expander codes were used to give an asymptotically good family of error-correcting codes [1]. Given a received word, these codes are known to have linear-time decoding algorithm that corrects a constant fraction of errors [2]. A linear-time decoding algorithm for $(\mathfrak{c}, \mathfrak{d}, \gamma, \alpha)$ expander codes is given, provided the expansion factor of G is greater than $\frac{3}{4}$ [1]. Several attempts have been made to find linear-time decoding algorithms for smaller values of α, that correct a constant fraction of errors, including that of Feldman, Malkin, Servedio, Stein, and Wainwright who obtained a polynomial-time algorithm decoding a constant factor of errors for codes based on expander graphs with expansion factor

$$\alpha > \frac{2}{3} + \frac{1}{3\mathfrak{c}},$$

where all the variable nodes of the underlying graph have degree $\mathfrak{c}$ [3]; Chilappagari, Nguyen, Vasic, and Marcellin's results giving a linear-time decoding algorithm for codes from graphs

with expansion factor

$$\alpha > \frac{\ell + 2}{2(\ell + 1)}$$

using as inner codes generalized parity-check codes with minimum distance at least $2\ell + 1$, $\ell > 1$ [4]; and Viderman's work [5], which yields a linear-time decoding algorithm for codes from expander graphs with

$$\alpha > \frac{2}{3} - \frac{1}{6\mathfrak{c}}.$$

In 2018, Dowling and Gao [6] presented a linear-time decoding algorithm for codes based on graphs with any expansion factor $\alpha > 0$ as long as for some positive integer t such that at most $t - 1$ errors are corrected and the minimum distance of the inner code is bounded below by

$$2t + \mathfrak{c}(t - 1)^2 - 1,$$

$t > 1/\alpha$. In each of these instances, the fraction of errors corrected is described in terms of γ, given a (c, d, α, γ) expander code.

We generalize the results of [6] to $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander codes which are not required to satisfy the regularity properties used above and instead allow for multiple left degrees and multiple right degrees. Given any expansion factor $\alpha > 0$, we obtain a linear-time decoding algorithm which corrects a constant fraction of errors. Here $\mathfrak{C}$ is the set of left degrees; taking $\mathfrak{D} = \{\mathfrak{d}\}$ and $\mathfrak{C} = \{\mathfrak{c}\}$ recovers the main result of [6]. Table 2.1 places this contribution in context of prior work.

This study is motivated by that of Richardson, Shokrollahi, and Urbanke [7] in which improved performance of codes designed from irregular bipartite graphs is demonstrated. The competing demands on the degrees of variable and check nodes in LDPC codes are noted in [8]. Loosely speaking, variable nodes with high degree receive more information from the check nodes whereas check nodes with low degree facilitate faster decoding. Irregular

	Expansion Requirement	Number of Errors Corrected	Requirements on $\mathcal{C}_{\mathfrak{d}}$	Expander code	Run Time
[1]	$\alpha > \frac{3}{4}$	$(2\alpha - 1)\gamma n$	parity-check code	$(\mathfrak{c}, \mathfrak{d})$ expander code	linear
[3]	$\alpha > \frac{2}{3} + \frac{1}{3\mathfrak{c}}$	$\frac{3\alpha-2}{2\alpha-1}\gamma n$	parity-check code	$(\mathfrak{c}, \mathfrak{d})$ expander code	poly
[4]	$\alpha > \frac{\ell+2}{2(\ell+1)}$	γn	minimum distance at least $2\ell - 1$	$(\mathfrak{c}, \mathfrak{d})$ expander code	linear
[5]	$\alpha > \frac{2}{3} - \frac{1}{6\mathfrak{c}}$	$\frac{3\alpha-2+\frac{1}{2\mathfrak{c}}}{2}\gamma n$	parity-check code	$(\mathfrak{c}, \varepsilon, \delta)$ expander code	linear
[6]	$\alpha > 0$	γn	minimum distance at least $2t + \mathfrak{c}(t-1)^2 - 1$	$(\mathfrak{c}, \mathfrak{d})$ expander code	linear
[9]	$\alpha > 0$	γn	minimum distance at least $2t + \mathfrak{c}_{\ell_1}(t-1)^2 - 1$	$(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander code	linear

Table 2.1: Summary of decoding algorithms for various expander codes, where $\ell > 1$, and $t > \frac{1}{\alpha}$.

graphs allow more flexibility to capitalize on these properties. To the best of our knowledge, this work is a first step towards writing a linear-time error correction algorithm correcting a constant fraction of errors in expander codes with arbitrary expansion factors subject to $\alpha > 0$. We introduce a bit of notation to describe our results.

Let $G = (L \dot{\cup} R, E)$ be a bipartite graph, $\mathfrak{C} := \{\mathfrak{c}_1, \ldots, \mathfrak{c}_{\ell_1}\}$, $|L| = n$, $\mathfrak{D} := \{\mathfrak{d}_1, \ldots, \mathfrak{d}_{\ell_2}\}$, $|R| = m$. Assume $\mathfrak{c}_1 < \cdots < \mathfrak{c}_{\ell_1}$ and $\mathfrak{d}_1 < \cdots < \mathfrak{d}_{\ell_2}$. Consider the $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander. Partition the vertices in L so that

$$L = L_1 \dot{\cup} L_2 \dot{\cup} \cdots \dot{\cup} L_{\ell_1}$$

where for each $v \in L_i$, $\deg(v) = \mathfrak{c}_i$, and set $n_i := |L_i|$. Let

$$R = R_1 \dot{\cup} R_2 \dot{\cup} \cdots \dot{\cup} R_{\ell_2}$$

where for each $u \in R_i$, $\deg(u) = \mathfrak{d}_i$, and $m_i := |R_i|$.

In this chapter, we present a linear-time decoding algorithm for $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander codes

where for $t > \frac{1}{\alpha}$ the minimum distance of the inner codes is bounded below by

$$2t + \mathfrak{c}_{\ell_1}(t-1)^2 - 1.$$

2.2 Preliminaries

In this section, we determine the parameters of $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander codes and provide counting arguements used in the proof of the main theorem. Consider a bipartite graph $G = (L \dot{\cup} R, E)$. Let G be a $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander graph. For every subset of variable nodes $S \subseteq L$, $S_i := S \cap L_i$ such that $|S_i| \leq \gamma n_i$. Since $\alpha \leq 1$, we have

$$\alpha \left(\sum_{i=1}^{\ell_1} \mathfrak{c}_i |S_i| \right) \leq |N(S)|.$$

For a subset $S \subseteq L$, its set of neighbors of degree k is

$$N_k(S) = \{v \, : \, |N(v) \cap S| = k\} \subseteq N(S)$$

for $k \in [\mathfrak{d}_{\ell_2}]$. Note that $N_k(S)$ represents the set of all neighbors of S which have exactly k neighbors in S. Then the set $N(S)$ can then be partitioned as follows

$$N(S) = N_1(S) \dot{\cup} N_2(S) \dot{\cup} \cdots \dot{\cup} N_{\mathfrak{d}_{\ell_2}}(S),$$

and $|N(S)| = \sum_{k=1}^{\mathfrak{d}_{\ell_2}} |N_k(S)|$.

Next, we provide lower bounds on the minimum distance and rate of a $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander code. They depend on the expansion factor of the graph as well as the minimum distances and rates of the inner codes.

Lemma 2.4. *Consider a* $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ *expander graph* $G = (L \dot{\cup} R, E)$. *Let* $|L| = n$.

(a) Assume $t > \frac{1}{\alpha}$. *Let* $S \subseteq L$ *such that* $|S| \leq \gamma n$,

$$(t\alpha - 1)\mathfrak{c}_1|S| \leq \sum_{k=1}^{\mathfrak{d}_{\ell_2}} (t-k)|N_k(S)|. \tag{2.1}$$

(b) Consider the inner code $\mathcal{C}_i \subseteq \mathbb{F}_q^{\mathfrak{d}_i}$, *which is a linear code whose minimum distance is bounded below* $\nu_i > \frac{1}{\alpha}\ \forall\ i \in [\ell_2]$. *Then the rate of Tanner code* $\mathcal{T}(G, \{\mathcal{C}_1, \ldots, \mathcal{C}_{\ell_2}\}) \subseteq \mathbb{F}_q^n$ *is bounded below by*

$$1 - \tfrac{\mathfrak{c}_{\ell_1}}{\mathfrak{d}_1}\omega_{max}$$

and minimum distance is bounded below by

$$\nu_{min}\alpha\lfloor\gamma n\rfloor\tfrac{\mathfrak{c}_1}{\mathfrak{c}_{\ell_1}},$$

where

$$\omega_i = \mathfrak{d}_i - \dim(\mathcal{C}_i)\,\forall\, i \in [\ell_2],$$

$$\omega_{max} = \max\{\omega_1, \omega_2, \ldots, \omega_{\ell_2}\}$$

and

$$\nu_{min} = \min\{\nu_1, \nu_2, \ldots, \nu_{\ell_2}\}.$$

Proof. (a) Note that

$$\alpha\mathfrak{c}_1|S| \leq \alpha\left(\sum_{i=1}^{\ell_1}\mathfrak{c}_i|S_i|\right) \leq |N(S)|.$$

Consider the number of edges incident with vertices in S. When counted from the left, number of edges incident with vertices in S is $\sum_{i=1}^{\ell_1}\mathfrak{c}_i|S_i|$ whereas number of edges

incident with vertices in S is $\sum_{k=1}^{\mathfrak{d}_{\ell_2}} k|N_k(S)|$ when counted from the right. Thus,

$$\sum_{i=1}^{\ell_1} \mathfrak{c}_i|S_i| = \sum_{k=1}^{\mathfrak{d}_{\ell_2}} k|N_k(S)|.$$

It follows that

$$\begin{aligned}(t\alpha-1)\mathfrak{c}_1|S| &\leq (t\alpha-1)\left(\sum_{i=1}^{\ell_1}\mathfrak{c}_i|S_i|\right)\\ &\leq t|N(S)| - \sum_{i=1}^{\ell_1}\mathfrak{c}_i|S_i|\\ &= t\sum_{k=1}^{\mathfrak{d}_{\ell_2}}|N_k(S)| - \sum_{k=1}^{\mathfrak{d}_{\ell_2}} k|N_k(S)|\\ &= \sum_{k=1}^{\mathfrak{d}_{\ell_2}}(t-k)|N_k(S)|.\end{aligned}$$

(b) For each $i \in [\ell_2]$, the codewords of $\mathcal{C}_i$ are determined by ω_i equations over $\mathbb{F}_q$ $\forall\ i \in [\ell_2]$. Therefore $\mathcal{T}(G, \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{\ell_2}\})$ can be defined using at most $\omega_{max}|R|$ equations over $\mathbb{F}_q$ and

$$\dim(\mathcal{T}(G, \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{\ell_2}\}) \geq n - \omega_{max}|R|.$$

Note that

$$\mathfrak{d}_1 m \leq \sum_{i=1}^{\ell_2}\mathfrak{d}_i m_i = \sum_{i=1}^{\ell_1}\mathfrak{c}_i n_i \leq \mathfrak{c}_{\ell_1} n.$$

Therefore,

$$\frac{m}{n} \leq \frac{\mathfrak{c}_{\ell_1}}{\mathfrak{d}_1}.$$

The lower bound on the rate of $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander code is as follows.

$$\begin{aligned}\text{rate}(\mathcal{T}(G, \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{\ell_2}\})) &\geq \frac{n - \omega_{max}|R|}{n} \\ &= 1 - \frac{|R|}{|L|}\omega_{max} \\ &\geq 1 - \frac{\mathfrak{c}_{\ell_1}}{\mathfrak{d}_1}\omega_{max}.\end{aligned}$$

Let $\mathbf{c} = (c_i)_{i \in L}$ be a non-zero codeword of $\mathcal{T}(G, \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{\ell_2}\})$ and

$$S = \text{supp}(\mathbf{c}) = \{i \in L : c_i \neq 0\}.$$

Given $\mathcal{C}_j$ has minimum distance at least $\nu_j \ \forall \ j \in [\ell_2]$, thus $N_k(S) = 0$ for $1 \leq k \leq \nu_{min} - 1$. Then

$$\begin{aligned}\mathfrak{c}_{\ell_1}|S| \geq \sum_{i=1}^{\ell_1} \mathfrak{c}_i|S_i| &= \sum_{k=1}^{\mathfrak{d}_{\ell_2}} k|N_k(S)| \\ &= \sum_{k=\nu_{min}}^{\mathfrak{d}_{\ell_2}} k|N_k(S)| \\ &\geq \nu_{min} \sum_{k=\nu_{min}}^{\mathfrak{d}_{\ell_2}} |N_k(S)| \\ &= \nu_{min} \sum_{k=1}^{\mathfrak{d}_{\ell_2}} |N_k(S)| \\ &= \nu_{min}|N(S)|.\end{aligned}$$

If $|S| \leq \gamma n$, then we have

$$|N(S)| \geq \alpha \left(\sum_{i=1}^{\ell_1} \mathfrak{c}_i|S_i| \right) \geq \alpha \mathfrak{c}_1 |S|$$

and

$$\sum_{i=1}^{\ell_1} \mathfrak{c}_i |S_i| \geq \nu_{min} |N(S)| \geq \nu_{min}\alpha \left(\sum_{i=1}^{\ell_1} \mathfrak{c}_i |S_i| \right);$$

that is, $1 \geq \nu_{min}\alpha$ which is a contradiction, $|S| > \gamma n$. Let $S_0 \subseteq S$ such that $|S_0| = \lfloor \gamma n \rfloor$. Note that

$$|N(S)| \geq |N(S_0)| \geq \alpha \mathfrak{c}_1 |S_0| = \alpha \mathfrak{c}_1 \lfloor \gamma n \rfloor$$

and

$$\mathfrak{c}_{\ell_1} |S| \geq \nu_{min} |N(S)| \geq \nu_{min} \alpha \mathfrak{c}_1 \lfloor \gamma n \rfloor.$$

This implies that

$$|S| \geq \nu_{min} \alpha \lfloor \gamma n \rfloor \tfrac{\mathfrak{c}_1}{\mathfrak{c}_{\ell_1}}.$$

Since S is the support of an arbitrary nonzero codeword of $\mathcal{T}(G, \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{\ell_2}\})$, the code has minimum distance at least

$$\nu_{min} \alpha \lfloor \gamma n \rfloor \tfrac{\mathfrak{c}_1}{\mathfrak{c}_{\ell_1}}.$$

□

Better estimates may be used in the proof, but (as we will see) these calculations are sufficient to prove that the decoding algorithm presented is linear time. For the special case of

$$\mathfrak{c}_1 = \ldots = \mathfrak{c}_{\ell_1} = \mathfrak{c}$$

and

$$\mathfrak{d}_1 = \ldots = \mathfrak{d}_{\ell_2} = \mathfrak{d},$$

we get the result by Dowling and Gao as a corollary [6, Lemma 1].

2.3 Algorithm and analysis

In this section, we build on [6] to give a decoding algorithm for $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander codes and prove that it corrects a constant fraction of errors in linear time.

Input:

- $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander graph $G = (L \dot{\cup} R)$ such that $|L| = n$ and $|\mathfrak{C}| = \ell_1$.
- linear codes $\mathcal{C}_j \subseteq \mathbb{F}_q^{\mathfrak{d}_j}$ whose minimum distances are bounded below by $2t + \mathfrak{c}_{\ell_1}(t-1)^2 - 1$ $\forall j \in [\ell_2]$.
- received word $\mathbf{w} = (w_i)_{i \in L} \in \mathbb{F}_q^n$.
- constants τ, τ'.

Initialize: Set $\mathbf{z} = \mathbf{w}$.

Loop: Repeat the following two steps $log_\tau(\tau' n)$ times.

- **local decoding**: If for every parity-check node $j \in R$, there exists an associated codeword $\mathbf{c}^{(j)} \in \mathcal{C}_j$ such that $d\left(\mathbf{z}|_{N(j)}, \mathbf{c}^{(j)}\right) \leq t - 1$, then send values of $\mathbf{c}^{(j)}$ to nodes in $N(j)$.
- **updating**: Set $\mathbf{z}_i = \mathbf{c}^{(j)}_{\eta(i,j)}$ for every variable node $i \in L$, if i receives some value from its neighbor $j \in N(i)$. Randomly choose j if more than one exists. If z is unchanged, exit **Loop** and go to **Return**.

Return: If for some $j \in R$ there exists some $\mathbf{z}|_{N(j)} \notin \mathcal{C}_j$, then output "failure" message. Else, output return $\mathbf{z}$.

Output: Either a codeword or "failure".

Lemma 2.5. *Consider a subset of the variable nodes, $\mathcal{E} \subseteq L$ such that $|\mathcal{E}| \leq \gamma n$. Let $\mathcal{E}$ represent the number of errors in the received word $\boldsymbol{z}$ just before any decoding round. Consider a subset of the variable nodes, $\mathcal{E}' \subseteq L$. Let $\mathcal{E}'$ represent the number of errors in the received word $\boldsymbol{z}$ just after the decoding round. Then*

$$\frac{|\mathcal{E}'|}{|\mathcal{E}|} \leq \left(1 - \frac{t\alpha - 1}{t-1}\frac{\mathfrak{c}_1}{\mathfrak{c}_{\ell_1}}\right). \tag{2.2}$$

Proof. Consider the following partition of $N(\mathcal{E})$:

- $T_1 = \cup_{k=1}^{t-1} N_k(\mathcal{E})$,
- $T_2 = \cup_{k=t}^{t+\mathfrak{c}_{\ell_1}(t-1)^2-1} N_k(\mathcal{E})$,
- $T_3 = \cup_{k=t+\mathfrak{c}_{\ell_1}(t-1)^2}^{\mathfrak{d}_{\ell_2}} N_k(\mathcal{E})$.

Note that each node in T_1 sends only correct values from $\mathbf{z}$, each node in T_2 sends no value from $\mathbf{z}$ and each node in T_3 may or may not send values from $\mathbf{z}$. If a node in $N(\mathcal{E})$ sends a value, then it either sends a correct value or an incorrect value from $\mathbf{z}$. We also partition $\mathcal{E}$ into 3 subsets:

- $\mathcal{E}_0$, the set of nodes that receives no value from T_3 and at least one correct value from T_1,
- $\mathcal{E}_1$, the set of nodes that receives at most one value from T_3 and at least one correct value from T_1,
- $\mathcal{E}_2 = \mathcal{E}\backslash(\mathcal{E}_0 \dot{\cup} \mathcal{E}_1)$, the set of nodes that received no value from $N(\mathcal{E})$.

Define $\mathcal{E}_3 := \{i \in L\backslash\mathcal{E} \ : \ i \text{ receives a value from } j \in T_3 \text{ and } N(i) \cap L \neq \phi\}$. Note that $\mathcal{E}_3$ represents the set of errors in $\mathbf{z}$ after the decoding round; $\mathcal{E}_0, \mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ are pairwise disjoint

and

$$\mathcal{E} = \mathcal{E}_0 \dot{\cup} \mathcal{E}_1 \dot{\cup} \mathcal{E}_2;$$

$$\mathcal{E}_2 \dot{\cup} \mathcal{E}_3 \subseteq \mathcal{E}' \subseteq \mathcal{E}_1 \dot{\cup} \mathcal{E}_2 \dot{\cup} \mathcal{E}_3.$$

Hence,

$$|\mathcal{E}_0 \dot{\cup} \mathcal{E}_1| - |\mathcal{E}_1 \dot{\cup} \mathcal{E}_3| \leq |\mathcal{E}| - |\mathcal{E}'|. \tag{2.3}$$

The set T_1 sends values to $\mathcal{E}_0$ or $\mathcal{E}_1$. The number of values sent is at most equal to the number of edges which is equal to $\sum_{k=1}^{t-1} k|N_k(\mathcal{E})|$. Write

$$\mathcal{E}_0 = \mathcal{E}_{00} \dot{\cup} \cdots \dot{\cup} \mathcal{E}_{0\ell_1}$$

where $\forall v_i \in \mathcal{E}_{0i}, \deg(v_i) = \mathfrak{c}_i$, $1 \leq i \leq \ell_1$ and

$$\mathcal{E}_1 = \mathcal{E}_{10} \dot{\cup} \cdots \dot{\cup} \mathcal{E}_{1\ell_1}$$

where $\forall v_i \in \mathcal{E}_{1i}, \deg(v_i) = \mathfrak{c}_i$, $1 \leq i \leq \ell_1$. Then

$$\mathfrak{c}_{\ell_1} |\mathcal{E}_0 \dot{\cup} \mathcal{E}_1| \geq \sum_{i=1}^{\ell_1} \mathfrak{c}_i |\mathcal{E}_{0i} \dot{\cup} \mathcal{E}_{1i}| \geq \sum_{k=1}^{t-1} k|N_k(\mathcal{E})|. \tag{2.4}$$

The set T_3 sends at least one incorrect value to $\mathcal{E}_1 \dot{\cup} \mathcal{E}_3$. Each $j \in T_3$ sends at most $t-1$ values to $\mathcal{E}_1 \dot{\cup} \mathcal{E}_3$. Thus,

$$|\mathcal{E}_1 \dot{\cup} \mathcal{E}_3| \leq (t-1) \sum_{k=t+\mathfrak{c}_{\ell_1}(t-1)^2}^{\mathfrak{d}_{\ell_2}} |N_k(\mathcal{E})|. \tag{2.5}$$

Combining equations (2.3), (2.4) and (2.5) yields

$$|\mathcal{E}| - |\mathcal{E}'| \geq \frac{\sum_{k=1}^{t-1} k|N_k(\mathcal{E})|}{\mathfrak{c}_{\ell_1}} - (t-1) \sum_{k=t+\mathfrak{c}_{\ell_1}(t-1)^2}^{\mathfrak{d}_{\ell_2}} |N_k(\mathcal{E})|.$$

Since $\mathcal{E} \subseteq L$ such that $|\mathcal{E}| \leq \gamma n$, by Lemma 2.4,

$$\begin{aligned}
(t\alpha - 1)\mathfrak{c}_1|\mathcal{E}| &\leq \sum_{k=1}^{t-1}(t-k)|N_k(\mathcal{E})| \\
&= \sum_{k=1}^{t-1}(t-k)|N_k(\mathcal{E})| \\
&\quad - \sum_{k=t}^{t+\mathfrak{c}_{\ell_1}(t-1)^2-1} (k-t)|N_k(\mathcal{E})| \\
&\quad - \sum_{k=t+\mathfrak{c}_{\ell_1}(t-1)^2}^{\mathfrak{d}_{\ell_2}} (k-t)|N_k(\mathcal{E})| \\
&= \sum_{k=1}^{t-1}(t-k)|N_k(\mathcal{E})| \\
&\quad - \sum_{k=t+\mathfrak{c}_{\ell_1}(t-1)^2}^{\mathfrak{d}_{\ell_2}} (k-t)|N_k(\mathcal{E})|.
\end{aligned}$$

Note that T_2 receives no value from $\mathbf{z}$. Also note that when $1 \leq k \leq t-1$,

$$k \geq \frac{t-k}{t-1}$$

and when $k \geq t + \mathfrak{c}_{\ell_1}(t-1)^2$,

$$t - 1 \leq \frac{t-k}{\mathfrak{c}_{\ell_1}(t-1)}.$$

Therefore,

$$\begin{aligned}|\mathcal{E}| - |\mathcal{E}'| &\geq \frac{\sum_{k=1}^{t-1} k|N_k(\mathcal{E})|}{\mathfrak{c}_{\ell_1}} \\ &\quad - (t-1) \sum_{k=t+\mathfrak{c}_{\ell_1}(t-1)^2}^{\mathfrak{d}_{\ell_2}} |N_k(\mathcal{E})| \\ &\geq \frac{\sum_{k=1}^{t-1}(t-k)|N_k(\mathcal{E})|}{\mathfrak{c}_{\ell_1}(t-1)} \\ &\quad - \frac{\sum_{k=t+\mathfrak{c}_{\ell_1}(t-1)^2}^{\mathfrak{d}_{\ell_2}}(k-t)|N_k(\mathcal{E})|}{\mathfrak{c}_{\ell_1}(t-1)} \\ &\geq \frac{(t\alpha-1)\mathfrak{c}_1}{(t-1)\mathfrak{c}_{\ell_1}}|\mathcal{E}|.\end{aligned}$$

Thus, $\dfrac{|\mathcal{E}'|}{|\mathcal{E}|} \leq \left(1 - \dfrac{t\alpha-1}{t-1}\dfrac{\mathfrak{c}_1}{\mathfrak{c}_{\ell_1}}\right)$. □

For the special case of

$$\mathfrak{c}_1 = \cdots = \mathfrak{c}_{\ell_1} = \mathfrak{c}$$

and

$$\mathfrak{d}_1 = \cdots = \mathfrak{d}_{\ell_2} = \mathfrak{d},$$

we get the result by Dowling and Gao as a corollary [6, Lemma 2].

Let $\mathcal{C}_i \subseteq \mathcal{F}_q^{\mathfrak{d}_i}$ be a linear code with minimum distance

$$2t + \mathfrak{c}_{\ell_1}(t-1)^2 + 1$$

for all $i \in [\ell_2]$; let $\alpha > 0$ and t be an integer such that $t > \frac{1}{\alpha}$. We assume that in a round at most $t-1$ errors can be detected. Let

$$\tau = \left(1 - \frac{t\alpha-1}{t-1}\frac{\mathfrak{c}_1}{\mathfrak{c}_{\ell_1}}\right)$$

and $\tau' = \gamma$ as suggested by the proof of Lemma 2.5. We will now prove the main theorem.

Theorem 2.6. *Consider a* $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ *expander graph* $G = (L \dot{\cup} R, E)$. *Let*

$$\mathfrak{C} = \{\mathfrak{c}_1, \dots \mathfrak{c}_{\ell_1}\},$$

$$\mathfrak{D} = \{\mathfrak{d}_1, \dots, \mathfrak{d}_{\ell_2}\},$$

$\alpha > 0$ *and* $|L| = n$. *Let* $\mathcal{C}_j \subseteq \mathbb{F}_q^{\mathfrak{d}_j}$ *be an inner code whose minimum distance is bounded below by*

$$2t + \mathfrak{c}_{\ell_1}(t-1)^2 - 1$$

for all $j \in [\ell_2]$, *where* $t > \frac{1}{\alpha}$. *Then there exists a linear-time decoding algorithm which corrects all error patterns whose size is bounded above by* γn *for the Tanner code* $\mathcal{T}(G, \{\mathcal{C}_1, \dots, \mathcal{C}_{\ell_2}\}) \subseteq \mathbb{F}_q^n$.

Proof. Note that the algorithm corrects a (positive) constant fraction of errors after every decoding round, by Lemma 2.5. We consider the set of errors before round $k+1$ of decoding, $\mathcal{E}_k$. Each decoding operation takes t_1 amount of time. After the first step, the decoder checks the neighboring constraints of adjusted variable nodes. After every iteration of the algorithm the number of errors is reduced by a constant factor, so

$$|\mathcal{E}_k| + |\mathcal{E}_{k-1}| \leq 2|\mathcal{E}_{k-1}|.$$

Note that $\{|\mathcal{E}_{k-1}|\}_{k=1}^{\infty}$ represents a geometric sequence. Therefore, the number of decoding

operations is bounded above by:

$$\begin{aligned} & t_1|R| + 2\mathfrak{c}_{\ell_1} t_1 \sum_{k=0}^{log_\tau(\tau' n)} |\mathcal{E}_k| \\ & \leq t_1 \frac{\mathfrak{c}_{\ell_1} n}{\mathfrak{d}_1} + 2\mathfrak{c}_{\ell_1} t_1 \sum_{k=0}^{log_\tau(\tau' n)} \left(1 - \frac{t\alpha - 1}{t-1} \frac{\mathfrak{c}_1}{\mathfrak{c}_{\ell_1}}\right)^k |\mathcal{E}_0| \\ & \leq \frac{\mathfrak{c}_{\ell_1} t_1}{\mathfrak{d}_1} n + 2\left(\frac{t-1}{t\alpha - 1} \frac{\mathfrak{c}_{\ell_1}}{\mathfrak{c}_1}\right) \gamma n. \end{aligned}$$

Therefore the number of decoding operations is linear in n. □

Vertex in R	Neighbors in L
A	1,3,4,5,7,8,9,11,12,13,15,16,17,19,20,21,23,24,25,27,29,31,33,35,37,39,41,43,45,47,49,51,53,55,57,59
B	1,2,4,5,6,8,9,10,12,13,14,16,17,18,20,21,22,24,25,27,29,31,33,35,37,39,41,43,45,47,49,51,53,55,57,59
C	1,2,3,5,6,7,9,10,11,13,14,15,17,18,19,21,22,23,26,28,30,32,34,36,38,40,42,44,46,48,50,52,54,56,58
D	2,3,4,6,7,8,10,11,12,14,15,16,18,19,20,22,23,24,26,28,30,32,34,36,38,40,42,44,46,48,50,52,54,56,58

Table 2.2: A $(\{2,3\},\{35,36\},1/2,1/59)$ expander graph $G = (L \dot{\cup} R, E)$ described in terms of neighborhoods of vertices of $R = \{A, B, C, D\}$

Example 2.7. Let $\mathfrak{C} = \{2,3\}$, $\mathfrak{D} = \{35,36\}$, $\alpha = 1/2$, $\gamma = 1/59$, $n = 59$, $m = 4$, and $G = (L \dot{\cup} R, E)$ be the $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander graph which neighborhoods of vertices in $R := \{A, B, C, D\}$ as given in Table 2.2, where $L = \{1, \ldots, 59\}$. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be codes of lengths 36 and 35 respectively so that each has minimum distance at least 17, and consider the resulting expander code $\mathcal{T}(G, \{\mathcal{C}_1, \mathcal{C}_2\})$.

Suppose $\mathbf{z} = (z_1, \ldots, z_{59})$ is a received word with errors in positions z_{21} and z_{52}. Assume that A and B correspond to $\mathcal{C}_1$ and that C and D correspond to $\mathcal{C}_2$. Then A and B send the same value σ_1 associated with z_{21}. We assume that decoding in this round at A and B happens in such a way that only the coordinate at z_{21} is modified. This means that all other neighbors of A and B receive same value as before from A and B. Assume decoding at C and D happens such that node 21 receives σ_2 and node 52 receives σ_3 from C as well as σ_4 from D. Let this decoding be such that $\sigma_1 = \sigma_2$ and $\sigma_3 = \sigma_4$. Moreover, all coordinates of

$\mathbf{z}$ other than z_{21} and z_{52} take the same values before decoding (as a random choice from all received values). Thus, the new $\mathbf{z}$ is a codeword of the $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander code.

For the special case of

$$\mathfrak{c}_1 = \ldots = \mathfrak{c}_{\ell_1} = \mathfrak{c}$$

and

$$\mathfrak{d}_1 = \ldots = \mathfrak{d}_{\ell_2} = \mathfrak{d},$$

we get the result by Dowling and Gao as a corollary of Theorem 2.6 [6, Theorem 1].

2.4 Conclusion

We provide a linear-time decoding algorithm which corrects a constant factor of errors for $(\mathfrak{C}, \mathfrak{D}, \alpha, \gamma)$ expander codes of any positive expansion factor provided the minimum distance of inner codes satistfy $d \geq 2t + \mathfrak{c}_{\ell_1}(t-1)^2 - 1$. To our knowledge, this is the first such decoding algorithm for codes based on graphs with multiple left or multiple right degrees. It remains a challenge to obtain explicit construction of the underlying expander graphs.

Chapter 3

Graph-based codes for hierarchical recovery

Hierarchical locally recoverable codes (HLRCs) are linear codes which provide a multi-tier erasure recover. The hierarchical structure allows for an efficient recovery of small number of erasures by accessing a small subset of symbols and recover a large number of erasures by accessing bigger recovery sets. In this chapter, we harness graphical properties and inner codes of Tanner codes to give rise to hierarchical LRCs. Clearly, any LRC can be expressed as a graph-based code; in contrast, here we begin with a graph to construct an (H)LRC. Some of this work was done in collaboration with Allison Beemer [63]. In graph-based message-passing decoding, stopping sets characterize decoder failure over erasure channels [57]. As LRCs are designed for the erasure setting, we can express message-passing decoder failure for HLRCs in each level of the hierarchy as specialized stopping sets within that level. We show that the minimum size of a stopping set increases with the level of hierarchical repair. We consider the following definition of Tanner codes throughout this chapter.

Definition 3.1 (Tanner Codes)**.** Let $G = (L \dot{\cup} R, E)$ be a bipartite graph where the nodes

in L have degrees

$$\mathfrak{C} := \{\mathfrak{c}_1, \ldots, \mathfrak{c}_n\}$$

such that $|L| = n$ and nodes in R have degrees

$$\mathfrak{D} := \{\mathfrak{d}_1, \ldots, \mathfrak{d}_m\}$$

such that $|R| = m$. The Tanner code

$$\mathcal{T}(G, \{\mathcal{C}_1, \ldots, \mathcal{C}_m\})$$

over $\mathbb{F}_q$ is defined as follows:

$$\mathcal{T}(G, \{\mathcal{C}_1, \ldots, \mathcal{C}_m\}) = \{\mathbf{c} : \mathbf{c}|_{N(j)} \in \mathcal{C}_j \ \forall j \in [m]\} \subseteq \mathbb{F}_q^n,$$

where the *neighborhood* $N(j)$ is the set of nodes adjacent to the jth node in R.

Assume that

$$\mathfrak{c}_1 \leq \mathfrak{c}_2 \leq \ldots \leq \mathfrak{c}_n$$

and

$$\mathfrak{d}_1 \leq \mathfrak{d}_2 \leq \ldots \leq \mathfrak{d}_m.$$

Moreover,

$$\mathcal{C}_j \subseteq \mathbb{F}_q^{\mathfrak{d}_j}$$

for all $j \in [m]$. It is possible that for some $j, k \in [m]$, $j \neq k$, $\mathfrak{d}_j = \mathfrak{d}_k$ but $\mathcal{C}_j \neq \mathcal{C}_k$.

Recall that the *girth* of a graph G, denoted $g(G)$, is the minimum length of a cycle contained within the graph. Because a Tanner code is derived from a bipartite graph, its girth must be

even. Hierarchical locally recoverable codes (HLRCs) [12, 53] are linear codes that provide a method of multi-tier erasure recovery; they are defined as follows.

Definition 3.2 (HLRCs, [12])**.** An $[n, k, d]$ code $\mathcal{C}$ is a code with *h-level hierarchical locality with local parameters*

$$[(t_1, \rho_1), \ldots, (t_h, \rho_h)]$$

if

$$\rho_1 \geq \cdots \geq \rho_h,$$

and for every $i \in [n]$, there exists a punctured code $\mathcal{C}_i$ such that

$$i \in \text{supp}(\mathcal{C}_i)$$

and the following conditions hold:

- $\dim(\mathcal{C}_i) \leq t_1$,
- $d_{\min}(\mathcal{C}_i) \geq \rho_1$,
- $\mathcal{C}_i$ is a code with $(h-1)$-level hierarchical locality with local parameters

$$[(t_2, \rho_2), \ldots, (t_h, \rho_h)].$$

For an HLRC as in Definition 3.2, we refer to the punctured codes $\mathcal{C}_j$ with parameters

$$(t_j, \rho_j)$$

as belonging to the j^{th} *level* of hierarchy. Up to $\rho_j - 1$ erasures can be corrected using the j^{th} level of hierarchy based on the minimum distance. Notice that to fully exploit the

hierarchical structure, we should choose the highest index of a level such that correction is possible with a code in that level (thus minimizing the dimension of the code $\mathcal{C}_j$); as a result, level j may be used to correct between ρ_{j+1} and $\rho_j - 1$ erasures. The notion of availability can be extended to HLRCs as follows.

Definition 3.3 (HLRCs with availability)**.** An $[n, k, d]$ code $\mathcal{C}$ is code with a h-level hierarchical locality with local parameters

$$[(t_1, \rho_1), \ldots, (t_h, \rho_h)]$$

and availability

$$\tau_1, \ldots, \tau_h$$

if the following conditions hold.

- $\mathcal{C}$ is an

  $$(t_1, \rho_1)$$

  LRC with availability τ_1.

- Each of the punctured codes

  $$\mathcal{C}|_{I_{j_1,i} \cup \{i\}} \ \forall j_1 \in [\tau_1], i \in [n]$$

  is a $(h-1)$-level HLRC with local parameters

  $$[(t_2, \rho_2), \ldots, (t_h, \rho_h)]$$

  and availability

  $$\tau_2, \ldots, \tau_h.$$

3.1 Tanner codes for (hierarchical) recovery

In this section, we show how Tanner codes can be considered as (H)LRCs when the inner codes are chosen to be locally recoverable codes. Let $\mathcal{T} := \mathcal{T}(G = (L \dot{\cup} R, E), \{\mathcal{C}_1, \ldots, \mathcal{C}_m\}) \subseteq \mathbb{F}_q^n$. Let $|L| = n$, $\mathfrak{C} := \{\mathfrak{c}_1, \ldots, \mathfrak{c}_n\}$ be set of all degrees of nodes in L such that $\ell_1 \leq n$ are distinct. Assume n_i variable nodes have degree $\mathfrak{c}_i$ $\forall i \in [\ell_1]$. For all $j \in [n_i]$ given $x_{ij} \in L$ of degree $\mathfrak{c}_i$, neighborhood of x_{ij} is

$$N(x_{ij}) = \{y_{ij1}, \ldots, y_{ij\mathfrak{c}_i}\}.$$

Let the code associated with $y_{ij\ell \in N(x_{ij})}$: $\mathcal{C}_{ij\ell}$ for all $1 \leq \ell \leq \mathfrak{c}_i$. If $y_{ij\ell} = y_{i'j'\ell'}$ for some $(i, j, \ell) \neq (i', j', \ell')$; then $\mathcal{C}_{ij\ell} = \mathcal{C}_{i'j'\ell'}$.

3.1.1 Tanner codes as LRCs

We begin the study of Tanner codes as LRCs with repair sets by considering locality properties to recover a single erasure.

Theorem 3.4. *For each $x_{ij} \in L$, let $\mathcal{C}_{ij\ell}$ be an*

$$(d_{ij\ell}, k_{ij\ell}, r_{ij\ell})$$

LRC with availability

$$a_{ij\ell}$$

for all $1 \leq \ell \leq \mathfrak{c}_i$.

1. *If $g(G) = 4$, $\mathcal{T}$ has locality r and availability a given by*

$$r = \max_{(i,j)} \min_{\substack{\ell \ s.t. \\ y_{ij\ell} \in N(x_{ij})}} \{r_{ij\ell}\}$$

and

$$a = \min_{(i,j)} \max_{\substack{\ell \ s.t. \\ y_{ij\ell} \in N(x_{ij}),\ r_{ij\ell} \leq r}} \{a_{ij\ell}\}.$$

2. *If $g(G) \geq 6$, $\mathcal{T}$ has locality r and availability a given by*

$$r = \max_{(i,j,\ell)} \{r_{ij\ell}\}$$

and

$$a = \min_{(i,j)} \sum_{\ell=1}^{\mathfrak{c}_i} a_{ij\ell}.$$

Proof. 1. Let $g(G) = 4$ and consider an erased node x_{ij} for some $i \in [\ell_1]$ and $j \in [n_i]$. The most efficient way to recover x_{ij} is to access the neighbor $y_{ij\ell}$ such that the associated inner code $\mathcal{C}_{ij\ell}$ has minimum locality:

$$\min_{\ell \ s.t. \ y_{ij\ell} \in N(x_{ij})} \{r_{ij\ell}\}.$$

To ensure that any choice of erased node can be recovered, we maximize over all possible i, j pairs, yielding the result.

The number of disjoint sets of size at most r that can then recover the erased node x_{ij} is

$$\max_{\ell \ s.t. \ y_{ij\ell} \in N(x_{ij}),\ r_{ij\ell} \leq r} \{a_{ij\ell}\}.$$

The availability must apply to the recovery of any erasure, so we minimize over all

possible i, j pairs, yielding the result.

2. Now, let $g(G) \geq 6$. Since there are no 4-cycles in G, none of the repair groups of x_{ij} associated with different $y_{ij\ell}$'s intersect. Thus, we may increase availability significantly by taking the locality r to be a maximum over the neighboring $r_{ij\ell}$'s. Consider the erased node x_{ij} and its neighboring set

$$N(S) = \{y_{ij1}, \ldots, y_{ij\mathfrak{c}_i}\}.$$

Again due to the lack of 4-cycles, x_{ij} can now be repaired using

$$\sum_{\ell=1}^{\mathfrak{c}_i} a_{ij\ell}$$

disjoint repair groups of size at most r. We again minimize over all i, j pairs, yielding the result.

□

We now extend the above results to the case of multiple erasures, so that the set of erased nodes is given by

$$S = \{x_{i_1 j_1}, \ldots, x_{i_s j_s}\},$$

where

$$|S| = s \leq \mathfrak{c}_1$$

and any pair of erased nodes shares at most one common neighbor in R. If the girth of $\mathcal{T}$ is at least 6, then this last condition is guaranteed; in graphs of girth 4 it remains possible to have such a set S, though not every erasure set of size $s \geq 2$ will have this property. The

neighborhood of S is equal to

$$N(S) = \bigcup_{\ell=1}^{s} N(x_{i_\ell j_\ell}),$$

a union that is not necessarily disjoint.

Theorem 3.5. *For each $x_{ij} \in L$, let $\mathcal{C}_{ij\ell}$ be an*

$$(d_{ij\ell}, k_{ij\ell}, r_{ij\ell})$$

LRC with availability

$$a_{ij\ell}$$

for all $1 \leq \ell \leq \mathfrak{c}_i$. Then $\mathcal{T}$ has locality equal to

$$r = s \max_{(i,j,\ell)} \{r_{ij\ell}\}.$$

Furthermore,

1. *If $g(G) = 4$, $\mathcal{T}$ has availability given by*

$$a = \min_{(i,j,\ell)} \{a_{ij\ell}\}.$$

2. *If $g(G) \geq 6$, $\mathcal{T}$ has availability given by*

$$a = \min_{(i,j,\ell)} \left\{(\mathfrak{c}_i - s + 1)a_{ij\ell}\right\}.$$

Proof. Consider the set of erased nodes S such that

$$|S| = s \leq \mathfrak{c}_1$$

and the intersection of the neighborhoods of any two elements in S has size at most one. The most efficient way to recover x_{ij} would be to access its neighbor $y_{ij\ell}$ such that the associated inner code $\mathcal{C}_{ij\ell}$ has minimum locality. Unfortunately, there is no guarantee that another node in this repair group does not also belong to S. However, there are at least

$$\mathfrak{c}_i - (s-1) \geq 1$$

neighbors of x_{ij} that have no other elements of S in its neighborhood. Thus, at most

$$\max_{\ell \ s.t. \ y_{ij\ell} \in N(x_{ij})} \{r_{ij\ell}\}$$

other nodes need to be contacted to repair x_{ij}. To ensure that every erased node can be recovered, we maximize this over all $i \in [\ell_1]$ and $j \in [n_i]$.

1. Let $g(G) = 4$. The number of disjoint sets that can recover a single erased node x_{ij} for some $i \in [\ell_1]$ and $j \in [n_i]$ is at least

$$\min_{\ell} \{a_{ij\ell}\}.$$

   The collection of s erasures is then recovered using s (not necessarily disjoint) recovery sets, each of size at most

$$\max_{(i,j)} \ \max_{\ell \ s.t. \ y_{ij\ell} \in N(x_{ij})} \{r_{ij\ell}\}.$$

   By taking unions comprised of one repair group per bit, we will have at least

$$a = \min_{(i,j,\ell)} \{a_{ij\ell}\}$$

repair groups of size at most

$$r = s \max_{(i,j,\ell)} \{r_{ij\ell}\}$$

for the set S.

2. Now, let $g(G) \geq 6$, and consider the erased node x_{ij} for some $i \in [\ell_1]$ and $j \in [n_i]$ and its neighboring set

$$N(x_{ij}) = \{y_{ij1}, \ldots, y_{ij\mathfrak{c}_i}\}.$$

Since G has no 4-cycles, none of the repair groups of x_{ij} associated with $y_{ij\ell}$ intersect with the repair groups of $y_{ij\ell'}$, for all $\ell \neq \ell' \in [\mathfrak{c}_i]$. Recall that at least

$$\mathfrak{c}_i - s + 1$$

of x_{ij}'s neighbors are not adjacent to any other element of S. This means that x_{ij} can be repaired using at least

$$(\mathfrak{c}_i - s + 1) \min_{\ell} \{a_{ij\ell}\}$$

different repair groups of size at most

$$\max_{(i,j,\ell)} \{r_{ij\ell}\}.$$

As before, by taking unions comprised of one repair group per bit, we will have at least

$$a = \min_{(i,j,\ell)} (\mathfrak{c}_i - s + 1)\{a_{ij\ell}\}$$

repair groups of size at most

$$s \max_{(i,j,\ell)} \{r_{ij\ell}\}$$

for the set S.

□

From the previous two results, we can see that in the case of s erasures, the best that can be guaranteed by exploiting the inner code LRC structure is that the size of a repair set for the erasures increases a full s-fold from the size of a repair group for a single erasure in a girth ≥ 6 graph. This motivates the study of Tanner codes as HLRCs for the case of multiple erasures.

3.1.2 Tanner codes as HLRCs

Next, we show that Tanner codes may be viewed as HLRCs with $h = 2$ or $h = 3$ levels by presenting results on the parameters of h particular choices of inner codes (see the proofs of Theorems 3.6 and 3.7, respectively).

Theorem 3.6. *Let the inner code*

$$\mathcal{C}_i := (d_i, k_i, \delta_i)$$

of Tanner code $\mathcal{T}$ be an LRC with locality parameters (t_i, ρ_i) and availability τ_i for all $i \in [m]$. Then $\mathcal{T}$ is an HLRC with 3-level hierarchical locality with locality parameters

$$[(\tilde{t}_1, \tilde{\rho}_1), (\tilde{t}_2, \tilde{\rho}_2), (\tilde{t}_3, \tilde{\rho}_3)],$$

where

$$(\tilde{t}_1, \tilde{\rho}_1) = \left(\max_{(i,j)} \sum_{\ell=1}^{\mathfrak{c}_i} k_{ij\ell}, \min_{u\in[m]} \delta_u \right),$$
$$(\tilde{t}_2, \tilde{\rho}_2) = \left(\max_{u\in[m]} k_u, \min_{u\in[m]} \delta_u \right),$$
$$(\tilde{t}_3, \tilde{\rho}_3) = \left(\max_{u\in[m]} t_u, \min_{u\in[m]} \rho_u \right).$$

Furthermore, the HLRC has availability

$$\tilde{\tau}_1 = 1,$$

$$\tilde{\tau}_2 = \min_j \mathfrak{c}_j,$$

$$\tilde{\tau}_3 = \min_{u\in[m]} \tau_u$$

if $g(G) \geq 6$ *and availability*

$$\tilde{\tau}_1 = 1,$$

$$\tilde{\tau}_2 = 1,$$

$$\tilde{\tau}_3 = \min_{u\in[m]} \tau_u$$

if $g(G) = 4$.

Proof. Let x_{ij} denote an erased node. Consider the code comprised of x_{ij} and all variable nodes distance 2 from x_{ij} (i.e. all neighbors of neighbors of x_{ij}); this is a punctured code relative to $\mathcal{T}$. The dimension of this concatenated code is bounded above by

$$\sum_{\ell=1}^{\mathfrak{c}_i} k_{ij\ell}$$

and its minimum distance is equal to

$$\min_{\ell \in [\mathfrak{c}_i]} \delta_{ij\ell}.$$

The result for the 1^{st} level of hierarchy follows from maximizing the upper bound and minimizing the lower bound on minimum distance over all elements of L. For the 2^{nd} level of hierarchy, consider the set of inner codes associated with neighbors of erased node x_{ij}. Each of these inner codes is a punctured code obtained from the 1^{st} level concatenated code associated with x_{ij}, the dimension of each is bounded above by

$$\max_{u \in [m]} k_u,$$

and the minimum distance of each is bounded below by

$$\min_{u \in [m]} \delta_u.$$

The 3^{rd} level of hierarchy is associated with the locality of each of the inner codes. In particular, the punctured codes associated with the recovery set of each inner code are have dimension at most

$$\max_{u \in [m]} t_u$$

and the minimum distance is at least

$$\min_{u \in [m]} \rho_u.$$

Regardless of $g(G)$, the availability at the 1^{st} level of hierarchy is 1 because a single punctured code associated with the recovery set of each inner code at this level consists of all (distance 2) variable node neighbors of an erased node. When $g(G) \geq 6$, availability at the 2^{nd} level

of hierarchy is

$$\min_j \mathfrak{c}_j,$$

since any inner code associated with any neighbor of an erased node can be used for recovery and the neighborhoods of the check node neighbors of an erased node are pairwise disjoint. The availability at the 3^{rd} level of hierarchy in this case is

$$\tilde{\tau}_3 = \min_{u\in[m]} \tau_u$$

because we may only look at a punctured code associated with the recovery set of a particular inner code per Definition 3.3. Thus, the availability is given by the minimum availability of an inner code LRC. Now, suppose $g(G) = 4$. The availability at the 2^{nd} level of hierarchy is 1 because the inner code associated with any neighbor of an erased node can be used for recovery, but we can no longer guarantee that the neighborhoods of these check nodes are disjoint. The availability at the 3^{rd} level of hierarchy is again

$$\min_{u\in[m]} \tau_u.$$

□

We can also consider $\mathcal{T}$ as an HLRC with two levels of hierarchy, as described in the next theorem. The two level recovery offers an advantage in terms of availability over the three level recovery above given $g(G) \geq 6$. The availability in the 2^{nd} level (3^{rd} level of three tier recovery) is larger due to the larger punctured codes (the 1^{st} level) containing the 2^{nd} level. This means that we can simultaneously access the locality of any inner code in the neighborhood of the erased symbol. It is always ideal to eliminate small cycles in graph-based codes and hence the improvement in availability for Tanner codes based on graphs

with $g(G) \geq 6$ is meaningful.

Theorem 3.7. *Let the inner code*

$$\mathcal{C}_i := (d_i, k_i, \delta_i)$$

of Tanner code $\mathcal{T}$ be an LRC with locality parameters (t_i, ρ_i) and availability τ_i for all $i \in [m]$. Then $\mathcal{T}$ is an HLRC with 2-level hierarchical locality with locality parameters

$$[(\tilde{t}_1, \tilde{\rho}_1), (\tilde{t}_2, \tilde{\rho}_2)],$$

where

$$(\tilde{t}_1, \tilde{\rho}_1) = \left(\max_{\ell \in [m]} \sum_{\ell=1}^{\mathfrak{c}_i} k_{ij\ell}, \min_{u \in [m]} \delta_u \right)$$

$$(\tilde{t}_2, \tilde{\rho}_2) = \left(\max_{u \in [m]} t_u, \min_{u \in [m]} \rho_u \right)$$

Furthermore, the HLRC has availability

$$\tilde{\tau}_1 = 1,$$

$$\tilde{\tau}_2 = \min_{(i,j)} \sum_{\ell=1}^{\mathfrak{c}_i} \tau_{ij\ell}$$

if $g(G) \geq 6$ and availability

$$\tilde{\tau}_1 = 1,$$

$$\tilde{\tau}_2 = \min_{u \in [m]} \tau_u$$

if $g(G) = 4$.

Proof. The proof follows from the proof of Theorem 3.6 by letting the 1^{st} level of the 3-level

HLRC be the 1^{st} level of the 2-level HLRC, and the 3^{rd} level of the 3-level HLRC be the 2^{nd} level of the 2-level HLRC. Notice that the availability at the 3^{rd} level in a 3-level HLRC, that is 2^{nd} level of the 2-level HLRC, has increased for the case $g(G) \geq 6$. This is because we may take all punctured codes associated with the recovery sets of all inner codes within the entire concatenated 1^{st} level code, and are not limited to a single inner code. In the case where $g(G) \geq 6$, the neighborhoods of the check node neighbors of an erased node are pairwise disjoint and each punctured codes associated with the recovery sets of each inner code can be considered. □

3.2 Stopping Sets & Local Recovery

A significant advantage of giving graph-based codes an (H)LRC structure is the opportunity to implement graph-based message-passing decoding algorithms, which have low implementation complexity when operating on sparse graphs. Over an erasure channel, a so-called *peeling decoder*, which iteratively "peels off" erasures by contacting neighboring check nodes, is used [58]. *Stopping sets* of Tanner codes where each inner code is a simple parity-check (e.g. in the case of low-density parity-check codes) are patterns that cause iterative decoder failure over an erasure channel [57]. Formally, a stopping set is a subset S of variable nodes such that every check node adjacent to S is adjacent to at least two elements of S, stopping sets completely characterize erasure patterns where a peeling decoder will get stuck. In the case where each check node acts as its own (nontrivial) inner code on a subset of variable nodes (i.e. Tanner codes), the definition of stopping sets generalizes. Several previous works take the generalization of two to be

$$d_{\min}(\mathcal{C}),$$

where $\mathcal{C}$ is an inner code [59]. However, it is not necessarily the case that every word of weight

$$d_{\min}(\mathcal{C})$$

is a codeword, and thus some such erasure patterns remain correctable with this definition. Hence for our application we adopt the following:

Definition 3.8. Consider a Tanner code with graph $G = (L \dot{\cup} R, E)$. A *generalized stopping set* is a nonempty subset $S \subseteq L$ of variable nodes such that the support of the variable nodes in S adjacent to any check node j contains the support of a codeword of $\mathcal{C}_j$, the inner code at check node i.

Notice that a codeword whose values are erased at a generalized stopping set could be corrected by each adjacent inner code in at least two distinct ways; hence, the peeling decoder will be stuck. Conversely, if the peeling decoder gets stuck, the erased set must form a generalized stopping set. In the case of our 3-level graph-based HLRCs, we define hierarchical stopping sets in order to characterize message-passing decoder failure at each level.

Definition 3.9.

1. A 3^{rd} *level stopping set*, $\phi \neq S \subseteq L$ is contained within a single inner code $\mathcal{C}_j$ such that the punctured code obtained by restriction to each recovery set of the LRC $\mathcal{C}_j$ contains the support of a codeword of that punctured code.

2. A 2^{nd} *level stopping set* is a nonempty subset S of variable nodes contained within the neighborhood of a single check node such that S contains the support of a codeword of the associated inner code (i.e. S is a generalized stopping set within a single inner code of the 2^{nd} level of the HLRC).

3. A 1^{st} *level stopping set* is a nonempty subset S of variable nodes contained within a concatenated code associated with the 1^{st} level of the HLRC such that the intersection

of S with the neighborhood of each check node of the concatenated code contains the support of a codeword of the associated inner code (i.e. S is a generalized stopping set within a single concatenated code of the 1^{st} level of the HLRC).

One important parameter of a given graphical representation G of a code $\mathcal{C}$ is the minimum size of a stopping set, $s_{\min}(G)$. Note that in any code $\mathcal{C}$ fewer than $s_{\min}(G)$ erasures are guaranteed to be correctable by the peeling decoder. This value is referred to as the *stopping distance* or *stopping number* of the representation [60, 61, 62]. Considering that the support of any codeword of $\mathcal{C}$ must form a stopping set in any representation, we observe that

$$s_{\min}(G) \leq d_{\min}(\mathcal{C}).$$

Importantly, the inequality may be strict. The fact that a peeling decoder is being used is paramount: stopping sets indicate where iterative decoders fail, not necessarily where any decoder would fail. This is comparable to the failure of local recovery not necessarily implying failure of global recovery in an LRC.

Theorem 3.10. *Let*

$$s_{\min}(G_j)$$

denote the minimum size of a j^{th} level stopping set for $j \in [3]$, and let ρ_j denote the minimum distance of the LRC inner code $\mathcal{C}_j$. Then,

$$\min_j \rho_j \leq s_{\min}(G_3) \leq s_{\min}(G_2) = \min_j d_{\min}(\mathcal{C}_j) \leq s_{\min}(G_1)$$

Proof. Any 2^{nd} level stopping set associated with inner code $\mathcal{C}_j$ has weight lower bounded by

$$d_{\min}(\mathcal{C}_j),$$

and a minimum weight codeword of $\mathcal{C}_j$ is a 2^{nd} level stopping set. In other words,

$$s_{\min}(G_2) = \min_j d_{\min}(\mathcal{C}_j).$$

Consider a minimum 2^{nd} level stopping set S; by the above argument,

$$|S| = \min_j d_{\min}(\mathcal{C}_j).$$

Consider a node $j \in R$ so that S is contained in the neighborhood of the associated inner code $\mathcal{C}_j$ and

$$|S| = d_{\min}(\mathcal{C}_j).$$

By definition, S forms the support of a codeword of LRC $\mathcal{C}_j$, so the intersection of S with any punctured code associated with a recovery set of C_j must either be empty or must contain at least ρ_j elements by the definition of the minimum distance of the punctured code associated with a recovery set of C_j. Thus, S forms a 3^{rd} level stopping set, and

$$s_{\min}(G_3) \leq |S| = s_{\min}(G_2).$$

For the lower bound on $s_{\min}(G_3)$, notice that the intersection of any 3^{rd} level stopping set associated with LRC inner code $\mathcal{C}_j$ with each punctured code associated with a recovery set of $\mathcal{C}_j$ must be a codeword of the punctured code associated with a recovery set of an inner code. Thus, the minimum distance of a punctured code associated with a recovery set of an inner code of $\mathcal{C}_j$, ρ_j, gives a lower bound on the stopping set size. We then minimize over all inner codes. Finally, consider a minimum 1^{st} level stopping set S, and the intersection of S with the neighborhood of some check node y_j that is adjacent to a vertex in S. Call this subset S'. By definition of a 1^{st} level stopping set, it must be the case that S' contains the

support of a codeword of $\mathcal{C}_j$, where $\mathcal{C}_j$ the inner code associated with y_j; in other words, S' is a 2^{nd} level stopping set. Then,

$$s_{\min}(G_2) \leq |S'| \leq |S| = s_{\min}(G_1).$$

□

Remark 3.11. Notice that

$$d_{\min}(\mathcal{C}),$$

where $\mathcal{C}$ is the code defined by the entire Tanner graph, gives an upper bound on

$$s_{\min}(G_1)$$

since the support of any codeword of $\mathcal{C}$ restricted to any concatenated code (such that the result is nonempty) must result in codewords at each of the constituent inner codes.

Remark 3.12. A natural question is when the inequalities of Theorem 3.10 are met with equality. First observe that the collection of 2^{nd} level stopping sets is contained in the collection of 3^{rd} level stopping sets: any codeword of an inner code $\mathcal{C}_j$ satisfies each of the recovery sets of $\mathcal{C}_j$. Strict set inclusion occurs exactly when the punctured code associated with a recovery set of an inner code does not completely define $\mathcal{C}_j$ (i.e. when more checks beyond the code checks are needed). If the punctured code associated with a recovery set of an inner code does define the code, we have

$$s_{\min}(G_3) = s_{\min}(G_2);$$

otherwise the inequality may be strict. Next, consider a 1^{st} level stopping set S of size

$$s_{\min}(G_1),$$

and suppose

$$s_{\min}(G_1) = \min_j d_{\min}(\mathcal{C}_j).$$

Then the intersection of S with the neighborhood of each constituent check node of its associated concatenated code must be equal to S. As long as $\mathfrak{c}_1 > 1$, this can only occur if

$$\min_j d_{\min}(\mathcal{C}_j) = 1$$

or $g(G) = 4$. Otherwise,

$$s_{\min}(G_2) < s_{\min}(G_1).$$

Recall that we iteratively correct erasures in an HLRC using punctured codes within the Tanner codes, i.e. by decreasing the level index. Increasing the level of hierarchy needed for correction is detrimental in terms of locality, but may be necessary if a higher number of erasures must be corrected. Theorem 3.10 and Remark 3.12 imply that decreasing the level index of an HLRC from a Tanner code does not decrease the number of correctable erasures, and in fact can give an erasure correction advantage in many cases, even when restricting to a message-passing peeling decoder.

3.3 Conclusion

In this chapter, we study local erasure recovery in Tanner codes. Establishing some independent results that were built upon in joint work with Allison Beemer. We provide bounds

on the locality and availability of Tanner codes when the inner codes are locally recoverable codes. Moreover, we show that in this setting the Tanner codes allow hierarchical local recovery. This analysis results in insights about the behaviour of tiered stopping sets of Tanner code HLRCs.

We are currently comparing our bounds on the locality and availability of Tanner codes where the underlying inner codes are LRCs with bounds on the locality and availability of existing (H)LRC constructions.

Chapter 4

Twisted algebraic geometry codes

In this chapter, we modify the construction of twisted Reed-Solomon codes given by [16] and twisted Hermitian codes [31] for codes on a quotient of the Hermitian curve and norm-trace codes to yield new families of codes, with the goal of producing codes which have large Schur squares. We focus on one-point algebraic geomtry codes.

4.1 Code-based cryptography

Post-quantum cryptography uses classical techniques to secure information from quantum attacks. Some major topics in post-quantum cryptography include lattice-based, supersingular elliptic curve isogeny-based, code-based, etc. Here we consider code-based cryptography. A typical cryptosystem can be defined using 3 main algorithms: key generation, encryption and decryption. A code-based cryptosystem can be defined as follows:

- **Key Generation**: Consider an $[n, k, d]$ code $\mathcal{C}$ over a finite field $\mathbb{F}_q$ capable of correcting at least t errors. Let $G \in \mathbb{F}_q^{k\times n}$ be a generator matrix of $\mathcal{C}$. Let $P \in \mathbb{F}_q^{k\times k}$ a

random permutation matrix. Choose a random nonsingular matrix $S \in \mathbb{F}_q^{k\times k}$ and a permutation matrix $P \in \mathbb{F}_q^{n\times n}$. The public key is

$$G^{pub} := SGP.$$

The private key is

$$(S, D, P)$$

where D is a suitable decoding algorithm of $\mathcal{C}$.

- **Encryption**: Given a message $m \in \mathbb{F}_q^k$, Alice chooses a random vector $z \in \mathbb{F}_q^{1\times n}$ such that $wt(z) < t$, and sends

$$c = mG^{pub} + z = mSGP + z$$

to Bob.

- **Decryption**: On receiving c, Bob computes

$$cP^{-1} = mSG + zP^{-1},$$

recovers mS using the decoding algorithm D and computes

$$mSS^{-1}$$

to retrieve m.

4.1.1 McElice cryptosystem

The McElice cryptosystem is a code-based cryptosystem introduced in [10]. The underlying code is a binary Goppa code.

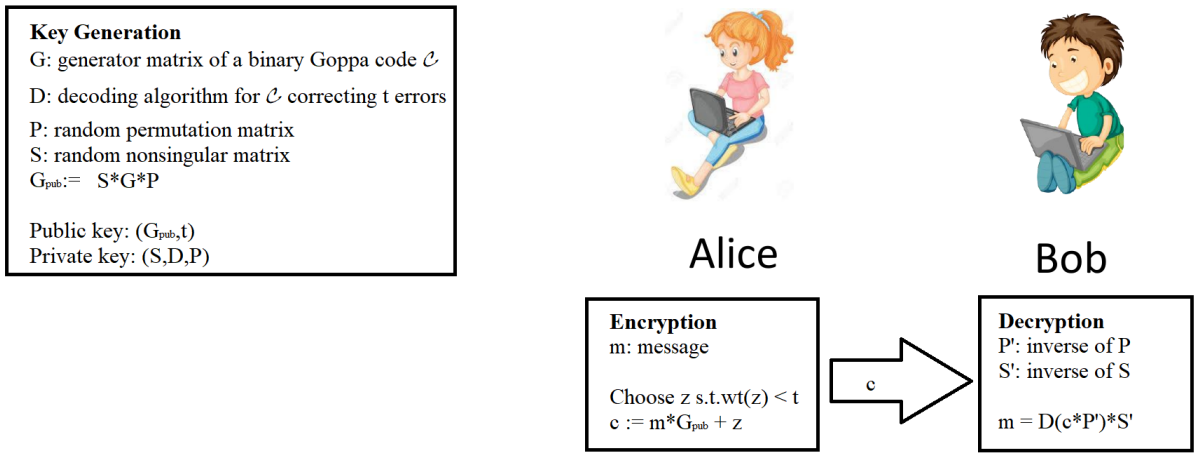

Figure 4.1: McEliece Cryptosystem

To maintain security, the underlying code $\mathcal{C}$ must not be revealed. This is ensured by choosing random linear codes whose decoding is an NP-hard problem, as shown in [24]. The McEliece cryptosystem is thought to be resistant to the existing attacks (including quantum attacks). The key size of the McEliece cryptosystem is very large and this makes practical adoption of the cryptosystem harder. Therefore, variants of the McEliece cryptosystem are studied by replacing the underlying Goppa codes with other linear codes [25], [48]. However, the additional structure can cause vulnerabilities and thus lead to attacks on the cryptosystem [27], [15], [36].

Schur products were originally used to define error-locating pairs [13] and now arise in several applications, such as secret sharing [14] and code-based cryptography [15]. It is difficult to

find codes whose Schur squares have a high dimension. Beelen, Puchinger, and Nielsen [16], introduced twisted Reed-Solomon codes, drawing upon ideas from the twisted Gabidulin codes of Sheekey [17]. These codes have high Schur square dimensions. In prior work, we extended these ideas to construct twisted Hermitian codes [31] whose Schur square has large dimension and could be considered as a replacement of Goppa codes in the McEliece cryptosystem. Later we consider an attack on this cryptosystem. The results are summarized in the next two sections.

We employ a few basic results from additive number theory (the notion of a Sidon set) to determine the lower bound on Schur squares of twisted algebraic geometry codes.

Definition 4.1. A set $A \subseteq \mathbb{N}$ is a finite Sidon set provided it is finite and $\forall a, b, c, d \in A$, $a + b = c + d$ if and only if $(a, b) = (c, d)$ or $(a, b) = (d, c)$.

Erdös and Turan show in [43] that every subset of a Sidon set is itself a Sidon set and that every nonempty subset of $\mathbb{N}$ contains a Sidon set. For finite and nonempty $A \subseteq \mathbb{N}$, let $S[A]$ denote the largest subset of A that is a Sidon set. Gowers shows in [44] that $| S[A] | \leq 2\sqrt{| A |}$.

Given an algebraic geometry code $\mathcal{C}(\alpha P_\infty)$ on the curve $\mathcal{X}$. Consider $c = ev_{QH}(f), c' = ev_{QH}(f') \in \mathcal{C}(\alpha P_\infty)$ with $f, f' \in \mathcal{L}(\alpha P_\infty)$. Then

$$c * c' = ev_{QH}(f) * ev_{QH}(f') = ev_{QH}(ff').$$

Since $(f) \geq -\alpha P_\infty$ and $(f') \geq -\alpha P_\infty$,

$$(ff') = (f) + (f') \geq -2\alpha P_\infty.$$

Thus $ff' \in \mathcal{L}(2\alpha P_\infty)$, that is $\mathcal{C}(\alpha P_\infty)^2 \subseteq \mathcal{C}(2\alpha P_\infty)$, and equality is achieved when $\alpha \geq 2g+1$.

In this case, $\mathcal{C}(\alpha P_\infty)$ has dimension $\alpha + 1 - g$ and

$$\dim \mathcal{C}(\alpha P_\infty)^2 = \dim \mathcal{C}(2\alpha P_\infty) = 2\alpha + 1 - g \ << \ \binom{(\alpha + 1 - g) + 1}{2}; \tag{4.1}$$

see also [37] for details. Note the following proposition where given a code $\mathcal{C}$ of dimension k, it is desirable for $\mathcal{C}^2$ to have dimension close to $\binom{k+1}{2}$ or quadratic in k. This is in contrast to that seen in (4.1) where the dimension is linear in k. This serves as motivation to consider twisted algebraic geometry codes.

Proposition 4.2. *[[14, Theorem 2.3]] Let $n : \mathbb{N} \to \mathbb{N}$ be such that $n(k) \geq \binom{k+1}{2}$. Then for some positive real number δ and k large enough,*

$$\Pr\left[\dim \mathcal{C}^2 = \binom{k+1}{2}\right] \geq 1 - 2^{-\delta\left(n(k) - \binom{k+1}{2}\right)} \tag{4.2}$$

where $\mathcal{C}$ is chosen uniformly at random from the family of all $[n(k), k, d]$ codes over $\mathbb{F}_q$ whose generator matrices are in systematic form.

4.1.2 Code-based cryptosystem based on twisted Hermitian codes

Consider the set

$$B(\alpha P_\infty) := \left\{x^i y^j : i, j \in \mathbb{N}, j \leq q - 1, \delta_H(x^i y^j) \leq \alpha\right\},$$

and the vector space $\mathcal{L}(\alpha P_\infty) := \langle B(\alpha P_\infty)\rangle$ on the Hermitian curve

$$\mathcal{X}_q : y^q + y = x^{q+1}.$$

Let $\alpha = uq + v(q+1) \geq q^2 - q - 1$ where $u, v \in \mathbb{N}$. Let $\ell \in \mathbb{Z}^+$,

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2\right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of nonzero integers, and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of integers such that

$$a_k q + b_k(q+1) \leq uq + v(q+1) < (u + r_k)q + (v + s_k)(q+1) < q^3$$

for $k = 1, \ldots, \ell$. Let

$$\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell) \in \left(\mathbb{F}_{q^2} \setminus \{0\}\right)^\ell.$$

The set of $(\mathbf{t}, \mathbf{h}, \boldsymbol{\eta})$-twisted bivariate polynomials is

$$B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \left(B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right) \cup \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} + \eta_k x^{u+r_k} y^{v+s_k} \right\}.$$

Let $\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \langle B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \rangle$. The twisted Hermitian code $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ is

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) := ev_H\left(\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}\right) \subseteq \mathbb{F}_{q^2}^n.$$

We consider the potential use of twisted Hermitian codes in a code-based cryptosystem. First, we abstract the key elements of the McEliece cryptosystem for use with an arbitrary linear code (in place of the Goppa code in [10]). Then we consider the role of squares in attacking the resulting system, noting how the twisted codes avoid direct distinguisher attack.

This section concludes with considerations prompted by the recent attack of Lavauzelle and Renner [28] on a twisted Reed-Solomon code-based cryptosystem.

The Schur square distinguisher is an attack applied to the McEliece cryptosystem implemented with Reed-Solomon codes in [36]. Though the attacker does not know the linear code $\mathcal{C}$ underlying G^{PUB}, the distinguisher may allow the attacker to know $\dim \mathcal{C}^2$. Schur squares of Reed-Solomon and Hermitian codes have low dimensions. Therefore, $\dim \mathcal{C}^2$ can be used to distinguish these codes from a random linear code. This is demonstrated in [36] where generalized Reed-Solomon codes are considered; Schur products are used to identify $\mathcal{C}^2$ within the family from which it is drawn; and the Sidelnikov and Shestakov algorithm may then be used to identify $\mathcal{C}$. See also [47] for other approaches involving generalized Reed-Solomon codes. Since $\dim \mathcal{C}^2$ can be an identifying characteristic of the family of codes from which $\mathcal{C}$ is drawn, the attacker may then use a family-specific structural attack on intercepted messages. Both twisted Reed–Solomon and twisted Hermitian codes may avoid a direct application of this attack if constructed to have large dimensional squares.

Based on the attacks described above, it is desirable to implement this code-based cryptosystem with a family of codes whose Schur squares are indistinguishable from those of random codes. With this in mind twisted Reed-Solomon codes were introduced in [16] and can be defined as follows.

Definition 4.3. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ be pairwise distinct field elements, and fix $1 \leq k \leq n$, $\ell \geq 1$. Let

$$\mathbf{t} \in \{1, \ldots, n-k\}^\ell,$$

$$\mathbf{h} \in \{0, \cdots, k-1\}^\ell,$$

and

$$\boldsymbol{\eta} \in (\mathbb{F}_q \backslash \{0\})^\ell.$$

Let

$$f \in \left\{ \sum_{i=0}^{k-1} a_i x^i + \sum_{j=1}^{\ell} \eta_j a_{h_j} x^{k-1+t_j} : a_i \in \mathbb{F}_q \right\}.$$

A twisted Reed-Solomon code of length n and dimension k is:

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(k) = \{(f(\alpha_1), \cdots, f(\alpha_n))\}.$$

Consider the evaluation map

$$\begin{array}{rccc} ev_\alpha : & \mathbb{F}_q[x] & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(\alpha_1), \cdots, f(\alpha_n)). \end{array}$$

Let q_0 be a prime, and $q = q_\ell = q_0^{2^\ell}$. Lavazuelle and Renner showed in [28] that the subfield subcode $\mathcal{C}_{sub} = \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(k) \cap \mathbb{F}_{q_0}^n$ of $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(k)$ is given by

$$\mathcal{C}_{sub} = \left\langle ev_\alpha(x^i) : i \in \{0, 1, \cdots, k-1\} \backslash \{h_1, h_2, \cdots, h_\ell\} \right\rangle_{\mathbb{F}_{q_0}}.$$

Given that $\mathcal{C}_{sub}$ is not a Reed-Solomon code, the Sidelnikov-Shestakov attack cannot be directly applied. However, for $\ell \leq \frac{1}{2}(\sqrt{n} - 3)$ the Schur square $\mathcal{C}_{sub}^2$ is a Reed-Solomon code. The length of $\mathcal{C}_{sub}^2$ is n and its dimension is $2k - 1$. This idea forms the basis for an efficient key-recovery attack on the code-based cryptosystem employing twisted Reed-Solomon codes.

The similarity in construction of twisted Hermitian codes and twisted Reed-Solomon codes suggests a possible attack on the cryptosystem based on the twisted Hermitian codes. We now consider the possible components of such an attack. The code $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ over $\mathbb{F}_{q^2}$, where

$$\mathbb{F}_{q_0^2} = \mathbb{F}_{s_0} \subsetneqq \mathbb{F}_{s_1} \subsetneqq \cdots \subsetneqq \mathbb{F}_{s_\ell} = \mathbb{F}_{q^2},$$

and consider the subfield subcode

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \cap \left(\mathbb{F}_{q_0}^2\right)^n$$

where $\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell$.

Lemma 4.4. *Let $f \in \langle \mathcal{M} \rangle_{\mathbb{F}_{q^2}} \subseteq \mathbb{F}_{q^2}[x, y]$ and $P_1, \ldots, P_n \in \mathcal{X}_{q_0^2}(\mathbb{F}_{q_0^2})$. Then $ev_H(f) \in \mathbb{F}_{q_0^2}^n$ if and only if $f \in \langle \mathcal{M}_0 \rangle_{\mathbb{F}_{q_0^2}}$ where*

$$\mathcal{M}_0 := \left\{ x^i y^j : i, j \in \mathbb{N}, 0 \leq i \leq q_0^2 - 1, 0 \leq j \leq q_0 - 1 \right\}.$$

Proof. Suppose $f \in \langle \mathcal{M}_0 \rangle_{\mathbb{F}_{q_0^2}}$ and $P_1, \ldots, P_n \in \mathcal{X}_{q_0^2}(\mathbb{F}_{q_0^2})$. Then it is clear that $ev_H(f) \in \mathbb{F}_{q_0^2}^n$. Conversely, consider $c := ev_H(f) \in \mathbb{F}_{q_0^2}^n$ where $f \in \langle \mathcal{M} \rangle_{\mathbb{F}_{q^2}} \subseteq \mathbb{F}_{q^2}[x, y]$. According to [46, Lemma 6], there exists

$$p = \sum_{\alpha \in \mathbb{F}_{q_0^2}} \prod_{\alpha' \in \mathbb{F}_{q_0^2} \setminus \{\alpha\}} \frac{x - \alpha'}{\alpha - \alpha'} \left(\sum_{\beta \in B_\alpha} \gamma_{\alpha,\beta} \prod_{\beta' \in B_\alpha \setminus \{\beta\}} \frac{y - \beta'}{\beta - \beta'} \right)$$

such that $ev_H(p) = c$. Notice that $p \in \langle \mathcal{M}_0 \rangle_{\mathbb{F}_{q_0^2}} \subseteq \langle \mathcal{M} \rangle_{\mathbb{F}_{q^2}}$. Since $ev_H : \langle \mathcal{M} \rangle_{\mathbb{F}_{q^2}} \to \mathbb{F}_{q^2}^n$ is an injective map and

$$c = ev_H(p) = ev_H(f),$$

it follows that

$$f = p \in \langle \mathcal{M}_0 \rangle_{\mathbb{F}_{q_0^2}}.$$

□

Proposition 4.5. *Given a twisted Hermitian code* $\mathcal{C} = \mathcal{C}_{\boldsymbol{t},\boldsymbol{h},\boldsymbol{\eta}}(\alpha P_\infty)$ *and* $P_1, \ldots, P_n \in \mathcal{X}_{q_0^2}(\mathbb{F}_{q_0^2})$,

$$\mathcal{C} \cap \mathbb{F}_{q_0^2}^n = \left\{ ev_H(f) : f \in \left\langle B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right\rangle_{\mathbb{F}_{q_0^2}} \right\}.$$

Proof. Consider $ev_H(f)$ where $f \in \left\langle B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right\rangle_{\mathbb{F}_{q_0^2}}$. Then $ev_H(f) \in \mathcal{C} \cap \mathbb{F}_{q_0^2}^n$ as each $P_i \in \mathcal{X}_{q_0}(\mathbb{F}_{q_0^2})$. On the other hand, suppose that $ev_H(f) \in \mathcal{C} \cap \mathbb{F}_{q_0^2}^n$. Then Lemma 4.4 applies so that

$$f \in \left\langle B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right\rangle_{\mathbb{F}_{q_0^2}}.$$

□

This result prompts the conjecture that the Schur square of the subfield subcode of a twisted Hermitian code in Proposition 4.5 is a Hermitian code. This is related to [27, Conjecture 19]. Positive resolution of these conjectures would lay the groundwork for an attack on a twisted Hermitian code-based cryptosystem.

4.2 Twisted codes from a quotient of the Hermitian curve

Codes over a quotient of the Hermitian curve are studied because they can have better code parameters (such as rate or relative distance) as compared to those of the Hermitian code. In this section, we look at the twisted codes from a quotient of the Hermitian curve which may offer similar advantages over the twisted Hermitian codes.

Consider the set

$$B(\alpha P_\infty) := \left\{ x^i y^j : i, j \in \mathbb{N}, j \leq q-1, \delta_{QH}(x^i y^j) \leq \alpha \right\},$$

and the vector space $\mathcal{L}(\alpha P_\infty) := \langle B(\alpha P_\infty) \rangle$ from a quotient of the Hermitian curve

$$\mathcal{X}_{q,m} : y^q + y = x^m$$

such that $m \in \mathbb{N}$ and $m|(q+1)$. Let

$$\alpha = uq + vm \geq (m-1)(q-1) - 1$$

where $u, v \in \mathbb{N}$. Let $\ell \in \mathbb{Z}^+$,

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2 \right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of nonzero integers, and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2 \right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of integers satisfying

$$a_k q + b_k m \leq uq + vm < (u + r_k)q + (v + s_k)m < q(m(q-1) + 1)$$

for $k = 1, \ldots, \ell$. Let $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell) \in (\mathbb{F}_{q^2} \setminus \{0\})^\ell$. The set of $(\mathbf{t}, \mathbf{h}, \boldsymbol{\eta})$-twisted bivariate

polynomials is

$$B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \left(B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right) \cup \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} + \eta_k x^{u+r_k} y^{v+s_k} \right\}.$$

Let $\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \langle B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \rangle$. The twisted code from a quotient of the Hermitian curve $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ is

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) := ev_{QH}\left(\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}\right) \subseteq \mathbb{F}_{q^2}^n.$$

Note that $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ has the same length as the one-point code from a quotient of the Hermitian curve $\mathcal{C}(\alpha P_\infty)$. The dimension of the twisted code from a quotient of the Hermitian curve is

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \dim \mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = |B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)| = |B(\alpha P_\infty)| = \dim \mathcal{C}(\alpha P_\infty),$$

and a generator matrix of the twisted code from a quotient of the Hermitian curve is

$$\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \begin{bmatrix} ev_{QH}(f_1) \\ ev_{QH}(f_2) \\ \vdots \\ ev_{QH}(f_k) \end{bmatrix}$$

where $B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \langle f_1, f_2, \ldots, f_k \rangle$. Let us consider an example of twisted code from a quotient of the Hermitian curve.

Example 4.6. Let $q = 3$, $m = 2$ and $\alpha = 1(q) + 1(m) = 5$. Consider a quotient of the Hermitian curve $\mathcal{X}_{3,2} : y^2 + y = x^2$ over a finite field of order $q^2 = 9$, $\mathbb{F}_9 = \{0, 1, 2, a, a+1, a+2, 2a, 2a+1, 2a+2\} \cong {}^{\mathbb{Z}_3[x]}/_{\langle x^2+1 \rangle}$. Consider the set

$$B(5P_\infty) = \{1, x, y, x^2, xy\}.$$

The $q(m(q-1)+1) = 15$ affine rational points on $\mathcal{X}_{3,2}$ are:

$$\begin{aligned}
P_1 &= (0:0:1)\\
P_2 &= (0:a:1)\\
P_3 &= (0:2a:1)\\
P_4 &= (1:2:1)\\
P_5 &= (1:a+2:1)\\
P_6 &= (1:2a+2:1)\\
P_7 &= (2:2:1)\\
P_8 &= (2:a+2:1)\\
P_9 &= (2:2a+2:1)\\
P_{10} &= (a:1:1)\\
P_{11} &= (a:a+1:1)\\
P_{12} &= (a:2a+1:1)\\
P_{13} &= (2a:1:1)\\
P_{14} &= (2a:a+1:1)\\
P_{15} &= (2a:2a+1:1).
\end{aligned}$$

Let $\ell = 2$,

$$\mathbf{t} = ((1,0),(2,0))\,,$$
$$\mathbf{h} = ((2,0),(1,1))\,,$$

and

$$\boldsymbol{\eta} = (1,a)\,.$$

Then

$$\bigcup_{k=1}^{2}\{x^{a_k}y^{b_k}\} = \{x^2, xy\},$$

and

$$\bigcup_{k=1}^{2}\{x^{a_k}y^{b_k} + \eta_k x^{u+r_k}y^{v+s_k}\} = \{x^2 + x^2y, xy + ax^3y\}$$

so that

$$B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) = \{1, x, y, x^2 + x^2y, xy + ax^3y\}.$$

We get the following vector space by applying ev_{QH} to $B(5P_\infty)$

$$\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) = \langle B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)\rangle.$$

The resulting twisted code from a quotient of the Hermitian curve is

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) = ev_{QH}\left(\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)\right).$$

A generator matrix $\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)$ for the twisted code from a quotient of the Hermitian curve may be obtained by evaluating each element of $B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty)$ at each of the P_i, $1 \le i \le 15$, to obtain $\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(5P_\infty) =$

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}	P_{12}	P_{13}	P_{14}	P_{15}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
x	0	0	0	1	1	1	2	2	2	a	a	a	$2a$	$2a$	$2a$
y	0	a	$2a$	2	$a+2$	$2a+2$	2	$a+2$	$2a+2$	1	$a+1$	$2a+1$	1	$a+1$	$2a+1$
x^2+x^2y	0	0	0	0	a	$2a$	0	a	$2a$	1	$2a+1$	$a+1$	1	$2a+1$	$a+1$
$xy+ax^3y$	0	0	0	$a+2$	$2a$	1	$2a+1$	a	2	$a+1$	$2a$	2	$2a+2$	a	1

.

However, twisted codes from quotient of the Hermitian curve differ from codes from a quotient of the Hermitian curve. They have the same length and dimension. However, the

distinction can be shown by considering the largest code from quotient of the Hermitian curve containing the twisted code of quotient of the Hermitian curve and the smallest code from quotient of the Hermitian curve contained in the twisted code from quotient of the Hermitian curve. Note that

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2\right)^\ell$$

and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell .$$

Let

$$\alpha' = \min\{a_i q + b_i m : i = 1, \ldots, \ell\} - 1$$

and

$$\alpha'' = \alpha + \max\{r_i q + s_i m : i = 1, \ldots, \ell\} .$$

Then

$$\mathcal{L}(\alpha' P_\infty) \subseteq \mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subseteq \mathcal{L}(\alpha'' P_\infty)$$

and

$$\mathcal{C}(\alpha' P_\infty) \subseteq \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subseteq \mathcal{C}(\alpha'' P_\infty).$$

Furthermore, $\dim \mathcal{C}(\alpha' P_\infty) =$

$$| \left\{ x^i y^j \in B(\alpha P_\infty) \mid \delta_{QH}(x^i y^j) < \min\{a_i q + b_i m : i = 1, \ldots, \ell\} \right\} | < k,$$

and

$$a_k q + b_k m \leq uq + vm$$

for all $1 \leq k \leq l$, and the (a_k, b_k) are distinct, and

$$\dim \mathcal{C}(\alpha'' P_\infty) = (\alpha + \max\{r_k q + s_k m \mid k = 1, \ldots, \ell\}) + 1 - g \geq k + q.$$

This shows that twisted codes from this quotient of the Hermitian curve are not codes from this quotient of the Hermitian curve. This observation helps in determining bounds on the minimum distance of twisted codes from this quotient of the Hermitian curve.

Consider a twisted code from this quotient of the Hermitian curve $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ with

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2\right)^\ell$$

and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell.$$

Then

$$\mathcal{C}(\alpha' P_\infty) \subsetneqq \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subsetneqq \mathcal{C}(\alpha'' P_\infty)$$

where

$$\alpha' = \min\{a_i q + b_i m : i = 1, \ldots, \ell\} - 1$$

and

$$\alpha'' = \alpha + \max\{r_i q + s_i m : i = 1, \ldots, \ell\}.$$

In the case that $2g - 2 < \alpha'$ and $\alpha'' < n$, as given in [21], we have that

$$n - \alpha'' \leq d\left(\mathcal{C}(\alpha'' P_\infty)\right) \leq n - \alpha'.$$

Therefore, the minimum distance d of $\mathcal{C}^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ satisfies

$$n - \alpha'' \leq d\left(\mathcal{C}(\alpha'' P_\infty)\right) \leq d \leq d\left(\mathcal{C}(\alpha' P_\infty)\right).$$

Example 4.7. Consider the twisted code $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(9P_\infty)$ from the quotient of the Hermitian curve $y^3 + y = x^2$ with $q = 3$, $m = 2$, $\alpha = 9$,

$$\begin{aligned} \mathbf{t} &= ((1,0),(0,1)), \\ \mathbf{h} &= ((1,2),(0,3)), \end{aligned}$$

and $\boldsymbol{\eta} = (\eta_1, \eta_2)$, where $\eta_1, \eta_2 \in \mathbb{F}_9$. Then

$$\alpha'' = 9 + \max\{r_i q + s_i m : i = 1, 2\} = 12$$

and

$$\alpha' = \min\{a_i q + b_i m : i = 1, 2\} - 1 = 5$$

from which it follows that

$$\mathcal{C}(5P_\infty) \subsetneqq \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(9P_\infty) \subsetneqq \mathcal{C}(12P_\infty).$$

According to [32, Theorem 2.2.2], $d\left(\mathcal{C}(5P_\infty)\right) = 10$ and $d\left(\mathcal{C}(12P_\infty)\right) = 3$ so that

$$3 \leq d\left(\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(9P_\infty)\right) \leq 10.$$

We now show that the twisted code $\mathcal{C}^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ from a quotient of the Hermitian curve may have a Schur square with much larger dimension in comparison to the square of the code

from a quotient of the Hermitian curve itself. Consider the set of bivariate polynomials

$$\mathcal{M} := \left\{ x^i y^j : i, j \in \mathbb{N}, 0 \leq i \leq m(q-1), 0 \leq j \leq q-1 \right\} \subseteq \mathbb{F}_{q^2}[x, y].$$

Let the domain of ev_{QH} be restricted to $\langle \mathcal{M} \rangle$ as described above. Assume that $0 \neq p(x, y) \in \langle \mathcal{M} \rangle$ such that $ev_{QH}(p(x, y)) = \mathbf{0} \in \mathbb{F}_{q^2}^n$. Then every rational affine point $(x : y : 1)$ of a quotient of the Hermitian curve $\mathcal{X}_{q,m}$ also satisfies $p(x, y) = 0$. Fix $a \in \mathbb{F}_{q^2}$. There are $m(q-1)+1$ choices of a such that there is a corresponding b value where $(a : b : 1)$ satisfies a quotient of the Hermitian curve $\mathcal{X}_{q,m}$. Then the univariate polynomial $p(a, y)$ has q distinct zeros in $\mathbb{F}_{q^2}$, despite the fact that $\deg(p(a, y)) \leq q-1$. Hence $p(a, y) \equiv 0$ for all $a \in \mathbb{F}_{q^2}$. On the other hand,

$$p(x, y) = \sum_{j=0}^{q-1} \left(\sum_{i=0}^{m(q-1)} a_{ij} x^i \right) y^j = \sum_{j=0}^{q-1} q_j(x) y^j$$

where $q_j(x) = \sum_{i=0}^{m(q-1)} a_{ij} x^i$ and $q_j(a) = 0$ for all $a \in \mathbb{F}_{q^2}$. This implies the univariate polynomial $q_j(x)$ has $m(q-1)+1$ zeros in $\mathbb{F}_{q^2}^n$, despite the fact that $\deg(q_j) \leq m(q-1)$. As a result, $p(x, y) \equiv 0$, which is a contradiction. Then the evaluation map $ev_{QH} : \langle \mathcal{M} \rangle \to \mathbb{F}_{q^2}^n$ is an injective mapping.

Definition 4.8. Suppose $i, j \in \mathbb{N}$ are such that $0 \leq i \leq 2m(q-1)$ and $0 \leq j \leq q-1$. We define

$$\overline{x^i y^j} := \begin{cases} x^i y^j & \text{if } 0 \leq i \leq m(q-1) \\ x^{i-m(q-1)} y^j & \text{otherwise.} \end{cases}$$

For $f(x, y) = \sum c_k x^{i_k} y^{j_k} \in \mathbb{F}_{q^2}[x, y]$, we define

$$\overline{f} := \sum c_k \overline{x^{i_k} y^{j_k}}. \tag{4.3}$$

It follows immediately that for $f = \sum c_k x^{i_k} y^{j_k}$ and $g = \sum d_h x^{i_h} y^{j_h} \in \mathcal{L}(\alpha P_\infty)$,

$$ev_{QH}(f \cdot g) = ev_{QH}(\overline{f \cdot g}).$$

Given $f(x,y) = \sum_{k=1}^{n} c_k x^{i_k} y^{j_k} \in \mathbb{F}_{q^2}[x,y]$,

$$\delta_{QH}(f) := \max\left\{i_k q + j_k m : k = 1, \ldots, n\right\}. \tag{4.4}$$

If $B = \{f_1, \ldots, f_m\} \subseteq \mathbb{F}_{q^2}[x,y]$, then

$$\delta_{QH}(B) := \left\{\delta_{QH}(f_k) : k = 1, \ldots, m\right\}. \tag{4.5}$$

Lemma 4.9. *Let $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ be a twisted code from a quotient of the Hermitian curve. Then*

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \mid \overline{D} \mid$$

where $\overline{D} := \{\delta_{QH}(\overline{f \cdot g}) \mid f, g \in \mathcal{L}(\alpha P_\infty)\}$.

Note that $\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2$ can be made large by choosing $\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}$ to maximize the size of $\overline{D}$.

Given $\mathcal{M} = \{x^i y^j : i, j \in \mathbb{N}, 0 \leq i \leq m(q-1), 0 \leq j \leq q-1\}$, set

$$\mathcal{M}_2 := \left\{x^i y^j \in \mathcal{M} : \delta_{QH}(x^i y^j) \leq \left\lceil \frac{\max \delta_{QH}(\mathcal{M})}{2} \right\rceil \right\}.$$

Observe that for any prime power q,

$$\left\lceil \frac{\max \delta_{QH}(\mathcal{M})}{2} \right\rceil = \left\lceil \frac{m(q-1)q + (q-1)m}{2} \right\rceil \geq 2g + 1.$$

It follows that

$$\mathcal{M} \subseteq \mathcal{M}_2^2.$$

We make use of this observation in the following lemma.

Lemma 4.10. *Let $A \subseteq \mathbb{F}[x,y]$ be a set of elements with distinct pole orders such that $\delta_{QH}(A) \subseteq \delta_{QH}(\mathcal{M}_2)$. Then $\mid \delta_{QH}(A^{\underline{2}}) \setminus \delta_{QH}(\mathcal{M}) \mid \leq g$.*

Proof. Since $\mathcal{M} \subseteq \mathcal{M}_2^2$, $\delta_{QH}(\mathcal{M}) \subseteq \delta_{QH}(\mathcal{M}^{\underline{2}})$. Observe that

$$\mid \delta_{QH}(\mathcal{M}_2^2) \setminus \delta_{QH}(\mathcal{M}) \mid = \mid \delta_{QH}\left(\mathcal{M}_2^2\right) \mid - \mid \delta_{QH}(\mathcal{M}) \mid = \big[(mq^2 - m - 1) + 1 - g\big] - (mq^2 - mq - q) = g.$$

Since $\delta_{QH}(A^{\underline{2}}) \subseteq \delta_{QH}(\mathcal{M}_2^2)$, it follows that $\mid (\delta_{QH}(A^{\underline{2}}) \setminus \delta_{QH}(\mathcal{M})) \mid \leq g$. □

Consider the map

$$\begin{aligned} \phi_q : \ \mathbb{N} &\to \mathbb{Z}^2 \\ w &\mapsto (m\lfloor \tfrac{w}{q} \rfloor - w, w - q\lfloor \tfrac{w}{q} \rfloor). \end{aligned}$$

Theorem 4.11. *For a given prime power q_0, let $\alpha \in \delta_{QH}(\mathcal{M})$ be such that*

$$\alpha \leq \frac{mq^2 - mq - q + 2\sqrt{mq^2 - mq - q + 1} + 1}{4}$$

and

$$\begin{aligned} \mathcal{P} &:= \left\{ \delta_{QH}(x^i y^j) : x^i y^j \in \mathcal{M}, \delta_{QH}(x^i y^j) \leq \alpha \right\} \\ \mathcal{T} &:= \left\{ \delta_{QH}(x^i y^j) : x^i y^j \in \mathcal{M}, \delta_{QH}(x^i y^j) > \alpha \right\} = \{t_1, \ldots, t_\ell\} \\ \mathcal{H} &:= \mathcal{P} \setminus S[\mathcal{P}] = \{h_1, \ldots, h_\ell\} \end{aligned}$$

satisfying $\ell := \mid \mathcal{H} \mid \leq \mid \mathcal{T} \mid$. *Let*

$$\mathbf{h} = (\phi(h_1), \ldots, \phi(h_\ell));$$
$$\mathbf{t} = (\phi(t_1) - (u, v), \ldots, \phi(t_\ell) - (u, v));$$

$s_1, \ldots, s_\ell$ *be prime powers such that*

$$\mathbb{F}_{q_0^2} = \mathbb{F}_{s_0} \subsetneqq \mathbb{F}_{s_1} \subsetneqq \cdots \subsetneqq \mathbb{F}_{s_\ell} = \mathbb{F}_{q^2}; \tag{4.6}$$

and $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell)$ *be such that* $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$ *for* $i = 1, \ldots, \ell$. *Then*

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \binom{k+1}{2} - g$$

where $k := \dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$.

Proof. Let

$$B = \left\{ x^i y^j : \delta_{QH}(x^i y^j) \in S[\mathcal{P}] \right\}$$

and

$$B_t = \left\{ x^{a_m} y^{b_m} + \eta_m x^{u+r_m} y^{v+s_m} : m = 1, \ldots, \ell \right\}.$$

Then

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = ev_{QH}\langle B \cup B_t \rangle$$

and

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 = ev_{QH}\langle (B \cup B_t)^{\underline{2}} \rangle.$$

Note that $B \cup B_t$ is a set of functions with distinct pole orders. We claim that $(B \cup B_t)^{\underline{2}}$ is

a linearly independent set. Consider

$$f_m := x^{i_m} y^{j_m} \in B$$

and

$$f'_m := x^{a_m} y^{b_m} + \eta_m x^{u+r_m} y^{v+s_m} \in B_t.$$

Then $(B \cup B_t)^{\underline{2}}$ can be written as

$$(B \cup B_t)^{\underline{2}} = A \cup C \cup D$$

where

$$A := \{ f_m f_{m'} : \delta_{QH}(f_m), \delta_{QH}(f_{m'}) \in S[\mathcal{P}] \},$$

$$C := \{ f_m f'_{m'} : \delta_{QH}(f_m) \in S[\mathcal{P}], m' = 1, \ldots, \ell \},$$

and

$$D := \{ f'_m f'_{m'} : m, m' = 1, \ldots, \ell \}.$$

Notice that if

$$\delta_{QH}(x^{i+i'} y^{j+j'}) = \delta_{QH}(x^{i''+i'''} y^{j''+j'''})$$

for $x^{i+i'} y^{j+j'}, x^{i''+i'''} y^{j''+j'''} \in A$, then

$$\delta_{QH}(x^i y^j) = \delta_{QH}(x^{i''} y^{j''})$$

(in which case $\delta_{QH}(x^{i'} y^{j'}) = \delta_{QH}(x^{i'''} y^{j'''})$) or

$$\delta_{QH}(x^i y^j) = \delta_{QH}(x^{i'''} y^{j'''})$$

(in which case $\delta_{QH}(x^{i'}y^{j'}) = \delta_{QH}(x^{i''}y^{j''})$) follows from the properties of the Sidon set. In the first case, this fact implies that $i = i''$ and $j = j''$. In the second, $i = i'''$ and $j = j'''$. As a result, all elements of A have distinct pole orders. Furthermore, no pole order of an element of A is that of an element of C or D as

$$\delta_{QH}(f_m f_{m'}) \leq \alpha \leq \delta_{QH}(f)$$

for all $f_m f_{m'} \in A$ and $f \in C \cup D$. Continuing in this way, we see that

$$\begin{aligned} \mid (B \cup B_t)^{\underline{2}} \mid &= \binom{\mid B \mid + \mid B_t \mid +1}{2} \\ &= \binom{k+1}{2} \end{aligned}$$

and

$$\mid \delta_{QH}\left((B \cup B_t)\right)^{\underline{2}} \setminus \delta_{QH}\left(\mathcal{M}\right) \mid \leq g$$

which implies that at most g elements of $\delta_{QH}\left(B \cup B_t\right)^{\underline{2}}$ are not in $\mathcal{M}$. Then at least $\binom{k+1}{2} - g$ elements of $\delta_{QH}\left((B \cup B_t)^{\underline{2}}\right)$ lie in $\mathcal{M}$; i.e.,

$$\dim ev_{QH}\langle (B \cup B_t)^{\underline{2}} \rangle \geq \binom{k+1}{2} - g.$$

Thus,

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \binom{k+1}{2} - g.$$

□

This particular subfamily achieves a large Schur square dimension by first maximizing the size of $\overline{D}$ as seen in Theorem 4.9 and then forcing linear independence by choosing coefficients according to the nested field structure shown in equation 4.6.

4.3 Twisted norm-trace codes

Norm-trace are studied because they can have better code parameters (such as rate or relative distance) as compared to those of the Hermitian code. In this section, we look at the twisted norm-trace codes which offer similar advantages over the twisted Hermitian codes. Consider the set

$$B(\alpha P_\infty) := \left\{ x^i y^j : i, j \in \mathbb{N}, j \leq q^{r-1} - 1, \delta_{NT}(x^i y^j) \leq \alpha \right\},$$

and the vector space $\mathcal{L}(\alpha P_\infty) := \langle B(\alpha P_\infty) \rangle$ from the norm-trace curve

$$\mathcal{X}_q^r : y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^{\frac{q^r-1}{q-1}}$$

where $r \in \mathbb{N}$. Let

$$\alpha = u(q^{r-1}) + v\left(\frac{q^r-1}{q-1}\right) \geq (q^{r-1}-1)\left(\frac{q^r-1}{q-1} - 1\right) - 1$$

where $u, v \in \mathbb{N}$. Let $\ell \in \mathbb{Z}^+$,

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2\right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of nonzero integers, and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell$$

be a vector whose coordinates are ℓ pairwise distinct ordered pairs of integers satisfying

$$a_k(q^{r-1}) + b_k\left(\frac{q^r-1}{q-1}\right) \leq u(q^{r-1}) + v\left(\frac{q^r-1}{q-1}\right) < (u+r_k)(q^{r-1}) + (v+s_k)\left(\frac{q^r-1}{q-1}\right) < q^{2r-1}$$

for $k = 1, \ldots, \ell$. Let $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell) \in (\mathbb{F}_{q^r} \setminus \{0\})^\ell$. The set of $(\mathbf{t}, \mathbf{h}, \boldsymbol{\eta})$-twisted bivariate polynomials is

$$B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \left(B(\alpha P_\infty) \setminus \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} \right\} \right) \cup \bigcup_{k=1}^{\ell} \left\{ x^{a_k} y^{b_k} + \eta_k x^{u+r_k} y^{v+s_k} \right\}.$$

Let $\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \langle B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \rangle$. The twisted norm-trace code $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ is

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) := ev_{NT}\left(\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}\right) \subseteq \mathbb{F}_{q^r}^n.$$

Note that $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ has the same length as the one-point norm-trace code $\mathcal{C}(\alpha P_\infty)$. The dimension of the twisted norm-trace code is

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \dim \mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = |B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)| = |B(\alpha P_\infty)| = \dim \mathcal{C}(\alpha P_\infty),$$

and a generator matrix of the twisted norm-trace code is

$$\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \begin{bmatrix} ev_{NT}(f_1) \\ ev_{NT}(f_2) \\ \vdots \\ ev_{NT}(f_k) \end{bmatrix}$$

where $B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = \langle f_1, f_2, \ldots, f_k \rangle$. Let us consider an example of twisted norm-trace code.

Example 4.12. Let $q = 2$, $r = 3$ and $\alpha = 2(q^{r-1}) + 1 \left(\frac{q^r - 1}{q - 1} \right) = 15$. Consider the norm-trace curve $\mathcal{X}_2^3 : y^4 + y^2 + y = x^7$ over a finite field of order $q^3 = 8$, $\mathbb{F}_8 = \{0, 1, a, a+1, a^2, a^2+1, a^2+a, a^2+a+1\} \cong \mathbb{Z}_2[x]/\langle x^3+x+1 \rangle$. Consider the set

$$B(15P_\infty) = \{1, x, y, x^2, y^2, x^3, xy, x^2 y\}.$$

The $q^{2r-1} = 32$ affine rational points on $\mathcal{X}_2^3$ are:

$$
\begin{aligned}
P_1 &= (0:0:1)\\
P_2 &= (0:a:1)\\
P_3 &= (0:a^2:1)\\
P_4 &= (0:a^2+a:1)\\
P_5 &= (1:1:1)\\
P_6 &= (1:a+1:1)\\
P_7 &= (1:a^2+1:1)\\
P_8 &= (1:a^2+a+1:1)\\
P_9 &= (a:1:1)\\
P_{10} &= (a:a+1:1)\\
P_{11} &= (a:a^2+1:1)\\
P_{12} &= (a:a^2+a+1:1)\\
P_{13} &= (a+1:1:1)\\
P_{14} &= (a+1:a+1:1)\\
P_{15} &= (a+1:a^2+1:1)\\
P_{16} &= (a+1:a^2+a+1:1)\\
P_{17} &= (a^2:1:1)\\
P_{18} &= (a^2:a+1:1)\\
P_{19} &= (a^2:a^2+1:1)\\
P_{20} &= (a^2:a^2+a+1:1)\\
P_{21} &= (a^2+1:1:1)\\
P_{22} &= (a^2+1:a+1:1)\\
P_{23} &= (a^2+1:a^2+1:1)\\
P_{24} &= (a^2+1:a^2+a+1:1)\\
P_{25} &= (a^2+a:1:1)
\end{aligned}
$$

$$\begin{aligned}
P_{26} &= (a^2+a : a+1 : 1) \\
P_{27} &= (a^2+a : a^2+1 : 1) \\
P_{28} &= (a^2+a : a^2+a+1 : 1) \\
P_{29} &= (a^2+a+1 : 1 : 1) \\
P_{30} &= (a^2+a+1 : a+1 : 1) \\
P_{31} &= (a^2+a+1 : a^2+1 : 1) \\
P_{32} &= (a^2+a+1 : a^2+a+1 : 1).
\end{aligned}$$

Let $\ell = 2$,

$$\mathbf{t} = ((1,0),(2,0)),$$

$$\mathbf{h} = ((2,0),(1,1)),$$

and

$$\boldsymbol{\eta} = (1, a).$$

Then

$$\bigcup_{k=1}^{2} \{x^{a_k} y^{b_k}\} = \{x^2, xy\},$$

and

$$\bigcup_{k=1}^{2} \{x^{a_k} y^{b_k} + \eta_k x^{u+r_k} y^{v+s_k}\} = \{x^2 + x^2 y, xy + ax^3 y\}$$

so that

$$B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty) = \{1, x, y, x^2 + x^2 y, y^2, x^3, xy + ax^3 y, x^2 y\}.$$

We get the following vector space by applying ev_{NT} to $B(15P_\infty)$:

$$\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty) = \langle B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty)\rangle.$$

The resulting twisted norm-trace code is

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty) = ev_{NT}\left(\mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty)\right).$$

A generator matrix $\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty)$ for the twisted norm-trace code may be obtained by evaluating each element of $B_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty)$ at each of the P_i, $1 \leq i \leq 32$, to obtain, to obtain $\mathcal{G}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty) =$

$$\begin{array}{c}
\begin{array}{cccccccccccccccccccccccccccccccc}
 & P_1 & P_2 & P_3 & P_4 & P_5 & P_6 & P_7 & P_8 & P_9 & P_{10} & P_{11} & P_{12} & P_{13} & P_{14} & P_{15} & P_{16} & P_{17} & P_{18} & P_{19} & P_{20} & P_{21} & P_{22} & P_{23} & P_{24} & P_{25} & P_{26} & P_{27} & P_{28} & P_{29} & P_{30} & P_{31} & P_{32}
\end{array} \\
\begin{array}{c} 1 \\ x \\ y \\ x^2+x^2y \\ y^2 \\ x^3 \\ xy+ax^2y \\ x^2y \end{array}
\left[\begin{array}{cccccccccccccccccccccccccccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & a & a & a & a & a+1 & a+1 & a+1 & a+1 & a^2 & a^2 & a^2 & a^2 & a^2+1 & a^2+1 & a^2+1 & a^2+1 & a^2+a & a^2+a & a^2+a & a^2+a & a^2+a+1 & a^2+a+1 & a^2+a+1 & a^2+a+1 \\
0 & a & a^2 & a^2+a & 1 & a+1 & a^2+1 & a^2+a+1 & 1 & a+1 & a^2+1 & a^2+a+1 & 1 & a+1 & a^2+1 & a^2+a+1 & 1 & a+1 & a^2+1 & a^2+a+1 & 1 & a+1 & a^2+1 & a^2+a+1 & 1 & a+1 & a^2+1 & a^2+a+1 & & & & \\
0 & 0 & 0 & 0 & 0 & a & a^2 & a^2+a & 0 & a+1 & a^2+a & 0 & a^2 & 1 & a & a+1 & 0 & a^2+a+1 & a^2+1 & a & 0 & a^2+1 & 1 & a^2 & 0 & a^2 & a+1 & a^2+a+1 & 0 & a^2+a & a^2+a+1 & 1 \\
0 & a^2 & a^2+a & a & 1 & a^2+1 & a & a+1 & 1 & a^2+1 & a & a+1 & 1 & a^2+1 & a & a+1 & 1 & a^2+1 & a & a+1 & 1 & a^2+1 & a & a+1 & 1 & a^2+1 & a & a+1 & & & & \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & a+1 & a+1 & a+1 & a+1 & a & a & a & a & a & a^2+1 & a^2+1 & a^2+1 & a^2+1 & a^2 & a^2 & a^2 & a^2 & a^2+a+1 & a^2+a+1 & a^2+a+1 & a^2+a+1 & a^2+a & a^2+a & a^2+a & a^2+a \\
0 & 0 & 0 & 0 & a+1 & a^2+1 & a^2 & 1 & a^2 & a^2+a+1 & a & 1 & 0 & 1 & a^2+a & a+1 & a^2+1 & a^2 & a+1 & a^2+a & a^2+a & 1 & a+1 & a^2 & a+1 & a^2+1 & a^2 & a & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & a+1 & a^2+1 & a^2+a+1 & a^2 & a^2+a+1 & a & a^2 & a^2+1 & a^2 & a^2+a+1 & a^2+a & a^2+a & 1 & a+1 & a^2 & a^2+a+1 & a & a^2+a & a+1 & a & a^2+a & 1 & a^2+1 & a+1 & a^2+1 & a^2 & a
\end{array}\right]
\end{array}$$

However, twisted norm-trace codes differ from norm-trace codes. They have the same length and dimension. However, the distinction can be shown by considering the largest norm-trace code containing the twisted norm-trace code and the smallest norm-trace code contained in the twisted norm-trace code. Note that

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2\right)^\ell$$

and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2\right)^\ell.$$

Let

$$\alpha' = \min\left\{a_i q^{r-1} + b_i\left(\frac{q^r - 1}{q-1}\right) : i = 1, \ldots, \ell\right\} - 1$$

and

$$\alpha'' = \alpha + \max\left\{ r_i q^{r-1} + s_i \left(\frac{q^r - 1}{q-1} \right) : i = 1, \ldots, \ell \right\}.$$

Then

$$\mathcal{L}(\alpha' P_\infty) \subseteq \mathcal{L}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subseteq \mathcal{L}(\alpha'' P_\infty)$$

and

$$\mathcal{C}(\alpha' P_\infty) \subseteq \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subseteq \mathcal{C}(\alpha'' P_\infty).$$

Furthermore, $\dim \mathcal{C}(\alpha' P_\infty) =$

$$\left| \left\{ x^i y^j \in B(\alpha P_\infty) \mid \delta_{NT}(x^i y^j) < \min\left\{ a_i q^{r-1} + b_i \left(\frac{q^r - 1}{q-1} \right) : i = 1, \ldots, \ell \right\} \right\} \right| < k,$$

and

$$a_k q^{r-1} + b_k \left(\frac{q^r - 1}{q-1} \right) \leq u q^{r-1} + v \left(\frac{q^r - 1}{q-1} \right)$$

for all $1 \leq k \leq l$, and the (a_k, b_k) are distinct, and

$$\dim \mathcal{C}(\alpha'' P_\infty) = \left(\alpha + \max\left\{ r_k q^{r-1} + s_k \left(\frac{q^r - 1}{q-1} \right) \mid k = 1, \ldots, \ell \right\} \right) + 1 - g \geq k + q.$$

This shows that twisted norm-trace codes are not norm-trace codes. This observation helps in determining bounds on the minimum distance of twisted norm-trace codes.

Consider a twisted norm-trace code $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ with

$$\mathbf{t} = ((r_1, s_1), \ldots, (r_\ell, s_\ell)) \in \left((\mathbb{Z} \setminus \{0\})^2 \right)^\ell$$

and

$$\mathbf{h} = ((a_1, b_1), \ldots, (a_\ell, b_\ell)) \in \left(\mathbb{Z}^2 \right)^\ell.$$

Then

$$\mathcal{C}(\alpha' P_\infty) \subsetneqq \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) \subsetneqq \mathcal{C}(\alpha'' P_\infty)$$

where

$$\alpha' = \min\left\{ a_i q^{r-1} + b_i \left(\frac{q^r - 1}{q-1} \right) : i = 1, \ldots, \ell \right\} - 1$$

and

$$\alpha'' = \alpha + \max\left\{ r_i q^{r-1} + s_i \left(\frac{q^r - 1}{q-1} \right) : i = 1, \ldots, \ell \right\}.$$

In the case that $2g - 2 < \alpha'$ and $\alpha'' < n$, as given in [22] we have that

$$n - \alpha'' \leq d(\mathcal{C}(\alpha'' P_\infty)) \leq n - \alpha'.$$

Therefore, the minimum distance d of $\mathcal{C}^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ satisfies

$$n - \alpha'' \leq d\left(\mathcal{C}(\alpha'' P_\infty)\right) \leq d \leq d\left(\mathcal{C}(\alpha' P_\infty)\right).$$

Example 4.13. Consider the twisted norm-trace code $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty)$ with $q = 2$, $r = 3$, $\alpha = 15$,

$$\begin{aligned} \mathbf{t} &= ((1,0),(0,1)), \\ \mathbf{h} &= ((1,2),(0,3)), \end{aligned}$$

and $\boldsymbol{\eta} = (\eta_1, \eta_2)$, where $\eta_1, \eta_2 \in \mathbb{F}_8$. Then

$$\alpha'' = 15 + \max\left\{ r_i q^{r-1} + s_i \left(\frac{q^r - 1}{q-1} \right) : i = 1, 2 \right\} = 22$$

and

$$\alpha' = \min\left\{ a_i q^{r-1} + b_i \left(\frac{q^r - 1}{q-1} \right) : i = 1, 2 \right\} - 1 = 17$$

from which it follows that

$$\mathcal{C}(17P_\infty) \subsetneqq \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty) \subsetneqq \mathcal{C}(22P_\infty).$$

According to [32, Theorem 2.2.2], $d\left(\mathcal{C}(17P_\infty)\right) = 15$ and $d\left(\mathcal{C}(22P_\infty)\right) = 10$ so that

$$10 \leq d\left(\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(15P_\infty)\right) \leq 15.$$

We now show that the twisted norm-trace code $\mathcal{C}^{n,k}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ may have a Schur square with much larger dimension in comparison to the square of the code itself. Consider the set of bivariate polynomials

$$\mathcal{M} := \left\{x^i y^j : i,j \in \mathbb{N}, 0 \leq i \leq q^{r-1}-1, 0 \leq j \leq q^r - 1\right\} \subseteq \mathbb{F}_{q^r}[x,y].$$

Let the domain of ev_{NT} be restricted to $\langle \mathcal{M} \rangle$ as described above. Assume that $0 \neq p(x,y) \in \langle \mathcal{M} \rangle$ such that $ev_{NT}(p(x,y)) = \mathbf{0} \in \mathbb{F}_{q^r}^n$. Then every rational affine point $(x : y : 1)$ of the norm-trace curve $\mathcal{X}_q^r$ also satisfies $p(x,y) = 0$. Fix $a \in \mathbb{F}_{q^r}$. Then there are then q^{r-1} distinct $b_i \in \mathbb{F}_{q^r}$ such that $(a : b_i : 1)$ is a rational point on the norm-trace curve $\mathcal{X}_q^r$. Then the univariate polynomial $p(a,y)$ has q^{r-1} distinct zeros in $\mathbb{F}_{q^r}$, despite the fact that $\deg(p(a,y)) \leq q^{r-1}-1$. Hence $p(a,y) \equiv 0$ for all $a \in \mathbb{F}_{q^r}$. On the other hand,

$$p(x,y) = \sum_{j=0}^{q^{r-1}-1} \left(\sum_{i=0}^{q^r-1} a_{ij} x^i \right) y^j = \sum_{j=0}^{q^{r-1}-1} q_j(x) y^j$$

where $q_j(x) = \sum_{i=0}^{q^r-1} a_{ij} x^i$ and $q_j(a) = 0$ for all $a \in \mathbb{F}_{q^r}$. This implies the univariate polynomial $q_j(x)$ has q^r zeros in $\mathbb{F}_{q^r}^n$, despite the fact that $\deg(q_j) \leq q^r - 1$. As a result, $p(x,y) \equiv 0$, which is a contradiction. Then the evaluation map $ev_{NT} : \langle \mathcal{M} \rangle \to \mathbb{F}_{q^r}^n$ is an

injective mapping.

Definition 4.14. Suppose $i, j \in \mathbb{N}$ are such that $0 \leq i \leq 2(q^r - 1)$ and $0 \leq j \leq q^{r-1} - 1$. We define

$$\overline{x^i y^j} := \begin{cases} x^i y^j & \text{if } 0 \leq i \leq q^r - 1 \\ x^{i-(q^r-1)} y^j & \text{otherwise.} \end{cases}$$

For $f(x,y) = \sum c_k x^{i_k} y^{j_k} \in \mathbb{F}_{q^r}[x,y]$, we define

$$\overline{f} := \sum c_k \overline{x^{i_k} y^{j_k}}. \tag{4.7}$$

It follows immediately that for $f = \sum c_k x^{i_k} y^{j_k}$ and $g = \sum d_h x^{i_h} y^{j_h} \in \mathcal{L}(\alpha P_\infty)$,

$$ev_{NT}(f \cdot g) = ev_{NT}(\overline{f \cdot g}).$$

Given $f(x,y) = \sum_{k=1}^{n} c_k x^{i_k} y^{j_k} \in \mathbb{F}_{q^r}[x,y]$,

$$\delta_{NT}(f) := \max\left\{ i_k q^{r-1} + j_k \left(\frac{q^r - 1}{q - 1} \right) : k = 1, \ldots, n \right\}. \tag{4.8}$$

If $B = \{f_1, \ldots, f_m\} \subseteq \mathbb{F}_{q^r}[x,y]$, then

$$\delta_{NT}(B) := \{\delta_{NT}(f_k) : k = 1, \ldots, m\}. \tag{4.9}$$

Lemma 4.15. *Let $\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$ be a twisted norm-trace code. Then*

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq | \overline{D} |$$

where $\overline{D} := \{\delta_{NT}(\overline{f \cdot g}) \mid f, g \in \mathcal{L}(\alpha P_\infty)\}$.

Note that $\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2$ can be made large by choosing $\mathbf{t}, \mathbf{h}, \boldsymbol{\eta}$ to maximize the size of $\overline{D}$.

Given $\mathcal{M} = \{x^i y^j : i, j \in \mathbb{N}, 0 \leq i \leq q^{r-1} - 1, 0 \leq j \leq q^r - 1\}$, set

$$\mathcal{M}_2 := \left\{ x^i y^j \in \mathcal{M} : \delta_{NT}(x^i y^j) \leq \left\lceil \frac{\max \delta_{NT}(\mathcal{M})}{2} \right\rceil \right\}.$$

Observe that for any prime power q,

$$\left\lceil \frac{\max \delta_{NT}(\mathcal{M})}{2} \right\rceil = \left\lceil \frac{(q^r - 1)q^{r-1} + (q^{r-1} - 1)\left(\frac{q^r-1}{q-1}\right)}{2} \right\rceil \geq 2g + 1.$$

It follows that

$$\mathcal{M} \subseteq \mathcal{M}_2^{\underline{2}}.$$

We make use of this observation in the following lemma.

Lemma 4.16. *Let* $A \subseteq \mathbb{F}[x, y]$ *be a set of elements with distinct pole orders such that* $\delta_{NT}(A) \subseteq \delta_{NT}(\mathcal{M}_2)$. *Then* $\mid \delta_{NT}(A^{\underline{2}}) \setminus \delta_{NT}(\mathcal{M}) \mid \leq g$.

Proof. Since $\mathcal{M} \subseteq \mathcal{M}_2^{\underline{2}}$, $\delta_{NT}(\mathcal{M}) \subseteq \delta_{NT}(\mathcal{M}_2^{\underline{2}})$. Observe that

$$\begin{aligned} \mid \delta_{NT}(\mathcal{M}_2^{\underline{2}}) \setminus \delta_{NT}(\mathcal{M}) \mid &= \mid \delta_{NT}\left(\mathcal{M}_2^{\underline{2}}\right) \mid - \mid \delta_{NT}(\mathcal{M}) \mid \\ &= \left[(q^r - 1)q^{r-1} + (q^{r-1} - 1)\left(\frac{q^r - 1}{q - 1}\right) + 1 - g\right] - q^{2r-1} \\ &= g. \end{aligned}$$

Since $\delta_{NT}(A^{\underline{2}}) \subseteq \delta_{NT}(\mathcal{M}_2^{\underline{2}})$, it follows that $\mid (\delta_{NT}(A^{\underline{2}}) \setminus \delta_{NT}(\mathcal{M})) \mid \leq g$. □

Consider the map

$$\begin{array}{rccc} \phi_q: & \mathbb{N} & \to & \mathbb{Z}^2 \\ & w & \mapsto & (\left(\frac{q^r-1}{q-1}\right)\lfloor \frac{w}{q} \rfloor - w, w - q^{r-1}\lfloor \frac{w}{q} \rfloor). \end{array}$$

Theorem 4.17. *For a given prime power q_0, let $\alpha \in \delta_{NT}(\mathcal{M})$ be such that*

$$\alpha \leq \frac{q^{2r-1} + 2\sqrt{q^{2r-1}+1} + 1}{4}$$

and

$$\begin{aligned} \mathcal{P} &:= \left\{\delta_{NT}(x^i y^j) : x^i y^j \in \mathcal{M}, \delta_{NT}(x^i y^j) \leq \alpha\right\} \\ \mathcal{T} &:= \left\{\delta_{NT}(x^i y^j) : x^i y^j \in \mathcal{M}, \delta_{NT}(x^i y^j) > \alpha\right\} = \{t_1, \ldots, t_\ell\} \\ \mathcal{H} &:= \mathcal{P} \setminus S[\mathcal{P}] = \{h_1, \ldots, h_\ell\} \end{aligned}$$

satisfying $\ell :=\mid \mathcal{H} \mid \leq \mid \mathcal{T} \mid$. Let

$$\begin{aligned} \mathbf{h} &= (\phi(h_1), \ldots, \phi(h_\ell)); \\ \mathbf{t} &= (\phi(t_1) - (u,v), \ldots, \phi(t_\ell) - (u,v)); \end{aligned}$$

$s_1, \ldots, s_\ell$ be prime powers such that

$$\mathbb{F}_{q_0^r} = \mathbb{F}_{s_0} \subsetneqq \mathbb{F}_{s_1} \subsetneqq \cdots \subsetneqq \mathbb{F}_{s_\ell} = \mathbb{F}_{q^r}; \tag{4.10}$$

and $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_\ell)$ be such that $\eta_i \in \mathbb{F}_{s_i} \setminus \mathbb{F}_{s_{i-1}}$ for $i = 1, \ldots, \ell$. Then

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \binom{k+1}{2} - g$$

where $k := \dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)$.

Proof. Let

$$B = \left\{x^i y^j : \delta_{NT}(x^i y^j) \in S[\mathcal{P}]\right\}$$

and

$$B_t = \left\{x^{a_m} y^{b_m} + \eta_m x^{u+r_m} y^{v+s_m} : m = 1, \ldots, \ell\right\}.$$

Then

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty) = ev_{NT}\langle B \cup B_t\rangle$$

and

$$\mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 = ev_{NT}\langle (B \cup B_t)^{\underline{2}}\rangle.$$

Note that $B \cup B_t$ is a set of functions with distinct pole orders. We claim that $(B \cup B_t)^{\underline{2}}$ is a linearly independent set. Consider

$$f_m := x^{i_m} y^{j_m} \in B$$

and

$$f'_m := x^{a_m} y^{b_m} + \eta_m x^{u+r_m} y^{v+s_m} \in B_t.$$

Then $(B \cup B_t)^{\underline{2}}$ can be written as

$$(B \cup B_t)^{\underline{2}} = A \cup C \cup D$$

where

$$A := \{f_m f_{m'} : \delta_{NT}(f_m), \delta_{NT}(f_{m'}) \in S[\mathcal{P}]\},$$

$$C := \{f_m f'_{m'} : \delta_{NT}(f_m) \in S[\mathcal{P}], m' = 1, \ldots, \ell\},$$

and

$$D := \{f'_m f'_{m'} : m, m' = 1, \ldots, \ell\}.$$

Notice that if

$$\delta_{NT}(x^{i+i'}y^{j+j'}) = \delta_{NT}(x^{i''+i'''}y^{j''+j'''})$$

for $x^{i+i'}y^{j+j'}, x^{i''+i'''}y^{j''+j'''} \in A$, then

$$\delta_{NT}(x^i y^j) = \delta_{NT}(x^{i''}y^{j''})$$

(in which case $\delta_{NT}(x^{i'}y^{j'}) = \delta_{NT}(x^{i'''}y^{j'''})$) or

$$\delta_{NT}(x^i y^j) = \delta_{NT}(x^{i'''}y^{j'''})$$

(in which case $\delta_{NT}(x^{i'}y^{j'}) = \delta_{NT}(x^{i''}y^{j''})$) follows from the properties of the Sidon set. In the first case, this fact implies that $i = i''$ and $j = j''$. In the second, $i = i'''$ and $j = j'''$. As a result, all elements of A have distinct pole orders. Furthermore, no pole order of an element of A is that of an element of C or D as

$$\delta_{NT}(f_m f_{m'}) \leq \alpha \leq \delta_{NT}(f)$$

for all $f_m f_{m'} \in A$ and $f \in C \cup D$. Continuing in this way, we see that

$$\begin{aligned} \mid (B \cup B_t)^{\underline{2}} \mid &= \binom{\mid B \mid + \mid B_t \mid + 1}{2} \\ &= \binom{k+1}{2} \end{aligned}$$

and

$$\mid \delta_{NT}\left((B \cup B_t)\right)^{\underline{2}} \setminus \delta_{NT}\left(\mathcal{M}\right) \mid \leq g$$

which implies that at most g elements of $\delta_{NT}\left(B \cup B_t\right)^{\underline{2}}$ are not in $\mathcal{M}$. Then at least $\binom{k+1}{2} - g$ elements of $\delta_{NT}\left(\left(B \cup B_t\right)^{\underline{2}}\right)$ lie in $\mathcal{M}$; i.e.,

$$\dim ev_{NT}\langle (B \cup B_t)^{\underline{2}} \rangle \geq \binom{k+1}{2} - g.$$

Thus,

$$\dim \mathcal{C}_{\mathbf{t},\mathbf{h},\boldsymbol{\eta}}(\alpha P_\infty)^2 \geq \binom{k+1}{2} - g.$$

□

This particular subfamily achieves a large Schur square dimension by first maximizing the size of $\overline{D}$ as seen in Theorem 4.15 and then forcing linear independence by choosing coefficients according to the nested field structure shown in equation 4.10.

Chapter 5

Conclusions

This work studies error correction and erasure recovery in graph-based codes. Moreover, we design new family of algebraic geometry codes which can be possible replacements of Goppa codes in the McEliece cryptosystem.

In Chapter 2, we generalize the construction of standard to $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander codes. These codes are constructed using bipartite graphs and shorter codes, called inner codes. Given the minimum distance and rate of the inner codes, we determine lower bounds on the minimum distance and rate of $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander codes. Furthermore, we study the decoding abilities of $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander codes. We provide a linear-time decoding algorithm that corrects a constant fraction of errros and allows for any expansion factor.

Expander graphs are hard to construct. Some popular examples of regular expander graphs include Ramanujan graphs, Cayley graphs, etc. Explicit constructions of irregular expander graphs would provide more insights. Our algorithm uses a random choice of coordinates in the 'updating' step of the algorithm. We would like consider a structured approach while choosing coordinate assignment and its impact on the efficiency of the decoding algorithm.

We provide a worst-case analysis of the decoding algorithm. It would be interesting to study the efficiency of the decoding algorithm under an average-case analysis. There exist linear-time encoding algorithms have $(\mathfrak{c}, \mathfrak{d}, \gamma, \alpha)$ expander codes [1], [3], [4], [5], [6]. We are currently studying encoding algorithms for $(\mathfrak{C}, \mathfrak{D}, \gamma, \alpha)$ expander codes.

In Chapter 3, we study erasure recovery in Tanner codes: reviewing our independent results and including some results obtained in collaboration with Allison Beermer. We show that any locally recoverable code can be expressed as a modified Tanner code. We provide bounds on the locality and availability of modified Tanner codes when the inner codes are replaced with locally recoverable codes. Moreover, we show that in this setting the modified Tanner codes allow hierarchical local recovery. This analysis results in insights about the behaviour of stopping sets of modified Tanner codes.

We are curently comparing bounds on the locality and availability of modified Tanner codes where the underlying inner codes are locally recoverable codes, with the existing bounds on the locality and availability of existing locally recoverable code constructions.

In Chapter 4, we provide constructions of new algebraic geometry codes. We call them twisted algebraic geometry codes. In particular, we study properties of twisted Hermitian codes, twisted codes from a quotient of the Hermitian curve and twisted norm-trace codes. We show that these codes have Schur squares with high dimension and hence can be considered as suitable candidates to replace Goppa codes in the McEliece cryptosystem. Furthermore, we explicitly studied the code-based cryptosystem based on twisted Hermitian codes. We lay the foundations for an attack on a twisted Hermitian code-based cryptosystem.

We provide bounds on the minimum distance of twisted algebraic geometry codes in order to distinguish them from ordinary algebraic geometry codes. It would be interesting to provide better bounds on the minimum distance for twisted algebraic geometry codes and compare

them with the minimum distance of ordinary algebraic geometry codes. Given a code $\mathcal{C}$, it is said to have a linear complimentary dual if $\mathcal{C} \cap \mathcal{C}^{\perp} = \{0\}$. We are also interested in proving some of the conjectures used to show an attack on the code-based cryptosystem based on twisted Hermitian codes. Furthermore, we would like to study the code-based cryptosystem based on twisted codes from a quotient of the Hermitian curve and twisted norm-trace codes as well as attacks on these cryptosystems.

Bibliography

[1] M. Sipser and D. A. Spielman, "xpander codes", in IEEE Transactions on Information Theory, Vol. 42, No. 6, pp. 1710-1722, Nov. 1996, doi: 10.1109/18.556667.

[2] D. A. Spielman, "Linear-time encodable and decodable error-correcting codes", in IEEE Transactions on Information Theory, Vol. 42, No. 6, pp. 1723-1731, 1996.

[3] J. Feldman, T. Malkin, R. A. Servedio, C. Stein and M. J. Wainwright, "LP decoding corrects a constant fraction of errors", in IEEE Transactions on Information Theory, Vol. 53, No. 1, pp. 82–89, Jan. 2007.

[4] S. K. Chilappagari, D. V. Nguyen, B. Vasic and M. W. Marcellin, "On trapping sets and guaranteed error correction capability of LDPC codes and GLDPC codes", in IEEE Transactions on Information Theory, Vol. 56, No. 4, pp. 1600–1611, Apr. 2010.

[5] M. Viderman, "Linear-time decoding of regular expander codes", ACM Transactions and Computation Theory, Vol. 5, No. 3, pp. 10-1–10-25, Aug. 2013.

[6] M. Dowling and S. Gao, "Fast Decoding of Expander Codes", in IEEE Transactions of Information Theory, Vol. 64, No. 2, Feb 2018.

[7] T. Richardson, A. Shokrollahi and R. Urbanke, "Design of Capacity-Approaching Irreg-

ular Low-Density Parity-Check Codes", in IEEE Transactions of Information Theory, Vol. 47, No. 2, Feb 2001.

[8] M. Luby, M. Mitzenmacher, A. Shokrollahi, D. Spielman and V. Stemann, "Practical loss-resilient codes", in IEEE Transactions of Information Theory, Vol. 47, No. 2, Feb 2001.

[9] R. Kshirsagar, G. L. Matthews, "Linear-time Decoding of Irregular Expander Codes Correcting a Constant Fraction of Errors", Preprint.

[10] R. J. McEliece, "A public key cryptosystem based on algebraic coding theory", in Deep Space Network Progress Report, 1978, 44, 114–116..

[11] P. Gopalan, C. Huang, H. Simitci and S. Yekhanin, "On the Locality of Codeword Symbols", in IEEE Transactions on Information Theory, Vol. 58, No. 11, pp. 6925-6934, Nov. 2012, doi: 10.1109/TIT.2012.2208937.

[12] B. Sasidharan, G. K. Agarwal, and P. V. Kumar,"Codes with hierarchical locality", in Proceedings of IEEE International Symposium on Information Theory (ISIT), Hong Kong, Jun. 2015, pp. 1257–1261

[13] R. Pellikaan, "On decoding by error location and dependent sets of error positions", in Discrete Math, 1992, 106–107, 369–381.

[14] I. Cascudo, R. Cramer, D. Mirandola and G. Zémor, "Squares of Random Linear Codes," in IEEE Transactions on Information Theory, Vol. 61, No. 3, pp. 1159-1173, March 2015, doi: 10.1109/TIT.2015.2393251.

[15] I. Márquez-Corbella, E. Martínez-Moro and R. Pellikaan, "The non-gap sequence of a subcode of a generalized Reed-Solomon code", in Designs, Codes and Cryptography 66, 1–3 (January 2013), 317–333. DOI:https://doi.org/10.1007/

[16] P. Beelen, S. Puchinger and J. Rosenkilde né Nielsen, "Twisted Reed-Solomon codes", in IEEE International Symposium on Information Theory (ISIT), 2017, pp. 336-340, doi: 10.1109/ISIT.2017.8006545.

[17] J. Sheekey, "A new family of linear maximum rank distance codes", in Advances in Mathematics of Communications, 2016, 10, 475–488.

[18] J. Lv, R. Li and J. Wang, "Constructions of quasi-twisted quantum codes", in Quantum Information Processing, 2020, 19, 1–25.

[19] G. M. Kamath, N. Prakash, V. Lalitha and P. V. Kumar, "Codes With Local Regeneration and Erasure Correction", in IEEE Transactions on Information Theory, Vol. 60, No. 8, pp. 4637-4660, Aug. 2014, doi: 10.1109/TIT.2014.2329872.

[20] R. Tanner, "A recursive approach to low complexity codes", in IEEE Transactions on Information Theory, Vol. 27, No. 5, pp. 533-547, September 1981, doi: 10.1109/TIT.1981.1056404.

[21] T. Johnsen, S. Manshadi and N. Monzavi, "A determination of the parameters of a large class of Goppa codes", in IEEE Transactions on Information Theory, Vol. 40, No. 5, pp. 1678-1681, Sept. 1994, doi: 10.1109/18.333893.

[22] O. Geil, "On codes from norm-trace curves", in Finite Fields and Their Applications 9 (2003): 351-371.

[23] R. Gallager, "Low-density parity-check codes", in IEEE Transactions on Information Theory, Vol. 8, No. 1, pp. 21-28, January 1962, doi: 10.1109/TIT.1962.1057683.

[24] E. Berlekamp, R. McEliece and H. Van Tilborg, "On the inherent interactability of certain coding problems", in IEEE Transactions on Information Theory,1978, IT-24, 384–386.

[25] H. Janwa and O. Moreno, "McEliece public key cryptosystems using algebraic-geometric codes", in Designs, Codes and Cryptography,1996, 8, 293–307.

[26] I. S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields", in Journal of The Society for Industrial and Applied Mathematics, 8, (1960): 300-304.

[27] A. Couvreur, I. Márquez-Corbella and R. Pellikaan, "Cryptanalysis of McEliece cryptosystem based on algebraic geometry codes and their subcodes", in IEEE Transactions on Information Theory, 2017, 63, 5404–5418.

[28] J. Lavauzelle and J. Renner, "Cryptanalysis of a system based on twisted Reed-Solomon codes", in Designs, Codes and Cryptography, 2020, 88, 1285–1300.

[29] T. Høholdt, J. Lint and R. Pellikaan, "Algebraic geometry codes", in Handbook of Coding Theory", in MDPI Elsevier, Amsterdam, The Netherlands, 1998; Volume 1, pp. 871–961.

[30] H. Stichtenoth, "A note on Hermitian codes over GF(q^2)", in IEEE Transactions on Information Theory, 1988, 34, 1345–1348.

[31] A. Allen, K. Blackwell, O. Fiol, R. Kshirsagar, B. Matsick, G. L. Matthews, and Z. Nelson, "Twisted Hermitian Codes", in Mathematics 9, No. 1: 40, 2020. https://doi.org/10.3390/math9010040

[32] H. Stichtenoth,"Algebraic Function Fields and Codes", in 2nd ed., Springer: Berlin, Germany, 2008.

[33] S. Vladut, D. Nogin and M. Tsfasman, "Algebraic Geometric Codes: Basic Notions", in American Mathematical Society: Providence, RI, USA, 2007.

[34] R.B. Christensen and O. Geil, "On nested code pairs from the Hermitian curve", in Finite Fields Their Appl., 2020, 68, 101742.

[35] K.Yang and P.V. Kumar, "On the true minimum distance of Hermitian codes", in Coding Theory and Algebraic Geometry (Luminy, 1991), Volume 1518 of Lecture Notes in Mathematics; Springer: Berlin, Germany, 1992; pp. 99–107

[36] A. Couvreur, P. Gaborit, V. Gauthier-Umana, A. Otmani and J.-P. Tillich, "Distinguisher-based attacks on public-key cryptosystems using Reed-Solomon codes", in Designs, Codes and Cryptography, 2014, 73, 641–666.

[37] J. Bolkema, H. Gluesing-Luerssen, C.A. Kelley, K.E. Lauter, B. Malmskog and J. Rosenthal, "Variations of the McEliece cryptosystem", in Algebraic Geometry for Coding Theory and Cryptography, Volume 9 of Association for Women in Mathematics Series, Springer: Cham, Switzerland, 2017; pp. 129–150.

[38] R. Pellikaan and I. Márquez-Corbella, "Error-correcting pairs for a public-key cryptosystem", in Journal of Physics: Conference Series, 2017, 855, 012032.

[39] P. Beelen, M. Bossert, S. Puchinger and J. Rosenkilde, "Structural Properties of Twisted Reed-Solomon Codes with Applications to Cryptography", in IEEE International Symposium on Information Theory (ISIT), 2018, pp. 946-950, doi: 10.1109/ISIT.2018.8437923.

[40] Q. Cheng, S. Gao, J. M. Rojas and D. Wan, "Sparse univariate polynomials with many roots over finite fields", in Finite Fields and Their Applications, 2017, 46, 235–246.

[41] Z. Kelley, "Roots of sparse polynomials over a finite field", in LMS Journal of Computation and Mathematics, 2016, 19, 196–204.

[42] H. Liu and S. Liu, " New constructions of MDS twisted Reed-Solomon codes and LCD MDS codes", arXiv, 2020, arXiv:2008.03708.

[43] P. Erdos and P. Turan, "On a problem of Sidon in additive number theory, and on some related problems", in Journal of the London Mathematical Society, 1941, 16, 212–215.

[44] T. Gowers, "What are dense Sidon subsets of {1,2,...,n} like?", Available online: https://gowers.wordpress.com/2012/07/13/what-are-dense-sidon-subsets-of-12-n-like/ (accessed on 16 July 2018).

[45] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes", in Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280), 1998, pp. 28-37, doi: 10.1109/SFCS.1998.743426.

[46] J. S. R. Nielsen and P. Beelen, "Sub-Quadratic Decoding of One-Point Hermitian Codes", in IEEE Transactions on Information Theory, Vol. 61, No. 6, pp. 3225-3240, June 2015, doi: 10.1109/TIT.2015.2424415.

[47] C. Wieschebrink, "Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes", in Post-Quantum Cryptography, Springer: Berlin/Heidelberg, Germany, 2010; pp. 61–72.

[48] H. Niederreiter, "Knapsack-type cryptosystems and algebraic coding theory", in Problems of Control and Information Theory, 1986, 15(2):157–166

[49] I. Tamo, D. S. Papailiopoulos and A. G. Dimakis, "Optimal Locally Repairable Codes and Connections to Matroid Theory", in IEEE Transactions on Information Theory, Vol. 62, No. 12, pp. 6661-6671, Dec. 2016, doi: 10.1109/TIT.2016.2555813.

[50] B. Chen, S. Xia, J. Hao and F. Fu, "Constructions of Optimal Cyclic (r, δ) Locally Repairable Codes", in IEEE Transactions on Information Theory, Vol. 64, No. 4, pp. 2499-2511, April 2018, doi: 10.1109/TIT.2017.2761120.

[51] J. Liu, S. Mesnager and L. Chen, "New Constructions of Optimal Locally Recoverable Codes via Good Polynomials", in IEEE Transactions on Information Theory, Vol. 64, No. 2, pp. 889-899, Feb. 2018, doi: 10.1109/TIT.2017.2713245.

[52] I. Tamo and A. Barg, "A Family of Optimal Locally Recoverable Codes", in IEEE Transactions on Information Theory, Vol. 60, No. 8, pp. 4661-4676, Aug. 2014, doi: 10.1109/TIT.2014.2321280.

[53] B. Sasidharan, G. K. Agarwal and P. V. Kumar, "Codes with hierarchical locality", in IEEE International Symposium on Information Theory (ISIT), 2015, pp. 1257-1261, doi: 10.1109/ISIT.2015.7282657.

[54] N. Prakash, V. Lalitha, S. B. Balaji and P. V. Kumar, "Codes With Locality for Two Erasures", in IEEE Transactions on Information Theory, Vol. 65, No. 12, pp. 7771-7789, Dec. 2019, doi: 10.1109/TIT.2019.2934124.

[55] L. Pamies-Juarez, H. D. L. Hollmann and F. Oggier, "Locally repairable codes with multiple repair alternatives", in IEEE International Symposium on Information Theory, 2013, pp. 892-896, doi: 10.1109/ISIT.2013.6620355.

[56] P. Huang, E. Yaakobi and P. H. Siegel, "Multi-Erasure Locally Recoverable Codes Over Small Fields: A Tensor Product Approach", in IEEE Transactions on Information Theory, Vol. 66, No. 5, pp. 2609-2624, May 2020, doi: 10.1109/TIT.2019.2962012.

[57] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel", in IEEE Transactions on Information Theory, Vol. 48, No. 6, pp. 1570-1579, June 2002, doi: 10.1109/TIT.2002.1003839.

[58] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi and D. A. Spielman, "Efficient

erasure correcting codes", in IEEE Transactions on Information Theory, Vol. 47, No. 2, pp. 569-584, Feb 2001, doi: 10.1109/18.910575.

[59] C. A. Kelley and D. Sridhara, "Pseudocodewords of Tanner Graphs", in IEEE Transactions on Information Theory, Vol. 53, No. 11, pp. 4013-4038, Nov. 2007, doi: 10.1109/TIT.2007.907501.

[60] A. Orlitsky, R. Urbanke, K. Viswanathan and J. Zhang, "Stopping sets and the girth of Tanner graphs", in Proceedings IEEE International Symposium on Information Theory, 2002, pp. 2-, doi: 10.1109/ISIT.2002.1023274.

[61] A. Orlitsky, K. Viswanathan and J. Zhang, "Stopping set distribution of LDPC code ensembles", in IEEE Transactions on Information Theory, Vol. 51, No. 3, pp. 929-953, March 2005, doi: 10.1109/TIT.2004.842571.

[62] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes", in IEEE Transactions on Information Theory, Vol. 52, No. 3, pp. 922-932, March 2006, doi: 10.1109/TIT.2005.864441.

[63] A. Beemer, R. Kshirsagar and G. L. Matthews, "Graph-based codes for hierarchical recovery", Submitted to 2022 IEEE International Symposium on Information Theory (ISIT).